ROBIN ABERNATHY
TROY McMILLAN

Cert Guide

Learn, prepare, and practice for exam success

CISSP

Second Edition

PEARSON IT
CERTIFICATION

CISSP Cert Guide

Second Edition

Robin Abernathy
Troy McMillian

PEARSON

800 East 96th Street
Indianapolis, Indiana 46240 USA

CISSP Cert Guide, Second Edition

ISBN-13: 978-0-7897-5518-6
ISBN-10: 0-7897-5518-1

Library of Congress Control Number: 2016940246

Printed in the United States of America

First Printing: June 2016

Editor in Chief
Mark Taub

Acquisitions Editor
Michelle Newcomb

Senior Development Editor
Christopher Cleveland

Managing Editor
Sandra Schroeder

Project Editor
Mandie Frank

Copy Editor
Kitty Wilson

Indexer
Larry Sweazy

Proofreader
The Wordsmithery LLC

Technical Reviewers
Chris Crayton
Troy McMillan

Publishing Coordinator
Vanessa Evans

Cover Designer
Chuti Prasertsith

Compositor
Bronkella Publishing

Contents at a Glance

Table of Contents

About the Author

Robin M. Abernathy has been working in the IT certification preparation industry at Kaplan IT Certification Preparation, the owners of the Transcender and Self Test brands, for more than a decade. Robin has written and edited certification preparation materials for many $(ISC)^2$, Microsoft, CompTIA, PMI, Cisco, and ITIL certifications and holds multiple IT certifications from these vendors.

Robin provides training on computer hardware and software, networking, security, and project management. Over the past couple years, she has ventured into the traditional publishing industry by technically editing several publications and co-authoring Pearson's *CASP Cert Guide*. She presents at technical conferences and hosts webinars on IT certification topics.

Dedication

For my husband, Michael, and my son, Jonas. You are everything!

Acknowledgments

I would be remiss if I did not first of all mention my gratitude to God for blessing me throughout my life. I do nothing on my own. It is only through Him that I have the strength and wisdom to accomplish my goals.

When my father and his business partner asked me to take over a retail computer store in the mid-1990s, I had no idea that a BIG journey was just starting. So thanks, Wayne McDaniel (a.k.a. Dad) and Roy Green for seeing something in me that I didn't even see in myself and for taking a chance on a very green techie. Also, thanks to my mom, Lucille McDaniel, for supporting my career changes over the years, even if you didn't understand them. Thanks to Mike White for sharing your knowledge and giving me a basis on which to build my expertise over the coming years. Thanks to Zackie Bosarge, a great mentor, who gave me my first "real" job in the IT field at Alabama Institute for the Deaf and Blind.

Thanks also to my little family, my husband, Michael, and my son, Jonas. Thanks for being willing to have Friday night fun nights without me while I spent my extra time knee-deep in security topics. Thanks to Michael for always making sure I knew that everything was easier on a Mac. Thanks to Jonas for keeping mom humble by making sure she understood that you couldn't see why someone was paying mom to write a book where Percy Jackson or Harry Potter was NOT the main character. I love you both immensely!

Pearson has put together an outstanding team to help me on my journey. Thanks to everyone at Pearson for polishing my work so brilliantly. Thanks especially to Chris Crayton and Troy McMillan for completing such thorough reviews of my work and even managing to make some great suggestions!

It is my wish that you, the reader, succeed in your IT certification and career goals. I wish you the very best.

About the Technical Reviewers

Chris Crayton, MCSE, is an author, technical consultant, and trainer. Formerly, he 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 teaching awards, and has served as a state-level SkillsUSA competition judge.

Troy McMillan writes practice tests, study guides, and online course materials for Kaplan IT Cert Prep, while also running his own consulting and training business. He holds over 30 industry certifications and also appears in training videos for Oncourse Learning and Pearson Press. Troy can be reached at mcmillantroy@hotmail.com.

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 or write 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: feedback@pearsonitcertification.com

Mail: Pearson IT Certification
ATTN: Reader Feedback
800 East 96th Street
Indianapolis, IN 46240 USA

Reader Services

Register your copy of *CISSP 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 9780789755186 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

Book Features and Exam Preparation Methods

This book uses several key methodologies to help you discover the exam topics on which you need more review, to help you fully understand and remember those details, and to help you prove to yourself that you have retained your knowledge of those topics. Therefore, this book does not try to help you pass the exams only by memorization but by truly learning and understanding the topics.

The book includes many features that provide different ways to study so you can be ready for the exam. If you understand a topic when you read it, but do not study it any further, you probably will not be ready to pass the exam with confidence. The features included in this book give you tools that help you determine what you know, review what you know, better learn what you don't know, and be well prepared for the exam. These tools include

- **Foundation Topics:** These are the core sections of each chapter. They explain the protocols, concepts, and configuration for the topics in that chapter.
- **Exam Preparation Tasks:** These sections list a series of study activities that should be done after reading the Foundation Topics section. Each chapter includes the activities that make the most sense for studying the topics in that chapter. The activities include
- **Key Topics Review:** The Key Topic icon appears next to the most important items in the Foundation Topics section of the chapter. The Key Topics Review activity lists the key topics from the chapter and their page numbers. Although the contents of the entire chapter could be on the exam, you should definitely know the information listed in each key topic. Review these topics carefully.
- **Definition of Key Terms:** Although certification exams might be unlikely to ask a question such as "Define this term," the CISSP exam requires you to learn and know a lot of terminology. This section lists some of the most important terms from the chapter, asking you to write a short definition and compare your answer to the Glossary.
- **End of Chapter Review Questions:** Confirm that you understand the content that you just covered.

Companion Website

Register this book to get access to the Pearson IT Certification test engine 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 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: 9780789755186
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.

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 these steps, visit www.pearsonITcertification.com/contact and select the Site Problems/Comments option. Our customer service representatives will assist you.

Pearson IT Certification Practice Test Engine and Questions

The companion website includes the Pearson IT Certification Practice Test engine—software that displays and grades a set of exam-realistic multiple-choice questions. Using the Pearson IT Certification Practice Test engine, you can either study by going through the questions in Study Mode or take a simulated exam that mimics real exam conditions. You can also serve up questions in a Flash Card Mode, which displays just the question and no answer, challenging you to state the answer in your own words before checking the actual answer to verify your work.

The installation process requires two major steps: installing the software and then activating the exam. The website has a recent copy of the Pearson IT Certification Practice Test engine. The practice exam (the database of exam questions) is not on this site.

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

Install the Software

The Pearson IT Certification Practice Test is a Windows-only desktop application. You can run it on a Mac using a Windows virtual machine, but it was built specifically for the PC platform. The minimum system requirements are as follows:

- Windows 10, Windows 8.1, Windows 7, or Windows 8
- Microsoft .NET Framework 4.0 Client
- Pentium-class 1 GHz processor (or equivalent)
- 512 MB RAM
- 650 MB disk space plus 50 MB for each downloaded practice exam
- Access to the Internet to register and download exam databases

The software installation process is routine as compared with other software installation processes. If you have already installed the Pearson IT Certification Practice Test software from another Pearson product, there is no need for you to reinstall the software. Simply launch the software on your desktop and proceed to activate the practice exam from this book by using the activation code included in the cardboard sleeve.

The following steps outline the installation process:

1. Download the exam practice test engine from the companion site.
2. Respond to Windows prompts as with any typical software installation process.

The installation process gives you the option to activate your exam with the activation code supplied on the paper in the cardboard sleeve. This process requires that you establish a Pearson website login. You need this login to activate the exam, so please do register when prompted. If you already have a Pearson website login, there is no need to register again. Just use your existing login.

Activate and Download the Practice Exam

Once the exam engine is installed, you should then activate the exam associated with this book (if you did not do so during the installation process) as follows:

1. Start the Pearson IT Certification Practice Test software from the Windows Start menu or from your desktop shortcut icon.
2. To activate and download the exam associated with this book, from the My Products or Tools tab, click the **Activate Exam** button.

3. At the next screen, enter the activation key from the paper inside the cardboard sleeve in the back of the book. Once entered, click the **Activate** button.
4. The activation process downloads the practice exam. Click **Next**, and then click **Finish**.

When the activation process completes, the My Products tab should list your new exam. If you do not see the exam, make sure that you have selected the **My Products** tab on the menu. At this point, the software and practice exam are ready to use. Simply select the exam and click the **Open Exam** button.

To update a particular exam you have already activated and downloaded, display the **Tools** tab and click the **Update Products** button. Updating your exams ensures that you have the latest changes and updates to the exam data.

If you want to check for updates to the Pearson Certification Practice Test exam engine software, display the **Tools** tab and click the **Update Application** button. You can then ensure that you are running the latest version of the software engine.

Activating Other Exams

The exam software installation process and the registration process, only have to happen once. Then, for each new exam, only a few steps are required. For instance, if you buy another Pearson IT Certification Cert Guide, extract the activation code from the cardboard sleeve in the back of that book; you do not even need the exam engine at this point. From there, all you have to do is start the exam engine (if not still up and running) and perform steps 2 through 4 from the previous list.

Assessing Exam Readiness

Exam candidates never really know whether they are adequately prepared for the exam until they have completed about 30% of the questions. At that point, if you are not prepared, it is too late. It is best to work your way through the entire book unless you can complete each subject without having to do any research or look up any answers.

Premium Edition eBook and Practice Tests

This book also includes an exclusive offer for 70% off the Premium Edition eBook and Practice Tests edition of this title. See the coupon code included with the cardboard sleeve for information on how to purchase the Premium Edition.

This page intentionally left blank

This Introduction covers the following subjects:

- **The Goals of the CISSP Certification:** Describes the sponsoring bodies and the stated goals of the certification.
- **The Value of the CISSP Certification:** Examines the career and business drivers that comprise the value of the certification.
- **The Common Body of Knowledge:** Lists the eight domains of information that make up the topics covered in the certification.
- **Steps to Becoming a CISSP**: Describes the process involved in achieving CISSP certification.

Certified Information Systems Security Professional (CISSP) is one of the most respected and sought-after security certifications available today. It is a globally recognized credential which demonstrates that the holder has knowledge and skills across a broad range of security topics.

The CISSP Certification

As the number of security threats to organizations grows and the nature of these threats broaden, companies large and small have realized that security can no longer be an afterthought. It must be built into the DNA of the enterprise to be successful. This requires trained professionals being versed not only in technology security but all aspects of security. It also requires a holistic approach to protecting the enterprise.

