

PEARSON
Prentice
Hall

大学计算机教育国外著名教材系列



Network Security Essentials

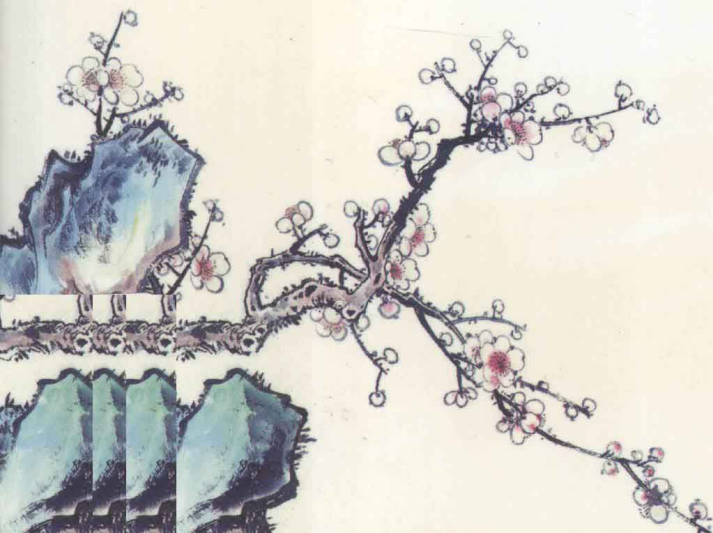
Applications and Standards
Fourth Edition

网络安全基础

应用与标准 (第4版)

William Stallings 著

清华大学出版社



大学计算机教育国外著名教材系列（影印版）

Network Security Essentials

Applications and Standards

Fourth Edition

网络安全基础

应用与标准

（第4版）

William Stallings 著

清华大学出版社
北 京

English reprint edition copyright © 2010 by PEARSON EDUCATION ASIA LIMITED and TSINGHUA UNIVERSITY PRESS.

Original English language title from Proprietor's edition of the Work.

Original English language title: Network Security Essentials: Applications and Standards, Fourth Edition by William Stallings, Copyright © 2010

All Rights Reserved.

Published by arrangement with the original publisher, Pearson Education, Inc., publishing as Prentice Hall, Inc.

This edition is authorized for sale and distribution only in the People's Republic of China (excluding the Special Administrative Region of Hong Kong, Macao SAR and Taiwan).

本书影印版由 Pearson Education (培生教育出版集团) 授权给清华大学出版社出版发行。

For sale and distribution in the People's Republic of China exclusively (except Taiwan, Hong Kong SAR and Macao SAR).

仅限于中华人民共和国境内 (不包括中国香港、澳门特别行政区和中国台湾地区) 销售发行。

北京市版权局著作权合同登记号 图字: 01-2010-3107 号

本书封面贴有 Pearson Education (培生教育出版集团) 激光防伪标签, 无标签者不得销售。
版权所有, 侵权必究。侵权举报电话: 010-62782989 13701121933

图书在版编目(CIP)数据

网络安全基础: 应用与标准=Network Security Essentials: Applications and Standards: 第4版: 英文/(美) 斯托林斯(Stallings, W.) 著.--影印本.--北京: 清华大学出版社, 2010.7
(大学计算机教育国外著名教材系列)

