

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