

GLOBAL
EDITION



Computer Security

Principles and Practice

FOURTH EDITION

William Stallings • Lawrie Brown



Pearson

COMPUTER SECURITY

PRINCIPLES AND PRACTICE

Fourth Edition

Global Edition

~~14785~~ 14785

William Stallings

Lawrie Brown

UNSW Canberra at the Australian Defence Force Academy

Pearson

330 Hudson Street, New York, NY 10013

Director, Portfolio Management: Engineering,
 Computer Science & Global Editions
 Julian Perleberg
 Specialist, Higher Ed Portfolio Management:
 Tracy Johnson (Thomson Digital)
 Acquisitions Editor, Global Editions: Sarah
 Albrecht
 Portfolio Management Assistant: Meghan Jucoby
 Managing Content Producer: Scott Duxman
 Content Producer: Robert Englehardt
 Project Editor, Global Editions: K. K. Neelakantan
 Web Developer: Steve Wright
 Manager, Media Production, Global Editions: Vikram
 Kumar

Rights and Permissions Manager: Ben Brown
 Manufacturing Buyer, Higher Ed, Lake Side
 Communications Inc (LSC): Maura Zahler
 Senior Manufacturing Controller, Global Editions:
 Angela Hawksbee
 Inventory Manager: Ann Lam
 Product Marketing Manager: Yvonne Vannatta
 Field Marketing Manager: Demetrius Hall
 Marketing Assistant: Jon Bryant
 Cover Designer: Lumina Datamatics, Inc.
 Cover Photo: Alex Kosev / Shutterstock
 Full-Service Project Management: Karthika Raj
 SPi Global

Credits and acknowledgments borrowed from other sources and reproduced, with permission, in this textbook appear on page 777.

Many of the designations by manufacturers and seller to distinguish their products are claimed as trademarks. Where those designations appear in this book, and the publisher was aware of a trademark claim, the designations have been printed in initial caps or all caps.

Pearson Education Limited
 KAO Two
 KAO Park
 Harlow
 CM17 9NA
 United Kingdom

and Associated Companies throughout the world

Visit us on the World Wide Web at:
www.pearsonedglobal.com

© Pearson Education Limited 2018

The rights of William Stallings and Lawrie Brown to be identified as the authors of this work have been asserted by them in accordance with the Copyright, Designs and Patents Act 1988.

Authorized adaptation from the United States edition, entitled Computer Security: Principles and Practice, 4th Edition, ISBN 978-0-13-479410-5 by William Stallings and Lawrie Brown published by Pearson Education.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without either the written permission of the publisher or a license permitting restricted copying in the United Kingdom issued by the Copyright Licensing Agency Ltd, Saffron House, 6-10 Kirby Street, London EC1N 8TS.

All trademarks used herein are the property of their respective owners. The use of any trademark in this book does not vest in the author or publisher any trademark ownership rights in such trademarks, nor does the use of trademarks imply any affiliation with or endorsement of this book by such owners.

British Library Cataloguing-in-Publication Data

A catalogue record for this book is available from the British Library

10 9 8 7 6 5 4 3 2 1

ISBN 10: 1-292-22061-9

ISBN 13: 978-1-292-22061-1

Typeset by SPi Global

Printed and bound in Malaysia

CONTENTS

Preface 12

Notation 21

About the Authors 22

Chapter 1 Overview 23

- 1.1 Computer Security Concepts 24
- 1.2 Threats, Attacks, and Assets 31
- 1.3 Security Functional Requirements 37
- 1.4 Fundamental Security Design Principles 39
- 1.5 Attack Surfaces and Attack Trees 43
- 1.6 Computer Security Strategy 46
- 1.7 Standards 48
- 1.8 Key Terms, Review Questions, and Problems 49

PART ONE COMPUTER SECURITY TECHNOLOGY AND PRINCIPLES 52

Chapter 2 Cryptographic Tools 52

- 2.1 Confidentiality with Symmetric Encryption 53
- 2.2 Message Authentication and Hash Functions 59
- 2.3 Public-Key Encryption 67
- 2.4 Digital Signatures and Key Management 72
- 2.5 Random and Pseudorandom Numbers 77
- 2.6 Practical Application: Encryption of Stored Data 79
- 2.7 Key Terms, Review Questions, and Problems 80

Chapter 3 User Authentication 85

- 3.1 Digital User Authentication Principles 86
- 3.2 Password-Based Authentication 92
- 3.3 Token-Based Authentication 104
- 3.4 Biometric Authentication 109
- 3.5 Remote User Authentication 114
- 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 Key Terms, Review Questions, and Problems 124

