Instructor's Manual Materials to Accompany
INFORMATION SECURITY PRINCIPLES AND PRACTICES

CHAPTER 2
INFORMATION SECURITY PRINCIPLES OF SUCCESS

CHAPTER OBJECTIVES

When students have finished reading this chapter, they will be able to:

- Build an awareness of 12 generally accepted basic principles of information security to help you determine how these basic principles are applied to real-life situations.
- Distinguish between the three main security goals.
- Learn how to design and apply the principle of "Defense in Depth."
- Comprehend human vulnerabilities in security systems to better design solutions to counter them.
- Explain the difference between functional and assurance requirements.
- Comprehend the fallacy of *security through obscurity* to avoid using it as a measure of security.
- Comprehend the importance of risk analysis and risk management tools and techniques for balancing the needs of business.
- Determine which side of the open disclosure debate you would take.

CHAPTER OVERVIEW

This chapter describes the 12 basic principles of information security. Students learn the importance of taking a principles-based approach to risk management, as well as the three primary goals of information security.

The major sections in this chapter are:

1. Principle 1: There Is No Such Thing as Absolute Security Explains that no information system can ever be totally secure, but can be configured to minimize risks.

2. Principle 2: The Three Security Goals Are Confidentiality, Integrity, and Availability Discusses the three primary goals of information security.

3. Principle 3: Defense in Depth as Strategy Explains the importance of creating a layered defense around any information system.

4. Principle 4: When Left on Their Own, People Tend to Make the Worst Security Decisions Discusses the need for security-minded professionals in any organization where people use the information system.

5. Principle 5: Computer Security Depends on Two Types of Requirements: Functional and Assurance Explains the need for verification and validation of products, processes, and systems to ensure they function correctly.

6. Principle 6: Security Through Obscurity Is Not an Answer Dispels the myth that hiding details about security mechanisms enhances security.

7. Principle 7: Security = Risk Management Explains simple methods for evaluating the risk level of any information system.

8. Principle 8: The Three Types of Security Controls Are Preventative, Detective, and Responsive Tells students how to recognize security-related products and processes as belonging in one of these categories.

9. Principle 9: Complexity Is the Enemy of Security Explains the need for simplicity in designing and maintaining an information system.

10. Principle 10: Fear, Uncertainty, and Doubt Do Not Work in Selling Security Discusses the benefits of taking a business-centric approach (as opposed to scare tactics) when convincing management to make security investments.

11. Principle 11: People, Process, and Technology Are All Needed to Adequately Secure a System or Facility Describes the unique roles that people, processes, and technology play in information security, and how they interact to enhance security.

12. Principle 12: Open Disclosure of Vulnerabilities Is Good for Security! Explains how open communications among IT professionals and users can improve security.

CHAPTER OUTLINE

I. Chapter Objectives

II. Introduction

III. Principle 1: There Is No Such Thing as Absolute Security

IV. Principle 2: The Three Security Goals Are Confidentiality, Integrity, and Availability

Integrity Models

Availability Models

V. Principle 3: Defense in Depth as Strategy

VI. Principle 4: When Left on Their Own, People Tend to Make the Worst Security Decisions

VII. Principle 5: Computer Security Depends on Two Types of Requirements: Functional and Assurance

VIII. Principle 6: Security Through Obscurity Is Not an Answer

IX. Principle 7: Security = Risk Management

X. Principle 8: The Three Types of Security Controls Are Preventative, Detective, and Responsive

XI. Principle 9: Complexity Is the Enemy of Security

XII. Principle 10: Fear, Uncertainty, and Doubt Do Not Work in Selling Security

XIII. Principle 11: People, Process, and Technology Are All Needed to Adequately Secure a System or Facility

XIV. Principle 12: Open Disclosure of Vulnerabilities Is Good for Security!

XV. Summary

XVI. Test Your Skills

Multiple Choice Questions

Exercises

Projects

TEACHING NOTES

I. Principle 1: There Is No Such Thing as Absolute Security

Teaching Tips: Pose this question to students: "If no system can be made absolutely secure, then why bother with security at all?" List students' answers on the board.

