Chapter 1: Security Blanket or Security Theater?

This chapter is intended to introduce the student to the entire field of computer and information security. It defines important terms and concepts, such as threat, vulnerability, countermeasure, method, opportunity, motive, attack, harm, confidentiality, integrity, and availability. The student must understand these terms well, because they are fundamental to understanding everything else in this book. Therefore, these exercises are important for determining whether a student is ready to move on to the more specific chapters of the rest of the book.

Instructional Suggestions

Because this chapter introduces the student to many fundamental concepts, it is important to present them slowly and carefully. You may want to present a topic, such as method–opportunity–motive, and then challenge your students to cite examples of those elements from everyday experience or recent incidents. Fortunately, the news media are replete with examples in the area of computer security.

Chapter Exercises

1. List at least three kinds of harm a company could experience from electronic espionage or unauthorized viewing of company confidential materials.

   Loss of business or competitive advantage, public embarrassment (leading to loss of business), legal action for failing to maintain secrecy of protected data (such as healthcare data, employee private data, personal financial data).

2. List at least three kinds of harm a student could experience from electronic espionage or unauthorized viewing of personal materials.

   Public humiliation, loss of friends' confidence, legal action for failing to maintain secrecy of protected data.

3. Describe a situation in which complete denial of service to a user (that is, the user gets no response from the computer) is a serious problem to that user. Describe a situation in which 10% denial of service (that is, the response from the computer is 10 percent slower than normal) is a serious problem to a user.

   Complete denial of service: any critical computing task, such as computer-assisted education, real-time accounting, or word processing for a student preparing a paper. Loss of 10 percent service: Computer-assisted medicine (surgery or drug dosing), streaming audio or video, or competitive online merchandising.

4. Consider the web site of an organization many people would support, for example, an environmental group or a charity. List at least three classes of people who might attack that web site. What are their motives? Consider the web site of a controversial organization, for example, a group of extreme ideology. List at least three classes of people who might attack that web site. What are their motives? Can you build a list of three classes that would attack both types of sites?

   Charity: opponents of the cause, rivals, undirected (random) attackers. Controversial: same.

5. Do you think attempting to break in to (that, is obtain access to or use of) a computing system is ethical? Why or why not? Do you think that act should be

illegal? Why or why not? Base your answer on harm: Who is harmed, to what degree, and does benefit to the person breaking in override the harm?

First point: Ethics is not the same as law. Something can be unethical (for example, cheating on an exam) but not illegal. Breaking in harms the victim through loss of confidentiality, inappropriate modification, denial or disruption of service, or even just a sense of violation. Thus, even if nothing is "taken," it is hard to argue that breaking in is not unethical. As to legality, there are laws against breaking into certain computing systems, even without causing apparent damage. (Passing a law does not make unwanted behavior disappear, however; there are laws against murder, but murders occur daily.) Having a law may improve the likelihood or ease of prosecution.

6. Consider electronic medical records. Which of confidentiality, integrity and availability do their users require? Cite examples of each of these properties you think are required. Describe at least two kinds of people or situations that could threaten each property you name.

All three. Confidentiality to preserve patients' privacy; integrity to ensure correct treatment, and availability to ensure necessary data are available for treatment. Confidentiality, integrity, and availability can be attacked by careless medical professionals, hackers, or unscrupulous people in the industry (for example, drug manufacturers or even medical software developers).

7. Distinguish among threat, threat agent, vulnerability, harm, and control.

A *threat* is a situation with the potential to cause harm. A *threat agent* is an actor— often a person but sometimes an object such as a vicious dog, an exposed electrical wire, or a windstorm—that allows a threat to be actualized. A *vulnerability* is a weakness, a hole through which harm takes place. *Harm* is unwanted behavior. A *control* prevents, detects, deters, or otherwise mitigates the harm of a threat exploiting a vulnerability.

8. Not all kinds of computer harm are illegal. List five examples of harm that is not illegal.

Fire, floods, and other kinds of physical disasters. Harm from inadvertent human errors (other than negligent behavior). Failed or degraded access because of inadequate capacity. Hardware failures. Access failure from forgetting a password.

9. Consider the example with which this chapter began: a series of seemingly unrelated events, including failure of the communications and electrical power networks. Describe a scenario in which these could all occur concurrently but not be related. Describe a way at least one could lead to another. Describe a way you could determine the root cause of each failure.

Concurrent but unrelated: accident of nature. One leading to another: electrical failure leads to communications failure (because communications providers, such as mobile phone networks, cannot operate without power). Root cause: difficult to discern. A precise timeline would show which event occurred before, especially immediately before, others, and error logs of the electrical and communications networks would show which conditions were detected when (although time of detection is not necessarily the same as time of occurrence.)

10. Continuing from question 9, suppose you were a malicious agent assigned to cause failure of the telecommunications and electric power systems. What steps could you take to make it difficult to determine who you are? What steps could you take to make it difficult to determine that the attack was malicious and not a natural accident? What steps could you take to make it seem as though the cause was someone else, for example, a particular foreign country?

