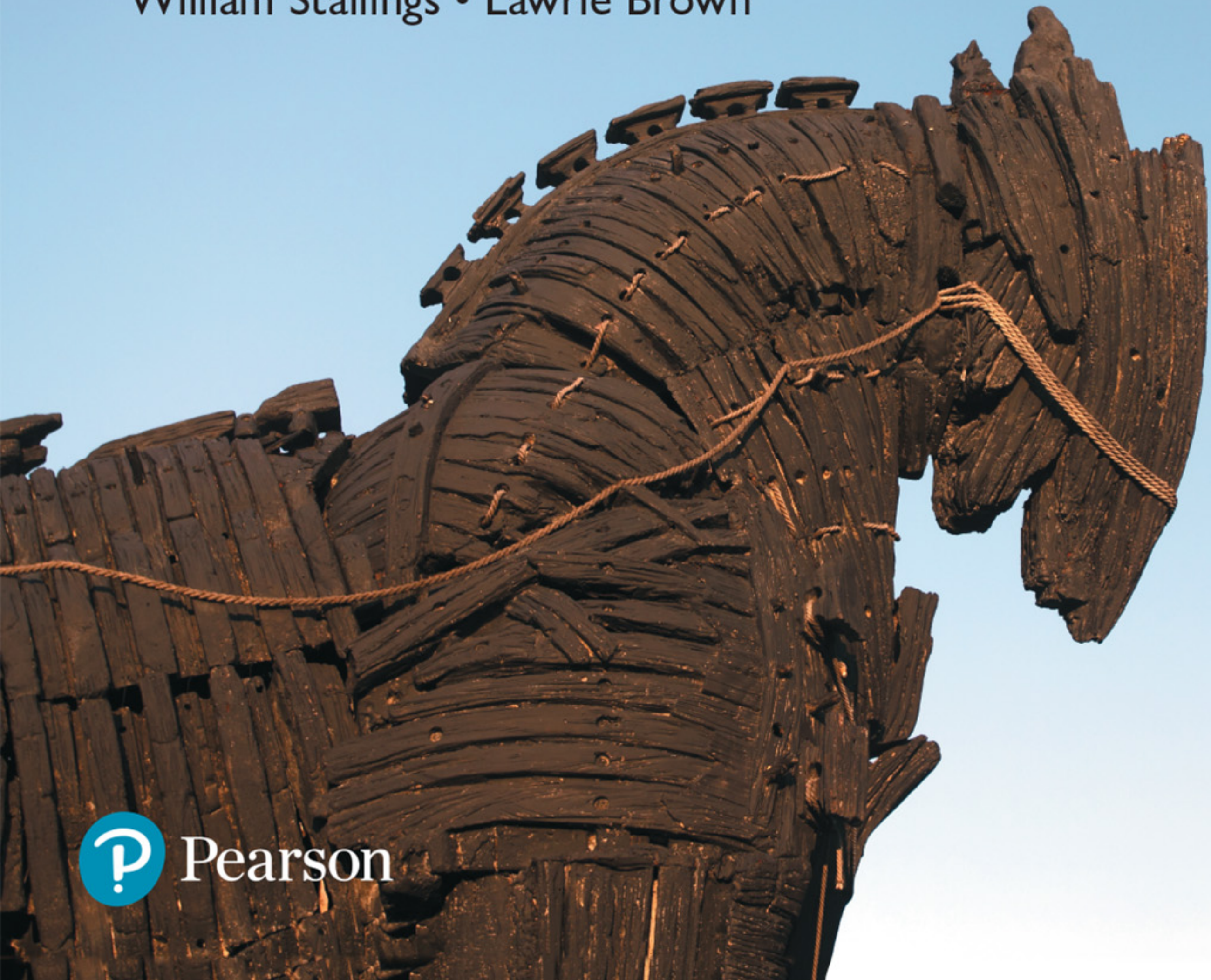
GLOBAL EDITION

Computer Security

Principles and Practice

FOURTH EDITION

William Stallings • Lawrie Brown



Pearson

Digital Resources for Students

Your new textbook provides 12-month access to digital resources that may include VideoNotes (step-by-step video tutorials on programming concepts), source code, web chapters, quizzes, and more. Refer to the preface in the textbook for a detailed list of resources.

Follow the instructions below to register for the Companion Website for William Stallings/Lawrie Brown's *Computer Security: Principles and Practice,* Fourth Edition, Global Edition.

1. Go to www.pearsonglobaleditions.com/stallings.
2. Enter the title of your textbook or browse by author name.
3. Click Companion Website.
4. Click Register and follow the on-screen instructions to create a login name and password.

