security topics can be learned to a reasonable depth without diving too deeply into the theory. For example, cryptography can be (and often is) taught from a highly mathematical perspective. However, with rare exception, a little elementary math is all that is needed to understand cryptographic principles.

This book is certainly not an attacker's how-to guide either. Nevertheless, your practical author has consciously tried to keep the focus on real-world issues, but at a deep enough level to give the reader some understanding of—and appreciation for—the underlying concepts. The goal is to get into some depth without overwhelming the reader with excessive trivial details. Admittedly, this is a delicate balancing act and, no doubt, many will disagree that a proper balance has been struck. In your defensive author's defense, it should be noted that this book touches on a very large number of security issues related to a wide variety of fundamental principles. This breadth necessarily comes at the expense of some rigor and detail.

For those who yearn for a more theoretical treatment of the some of the topics covered here, Bishop's book [10] is the obvious choice. There are numerous fine books and articles available that focus in more detail on the various security topics discussed in this book. Your favorite search engine will quickly reveal many such sources.

1.6 Problems

The problem is not that there are problems. The problem is expecting otherwise and thinking that having problems is a problem.
— Theodore I. Rubin

1. Among the fundamental challenges in information security are confidentiality, integrity, and availability, or CIA.
   a) Define each of the terms confidentiality, integrity, and availability.
   b) Give a concrete example where both confidentiality and integrity are critically important.
   c) Give a concrete example where integrity is more important than confidentiality.
   d) Give a concrete example where availability is the overriding concern.
2. From a bank's perspective, which is likely to be more important (and why), the integrity of its customer's data or the confidentiality of the data? From the perspective of the bank's customers, which is more important (and why)?
3. Some authors distinguish between secrecy, privacy, and confidentiality. In this usage, secrecy is equivalent to our use of the term confidentiality, whereas privacy is secrecy applied to personal data, and confidentiality

(in this misguided sense) is somewhat more restrictive than the terminology as used in this book, as it refers to an obligation not to divulge certain information.

a) Discuss a real-world situation where privacy is an important security issue.

b) Discuss a real-world situation where confidentiality (in this restricted sense) is a critical security issue.

4. Cryptography is sometimes said to be "brittle," in the sense that it can be very strong, but when it breaks, it's strength is shattered.[8] In contrast, some security features can "bend" without breaking completely—security may be lost as a result of such bending, but some useful level of security can remain.

a) Other than cryptography, give an example of a security mechanism that is brittle.

b) Provide an example of a security mechanism that is not brittle, that is, the security can bend without completely breaking.

5. Read Diffie and Hellman's classic paper [30].

a) Briefly summarize the paper.

b) Diffie and Hellman give a system for distributing keys over an insecure channel (see Section 3 of the paper). How does this system work?

c) Diffie and Hellman also conjecture that a "one way compiler" might be used to construct a public key cryptosystem. Do you believe this is a plausible approach? Why or why not?

6. The most famous cipher of World War II is the German Enigma. This cipher was broken by the Allies and intelligence gained from Enigma messages proved invaluable. At first, the Allies were very careful when using the information gained from broken Enigma messages—sometimes the Allies did not use information that could have given them an advantage. However, later in the war, the Allies (and, in particular, the Americans) were much less careful, as they tended to use virtually all information obtained from broken Enigma messages.

a) Briefly discuss a significant World War II event where broken Enigma messages played a major role.

b) The Allies were cautious about using information gained from broken Enigma messages for fear that the Germans would realize their cipher was compromised. Discuss two different approaches that the Germans might have taken if they had realized that the Enigma was broken.

[8] Shadoobie [116].

c) At some point, it should have become obvious to the Germans that the Enigma was broken, yet the cipher was used until the end of the war. Why did the Nazis continue to use the Enigma?

