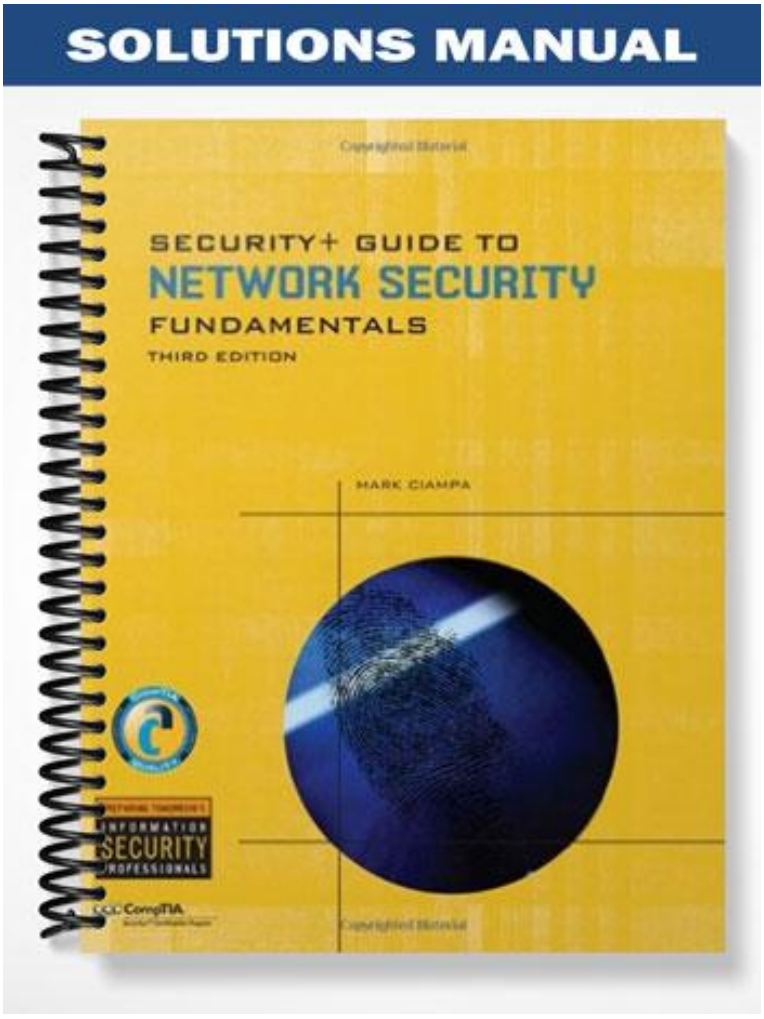
SOLUTIONS MANUAL



Chapter 2

Systems Threats and Risks

At a Glance

Instructor's Manual Table of Contents

Lecture Notes

Overview

This chapter examines the threats and risks that a computer system faces today. It begins by looking at software-based attacks. Then, it considers attacks directed against the computer hardware. Finally, the chapter turns to the expanding world of virtualization and how virtualized environments are increasingly becoming the target of attackers.

Chapter Objectives

- Describe the different types of software-based attacks
- List types of hardware attacks
- Define virtualization and explain how attackers are targeting virtual systems

Teaching Tips

Software-Based Attacks

1. Define malicious software, or malware, as software that enters a computer system without the owner's knowledge or consent. Malware is a general term that refers to a wide variety of damaging or annoying software.

2. Describe the three primary objectives of malware:
    a. To infect a computer system
    b. Conceal the malware's malicious actions
    c. Bring profit from the actions that it performs

Infecting Malware

1. Define a virus as a program that secretly attaches to another document or program and executes when that document or program is opened.

2. Explain that once a virus infects a computer, it performs two separate tasks:
    a. Replicates itself by spreading to other computers
    b. Activates its malicious payload

3. Mention that viruses cause problems ranging from displaying an annoying message to erasing files from a hard drive or causing a computer to crash repeatedly. Use Figure 2-1 to illustrate your explanation.

4. Describe the following types of computer viruses:
    a. File infector virus
    b. Resident virus

c. Boot virus
d. Companion virus
e. Macro virus

Teaching Tip	Because of the risk of macro viruses, users should be cautious of opening any e-mail attachment, because doing so could launch a macro virus.

5. Explain that metamorphic viruses avoid detection by altering how they appear. Polymorphic viruses also encrypt their contents differently each time.