ISBN 978-7-302-22972-8

I. ①网… II. ①斯… III. ①计算机网络—安全技术—高等学校—教材—英文 IV. ①TP393.08

中国版本图书馆 CIP 数据核字 (2010) 第 105507 号

责任印制: 王秀菊

出版发行: 清华大学出版社

地 址: 北京清华大学学研大厦 A 座

<http://www.tup.com.cn>

邮 编: 100084

社 总 机: 010-62770175

邮 购: 010-62786544

投稿与读者服务: 010-62795954, jsjic@tup.tsinghua.edu.cn

质 量 反 馈: 010-62772015, zhiliang@tup.tsinghua.edu.cn

印 刷 者: 北京市清华园胶印厂

装 订 者: 三河市金元印装有限公司

经 销: 全国新华书店

开 本: 185×230 印 张: 27.25

版 次: 2010 年 7 月第 1 版 印 次: 2010 年 7 月第 1 次印刷

印 数: 1~3000

定 价: 46.00 元

产品编号: 037756-01

出版说明

进入 21 世纪, 世界各国的经济、科技以及综合国力的竞争将更加激烈。竞争的中心无疑是对人才的竞争。谁拥有大量高素质的人才, 谁就能在竞争中取得优势。高等教育, 作为培养高素质人才的事业, 必然受到高度重视。目前我国高等教育的教材更新较慢, 为了加快教材的更新频率, 教育部正在大力促进我国高校采用国外原版教材。

清华大学出版社从 1996 年开始, 与国外著名出版公司合作, 影印出版了“大学计算机教育丛书(影印版)”等一系列引进图书, 受到国内读者的欢迎和支持。跨入 21 世纪, 我们本着为我国高等教育教材建设服务的初衷, 在已有的基础上, 进一步扩大选题内容, 改变图书开本尺寸, 一如既往地请有关专家挑选适用于我国高校本科及研究生计算机教育的国外经典教材或著名教材, 组成本套“大学计算机教育国外著名教材系列(影印版)”, 以飨读者。深切期盼读者及时将使用本系列教材的效果和意见反馈给我们。更希望国内专家、教授积极向我们推荐国外计算机教育的优秀教材, 以利我们把“大学计算机教育国外著名教材系列(影印版)”做得更好, 更适合高校师生的需要。

清华大学出版社

*To Antigone
never dull
never boring
always a Sage*

PREFACE

“The tie, if I might suggest it, sir, a shade more tightly knotted. One aims at the perfect butterfly effect. If you will permit me _”

“What does it matter, Jeeves, at a time like this? Do you realize that Mr. Little’s domestic happiness is hanging in the scale?”

“There is no time, sir, at which ties do not matter.”

— *Very Good, Jeeves!* P. G. Wodehouse

In this age of universal electronic connectivity, of viruses and hackers, of electronic eavesdropping and electronic fraud, there is indeed no time at which security does not matter. Two trends have come together to make the topic of this book of vital interest. First, the explosive growth in computer systems and their interconnections via networks has increased the dependence of both organizations and individuals on the information stored and communicated using these systems. This, in turn, has led to a heightened awareness of the need to protect data and resources from disclosure, to guarantee the authenticity of data and messages, and to protect systems from network-based attacks. Second, the disciplines of cryptography and network security have matured, leading to the development of practical, readily available applications to enforce network security.

OBJECTIVES

It is the purpose of this book to provide a practical survey of network security applications and standards. The emphasis is on applications that are widely used on the Internet and for corporate networks, and on standards (especially Internet standards) that have been widely deployed.

INTENDED AUDIENCE

This book is intended for both an academic and a professional audience. As a textbook, it is intended as a one-semester undergraduate course on network security for computer science, computer engineering, and electrical engineering majors. It covers the material in IAS2 Security Mechanisms, a core area in the Information Technology body of knowledge; and NET4 Security, another core area in the Information Technology body of knowledge. These subject areas are part of the Draft ACM/IEEE Computer Society Computing Curricula 2005.

The book also serves as a basic reference volume and is suitable for self-study.

PLAN OF THE BOOK

The book is organized in three parts:

Part One. Cryptography: A concise survey of the cryptographic algorithms and protocols underlying network security applications, including encryption, hash functions, digital signatures, and key exchange.

Part Two. Network Security Applications: Covers important network security tools and applications, including Kerberos, X.509v3 certificates, PGP, S/MIME, IP Security, SSL/TLS, SET, and SNMPv3.

Part Three. System Security: Looks at system-level security issues, including the threat of and countermeasures for intruders and viruses and the use of firewalls and trusted systems.

In addition, this book includes an extensive glossary, a list of frequently used acronyms, and a bibliography. Each chapter includes homework problems, review questions, a list of key words, suggestions for further reading, and recommended Web sites. In addition, a test bank is available to instructors.

