

CONTENTS

Preface 10

About the Author 16

Chapter 1 Introduction 17

- 1.1 Computer Security Concepts 20
- 1.2 The OSI Security Architecture 24
- 1.3 Security Attacks 25
- 1.4 Security Services 27
- 1.5 Security Mechanisms 31
- 1.6 Fundamental Security Design Principles 32
- 1.7 Attack Surfaces and Attack Trees 36
- 1.8 A Model for Network Security 39
- 1.9 Standards 42
- 1.10 Key Terms, Review Questions, and Problems 42

PART ONE: CRYPTOGRAPHY 45

Chapter 2 Symmetric Encryption and Message Confidentiality 45

- 2.1 Symmetric Encryption Principles 46
- 2.2 Symmetric Block Encryption Algorithms 52
- 2.3 Random and Pseudorandom Numbers 59
- 2.4 Stream Ciphers and RC4 63
- 2.5 Cipher Block Modes of Operation 68
- 2.6 Key Terms, Review Questions, and Problems 73

Chapter 3 Public-Key Cryptography and Message Authentication 78

- 3.1 Approaches to Message Authentication 79
- 3.2 Secure Hash Functions 84
- 3.3 Message Authentication Codes 91
- 3.4 Public-Key Cryptography Principles 96
- 3.5 Public-Key Cryptography Algorithms 100
- 3.6 Digital Signatures 109
- 3.7 Key Terms, Review Questions, and Problems 112

PART TWO: NETWORK SECURITY APPLICATIONS 119

Chapter 4 Key Distribution and User Authentication 119

- 4.1 Remote User Authentication Principles 120
- 4.2 Symmetric Key Distribution Using Symmetric Encryption 123
- 4.3 Kerberos 124
- 4.4 Key Distribution Using Asymmetric Encryption 137
- 4.5 X.509 Certificates 139
- 4.6 Public-Key Infrastructure 146

6 CONTENTS

- 4.7 Federated Identity Management 149
- 4.8 Key Terms, Review Questions, and Problems 155
- Chapter 5 Network Access Control and Cloud Security 160**
 - 5.1 Network Access Control 161
 - 5.2 Extensible Authentication Protocol 164
 - 5.3 IEEE 802.1X Port-Based Network Access Control 168
 - 5.4 Cloud Computing 170
 - 5.5 Cloud Security Risks and Countermeasures 176
 - 5.6 Data Protection in the Cloud 178
 - 5.7 Cloud Security as a Service 182
 - 5.8 Addressing Cloud Computing Security Concerns 185
 - 5.9 Key Terms, Review Questions, and Problems 186
- Chapter 6 Transport-Level Security 187**
 - 6.1 Web Security Considerations 188
 - 6.2 Transport Layer Security 190
 - 6.3 HTTPS 207
 - 6.4 Secure Shell (SSH) 208
 - 6.5 Key Terms, Review Questions, and Problems 220
- Chapter 7 Wireless Network Security 222**
 - 7.1 Wireless Security 223
 - 7.2 Mobile Device Security 226
 - 7.3 IEEE 802.11 Wireless LAN Overview 230
 - 7.4 IEEE 802.11i Wireless LAN Security 236
 - 7.5 Key Terms, Review Questions, and Problems 251
- Chapter 8 Electronic Mail Security 253**
 - 8.1 Internet Mail Architecture 254
 - 8.2 E-mail Formats 258
 - 8.3 E-mail Threats and Comprehensive E-mail Security 266
 - 8.4 S/MIME 268
 - 8.5 Pretty Good Privacy 279
 - 8.6 DNSSEC 280
 - 8.7 DNS-Based Authentication of Named Entities 285
 - 8.8 Sender Policy Framework 286
 - 8.9 DomainKeys Identified Mail 289
 - 8.10 Domain-Based Message Authentication, Reporting, and Conformance 295
 - 8.11 Key Terms, Review Questions, and Problems 300
- Chapter 9 IP Security 302**
 - 9.1 IP Security Overview 303
 - 9.2 IP Security Policy 309
 - 9.3 Encapsulating Security Payload 314
 - 9.4 Combining Security Associations 322
 - 9.5 Internet Key Exchange 325
 - 9.6 Cryptographic Suites 333
 - 9.7 Key Terms, Review Questions, and Problems 335

PART THREE: SYSTEM SECURITY 337**Chapter 10 Malicious Software 337**

- 10.1** Types of Malicious Software (Malware) 338
- 10.2** Advanced Persistent Threat 341
- 10.3** Propagation—Infected Content—Viruses 342
- 10.4** Propagation—Vulnerability Exploit—Worms 347
- 10.5** Propagation—Social Engineering—Spam E-mail, Trojans 353
- 10.6** Payload—System Corruption 355
- 10.7** Payload—Attack Agent—Zombie, Bots 356
- 10.8** Payload—Information Theft—Keyloggers, Phishing, Spyware 357
- 10.9** Payload—Stealth—Backdoors, Rootkits 359
- 10.10** Countermeasures 360
- 10.11** Distributed Denial of Service Attacks 367
- 10.12** Key Terms, Review Questions, and Problems 372

Chapter 11 Intruders 375

- 11.1** Intruders 376
- 11.2** Intrusion Detection 381
- 11.3** Password Management 396
- 11.4** Key Terms, Review Questions, and Problems 406

Chapter 12 Firewalls 410

- 12.1** The Need for Firewalls 411
- 12.2** Firewall Characteristics and Access Policy 412
- 12.3** Types of Firewalls 414
- 12.4** Firewall Basing 420
- 12.5** Firewall Location and Configurations 423
- 12.6** Key Terms, Review Questions, and Problems 428

APPENDICES 432**Appendix A Some Aspects of Number Theory 432**

- A.1** Prime and Relatively Prime Numbers 433
- A.2** Modular Arithmetic 435

Appendix B Projects for Teaching Network Security 437

- B.1** Research Projects 438
- B.2** Hacking Project 439
- B.3** Programming Projects 439
- B.4** Laboratory Exercises 440
- B.5** Practical Security Assessments 440
- B.6** Firewall Projects 440
- B.7** Case Studies 441
- B.8** Writing Assignments 441
- B.9** Reading/Report Assignments 441

References 442**Credits 448****Index 450**