6. Define a worm as a program designed to take advantage of a vulnerability in an application or an operating system in order to enter a system.

Teaching Tip	A worm uses a network to send copies of itself to other devices connected to the network.

7. Explain that worms are different from viruses in two regards:
   a. A worm can travel by itself
   b. A worm does not require any user action to begin its execution

8. Mention that some actions that worms perform include deleting files on the computer or allowing the computer to be remote-controlled by an attacker.

Concealing Malware

1. Define a Trojan horse (or just Trojan) as a program advertised as performing one activity but actually doing something else.

2. Explain that Trojan horse programs are typically executable programs that contain hidden code that attack the computer system.

3. Define a rootkit as a set of software tools used by an intruder to break into a computer, obtain special privileges to perform unauthorized functions, and then hide all traces of its existence.

4. Mention that the rootkit's goal is to hide the presence of other types of malicious software.

Teaching Tip	Originally the term "rootkit" referred to a set of modified and recompiled tools for the UNIX operating system. A root is the highest level of privilege available in UNIX, so a "rootkit" described programs that an attacker used to gain root privileges and to hide the malicious software.

5. Explain that rootkits function by replacing operating system commands with modified versions that are specifically designed to ignore malicious activity in order to escape detection.

6. Mention that detecting a rootkit can be difficult. Removing a rootkit from an infected computer is extremely difficult. You need to reformat the hard drive and reinstall the operating system.

7. Define a logic bomb as a computer program or a part of a program that lies dormant until it is triggered by a specific logical event. Once triggered, the program can perform any number of malicious activities. Use Table 2-1 to describe the most famous logic bombs.

8. Mention that logic bombs are extremely difficult to detect before they are triggered.

9. Define privilege escalation as exploiting a vulnerability in software to gain access to resources that the user would normally be restricted from obtaining.

10. Describe the following types of privilege escalation:
    a. When a user with a lower privilege uses privilege escalation to access functions reserved for higher privilege users
    b. When a user with restricted privileges accesses the different restricted functions of a similar user

Teaching Tip	Privilege escalation has been discovered in Microsoft Windows, Cisco software, antivirus software, Apple Mac OS X, Microsoft Internet Information Services, and Linux.

Quick Quiz 1

1. A(n) ____ is a program that secretly attaches itself to a legitimate "carrier," such as a document or program, and then executes when that document is opened or program is launched.
   Answer: computer virus

2. A(n) ____ is a set of software tools used by an intruder to break into a computer, obtain special privileges to perform unauthorized functions, and then hide all traces of its existence.
   Answer: rootkit

3. A(n) ____ is a computer program or a part of a program that lies dormant until it is triggered by a specific logical event, such as a certain date reached on the system calendar or a drop below a previous level of a person's rank in an organization.
   Answer: logic bomb

4. ____ is exploiting a vulnerability in software to gain access to resources that the user would normally be restricted from obtaining.
   Answer: Privilege escalation

Malware for Profit

1. Define spam as unsolicited e-mail.

2. Mention that spam is a lucrative business. Describe the costs involved for spamming:
   a. E-mail address
   b. Equipment and Internet connection

Teaching Tip	The profit from spamming can be substantial. If a spammer sent spam to six million users for a product with a sale price of $50 that cost only $5 to make, and if only 0.001 percent of the recipients responded and bought the product (a typical response rate), the spammer would make over $270,000 in profit.

3. Mention that text-based spam messages can easily by trapped by spam filters.

4. Explain that image spam uses graphical images of text in order to circumvent text-based spam filters. It includes nonsense text so that it appears the e-mail message is legitimate. Use Figure 2-2 to illustrate your explanation.

5. Explain that in addition to sending a single graphical image, spammers also use other techniques, such as the following:
   a. GIF Layering (See Figure 2-3)
   b. Word Splitting (See Figure 2-4)
   c. Geometric variance (See Figure 2-5)

6. Explain that image spam cannot be easily filtered based on the content of the message. To detect image spam, one approach is to examine the context of the message and create a profile, asking questions such as:
   a. Who sent the message?
   b. What is known about the sender?
   c. Where does the user go if she responds to this e-mail?
   d. What is the nature of the message content?
   e. How is the message technically constructed?

