

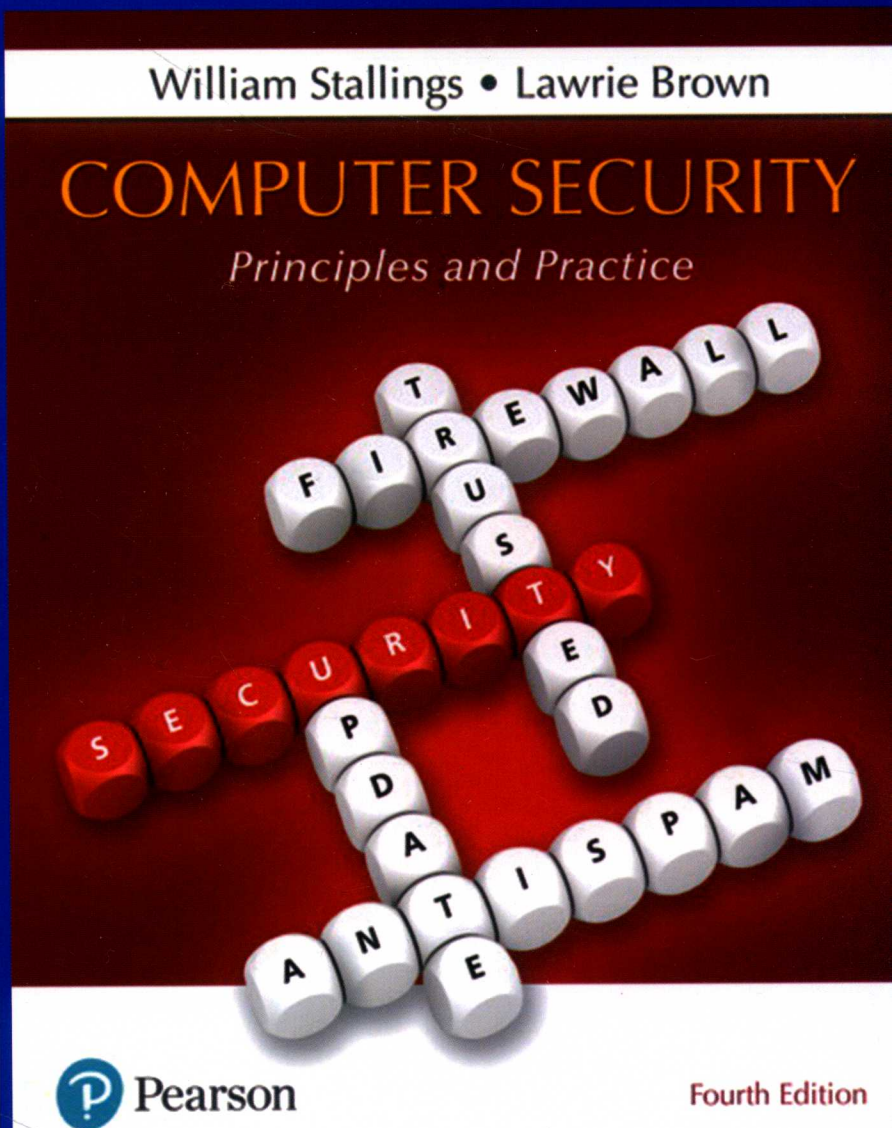
计算机安全

原理与实践

[美] 威廉·斯托林斯 [澳] 劳里·布朗 著
William Stallings Lawrie Brown

(英文版·原书第4版)

Computer Security
Principles and Practice (Fourth Edition)



经典原版书库

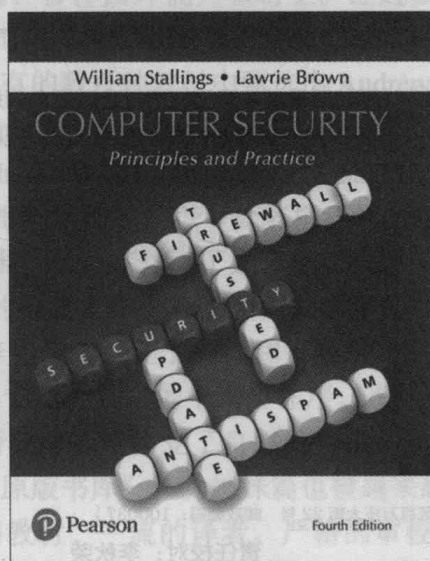
计算机安全

原理与实践

(英文版·原书第4版)

