

## *Security*

The computer resources must be guarded against unauthorized access, malicious destruction or alteration, and accidental introduction of inconsistency. These resources include information stored in the system (both data and code), as well as the CPU, memory, disks, tapes and networking that are the computer. In this chapter, we start by examining ways in which resources may be accidentally or purposefully misused. We then explore a key security enabler—cryptography. Finally, we look at mechanisms to guard against or detect attacks.

### CHAPTER OBJECTIVES

- To discuss security threats and attacks.
- To explain the fundamentals of encryption, authentication, and hashing.
- To examine the uses of cryptography in computing.
- To describe the various countermeasures to security attacks.

**16.1 The Security Problem**

**16.2 Program Threats**

**16.3 System and Network Threats**

**16.4 Cryptography as a Security Tool**

**16.5 User Authentication**

**16.6 Implementing Security Defenses**

**16.7 Firewalls**

**16.8 Summary**

**Exercises**

16.1 xx

**Bibliographical Notes**

General discussions concerning security are given by Hsiao et al. [1979], Landwehr [1981], Denning [1982], Pfleeger and Pfleeger [2003], Tanenbaum 2003, and Russell and Gangemi [1991]. Also of general interest is the text by Lobel [1986]. Computer networking is discussed in Kurose and Ross [2005].