7. Define spyware as a general term used for describing software that imposes upon a user's privacy or security.

8. Mention that the Antispyware Coalition defines spyware as technologies that are deployed without the user's consent and impair the user's control over:
   a. Material changes that affect their user experience, privacy, or system security
   b. Use of their system resources, including what programs are installed on their computers
   c. Collection, use, and distribution of their personal or other sensitive information

9. Describe the two characteristics that make spyware very treacherous:
    a. Spyware creators are motivated by profit. Because of this, spyware in many instances is more intrusive than viruses, harder to detect, and more difficult to remove
    b. Spyware is not always easy to identify

10. Use Table 2-2 to explain the effects of spyware.

11. Mention that spyware is very widespread. Although attackers use several different spyware tools, the two most common are adware and keyloggers.

Teaching Tip	Read more about spyware at: http://en.wikipedia.org/wiki/Spyware.

12. Define adware a software program that delivers advertising content in a manner that is unexpected and unwanted by the user.

13. Explain that adware can be a security risk. Many adware programs perform a tracking function, which monitors and tracks a user's activities and then sends a log of these activities to third parties without the user's authorization or knowledge.

14. Define a keylogger as a small hardware device or a program that monitors each keystroke a user types on the computer's keyboard. As the user types, the keystrokes are collected and saved as text**.**

15. Explain that as a hardware device, a keylogger is a small device inserted between the keyboard connector and computer keyboard port. Use Figure 2-6 to illustrate your explanation.

16. Define software keyloggers as programs that silently capture all keystrokes, including passwords and sensitive information. They hide themselves so that they cannot be easily detected even if a user is searching for them. Use Figure 2-7 to illustrate your explanation.

Teaching Tip	Keyloggers are frequently found on public access computers, such as those in a library or a student computing lab. Users should not use these computers to perform any actions that require entering sensitive data.

17. Define a botnet as hundreds, thousands, or even tens of thousands of zombie computers that are under the control of an attacker.

18. Define a zombie as an infected computer with a program that will allow the attacker to remotely control it.

19. Explain that attackers use Internet Relay Chat (IRC) to remotely control the zombies. An attacker is knows as a bot herder.

20. Use Table 2-3 to describe the uses of botnets.

Hardware-Based Attacks

1. Mention that hardware that often is the target of attacks includes the BIOS, USB devices, network attached storage, and even cell phones.

BIOS

2. Define the Basic Input/Output System (BIOS) as a coded program embedded on the processor chip that recognizes and controls different devices on the computer system.

3. Explain that the BIOS is executed when the computer system is first turned on and provides low-level access to the hard disk, video, and keyboard.

4. Mention that on older computer systems, the BIOS was a Read Only Memory (ROM) chip. Today's computer systems have a PROM (Programmable Read Only Memory) chip.

5. Explain that because it can be flashed, the BIOS can be the object of attacks:
    a. One virus overwrites the contents of the BIOS and the first part of the hard disk drive, rendering the computer completely dead
    b. An attacker could infect a computer with a virus and then flash the BIOS to install a rootkit on the BIOS

Teaching Tip	To prevent an attacker from flashing the BIOS, it is recommended that the BIOS be set to not allow flashing. Disabling BIOS flashing can be done through the BIOS setting usually named Write Protect BIOS. Some motherboards have a jumper that write-protects the BIOS.

USB Devices

1. Explain that USB devices use flash memory. Flash memory is a type of EEPROM, nonvolatile computer memory that can be electrically erased and rewritten repeatedly.

2. Explain that USB devices are widely used to spread malware. Also, USB devices allow spies or disgruntled employees to copy and steal sensitive corporate data. In addition, data stored on USB devices can be lost or fall into the wrong hands.

3. Describe some mechanisms to reduce the risk introduced by USB devices:
    a. Disable the USB in hardware
    b. Disable the USB through the operating system
    c. Use third-party software

Network Attached Storage (NAS)

1. Define a Storage Area Network (SAN) as a specialized high-speed network for attaching servers to storage devices. SAN can be shared between servers and can be local or extended over geographical distances. Use Figure 2-8 to illustrate your explanation.

2. Define a Network Attached Storage (NAS), another type of network storage, as a single, dedicated hard disk-based file storage device that provides centralized and consolidated disk storage to LAN users through a standard network connection. Use Figure 2-9 to illustrate your explanation.

3. Describe the advantages to using NAS devices on a network, including:
    a. They offer the ability to easily expand storage requirements
    b. NAS allows for the consolidation of storage

4. Mention that the operating system on NAS devices can be either a standard operating system, a proprietary operating system, or a "stripped-down" operating system with many of the standard features omitted.

