

COMPUTER SECURITY

PRINCIPLES AND PRACTICE

Third Edition

William Stallings

Lawrie Brown

UNSW Canberra at the Australian Defence Force Academy

PEARSON

Boston Columbus Indianapolis New York San Francisco Upper Saddle River
Amsterdam CapeTown Dubai London Madrid Milan Munich Paris Montreal Toronto
Delhi Mexico City São Paulo Sydney Hong Kong Seoul Singapore Taipei Tokyo

CONTENTS

Online Resources xi

Preface xii

Notation xviii

About the Authors xix

Chapter 0 Reader's and Instructor's Guide 1

- 0.1 Outline of this Book 2
- 0.2 A Roadmap for Readers and Instructors 2
- 0.3 Support for CISSP Certification 3
- 0.4 Support for NSA/DHS Certification 5
- 0.5 Support for ACM/IEEE Computer Society Computer Science Curricula 2013 6
- 0.6 Internet and Web Resources 8
- 0.7 Standards 9

Chapter 1 Overview 11

- 1.1 Computer Security Concepts 12
- 1.2 Threats, Attacks, and Assets 19
- 1.3 Security Functional Requirements 25
- 1.4 Fundamental Security Design Principles 27
- 1.5 Attack Surfaces and Attack Trees 31
- 1.6 Computer Security Strategy 34
- 1.7 Recommended Reading 36
- 1.8 Key Terms, Review Questions, and Problems 37

PART ONE COMPUTER SECURITY TECHNOLOGY AND PRINCIPLES 40

Chapter 2 Cryptographic Tools 40

- 2.1 Confidentiality with Symmetric Encryption 41
- 2.2 Message Authentication and Hash Functions 47
- 2.3 Public-Key Encryption 55
- 2.4 Digital Signatures and Key Management 60
- 2.5 Random and Pseudorandom Numbers 64
- 2.6 Practical Application: Encryption of Stored Data 66
- 2.7 Recommended Reading 67
- 2.8 Key Terms, Review Questions, and Problems 68

Chapter 3 User Authentication 72

- 3.1 Electronic User Authentication Principles 74
- 3.2 Password-Based Authentication 78
- 3.3 Token-Based Authentication 90
- 3.4 Biometric Authentication 96
- 3.5 Remote User Authentication 100

- 3.6 Security Issues for User Authentication 103
- 3.7 Practical Application: An Iris Biometric System 105
- 3.8 Case Study: Security Problems for ATM Systems 107
- 3.9 Recommended Reading 110
- 3.10 Key Terms, Review Questions, and Problems 110

Chapter 4 Access Control 113

- 4.1 Access Control Principles 114
- 4.2 Subjects, Objects, and Access Rights 117
- 4.3 Discretionary Access Control 118
- 4.4 Example: UNIX File Access Control 124
- 4.5 Role-Based Access Control 127
- 4.6 Attribute-Based Access Control 133
- 4.7 Identity, Credential, and Access Management 139
- 4.8 Trust Frameworks 143
- 4.9 Case Study: RBAC System for a Bank 147
- 4.10 Recommended Reading 150
- 4.11 Key Terms, Review Questions, and Problems 151

Chapter 5 Database and Cloud Security 155

- 5.1 The Need for Database Security 156
- 5.2 Database Management Systems 157
- 5.3 Relational Databases 159
- 5.4 SQL Injection Attacks 163
- 5.5 Database Access Control 169
- 5.6 Inference 173
- 5.7 Database Encryption 176
- 5.8 Cloud Computing 180
- 5.9 Cloud Security Risks and Countermeasures 187
- 5.10 Data Protection in the Cloud 189
- 5.11 Cloud Security as a Service 189
- 5.12 Recommended Reading 193
- 5.13 Key Terms, Review Questions, and Problems 194

Chapter 6 Malicious Software 199

- 6.1 Types of Malicious Software (Malware) 200
- 6.2 Advanced Persistent Threat 203
- 6.3 Propagation—Infected Content—Viruses 204
- 6.4 Propagation—Vulnerability Exploit—Worms 210
- 6.5 Propagation—Social Engineering—Spam E-Mail, Trojans 218
- 6.6 Payload—System Corruption 221
- 6.7 Payload—Attack Agent—Zombie, Bots 222
- 6.8 Payload—Information Theft—Keyloggers, Phishing, Spyware 224
- 6.9 Payload—Stealth—Backdoors, Rootkits 226
- 6.10 Countermeasures 229
- 6.11 Recommended Reading 235
- 6.12 Key Terms, Review Questions, and Problems 236

Chapter 7 Denial-of-Service Attacks 240

- 7.1 Denial-of-Service Attacks 241
- 7.2 Flooding Attacks 248
- 7.3 Distributed Denial-of-Service Attacks 250
- 7.4 Application-Based Bandwidth Attacks 252
- 7.5 Reflector and Amplifier Attacks 254
- 7.6 Defenses Against Denial-of-Service Attacks 259
- 7.7 Responding to a Denial-of-Service Attack 263
- 7.8 Recommended Reading 264
- 7.9 Key Terms, Review Questions, and Problems 264

