

# COMPUTER SECURITY

*PRINCIPLES AND PRACTICE*

Fourth Edition

**William Stallings**

**Lawrie Brown**

UNSW Canberra at the Australian Defence Force Academy



330 Hudson Street, New York, NY 10013

# CONTENTS

Cover

Title Page

Copyright

Dedication

## ONLINE CHAPTERS AND APPENDICES

Preface xii

Notation xxi

About the Authors xxii

### Chapter 1 Overview 1

1.1 Computer Security Concepts 2

1.2 Threats, Attacks, and Assets 9

1.3 Security Functional Requirements 15

1.4 Fundamental Security Design Principles 17

1.5 Attack Surfaces and Attack Trees 21

1.6 Computer Security Strategy 24

1.7 Standards 26

1.8 Key Terms, Review Questions, and Problems 27

## PART ONE COMPUTER SECURITY TECHNOLOGY AND PRINCIPLES 30

### Chapter 2 Cryptographic Tools 30

2.1 Confidentiality with Symmetric Encryption 31

2.2 Message Authentication and Hash Functions 37

2.3 Public-Key Encryption 45

2.4 Digital Signatures and Key Management 50

2.5 Random and Pseudorandom Numbers 55

2.6 Practical Application: Encryption of Stored Data 57

2.7 Key Terms, Review Questions, and Problems 58

## **Chapter 3 User Authentication 63**

- 3.1 Digital User Authentication Principles 65**
- 3.2 Password-Based Authentication 70**
- 3.3 Token-Based Authentication 82**
- 3.4 Biometric Authentication 87**
- 3.5 Remote User Authentication 92**
- 3.6 Security Issues for User Authentication 95**
- 3.7 Practical Application: An Iris Biometric System 97**
- 3.8 Case Study: Security Problems for ATM Systems 99**
  
- 3.9 Key Terms, Review Questions, and Problems 102**

## **Chapter 4 Access Control 105**

- 4.1 Access Control Principles 106**
- 4.2 Subjects, Objects, and Access Rights 109**
- 4.3 Discretionary Access Control 110**
- 4.4 Example: UNIX File Access Control 117**
- 4.5 Role-Based Access Control 120**
- 4.6 Attribute-Based Access Control 126**
- 4.7 Identity, Credential, and Access Management 132**
- 4.8 Trust Frameworks 136**
- 4.9 Case Study: RBAC System for a Bank 140**
  
- 4.10 Key Terms, Review Questions, and Problems 142**

## **Chapter 5 Database and Data Center Security 147**

- 5.1 The Need for Database Security 148**
- 5.2 Database Management Systems 149**
- 5.3 Relational Databases 151**
- 5.4 SQL Injection Attacks 155**
- 5.5 Database Access Control 161**
- 5.6 Inference 166**
- 5.7 Database Encryption 168**
- 5.8 Data Center Security 172**

5.9 Key Terms, Review Questions, and Problems	178
<b>Chapter 6 Malicious Software</b>	<b>183</b>
6.1 Types of Malicious Software (Malware)	185
6.2 Advanced Persistent Threat	187
6.3 Propagation—Infected Content—Viruses	188
6.4 Propagation—Vulnerability Exploit—Worms	193
6.5 Propagation—Social Engineering—Spam E-mail, Trojans	202
6.6 Payload—System Corruption	205
6.7 Payload—Attack Agent—Zombie, Bots	207
6.8 Payload—Information Theft—Keyloggers, Phishing, Spyware	209
6.9 Payload—Stealth—Backdoors, Rootkits	211
6.10 Countermeasures	214
6.11 Key Terms, Review Questions, and Problems	220
<b>Chapter 7 Denial-of-Service Attacks</b>	<b>224</b>
7.1 Denial-of-Service Attacks	225
7.2 Flooding Attacks	233
7.3 Distributed Denial-of-Service Attacks	234
7.4 Application-Based Bandwidth Attacks	236
7.5 Reflector and Amplifier Attacks	239
7.6 Defenses Against Denial-of-Service Attacks	243
7.7 Responding to a Denial-of-Service Attack	247
7.8 Key Terms, Review Questions, and Problems	248
<b>Chapter 8 Intrusion Detection</b>	<b>251</b>
8.1 Intruders	252
8.2 Intrusion Detection	256
8.3 Analysis Approaches	259
8.4 Host-Based Intrusion Detection	262
8.5 Network-Based Intrusion Detection	267
8.6 Distributed or Hybrid Intrusion Detection	273