Chapter 4 Access Control 127

- 4.1 Access Control Principles 128
- 4.2 Subjects, Objects, and Access Rights 131
- 4.3 Discretionary Access Control 132
- 4.4 Example: UNIX File Access Control 139
- 4.5 Role-Based Access Control 142
- 4.6 Attribute-Based Access Control 148

4.7	Identity, Credential, and Access Management	154
4.8	Trust Frameworks	158
4.9	Case Study: RBAC System for a Bank	162
4.10	Key Terms, Review Questions, and Problems	164
Chapter 5	Database and Data Center Security	169
5.1	The Need for Database Security	170
5.2	Database Management Systems	171
5.3	Relational Databases	173
5.4	SQL Injection Attacks	177
5.5	Database Access Control	183
5.6	Inference	188
5.7	Database Encryption	190
5.8	Data Center Security	194
5.9	Key Terms, Review Questions, and Problems	200
Chapter 6	Malicious Software	205
6.1	Types of Malicious Software (Malware)	207
6.2	Advanced Persistent Threat	209
6.3	Propagation—Infected Content—Viruses	210
6.4	Propagation—Vulnerability Exploit—Worms	215
6.5	Propagation—Social Engineering—Spam E-mail, Trojans	224
6.6	Payload—System Corruption	227
6.7	Payload—Attack Agent—Zombie, Bots	229
6.8	Payload—Information Theft—Keyloggers, Phishing, Spyware	231
6.9	Payload—Stealth—Backdoors, Rootkits	233
6.10	Countermeasures	236
6.11	Key Terms, Review Questions, and Problems	242
Chapter 7	Denial-of-Service Attacks	246
7.1	Denial-of-Service Attacks	247
7.2	Flooding Attacks	255
7.3	Distributed Denial-of-Service Attacks	256
7.4	Application-Based Bandwidth Attacks	258
7.5	Reflector and Amplifier Attacks	261
7.6	Defenses Against Denial-of-Service Attacks	265
7.7	Responding to a Denial-of-Service Attack	269
7.8	Key Terms, Review Questions, and Problems	270
Chapter 8	Intrusion Detection	273
8.1	Intruders	274
8.2	Intrusion Detection	278
8.3	Analysis Approaches	281
8.4	Host-Based Intrusion Detection	284
8.5	Network-Based Intrusion Detection	289
8.6	Distributed or Hybrid Intrusion Detection	295
8.7	Intrusion Detection Frameworks	297

- 8.8 Honeypots 300
- 8.9 Example System: Snort 302
- 8.10 Key Terms, Review Questions, and Problems 306

Chapter 9 Firewalls and Intrusion Prevention Systems 310

- 9.1 The Need for Firewalls 311
- 9.2 Firewall Characteristics and Access Policy 312
- 9.3 Types of Firewalls 314
- 9.4 Firewall Basing 320
- 9.5 Firewall Location and Configurations 323
- 9.6 Intrusion Prevention Systems 328
- 9.7 Example: Unified Threat Management Products 332
- 9.8 Key Terms, Review Questions, and Problems 336

PART TWO SOFTWARE AND SYSTEM SECURITY 341

Chapter 10 Buffer Overflow 341

- 10.1 Stack Overflows 343
- 10.2 Defending Against Buffer Overflows 364
- 10.3 Other forms of Overflow Attacks 370
- 10.4 Key Terms, Review Questions, and Problems 377

Chapter 11 Software Security 379

- 11.1 Software Security Issues 380
- 11.2 Handling Program Input 384
- 11.3 Writing Safe Program Code 395
- 11.4 Interacting with the Operating System and Other Programs 400
- 11.5 Handling Program Output 413
- 11.6 Key Terms, Review Questions, and Problems 415

Chapter 12 Operating System Security 419

- 12.1 Introduction to Operating System Security 421
- 12.2 System Security Planning 422
- 12.3 Operating Systems Hardening 422
- 12.4 Application Security 426
- 12.5 Security Maintenance 428
- 12.6 Linux/Unix Security 429
- 12.7 Windows Security 433
- 12.8 Virtualization Security 435
- 12.9 Key Terms, Review Questions, and Problems 443

Chapter 13 Cloud and IoT Security 445

- 13.1 Cloud Computing 446
- 13.2 Cloud Security Concepts 454
- 13.3 Cloud Security Approaches 457
- 13.4 The Internet of Things 466
- 13.5 IoT Security 470
- 13.6 Key Terms and Review Questions 478

