Chapter 1

Introduction to Information Security

At a Glance

Instructor's Manual Table of Contents

Lecture Notes

Overview

In Chapter 1, students will gain an understanding of the information security field. They will learn about key terms and concepts relating to securing information. Students will learn about the roles within an organization that are responsible for security. Finally, the chapter provides an overview of common attacks and threats to information within systems.

Chapter Objectives

In this chapter, your students will learn to:

- Explain the component parts of information security in general and network security in particular
- Define the key terms and critical concepts of information and network security
- Describe the organizational roles of information and network security professionals
- Discuss the business need for information and network security
- Identify the threats posed to information and network security, as well as the common attacks associated with those threats
- Differentiate threats to information within systems from attacks against information within systems

Teaching Tips

Introduction

1. Introduce the key concepts in network security that will be covered in this chapter. Be sure to describe the term perimeter defense.

What Is Information Security?

1. Describe the key aspects of information security including network, physical, personnel, operations, and communications security.

2. Introduce the C.I.A. triangle and explain that this approach does not address the constantly changing environment of the IT industry.

Critical Characteristics of Information

1. Discuss the following important characteristics of information, providing a brief description of each:

- Availability
- Accuracy
- Authenticity
- Confidentiality
- Integrity
- Utility
- Possession

Teaching Tip	To learn more about measuring the value of information, see: http://www.umsl.edu/~sauterv/analysis/info/info.htm.

CNSS Security Model

1. Explain that the U.S. Committee on National Systems Security (CNSS) has created a document that presents a comprehensive model for information security. This is known as the McCumber Cube and shown in Figure 1-1.

Balancing Information Security and Access

1. Discuss the importance of balancing security with access to information.

Business Needs First

1. Describe the four organizational functions of information security.
   - Protecting the functionality of an organization
   - Enabling the safe operation of applications
   - Protecting data that organizations collect and use
   - Safeguarding technology assets in organizations

Security Professionals and the Organization

1. Describe the role of the following professionals who affect the security of an organization:
   - Chief information officer (CIO)
   - Chief information security officer (CISO)
   - Information security project team members:
     - Champion
     - Team leader
     - Security policy developers
     - Risk assessment specialists
     - Security professionals
     - Systems, network, and storage administrators
     - End users

Teaching Tip	Ask students to discuss how other roles within an organization might fit into securing the information owned by the organization.

Data Management

1. Describe the roles of data owners, custodians, and users. Data owners are responsible for securing and using information. Data custodians are responsible for storing, maintaining, and protecting information. Data users are allowed to access the information.

Quick Quiz 1

1. The _____, an industry standard for computer security since the development of the mainframe, is based on the three characteristics of information that make it valuable to organizations: confidentiality, integrity, and availability.
   Answer: C.I.A. triangle

2. The _____ provides a graphical description of the architectural approach widely used in computer and information security
   Answer: McCumber Cube

3. (True/False) Although many managers shy away from addressing information security because they perceive it to be a technically complex task, information security has more to do with management than with technology.
   Answer: True

4. _____ are individuals who understand financial risk assessment techniques, the value of organizational assets, and the security methods to be used.
   Answer: Risk assessment specialists

Key Information Security Terminology

1. Note that the next section will describe the terminology used for describing information security concepts.

Threats and Attacks

1. Define the terms threat, asset, attack, subject of an attack, object of an attack, direct attack, and indirect attack. Use Figure 1-2 to explain the difference between the subject of an attack and the object of an attack.

Teaching Tip	Make sure that students understand the importance of protecting against indirect attacks as well as direct attacks.

Vulnerabilities and Exploits

1. Describe the terms threat agent, vulnerability, well-known vulnerability. Describe the two common uses of the term "exploit:" one means to exploit a system, and the other is a formula for an attack. Explain that defenders use controls, safeguards, and countermeasures to protect the systems that they are responsible for securing.

Teaching Tip	Assign students a research project to find one or more well-known vulnerabilities in the computer operating system they use most frequently.

Risk

1. Discus the concept of risk. Note that risk is described in terms of likelihood of attack. Explain how organizations manage risk using four major strategies:
   - Self-protection
   - Risk transfer
   - Self-insurance or acceptance
   - Avoidance

Security Perimeter and Defense in Depth

1. Using Figure 1-3, introduce the concept of a security perimeter. Note that a security perimeter may be implemented using multiple layers and technologies.

2. Define the term defense in depth (Figure 1-4) and explain how this concept helps to protect information.

Threats to Information Security

1. Walk through the data presented in Table 1-1, which shows types of attacks or misuse reposted to the Computer Security Institute (CSI) Computer Crime and Security Survey.