ONLINE DOCUMENTS FOR STUDENTS

For this new edition, a tremendous amount of original supporting material has been made available online in the following categories.

- **Online chapters:** To limit the size and cost of the book, two chapters of the book are provided in PDF format. This includes a chapter on SNMP security and one on legal and ethical issues. The chapters are listed in this book's table of contents.
- **Online appendices:** There are numerous interesting topics that support material found in the text but whose inclusion is not warranted in the printed text. Seven online appendices cover these topics for the interested student. The appendices are listed in this book's table of contents.
- **Homework problems and solutions:** To aid the student in understanding the material, a separate set of homework problems with solutions are provided. These enable the students to test their understanding of the text.
- **Supporting documents:** A variety of other useful documents are referenced in the text and provided online.
- **Key papers:** Twenty-Four papers from the professional literature, many hard to find, are provided for further reading.

Purchasing this textbook new grants the reader six months of access to this online material.

INSTRUCTIONAL SUPPORT MATERIALS

To support instructors, the following materials are provided.

- **Solutions Manual:** Solutions to end-of-chapter Review Questions and Problems.
- **Projects Manual:** Suggested project assignments for all of the project categories listed subsequently in this Preface.
- **PowerPoint Slides:** A set of slides covering all chapters, suitable for use in lecturing.
- **PDF Files:** Reproductions of all figures and tables from the book.
- **Test Bank:** A chapter-by-chapter set of questions.

All of these support materials are available at the Instructor Resource Center (IRC) for this textbook, which can be reached via pearsonhighered.com/stallings or by clicking on the button labeled "Book Info and More Instructor Resources" at this book's Web site WilliamStallings.com/Crypto/Crypto5e.html. To gain access to the IRC, please contact your

local Prentice Hall sales representative via pearsonhighered.com/educator/replocator/requestSalesRep.page or call Prentice Hall Faculty Services at 1-800-526-0485.

INTERNET SERVICES FOR INSTRUCTORS AND STUDENTS

There is a Web page for this book that provides support for students and instructors. The page includes links to other relevant sites, transparency masters of figures and tables in the book in PDF (Adobe Acrobat) format, and PowerPoint slides. The Web page is at WilliamStallings.com/NetSec/NetSec4e.html.

An Internet mailing list has been set up so that instructors using this book can exchange information, suggestions, and questions with each other and with the author. As soon as typos or other errors are discovered, an errata list for this book will be available at WilliamStallings.com. In addition, the Computer Science Student Resource site, at WilliamStallings.com/StudentSupport.html, provides documents, information, and useful links for computer science students and professionals.

PROJECTS FOR TEACHING NETWORK SECURITY

For many instructors, an important component of a network security course is a project or set of projects by which the student gets hands-on experience to reinforce concepts from the text. This book provides an unparalleled degree of support for including a projects component in the course. The IRC not only includes guidance on how to assign and structure the projects, but also includes a set of suggested projects that covers a broad range of topics from the text:

- **Research projects:** A series of research assignments that instruct the student to research a particular topic on the Internet and write a report.
- **Hacking project:** This exercise is designed to illuminate the key issues in intrusion detection and prevention.
- **Programming projects:** A series of programming projects that cover a broad range of topics and that can be implemented in any suitable language on any platform.
- **Lab exercises:** A series of projects that involve programming and experimenting with concepts from the book.
- **Practical security assessments:** A set of exercises to examine current infrastructure and practices of an existing organization.
- **Writing assignments:** A set of suggested writing assignments organized by chapter.
- **Reading/report assignments:** A list of papers in the literature, one for each chapter, that can be assigned for the student to read and then write a short report.

See Appendix B for details.

WHAT'S NEW IN THE FOURTH EDITION

The changes for this new edition of *Network Security Essentials* are more substantial and comprehensive than those for any previous revision.

In the four years since the third edition of this book was published, the field has seen continued innovations and improvements. In this fourth edition, I try to capture these

changes while maintaining a broad and comprehensive coverage of the entire field. To begin this process of revision, the third edition was extensively reviewed by a number of professors who teach the subject. In addition, a number of professionals working in the field reviewed individual chapters. The result is that, in many places, the narrative has been clarified and tightened, and illustrations have been improved. Also, a large number of new “field-tested” problems have been added.

