

CONTENTS

Online Resources 11

Preface 12

Notation 18

About the Authors 19

Chapter 0 Reader's and Instructor's Guide 21

- 0.1 Outline of this Book 22
- 0.2 A Roadmap for Readers and Instructors 22
- 0.3 Support for CISSP Certification 23
- 0.4 Support for NSA/DHS Certification 25
- 0.5 Support for ACM/IEEE Computer Society Computer Science Curricula 2013 26
- 0.6 Internet and Web Resources 28
- 0.7 Standards 29

Chapter 1 Overview 31

- 1.1 Computer Security Concepts 32
- 1.2 Threats, Attacks, and Assets 39
- 1.3 Security Functional Requirements 45
- 1.4 Fundamental Security Design Principles 47
- 1.5 Attack Surfaces and Attack Trees 51
- 1.6 Computer Security Strategy 54
- 1.7 Recommended Reading 56
- 1.8 Key Terms, Review Questions, and Problems 57

PART ONE COMPUTER SECURITY TECHNOLOGY AND PRINCIPLES 60

Chapter 2 Cryptographic Tools 60

- 2.1 Confidentiality with Symmetric Encryption 61
- 2.2 Message Authentication and Hash Functions 67
- 2.3 Public-Key Encryption 75
- 2.4 Digital Signatures and Key Management 80
- 2.5 Random and Pseudorandom Numbers 84
- 2.6 Practical Application: Encryption of Stored Data 86
- 2.7 Recommended Reading 87
- 2.8 Key Terms, Review Questions, and Problems 88

Chapter 3 User Authentication 92

- 3.1 Electronic User Authentication Principles 94
- 3.2 Password-Based Authentication 98
- 3.3 Token-Based Authentication 110
- 3.4 Biometric Authentication 116
- 3.5 Remote User Authentication 120

6 CONTENTS

| | | |
|------------------|---|------------|
| 3.6 | Security Issues for User Authentication | 123 |
| 3.7 | Practical Application: An Iris Biometric System | 125 |
| 3.8 | Case Study: Security Problems for ATM Systems | 127 |
| 3.9 | Recommended Reading | 130 |
| 3.10 | Key Terms, Review Questions, and Problems | 130 |
| Chapter 4 | Access Control | 133 |
| 4.1 | Access Control Principles | 134 |
| 4.2 | Subjects, Objects, and Access Rights | 137 |
| 4.3 | Discretionary Access Control | 138 |
| 4.4 | Example: UNIX File Access Control | 144 |
| 4.5 | Role-Based Access Control | 147 |
| 4.6 | Attribute-Based Access Control | 153 |
| 4.7 | Identity, Credential, and Access Management | 159 |
| 4.8 | Trust Frameworks | 163 |
| 4.9 | Case Study: RBAC System for a Bank | 167 |
| 4.10 | Recommended Reading | 170 |
| 4.11 | Key Terms, Review Questions, and Problems | 171 |
| Chapter 5 | Database and Cloud Security | 175 |
| 5.1 | The Need for Database Security | 176 |
| 5.2 | Database Management Systems | 177 |
| 5.3 | Relational Databases | 179 |
| 5.4 | SQL Injection Attacks | 183 |
| 5.5 | Database Access Control | 189 |
| 5.6 | Inference | 193 |
| 5.7 | Database Encryption | 196 |
| 5.8 | Cloud Computing | 200 |
| 5.9 | Cloud Security Risks and Countermeasures | 207 |
| 5.10 | Data Protection in the Cloud | 209 |
| 5.11 | Cloud Security as a Service | 209 |
| 5.12 | Recommended Reading | 213 |
| 5.13 | Key Terms, Review Questions, and Problems | 214 |
| Chapter 6 | Malicious Software | 219 |
| 6.1 | Types of Malicious Software (Malware) | 220 |
| 6.2 | Advanced Persistent Threat | 223 |
| 6.3 | Propagation—Infected Content—Viruses | 224 |
| 6.4 | Propagation—Vulnerability Exploit—Worms | 230 |
| 6.5 | Propagation—Social Engineering—Spam E-Mail, Trojans | 238 |
| 6.6 | Payload—System Corruption | 241 |
| 6.7 | Payload—Attack Agent—Zombie, Bots | 242 |
| 6.8 | Payload—Information Theft—Keyloggers, Phishing, Spyware | 244 |
| 6.9 | Payload—Stealth—Backdoors, Rootkits | 246 |
| 6.10 | Countermeasures | 249 |
| 6.11 | Recommended Reading | 255 |
| 6.12 | Key Terms, Review Questions, and Problems | 256 |