2. Review the threats to information security listed in Table 1-2.

The TVA Triple

1. Introduce the concept of the TVA Triple: Threat-Vulnerability-Asset. This is used to determine which assets need to be protected the most. The TVA worksheet shown in Table 1-3 is used to analyze risk. Explain how to create a TVA worksheet.

Teaching Tip	Ask students to discuss the benefits of creating a TVA worksheet.

Other Ways to View Threats

1. Provide a brief description of the following perspectives on threats:
   - Intellectual property
   - Software piracy
   - Shoulder surfing
   - Hackers
   - Script kiddies
   - Packet monkeys
   - Cracker
   - Phreaker
   - Hacktaivist or cyberactivist
   - Cyperterrorist
   - Malicious code, software, or malware
   - Power irregularities

Quick Quiz 2

1. A threat _____ is a specific instance of a general threat.
   Answer: agent

2. (True/False) Some organizations remove risk completely.
   Answer: False

3. The "TVA Triple" stands for _____.
   Answer: Threat-Vulnerability-Asset

4. A(n) _____ is an individual who, sometimes working with others, hacks systems to conduct terrorist activities through a network or Internet pathway.
   Answer: cyberterrorist

Attacks on Information Assets

1. Explain that the final sections of the chapter will cover the different major types of attacks used against information systems.

Malicious Code

1. Note that malicious code includes viruses, worms, Trojan horses, and some Web scripts.

Teaching Tip	To learn more about malicious code, see: http://csrc.nist.gov/publications/nistir/threats/section3_3.html.

2. Review the six categories of attack vectors listed in Table 1-6.

Compromising Passwords

1. Explain that there are several different types of attack used to get passwords.

2. Define the term cracking.

3. Describe a brute force attack (also called a password attack). Note that brute force attacks are not usually successful against systems that have been secured with industry-standard security practices.

4. Describe the variation on a brute force attack called a dictionary attack.

Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS)

1. Using Figure 1-5, describe a denial-of-service (DoS) attack. Also describe a distributed denial-of-service (DDoS) attack.

Spoofing

1. Define the term spoofing. Using Figure 1-6 to explain how spoofing works.

Man-in-the-Middle

1. Explain that a man-in-the-middle attack builds on a spoofing attack to eavesdrop, change, delete, reroute, add, forge, or divert data. Use Figure 1-7 to illustrate this type of attack.

E-mail Attacks

1. Note that e-mail is a vehicle for attacks on information systems.

2. Define the term spam and describe the negative effect of spam on organizations.

3. Define the term mail bomb. Explain how a mail bomb works.

Sniffers

1. Explain how sniffers are used to monitor network traffic. Define the term packet sniffer.

Social Engineering

1. Describe the use of social engineering attacks to gain sensitive information.

Teaching Tip	To learn more about social engineering, see: http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics.

Buffer Overflow

1. Describe the use of a buffer overflow attack.

Quick Quiz 3

1. _____ includes viruses, worms, Trojan horses, and active Web scripts that are executed with the intent to destroy or steal information
   Answer: Malicious code

2. The application of computing and network resources to try every possible combination of options for a password is called a(n) _____ attack.
   Answer: brute force

3. A(n) _____ is a program or device that can monitor data traveling over a network.
   Answer: sniffer

4. A(n) _____ is an application error that occurs when more data is sent to a buffer than it can handle.
   Answer: buffer overflow

Class Discussion Topics

1. Why are so many different roles within an organization concerned with information security?

2. Why is it important to have an understanding of the most common types of attacks and threats?

Additional Projects

1. Using the World Wide Web, research one of the types of attacks discussed in this chapter. Provide a more in-depth description of the attack, as well as information on the most common countermeasures.

2. Using a library with current periodicals, find a recent news article about a topic related to information security. Write a one- to two-page review of the article and how it is related to the principles of information security introduced in the textbook.

Additional Resources

1. McCumber Cube
   http://protectyourbits.wordpress.com/2009/10/05/review-mccumber-cube-methodology/

2. CNSS Directives
   http://www.cnss.gov/directives.html

3. Top information security threats
   http://www.net-security.org/secworld.php?id=8709

4. What is a Chief Security Officer
   http://www.csoonline.com/article/221739/what-is-a-chief-security-officer-

Key Terms

- **Accuracy** – Indicates that information is free from mistakes or errors, and has the value that the end user expects.
- **Attack** – An act or action that takes advantage of a vulnerability to compromise a controlled system.
- **Authenticity** – The quality or state of being genuine or original, rather than a reproduction or fabrication. Information is authentic when it is the information that was originally created, placed, stored, or transferred.
- **Availability** – Enables authorized users—persons or computer systems—to access information without interference or obstruction, and to receive it in the required format.
- **Back door** – Vulnerability created in a system by a virus or
- **Blackout** – A lengthy complete loss of power
- **Boot virus** – A virus that infects the key operating system files located in a computer's boot sector.
- **Brownout** – A prolonged drop in voltage.
- **Brute force attack** – The application of computing and network resources to try every possible combination of options of a password.
- **Buffer overflow** – An application error that occurs when more data is sent to a buffer than it can handle.
- **Champion** – A senior executive who promotes a project and ensures that it is supported, both financially and administratively, at the highest levels of the organization.

