

CONTENTS

Preface ix

About the Author xiv

Chapter 1 Introduction 1.1 Computer Security Concepts 1.2 The OSI Security Architecture 1.3 Security Attacks 1.4 Security Services 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 1.11 Key Terms, Review Questions, and Problems

PART ONE CRYPTOGRAPHY

Chapter 2 Symmetric Encryption and Message Confidentiality 2.1 Symmetric Encryption Principles 2.2 Symmetric Block Encryption Algorithms 2.3 Random and Pseudorandom Numbers 2.4 Stream Ciphers and RC4 2.5 Cipher Block Modes of Operation 2.6 Recommended Reading and Web Sites 2.7 Key Terms, Review Questions, and Problems

Chapter 3 Public-Key Cryptography and Message Authentication 3.1 Approaches to Message Authentication 3.2 Secure Hash Functions 3.3 Message Authentication Codes 3.4 Public-Key Cryptography Principles 3.5 Public-Key Cryptography Algorithms 3.6 Digital Signatures 3.7 Recommended Reading and Web Sites 3.8 Key Terms, Review Questions, and Problems

PART TWO NETWORK SECURITY APPLICATIONS

Chapter 4 Key Distribution and User Authentication 4.1 Symmetric Key Distribution Using Symmetric Encryption 4.2 Kerberos 4.3 Key Distribution Using Asymmetric Encryption 4.4 X.509 Certificates 4.5 Public-Key Infrastructure 4.6 Federated Identity Management 4.7 Recommended Reading and Web Sites 4.8 Key Terms, Review Questions, and Problems 133

Chapter 5 Transport-Level Security 5.1 Web Security Considerations 5.2 Secure Socket Layer and Transport Layer Security 5.3 Transport Layer Security 5.4 HTTPS 5.5 Secure Shell (SSH) 5.6 Recommended Reading and Web Sites 5.7 Key Terms, Review Questions, and Problems 173

Chapter 6 Wireless Network Security 6.1 IEEE 802.11 Wireless LAN Overview 6.2 IEEE 802.11i Wireless LAN Security 6.3 Wireless Application Protocol Overview 6.4 Wireless Transport Layer Security 6.5 WAP End-to-End Security 6.6 Recommended Reading and Web Sites 6.7 Key Terms, Review Questions, and Problems

Chapter 7 Electronic Mail Security 7.1 Pretty Good Privacy 7.2 S/MIME 7.3 DomainKeys Identified Mail 7.4 Recommended Reading and Web Sites 7.5 Key Terms, Review Questions, and Problems Appendix 7A Radix-64 Conversion

Chapter 8 IP Security 8.1 IP Security Overview 8.2 IP Security Policy 8.3 Encapsulating Security Payload
8.4 Combining Security Associations 8.5 Internet Key Exchange 8.6 Cryptographic Suites 8.7
Recommended Reading and Web Sites 8.8 Key Terms, Review Questions, and Problems 303

PART THREE SYSTEM SECURITY 305

Chapter 9 Intruders 9.1 Intruders 9.2 Intrusion Detection 9.3 Password Management 9.4 Recommended
Reading and Web Sites 9.5 Key Terms, Review Questions, and Problems 334 Appendix 9A The Base-Rate
Fallacy 337

Chapter 10 Malicious Software 10.1 Types of Malicious Software 10.2 Viruses 10.3 Virus
Countermeasures 10.4 Worms 10.5 Distributed Denial of Service Attacks 10.6 Recommended Reading
and Web Sites 10.7 Key Terms, Review Questions, and Problems 371

Chapter 11 Firewalls 11.1 The Need for Firewalls 11.2 Firewall Characteristics 11.3 Types of Firewalls
11.4 Firewall Basing 11.5 Firewall Location and Configurations 11.6 Recommended Reading and Web
Site 11.7 Key Terms, Review Questions, and Problems APPENDICES Appendix A Some Aspects of Number
Theory A.1 Prime and Relatively Prime Numbers A.2 Modular Arithmetic

Appendix B Projects for Teaching Network Security B.1 Research Projects B.2 Hacking Project B.3
Programming Projects B.4 Laboratory Exercises B.5 Practical Security Assessments B.6 Writing
Assignments B.7 Reading/Report Assignments

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 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