Security today is no longer a one-size-fits-all proposition. The CISSP credential is a way security professionals can demonstrate the ability to design, implement, and maintain the correct security posture for an organization, based on the complex environments in which today's organizations exist.

The Goals of the CISSP Certification

The CISSP certification is created and managed by one of the most prestigious security organizations in the world and has a number of stated goals. Although not critical for passing the exam, having knowledge of the organization and of these goals is helpful in understanding the motivation behind the creation of the exam.

Sponsoring Bodies

The CISSP is created and maintained by the International Information Systems Security Certification Consortium $(ISC)^2$. The $(ISC)^2$ is a global not-for-profit organization that provides both a vendor-neutral certification process and supporting educational materials.

The CISSP is one of a number of security-related certifications offered by $(ISC)^2$. Other certifications offered by this organization include the following:

- Systems Security Certified Practitioner (SSCP)
- Certified Authorization Professional (CAP)
- Certified Secure Software Lifecycle Professional (CSSLP)

Several additional versions of the CISSP are offered that focus in particular areas:

- CISSP-Information Systems Security Architecture Professional (CISSP-ISSAP)
- CISSP-Information Systems Security Engineering Professional (CISSP-ISSEP)
- CISSP-Information Systems Security Management Professional (CISSP-ISSMP)

$(ISC)^2$ derives some of its prestige from the fact that it was the first security certification body to meet the requirements set forth by ANSI/ISO/IEC Standard 17024, a global benchmark for personnel certification. This ensures that certifications offered by this organization are both highly respected and sought after.

Stated Goals

The goal of $(ISC)^2$, operating through its administration of the CISSP certification, is to provide a reliable instrument to measure an individual's knowledge of security. This knowledge is not limited to technology issues alone but extends to all aspects of security that face an organization.

In that regard, the topics are technically more shallow than those tested by some other security certifications, while also covering a much wider range of issues than those other certifications. Later in this section, the topics that comprise the eight domains of knowledge are covered in detail, but it is a wide range of topics. This vast breadth of knowledge and the experience needed to pass the exam are what set the CISSP certification apart.

The Value of the CISSP Certification

The CISSP certification holds value for both the exam candidate and the enterprise. This certification is routinely in the top 10 of yearly lists that rank the relative demand for various IT certifications.

To the Security Professional

Numerous reasons exist for why a security professional would spend the time and effort required to achieve this credential:

- To meet growing demand for security professionals
- To become more marketable in an increasingly competitive job market
- To enhance skills in a current job

- To qualify for or compete more successfully for a promotion
- To increase salary

In short, this certification demonstrates that the holder not only has the knowledge and skills tested in the exam but also that the candidate has the wherewithal to plan and implement a study plan that addresses an unusually broad range of security topics.

To the Enterprise

For an organization, the CISSP certification offers a reliable benchmark to which job candidates can be measured by validating knowledge and experience. Candidates who successfully pass the rigorous exam are required to submit documentation verifying experience in the security field. Individuals holding this certification will stand out from the rest, not only making the hiring process easier but also adding a level of confidence in the final hire.

The Common Body of Knowledge

The material contained in the CISSP exam is divided into eight domains, which comprise what is known as the Common Body of Knowledge. This book devotes a chapter to each of these domains. Inevitable overlap occurs between the domains, leading to some overlap between topics covered in the chapters; the topics covered in each chapter are described next.

Security and Risk Management (e.g. Security, Risk, Compliance, Law, Regulations, Business Continuity)

The security and risk management domain covers a broad spectrum of general information security and risk management topics. Topics include:

- Concepts of confidentiality, integrity, and availability
- Security governance principles, including organizational processes and control frameworks
- Compliance with laws, regulations, and privacy requirements
- Professional ethics
- Security policies, standards, procedures, and guidelines
- Business continuity requirements
- Personnel security policies

- Risk management concepts
- Threat modeling
- Security risk considerations during acquisitions
- Information security education, training, and awareness

Asset Security (Protecting Security of Assets)

The asset security domain focuses on the collection, handling, and protection of information throughout its life cycle. Topics include:

- Information and supporting asset classification
- Asset ownership
- Privacy protection
- Asset retention
- Security controls
- Handling requirements

Security Engineering (Engineering and Management of Security)

The security engineering domain addresses the practice of building information systems and related architecture that deliver the required functionality when threats occur. Topics include:

- Engineering processes using secure design principles
- Security model concepts
- Control and countermeasure selection
- Security capabilities of information systems
- Vulnerabilities of security architectures, designs, and solution elements
- Vulnerabilities in web-based systems
- Vulnerabilities in mobile systems
- Vulnerabilities in embedded devices and cyber-physical systems
- Cryptography
- Site and facility design
- Physical security

Communication and Network Security (Designing and Protecting Network Security)

The communication and network security domain focuses on protecting data in transit and securing the underlying networks over which the data travels. The topics include:

- Network architecture secure design principles
- Network components security
- Secure communication channels
- Network attacks

Identity and Access Management (Controlling Access and Managing Identity)

The identity and access management domain discusses provisioning and managing the identities and access used in the interaction of humans and information systems, of disparate information systems, and even between individual components of information systems. Topics include:

- Physical and logical asset access
- Identification and authentication of people and devices
- Identity as a Service integration
- Third-party identity service integration
- Authorization mechanisms
- Access control attacks
- Identity and access provisioning life cycle

Security Assessment and Testing (Designing, Performing, and Analyzing Security Testing)

The security assessment and testing domain covers the evaluation of information assets and associated infrastructure using tools and techniques for the purpose of identifying and mitigating risk due to architectural issues, design flaws, configuration errors, hardware and software vulnerabilities, coding areas, and any other weaknesses that may affect an information system's ability to deliver its intended functionality in a secure manner. The topics include:

- Assessment and test strategies design and validation
- Security control testing

- Security process data collection
- Test output analysis and reporting
- Internal and third-party audits

Security Operations (e.g. Foundational Concepts, Investigations, Incident Management, Disaster Recovery)

The operations security domain surveys the execution of security measures and maintenance of proper security posture. Topics include:

- Investigations and investigation types
- Logging and monitoring activities
- Resource provisioning security
- Security operations concepts
- Resource protection techniques
- Incident management
- Preventive measures
- Patch and vulnerability management
- Change management process
- Recovery strategies
- Disaster recovery processes
- Disaster recovery plan testing
- Business continuity planning and testing
- Physical security
- Personnel safety concerns

Software Development Security (Understanding, Applying, and Enforcing Software Security)

The software development security domain explores the software development life cycle and development best practices. Topics include:

- System and software development life cycle
- Security controls in development environments

- Software security effectiveness
- Security impact of acquired software

Steps to Becoming a CISSP

To become a CISSP, certain prerequisites must be met and procedures followed. This final section covers those topics.

Qualifying for the Exam

Candidates must have a minimum of five years of direct full-time professional security work experience in two or more of the eight domains in the Common Body of Knowledge. You may receive a one-year experience waiver with a four-year college degree or additional credential from the approved list, available at the (ISC)^2 website, thus requiring four years of direct full-time professional security work experience in two or more of the eight domains of the CISSP.

If you lack this experience, you can become an Associate of (ISC)^2 by successfully passing the CISSP exam. You'll then have six years to earn your experience to become a CISSP.

Signing Up for the Exam

The steps required to sign up for the CISSP are as follows:

- Create a Pearson Vue account and schedule your exam.
- Complete the Examination Agreement, attesting to the truth of your assertions regarding professional experience and legally committing to the adherence of the (ISC)² Code of Ethics.
- Review the Candidate Background Questions.
- Submit the examination fee.

Once you are notified that you have successfully passed the examination, you will be required to subscribe to the (ISC)² Code of Ethics and have your application endorsed before the credential can be awarded. An endorsement form for this purpose must be completed and signed by an (ISC)² certified professional who is an active member, and who is able to attest to your professional experience.

About the CISSP Exam

The CISSP exam is a computer-based test that the candidate can spend up to 6 hours completing. There are no formal breaks, but you are allowed to bring a snack and eat it at the back of the test room, but any time used for that counts toward the 6 hours. You must bring a government-issued identification card. No other forms of ID will be accepted. You may be required to submit to a palm vein scan.

The test consists of 250 items with 4 choices per item. Some of the items will not be scored and are for research, and these are not identified to the candidate. The passing grade is 700 out of a possible 1,000. Candidates will receive the unofficial results at the test center from the test administrator. $(ISC)^2$ will then follow up with an official result via email.

This page intentionally left blank

This chapter covers the following topics:

- **Security terms:** Concepts discussed include confidentiality, integrity, and availability (CIA); default stance; defense in depth; job rotation; and separation of duties.
- **Security governance principles:** Concepts discussed include security function alignment, organizational processes, security roles and responsibilities, control frameworks, due care, and due diligence.
- **Compliance:** Concepts discussed include legislative and regulatory compliance and privacy requirements compliance.
- **Legal and regulatory issues:** Concepts discussed include computer crime concepts, major legal systems, licensing and intellectual property, import/export controls, trans-border data flow, privacy, and data breaches.
- **Professional ethics:** Ethics discussed include $(ISC)^2$ Code of Ethics, Computer Ethics Institute, Internet Architecture Board, and organizational ethics.
- **Security documentation:** Documentation types include policies, standards, baselines, guidelines, and procedures.
- **Business continuity:** Concepts discussed include business continuity and disaster recovery concepts, project scope and plan, and business impact analysis.
- **Personnel security policies:** Policies discussed include employment candidate screening; employment agreement and policies; employment termination policies; vendor, consultant, and contractor controls; compliance; and privacy.
- **Risk management concepts:** Concepts discussed include vulnerability, threat, threat agent, risk, exposure, countermeasure, risk management policy, risk management team, risk analysis team, risk assessment, implementation, access control categories, access control types, control assessment, monitoring, measurement, reporting and continuous improvement, and risk frameworks.

- **Threat modeling:** Concepts discussed include identifying threats, potential attacks, and remediation technologies and processes.
- **Security risks in acquisitions:** Concepts discussed include hardware, software, and services; third-party governance; minimum security requirements; and minimum service-level requirements.
- **Security education, training, and awareness:** Concepts discussed include levels required and periodic review.