Beyond these refinements to improve pedagogy and user friendliness, there have been major substantive changes throughout the book. Highlights include:

- **Pseudorandom number generation and pseudorandom functions (revised):** The treatment of this important topic has been expanded, with the addition of new material in Chapter 2 and a new appendix on the subject.
- **Cryptographic hash functions and message authentication codes (revised):** The material on hash functions and MAC has been revised and reorganized to provide a clearer and more systematic treatment.
- **Key distribution and remote user authentication (revised):** In the third edition, these topics were scattered across three chapters. In the fourth edition, the material is revised and consolidated into a single chapter to provide a unified, systematic treatment.
- **Federated identity (new):** A new section covers this common identity management scheme across multiple enterprises and numerous applications and supporting many thousands, even millions, of users.
- **HTTPS (new):** A new section covers this protocol for providing secure communication between Web browser and Web server.
- **Secure Shell (new):** SSH, one of the most pervasive applications of encryption technology, is covered in a new section.
- **DomainKeys Identified Mail (new):** A new section covers DKIM, which has become the standard means of authenticating e-mail to counter spam.
- **Wireless network security (new):** A new chapter covers this important area of network security. The chapter deals with the IEEE 802.11 (WiFi) security standard for wireless local area networks and the Wireless Application Protocol (WAP) security standard for communication between a mobile Web browser and a Web server.
- **IPsec (revised):** The chapter on IPsec has been almost completely rewritten. It now covers IPsecv3 and IKEv2. In addition, the presentation has been revised to improve clarity and breadth.
- **Legal and ethical issues (new):** A new online chapter covers these important topics.
- **Online appendices (new):** Six online appendices provide addition breadth and depth for the interested student on a variety of topics.
- **Homework problems with solutions:** A separate set of homework problems (with solutions) is provided online for students.
- **Test bank:** A test bank of review questions is available to instructors. This can be used for quizzes or to enable the students to check their understanding of the material.
- **Firewalls (revised):** The chapter on firewalls has been significantly expanded.

With each new edition, it is a struggle to maintain a reasonable page count while adding new material. In part, this objective is realized by eliminating obsolete material and tightening the narrative. For this edition, chapters and appendices that are of less general interest have

been moved online as individual PDF files. This has allowed an expansion of material without the corresponding increase in size and price.

RELATIONSHIP TO CRYPTOGRAPHY AND NETWORK SECURITY

This book is adapted from *Cryptography and Network Security, Fifth Edition* (CNS5e). CNS5e provides a substantial treatment of cryptography, including detailed analysis of algorithms and a significant mathematical component, all of which covers 400 pages. *Network Security Essentials: Applications and Standards, Fourth Edition* (NSE4e) provides instead a concise overview of these topics in Chapters 2 and 3. NSE4e includes all of the remaining material of CNS5e. NSE4e also covers SNMP security, which is not covered in CNS5e. Thus, NSE4e is intended for college courses and professional readers where the interest is primarily in the application of network security and without the need or desire to delve deeply into cryptographic theory and principles.

ACKNOWLEDGEMENTS

This new edition has benefited from review by a number of people who gave generously their time and expertise. The following people reviewed all or a large part of the manuscript: Marius Zimand (Towson State University), Shambhu Upadhyaya (University of Buffalo), Nan Zhang (George Washington University), Dongwan Shin (New Mexico Tech), Michael Kain (Drexel University), William Bard (University of Texas), David Arnold (Baylor University), Edward Allen (Wake Forest University), Michael Goodrich (UC-Irvine), Xunhua Wang (James Madison University), Xianyang Li (Illinois Institute of Technology), and Paul Jenkins (Brigham Young University).

