
CHAPTER 1

Introduction

(Solution to Practice Set)

Review Questions

1. The three security goals are *confidentiality*, *integrity*, and *availability*.

- ☐ *Confidentiality* means protecting confidential information.
- ☐ *Integrity* means that changes to the information need to be done only by authorized entities.
- ☐ *Availability* means that information needs to be available to authorized entities.

2.

- ☐ In a *passive attack*, the attacker's goal is just to obtain information. This means that the attack does not modify data or harm the system. Examples of passive attacks are snooping and traffic analysis.
- ☐ An *active attack* may change the data or harm the system. Attacks that threaten the integrity and availability are active attacks. Examples of active attacks are modification, masquerading, replaying, repudiation, and denial of service.

3. We mentioned five security services: *data confidentiality*, *data integrity*, *authentication*, *nonrepudiation*, and *access control*.

- ☐ *Data confidentiality* is to protect data from disclosure attack.
- ☐ *Data integrity* is to protect data from modification, insertion, deletion, and replaying.
- ☐ *Authentication* means to identify and authenticate the party at the other end of the line.
- ☐ *Nonrepudiation* protects against repudiation by either the sender or the receiver of the data.
- ☐ *Access control* provides protection against unauthorized access to data.

4. Eight security mechanisms were discussed in this chapter. *encipherment, data integrity, digital signature, authentication exchange, traffic padding, routing control, notarization, and access control.*

- ☐ *Encipherment* provides confidentiality.
- ☐ The *data integrity* mechanism appends a short checkvalue to the data. The checkvalue is created by a specific process from the data itself.
- ☐ A *digital signature* is a means by which the sender can electronically sign the data and the receiver can electronically verify the signature.
- ☐ In *authentication exchange*, two entities exchange some messages to prove their identity to each other.
- ☐ *Traffic padding* means inserting some bogus data into the data traffic to thwart the adversary's attempt to use the traffic analysis.
- ☐ *Routing control* means selecting and continuously changing different available routes between the sender and the receiver to prevent the opponent from eavesdropping on a particular route.
- ☐ *Notarization* means selecting a third trusted party to control the communication between two entities.
- ☐ *Access control* uses methods to prove that a user has access right to the data or resources owned by a system.

5.

- ☐ *Cryptography*, a word with origin in Greek, means "secret writing." We used the term to refer to the science and art of transforming messages to make them secure and immune to attacks.
- ☐ *Steganography*, a word with origin in Greek, means "covered writing." Steganography refers to concealing the message itself by covering it with something else.

Exercises

6.

- a. A *regular mail* guarantees no security services. It is the *best-effort* delivery service. The mail can be lost, altered in the mail, opened by somebody other than the intended recipient.
- b. A *regular mail with delivery confirmation* can only show that the mail has been delivered. This can only give peace of mind to the sender that the packet is not lost. However, since there is no signature from the recipient, it does not guarantee any of the security services.
- c. A *regular mail with delivery confirmation and the recipient signature* can provide nonrepudiation service only at the mail level, not the contents level. In other words, the recipient of the mail cannot deny that she has not received the mail, but she can deny that the mail contained some specific information. For

example, if Alice sends a mail with \$100 cash inside to Bob via this type of mail, Bob cannot deny that he has received the mail, but he can deny that the mail contained some cash inside. In some cases, the sender is an authority and it is enough that Bob accepts he has received the mail. In this case, if there is a dispute, the court accept the testimony of the sender about the contents.

- d. A *certified mail* is actually the same as the *regular mail with delivery confirmation and the recipient signature*.
- e. A mail can be insured. However, this is not security in the sense we are talking in this chapter. Secured mail can only provide compensation if the mail is lost.
- f. A *registered mail* is different from all of the previous delivery methods. A registered mail is carried by the post office under the tight security. This means that the confidentiality and integrity of the mail is guaranteed. Since a registered mail normally includes the signed receipt, the nonrepudiation is also guaranteed. However, nonrepudiation is only at the mail level, not the content level. The recipient of the registered mail cannot deny that the mail has been delivered, but it can deny that it contained a special message or an item of some value.

7.

- a. This is *snooping* (attack to the confidentiality of stored data). Although the contents of the test is not confidential on the day of the test, it is confidential before the test day.
- b. This is modification (attack to the integrity of data). The value of the check is changed (from \$10 to \$100).

- c. This is *denial of service* (attack to availability). Sending so many e-mails may crash the server and the service may be interrupted.

8.

- a. This provides *access control* mechanism. The process is to prove that the student has right to access the school resources.
- b. This can provide *routing control*. The school may be doing this to prevent a student from eavesdropping on a particular route.
- c. This can be *authentication exchange* mechanism. The professor needs to authenticate the student before sending the grade. The preassigned identification is a secret between the student and the professor.
- d. The mechanism is similar to *digital signature*. It can be used for two purposes. If the signature of the customer is checked against a signature on the file, it can provide authentication. The signature on the withdrawal document definitely is served as the nonrepudiation. The customer cannot later denies that she has not received the cash.

9.

- a. This is *steganography*. The answers to the test has not been changed; they have been only hidden.
- b. This is *cryptography*. The characters in the message are not hidden; they are replaced by another characters.
- c. This is *steganography*. The special ink hides the actual writing on the check.
- d. This is *steganography*. The water marks hides the actual contents of the thesis.

10. A signature on a document is like a *digital signature* on a message. It protects the integrity of the document, it provides authentication, and it protects non-repudiation.