

# Chapter 11

## Security and Ethics

### At a Glance

#### Instructor's Manual Table of Contents

- Overview
- Objectives
- Teaching Tips
- Quick Quizzes
- Class Discussion Topics
- Additional Projects
- Additional Resources
- Key Terms

## Lecture Notes

### Overview

Every computing system has conflicting needs: to share resources and to protect them. In the early days, security consisted of a secure lock and a few keys. That was sufficient when the user group was limited to several dozen individuals. However, with the advent of data communication, networking, the proliferation of personal computers, telecommunications software, Web sites, and e-mail, the user community has grown to include millions of people making computer security much more difficult. System security is a vast and complex subject worthy of its own text.

This chapter introduces important concepts related to security. It begins by explaining the role of the operating system in security. The effects of system security practices on overall system performance are discussed. Unintentional attacks and various types of intentional attacks are described in detail. The chapter also presents four protection methods including use of firewalls, use of antivirus software, restricting access to only authorized users, and use of encryption technology. It also discusses password management. The chapter concludes by presenting the difficulties of teaching ethics to user groups and the role of education in system security.

### Learning Objectives

After completing this chapter, the student should be able to describe:

- The role of the operating system with regard to system security
- The effects of system security practices on overall system performance
- The levels of system security that can be implemented and the threats posed by evolving technologies
- The differences among computer viruses, worms, and blended threats
- The role of education and ethical practices in system security

### Teaching Tips

#### **Role of the Operating System in Security**

1. Provide students with a brief overview of the key role of operating systems in computer system security, discussing how vulnerability at the operating system level opens the entire system to attack.
2. Note that as operating systems increase in power and complexity, the more likely they are to be vulnerable to attack. Inform students that system administrators must always be on guard, using all available defenses against possible attack mechanisms.

## System Survivability

1. Review the definition of the term system survivability, expanding on each key term within the definition (*system, mission, in a timely manner, attack, failure accident*).
2. Explain the concept of system survivability, and outline the four key properties of survivable systems.
3. Use Table 11.1 on page 347 as a guide to explain these properties and strategies to achieve a survivable system.

### **Teaching Tip**

Details about the example strategies shown in Table 11.1 of the text can be found at [www.cert.org](http://www.cert.org).

## Levels of Protection

1. Explain the need to evaluate the risk for intrusion for each computer configuration, which in turn depends on the level of connectivity given to the system. Use Table 11.2 on page 347 as a guide.

## Backup and Recovery

1. Discuss the importance of having backup and recovery policies. Explain the concept of a layered backup schedule. Specifically, a layered schedule occurs when there is a backup of the entire system once a week and then there is a backup of daily files that were changed that day.
2. Outline potential sources of disaster, as mentioned in the bullet points on page 348. Point out that backups with one set stored off-site are crucial to disaster recovery.
3. Discuss the importance of written policies and procedures and regular user training. List the essential contents of written security procedures.

## Security Breaches

1. Provide students with an overview of security breaches. Point out that a gap in system security can be malicious or not.
2. Classify the intrusions. For example, some intrusions are due to uneducated users and the unauthorized access to system resources, while others are the result of a purposeful disruption of the system's operation. Still others are purely accidental (hardware or software failure).

## Unintentional Intrusions

1. Briefly explain unintentional intrusions, which are defined as any breach of security or modification of data that was not the result of a planned intrusion.
2. Using Figure 11.1 on page 341, provide examples such as accidental incomplete modification of data, or errors due to incorrect storage of data values. Point out that neither error would be discovered at the time of storage, but rather would be discovered only when the value is retrieved.

## Intentional Attacks

1. Briefly explain intentional attacks by listing the different types of intentional attacks, such as:
  - a. Intentional unauthorized access (denial of service attacks, browsing, wire tapping, repeated trials, trapdoors, and trash collection)
  - b. Viruses
  - c. Worms
  - d. Trojan horses
  - e. Bombs
  - f. Blended threats
2. Briefly explain intentional unauthorized access attacks, such as denial of service attacks, browsing, wire tapping (active and passive), repeated trials, trapdoors, and trash collection. Provide examples to illustrate these attacks.
3. Use Table 11.3 to illustrate the time required for a human and computer to guess passwords that are up to 10 alphanumeric characters in length.
4. Point out that a malicious attack on computers may violate state and federal law within the United States. Outline some consequences if convicted.
5. Provide students with an overview of viruses, pointing out some of their key features. These include that they are self-executing and self-replicating, they are usually written to attack a certain operating system, and they spread via a wide variety of applications.
6. Use Figure 11.2 on page 352 to illustrate a virus infection pictorially.
7. Using Table 11.4 on page 353 as a guide, explain five recognized types of viruses.
8. Discuss macro viruses, which work by attaching to a template, which in turn is attached to word processing documents.
9. Discuss worms, which are memory-resident programs that copy themselves from one system to the next without requiring the aid of an infected program file. Discuss the example of the Morris worm provided on page 354 in the text.
10. Discuss the consequences when a system is infected with worms. Point out that worms are especially destructive on networks.