Chapter 8 Intrusion Detection 267

- 8.1 Intruders 268
- 8.2 Intrusion Detection 272
- 8.3 Analysis Approaches 275
- 8.4 Host-Based Intrusion Detection 278
- 8.5 Network-Based Intrusion Detection 283
- 8.6 Distributed or Hybrid Intrusion Detection 289
- 8.7 Intrusion Detection Exchange Format 291
- 8.8 Honeypots 294
- 8.9 Example System: Snort 296
- 8.10 Recommended Reading 300
- 8.11 Key Terms, Review Questions, and Problems 300

Chapter 9 Firewalls and Intrusion Prevention Systems 304

- 9.1 The Need for Firewalls 305
- 9.2 Firewall Characteristics and Access Policy 306
- 9.3 Types of Firewalls 308
- 9.4 Firewall Basing 314
- 9.5 Firewall Location and Configurations 317
- 9.6 Intrusion Prevention Systems 322
- 9.7 Example: Unified Threat Management Products 326
- 9.8 Recommended Reading 330
- 9.9 Key Terms, Review Questions, and Problems 331

PART TWO SOFTWARE SECURITY AND TRUSTED SYSTEMS 336**Chapter 10 Buffer Overflow 336**

- 10.1 Stack Overflows 338
- 10.2 Defending Against Buffer Overflows 359
- 10.3 Other Forms of Overflow Attacks 365
- 10.4 Recommended Reading 372
- 10.5 Key Terms, Review Questions, and Problems 372

Chapter 11 Software Security 375

- 11.1 Software Security Issues 376
- 11.2 Handling Program Input 380

- 11.3 Writing Safe Program Code 392
- 11.4 Interacting with the Operating System and Other Programs 396
- 11.5 Handling Program Output 409
- 11.6 Recommended Reading 411
- 11.7 Key Terms, Review Questions, and Problems 412

Chapter 12 Operating System Security 416

- 12.1 Introduction to Operating System Security 418
- 12.2 System Security Planning 419
- 12.3 Operating Systems Hardening 419
- 12.4 Application Security 424
- 12.5 Security Maintenance 425
- 12.6 Linux/Unix Security 426
- 12.7 Windows Security 430
- 12.8 Virtualization Security 432
- 12.9 Recommended Reading 436
- 12.10 Key Terms, Review Questions, and Problems 437

Chapter 13 Trusted Computing and Multilevel Security 439

- 13.1 The Bell-LaPadula Model for Computer Security 440
- 13.2 Other Formal Models for Computer Security 450
- 13.3 The Concept of Trusted Systems 456
- 13.4 Application of Multilevel Security 459
- 13.5 Trusted Computing and the Trusted Platform Module 465
- 13.6 Common Criteria for Information Technology Security Evaluation 469
- 13.7 Assurance and Evaluation 475
- 13.8 Recommended Reading 480
- 13.9 Key Terms, Review Questions, and Problems 481

PART THREE MANAGEMENT ISSUES 485

Chapter 14 IT Security Management and Risk Assessment 485

- 14.1 IT Security Management 486
- 14.2 Organizational Context and Security Policy 489
- 14.3 Security Risk Assessment 492
- 14.4 Detailed Security Risk Analysis 495
- 14.5 Case Study: Silver Star Mines 507
- 14.6 Recommended Reading 512
- 14.7 Key Terms, Review Questions, and Problems 513

Chapter 15 IT Security Controls, Plans, and Procedures 515

- 15.1 IT Security Management Implementation 516
- 15.2 Security Controls or Safeguards 516
- 15.3 IT Security Plan 524
- 15.4 Implementation of Controls 525
- 15.5 Monitoring Risks 526
- 15.6 Case Study: Silver Star Mines 529
- 15.7 Recommended Reading 532
- 15.8 Key Terms, Review Questions, and Problems 532

Chapter 16 Physical and Infrastructure Security 534

- 16.1 Overview 535
- 16.2 Physical Security Threats 536
- 16.3 Physical Security Prevention and Mitigation Measures 543
- 16.4 Recovery From Physical Security Breaches 546
- 16.5 Example: A Corporate Physical Security Policy 546
- 16.6 Integration of Physical and Logical Security 547
- 16.7 Recommended Reading 553
- 16.8 Key Terms, Review Questions, and Problems 554

Chapter 17 Human Resources Security 556

- 17.1 Security Awareness, Training, and Education 557
- 17.2 Employment Practices and Policies 563
- 17.3 E-Mail and Internet Use Policies 566
- 17.4 Computer Security Incident Response Teams 567
- 17.5 Recommended Reading 574
- 17.6 Key Terms, Review Questions, and Problems 575