Thanks also to the many people who provided detailed technical reviews of one or more chapters: Martin Bealby, Martin Hlavac (Department of Algebra, Charles University in Prague, Czech Republic), Martin Rublik (BSP Consulting and University of Economics in Bratislava), Rafael Lara (President of Venezuela's Association for Information Security and Cryptography Research), Amitabh Saxena, and Michael Spratte (Hewlett-Packard Company). I would especially like to thank Nikhil Bhargava (IIT Delhi) for providing detailed reviews of various chapters of the book.

Nikhil Bhargava (IIT Delhi) developed the set of online homework problems and solutions. Professor Sreekanth Malladi of Dakota State University developed the hacking exercises. Sanjay Rao and Ruben Torres of Purdue developed the laboratory exercises that appear in the IRC.

The following people contributed project assignments that appear in the instructor's supplement: Henning Schulzrinne (Columbia University), Cetin Kaya Koc (Oregon State University), and David Balenson (Trusted Information Systems and George Washington University). Kim McLaughlin developed the test bank.

Finally, I would like to thank the many people responsible for the publication of the book, all of whom did their usual excellent job. This includes my editor Tracy Dunkelberger and her assistants Melinda Hagerty and Allison Michael. Also, Jake Warde of Warde Publishers managed the reviews.

With all this assistance, little remains for which I can take full credit. However, I am proud to say that, with no help whatsoever, I selected all of the quotations.

ABOUT THE AUTHOR

William Stallings has made a unique contribution to understanding the broad sweep of technical developments in computer security, computer networking, and computer architecture. He has authored 17 titles and, counting revised editions, a total of 42 books on various aspects of these subjects. His writings have appeared in numerous ACM and IEEE publications, including the *Proceedings of the IEEE* and *ACM Computing Reviews*.

He has 11 times received the award for the best Computer Science textbook of the year from the Text and Academic Authors Association.

In over 30 years in the field, he has been a technical contributor, technical manager, and an executive with several high-technology firms. He has designed and implemented both TCP/IP-based and OSI-based protocol suites on a variety of computers and operating systems, ranging from microcomputers to mainframes. As a consultant, he has advised government agencies, computer and software vendors, and major users on the design, selection, and use of networking software and products.

He created and maintains the **Computer Science Student Resource Site** at WilliamStallings.com/StudentSupport.html. This site provides documents and links on a variety of subjects of general interest to computer science students (and professionals). He is a member of the editorial board of *Cryptologia*, a scholarly journal devoted to all aspects of cryptology.

Dr. Stallings holds a PhD from M.I.T. in Computer Science and a B.S. from Notre Dame in electrical engineering.

CONTENTS

Preface ix

About the Author xiv

Chapter 1 Introduction 1

- 1.1 Computer Security Concepts 3
- 1.2 The OSI Security Architecture 8
- 1.3 Security Attacks 9
- 1.4 Security Services 13
- 1.5 Security Mechanisms 16
- 1.6 A Model for Network Security 19
- 1.7 Standards 21
- 1.8 Outline of This Book 21
- 1.9 Recommended Reading 22
- 1.10 Internet and Web Resources 23
- 1.11 Key Terms, Review Questions, and Problems 25

PART ONE CRYPTOGRAPHY 27

Chapter 2 Symmetric Encryption and Message Confidentiality 27

- 2.1 Symmetric Encryption Principles 28
- 2.2 Symmetric Block Encryption Algorithms 34
- 2.3 Random and Pseudorandom Numbers 42
- 2.4 Stream Ciphers and RC4 45
- 2.5 Cipher Block Modes of Operation 50
- 2.6 Recommended Reading and Web Sites 55
- 2.7 Key Terms, Review Questions, and Problems 56

Chapter 3 Public-Key Cryptography and Message Authentication 61

- 3.1 Approaches to Message Authentication 62
- 3.2 Secure Hash Functions 67
- 3.3 Message Authentication Codes 73
- 3.4 Public-Key Cryptography Principles 79
- 3.5 Public-Key Cryptography Algorithms 83
- 3.6 Digital Signatures 90
- 3.7 Recommended Reading and Web Sites 90
- 3.8 Key Terms, Review Questions, and Problems 91