Information security governance involves the principles, frameworks, and methods that establish criteria for protecting information assets, including security awareness. Risk management allows organizations to identify, measure, and control organizational risks. Threat modeling allows organizations to identify threats and potential attacks and implement appropriate mitigations against these threats and attacks. These facets ensure that security controls that are implemented are in balance with the operations of the organization. Each organization must develop a well-rounded, customized security program that addresses the needs of the organization while ensuring that the organization exercises due care and due diligence in its security plan. Acquisitions present special risks that management must understand prior to completing acquisitions.

Security professionals must take a lead role in their organization's security program and act as risk advisors to management. In addition, security professionals must ensure that they understand current security issues and risks, governmental and industry regulations, and security controls that can be implemented. Professional ethics for security personnel must also be understood. Security is an ever-evolving, continuous process, and security professionals must be watchful.

Business continuity and disaster recovery ensures that the organization can recover from any attack or disaster that affects operations. Using the results from the risks assessment, security professionals should ensure that the appropriate business continuity and disaster recovery plans are created, tested, and revised at appropriate intervals.

This chapter covers the following topics:

- **Access Control Process:** Concepts discussed include the steps of the access control process.
- **Physical and Logical Access to Assets:** Concepts discussed include access control administration, information access, systems access, device access, and facility access.
- **Identification and Authentication Concepts:** Concepts discussed include knowledge factors, ownership factors, characteristics factors, and time factors.
- **Identification and Authentication Implementation:** Concepts discussed include separation of duties, least privilege/need-to-know, default to no access, directory services, single sign-on, session management, registration and proof of identity, credential management systems, and accountability.
- **Identity as a Service (IDaaS) Implementation:** Describes the considerations when implementing IDaaS.
- **Third-Party Identity Services Implementation:** Details how to integrate third-party identity services in an enterprise.
- **Authorization Mechanisms**: Covers access control models and access control policies.
- **Access Control Threats:** Concepts discussed include password threats, social engineering threats, DoS/DDoS, buffer overflow, mobile code, malicious software, spoofing, sniffing and eavesdropping, emanating, and backdoor/trapdoor.
- **Prevent or Mitigate Access Control Threats:** Describes ways to prevent or mitigate access control threats.

Identity and Access Management is mainly concerned with controlling access to assets and managing identities. These assets include computers, equipment, networks, and applications. Security professionals must understand how to control physical and logical access to the assets and manage identification, authentication, and authorization systems. Finally, the access control threats must be addressed.

CHAPTER 5

Identity and Access Management

Identity and access management involve how access management works, why identity and access management (IAM) are important, and how IAM components and devices work together in an enterprise. Access control allows only authorized users, applications, devices, and systems to access enterprise resources and information. It includes facilities, support systems, information systems, network devices, and personnel. Security professionals use access controls to specify which users can access a resource, which resources can be accessed, which operations can be performed, and which actions will be monitored. Once again, the CIA triad is important in providing enterprise IAM.

Foundation Topics

Access Control Process

Key Topic

Although many approaches to implementing access controls have been designed, all the approaches generally involve the following steps:

1. Identify resources.
2. Identify users.
3. Identify the relationships between the resources and users.

Identify Resources

This first step in the access control process involves defining all resources in the IT infrastructure by deciding which entities need to be protected. When defining these resources, you must also consider how the resources will be accessed. The following questions can be used as a starting point during resource identification:

- Will this information be accessed by members of the general public?
- Should access to this information be restricted to employees only?
- Should access to this information be restricted to a smaller subset of employees?

Keep in mind that data, applications, services, servers, and network devices are all considered resources. Resources are any organizational asset that users can access. In access control, resources are often referred to as objects.

Identify Users

After identifying the resources, an organization should identify the users who need access to the resources. A typical security professional must manage multiple levels of users who require access to organizational resources. During this step, only identifying the users is important. The level of access these users will be given will be analyzed further in the next step.

As part of this step, you must analyze and understand the users' needs and then measure the validity of those needs against organizational needs, policies, legal issues, data sensitivity, and risk.

Remember that any access control strategy and the system deployed to enforce it should avoid complexity. The more complex an access control system is, the harder

that system is to manage. In addition, anticipating security issues that could occur in more complex systems is much harder. As security professionals, we must balance the organization's security needs and policies with the needs of the users. If a security mechanism that we implement causes too much difficulty for the user, the user might engage in practices that subvert the mechanisms that we implement. For example, if you implement a password policy that requires a very long, complex password, users might find remembering their passwords to be difficult. Users might then write their passwords on sticky notes that are attached to their monitor or keyboard.

Identify the Relationships Between Resources and Users

The final step in the access control process is to define the access control levels that need to be in place for each resource and the relationships between the resources and users. For example, if an organization has defined a web server as a resource, general employees might need a less restrictive level of access to the resource than the public and a more restrictive level of access to the resource than the web development staff. Access controls should be designed to support the business functionality of the resources that are being protected. Controlling the actions that can be performed for a specific resource based on a user's role is vital.

Physical and Logical Access to Assets

Access control is all about using physical or logical controls to control who has access to a network, system, or device. It also involves what type of access is given to the network, system, or device. Access control is primarily provided using physical and logical controls.

NOTE Physical and logical access controls are covered in more depth in Chapter 1, "Security and Risk Management."

Physical access focuses on controlling access to a network, system, or device. In most cases, physical access involves using access control to prevent users from being able to touch network components (including wiring), systems, or devices. While locks are the most popular physical access control method to preventing access to devices in a data center, other physical controls, such as guards and biometrics, should also be considered, depending on the needs of the organization and the value of the asset being protected.

Logical controls limit the access a user has through software or hardware components. Authentication and encryption are examples of logical controls.

When installing an access control system, security professionals should understand who needs access to the asset being protected and how those users need to access the asset. When multiple users need access to an asset, the organization should set up a multi-layer access control system. For example, users wanting access to the building may only need to sign in with a security guard. However, to access the locked data center within the same building, users would need a smart card. Both of these would be physical access controls. To protect data on a single server within the building (but not in the data center), the organization would need to deploy such mechanisms as authentication, encryption, and access control lists (ACLs) as logical access controls but could also place the server in a locked server room to provide physical access control.

When deploying physical and logical access controls, security professionals must understand the access control administration methods and the different assets that must be protected and their possible access controls.

Access Control Administration

Access control administration occurs in two basic manners: centralized and decentralized.

Centralized

In centralized access control, a central department or personnel oversees the access for all organizational resources. This administration method ensures that user access is controlled in a consistent manner across the entire enterprise. However, this method can be slow because all access requests are processed by the central entity.

Decentralized

In decentralized access control, personnel closest to the resources, such as department managers and data owners, oversee the access control for individual resources. This administration method ensures that those who know the data control the access rights to it. However, this method can be hard to manage because not just one entity is responsible for configuring access rights, thereby losing the uniformity and fairness of security.

Some companies may implement a hybrid approach that includes both centralized and decentralized access control. In this deployment model, centralized administration is used for basic access, but granular access to individual assets, such as data on a departmental server, is handled by the data owner.

Provisioning Life Cycle

Organizations should create a formal process for creating, changing, and removing users, which is the provisioning life cycle. This process includes user approval, user creation, user creation standards, and authorization. Users should sign a written statement that explains the access conditions, including user responsibilities. Finally, access modification and removal procedures should be documented.

User provision policies should be integrated as part of human resource management. Human resource policies should include procedures whereby the human resource department formally requests the creation or deletion of a user account when new personnel are hired or terminated.

Information

To fully protect information that is stored on an organization's network, servers, or other devices, security professionals must provide both physical and logical access controls. The physical access controls, such as placing devices in a locked room, protect the devices on which the information resides. The logical access controls—such as deploying data or drive encryption, transport encryption, ACLs, and firewalls—protect the data from unauthorized access.

The value of the information being protected will likely determine the controls that an organization is willing to deploy. For example, regular correspondence on a client computer will likely not require the same controls as financial data stored on a server. For the client computer, the organization may simply deploy a local software firewall and appropriate ACL permissions on the local folders and files. For the server, the organization may need to deploy more complex measures, including drive encryption, transport encryption, ACLs, and other measures.

Systems

To fully protect the systems used by the organization, including client and server computers, security professionals may rely on both physical and logical access controls. However, some systems, like client computers, may be deployed in such a manner that only minimal physical controls are used. If a user is granted access to a building, he or she may find client computers being used in non-secure cubicles throughout the building. For these systems, a security professional must ensure that the appropriate authentication mechanisms are deployed. If confidential information is stored on the client computers, encryption should also be deployed. But only the organization can best determine which controls to deploy on individual client computers.

When it comes to servers, determining which access controls to deploy is usually a more complicated process. Security professionals should work with the server owner, whether it is a department head or an IT professional, to determine the value of the asset and the needed protection. Of course, most servers should be placed in a locked room. In many cases, this will be a data center or server room. However, servers can be deployed in regular locked offices if necessary. In addition, other controls should be deployed to ensure that the system is fully protected. The access control needs of a file server are different from those of a web server or database server. It is vital that the organization perform a thorough assessment of the data that is being processed and stored on the system before determining which access controls to deploy. If limited resources are available, security professionals must ensure that their most important systems have more access controls than other systems.

Devices

As with systems, physical access to devices is best provided by placing the devices in a secure room. Logical access to devices is provided by implementing the appropriate ACL or rule list, authentication, and encryption, as well as securing any remote interfaces that are used to manage the device. In addition, security professionals should ensure that the default accounts and passwords are changed or disabled on the device.

For any IT professionals that need to access the device, a user account should be configured for the professional with the appropriate level of access needed. If a remote interface is used, make sure to enable encryption, such as SSL, to ensure that communication via the remote interface is not intercepted and read. Security professionals should closely monitor vendor announcements for any devices to ensure that the devices are kept up to date with the latest security patches and firmware updates.

Facilities

With facilities, the primary concern is physical access, which can be provided using locks, fencing, bollards, guards, and closed-circuit television (CCTV). Many organizations think that such measures are enough. But with today's advanced industrial control systems and the Internet of Things (IoT), organizations must also consider any devices involved in facility security. If an organization has an alarm/security system that allows remote viewing access from the Internet, the appropriate logical controls must be in place to prevent a malicious user from accessing the system and changing its settings or from using the system to gain inside information about the facility layout and day-to-day operations. If the organization uses an industrial control system (ICS), logical controls should also be a priority. Security professionals

must work with organizations to ensure that physical and logical controls are implemented appropriately to ensure that the entire facility is protected.