**8.7 Intrusion Detection Exchange Format 275**

**8.8 Honeypots 278**

**8.9 Example System: Snort 280**

**8.10 Key Terms, Review Questions, and Problems 284**

**Chapter 9 Firewalls and Intrusion Prevention Systems 288**

**9.1 The Need for Firewalls 289**

**9.2 Firewall Characteristics and Access Policy 290**

**9.3 Types of Firewalls 292**

**9.4 Firewall Basing 298**

**9.5 Firewall Location and Configurations 301**

**9.6 Intrusion Prevention Systems 306**

**9.7 Example: Unified Threat Management Products 310**

**9.8 Key Terms, Review Questions, and Problems 314**

**PART TWO SOFTWARE AND SYSTEM SECURITY 319**

**Chapter 10 Buffer Overflow 319**

**10.1 Stack Overflows 321**

**10.2 Defending Against Buffer Overflows 342**

**10.3 Other forms of Overflow Attacks 348**

**10.4 Key Terms, Review Questions, and Problems 355**

**Chapter 11 Software Security 357**

**11.1 Software Security Issues 358**

**11.2 Handling Program Input 362**

**11.3 Writing Safe Program Code 373**

**11.4 Interacting with the Operating System and Other Programs 378**

**11.5 Handling Program Output 391**

**11.6 Key Terms, Review Questions, and Problems 393**

**Chapter 12 Operating System Security 397**

**12.1 Introduction to Operating System Security 399**

**12.2 System Security Planning 400**

**12.3 Operating Systems Hardening 400**

**12.4 Application Security 404**

**12.5 Security Maintenance 406**

**12.6 Linux/Unix Security 407**

**12.7 Windows Security 411**

**12.8 Virtualization Security 413**

**12.9 Key Terms, Review Questions, and Problems 421**

**Chapter 13 Cloud and IoT Security 423**

**13.1 Cloud Computing 424**

**13.2 Cloud Security Concepts 432**

**13.3 Cloud Security Approaches 435**

**13.4 The Internet of Things 444**

**13.5 IoT Security 448**

**13.6 Key Terms and Review Questions 456**

**PART THREE MANAGEMENT ISSUES 458**

**Chapter 14 IT Security Management and Risk Assessment 458**

**14.1 IT Security Management 459**

**14.2 Organizational Context and Security Policy 462**

**14.3 Security Risk Assessment 465**

**14.4 Detailed Security Risk Analysis 468**

**14.5 Case Study: Silver Star Mines 480**

**14.6 Key Terms, Review Questions, and Problems 485**

**Chapter 15 IT Security Controls, Plans, and Procedures 488**

**15.1 IT Security Management Implementation 489**

**15.2 Security Controls or Safeguards 489**

**15.3 IT Security Plan 498**

**15.4 Implementation of Controls 499**

**15.5 Monitoring Risks 500**

**15.6 Case Study: Silver Star Mines 502**

**15.7 Key Terms, Review Questions, and Problems 505**

**Chapter 16 Physical and Infrastructure Security 507**

**16.1 Overview 508**

**16.2 Physical Security Threats 509**

**16.3 Physical Security Prevention and Mitigation Measures 516**

**16.4 Recovery from Physical Security Breaches 519**

**16.5 Example: A Corporate Physical Security Policy 519**

**16.6 Integration of Physical and Logical Security 520**

**16.7 Key Terms, Review Questions, and Problems 526**

**Chapter 17 Human Resources Security 528**

**17.1 Security Awareness, Training, and Education 529**

**17.2 Employment Practices and Policies 535**

**17.3 E-mail and Internet Use Policies 538**

**17.4 Computer Security Incident Response Teams 539**

**17.5 Key Terms, Review Questions, and Problems 546**

**Chapter 18 Security Auditing 548**

**18.1 Security Auditing Architecture 550**

**18.2 Security Audit Trail 554**

**18.3 