11. Discuss Trojan horses, which are programs disguised as useful applications. Point out that they do not replicate themselves like viruses; however, they can be just as destructive.
12. Use the numbered points on page 354 and Figure 11.3 on page 355 as a guide to outline the steps taken to capture user passwords using a Trojan horse.
13. Explain logic bombs and time bombs using examples provided in the text on page 355.
14. Explain a blended threat, which combines into one program the characteristics of other attacks, including a virus, worm, Trojan horse, spyware, and other malicious code.
15. Discuss the characteristics of blended threats, using the bullet points on page 356 as a guide.
16. Discuss the possible prevention of blended threats.

## **Quick Quiz 1**

1. Which of the following attacks denies service to authorized users by causing a computer to perform a task (often an unproductive task) repeatedly, thereby making the system unavailable to perform the work it is designed to do?
  - a. Browsing
  - b. Trojan horse
  - c. DoS
  - d. TrapdoorsAnswer: c
2. Which of the following accurately describes the difference between a Trojan horse and a worm?
  - a. A worm needs no user intervention to replicate.
  - b. A Trojan horse needs no user intervention to replicate.
  - c. A worm is open-source code and attacks only open-source software.
  - d. A Trojan horse is built to take advantage of a security hole in an existing application.Answer: a
3. A(n) \_\_\_\_\_ is a virus that is disguised as a legitimate or harmless program that sometimes carries within itself the means to allow the program's creator to secretly access the user's system.  
Answer: Trojan horse

## System Protection

1. Provide students with an overview of system protection. Emphasize that there is no single guaranteed method of protecting a system from assault because invasive programs evolve over time, becoming more and more adept at evading the increasingly sophisticated system defenses.
2. List different system vulnerabilities, such as file downloads, e-mail exchange, vulnerable firewalls, and improperly configured Internet connections.
3. Outline the following four protection methods: antivirus software, firewalls, restrictive access, and encryption.

### Antivirus Software

1. Provide students with an overview of antivirus software. Point out that software to combat viruses can be preventive, diagnostic, or both. Discuss the characteristics of preventive and diagnostic software.
2. Discuss the necessity of using the most current antivirus software for uncovering viruses.
3. List some organizations (and their Web sites) that are dedicated to system security and provide information about current viruses. Use Table 11.5 on page 357 as a guide.
4. Outline the structural differences between viruses, worms, and Trojans. Point out that antivirus software is generally unable to repair worms, Trojan horses, or blended threats. The only way to remove them is to remove the entire body of the malicious program. Use Figure 11.4 on page 357 to illustrate how a virus works by infecting an otherwise clean file.

<b>Teaching Tip</b>	Refer to the following Web sites for information about current viruses: <a href="http://csrc.nist.gov">http://csrc.nist.gov</a> <a href="http://www.cert.org">www.cert.org</a> <a href="http://www.mcafee.com">www.mcafee.com</a>
---------------------	--

### Firewalls

1. Provide students with an overview of a firewall, which is a set of hardware and/or software designed to protect a system by disguising its IP address from unauthorized users.
2. Use Figure 11.5 on page 359 to illustrate a firewall pictorially.
3. Outline the typical tasks of a firewall using the bullet points on page 358 as a guide.

4. Discuss the concepts of packet filtering and proxy servers. These are the two fundamental mechanisms used by firewalls to perform their tasks.

### Authentication

1. Provide students with an overview of authentication, which is verification that an individual trying to access a system is authorized to do so.
2. Explain Kerberos, a network authentication protocol developed as part of the Athena Project at MIT. Discuss its key features, such as:
  - a. It provides strong authentication for client/server applications.
  - b. It uses strong cryptography.
  - c. It requires systematic revocation of access rights from clients who no longer deserve to have access.
3. Explain the workings of Kerberos, using Figure 11.6 on page 360 as a guide.

