COMPUTER SECURITY
PRINCIPLES AND PRACTICE

Second Edition

William Stallings

Lawrie Brown
University of New South Wales, Australian Defence Force Academy

With Contributions by

Mick Bauer
Security Editor, Linux Journal
Dir. Of Value-Subtracted Svcs., Wiremonkeys.org

Michael Howard
Principle Security Program Manager, Microsoft Corporation

International Edition contributions by

Arup Kumar Bhattacharjee
RCC Institute of Information Technology

Soumen Mukherjee
RCC Institute of Information Technology

Technische Universität Darmstadt
FACHBEREICH INFORMATIK
BIBLIOTHEK
Inventar-Nr.: M12-00042
Sachgebiete: Daten
Standort: E.6/Stal

Fachbereichsbibliothek Informatik
TU Darmstadt
59485040

Boston Columbus Indianap Upper Saddle River
Amsterdam Cape Town Dubai London Madrid Milan Munich Paris Montreal Toronto
Delhi Mexico City Sao Paulo Sydney Hong Kong Seoul Singapore Taipei Tokyo

CONTENTS

Online Resources 13

Notation 14

About the Authors 15

Preface 17

Chapter 0 Reader's and Instructor's Guide 23

0.1 Outline of This Book 24
0.2 A Roadmap for Readers and Instructors 24
0.3 Support for CISSP Certification 25
0.4 Internet and Web Resources 27
0.5 Standards 29

Chapter 1 Overview 31

1.1 Computer Security Concepts 32
1.2 Threats, Attacks, and Assets 40
1.3 Security Functional Requirements 45
1.4 A Security Architecture for Open Systems 48
1.5 Computer Security Trends 53
1.6 Computer Security Strategy 55
1.7 Recommended Reading and Web Sites 57
1.8 Key Terms, Review Questions, and Problems 58

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 68
2.3 Public-Key Encryption 76
2.4 Digital Signatures and Key Management 81
2.5 Random and Pseudorandom Numbers 84
2.6 Practical Application: Encryption of Stored Data 86
2.7 Recommended Reading and Web Sites 88
2.8 Key Terms, Review Questions, and Problems 89

Chapter 3 User Authentication 93

3.1 Means of Authentication 95
3.2 Password-Based Authentication 95
3.3 Token-Based Authentication 106
3.4 Biometric Authentication 110
3.5 Remote User Authentication 115
3.6 Security Issues for User Authentication 117
3.7 Practical Application: An Iris Biometric System 119

3.8 Case Study: Security Problems for ATM Systems 121
3.9 Recommended Reading and Web Sites 123
3.10 Key Terms, Review Questions, and Problems 125

Chapter 4 Access Control 127

4.1 Access Control Principles 128
4.2 Subjects, Objects, and Access Rights 132
4.3 Discretionary Access Control 133
4.4 Example: UNIX File Access Control 140
4.5 Role-Based Access Control 143
4.6 Case Study: RBAC System for a Bank 151
4.7 Recommended Reading and Web Site 154
4.8 Key Terms, Review Questions, and Problems 155

Chapter 5 Database Security 159

5.1 The Need for Database Security 160
5.2 Database Management Systems 161
5.3 Relational Databases 163
5.4 Database Access Control 166
5.5 Inference 171
5.6 Statistical Databases 174
5.7 Database Encryption 184
5.8 Cloud Security 188
5.9 Recommended Reading and Web Site 194
5.10 Key Terms, Review Questions, and Problems 195

Chapter 6 Malicious Software 200

6.1 Types of Malicious Software (Malware) 201
6.2 Propagation—Infected Content—Viruses 204
6.3 Propagation—Vulnerability Exploit—Worms 210
6.4 Propagation—Social Engineering—SPAM E-mail, Trojans 217
6.5 Payload—System Corruption 219
6.6 Payload—Attack Agent—Zombie, Bots 221
6.7 Payload—Information Theft—Keyloggers, Phishing, Spyware 223
6.8 Payload—Stealthing—Backdoors, Rootkits 224
6.9 Countermeasures 228
6.10 Recommended Reading and Web Sites 237
6.11 Key Terms, Review Questions, and Problems 238