Identification and Authentication Concepts

To be able to access a resource, a user must profess his identity, provide the necessary credentials, and have the appropriate rights to perform the tasks he is completing. The first step in this process is called *identification*, which is the act of a user professing an identity to an access control system.

Authentication, the second part of the process, is the act of validating a user with a unique identifier by providing the appropriate credentials. When trying to differentiate between the two, security professionals should know that identification identifies the user and authentication verifies that the identity provided by the user is valid. Authentication is usually implemented through a user password provided at logon. When a user logs in to a system, the login process should validate the login after the user supplies all the input data.

After a user is authenticated, the user must be granted the rights and permissions to resources. The process is referred to as authorization.

The most popular forms of user identification include user IDs or user accounts, account numbers, and personal identification numbers (PINs).

Five Factors for Authentication

After establishing the user identification method, an organization must decide which authentication method to use.

Key Topic

Authentication methods are divided into five broad categories:

- **Knowledge factor authentication**: Something a person knows
- **Ownership factor authentication:** Something a person has or possesses
- **Characteristic factor authentication:** Something a person is
- **Location factor authentication:** Somewhere a person is
- **Time factor authentication:** The time a person is authenticating

Authentication usually ensures that a user provide 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 five factors. An example of two-factor authentication would be providing a username, password, and 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, password, smart card, and 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.)

NOTE Originally there were three factors (something you know, something you have, and something you are). They were referred to as Type I, Type II, and Type III factors, respectively. However, modern technology has forced the security field to recently recognize two additional factors: somewhere you are and the time of authentication.

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, 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 a person knows.

Knowledge Factors

As briefly described in the preceding section, *knowledge factor* authentication is authentication that is provided based on something that a person knows. Although 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.

Identity and Account Management

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 (provisioning), changing and monitoring (reviewing), and removing users from the access control system (revoking). This is referred to as the provisioning life cycle. When initially establishing a user account, new users 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 that standardize the structure of user accounts. For example, all user accounts should be *firstname.lastname* or some other structure. This ensures that users within an organization will be able to determine a new user's identification, mainly for communication purposes.

After creation, user accounts should be monitored to ensure that they remain active. Inactive accounts should be automatically disabled after a certain period of inactivity based on business requirements. In addition, any termination policy should include formal procedures to ensure that all user accounts are disabled or deleted. Elements of proper account management include the following:

- Establish a formal process for establishing, issuing, and closing user accounts.
- Periodically review user accounts.
- Implement a process for tracking access authorization.
- Periodically rescreen personnel in sensitive positions.
- Periodically verify the legitimacy of user accounts.

User account reviews are a vital part of account management. User accounts should be reviewed for conformity with the principle of least privilege. (The principle of least privilege is explained later in this chapter.) User account reviews can be performed on an enterprise-wide, system-wide, or application-by-application basis. The size of the organization will greatly affect which of these methods to use. As part of user account reviews, organizations should determine whether all user accounts are active.

Password Types and Management

As mentioned earlier, password authentication is the most popular authentication method implemented today. However, password types can vary from system to system. Understanding all the types of passwords that can be used is vital.

Key Topic

The types of passwords that you should be familiar with include:

- **Standard word or simple passwords:** As the name implies, these passwords consist of single words that often include a mixture of upper- and lowercase letters and numbers. 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, resulting in a compromised account.

- **Combination passwords:** This password type uses a mix of dictionary words, usually two unrelated words. These are also referred to as composition passwords. Like standard word passwords, they can include upper- and lowercase letters and numbers. An advantage of this password is that it is harder to break than simple passwords. 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 than standard or combination passwords.
- **Passphrase passwords:** This password type requires that a long phrase be used. 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. This information is provided to the system by answering a series of questions based on the user's life, such as favorite color, pet's name, mother's maiden name, and so on. An advantage to 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) might be able to provide this information as well.
- **One-time passwords:** Also called a dynamic password, this type of password is only used once to log in to the access control system. This password type provides the highest level of security because passwords are discarded when they are used.
- **Graphical passwords:** Also called CAPTCHA, which stands for Completely Automated Public Turing test to tell Computers and Humans Apart, 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 in the graphic displayed. This implementation ensures that a human

is entering the password, not a robot. Another popular implementation requires the user to select the appropriate graphic for his account from a list of graphics given.

- **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 4 digits, then the maximum number of password possibilities is 10,000, from 0000 through 9999. After an attacker realizes that only numbers are used, cracking user passwords would be much easier because the possibilities would be known.

Passwords are considered weaker than passphrases, one-time passwords, token devices, and login phrases. After an organization has decided which type of password to use, the organization must establish its password management policies.

Key Topic

Password management considerations include, but might not be limited to:

- **Password life:** How long the password will be valid. For most organizations, passwords are valid for 60 to 90 days.
- **Password history:** How long before a password can be reused. Password policies usually remember a certain number of previously used passwords.
- **Authentication period:** How long a user can remain logged in. If a user remains logged in for the period without activity, the user will be automatically logged out.
- **Password complexity:** How the password will be structured. Most organizations require upper- and lowercase letters, numbers, and special characters.
- **Password length:** How long the password must be. Most organizations require 8–12 characters.
- **Password masking:** Prevents a password from being learned through shoulder surfing by obscuring the characters entered except for the last one.

As part of password management, organizations should establish a procedure for changing passwords. Most organizations implement a service that allows users to automatically reset their password before the password expires. In addition, most organizations should consider establishing a password reset policy in cases where users have forgotten their password or passwords have been compromised. A self-service password reset approach allows users to reset their own passwords without the assistance of help desk employees. An assisted password reset approach requires that users contact help desk personnel for help in changing their passwords.

Password reset policies can also be affected by other organizational policies, such as account lockout policies. Account lockout policies are security policies that organizations

implement to protect against attacks that are carried out against passwords. Organizations often configure account lockout policies so that user accounts are locked after a certain number of unsuccessful login attempts. If an account is locked out, the system administrator might need to unlock or re-enable the user account. Security professionals should also consider encouraging organizations to require users to reset their password if their account has been locked or after a password has been used for a certain amount of time (90 days for most organizations). For most organizations, all the password policies, including account lockout policies, are implemented at the enterprise level on the servers that manage the network. Account lockout policies are most often used to protect against brute-force or dictionary attacks.

NOTE An older term that you might need to be familiar with is *clipping level*. A clipping level is a configured baseline threshold above which violations will be recorded. For example, an organization might want to start recording any unsuccessful login attempts after the first one, with account lockout occurring after five failed attempts.

Depending on which servers are used to manage the enterprise, security professionals must be aware of the security issues that affect user account and password management. Two popular server operating systems are Linux and Windows.

For Linux, passwords are stored in the */etc/passwd* and */etc/shadow* file. Because the */etc/passwd* file is a text file that can be easily accessed, you should ensure that any Linux servers use the */etc/shadow* file where the passwords in the file can be protected using a hash. The *root* user in Linux is a default account that is given administrative-level access to the entire server. If the *root* account is compromised, all passwords should be changed. Access to the *root* account should be limited only to systems administrators, and root login should only be allowed via a local system console, not remotely.

For Windows computers that are in workgroups, the Security Accounts Manager (SAM) stores user passwords in a hashed format. However, known security issues exist with a SAM, including the ability to dump the password hashes directly from the registry. You should take all Microsoft-recommended security measures to protect this file. If you manage a Windows network, you should change the name of the default Administrator account or disable it. If this account is retained, make sure that you assign it a password. The default Administrator account might have full access to a Windows server.

Ownership Factors

Ownership factor authentication is authentication that is provided based on something that a person has. Ownership factors can include token devices, memory cards, and smart cards.

Synchronous and Asynchronous Token

The token device (often referred to as a password generator) 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 an ownership authentication factor because its use requires ownership of the device.

Two basic token device authentication methods are used: synchronous or asynchronous. A synchronous token generates a unique password at fixed time intervals with the authentication server. An asynchronous token generates the password based on a challenge/response technique with the authentication server, with the token device providing the correct answer to the authentication server's challenge.

A token device is usually only implemented 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 lifespan of the token device.

Memory Cards

A memory card is a swipe card that is issued to valid users. 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, it is often worth the extra complexity and cost for the added security it provides, which is a definite benefit of this system. However, the data on the memory cards is not protected, a weakness that organizations should consider before implementing this type of system. Memory-only cards are very easy to counterfeit.

Smart Cards

Similar to a memory 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 a memory card but also contain an embedded chip like bank or credit cards. Smart cards use card readers. However, the data on the 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 a knowledge (PIN) and ownership (smart card) authentication factor.

Two basic types of smart cards are used: contact cards and contactless cards. Contact cards require physical contact with the card reader, usually by swiping. Contactless cards, also referred to as proximity cards, simply need to be in close proximity to the reader. Hybrid cards are available that allow a card to be used in both contact and contactless systems.

For comparative purposes, security professionals should remember that smart cards have processing power due to the embedded chips. Memory cards do not have processing power. Smart card systems are much more reliable than memory card systems.

Smart cards are even more expensive to implement than memory cards. Many organizations prefer smart cards over memory cards because they are harder to counterfeit and the data on them can be protected using encryption.

Characteristic Factors

Characteristic factor authentication is authentication that is provided based on something that a person is. 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.

Biometric technologies are now starting to creep into some of the most popular operating systems. Examples include Windows Hello and Apple's Touch ID technology. As a security professional, you need to be aware of such new technologies as they are deployed to provide added security. Educating users on these technologies should also be a priority to ensure that users adopt these technologies as they are deployed.

Physiological Characteristics

Physiological systems use a biometric scanning device to measure certain information about a physiological characteristic. You should understand the following physiological biometric systems:

- Fingerprint
- Finger scan
- Hand geometry

- Hand topography
- Palm or hand scans
- Facial scans
- Retina scans
- Iris scans
- Vascular scans

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 scans. Fingerprint scanning systems have a lower user acceptance rate than many systems because users are concerned with how the fingerprint information will be used and shared.

A finger 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.

A hand geometry 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.

A hand topography scan records the peaks and valleys of the hand and its shape. This system is usually implemented in conjunction with hand geometry scans because hand topography scans are not unique enough if used alone.

A palm or hand scan combines fingerprint and hand geometry technologies. It records fingerprint information from every finger as well as hand geometry information.