II. Principle 2: The Three Security Goals Are Confidentiality, Integrity, and Availability

Teaching Tips: Ask students to give examples of the "principle of least privilege." Students should think about specific types of workers and the kinds of information such workers do and do not need in order to perform their jobs.

III. Principle 3: Defense in Depth as Strategy

Teaching Tips: Compare and contrast layered security (defense in depth) with perimeter security. Provide detailed examples of each type of system.

IV. Principle 4: When Left on Their Own, People Tend to Make the Worst Security Decisions

Teaching Tips: Ask students if they have ever received an e-mail virus. How did it appear? What did students do?

Teaching Tips: Has your own system ever been struck by a computer virus? If so, share your experience with the class. How did your system get infected? Did any damage result? How did you deal with the problem? What did you learn from the experience?

V. Principle 5: Computer Security Depends on Two Types of Requirements: Functional and Assurance

Teaching Tips: Offer students some examples of specific kinds of verification and validation that must be done in the information security field. Note that this practice applies not only to hardware and software vendors, but also to IT departments that purchase and deploy such products.

VI. Principle 6: Security Through Obscurity Is Not an Answer

Teaching Tips: Ask students for one example of "security through obscurity" in a non-IT field. Does the practice seem to work well in that field? Why or why not?

VII. Principle 7: Security = Risk Management

Teaching Tips: Help students apply the risk-analysis matrix (page 28) to your school's information system. Based on the class' findings, what actions should be taken to enhance the system's security?

VIII. Principle 8: The Three Types of Security Controls Are Preventative, Detective, and Responsive

Teaching Tips: List several components of a complete information security system—both technical and non-technical. Ask students to categorize each item or practice as preventative, detective, or responsive.

IX. Principle 9: Complexity Is the Enemy of Security

Teaching Tips: Note that even if system complexity is not a problem for the IT staff that runs the system, it may be a problem for users. This is just one way complexity can be counterproductive.

X. Principle 10: Fear, Uncertainty, and Doubt Do Not Work in Selling Security

Teaching Tips: Ask students for examples of "scare tactics" that IT professionals might use to convince managers to invest in security. Then ask for examples of sound arguments to "sell" managers on the same kinds of investments.

XI. Principle 11: People, Process, and Technology Are All Needed to Adequately Secure a System or Facility

Teaching Tips: Ask students to describe specific examples of how separation of duties might be applied in an IT department. Ask students to explain how their examples enhance security.

XII. Principle 12: Open Disclosure of Vulnerabilities Is Good for Security!

Teaching Tips: Pose this question to the class: "As an IT manager, how could you notify workers of a potential security problem without letting word slip out into the larger community? Would it even be possible to do so?"

PROJECTS/EXERCISES

I. **Discussion Questions**

A. Discussion Question 1

Get into the mindset of a truly determined hacker. Why would someone devote tremendous time and energy to trying to break into an information system? What could the reward be? Discuss this question as a group.

Answer: Students' answers will vary. Successful students will focus on the motivations of hackers, whether that motivation is money, fame, reputation, or simply proving themselves.

B. Discussion Question 2

The CIA triad treats confidentiality, integrity, and availability as equally important. Do you agree, or do you feel that one of these goals is more important than the others? Discuss this as a group and be prepared to support your views.

Answer: Students' answers will vary. Although security professionals typically place equal importance on confidentiality, integrity, and availability, each is important in its own way. Successful students will understand why each goal is so important.

II. Web Projects

A. Web Project 1

Search the Web for information about the CIA triad. How does this concept impact security efforts in the real world? Create a brief presentation based on your findings.

Answer: Students' answers will vary, but successful students should be able to find information about the CIA triad, which helps them reach conclusions about its importance.

B. Web Project 2

Go online and search for information about a commercial off-the-shelf program that had a serious security problem. Describe the problem in a brief paper. Be prepared to share your findings with the class.