PART TWO NETWORK SECURITY APPLICATIONS 97

Chapter 4 Key Distribution and User Authentication 97

- 4.1 Symmetric Key Distribution Using Symmetric Encryption 98
- 4.2 Kerberos 99
- 4.3 Key Distribution Using Asymmetric Encryption 114
- 4.4 X.509 Certificates 116
- 4.5 Public-Key Infrastructure 124

vi CONTENTS

4.6	Federated Identity Management	126
4.7	Recommended Reading and Web Sites	132
4.8	Key Terms, Review Questions, and Problems	133
Chapter 5	Transport-Level Security	139
5.1	Web Security Considerations	140
5.2	Secure Socket Layer and Transport Layer Security	143
5.3	Transport Layer Security	156
5.4	HTTPS	160
5.5	Secure Shell (SSH)	162
5.6	Recommended Reading and Web Sites	173
5.7	Key Terms, Review Questions, and Problems	173
Chapter 6	Wireless Network Security	175
6.1	IEEE 802.11 Wireless LAN Overview	177
6.2	IEEE 802.11i Wireless LAN Security	183
6.3	Wireless Application Protocol Overview	197
6.4	Wireless Transport Layer Security	204
6.5	WAP End-to-End Security	214
6.6	Recommended Reading and Web Sites	217
6.7	Key Terms, Review Questions, and Problems	218
Chapter 7	Electronic Mail Security	221
7.1	Pretty Good Privacy	222
7.2	S/MIME	241
7.3	DomainKeys Identified Mail	257
7.4	Recommended Reading and Web Sites	264
7.5	Key Terms, Review Questions, and Problems	265
	Appendix 7A Radix-64 Conversion	266
Chapter 8	IP Security	269
8.1	IP Security Overview	270
8.2	IP Security Policy	276
8.3	Encapsulating Security Payload	281
8.4	Combining Security Associations	288
8.5	Internet Key Exchange	292
8.6	Cryptographic Suites	301
8.7	Recommended Reading and Web Sites	302
8.8	Key Terms, Review Questions, and Problems	303
PART THREE SYSTEM SECURITY 305		
Chapter 9	Intruders	305
9.1	Intruders	307
9.2	Intrusion Detection	312
9.3	Password Management	323
9.4	Recommended Reading and Web Sites	333
9.5	Key Terms, Review Questions, and Problems	334
	Appendix 9A The Base-Rate Fallacy	337

Chapter 10 Malicious Software 340

- 10.1 Types of Malicious Software 341
- 10.2 Viruses 346
- 10.3 Virus Countermeasures 351
- 10.4 Worms 356
- 10.5 Distributed Denial of Service Attacks 365
- 10.6 Recommended Reading and Web Sites 370
- 10.7 Key Terms, Review Questions, and Problems 371

Chapter 11 Firewalls 374

- 11.1 The Need for Firewalls 375
- 11.2 Firewall Characteristics 376
- 11.3 Types of Firewalls 378
- 11.4 Firewall Basing 385
- 11.5 Firewall Location and Configurations 388
- 11.6 Recommended Reading and Web Site 393
- 11.7 Key Terms, Review Questions, and Problems 394

APPENDICES 398**Appendix A Some Aspects of Number Theory 398**

- A.1 Prime and Relatively Prime Numbers 399
- A.2 Modular Arithmetic 401

Appendix B Projects for Teaching Network Security 403

- B.1 Research Projects 404
- B.2 Hacking Project 405
- B.3 Programming Projects 405
- B.4 Laboratory Exercises 406
- B.5 Practical Security Assessments 406
- B.6 Writing Assignments 406
- B.7 Reading/Report Assignments 407

Index 408**ONLINE CHAPTERS****Chapter 12 Network Management Security**

- 12.1 Basic Concepts of SNMP
- 12.2 SNMPv1 Community Facility
- 12.3 SNMPv3
- 12.4 Recommended Reading and Web Sites
- 12.5 Key Terms, Review Questions, and Problems