A facial scan records facial characteristics, including bone structure, eye width, and forehead size. This biometric method uses eigenfeatures or eigenfaces. Neither of these methods actually captures a picture of a face. With eigenfeatures, the distance 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 will use a combination of eigenfeatures and eigenfaces.

A retina scan scans the retina's blood vessel pattern. A retina scan is considered more intrusive than an iris scan.

An iris scan scans the colored portion of the eye, including all rifts, coronas, and furrows. Iris scans have a higher accuracy than any other biometric scan.

A vascular scan scans the pattern of veins in the user's hand or face. Although 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

Key Topic

Behavioral systems use a biometric scanning device to measure a person's actions. You should understand the following behavioral biometric systems:

- Signature dynamics
- Keystroke dynamics
- Voice pattern or print

Signature dynamics measure stroke speed, pen pressure, and acceleration and deceleration while the user writes his signature. Dynamic Signature Verification (DSV) analyzes signature features and specific features of the signing process.

Keystroke dynamics measure the typing pattern that a user uses when inputting a password or other predetermined phrase. In this case, even if the correct password or phrase is entered but the entry pattern on the keyboard is different, 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 measures the sound pattern of a user stating a certain word. 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

Key Topic

When considering biometric technologies, security professionals should understand the following terms:

- **Enrollment time:** 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:** The approach to obtaining biometric information from a collected sample of a user's physiological or behavioral characteristics.

- **Accuracy:** The most important characteristic of biometric systems. It is how correct the overall readings will be.
- **Throughput rate:** 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 6–10 subjects per minute. A single user should be able to complete the process in 5–10 seconds.
- **Acceptability:** Describes the likelihood that users will accept and follow the system.
- **False rejection rate (FRR):** A measurement of valid users that will be falsely rejected by the system. This is called a Type I error.
- **False acceptance rate (FAR):** 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):** The point at which FRR equals FAR. Expressed as a percentage, this is the most important metric.

When analyzing biometric systems, security professionals often refer to a Zephyr chart that illustrates the comparative strengths and weaknesses of biometric system. However, you should also consider how effective each biometric system is and its level of user acceptance. The following is a list of the more popular biometric methods ranked by effectiveness, with the most effective being first:

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 more popular biometric methods ranked by user acceptance, with the methods that are ranked more popular by users being first:

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, smaller values are better. FAR errors are more dangerous than FRR errors. Security professionals can use the CER rate 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.

Figure 5-1 shows the biometric enrollment and authentication process.

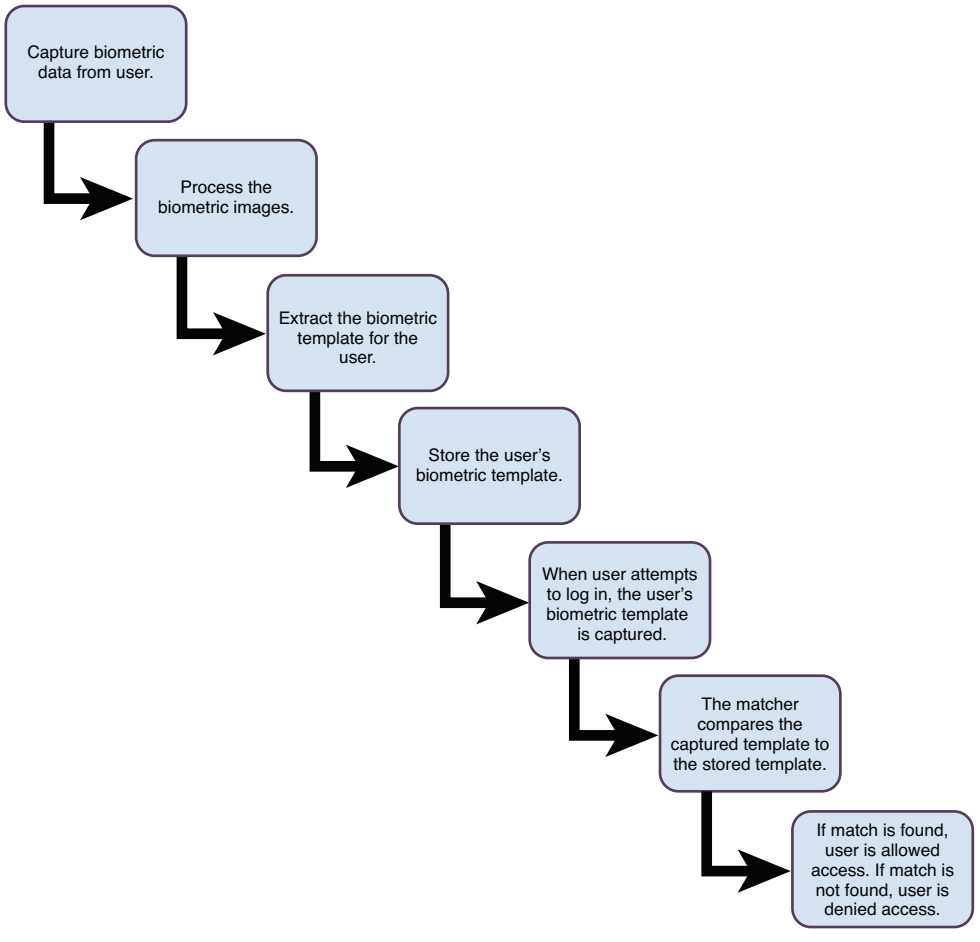


Figure 5-1 Biometric Enrollment and Authentication Process

Location Factors

Location factor authentication provides a means of authenticating the user based on the location from which the user is authenticating. This could include the computer or device the person is using or his or her geographic location based on GPS coordinates. The primary appeal to this type of authentication is that it limits the user to logging in from those certain locations only. This is particularly useful in large manufacturing environments for users who should only log in to certain terminals in the facility.

Geo-fencing is one example of the use of location factors. With geo-fencing, devices only operate correctly within the geo-fence boundaries. If a device enters or exits the geo-fenced area, an alert is generated and sent to the operator.

Time Factors

Time factor authentication authenticates a user based on the time and/or date the user is authenticating. For example, if certain users work only a set schedule, you can configure their accounts to only allow them to log in during those set work hours. However, keep in mind that such a limitation could cause administrative issues if overtime hours are allowed. Some organizations implement this effectively by padding the allowed hours with an hour or two leeway for the start and end times. Credit cards use this feature effectively to protect their customers. If transactions take place in a short timeframe from geographically dispersed locations, credit cards will often block the second transaction.

Identification and Authentication Implementation

Identification and authentication are necessary steps to providing authorization. Authorization is the point after identification and authentication at which a user is granted the rights and permissions to resources. The next sections cover important components in authorization: separation of duties, least privilege/need-to-know, default to no access, directory services, single sign-on (including Kerberos, SESAME, Federated Identity Management, and security domains), session management, registration and proof of identity, credential management systems, and accountability.

Separation of Duties

Separation of duties is an important concept 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 between more than one user. This helps deter fraud and collusion because any fraudulent act can occur only if there is collusion. A good example of separation of 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 to perform a particular task. An example of a split control is the military's requiring two individuals to each enter a unique combination to authorize missile firing.

Least Privilege/Need-to-Know

The principle of least privilege requires that a user or process is given only the minimum access privilege needed to perform a particular task. Its main purpose is to ensure that users only have access to 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 only to the identified privileges.

The need-to-know principle is closely associated with the concept of least privilege. Although least privilege seeks to reduce access to a minimum, the need-to-know principle actually defines what the minimums for each job or business function are. Excessive privileges become a problem when a user has more rights, privileges, and permissions than he needs to do his job. Excessive privileges are hard to control in large environments.

A common implementation of the least privilege and need-to-know principles is when 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 his normal user account. When the systems administrator needs to perform administrative-level tasks, he should use the administrative-level account. If the administrator uses his administrative-level account while performing routine tasks, he 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.

Default to No Access

During the authorization process, you should configure an organization's access control mechanisms so that the default level of security is to default to *no access*. This means that if nothing has been specifically allowed for a user or group, then the user or group will not be able to access the resource. The best security approach is to start with no access and add rights based on a user's need to know and least privilege needed to accomplish his daily tasks.

Directory Services

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.

The most common directory service standards are

- X.500
- Lightweight Directory Access Protocol (LDAP)
- X.400
- Active Directory Domain Services (AD DS)

X.500 uses the 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.

Based on X.500's DAP, LDAP is simpler than X.500. LDAP supports DN and RDN, but 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.

X.400 is mainly for message transfer and storage. It uses elements to create a series of name/value pairs separated by semicolons. X.400 has gradually been replaced by Simple Mail Transfer Protocol (SMTP) implementations.

Microsoft's implementation of LDAP is Active Directory Domain Services (AD DS), which stores and organizes directory data into trees and forests. It also manages

logon processes and authentication between users and domains and allows administrators to logically group users and devices into organizational units.

Single Sign-on

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 an SSO. Some of the objectives for the 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.
- They should be independent of any platform or operating system.

NOTE To obtain more information about the Open Group's Single Sign-On Standard, you should access the website at www.opengroup.org/security/sso_scope.htm.

SSO provides many advantages and disadvantages when it is implemented.

Advantages of an SSO system include:

- Users are able to use stronger passwords.
- User and password administration is simplified.
- Resource access is much faster.
- User login is more efficient.
- Users only need to remember the login credentials for a single system.

Disadvantages of an SSO system include:

- After a user obtains system access through the initial SSO login, the user is able to access all resources to which he is granted access. Although this is also an advantage for the user (only one login needed), it is also considered a disadvantage because only one sign-on can compromise all the systems that participate in the SSO network.
- If a user's credentials are compromised, attackers will have access to all resources to which the user has access.

Although the discussion on SSO so far has been mainly 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.

SSO can be implemented in Kerberos and Secure European System for Applications in a Multi-vendor Environment (SESAME) environments.

Kerberos

Kerberos is an authentication protocol that uses a client/server model developed by MIT's Project Athena. It is the default authentication model in the recent editions of Windows Server and is also used in Apple, Sun, and Linux operating systems. Kerberos is an SSO system that uses symmetric key cryptography. Kerberos provides confidentiality and integrity.

Kerberos assumes that messaging, cabling, and client computers are not secure and are easily accessible. In a Kerberos exchange involving a message with an authenticator, the authenticator contains the client ID and a timestamp. Because a Kerberos ticket is valid for a certain time, the timestamp ensures the validity of the request.