Use a coin to scratch off the coating and reveal your access code.
Do not use a sharp knife or other sharp object as it may damage the code.

Use the login name and password you created during registration to start using the online resources that accompany your textbook.

IMPORTANT:

This access code can only be used once. This subscription is valid for 12 months upon activation and is not transferrable. If the access code has already been revealed it may no longer be valid.

For technical support go to https://support.pearson.com/getsupport/

Computer Security: Principles and Practice, Global Edition

Table of Contents

Front Cover

Title Page

Copyright Page

Dedication Page

Contents

Preface

Notation

About the Authors

Chapter 1 Overview

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

Part One Computer Security Technology and Principles

- Chapter 2 Cryptographic Tools
  - 2.1 Confidentiality with Symmetric Encryption
  - 2.2 Message Authentication and Hash Functions

Table of Contents

2.3 Public-Key Encryption

2.4 Digital Signatures and Key Management

2.5 Random and Pseudorandom Numbers

2.6 Practical Application: Encryption of Stored Data

2.7 Key Terms, Review Questions, and Problems

Chapter 3 User Authentication

3.1 Digital User Authentication Principles

3.2 Password-Based Authentication

3.3 Token-Based Authentication

3.4 Biometric Authentication

3.5 Remote User Authentication

3.6 Security Issues for User Authentication

3.7 Practical Application: An Iris Biometric System

3.8 Case Study: Security Problems for ATM Systems

3.9 Key Terms, Review Questions, and Problems

Chapter 4 Access Control

4.1 Access Control Principles

4.2 Subjects, Objects, and Access Rights

4.3 Discretionary Access Control

4.4 Example: UNIX File Access Control

4.5 Role-Based Access Control

4.6 Attribute-Based Access Control

4.7 Identity, Credential, and Access Management

4.8 Trust Frameworks

4.9 Case Study: RBAC System for a Bank

4.10 Key Terms, Review Questions, and Problems

Chapter 5 Database and Data Center Security

5.1 The Need for Database Security

5.2 Database Management Systems

Table of Contents

5.3 Relational Databases

5.4 SQL Injection Attacks

5.5 Database Access Control

5.6 Inference

5.7 Database Encryption

5.8 Data Center Security

5.9 Key Terms, Review Questions, and Problems

Chapter 6 Malicious Software

6.1 Types of Malicious Software (Malware)

6.2 Advanced Persistent Threat

6.3 PropagationInfected ContentViruses

6.4 PropagationVulnerability ExploitWorms

6.5 PropagationSocial EngineeringSpam E-mail, Trojans

6.6 PayloadSystem Corruption

6.7 PayloadAttack AgentZombie, Bots

6.8 PayloadInformation TheftKeyloggers, Phishing, Spyware

6.9 PayloadStealthingBackdoors, Rootkits

6.10 Countermeasures

6.11 Key Terms, Review Questions, and Problems

Chapter 7 Denial-of-Service Attacks

7.1 Denial-of-Service Attacks

7.2 Flooding Attacks

7.3 Distributed Denial-of-Service Attacks

7.4 Application-Based Bandwidth Attacks

7.5 Reflector and Amplifier Attacks

7.6 Defenses Against Denial-of-Service Attacks

7.7 Responding to a Denial-of-Service Attack

7.8 Key Terms, Review Questions, and Problems

Chapter 8 Intrusion Detection

Table of Contents

8.1 Intruders

8.2 Intrusion Detection

8.3 Analysis Approaches

8.4 Host-Based Intrusion Detection

8.5 Network-Based Intrusion Detection

8.6 Distributed or Hybrid Intrusion Detection

8.7 Intrusion Detection Exchange Format

8.8 Honeypots

8.9 Example System: Snort

8.10 Key Terms, Review Questions, and Problems

Chapter 9 Firewalls and Intrusion Prevention Systems

9.1 The Need for Firewalls

9.2 Firewall Characteristics and Access Policy

9.3 Types of Firewalls

9.4 Firewall Basing

9.5 Firewall Location and Configurations

9.6 Intrusion Prevention Systems

9.7 Example: Unified Threat Management Products

9.8 Key Terms, Review Questions, and Problems

Part Two Software and System Security

Chapter 10 Buffer Overflow

10.1 Stack Overflows

10.2 Defending Against Buffer Overflows

10.3 Other forms of Overflow Attacks

10.4 Key Terms, Review Questions, and Problems

Chapter 11 Software Security

11.1 Software Security Issues

11.2 Handling Program Input

11.3 Writing Safe Program Code

Table of Contents

11.4 Interacting with the Operating System and Other Programs

11.5 Handling Program Output

11.6 Key Terms, Review Questions, and Problems

Chapter 12 Operating System Security