<b>Teaching Tip</b>	A free open-source implementation of Kerberos (under copyright permissions) is available from MIT at: <a href="http://web.mit.edu/kerberos/">http://web.mit.edu/kerberos/</a> .
---------------------	---

### Encryption

1. Provide students with an overview of encryption, the most extreme protection method for sensitive data in which data is put into a secret code. Point out that to communicate with another system, data is encrypted, transmitted, decrypted, and processed.
2. Discuss the concepts of private key and public key, which are essential elements in encryption.
3. Point out the disadvantages of encryption, such as the fact that it increases system overhead and the system becomes very dependent on the encryption process itself.
4. Briefly discuss sniffers and spoofing attacks. Point out that sniffer attacks are particularly problematic in wireless networks, and spoofing is used when unauthorized users want to disguise themselves as friendly sites.

### Password Management

1. Provide students with a brief overview of password management. Outline the two most basic techniques used to protect hardware and software investments: good passwords and careful user training.

## **Password Construction**

1. Discuss the key features of passwords. These include:
  - a. A good password is unusual, memorable, and changed often.
  - b. Password files are normally stored in encrypted form.
  - c. Password length has a direct effect on the ability of a password to survive password cracking attempts.
2. List several reliable techniques for generating a good password, using the bullet points listed on pages 364-365 as a guide.
3. Explain briefly the dictionary attack, pointing out its requirements and possible prevention techniques from this attack.

## **Password Alternatives**

1. Discuss alternatives to passwords, such as smart cards and biometrics. Explain how these techniques are used to provide security. Emphasize that they require “something you have and something you know.”
2. Describe the use of fingerprints in biometrics.
3. Explain a newer password technique involving the use of graphics and a pattern of clicks using a mouse, stylus, touch screen, or other pointing device. Describe the advantage of this evolving technique. Use Figure 11.9 on page 366 to illustrate this concept.

## **Social Engineering**

1. Provide students with an overview of social engineering, which is a technique whereby system intruders gain access to information about a legitimate user to learn active passwords.
2. Outline different methods used in social engineering to learn active passwords. Describe how this technique has even been effective against military targets, as discussed on page 367 in the text.
3. Discuss phishing, which is a form of social engineering whereby an intruder pretends to be a legitimate entity and contacts unwary users asking them to reconfirm their personal and/or financial information. Provide an example with the 2003 eBay case.
4. Discuss the unique vulnerabilities default passwords pose to system security.

## **Ethics**

1. Provide students with an overview of ethics. Point out that the IEEE and ACM issued a standard of ethics in 1992 for the global computing community.

2. Outline the consequences of ethical lapses, using the bullet points on pages 367-368 as a guide.
3. Outline specific activities to teach ethics, using the bullet points on page 368 as a guide.

<b><i>Teaching Tip</i></b>	For a guide to ethical behavior, see excerpts from the ACM Code of Ethics and Professional Conduct at <a href="http://www.acm.org">www.acm.org</a> .
----------------------------	--

## **Quick Quiz 2**

1. Which of the following attacks is targeted by exploiting human nature and human behavior?
  - a. Browsing
  - b. Social engineering
  - c. Brute Force
  - d. SpoofingAnswer: b
2. Which of the following attacks works by modifying the source address of traffic over the network?
  - a. Spoofing
  - b. Sniffers
  - c. DoS
  - d. TrapdoorsAnswer: a
3. (True or False) In general, the only way to remove a Trojan horse is to remove the entire body of the malicious program.  
Answer: True

## **Class Discussion Topics**

1. Have students discuss vulnerabilities surrounding the computing world today and the risks of computers being attacked. Do they think that companies are doing enough to make the computing environment safe? Why or why not?
2. Do students agree that the Internet poses a great threat to the security of a computing society? Why or why not? What security measures do they take in order to safeguard their computers?

## Additional Projects

1. Have students research online to find details on Microsoft's monthly updates service, which is aimed at providing security. Ask students to compile a list of key features of this service.
2. Have students research current literature to find the current state firewall design. Ask them to list at least five commercially available products with their cost, key features, and pros and cons.

