CHAPTER 0

READER'S GUIDE

This book, with its accompanying Web site, covers a lot of material. Here we give the reader an overview.

0.1 OUTLINE OF THIS BOOK

Following an introductory chapter, Chapter 1, the book is organized into six parts:

Part One: Computer Security Technology and Principles: This part covers technical areas that must underpin any effective security strategy. The first chapter lists the key cryptographic algorithms, discusses their use, and discusses issues of strength. The remaining chapters in this part look at specific technical areas of computer security: authentication, access control, database security, intrusion detection, malicious software, denial of service, firewalls, and trusted computing and multilevel security.

Part Two: Software Security: This part covers issues concerning software development and implementation, including operating systems, utilities, and applications. Chapter 11 covers the perennial issue of buffer overflow, while Chapter 12 examines a number of other software security issues.

Part Three: Management Issues: This part is concerned with management aspects of information and computer security. Chapter 13 looks at physical security measures that must complement the technical security measures of Part One. Chapter 14 examines a wide range of human factors issues that relate to computer security. A vital management tool is security auditing, examined in Chapter 15. Chapters 16 and 17 focus specifically on management practices related to risk assessment, the setting up of security controls, and plans and procedures for managing computer security. Finally, Chapter 18 examines legal and ethical aspects of computer security.

Part Four: Cryptographic Algorithms: Many of the technical measures that support computer security rely heavily on encryption and other types of cryptographic algorithms. Part Four is a technical survey of such algorithms.

Part Five: Internet Security: This part looks at the protocols and standards used to provide security for communications across the Internet. Chapter 21 discusses some of the most important security protocols for use over the Internet. Chapter 22 looks at various protocols and standards related to authentication over the Internet.

Part Six: Operating System Security: This part examines in detail the security approach of two widely-used operating systems: Windows (including the new Windows Vista) and Linux. These two operating systems serve as case studies in the implementation of security measures for operating systems.

The appendices following Part Six cover additional topics relevant to the book. Online appendices at this book's Web site cover additional, specialized topics.

0.2 A ROADMAP FOR READERS AND INSTRUCTORS

This book covers a lot of material. For the instructor or reader who wishes a shorter treatment, there are a number of alternatives.

To thoroughly cover the material in the first two parts, the chapters should be read in sequence. If a shorter treatment in **Part One** is desired, the reader may choose to skip Chapters 5 (Database Security) and 10 (Trusted Computing and Multilevel Security).

Although **Part Two** covers software security, it should be of interest to users as well as system developers.

The chapters in **Part Three** are relatively independent of one another, with the exception of Chapters 18 (IT Security Management and Risk Assessment) and 19 (IT Security Controls, Plans, and Procedures). The chapters can be read in any order and the reader or instructor may choose to select only some of the chapters.

Part Four provides technical detail on cryptographic algorithms for the interested reader.

Part Five covers Internet security and can be read at any point after Part One.

Part Six covers OS security using Linux and Windows Vista as examples. This part can be read at any point after Part Two.

0.3 INTERNET AND WEB RESOURCES

There are a number of resources available on the Internet and the Web to support this book and to help one keep up with developments in this field.

Web Sites for this Book

A special Web page has been set up for this book at **WilliamStallings.com/CompSec/CompSec1e.html.** The site includes the following:

- **Useful Web sites:** There are links to other relevant Web sites, organized by chapter.
- **Errata sheet:** An errata list for this book will be maintained and updated as needed. Please e-mail any errors that you spot to the address listed at the Web site. Errata sheets for other books by William Stallings are at **WilliamStallings.com**.
- **Figures:** All of the figures in this book in PDF (Adobe Acrobat) format.
- **Tables:** All of the tables in this book in PDF format.
- **Slides:** A set of PowerPoint slides, organized by chapter.
- **Computer security courses:** There are links to home pages for courses based on this book; these pages may be useful to other instructors in providing ideas about how to structure their course.

