

Chapter 1

What is Computer Security?

The meaning of the term *computer security* has evolved in recent years. Before the problem of data security became widely publicized in the media, most people's idea of computer security focused on the physical machine. Traditionally, computer facilities have been physically protected for three reasons:

- To prevent theft of or damage to the hardware
- To prevent theft of or damage to the information
- To prevent disruption of service

Strict procedures for access to the machine room are used by most organizations, and these procedures are often an organization's only obvious computer security measures. Today, however, with pervasive remote terminal access, communications, and networking, physical measures rarely provide meaningful protection for either the information or the service; only the hardware is secure. Nonetheless, most computer facilities continue to protect their physical machine far better than they do their data, even when the value of the data is several times greater than the value of the hardware.

You probably are not reading this book to learn how to padlock your PC. *Information security* is the subject of this book. Furthermore, we are limiting our study to the insider problem: the security violations perpetrated (perhaps inadvertently) by legitimate users whom padlocks and passwords cannot deter. Most computer crimes are in fact committed by insiders, and most of the research in computer security since 1970 has been directed at the insider problem.

1.1 SECRECY, INTEGRITY, AND DENIAL OF SERVICE

Throughout this book, the discussion of computer security emphasizes the problem of protecting information from unauthorized disclosure, or information secrecy. You may find it disconcerting, as you read this book, that information integrity-protecting information from unauthorized modification or destruction-seems to be receiving no sustained attention.

There are two reasons for this seemingly one-sided point of view, one historic and one technical. First, having been funded primarily by the United States government, most computer security endeavors have concentrated on maintaining the secrecy of classified information. This tradition has persisted even in commercial applications, where classified information is not the concern and where integrity, not secrecy, is often the primary goal. And second, the information disclosure problem is technically more interesting to computer security researchers, and the literature reflects this bias.

Fortunately, techniques to protect against information modification are almost always the same as (or a subset of) techniques to protect against information disclosure. This fact is consis-

tently borne out in the technical measures we will discuss. In the rare cases where the techniques differ, that fact will be pointed out explicitly.

While the definition of *computer security* used in this book does, therefore, include both secrecy and integrity, the closely related area termed *denial of service* is rarely discussed here. Denial of service can be defined as a temporary reduction in system performance, a system crash requiring manual restart, or a major crash with permanent loss of data. Although reliable operation of the computer is a serious concern in most cases, denial of service has not traditionally been a topic of computer security research. As in the case of data integrity, one reason for the lack of concern is historic: secrecy has been the primary goal of government-funded security programs. But there is also an important technical reason. While great strides have been made since the early 1970s toward ensuring secrecy and integrity, little progress has been made in solving denial of service because the problem is fundamentally much harder: preventing denial of service requires ensuring the complete functional correctness of a system—something unlikely to be done in the foreseeable future.

If denial of service is your only concern, you should refer to such topics as structured development, fault tolerance, and software reliability. Most of the techniques for building secure systems, however, also help you build more robust and reliable systems. In addition, some security techniques do address certain denial-of-service problems, especially problems related to data integrity. This book will indicate when those techniques apply.

To sum up, *security* relates to secrecy first, integrity second, and denial of service a distant third. To help you remember this, memorize the computer security researcher's favorite (tongue-in-cheek) phrase: "I don't care if it works, as long as it is secure."

1.2 TRUSTED SYSTEM EVALUATION CRITERIA

The U.S. Department of Defense has developed its own definition of computer security, documented in *Trusted Computer System Evaluation Criteria* (Department of Defense 1985), also called "the Orange Book" after the color of its cover /and hereafter shortened to "the *Criteria*"). The document employs the concept of a *trusted computing base*, a combination of computer hardware and an operating system that supports untrusted applications and users. The seven levels of trust identified by the Criteria range from systems that have minimal protection features to those that provide the highest level of security modern technology can produce (table 1-1). The Criteria attempts to define objective guidelines on which to base evaluations of both commercial systems and those developed for military applications. The National Computer Security Center, the official evaluator for the Defense Department, maintains an Evaluated Products List of commercial systems that it has rated according to the *Criteria*.

The *Criteria* is a technical document that defines many computer security concepts and provides guidelines for their implementation. It focuses primarily on general-purpose operating systems. To assist in the evaluation of networks, the National Computer Security Center has published the *Trusted Network Interpretation* (National Computer Security Center 1987), that interprets the Criteria from the point of view of network security. The *Trusted Network Interpreta-*

tion identifies security features not mentioned in the *Criteria* that apply to networks and individual components within networks, and shows how they fit into the *Criteria* ratings.

Class	Title	KeyFeatures
A1	Verified Design	Formal top-level specification and verification, formal covert channel analysis, informal code correspondence demonstration
B3	Security Domains	Reference monitor (security kernel), "highly resistant to penetration"
B2	Structured Protection	Formal model, covert channels constrained, security-oriented architecture, "relatively resistant to penetration"
B1	Labeled Security Protection	Mandatory access controls, security labeling, removal of security-related flaws
C2	Controlled Access	Individual accountability, extensive auditing, add-on packages
C1	Discretionary	Discretionary access controls, protection against accidents among cooperating users
D	Minimal Protection	Unrated

Table 1-1. Trusted System Evaluation Criteria Ratings. In order for a system to be assigned a rating, it must meet all the technical requirements for its class in the four areas of security policy, accountability, assurance, and documentation. The requirements are cumulative, moving from class D to class A1.

You can be sure that a system rated high according to the *Criteria* (that is, at class A1 or B3) has been subject to intense scrutiny, because such systems are intended to protect classified military information. In order to attain such a high rating, a system has to be designed with security as its most important goal. While systems rarely qualify for any rating without some changes, most commercial operating systems can achieve a C1 or C2 level with a few enhancements or add-on packages. The Evaluated Products List is short because the *Criteria* is relatively new and evaluations take a long time. Also, many vendors have not yet shown an interest in submitting their products for evaluation.

While most of the technical concepts in the *Criteria* are covered in this book, we will pay little attention to its rating scale. If your interest is in developing a system for United States government

use, the scale is important; for other applications, you will be more interested in specific features than in the ratings.

REFERENCES

Department of Defense. 1985a. DoD Trusted Computer System Evaluation Criteria. DOD 5200.28-STD. Washington, D.C.: Department of Defense. (U.S. Government Printing Office number 008-000-00461-7.)

The DoD criteria for evaluating and rating operating systems according to a scale based on security features and assurance. This document discusses many of the computer security concepts covered in this book.

National Computer Security Center. 1987. Trusted Network Interpretation. NCSC-TG-005. Ft. George G. Meade, Md.: National Computer Security Center.

An interpretation of the Trusted Computer System Evaluation Criteria for networks and network components.