5. Explain that NAS security is implemented through the standard operating system security features.

Teaching Tip	Because a NAS device can become the central data repository on a network, the network interface of the NAS to the network can become a bottleneck. It is recommended that a fast network interface or even multiple network interfaces for NAS devices be used.

Cell Phones

1. Define cellular telephones (cell phones) as portable communication devices that function in a manner that is unlike wired telephones.

2. Describe the following two keys to cellular telephone networks:
    a. The coverage area is divided into smaller individual sections called cells
    b. All of the transmitters and cell phones operate at a low power level

3. Explain that almost all cell phones today have the ability to send and receive text messages and connect to the Internet.

4. Describe the following types of attacks to cell phones:
    a. Lure users to malicious Web sites
    b. Infect a cell phone
    c. Launch attacks on other cell phones
    d. Access account information
    e. Abuse the cell phone service

Attacks on Virtualized Systems

1. Explain that just as attacks can be software-based or hardware-based, attacks can also target software that is emulating hardware.

2. Mention that this type of software, known as virtualization, is becoming one of the prime targets of attackers.

What Is Virtualization?

1. Define virtualization as a means of managing and presenting computer resources by function without regard to their physical layout or location.

2. Explain that with operating system virtualization, a virtual machine is simulated as a self-contained software environment by the host system, but that it appears as a guest system.

3. Define server virtualization as creating and managing multiple server operating systems. Use Table 2-4 to describe other types of virtualization.

4. Mention that one of the factors driving the adoption of virtualization is the cost of energy.

5. Explain that operating system virtualization is playing an increasingly important role in security. It has allowed increased flexibility in launching attacks and is also being used to make systems more secure.

Attacks on Virtual Systems

1. Mention that virtualization provides the ability to run multiple virtual computers on one physical computer.

2. Explain that virtualization can also be beneficial in providing uninterrupted server access to users by means of live migration and load balancing.

3. Describe some of the reasons why security for virtualized environments can be a concern:
    a. Existing security tools were designed for single physical servers and do not always adapt well to multiple virtual machines
    b. Virtual machines not only need to be protected from the outside world, but they also need to be protected from other virtual machines on the same physical computer.

4. Define hypervisor as software that runs on a physical computer and manages one or more virtual machine operating systems. It can contain security code that would allow the hypervisor to provide security by default to all virtual machines. Use Figure 2-10 to illustrate your explanation.

5. Mention that another option is for security software to function as a separate program that is "plugged in" to the hypervisor.

6. Explain that another approach for securing virtual systems is running security software, such as a firewall and intrusion detection system, as a specialized security virtual machine on the physical machine. Use Figure 2-11 to illustrate your explanation.

Quick Quiz 2

1. ____ is a general term used for describing software that imposes upon a user's privacy or security.
   Answer: Spyware

2. ____ is a software program that delivers advertising content in a manner that is unexpected and unwanted by the user.
   Answer: Adware

3. A(n) ____ is either a small hardware device or a program that monitors each keystroke a user types on the computer's keyboard.
   Answer: keylogger

4. ____ is a means of managing and presenting computer resources by function without regard to their physical layout or location.
   Answer: Virtualization

Class Discussion Topics

1. Describe and compare the main types of spyware.

2. Why is spam so difficult to eradicate?

Additional Projects

1. Have students do some research to find software and hardware that can be used to hack into a computer system. Ask them to summarize their research in a short paper.

2. Ask your students to read more about Network Attached Storage (NAS) and write a report briefly explaining the network protocols most commonly used by NAS devices.

Additional Resources

1. Introduction to NAS - Network Attached Storage
   http://compnetworking.about.com/od/itinformationtechnology/l/aa070101a.htm