Implementing the Logging Function 559**

**18.4 Audit Trail Analysis 570**

**18.5 Security Information and Event Management 574**

**18.6 Key Terms, Review Questions, and Problems 576**

**Chapter 19 Legal and Ethical Aspects 578**

**19.1 Cybercrime and Computer Crime 579**

**19.2 Intellectual Property 583**

**19.3 Privacy 589**

**19.4 Ethical Issues 596**

**19.5 Key Terms, Review Questions, and Problems 602**

**Chapter 20 Symmetric Encryption and Message Confidentiality 605**

**20.1 Symmetric Encryption Principles 606**

**20.2 Data Encryption Standard 611**

**20.3 Advanced Encryption Standard 613**

**20.4 Stream Ciphers and RC4 619**

**20.5 Cipher Block Modes of Operation 622**

**20.6 Key Distribution 628**

**20.7 Key Terms, Review Questions, and Problems 630**

**Chapter 21 Public-Key Cryptography and Message Authentication 634**

**21.1 Secure Hash Functions 635**

**21.2 HMAC 641**

**21.3 Authenticated Encryption 644**

**21.4 The RSA Public-Key Encryption Algorithm 647**

**21.5 Diffie-Hellman and Other Asymmetric Algorithms 653**

**21.6 Key Terms, Review Questions, and Problems 657**

**PART FIVE NETWORK SECURITY 660**

**Chapter 22 Internet Security Protocols and Standards 660**

**22.1 Secure E-mail and S/MIME 661**

**22.2 Domainkeys Identified Mail 664**

**22.3 Secure Sockets Layer (SSL) and Transport Layer Security (TLS) 668**

**22.4 HTTPS 675**

**22.5 IPv4 and IPv6 Security 676**

**22.6 Key Terms, Review Questions, and Problems 681**

**Chapter 23 Internet Authentication Applications 684**

**23.1 Kerberos 685**

**23.2 X.509 691**

**23.3 Public-Key Infrastructure 694**

**23.4 Key Terms, Review Questions, and Problems 697**

**Chapter 24 Wireless Network Security 700**

**24.1 Wireless Security 701**



**24.2 Mobile Device Security 704**

**24.3 IEEE 802.11 Wireless Lan Overview 708**

**24.4 IEEE 802.11i Wireless Lan Security 714**

**24.5 Key Terms, Review Questions, and Problems 729**

**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 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 Key Terms, Review Questions, Problems, and Projects**

**Chapter 27 Trusted Computing and Multilevel Security**

**27.1 The Bell-LaPadula Model for Computer Security**

**27.2 Other Formal Models for Computer Security**

**27.3 The Concept of Trusted Systems**

**27.4 Application of Multilevel Security**

**27.5 Trusted Computing and the Trusted Platform Module**

**27.6 Common Criteria for Information Technology Security Evaluation**

**27.7 Assurance and Evaluation**

## **27.8 Key Terms, Review**

### **Appendix A Projects and Other Student Exercises for Teaching Computer Security 732**

#### **A.1 Hacking Project 732**

#### **A.2 Laboratory Exercises 733**

#### **A.3 Security Education (SEED) Projects 733**

#### **A.4 Research Projects 735**

#### **A.5 Programming Projects 736**

#### **A.6 Practical Security Assessments 736**

#### **A.7 Firewall Projects 736**

#### **A.8 Case Studies 737**

#### **A.9 Reading/Report Assignments 737**

#### **A.10 Writing Assignments 737**

#### **A.11 Webcasts for Teaching Computer Security 738**

### **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 The Domain Name System**

### **Appendix I The Base-Rate Fallacy**

### **Appendix J SHA-3**

### **Appendix K Glossary**

### **Acronyms 739**

### **List of NIST and ISO Documents 740**

### **References 742**

### **Credits 755**

### **Index 758**