Chapter 7 Denial-of-Service Attacks 242

7.1 Denial-of-Service Attacks 243
7.2 Flooding Attacks 250
7.3 Distributed Denial-of-Service Attacks 252
7.4 Application-Based Bandwidth Attacks 254
7.5 Reflector and Amplifier Attacks 256
7.6 Defenses Against Denial-of-Service Attacks 261
7.7 Responding to a Denial-of-Service Attack 265
7.8 Recommended Reading and Web Sites 266
7.9 Key Terms, Review Questions, and Problems 267

Chapter 8 Intrusion Detection 270

8.1 Intruders 271
8.2 Intrusion Detection 275
8.3 Host-Based Intrusion Detection 278
8.4 Distributed Host-Based Intrusion Detection 285
8.5 Network-Based Intrusion Detection 287
8.6 Distributed Adaptive Intrusion Detection 292
8.7 Intrusion Detection Exchange Format 295
8.8 Honeypots 297
8.9 Example System: Snort 299
8.10 Recommended Reading and Web Sites 303
8.11 Key Terms, Review Questions, and Problems 304

Chapter 9 Firewalls and Intrusion Prevention Systems 307

9.1 The Need for Firewalls 308
9.2 Firewall Characteristics 309
9.3 Types of Firewalls 310
9.4 Firewall Basing 318
9.5 Firewall Location and Configurations 320
9.6 Intrusion Prevention Systems 325
9.7 Example: Unified Threat Management Products 328
9.8 Recommended Reading and Web Site 332
9.9 Key Terms, Review Questions, and Problems 333

PART TWO: SOFTWARE SECURITY AND TRUSTED SYSTEMS 338

Chapter 10 Buffer Overflow 338

10.1 Stack Overflows 340
10.2 Defending Against Buffer Overflows 361
10.3 Other Forms of Overflow Attacks 367
10.4 Recommended Reading and Web Sites 374
10.5 Key Terms, Review Questions, and Problems 375

Chapter 11 Software Security 377

11.1 Software Security Issues 378
11.2 Handling Program Input 382
11.3 Writing Safe Program Code 393
11.4 Interacting with the Operating System and Other Programs 398
11.5 Handling Program Output 411
11.6 Recommended Reading and Web Sites 413
11.7 Key Terms, Review Questions, and Problems 414

Chapter 12 Operating System Security 418

12.1 Introduction to Operating System Security 420
12.2 System Security Planning 421
12.3 Operating Systems Hardening 421
12.4 Application Security 426
12.5 Security Maintenance 427
12.6 Linux/Unix Security 428

12.7 Windows Security 432
12.8 Virtualization Security 434
12.9 Recommended Reading and Web Sites 438
12.10 Key Terms, Review Questions, and Problems 439

Chapter 13 Trusted Computing and Multilevel Security 442

13.1 The Bell-LaPadula Model for Computer Security 443
13.2 Other Formal Models for Computer Security 453
13.3 The Concept of Trusted Systems 459
13.4 Application of Multilevel Security 462
13.5 Trusted Computing and the Trusted Platform Module 469
13.6 Common Criteria for Information Technology Security Evaluation 473
13.7 Assurance and Evaluation 479
13.8 Recommended Reading and Web Sites 484
13.9 Key Terms, Review Questions, and Problems 485

PART THREE: MANAGEMENT ISSUES 488

Chapter 14 IT Security Management and Risk Assessment 488

14.1 IT Security Management 489
14.2 Organizational Context and Security Policy 492
14.3 Security Risk Assessment 495
14.4 Detailed Security Risk Analysis 498
14.5 Case Study: Silver Star Mines 510
14.6 Recommended Reading and Web Sites 515
14.7 Key Terms, Review Questions, and Problems 516

Chapter 15 IT Security Controls, Plans, and Procedures 519

15.1 IT Security Management Implementation 520
15.2 Security Controls or Safeguards 520
15.3 IT Security Plan 528
15.4 Implementation of Controls 529
15.5 Implementation Follow-up 530
15.6 Case Study: Silver Star Mines 533
15.7 Recommended Reading 536
15.8 Key Terms, Review Questions, and Problems 536