Chapter 18 Security Auditing 577

- 18.1 Security Auditing Architecture 579
- 18.2 Security Audit Trail 584
- 18.3 Implementing the Logging Function 588
- 18.4 Audit Trail Analysis 600
- 18.5 Example: An Integrated Approach 604
- 18.6 Recommended Reading 607
- 18.7 Key Terms, Review Questions, and Problems 608

Chapter 19 Legal and Ethical Aspects 610

- 19.1 Cybercrime and Computer Crime 611
- 19.2 Intellectual Property 615
- 19.3 Privacy 621
- 19.4 Ethical Issues 626
- 19.5 Recommended Reading 633
- 19.6 Key Terms, Review Questions, and Problems 634

PART FOUR CRYPTOGRAPHIC ALGORITHMS 637**Chapter 20 Symmetric Encryption and Message Confidentiality 637**

- 20.1 Symmetric Encryption Principles 638
- 20.2 Data Encryption Standard 643
- 20.3 Advanced Encryption Standard 645
- 20.4 Stream Ciphers and RC4 651
- 20.5 Cipher Block Modes of Operation 655
- 20.6 Location of Symmetric Encryption Devices 660
- 20.7 Key Distribution 662
- 20.8 Recommended Reading 664
- 20.9 Key Terms, Review Questions, and Problems 664

Chapter 21 Public-Key Cryptography and Message Authentication 669

- 21.1 Secure Hash Functions 670
- 21.2 HMAC 675
- 21.3 The RSA Public-Key Encryption Algorithm 679
- 21.4 Diffie-Hellman and Other Asymmetric Algorithms 684
- 21.5 Recommended Reading 689
- 21.6 Key Terms, Review Questions, and Problems 689

PART FIVE NETWORK SECURITY 693

Chapter 22 Internet Security Protocols and Standards 693

- 22.1 Secure E-Mail and S/MIME 694
- 22.2 DomainKeys Identified Mail 697
- 22.3 Secure Sockets Layer (SSL) and Transport Layer Security (TLS) 700
- 22.4 HTTPS 707
- 22.5 IPv4 and IPv6 Security 708
- 22.6 Recommended Reading 714
- 22.7 Key Terms, Review Questions, and Problems 714

Chapter 23 Internet Authentication Applications 717

- 23.1 Kerberos 718
- 23.2 X.509 724
- 23.3 Public-Key Infrastructure 727
- 23.4 Recommended Reading 729
- 23.5 Key Terms, Review Questions, and Problems 730

Chapter 24 Wireless Network Security 733

- 24.1 Wireless Security 734
- 24.2 Mobile Device Security 737
- 24.3 IEEE 802.11 Wireless LAN Overview 741
- 24.4 IEEE 802.11i Wireless LAN Security 747
- 24.5 Recommended Reading 762
- 24.6 Key Terms, Review Questions, and Problems 763

Appendix A Projects and Other Student Exercises for Teaching Computer Security 765

- A.1 Hacking Project 765
- A.2 Laboratory Exercises 766
- A.3 Security Education (SEED) Projects 766
- A.4 Research Projects 768
- A.5 Programming Projects 769
- A.6 Practical Security Assessments 769
- A.7 Firewall Projects 769
- A.8 Case Studies 770
- A.9 Reading/Report Assignments 770
- A.10 Writing Assignments 770
- A.11 Webcasts for Teaching Computer Security 771

Acronyms 772

References 773

Index 791

ONLINE CHAPTERS AND APPENDICES¹**Chapter 25 Linux Security**

- 25.1 Introduction
- 25.2 Linux's Security Model
- 25.3 The Linux DAC in Depth: Filesystem Security
- 25.4 Linux Vulnerabilities
- 25.5 Linux System Hardening
- 25.6 Application Security
- 25.7 Mandatory Access Controls
- 25.8 Recommended Reading
- 25.9 Key Terms, Review Questions, and Problems

Chapter 26 Windows and Windows Vista Security

- 26.1 Windows Security Architecture
- 26.2 Windows Vulnerabilities
- 26.3 Windows Security Defenses
- 26.4 Browser Defenses
- 26.5 Cryptographic Services
- 26.6 Common Criteria
- 26.7 Recommended Reading
- 26.8 Key Terms, Review Questions, Problems, and Projects

Appendix B Some Aspects of Number Theory**Appendix C Standards and Standard-Setting Organizations****Appendix D Random and Pseudorandom Number Generation****Appendix E Message Authentication Codes Based on Block Ciphers****Appendix F TCP/IP Protocol Architecture****Appendix G Radix-64 Conversion****Appendix H Security Policy-Related Documents****Appendix I The Domain Name System****Appendix J The Base-Rate Fallacy****Appendix K SHA-3****Appendix L Glossary**

¹Online chapters, appendices, and other documents are Premium Content, available via the access card at the front of this book.