- **Chief information officer (CIO)** – This individual is often the senior technology officer and is primarily responsible for advising the chief executive officer, president, or company owner on the strategic planning that affects the management of information in the organization.
- **Chief information security officer (CISO)** – The individual primarily responsible for the assessment, management, and implementation of information security in the organization. The CISO usually reports directly to the CIO, although in larger organizations it is not uncommon for one or more layers of management to exist between the two.
- **Communications security** – The protection of an organization's communications media, technology, and content.
- **Computer viruses** – A type of malicious code that runs inside another program on a computer.
- **Confidentiality** – Exists when information is protected from disclosure or exposure to unauthorized individuals or systems. This means that only those with the rights and
- **Controls** – Security mechanisms, policies, or procedures that can successfully counter attacks, reduce risk, resolve vulnerabilities, and generally improve the security within an organization.
- **Countermeasures** – see controls
- **Cracker** – An individual who "cracks" or removes software protection that is designed to prevent unauthorized duplication.
- **Cracking** – Attempting to reverse–calculate a password.
- **Cyberactivist** – see hacktavist
- **Cyberterrorist** – Activities conducted by individuals for the purpose of hacking systems to conduct terrorist activities through network or Internet pathways.
- **Data custodians** – Individuals responsible for the storage, maintenance, and protection of the data owner's information. The custodian could be a dedicated position, or it may be an additional responsibility of a systems administrator or other technology manager.
- **Data owners** – Those responsible for the security and use of a particular set of information. Usually members of senior management and sometimes even CIOs, data owners usually determine the level of data classification associated with the data, and work with subordinate managers to oversee the day–to–day administration of that data.
- **Data users** – End users who work with the information to perform their daily jobs supporting the mission of the organization.
- **Defense in depth** – One of the basic tenets of security architectures; the layered implementation of security.
- **Denial–of–service (DoS)** – An attack in which the attacker sends a large number of connection or information requests to a target. So many requests are made that the target system cannot handle them along with other, legitimate requests for service. The system may crash or may simply be unable to perform ordinary functions.
- **Dictionary attack** – A variation on the brute force attack, this attack narrows the field by selecting specific target accounts and using a list of commonly used passwords (the dictionary) instead of random combinations.
- **Direct attack** – An attack in which a hacker uses a personal computer to break into a system.
- **Distributed denial–of–service (DDoS)** – A coordinated attack in which streams of requests are launched against a target from many locations at the same time. Most DDoS attacks are preceded by a preparation phase in which many systems, perhaps thousands, are compromised.

- **End users** – Those who will be most directly affected by new implementations and changes to existing systems. Ideally, a selection of users from various departments, levels, and degrees of technical knowledge who assist a project team in focusing on the application of realistic controls applied in ways that do not disrupt the essential business activities they seek to safeguard.
- **Exploit** – To take advantage of a weakness in the defenses of an asset; also refers to a packaged attack that leverages a weakness to cause a loss to an asset.
- **Fault** – Complete loss of power for a moment.
- **Hackers** – The classic perpetrators of espionage or trespass, these are people who use and create computer software to gain access to information illegally.
- **Hacktivist** – Someone who interferes with or disrupts systems to protest the operations, policies, or actions of an organization or government agency.
- **Indirect attack** – An attack in which a system is compromised and used to attack other systems.
- **Integrity** – Indicates that information remains whole, complete, and uncorrupted. The integrity of information is threatened when the information is exposed to corruption, damage, destruction, or other disruption of its authentic state.
- **Intellectual property (IP)** – The control of ideas and innovation, an important part of the value of assets that organizations control.
- **Likelihood** – The possibility or probability of unwanted action on an information asset.
- macro virus – Virus that is embedded in the automatically executing macro code common in word processors, spreadsheets, and database applications.
- **Mail bomb** – A form of e–mail attack that is also a DoS attack in which an attacker routes large quantities of e–mail to the target system.
- **Maintenance hook** – see back door
- **Malicious code** – Software deliberately designed to cause a system or a program to act in a way that is not the intention of the system's owner or operator. Usually this code is designed to steal information or to make the system follow future commands from the attacker and become a "bot" or "zombie" system.
- **Malicious software** – see malicious code
- **Malware** – see malicious code
- man–in–the–middle – In this well–known type of attack, an attacker monitors (or sniffs) packets from the network, modifies them using IP spoofing techniques, and inserts them back into the network, allowing the attacker to eavesdrop as well as to change, delete, reroute, add, forge, or divert data.
- **McCumber Cube** – A comprehensive model for information security that is becoming the evaluation standard for the security of information systems. It provides a graphical description of the architectural approach widely used in computer and information security. The McCumber Cube uses a representation in three dimensions of a 3×3×3 cube with 27 cells representing areas that must be addressed to secure today's information systems.
- **Network security** – The protection of networking components, connections, and contents.
- **Object of an attack** – A computer that is the entity being attacked.
- **Operations security** – The protection of the details of a particular operation or series of activities.