Chapter 16 Physical and Infrastructure Security 538

16.1 Overview 539
16.2 Physical Security Threats 540
16.3 Physical Security Prevention and Mitigation Measures 547
16.4 Recovery from Physical Security Breaches 550
16.5 Example: A Corporate Physical Security Policy 551
16.6 Integration of Physical and Logical Security 551
16.7 Recommended Reading and Web Sites 558
16.8 Key Terms, Review Questions, and Problems 559

Chapter 17 Human Resources Security 561

17.1 Security Awareness, Training, and Education 562
17.2 Employment Practices and Policies 568

17.3 E-Mail and Internet Use Policies 571
17.4 Computer Security Incident Response Teams 572
17.5 Recommended Reading and Web Sites 579
17.6 Key Terms, Review Questions, and Problems 580

Chapter 18 Security Auditing 582

18.1 Security Auditing Architecture 584
18.2 The Security Audit Trail 589
18.3 Implementing the Logging Function 593
18.4 Audit Trail Analysis 605
18.5 Example: An Integrated Approach 609
18.6 Recommended Reading and Web Site 612
18.7 Key Terms, Review Questions, and Problems 613

Chapter 19 Legal and Ethical Aspects 615

19.1 Cybercrime and Computer Crime 616
19.2 Intellectual Property 620
19.3 Privacy 627
19.4 Ethical Issues 633
19.5 Recommended Reading and Web Sites 640
19.6 Key Terms, Review Questions, and Problems 642

PART FOUR CRYPTOGRAPHIC ALGORITHMS 645

Chapter 20 Symmetric Encryption and Message Confidentiality 645

20.1 Symmetric Encryption Principles 646
20.2 Data Encryption Standard 651
20.3 Advanced Encryption Standard 653
20.4 Stream Ciphers and RC4 659
20.5 Cipher Block Modes of Operation 662
20.6 Location of Symmetric Encryption Devices 668
20.7 Key Distribution 670
20.8 Recommended Reading and Web Sites 672
20.9 Key Terms, Review Questions, and Problems 672

Chapter 21 Public-Key Cryptography and Message Authentication 677

21.1 Secure Hash Functions 678
21.2 HMAC 684
21.3 The RSA Public-Key Encryption Algorithm 687
21.4 Diffie-Hellman and Other Asymmetric Algorithms 693
21.5 Recommended Reading and Web Sites 698
21.6 Key Terms, Review Questions, and Problems 698

PART FIVE NETWORK SECURITY 702

Chapter 22 Internet Security Protocols and Standards 702

22.1 Secure E-mail and S/MIME 703
22.2 DomainKeys Identified Mail 706
22.3 Secure Sockets Layer (SSL) and Transport Layer Security (TLS) 710
22.4 HTTPS 714

22.5 IPv4 and IPv6 Security 716
22.6 Recommended Reading and Web Sites 721
22.7 Key Terms, Review Questions, and Problems 722

Chapter 23 Internet Authentication Applications 725

23.1 Kerberos 726
23.2 X.509 732
23.3 Public-Key Infrastructure 735
23.4 Federated Identity Management 737
23.5 Recommended Reading and Web Sites 741
23.6 Key Terms, Review Questions, and Problems 742

Chapter 24 Wireless Network Security 744

24.1 Wireless Security Overview 745
24.2 IEEE 802.11 Wireless LAN Overview 748
24.3 IEEE 802.11i Wireless LAN Security 754
24.4 Recommended Reading and Web Sites 768
24.5 Key Terms, Review Questions, and Problems 769

APPENDICES

Appendix A Projects and Other Student Exercises for Teaching Computer Security 772

A.1 Hacking Project 773
A.2 Laboratory Exercises 774
A.3 Research Projects 774
A.4 Programming Projects 775
A.5 Practical Security Assessments 775
A.6 Firewall Projects 776
A.7 Case Studies 776
A.8 Writing Assignments 776
A.9 Reading/Report Assignments 777

References 778

Index 796

Credits 809