7. When you want to authenticate yourself to your computer, most likely you type in your username and password. The username is considered public knowledge, so it is the password that authenticates you. Your password is "something you know."
   a) It is also possible to authenticate based on "something you are," that is, a physical characteristic. Such a characteristic is known as a biometric. Give an example of biometric-based authentication.
   b) It is also possible to authenticate based on "something you have," that is, something in your possession. Give an example of authentication based on something you have.
   c) Two-factor authentication requires that two of the three authentication methods (something you know, something you have, something you are) be used. Give an example from everyday life where two-factor authentication is used. Which two of the three "somethings" are used?
8. CAPTCHAs [133] are often used in an attempt to restrict access to humans (as opposed to automated processes).
   a) Give a real-world example where you were required to solve a CAPTCHA to gain access to some resource. What did you have to do to solve the CAPTCHA?
   b) Discuss various technical methods that might be used to break the CAPTCHA you described in part a) of this problem.
   c) Outline a non-technical method that might be used to attack the CAPTCHA from part a).
   d) How effective is the CAPTCHA in part a)? How user-friendly is the CAPTCHA?
   e) Do you hate solving CAPTCHAs as much as your easily-annoyed author?
9. Suppose that a particular security protocol is well designed and secure. However, there is a fairly common situation where insufficient information is available to complete the security protocol. In such cases, the protocol fails and, ideally, communication between the participants, say, Alice and Bob, should not be allowed to occur. However, in the real world, protocol designers must decide how to handle cases where protocols fail and, as a practical matter, both security and convenience must be considered. Comment on the relative merits of each of the following solutions to protocol failure. Be sure to mention the relative security and user-friendliness of each.

a) When the protocol fails, a brief warning is given to Alice and Bob, but communication is allowed to continues as if the protocol had succeeded, without any intervention required from either Alice or Bob.

b) When the protocol fails, a warning is given to Alice and she decides (by clicking a checkbox) whether communication is allowed to continue or not.

c) When the protocol fails, a notification is given to Alice and Bob and the protocol terminates.

d) When the protocol fails, the protocol terminates, with no explanation given to Alice or Bob.

10. Automatic teller machines (ATMs) are an interesting case study in security. Anderson [3] claims that when ATMs were first developed, most attention was paid to high-tech attacks. However, most real-world attacks on ATMs were decidedly low tech.

    a) Examples of high-tech attacks on ATMs would include breaking the encryption or authentication protocol. If possible, find a real-world case where a high-tech attack on an ATM has actually occurred and provide the details.

    b) Shoulder surfing is an example of a low-tech attack. In a shoulder-surfing scenario, Trudy stands behind Alice in line and watches the numbers Alice presses when entering her PIN. Then Trudy bonks Alice in the head and takes her ATM card. Give another example of a low-tech attack on an ATM that has actually occurred in the real world.

11. Large and complex software systems invariably have many bugs.

    a) For honest users, such as Alice and Bob, buggy software is certainly annoying but why is it a security issue?

    b) Why does Trudy love buggy software?

12. Malware is software that is intentionally malicious, that is, malware is designed to do damage or break the security of a system. Malware comes in many familiar varieties, including viruses, worms, and Trojans.

    a) Has your computer ever been infected with malware? If so, what did the malware do and how did you get rid of the problem? If not, how have you been so lucky?

    b) In the past, most malware was designed to annoy users. Today, it is believed (with good evidence) that most malware is written for profit. How could malware possibly be profitable?

13. In the movie *Office Space*, software developers attempt to modify company software so that for each financial transaction, any leftover fraction

of a cent goes to the software developers, instead of staying where it belongs—with the company. The idea is that for any particular transaction, nobody will notice the missing fraction of a cent, but over time the developers will accumulate a large sum of money. This type of attack is sometimes known as a *salami attack*.

a) Discuss a real-world example of a salami attack.

b) In the movie, the salami attack fails. Why?

14. It has been said that "complexity is the enemy of security".

    a) Give an example of commercial software to which this statement applies, that is, find an example of software that is large and complex and has had significant security problems.

    b) Find a security protocol to which this statement applies.

15. Suppose that this textbook was sold online (as a PDF) by your money-grubbing author for, say, $5. Then the author would make more money off each copy sold than he currently does[9] and people who purchase the book would save a lot of money.

    a) What are the security issues related to the sale of an online book?

    b) How could you make the selling of an online book more secure, from the copyright holder's perspective?

    c) How secure is your approach in part b)? How user-friendly is your approach in part b)? What are some possible attacks on your proposed system?

16. The PowerPoint slides at [135] describe a security class project where students successfully hacked the Boston subway system.

    a) Summarize each of the various attacks. What was the crucial vulnerability that enabled each attack to succeed?

    b) The students planned to give a presentation at the self-proclaimed "hacker's convention," Defcon. At the request of the Boston transit authority, a judge issued a temporary restraining order that prevented the students from talking about their work. Do you think this was justified, based on the material in the slides?

    c) What are war dialing and war driving? What is war "carting"?

    d) Comment on the production quality of the "melodramatic video about the warcart" (a link to the video can be found at [124]).

[9] Believe it or not.