In a Kerberos environment, the Key Distribution Center (KDC) is the repository for all user and service secret keys. The client sends a request to the authentication server (AS), which might or might not be the KDC. The AS forwards the client credentials to the KDC. The KDC authenticates clients to other entities on a network and facilitates communication using session keys. The KDC provides security to clients or principals, which are users, network services, and software. Each principal must have an account on the KDC. The KDC issues a ticket-granting ticket (TGT) to the principal. The principal will send the TGT to the ticket-granting service (TGS) when the principal needs to connect to another entity. The TGS then transmits a ticket and session keys to the principal. The set of principles for which a single KDC is responsible is referred to as a realm.

Some advantages of implementing Kerberos include the following:

- User passwords do NOT need to be sent over the network.
- Both the client and server authenticate each other.
- The tickets passed between the server and client are time stamped and include lifetime information.
- The Kerberos protocol uses open Internet standards and is not limited to proprietary codes or authentication mechanisms.

Some disadvantages of implementing Kerberos include:

- KDC redundancy is required if providing fault tolerance is a requirement. The KDC is a single point of failure.
- The KDC must be scalable to ensure that performance of the system does not degrade.
- Session keys on the client machines can be compromised.
- Kerberos traffic needs to be encrypted to protect the information over the network.
- All systems participating in the Kerberos process must have synchronized clocks.
- Kerberos systems are susceptible to password-guessing attacks.

Figure 5-2 shows the ticket-issuing process for Kerberos.

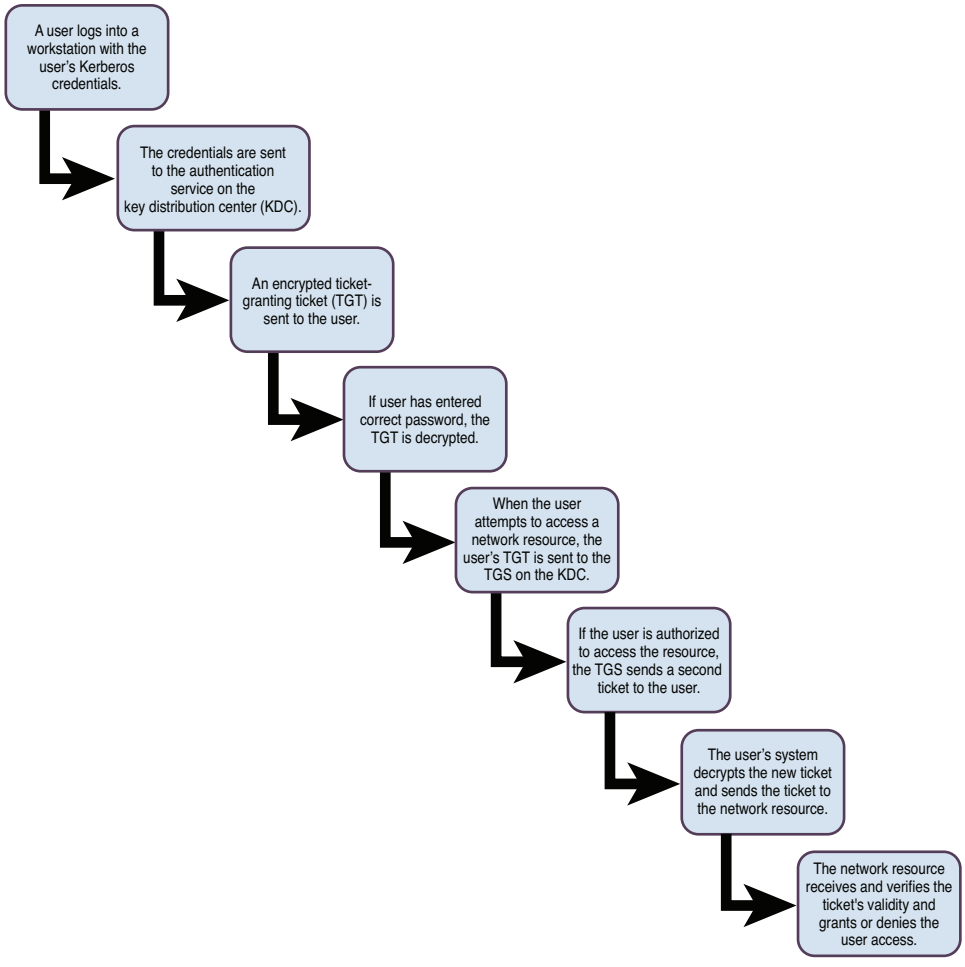


Figure 5-2 Kerberos Ticket-Issuing Process

SESAME

The Secure European System for Applications in a Multi-vendor Environment (SESAME) project extended Kerberos' functionality to fix Kerberos' weaknesses. SESAME uses both symmetric and asymmetric cryptography to protect interchanged data. SESAME uses a trusted authentication server at each host.

SESAME uses Privileged Attribute Certificates (PACs) instead of tickets. It incorporates two certificates: one for authentication and one for defining access privileges. The trusted authentication server is referred to as the Privileged Attribute Server (PAS), which performs roles similar to the KDC in Kerberos. SESAME can be integrated into a Kerberos system.

Federated Identity Management

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. Federated identity management uses two basic models for linking organizations within the federation: cross certification and trusted third-party or bridge model.

In the cross-certification 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 a problem. In addition, verifying the trustworthiness of other organizations can be time-consuming and resource intensive.

In the trusted third-party or bridge 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.

Security Assertion Markup Language (SAML) 2.0 is an SAML standard that exchanges authentication and authorization data between organizations or security domains. It uses an XML-based protocol to pass information about a principal between an SAML authority and a web service via security tokens. In SAML 2.0, there are three roles: the principal or user, the identity provider, and the service provider. The service provider requests identity verification from the identity provider. SAML is very flexible because it is based on XML. If an organization implements

enterprise SAML identity federation, the organization can select which identity attributes to share with another organization.

Security Domains

A domain is a set of resources that are available to a subject over a network. Subjects that access a domain include users, processes, and applications. A security domain is a set of resources that follows the same security policies and are available to a subject. The domains are usually arranged in a hierarchical structure of parent and child domains.

NOTE Do not confuse the term *security domain* with protection domain. Although a security domain usually encompasses a network, a protection domain resides within a single resource. A *protection domain* is a group of processes that share access to the same resource.

Session Management

Session management ensures that any instance of identification and authentication to a resource is managed properly. This includes managing desktop sessions and remote sessions.

Desktop sessions should be managed through a variety of mechanisms. Screensavers allow computers to be locked if left idle for a certain period of time. To reactivate a computer, the user must log back in. Screensavers are a timeout mechanism, and other timeout features may also be used, such as shutting down or placing a computer in hibernation after a certain period. Session or logon limitations allow organizations to configure how many concurrent sessions a user can have. Schedule limitations allow organizations to configure the time during which a user can access a computer.

Remote sessions usually incorporate some of the same mechanisms as desktop sessions. However, remote sessions do not occur at the computer itself. Rather, they are carried out over a network connection. Remote sessions should always use secure connection protocols. In addition, if users will only be remotely connecting from certain computers, the organization may want to implement some type of rule-based access that allows only certain connections.

Registration and Proof of Identity

A proof of identity process involves collecting and verifying information about an individual to prove that the person who has a valid account is who he or she claims

to be. The most basic method of proof of identity is providing a driver's license, passport, or some other government-issued identification. Proof of identity is performed before user account creation. Once proof of identity is completed, the user is issued a credential, and authentication factors are determined and recorded. From that point forward, authentication occurs each time the user logs in using the issued credential.

The National Institute of Standards and Technology (NIST) has issued documents that provide guidance on proof of identity:

- **FIPS Publication 201.2, Personal Identity Verification (PIV) of Federal Employees and Contractors:** This document specifies the architecture and technical requirements for a common identification standard for federal employees and contractors. This publication includes identification, security, and privacy requirements and personal identity verification system guidelines.
- **NIST 800-79-2, Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI):** This document includes preparation guidelines, issuer control implementation guidelines, and issuer control life cycle guidelines.

Both of these NIST publications are intended to guide federal government agencies in their proof of identity efforts and can also be used by private organizations to aid in the development of their own systems.

Credential Management Systems

Users are often required to remember usernames, passwords, and other authentication information for a variety of organizations. They often use the same authentication credentials across multiple platforms, which makes online identity theft and fraud easier to commit. Once a set of credentials has been discovered on one online system, attackers often use the same set of credentials on another organization's systems to see if they can gain access. Along with this problem comes an organization's own internal issue for maintaining different credentials for users needing access to multiple systems with different credentialing systems. Factor in the increasing use of mobile devices, and you have a recipe for disaster.

Credential management systems allow organizations to establish an enterprise-wide user authentication and authorization framework. Organizations should employ security professionals to design, deploy, and manage secure credential management systems. The business requirements for a credential management system should include individual privacy protection guidelines, automated identity solutions,

security, and innovation. Some of the guidelines of a credential management system include the following:

- Use strong passwords.
- Automatically generate complex passwords.
- Implement password history.
- Use access control mechanisms, including the who, what, how, and when of access.
- Implement auditing.
- Implement backup and restore mechanisms for data integrity.
- Implement redundant systems within the credential management systems to ensure 24/7/365 access.
- Implement credential management group policies or other mechanisms offered by operating systems.

When an organization implements a credential management system, separation of duties becomes even more important because the centralized credential management system can be used to commit fraud. Security professionals should provide guidance on how the separation should occur to best protect the organization and its assets.

Accountability

Accountability is an organization's ability to hold users responsible for the actions they perform. To ensure that users are accountable for their actions, organizations must implement auditing and other accountability mechanisms.

To ensure that users are accountable for their actions, organizations could implement any combination of the following components:

- **Strong identification:** Each user should have his or her own account. Group or role accounts cannot be traced back to a single individual.
- **Strong authentication:** Multi-factor authentication is best. At minimum, two-factor authentication should be implemented.
- **Monitoring:** User actions should be monitored, including login, privilege use, and other actions. Users should be warned as part of a no expectation of privacy statement that all actions can be monitored.
- **Audit Logs:** Audit logs should be maintained and stored according to organizational security policies. Administrators should periodically review these logs.

Although organizations should internally implement these accountability mechanisms, they should also periodically have a third party perform audits and tests. This is important because the outside third party can provide objectivity that internal personnel often cannot provide.