- **Packet monkeys** – Script kiddies who use automated exploits to engage in distributed denial–of–service attacks.
- **Password attack** – Repeatedly guessing passwords to commonly used accounts.
- **Personnel security** – The protection of the people who are authorized to access the organization and its operations.
- **Phreaker** – One who hacks the public telephone network to make free calls or disrupt services.
- **Physical security** – The protection of the physical items, objects, or areas of an organization from unauthorized access and misuse.
- **Possession** – The ownership or control of some object or item of information. Information is said to be in one's possession if one obtains it, independent of format or other characteristics.
- **Power irregularities** – Variations in the 120–volt, 60–cycle power provided to most businesses through a 15– or 20–amp circuit.
- **Residual risk** – The amount of risk that remains after an organization takes precautions, implements controls and safeguards, and performs other security activities.
- **Risk** – The state of being unsecure, either partially or totally, and thus susceptible to attack, as in "at risk."
- **Risk appetite** – The amount of risk an organization chooses to live with, also called risk tolerance.
- **Risk assessment specialists** – Individuals who understand financial risk assessment techniques, the value of organizational assets, and the security methods to be used.
- **Risk management** – The processes used to identify, assess, and control the risks that may cause losses to assets.
- **Risk tolerance** – See "risk appetite."
- **Rootkit** – A collection of software tools and a recipe used to gain control of a system by bypassing its legitimate security controls.
- **Safeguards** – see controls
- **Sag** – A momentary drop in voltage level.
- **Script kiddies** – Hackers of limited skill who use expertly written software to attack a system.
- **Security policy developers** – Individuals who understand the organizational culture, existing policies, and requirements for developing and implementing successful policies.
- **Security professionals** – Dedicated, trained, and well–educated specialists in all aspects of information security, both technical and nontechnical.
- **Shoulder surfing** – A technique used to gather information one is not authorized to have, by looking over another individual's shoulder or viewing the information from a distance, in a public or semipublic setting.
- **Sniffer** – A program or device that can monitor data traveling over a network.
- social engineering – The process of using social skills to convince people to reveal access credentials or other valuable information to an attacker.
- **Software piracy** – The unlawful use or duplication of software–based intellectual property.
- **Spam** – Unsolicited commercial e–mail.
- **Spike** – A momentary increase in voltage levels.
- **Spoofing** – A technique used to gain unauthorized access to computers, wherein the intruder sends messages whose IP address indicates to the recipient that the messages are coming from a trusted host.

- **Subject of an attack** – A computer that is used as an active tool to conduct an attack.
- **Surge** – A prolonged increase in voltage levels.
- **Systems, network, and storage administrators** – Individuals with the primary responsibility for administering the systems, storage, and networks that house and provide access to the organization's information
- **Team leader** – A project manager, who may be a departmental line manager or staff unit manager, who understands project management, personnel management, and information security technical requirements.
- **Threat** – In the context of information security, an object, person, or other entity that represents a constant danger to an asset.
- **Threat agent** – An object, person, or other entity that launches an attack in order to damage or steal an organization's information or physical asset.
- **Trojan horses** – A software program that reveals its designed behavior only when activated.
- **Trap door** – See back door**.**
- **Utility** – The quality or state of information having value for some purpose or end. To have utility, information must be in a format meaningful to the end user.
- **Vulnerability** – An identified weakness in a controlled system, where controls are not present or are no longer effective.
- **Well–known vulnerabilities** – Vulnerabilities that have been examined, documented, and published.
- worm which allows the attacker to access the system at will with special privileges.
- **Worms** – Malicious programs that replicate themselves constantly, without requiring another program to provide a safe environment for replication.
- **Zombies/bots** – Compromised machines that are directed during a distributed denial–of–service (usually by a transmitted command) to participate in the attack.