## Additional Resources

1. Microsoft.com:  
[www.microsoft.com](http://www.microsoft.com)
2. Microsoft Security Central:  
[www.microsoft.com/security/guidance](http://www.microsoft.com/security/guidance)
3. NTBugtraq for tracking the vulnerabilities:  
[www.ntbugtraq.com](http://www.ntbugtraq.com)
4. Symantec Corp.:  
[www.symantec.com](http://www.symantec.com)
5. U.S. Computer Emergency Readiness Team:  
[www.us-cert.gov/cas/techalerts/](http://www.us-cert.gov/cas/techalerts/)

## Key Terms

- **Access control:** the control of user access to a network or computer system.
- **Antivirus software:** software that is designed to detect and recover from attacks by viruses and worms. It is usually part of a system protection software package.
- **Authentication:** the means by which a system verifies that the individual attempting to access the system is authorized to do so.
- **Backup:** the process of making long-term archival file storage copies of files on the system.
- **Blended threat:** a system threat that combines into one program the characteristics of other attacks, including a virus, worm, Trojan horse, spyware, and other malicious code.
- **Biometrics:** the science and technology of identifying authorized users based on their biological characteristics.
- **Browsing:** a system security violation in which unauthorized users are allowed to search through secondary storage directories or files for information they should not have the privilege to read.
- **Cleartext:** in cryptography, a method of transmitting data without encryption, in text that is readable by anyone who sees it.

- **Cryptography:** the science of coding messages or text so unauthorized users cannot read them.
- **Denial of service (DoS) attack:** an attack on a network that makes it unavailable to perform the functions it was designed to do. This can be done by flooding the server with meaningless requests or information.
- **Dictionary attack:** the technique by which an intruder attempts to guess user passwords by trying words found in a dictionary.
- **Encryption:** translation of a message or data item from its original form to an encoded form, thus hiding its meaning and making it unintelligible without the key to decode it. Used to improve system security and data protection.
- **Ethics:** the rules or standards of behavior that individuals are expected to follow demonstrating the principles of right and wrong.
- **Firewall:** a set of hardware and software that disguises the internal network address of a computer or network to control how clients from outside can access the organization's internal servers.
- **Kerberos:** MIT-developed authentication system that allows network managers to administer and manage user authentication at the network level.
- **Logic bomb:** a virus with a trigger, usually an event, that causes it to execute.
- **Packet filtering:** reviewing incoming and outgoing Internet packets to verify that the source address, destination address, and protocol are correct. Usually a function of a firewall.
- **Packet sniffer:** software that intercepts Internet data packets sent in cleartext and searches them for information, such as passwords.
- **Password:** a user-defined access control method. Typically a word or character string that a user must specify in order to be allowed to log on to a computer system.
- **Phishing:** a technique used to trick consumers into revealing personal information by appearing as a legitimate entity.
- **Private key:** a tool that's used to decrypt a message that was encrypted using a public key.
- **Proxy server:** a server positioned between an internal network and an external network or the Internet to screen all requests for information and prevent unauthorized access to network resources.
- **Public key:** a tool that's used to encrypt a message, to be decoded later using a private key.
- **Recovery:** the steps that must be taken when a system is assaulted, to recover system operability and, in the best case, recover any lost data.
- **Smart card:** a small, credit-card-sized device that uses cryptographic technology to control access to computers and computer networks. Each smart card has its own personal identifier, which is known only to the user, as well as its own stored and encrypted password.
- **Social engineering:** a technique whereby system intruders gain access to information about a legitimate user to learn active passwords, sometimes by calling the user and posing as a system technician.
- **Spoofing:** the creation of false IP addresses in the headers of data packets sent over the Internet, sometimes with the intent of gaining access when it would not otherwise be granted.
- **Spyware:** a blended threat that covertly collects data about system users and sends it to a designated repository.

- **System survivability:** the capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents.
- **Time bomb:** a virus with a trigger linked to a certain year, month, day, or time that causes it to execute.
- **Trapdoor:** an unspecified and undocumented entry point to the system, which represents a significant security risk.
- **Trojan horse:** a malicious computer program with side effects that are not intended by the user who executes the program.
- **Virus:** a program that replicates itself by incorporating itself into other programs, including those in secondary storage, that are shared among other computer systems.
- **Wiretapping:** a system security violation in which unauthorized users monitor or modify a user's transmission.
- **Worm:** a computer program that replicates itself and is self-propagating in main memory.