Chapter 13 Legal and Ethical Aspects

- 13.1 Cybercrime and Computer Crime
- 13.2 Intellectual Property
- 13.3 Privacy
- 13.4 Ethical Issues
- 13.5 Recommended Reading and Web Sites

viii CONTENTS

13.6 Key Terms, Review Questions, and Problems

ONLINE APPENDICES

Appendix C Standards and Standards-Setting Organizations

- C.1** The Importance of Standards
- C.2** Internet Standards and the Internet Society
- C.3** National Institute of Standards and Technology

Appendix D TCP/IP and OSI

- D.1** Protocols and Protocol Architectures
- D.2** The TCP/IP Protocol Architecture
- D.3** The Role of an Internet Protocol
- D.4** IPv4
- D.5** IPv6
- D.6** The OSI Protocol Architecture

Appendix E Pseudorandom Number Generation

- E.1** PRNG Requirements
- E.2** PRNG Using a Block Cipher
- E.3** PRNG Using a Hash Function or Message Authentication Code

Appendix F Kerberos Encryption Techniques

- F.1** Password-to-Key Transformation
- F.2** Propagating Cipher Block Chaining Mode

Appendix G Data Compression Using ZIP

- G.1** Compression Algorithm
- G.2** Decompression Algorithm

Appendix H PGP Random Number Generation

- H.1** True Random Numbers
- H.2** Pseudorandom Numbers

Appendix I The International Reference Alphabet

Glossary

References

INTRODUCTION

1.1 Computer Security Concepts

A Definition of Computer Security

Examples

The Challenges of Computer Security

1.2 The OSI Security Architecture

1.3 Security Attacks

Passive Attacks

Active Attacks

1.4 Security Services

Authentication

Access Control

Data Confidentiality

Data Integrity

Nonrepudiation

Availability Service

1.5 Security Mechanisms

1.6 A Model for Network Security

1.7 Standards

1.8 Outline of This Book

1.9 Recommended Reading

1.10 Internet and Web Resources

Web Sites for This Book

Other Web Sites

USENET Newsgroups

1.11 Key Terms, Review Questions, and Problems

The combination of space, time, and strength that must be considered as the basic elements of this theory of defense makes this a fairly complicated matter. Consequently, it is not easy to find a fixed point of departure.

— *On War*, Carl Von Clausewitz

The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.

— *The Art of War*, Sun Tzu

The requirements of **information security** within an organization have undergone two major changes in the last several decades. Before the widespread use of data processing equipment, the security of information felt to be valuable to an organization was provided primarily by physical and administrative means. An example of the former is the use of rugged filing cabinets with a combination lock for storing sensitive documents. An example of the latter is personnel screening procedures used during the hiring process.

With the introduction of the computer, the need for automated tools for protecting files and other information stored on the computer became evident. This is especially the case for a shared system, such as a time-sharing system, and the need is even more acute for systems that can be accessed over a public telephone network, data network, or the Internet. The generic name for the collection of tools designed to protect data and to thwart hackers is **computer security**.

The second major change that affected security is the introduction of distributed systems and the use of networks and communications facilities for carrying data between terminal user and computer and between computer and computer. Network security measures are needed to protect data during their transmission. In fact, the term **network security** is somewhat misleading, because virtually all business, government, and academic organizations interconnect their data processing equipment with a collection of interconnected networks. Such a collection is often referred to as an internet,¹ and the term **internet security** is used.

There are no clear boundaries between these two forms of security. For example, one of the most publicized types of attack on information systems is the computer virus. A virus may be introduced into a system physically when it arrives on an optical disk and is subsequently loaded onto a computer. Viruses may also arrive over an internet. In either case, once the virus is resident on a computer system, internal computer security tools are needed to detect and recover from the virus.

This book focuses on internet security, which consists of measures to deter, prevent, detect, and correct security violations that involve the transmission of information. That is a broad statement that covers a host of possibilities. To give you a feel for the areas covered in this book, consider the following examples of security violations:

¹We use the term *internet* with a lowercase “i” to refer to any interconnected collection of network. A corporate intranet is an example of an internet. The Internet with a capital “I” may be one of the facilities used by an organization to construct its internet.