Answer: Students' answers will vary. Encourage each student to focus on a unique example of such a problem. Discourage the class from focusing on one software company's products; remind students that many manufacturers' programs suffer security weaknesses, as well. Successful students will describe the problem, the damage (or potential damage) it causes, and steps users must take to remedy the problem. If possible, students should determine who discovered the problem, who alerted the public to the problem, and how involved the manufacturer was in solving the problem.

C. Web Project 3

Go online and look for information about a specific buffer overflow vulnerability in a commercial software product. Write a short report detailing the vulnerability and any attacks that have exploited that vulnerability.

Answer: Students' answers will vary. Successful students will describe the problem, the damage (or potential damage) it causes, and steps users must take to remedy the problem. If possible, students should determine who discovered the problem, who alerted the public to the problem, and how involved the manufacturer was in solving the problem. Truly successful students will also locate the exploit for the vulnerability, reveal its source, and describe how the exploit works.

WEB RESOURCES

- http://www.247.prenhall.com/ Pearson/Prentice Hall product support

CHAPTER REVIEW/ANSWERS TO TEST YOUR SKILLS

Multiple Choice Questions

1. A

2. C

3. B

4. A

5. C

6. C

7. C

8. A

9. C

10. D

11. A

12. B

13. B

14. B

15. D

Exercises

EXERCISE 2.1: THE IMPORTANCE OF INFORMATION CONFIDENTIALITY

Students' answers will vary but should include issues such as customer privacy, enforcing the 'need to know' or least privilege principle, and trade secret protection. Abuses of unprotected information might include ID theft and theft or sale of trade secrets that lead to bad press, loss of customer confidence, loss of business, negative effects in stock prices, etc. Fraud and theft can be reduced through the proper implementation of controls for confidentiality.

EXERCISE 2.2: REAL-WORLD DEFENSE IN DEPTH

Students' answers will vary. Some examples should include the Pentagon, the Alamo, corporate office buildings with entry into various areas that include badging, biometrics, etc.

EXERCISE 2.3: AVOIDING SECURITY THROUGH OBSCURITY

Security through obscurity is a poor idea because it relies on keeping the means of security a secret from outsiders; once exposed, the entire security system fails. Cryptography systems are one of the better examples where keeping the algorithm a secret is a poor idea since no one can validate the security of the system; and once it is discovered, the entire system and protected data may be at risk.

EXERCISE 2.4: FINDING POOR SECURITY WITHIN SOCIETY

Students' answers will vary. Some examples should include security researchers who entice people into giving up their passwords for a trivial gift (a pen, a piece of candy, etc.). Other good examples should include:

- Phishing
- Downloading attachments
- Clicking on links to sites that download adware, spyware, etc.

EXERCISE 2.5: RISK MANAGEMENT IN ACTION

Students' answers will vary. Good answers should include determining where a piece of software comes from, copyright issues related to downloaded music, etc.

Projects

PROJECT 2.1: E-MAIL-BORNE VIRUSES

Students’ answers will vary based on what sites they visit, which viruses they choose to research, and where they locate information about user education and successful deployments of anti-virus tools and updates.

PROJECT 2.2: HACKERS COME IN MANY COLORS

Students’ answers will vary based on their own opinions on hackers and full disclosure. Discussions of Gray Hat hackers should include their desire to help improve the security of commercial products, but also that they are not too particular with whom they share information and that they often have a desire to gain press or notoriety in discovering and publishing information on new vulnerabilities or new exploits to known vulnerabilities.

PROJECT 2.3: COMPARING PHYSICAL AND VIRTUAL RISK MANAGEMENT TECHNIQUES

Risk management activity should be the same for physical or electronic assets. Differences will show up in threats to physical vs. electronic asset and skills of the attacker. Other elements of risk management should be the same, including how Single Loss Expectancy is determined, assigning rankings based on risk, and cost-benefit analysis of countermeasures to risks.

Case Study

Student answers will vary but should include examples of how defense in depth can be implemented to protect borders (perimeters) and multiple lines of protection to get to the center where assets are deemed most valuable.