Chapter 7 Denial-of-Service Attacks 260

- 7.1 Denial-of-Service Attacks 261
- 7.2 Flooding Attacks 268
- 7.3 Distributed Denial-of-Service Attacks 270
- 7.4 Application-Based Bandwidth Attacks 272
- 7.5 Reflector and Amplifier Attacks 274
- 7.6 Defenses Against Denial-of-Service Attacks 279
- 7.7 Responding to a Denial-of-Service Attack 283
- 7.8 Recommended Reading 284
- 7.9 Key Terms, Review Questions, and Problems 284

Chapter 8 Intrusion Detection 287

- 8.1 Intruders 288
- 8.2 Intrusion Detection 292
- 8.3 Analysis Approaches 295
- 8.4 Host-Based Intrusion Detection 298
- 8.5 Network-Based Intrusion Detection 303
- 8.6 Distributed or Hybrid Intrusion Detection 309
- 8.7 Intrusion Detection Exchange Format 311
- 8.8 Honeypots 314
- 8.9 Example System: Snort 316
- 8.10 Recommended Reading 320
- 8.11 Key Terms, Review Questions, and Problems 320

Chapter 9 Firewalls and Intrusion Prevention Systems 324

- 9.1 The Need for Firewalls 325
- 9.2 Firewall Characteristics and Access Policy 326
- 9.3 Types of Firewalls 328
- 9.4 Firewall Basing 334
- 9.5 Firewall Location and Configurations 337
- 9.6 Intrusion Prevention Systems 342
- 9.7 Example: Unified Threat Management Products 346
- 9.8 Recommended Reading 350
- 9.9 Key Terms, Review Questions, and Problems 351

PART TWO SOFTWARE SECURITY AND TRUSTED SYSTEMS 356**Chapter 10 Buffer Overflow 356**

- 10.1 Stack Overflows 358
- 10.2 Defending Against Buffer Overflows 379
- 10.3 Other Forms of Overflow Attacks 385
- 10.4 Recommended Reading 392
- 10.5 Key Terms, Review Questions, and Problems 392

Chapter 11 Software Security 395

- 11.1 Software Security Issues 396
- 11.2 Handling Program Input 400

- 11.3 Writing Safe Program Code 412
- 11.4 Interacting with the Operating System and Other Programs 416
- 11.5 Handling Program Output 429
- 11.6 Recommended Reading 431
- 11.7 Key Terms, Review Questions, and Problems 432

Chapter 12 Operating System Security 436

- 12.1 Introduction to Operating System Security 438
- 12.2 System Security Planning 439
- 12.3 Operating Systems Hardening 439
- 12.4 Application Security 444
- 12.5 Security Maintenance 445
- 12.6 Linux/Unix Security 446
- 12.7 Windows Security 450
- 12.8 Virtualization Security 452
- 12.9 Recommended Reading 456
- 12.10 Key Terms, Review Questions, and Problems 457

Chapter 13 Trusted Computing and Multilevel Security 459

- 13.1 The Bell-LaPadula Model for Computer Security 460
- 13.2 Other Formal Models for Computer Security 470
- 13.3 The Concept of Trusted Systems 476
- 13.4 Application of Multilevel Security 479
- 13.5 Trusted Computing and the Trusted Platform Module 485
- 13.6 Common Criteria for Information Technology Security Evaluation 489
- 13.7 Assurance and Evaluation 495
- 13.8 Recommended Reading 500
- 13.9 Key Terms, Review Questions, and Problems 501

PART THREE MANAGEMENT ISSUES 505

Chapter 14 IT Security Management and Risk Assessment 505

- 14.1 IT Security Management 506
- 14.2 Organizational Context and Security Policy 509
- 14.3 Security Risk Assessment 512
- 14.4 Detailed Security Risk Analysis 515
- 14.5 Case Study: Silver Star Mines 527
- 14.6 Recommended Reading 532
- 14.7 Key Terms, Review Questions, and Problems 533

Chapter 15 IT Security Controls, Plans, and Procedures 535

- 15.1 IT Security Management Implementation 536
- 15.2 Security Controls or Safeguards 536
- 15.3 IT Security Plan 544
- 15.4 Implementation of Controls 545
- 15.5 Monitoring Risks 546
- 15.6 Case Study: Silver Star Mines 549
- 15.7 Recommended Reading 552
- 15.8 Key Terms, Review Questions, and Problems 552