Auditing and Reporting

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. You should monitor network events, system events, application events, user events, and keystroke activity. 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. Also, organizations must ensure that any monitoring that occurs is in compliance with all applicable laws.

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-man control that requires the cooperation of at least two administrators. This ensures that a single administrator is not able to delete logs that might hold incriminating evidence.
- Monitor all high-privilege accounts (including all root users and administrative-level accounts).
- Ensure that the audit trail includes who processed the transaction, when the transaction occurred (date and time), where the transaction occurred (which system), and whether the transaction was successful or not.
- Ensure that deleting the log and deleting data within the logs cannot occur unless the user has the appropriate administrative-level permissions.

NOTE *Scrubbing* is the act of deleting incriminating data within an audit log.

Audit trails detect computer penetrations and reveal actions that identify misuse. As a security professional, you should use the 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 might choose to ignore the first invalid login attempt, knowing that initial failed login attempts are often due to user error. Any invalid login after the first would be recorded because it could be a sign of an attack. 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 is reached.

Audit trails deter attacker 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.

Finally, audit trails must be monitored, and automatic notifications should be configured. If no one monitors the audit trail, then the data recorded in the audit trail is useless. Certain actions should be configured to trigger automatic notifications. For example, you might want to configure an email alert to occur after a certain number of invalid login attempts because invalid login attempts might be a sign that a brute-force password attack is occurring.

Identity as a Service (IDaaS) Implementation

Identity as a Service (IDaaS) provides a set of identity and access management functions to target systems on customers' premises and/or in the cloud. IDaaS includes identity governance and administration (IGA), which provides the ability to provision identities held by the service to target applications. It includes user authentication, single sign-on (SSO), and authorization enforcement. IDaaS services are divided into two categories: web access software for cloud-based applications and cloud-delivered legacy identity management services. Web IDaaS applications do not work with on-premises applications. Most IDaaS deployments offer SSO authentication, federated identities, remote administration, and internal directory service integration. IDaaS is different from identity and access management (IAM) solutions, which are operated from within the organization's own network via bundled software and hardware. IAM solutions may use Active Directory and Lightweight Directory Access Protocol (LDAP).

If organizations consider IDaaS deployment, they should primarily be concerned with service availability, identity data protection, and trusting a third party with a critical business function. They should also be concerned with regulatory compliance. Moving identity management to the cloud brings up a whole host of questions for the organization regarding auditing, ensuring compliance of regulations, and what happens if disclosures occur.

An organization should perform a comprehensive risk analysis prior to deploying any IDaaS service. After performing the risk analysis, the organization should determine which identities should be placed on the IDaaS solution.

Third-Party Identity Services Implementation

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) Identity and Access Management (IAM) service and Oracle Identity Management.

Authorization Mechanisms

Authorization mechanisms are systems an organization deploys to control which systems a user or device can access. Authorization mechanisms include access control models and access control policies.

Access Control Models

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 a less secure subject.

The access control models and concepts that you need to understand include the following:

- Discretionary access control
- Mandatory access control
- Role-based access control
- Rule-based access control
- Content-dependent versus context-dependent access control
- Access control matrix

- Capabilities table
- ACL

Discretionary Access Control

In discretionary access control (DAC), the owner of the 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.

Non-discretionary access control is the opposite of DAC. In non-discretionary access control, access controls are configured by a security administrator or other authority. The central authority decides which subjects have access to objects based on the organization's policy. In non-discretionary access control, the system compares the subject's identity with the objects' ACL.

Mandatory Access Control

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.

MAC is more secure than DAC. 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 subject's privilege. Each subject and 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 the subject's clearance level with the object's security label.

Role-Based Access Control

In role-based access control (RBAC), each subject is assigned to one or more roles. Roles are hierarchical. 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 mentioned access control models because security is based on roles. RBAC usually has a much lower cost to implement 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 them access to multiple systems, but each user can 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 and is defined in RFC 2828. 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 allowing or denying access based on packet type, port number used, MAC address, and other parameters.

Content-Dependent Versus Context-Dependent

Content-dependent access control makes access decisions based on the data contained within the object. With this access control, the data that a user sees might change based on the policy and access rules that are applied.

Context-dependent access control is based on subject or object attributes or environmental characteristics. These characteristics can include location or time of day. An example of this is if administrators implement a security policy that ensures that a user only logs in from a particular workstation during certain hours of the day.

Security experts consider a constrained user interface as 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. Another example is database views that are filtered based on user or system criteria. Constrained user interfaces can be content- or context-dependent based on how the administrator constrains the interface.

Access Control Matrix

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 upon 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.

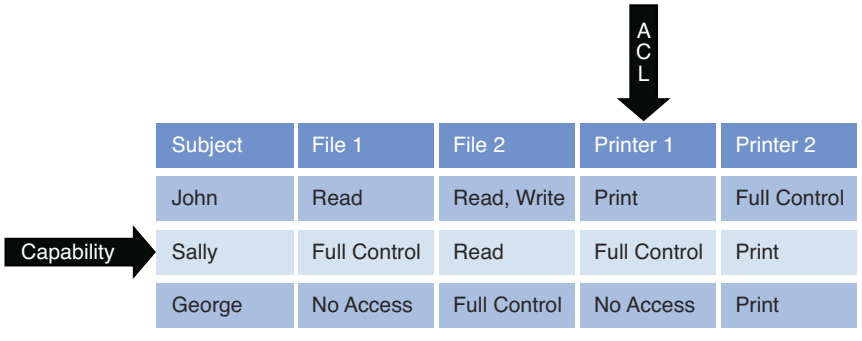
Capabilities Table

A capability corresponds to a subject's row from an access control matrix. A capability table lists the access rights that a particular subject has to objects. A capability table is about the subject.

ACL

An ACL corresponds to an object's column from an access control matrix. An ACL lists all the access rights that subjects have to a particular object. An ACL is about the object.

Figure 5-3 shows an access control matrix and how a capability and ACL are part of it.



Subject	File 1	File 2	Printer 1	Printer 2
John	Read	Read, Write	Print	Full Control
Sally	Full Control	Read	Full Control	Print
George	No Access	Full Control	No Access	Print

Figure 5-3 Access Control Matrix

Access Control Policies

An access control policy defines the method for identifying and authenticating users and the level of access that is granted to users. Organizations should put access control policies in place to ensure that access control decisions for users are based on formal guidelines. If an access control policy is not adopted, organizations will have trouble assigning, managing, and administering access management.

Access Control Threats

Access control threats directly impact the confidentiality, integrity, and availability of organizational assets. The purpose of most access control threats is to cause harm to an organization. Because harming an organization is easier to do from within its network, outsiders usually first attempt to attack any access controls that are in place.

Access control threats that you should understand include:

- Password threats
- Social engineering threats
- DoS/DDoS
- Buffer overflow
- Mobile code
- Malicious software
- Spoofing
- Sniffing and eavesdropping
- Emanating
- Backdoor/trapdoor

Password Threats

A password threat is any attack that attempts to discover user passwords. The two most popular password threats are dictionary attacks and brute-force attacks.

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.

Dictionary Attack

A dictionary attack occurs when attackers use a dictionary of common words to discover passwords. An automated program uses the hash of the dictionary word and compares this hash value to entries in the system password file. Although the program comes with a dictionary, attackers also use extra dictionaries that are found on the Internet.

You should implement a security rule that says that a password must NOT be a word found in the dictionary to protect against these attacks. You can also implement an account lockout policy so that an account is locked out after a certain number of invalid login attempts.

Brute-Force Attack

Brute-force attacks are more difficult to carry out because they work through all possible combinations of numbers and characters. A brute-force attack is also referred to as an exhaustive attack. It carries out password searches until a correct password is found. These attacks are also very time consuming.

Social Engineering Threats

Social engineering attacks occur when attackers use believable language and 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 very closely resembles a legitimate website. Users enter data, including credentials on the fake website, allowing the attackers to capture any 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 phishing attacks because of the information that must be gathered. Whaling is a type of phishing that specifically targets high-level executives or other high-profile individuals. Vishing is a type of phishing that uses a phone system or VoIP technologies. The user initially receives a call, text, or email that says to call a specific number and provide personal information such as name, birth date, Social Security number, and credit card information.

Pharming is similar to phishing, but it actually pollutes the contents of a computer's DNS cache so that requests to a legitimate site are actually routed to an alternate site.

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 SSL is being used, which is indicated by an HTTPS designation at the beginning of the URL address.

Shoulder Surfing

Shoulder surfing occurs when an attacker watches when a user enters login or other confidential data. Encourage users to always be aware of who is observing their actions. Implementing privacy screens helps to ensure that data entry cannot be recorded.

Identity Theft

Identity theft occurs when someone obtains personal information, including driver's license number, bank account number, and Social Security number, and uses that information to assume an identity of the individual whose information was stolen. After the identity is assumed, the attack can go in any direction. In most cases, attackers open financial accounts in the user's name. Attackers also can gain access to the user's valid accounts.

Dumpster Diving

Dumpster diving occurs when attackers examine garbage contents to obtain confidential information. This includes personnel information, account login information, network diagrams, and organizational financial data.

Organizations should implement policies for shredding documents that contain this information.

DoS/DDoS

A denial-of-service (DoS) attack occurs when attackers flood a device with enough requests to degrade the performance of the targeted device. Some popular DoS attacks include SYN floods and teardrop attacks.

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

Buffer Overflow

Buffers are portions of system memory that are used to store information. A buffer overflow occurs when the amount of data that is submitted to the application is larger than the buffer can handle. Typically, this type of attack is possible because of poorly written application or operating system code. This can result in an injection of malicious code.

To protect against this issue, organizations should ensure that all operating systems and applications are updated with the latest service packs, updates, and patches. In addition, programmers should properly test all applications to check for overflow conditions. Finally, programmers should use input validation to ensure that the data submitted is not too large for the buffer.

Mobile Code

Mobile code is any software that is transmitted across a network to be executed on a local system. Examples of mobile code include Java applets, Java script code, and ActiveX controls. Mobile code includes security controls, Java sandboxes, and ActiveX digital code signatures. Malicious mobile code can be used to bypass access controls.

Organizations should ensure that users understand the security concerns of malicious mobile code. Users should only download mobile code from legitimate sites and vendors.

NOTE For more information about mobile code, see the section, "Mobile Code," in Chapter 8, "Software Development Security."