Protecting identity: Obvious first step: work remotely. Second, employ local agents as necessary, but give each only partial information so no one person understands full plot. Third, work through several layers of intermediaries. Malicious or accident: Time activity to coincide with convenient natural disaster, for example, power disruption during a thunderstorm. Cause a "natural" disaster that diverts attention, for example, an truck accident that blocks traffic on a significant highway or an electrical power surge that affects a newspaper publisher or the emergency response telephone network. Redirecting the blame: Plant "seeds" that seem to come from the country, such as messages warning of an attack or stories leaked to friendly journalists.

11. Consider a restaurant with an online reservation system for patrons. What confidentiality, integrity, and availability threats might such a system experience? Hypothesize vulnerabilities in such a system that an attacker might try to exploit. What countermeasures could be applied against these threats?

Confidentiality: acts to determine identities of patrons or to learn how much business the restaurant is doing; integrity: acts to create fictitious reservations, delete reservations, or modify existing reservations. Availability: threats of hardware failure, software failure, unacceptable performance. Vulnerabilities: software faults, unstable hardware. Countermeasures: redundancy (paper backup).

12. Suppose a payroll system secretly leaks a list of names of employees earning more than a certain amount each pay period. Who would be harmed by such a vulnerability? How could such a vulnerability come about? What controls could be instituted to counter such a vulnerability? Suppose the leakage were not just names but also employees' identification numbers and full pay amounts. Would the people harmed or the degree of harm be different? Why or why not? If the employees are the ones suffering the greatest harm, who should be responsible for countering this vulnerability: the employee or the employer? Why?

Harm: Employees, company management. Names and personal details: People harmed, the same; degree of harm, greater (more sensitive details exposed). Responsibility: The employee has little control over a payroll system, and thus can do little to protect against its faults (other than, perhaps, giving a false name to the employer, which has other negative consequences).

13. A letter arrives in the surface mail apparently from your bank, but you are skeptical of its origin. What factors would make you skeptical? How could the bank help allay your skepticism in advance of sending the letter? What could the bank put in the letter itself that would reduce your skepticism? Would your answers be the same if the bank sends email instead of a surface mail letter?

Factors: quality of stationery and printing, appearance of envelope, wording of message (including spelling and grammar), also whether the content seems reasonable. Advance warning: a notice included with the regularly-sent monthly statement alerting customers that the bank would soon send a letter and outlining

the topic. In the letter: some characteristic of the account, for example, part of the account number or reference to a recent transaction. Email: same answers.

14. Consider a program you could install on your own personal web page to display your city's current time and temperature. What threats could this program cause to you? To people who visit your web site? What controls could counter those threats?

This question is a precursor for Chapter 4 on malicious code. Any program can affect other programs in concurrent execution by modifying the other programs' code, intercepting data before or after processing by the other program, or denying access. The fact that a program has an apparently benign function—in this case time and temperature—is irrelevant.

15. Consider a program that allows people to order goods over the Internet. What threats could this program cause to users (purchasers)? What threats could this program cause to the merchant? Hypothesize three vulnerabilities that could allow these threats to be actualized.

Threats to users: confidentiality, exposure of personal data (credit card number); integrity, incorrect order (wrong item, wrong quantity, wrong price); availability: inability to order desired merchandise. Threats to merchant: exposure of customers' personal data, disclosure of customer list, disclosure of business condition (number of orders, for which products, at what prices); integrity: failure to record or retain order, recording incorrect order or modification of order, deletion of existing order; availability: customers' inability to access system (and to place orders). Vulnerabilities: software fault, power failure, inadequate capacity.

16. Suppose you are a talented sailor about to race your boat in a yachting competition. A possible threat to winning is cancellation of the event because of adverse weather conditions. List three other threats you might encounter as you try to win by posting the fastest finishing time. List three vulnerabilities those threats might exploit. List three countermeasures against those threats.

Threats: foul weather, mechanical failure of boat, inaccurate (or maliciously faulty) officials. Vulnerabilities: wind causes boat to capsize (countermeasure: mechanical stabilizers, waiting out bad weather in a safe position); rotting wood cause boat to leak (countermeasure: inspection before race); bribery (countermeasure: multiple official, independent skeptical observers).

17. Suppose you are a spy, and you need to pass secret materials to another spy, Agent Smart. However, you and Smart have never before met. You are aware that hostile forces are all around, any one of whom might try to impersonate Smart; if you approach someone and asked if she is Agent Smart, she might say she is even if she is not. Suggest a control for this threat—that is, a way you could be convinced the person to whom you are talking is really Agent Smart. Would your technique work if you assumed your telephone and mail were being monitored by the hostile agents? Suggest a way that would work even if your communications were monitored.

This problem is hard; establishing a basis for trust between two previously-unknown parties is a continuing difficulty for computer situations. This exercise leads to the shared secret problem for cryptographic key exchange (of Chapters 11 and 13). If you and Smart had a common friend (or co-worker) you could cite some common