Chapter 16 Physical and Infrastructure Security 554

- 16.1 Overview 555
- 16.2 Physical Security Threats 556
- 16.3 Physical Security Prevention and Mitigation Measures 563
- 16.4 Recovery From Physical Security Breaches 566
- 16.5 Example: A Corporate Physical Security Policy 566
- 16.6 Integration of Physical and Logical Security 567
- 16.7 Recommended Reading 573
- 16.8 Key Terms, Review Questions, and Problems 574

Chapter 17 Human Resources Security 576

- 17.1 Security Awareness, Training, and Education 577
- 17.2 Employment Practices and Policies 583
- 17.3 E-Mail and Internet Use Policies 586
- 17.4 Computer Security Incident Response Teams 587
- 17.5 Recommended Reading 594
- 17.6 Key Terms, Review Questions, and Problems 595

Chapter 18 Security Auditing 597

- 18.1 Security Auditing Architecture 599
- 18.2 Security Audit Trail 604
- 18.3 Implementing the Logging Function 608
- 18.4 Audit Trail Analysis 620
- 18.5 Example: An Integrated Approach 624
- 18.6 Recommended Reading 627
- 18.7 Key Terms, Review Questions, and Problems 628

Chapter 19 Legal and Ethical Aspects 630

- 19.1 Cybercrime and Computer Crime 631
- 19.2 Intellectual Property 635
- 19.3 Privacy 641
- 19.4 Ethical Issues 646
- 19.5 Recommended Reading 653
- 19.6 Key Terms, Review Questions, and Problems 654

PART FOUR CRYPTOGRAPHIC ALGORITHMS 657**Chapter 20 Symmetric Encryption and Message Confidentiality 657**

- 20.1 Symmetric Encryption Principles 658
- 20.2 Data Encryption Standard 663
- 20.3 Advanced Encryption Standard 665
- 20.4 Stream Ciphers and RC4 671
- 20.5 Cipher Block Modes of Operation 675
- 20.6 Location of Symmetric Encryption Devices 680
- 20.7 Key Distribution 682
- 20.8 Recommended Reading 684
- 20.9 Key Terms, Review Questions, and Problems 684

Chapter 21 Public-Key Cryptography and Message Authentication 689

- 21.1 Secure Hash Functions 690
- 21.2 HMAC 695
- 21.3 The RSA Public-Key Encryption Algorithm 699
- 21.4 Diffie-Hellman and Other Asymmetric Algorithms 704
- 21.5 Recommended Reading 709
- 21.6 Key Terms, Review Questions, and Problems 709

PART FIVE NETWORK SECURITY 713

Chapter 22 Internet Security Protocols and Standards 713

- 22.1 Secure E-Mail and S/MIME 714
- 22.2 DomainKeys Identified Mail 717
- 22.3 Secure Sockets Layer (SSL) and Transport Layer Security (TLS) 720
- 22.4 HTTPS 727
- 22.5 IPv4 and IPv6 Security 728
- 22.6 Recommended Reading 734
- 22.7 Key Terms, Review Questions, and Problems 734

Chapter 23 Internet Authentication Applications 737

- 23.1 Kerberos 738
- 23.2 X.509 744
- 23.3 Public-Key Infrastructure 747
- 23.4 Recommended Reading 749
- 23.5 Key Terms, Review Questions, and Problems 750

Chapter 24 Wireless Network Security 753

- 24.1 Wireless Security 754
- 24.2 Mobile Device Security 757
- 24.3 IEEE 802.11 Wireless LAN Overview 761
- 24.4 IEEE 802.11i Wireless LAN Security 767
- 24.5 Recommended Reading 782
- 24.6 Key Terms, Review Questions, and Problems 783

Appendix A Projects and Other Student Exercises for Teaching Computer Security 785

- A.1 Hacking Project 785
- A.2 Laboratory Exercises 786
- A.3 Security Education (SEED) Projects 786
- A.4 Research Projects 788
- A.5 Programming Projects 789
- A.6 Practical Security Assessments 789
- A.7 Firewall Projects 789
- A.8 Case Studies 790
- A.9 Reading/Report Assignments 790
- A.10 Writing Assignments 790
- A.11 Webcasts for Teaching Computer Security 791

Acronyms 792

References 793

Index 811

Credits 835