Malicious Software

Malicious software, also called malware, is any software that is designed to perform malicious acts.

Key Topic

The following are the five classes of malware you should understand:

- **Virus:** Any malware that attaches itself to another application to replicate or distribute itself.
- **Worm:** Any malware that replicates itself, meaning that it does not need another application or human interaction to propagate.
- **Trojan horse:** Any malware that disguises itself as a needed application while carrying out malicious actions.

- **Spyware:** Any malware that collects private user data, including browsing history or keyboard input.
- **Ransomware:** Any malware that prevents or limits a user's access to his or her system or device. Usually it forces victims to pay the ransom for the return of system access.

The best defense against malicious software is to implement anti-virus and anti-malware software. Today most vendors package these two types of software in the same package. Keeping anti-virus and anti-malware software up to date is vital. This includes ensuring that the latest virus and malware definitions are installed.

Spoofing

Spoofing, also referred to as masquerading, occurs when communication from an attacker appears to come from trusted sources. Spoofing examples include IP spoofing and hyperlink spoofing. The goal of this type of attack is to obtain access to credentials or other personal information.

A man-in-the-middle attack uses spoofing as part of the attack. Some security professionals consider phishing attacks as a type of spoofing attack.

Sniffing and Eavesdropping

Sniffing, also referred to as eavesdropping, occurs when an attacker inserts a device or software into the communication medium that collects all the information transmitted over the medium. Network sniffers are used by both legitimate security professionals and attackers.

Organizations should monitor and limit the use of sniffers. To protect against their use, you should encrypt all traffic on the network.

Emanating

Emanations are electromagnetic signals that are emitted by an electronic device. Attackers can target certain devices or transmission mediums to eavesdrop on communication without having physical access to the device or medium.

The TEMPEST program, initiated by the United States and UK, researches ways to limit emanations and standardizes the technologies used. Any equipment that meets TEMPEST standards suppresses signal emanations using shielding material. Devices that meet TEMPEST standards usually implement an outer barrier or coating, called a Faraday cage or Faraday shield. TEMPEST devices are most often used in government, military, or law enforcement.

Backdoor/Trapdoor

A backdoor or trapdoor is a mechanism implemented in many devices or applications that gives the user who uses the backdoor unlimited access to the device or application. Privileged backdoor accounts are the most common method of backdoor that you will see today.

Most established vendors no longer release devices or applications with this security issue. You should be aware of any known backdoors in the devices or applications you manage.

Prevent or Mitigate Access Control Threats

Because access control threats are so widespread, organizations must do all they can to protect their access control systems, including deploying anti-malware, firewalls, intrusion detection and prevention, and other defense tools. Security professionals should encourage their organizations to deploy the following measures to prevent or mitigate access control threats:

- Deploy physical access controls for all systems and devices.
- Control and monitor access to password files.
- Encrypt password files.
- Deploy an enterprise-wide strong password policy.
- Deploy password masking on all operating systems and applications.
- Deploy multi-factor authentication.
- Deploy account lockout.
- Deploy auditing for access controls.
- Deploy a user account management policy to ensure that user accounts are created and removed as necessary.
- Provide user security awareness training that specifically focuses on access control.

Exam Preparation Tasks

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 5-1 lists a reference of these key topics and the page numbers on which each is found.

Key Topic

Table 5-1 Key Topics for Chapter 5

Key Topic Element	Description	Page Number
Paragraph	Access control process	410
Paragraph	Provisioning life cycle	413
Paragraph	Five factors of authentication	415
Paragraph	Password types	417
Paragraph	Password management considerations	419
Paragraph	Physiological characteristics	422
Paragraph	Behavioral characteristics	424
Paragraph	Biometric considerations	424
Paragraph	Advantages and disadvantages of SSO	430
Paragraph	Advantages and disadvantages of Kerberos	431
Paragraph	Auditing mechanism guidelines	437
Paragraph	Classes of malware	446

Define Key Terms

Define the following key terms from this chapter and check your answers in the glossary:
access control, access control list (ACL), access control matrix, access control policy, authentication, authorization, backdoor, biometric acceptability, biometric accuracy, biometric throughput, brute-force attack, buffer overflow, capability table, centralized access control, characteristic factors, context-dependent access control, cross-certification federated identity model, crossover error rate, decentralized access control, Dictionary attack, discretionary access control (DAC), dumpster diving, false acceptance rate (FAR), false rejection rate (FRR), federated identity, identification, Identity as a Service (IDaaS), Kerberos, knowledge factors, least privilege,

Lightweight Directory Access Protocol (LDAP), location factors, logical control, mandatory access control (MAC), multi-factor authentication, need-to-know, ownership factors, password masking, pharming, phishing, physical control, provisioning life cycle, ransomware, role-based access control (RBAC), rule-based access control, Secure European System for Applications in a Multi-vendor Environment (SESAME), Security Assertion Markup Language (SAML), security domain, separation of duties, shoulder surfing, single-factor authentication, single sign-on (SSO), spyware, trapdoor, Trojan horse, trusted third-party federated identity model, virus, vishing, whaling, worm

Review Questions

1. Which of the following is NOT an example of a knowledge authentication factor?
   a. password
   b. mother's maiden name
   c. city of birth
   d. smart card

2. Which of the following statements about memory cards and smart cards is false?
   a. A memory card is a swipe card that contains user authentication information.
   b. Memory cards are also known as integrated circuit cards (ICCs).
   c. Smart cards contain memory and an embedded chip.
   d. Smart card systems are more reliable than memory card systems.

3. Which biometric method is most effective?
   a. iris scan
   b. retina scan
   c. fingerprint
   d. hand print

4. What is a Type I error in a biometric system?
   a. crossover error rate (CER)
   b. false rejection rate (FRR)
   c. false acceptance rate (FAR)
   d. throughput rate

5. Which access control model is most often used by routers and firewalls to control access to networks?
   a. discretionary access control
   b. mandatory access control
   c. role-based access control
   d. rule-based access control

6. Which threat is NOT considered a social engineering threat?
   a. phishing
   b. pharming
   c. DoS attack
   d. dumpster diving

7. Which of the following statements best describes an IDaaS implementation?
   a. Ensures that any instance of identification and authentication to a resource is managed properly.
   b. Collects and verifies information about an individual to prove that the person who has a valid account is who he or she claims to be.
   c. Provides a set of identity and access management functions to target systems on customers' premises and/or in the cloud.
   d. It is an SAML standard that exchanges authentication and authorization data between organizations or security domains.

8. Which of the following is an example of multi-factor authentication?
   a. username and password
   b. username, retina scan, and smart card
   c. retina scan and finger scan
   d. smart card and security token

9. You decide to implement an access control policy that requires that users logon from certain workstations within your enterprise. Which type of authentication factor are you implementing?
   a. knowledge factor
   b. location factor
   c. ownership factor
   d. characteristic factor

10. Which threat is considered a password threat?
    a. buffer overflow
    b. sniffing
    c. spoofing
    d. brute-force attack
11. Which session management mechanisms are often used to manage desktop sessions?
    a. screensavers and timeouts
    b. FIPS 201.2 and NIST SP 800-79-2
    c. Bollards and locks
    d. KDC, TGT, and TGS
12. Which of the following is a major disadvantage of implementing an SSO system?
    a. Users are able to use stronger passwords.
    b. Users need to remember the login credentials for a single system.
    c. User and password administration are simplified.
    d. If a user's credentials are compromised, attacker can access all resources.
13. Which type of attack is carried out from multiple locations using zombies and botnets?
    a. TEMPEST
    b. DDoS
    c. Backdoor
    d. Emanating

Answers and Explanations

1. **d.** Knowledge factors are something a person knows, including passwords, mother's maiden name, city of birth, and date of birth. Ownership factors are something a person has, including a smart card.
2. **b.** Memory cards are NOT also known as integrated circuit cards (ICCs). Smart cards are also known as ICCs.
3. **a.** Iris scans are considered more effective than retina scans, fingerprints, and hand prints.
4. **b.** A Type I error in a biometric system is false rejection rate (FRR). A Type II error in a biometric system is false acceptance rate (FAR). Crossover error rate

(CER) is the point at which FRR equals FAR. Throughput rate is the rate at which users are authenticated.

5. **d.** Rule-based access control is most often used by routers and firewalls to control access to networks. The other three types of access control models are not usually implemented by routers and firewalls.
6. **c.** A denial-of-service (DoS) attack is not considered a social engineering threat. The other three options are considered to be social engineering threats.
7. **c.** An Identity as a Service (IDaaS) implementation provides a set of identity and access management functions to target systems on customers' premises and/or in the cloud. Session management ensures that any instance of identification and authentication to a resource is managed properly. A proof of identity process collects and verifies information about an individual to prove that the person who has a valid account is who he or she claims to be.
8. **b.** Using username, retina scan, and a smart card is an example of multi-factor authentication. The username is something you know, the retina scan is something you are, and the smart card is something you have.
9. **b.** You are implementing location factors, which are based on where a person is located when logging in.
10. **d.** A brute-force attack is considered a password threat.
11. **a.** Desktop sessions can be managed through screensavers, timeouts, logon, and schedule limitations. Federal Information Processing Standards (FIPS) Publication 201.2 and NIST Special Publication 800-79-2 are documents that provide guidance on proof of identity. Physical access to facilities can be provided securely using locks, fencing, bollards, guards, and closed-circuit television (CCTV). In Kerberos, the key distribution center (KDC) issues a ticket-granting ticket (TGT) to the principal. The principal sends the TGT to the ticket-granting service (TGS) when the principal needs to connect to another entity.
12. **d.** If a user's credentials are compromised in a single sign-on (SSO) environment, attackers have access to all resources to which the user has access. All other choices are advantages to implementing an SSO system.
13. **b.** A distributed DoS (DDoS) attack is a DoS attack that is carried out from multiple attack locations. Vulnerable devices are infected with software agents, called zombies. This turns the vulnerable devices into botnets, which then carry out the attack. Devices that meet TEMPEST standards implement an outer barrier or coating, called a Faraday cage or Faraday shield. A backdoor or trapdoor is a mechanism implemented in many devices or applications that gives the user who uses the backdoor unlimited access to the device or application. Emanations are electromagnetic signals that are emitted by an electronic device. Attackers can target certain devices or transmission mediums to eavesdrop on communication without having physical access to the device or medium.

Index

Numerics

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z