Chapter 14 IT Security Management and Risk Assessment 480

- 14.1 IT Security Management 481
- 14.2 Organizational Context and Security Policy 484
- 14.3 Security Risk Assessment 487
- 14.4 Detailed Security Risk Analysis 490
- 14.5 Case Study: Silver Star Mines 502
- 14.6 Key Terms, Review Questions, and Problems 507

Chapter 15 IT Security Controls, Plans, and Procedures 510

- 15.1 IT Security Management Implementation 511
- 15.2 Security Controls or Safeguards 511
- 15.3 IT Security Plan 520
- 15.4 Implementation of Controls 521
- 15.5 Monitoring Risks 522
- 15.6 Case Study: Silver Star Mines 524
- 15.7 Key Terms, Review Questions, and Problems 527

Chapter 16 Physical and Infrastructure Security 529

- 16.1 Overview 530
- 16.2 Physical Security Threats 531
- 16.3 Physical Security Prevention and Mitigation Measures 538
- 16.4 Recovery from Physical Security Breaches 541
- 16.5 Example: A Corporate Physical Security Policy 541
- 16.6 Integration of Physical and Logical Security 542
- 16.7 Key Terms, Review Questions, and Problems 548

Chapter 17 Human Resources Security 550

- 17.1 Security Awareness, Training, and Education 551
- 17.2 Employment Practices and Policies 557
- 17.3 E-mail and Internet Use Policies 560
- 17.4 Computer Security Incident Response Teams 561
- 17.5 Key Terms, Review Questions, and Problems 568

Chapter 18 Security Auditing 570

- 18.1 Security Auditing Architecture 572
- 18.2 Security Audit Trail 576
- 18.3 Implementing the Logging Function 581
- 18.4 Audit Trail Analysis 592
- 18.5 Security Information and Event Management 596
- 18.6 Key Terms, Review Questions, and Problems 598

Chapter 19 Legal and Ethical Aspects 600

- 19.1 Cybercrime and Computer Crime 601
- 19.2 Intellectual Property 605
- 19.3 Privacy 611
- 19.4 Ethical Issues 618
- 19.5 Key Terms, Review Questions, and Problems 624

PART FOUR CRYPTOGRAPHIC ALGORITHMS 627**Chapter 20 Symmetric Encryption and Message Confidentiality 627**

- 20.1 Symmetric Encryption Principles 628
- 20.2 Data Encryption Standard 633
- 20.3 Advanced Encryption Standard 635
- 20.4 Stream Ciphers and RC4 641
- 20.5 Cipher Block Modes of Operation 644
- 20.6 Key Distribution 650
- 20.7 Key Terms, Review Questions, and Problems 652

Chapter 21 Public-Key Cryptography and Message Authentication 656

- 21.1 Secure Hash Functions 657
- 21.2 HMAC 663
- 21.3 Authenticated Encryption 666
- 21.4 The RSA Public-Key Encryption Algorithm 669
- 21.5 Diffie-Hellman and Other Asymmetric Algorithms 675
- 21.6 Key Terms, Review Questions, and Problems 679

PART FIVE NETWORK SECURITY 682**Chapter 22 Internet Security Protocols and Standards 682**

- 22.1 Secure E-mail and S/MIME 683
- 22.2 Domainkeys Identified Mail 686
- 22.3 Secure Sockets Layer (SSL) and Transport Layer Security (TLS) 690
- 22.4 HTTPS 697
- 22.5 IPv4 and IPv6 Security 698
- 22.6 Key Terms, Review Questions, and Problems 703

Chapter 23 Internet Authentication Applications 706

- 23.1 Kerberos 707
- 23.2 X.509 713
- 23.3 Public-Key Infrastructure 716
- 23.4 Key Terms, Review Questions, and Problems 719

Chapter 24 Wireless Network Security 722

- 24.1 Wireless Security 723
- 24.2 Mobile Device Security 726
- 24.3 IEEE 802.11 Wireless LAN Overview 730
- 24.4 IEEE 802.11i Wireless LAN Security 736
- 24.5 Key Terms, Review Questions, and Problems 751

Appendix A Projects and Other Student Exercises for Teaching Computer Security 754

- A.1 Hacking Project 754
- A.2 Laboratory Exercises 755
- A.3 Security Education (SEED) Projects 755
- A.4 Research Projects 757
- A.5 Programming Projects 758
- A.6 Practical Security Assessments 758

10 CONTENTS

- A.7** Firewall Projects 758
- A.8** Case Studies 759
- A.9** Reading/Report Assignments 759
- A.10** Writing Assignments 759
- A.11** Webcasts for Teaching Computer Security 760

Acronyms 761

List of NIST and ISO Documents 762

References 764

Credits 777

Index 780