12.1 Introduction to Operating System Security

12.2 System Security Planning

12.3 Operating Systems Hardening

12.4 Application Security

12.5 Security Maintenance

12.6 Linux/Unix Security

12.7 Windows Security

12.8 Virtualization Security

12.9 Key Terms, Review Questions, and Problems

Chapter 13 Cloud and IoT Security

13.1 Cloud Computing

13.2 Cloud Security Concepts

13.3 Cloud Security Approaches

13.4 The Internet of Things

13.5 IoT Security

13.6 Key Terms and Review Questions

Part Three Management Issues

Chapter 14 IT Security Management and Risk Assessment

14.1 IT Security Management

14.2 Organizational Context and Security Policy

14.3 Security Risk Assessment

14.4 Detailed Security Risk Analysis

14.5 Case Study: Silver Star Mines

14.6 Key Terms, Review Questions, and Problems

Chapter 15 IT Security Controls, Plans, and Procedures

Table of Contents

15.1 IT Security Management Implementation

15.2 Security Controls or Safeguards

15.3 IT Security Plan

15.4 Implementation of Controls

15.5 Monitoring Risks

15.6 Case Study: Silver Star Mines

15.7 Key Terms, Review Questions, and Problems

Chapter 16 Physical and Infrastructure Security

16.1 Overview

16.2 Physical Security Threats

16.3 Physical Security Prevention and Mitigation Measures

16.4 Recovery from Physical Security Breaches

16.5 Example: A Corporate Physical Security Policy

16.6 Integration of Physical and Logical Security

16.7 Key Terms, Review Questions, and Problems

Chapter 17 Human Resources Security

17.1 Security Awareness, Training, and Education

17.2 Employment Practices and Policies

17.3 E-mail and Internet Use Policies

17.4 Computer Security Incident Response Teams

17.5 Key Terms, Review Questions, and Problems

Chapter 18 Security Auditing

18.1 Security Auditing Architecture

18.2 Security Audit Trail

18.3 Implementing the Logging Function

18.4 Audit Trail Analysis

18.5 Security Information and Event Management

18.6 Key Terms, Review Questions, and Problems

Chapter 19 Legal and Ethical Aspects

Table of Contents

19.1 Cybercrime and Computer Crime

19.2 Intellectual Property

19.3 Privacy

19.4 Ethical Issues

19.5 Key Terms, Review Questions, and Problems

Part Four Cryptographic Algorithms

Chapter 20 Symmetric Encryption and Message Confidentiality

20.1 Symmetric Encryption Principles

20.2 Data Encryption Standard

20.3 Advanced Encryption Standard

20.4 Stream Ciphers and RC4

20.5 Cipher Block Modes of Operation

20.6 Key Distribution

20.7 Key Terms, Review Questions, and Problems

Chapter 21 Public-Key Cryptography and Message Authentication

21.1 Secure Hash Functions

21.2 HMAC

21.3 Authenticated Encryption

21.4 The RSA Public-Key Encryption Algorithm

21.5 Diffie-Hellman and Other Asymmetric Algorithms

21.6 Key Terms, Review Questions, and Problems

Part Five Network Security

Chapter 22 Internet Security Protocols and Standards

22.1 Secure E-mail and S/Mime

22.2 Domainkeys Identified Mail

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

22.4 HTTPS

22.5 IPv4 and IPv6 Security

22.6 Key Terms, Review Questions, and Problems

Table of Contents

Chapter 23 Internet Authentication Applications

23.1 Kerberos

23.2 X.509

23.3 Public-Key Infrastructure

23.4 Key Terms, Review Questions, and Problems

Chapter 24 Wireless Network Security

24.1 Wireless Security

24.2 Mobile Device Security

24.3 IEEE 802.11 Wireless Lan Overview

24.4 IEEE 802.11i Wireless Lan Security

24.5 Key Terms, Review Questions, and Problems

Appendix A Projects and Other Student Exercises for Teaching Computer Security

A.1 Hacking Project

A.2 Laboratory Exercises

A.3 Security Education (SEED) Projects

A.4 Research Projects

A.5 Programming Projects

A.6 Practical Security Assessments

A.7 Firewall Projects

A.8 Case Studies

A.9 Reading/Report Assignments

A.10 Writing Assignments

A.11 Webcasts for Teaching Computer Security

Acronyms

List of NIST and ISO Documents

References

Pearson

Table of Contents

Credits

Index

Online Chapters and Appendices

Chapter 25 Linux Security

25.1 Introduction

25.2 Linuxs 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 References

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 References

26.8 Key Terms 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

Table of Contents

27.8 References

27.9 Key Terms, Review Questions and Problems

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

Back Cover

Pearson