2. Adware
   http://en.wikipedia.org/wiki/Spyware

3. An Introduction to Virtualization
   http://www.kernelthread.com/publications/virtualization/

4. Virtualization
   http://en.wikipedia.org/wiki/Virtualization

5. Hypervisor
   http://en.wikipedia.org/wiki/Hypervisor

Key Terms

- **adware** A software program that delivers advertising content in a manner that is unexpected and unwanted by the user.
- **Basic Input/Output System (BIOS)** A coded program embedded on a processor chip that recognizes and controls different devices on the computer system.
- **boot virus** A virus that infects the Master Boot Record (MBR) of a hard disk drive.
- **bot herder** An attacker who controls several botnets.
- **botnet** A group of zombie computers that are under the control of an attacker.
- **cells** The coverage areas for cellular communications.
- **cellular telephones (cell phones)** Portable communications devices that function in a manner unlike wired telephones.
- **channels** Internet Relay Chat (IRC) discussion forums.
- **companion virus** A virus that adds a program to the operating system that is a copycat "companion" to a legitimate program.
- **EEPROM (Electrically Erasable Programmable Read-Only Memory)** Non-volatile computer memory that can be electrically erased and rewritten repeatedly.
- **file infector virus** A virus that infects program executable files with an .EXE or .COM file extension.
- **flash memory** A type of non-volatile computer memory that can be electrically erased and rewritten repeatedly.
- **flashing** The process for rewriting the contents of the BIOS.
- **geometric variance** Spam that uses "speckling" and different colors so that no two spam e-mails appear to be the same.
- **GIF layering** Spam that is divided into multiple images but still create a legible message.
- **guest system** A foreign virtual operating system.
- **host system** The native operating system to the hardware.
- **hypervisor** Software that runs on a physical computer and manages one or more virtual machine operating systems.

- **image spam** Spam that uses graphical images of text in order to circumvent text-based spam filters.
- **instant messaging (IM)** A method of online communication like e-mail except that it is conducted instantaneously in real time.
- **Internet Relay Chat (IRC)** An open communication protocol that is used for real-time "chatting" with other IRC users over the Internet. Also used to remotely control zombie computers in a botnet.
- **keylogger** A small hardware device or a program that monitors each keystroke a user types on the computer's keyboard.
- **live migration** Technology that enables a virtual machine to be moved to a different physical computer with no impact to the users.
- **load balancing** Balancing processing load among several servers; moving a virtual machine to another physical server with more RAM or CPU resources.
- **logic bomb** A computer program or a part of a program that lies dormant until it is triggered by a specific logical event.
- **macro** A series of commands and instructions that can be grouped together as a single command.
- **macro virus** A virus written in a scripting language.
- **malware** Malicious software that enters a computer system without the owner's knowledge or consent.
- **Master Boot Record (MBR)** An area on a hard disk drive that contains the program necessary for the computer to start up and a description of how the hard drive is organized.
- **metamorphic virus** A virus that alters how it appears in order to avoid detection.
- **mobile telecommunications switching office (MTSO)** The link between the cellular network and the wired telephone world that controls all of the transmitters and base stations in the cellular network.
- **Network Attached Storage (NAS)** A single dedicated hard disk-based file storage device that provides centralized and consolidated disk storage that is available to LAN users through a standard network connection.
- **operating system virtualization** A virtualized environment in which an entire operating system environment is simulated.
- **partition table** A table on the hard drive that describes how the hard drive is organized.
- **polymorphic virus** A virus that changes how it appears and also encrypts its contents differently each time.
- **privilege escalation** The act of exploiting a vulnerability in the software to gain access to resources that the user would normally be restricted from obtaining.
- **PROM (Programmable Read Only Memory)** A chip with which the contents can be rewritten to provide new functionality.
- **Read Only Memory (ROM)** A chip that cannot be reprogrammed.
- **removable storage** Devices, such as USB flash drives, that can store data from a computer and then be disconnected.
- **resident virus** A virus that is loaded into random access memory and can interrupt almost any function executed by the computer operating system and alter it.
- **rootkit** A set of software tools used by an intruder to break into a computer, obtain special privileges to perform unauthorized functions, and then hide all traces of its existence.
- **server virtualization** Creating and managing multiple server operating systems.
- **spam** Unsolicited e-mail.

- **spyware** A general term used to describe software that violates a user's personal security.
- **Storage Area Network (SAN)** A specialized high-speed network for attaching servers to storage devices.
- **Trojan horse (Trojan)** A program advertised as performing one activity but actually does something else, or it may perform both the advertised and malicious activities.
- **virtual machine** A self-contained software environment.
- **virtualization** A means of managing and presenting computer resources by function without regard to their physical layout or location.
- **virus** A program that secretly attaches itself to a legitimate "carrier," such as a document or program, and then executes when that document is open or the program is launched.
- **word splitting** Spam that horizontally separates words so that they can still be read by the human eye.
- **worm** A program that is designed to take advantage of a vulnerability in an application or an operating system in order to enter a system.
- **zombie** Computer under the control of an attacker.