William Stallings also maintains the Computer Science Student Resource Site, at **WilliamStallings.com/StudentSupport.html.** The purpose of this site is to provide documents, information, and links for computer science students and professionals. Links and documents are organized into four categories:

- **Math:** Includes a basic math refresher, a queuing analysis primer, a number system primer, and links to numerous math sites
- **How-to:** Advice and guidance for solving homework problems, writing technical reports, and preparing technical presentations
- **Research resources:** Links to important collections of papers, technical reports, and bibliographies
- **Miscellaneous:** A variety of other useful documents and links

Other Web Sites

There are numerous Web sites that provide information related to the topics of this book. In subsequent chapters, pointers to specific Web sites can be found in the *Recommended Reading and Web Sites* section. Because the addresses for Web sites tend to change frequently, we have not included URLs in the book. For all of the Web sites listed in the book, the appropriate link can be found at this book's Web site. Other links not mentioned in this book will be added to the Web site over time.

Online Groups

USENET Newsgroups A number of USENET newsgroups are devoted to some aspect of computer security. As with virtually all USENET groups, there is a high noise-to-signal ratio, but it is worth experimenting to see if any meet your needs. The most relevant are as follows:

- **sci.crypt.research:** The best group to follow on cryptography. This is a moderated newsgroup that deals with research topics; postings must have some relationship to the technical aspects of cryptology.
- **sci.crypt:** A general discussion of cryptology and related topics.
- **alt.security:** A general discussion of security topics.
- **comp.security.misc:** A general discussion of computer security topics.
- **comp.security.firewalls:** A discussion of firewall products and technology.
- **comp.security.announce:** News and announcements from CERT (computer emergency response team).
- **comp.risks:** A discussion of risks to the public from computers and users.
- **comp.virus:** A moderated discussion of computer viruses.

Yahoo Groups Yahoo has more than 2000 public groups devoted to security topics, in the following subcategories: cryptography, networking, hardware, and viruses. Three of the most interesting are Infosec, securitytech, and Ring-of-Fire.

0.4 STANDARDS

Many of the security techniques and applications described in this book have been specified as standards. Additionally, standards have been developed to cover management practices and the overall architecture of security mechanisms and services. Throughout this book, we describe the most important standards in use or being developed for various aspects of computer security. Various organizations have been involved in the development or promotion of these standards. The most important (in the current context) of these organizations are as follows:

- **National Institute of Standards and Technology:** NIST is a U.S. federal agency that deals with measurement science, standards, and technology related to U.S. government use and to the promotion of U.S. private-sector innovation. Despite its national scope, NIST Federal Information Processing Standards (FIPS) and Special Publications (SP) have a worldwide impact.
- **Internet Society:** ISOC is a professional membership society with worldwide organizational and individual membership. It provides leadership in addressing issues that confront the future of the Internet and is the organization home for the groups responsible for Internet infrastructure standards, including the Internet Engineering Task Force (IETF) and the Internet Architecture Board (IAB). These organizations develop Internet standards and related specifications, all of which are published as Requests for Comments (RFCs).
- **ITU-T:** The International Telecommunication Union (ITU) is an international organization within the United Nations System in which governments and the private sector coordinate global telecom networks and services. The ITU Telecommunication Standardization Sector (ITU-T) is one of the three sectors of the ITU. ITU-T's mission is the production of standards covering all fields of telecommunications. ITU-T standards are referred to as Recommendations.
- **ISO:** The International Organization for Standardization (ISO)[1] is a worldwide federation of national standards bodies from more than 140 countries, one from each country. ISO is a nongovernmental organization that promotes the development of standardization and related activities with a view to facilitating the international exchange of goods and services, and to developing cooperation in the spheres of intellectual, scientific, technological, and economic activity. ISO's work results in international agreements that are published as International Standards.

A more detailed discussion of these organizations is contained in Appendix D.

[1]ISO is not an acronym (in which case it would be IOS), but a word, derived from the Greek, meaning *equal*.