# CONTENTS

**Preface xiii**

**Chapter 1 Introduction 1**

1.1 Security Trends 4
1.2 The OSI Security Architecture 6
1.3 Security Attacks 7
1.4 Security Services 11
1.5 Security Mechanisms 14
1.6 A Model for Internetwork Security 17
1.7 Internet Standards the Internet Society 19
1.8 Outline of This Book 22
1.9 Recommended Reading 23
1.10 Internet and Web Resources 23
1.11 Key Terms, Review Questions, and Problems 25

**PART ONE CRYPTOGRAPHY 26**

**Chapter 2 Symmetric Encryption and Message Confidentiality 28**

2.1 Symmetric Encryption Principles 29
2.2 Symmetric Block Encryption Algorithms 35
2.3 Stream Ciphers and RC4 43
2.4 Cipher Block Modes of Operation 46
2.5 Location of Encryption Devices 51
2.6 Key Distribution 52
2.7 Recommended Reading and Web Sites 55
2.8 Key Terms, Review Questions, and Problems 56

**Chapter 3 Public-Key Cryptography and Message Authentication 59**

3.1 Approaches to Message Authentication 60
3.2 Secure Hash Functions and HMAC 64
3.3 Public Key Cryptography Principles 74
3.4 Public-Key Cryptography Algorithms 78
3.5 Digital Signatures 85
3.6 Key Management 85
3.7 Recommended Reading and Web Sites 87
3.8 Key Terms, Review Questions, and Problems 88

**PART TWO NETWORK SECURITY APPLICATIONS 92**

**Chapter 4 Authentication Applications 94**

4.1 Kerberos 95
4.2 X.509 Directory Authentication Service 113
4.3 Public Key Infrastructure 122

4.4 Recommended Reading and Web Sites 124
4.4 Key Terms, Review Questions, and Problems 125
Appendix 4A: Kerberos Encryption Techniques 127

**Chapter 5 Electronic Mail Security 130**

5.1 Pretty Good Privacy (PGP) 132
5.2 S/MIME 151
5.3 Recommended Web Sites 168
5.4 Key Terms, Review Questions, and Problems 168
Appendix 5A: Data Compression Using ZIP 169
Appendix 5B: Radix-64 Conversion 172
Appendix 5C: PGP Random Number Generation 173

**Chapter 6 IP Security 177**

6.1 IP Security Overview 179
6.2 IP Security Architecture 181
6.3 Authentication Header 187
6.4 Encapsulating Security Payload 192
6.5 Combining Security Associations 197
6.6 Key Management 200
6.7 Recommended Reading and Web Sites 210
6.8 Key Terms, Review Questions, and Problems 211
Appendix 6A: Internetworking and Internet Protocols 212

**Chapter 7 Web Security 221**

7.1 Web Security Requirements 222
7.2 Secure Sockets Layer (SSL) and Transport Layer Security (TLS) 225
7.3 Secure Electronic Transaction (SET) 243
7.4 Recommended Reading and Web Sites 254
7.5 Key Terms, Review Questions, and Problems 255

**Chapter 8 Network Management Security 257**

8.1 Basic Concepts of SNMP 258
8.2 SNMPv1 Community Facility 266
8.3 SNMPv3 269
8.4 Recommended Reading and Web Sites 292
8.5 Key Terms, Review Questions, and Problems 293

**PART THREE SYSTEM SECURITY 297**

**Chapter 9 Intruders 299**

9.1 Intruders 301
9.2 Intrusion Detection 304
9.3 Password Management 316
9.4 Recommended Reading and Web Sites 325
9.5 Key Terms, Review Questions, and Problems 326
Appendix 9A: The Base-Rate Fallacy 328

**Chapter 10 Malicious Software 332**

10.1 Viruses and Related Threats 333
10.2 Virus Countermeasures 344
10.3 Distributed Denial of Service Attacks 348
10.4 Recommended Reading and Web Sites 353
10.5 Key Terms, Review Questions, and Problems 354

**Chapter 11 Firewalls 355**

11.1 Firewall Design Principles 356
11.2 Trusted Systems 368
11.3 Common Criteria for Information Technology Security Evaluation 374
11.4 Recommended Reading and Web Sites 378
11.5 Key Terms, Review Questions, and Problems 379

**APPENDICES 381**

**Appendix A Some Aspects of Number Theory 381**

A.1 Prime and Relatively Prime Numbers 382
A.2 Modular Arithmetic 384

**Appendix B Projects for Teaching Network Security 386**

B.1 Research Projects 387
B.2 Programming Projects 388
B.3 Laboratory Exercises 388
B.4 Writing Assignments 388
B.5 Reading/Report Assignments 389

**Glossary 390**

**References 396**

**Index 402**