Computer Security

Principles and Practice (Fourth Edition)



[美] 威廉·斯托林斯 [澳] 劳里·布朗 著
William Stallings Lawrie Brown

华章网站: www.hzbook.com
电子邮件: hzjsj@hzbook.com

联系电话: (010) 88379604

联系地址: 北京市西城区百万庄大街24号

邮政编码: 100037



机械工业出版社
China Machine Press

华章科技图书出版中心

图书在版编目 (CIP) 数据

计算机安全: 原理与实践 (英文版·原书第4版) / (美) 威廉·斯托林斯 (William Stallings) 等著.
—北京: 机械工业出版社, 2019.3

(经典原版书库)

书名原文: Computer Security: Principles and Practice, Fourth Edition

ISBN 978-7-111-62228-4

I. 计… II. 威… III. 计算机安全—教材—英文 IV. TP309

中国版本图书馆 CIP 数据核字 (2019) 第 046070 号

本书版权登记号: 图字 01-2018-7389

Authorized Reprint from the English language edition, entitled *Computer Security: Principles and Practice*, Fourth Edition, William Stallings, Lawrie Brown, published by Pearson Education, Inc., Copyright © Pearson Education Limited 2018.

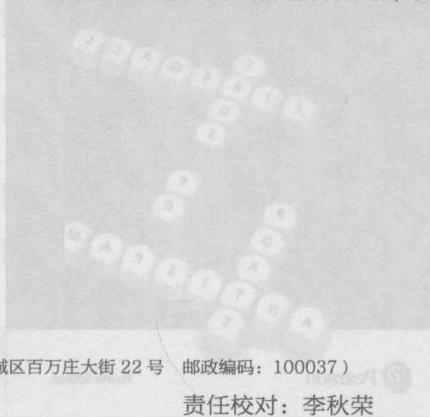
All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without permission from Pearson Education, Inc.

English language edition published by China Machine Press, Copyright © 2019.

本书英文影印版由 Pearson Education Inc. 授权机械工业出版社独家出版。未经出版者书面许可, 不得以任何方式复制或抄袭本书内容。

此影印版仅限于中华人民共和国境内 (不包括香港、澳门特别行政区及台湾地区) 销售发行。

本书封面贴有 Pearson Education (培生教育出版集团) 激光防伪标签, 无标签者不得销售。



出版发行: 机械工业出版社 (北京市西城区百万庄大街 22 号 邮政编码: 100037)

责任编辑: 曲 熠

责任校对: 李秋荣

印 刷: 中国电影出版社印刷厂

版 次: 2019 年 4 月第 1 版第 1 次印刷

开 本: 186mm×240mm 1/16

印 张: 48.5

书 号: ISBN 978-7-111-62228-4

定 价: 139.00 元

凡购本书, 如有缺页、倒页、脱页, 由本社发行部调换

客服热线: (010) 88378991 88379833

投稿热线: (010) 88379604

购书热线: (010) 68326294

读者信箱: hzjsj@hzbook.com

版权所有·侵权必究

封底无防伪标均为盗版

本书法律顾问: 北京大成律师事务所 韩光/邹晓东

目 录

第 1 章 概述	23	第 4 章 访问控制	127
1.1 计算机安全的概念	24	4.1 访问控制原理	128
1.2 威胁、攻击和资产	31	4.2 主体、客体和访问权	131
1.3 安全功能要求	37	4.3 自主访问控制	132
1.4 基本安全设计原则	39	4.4 实例：UNIX 文件访问控制	139
1.5 攻击面和攻击树	43	4.5 基于角色的访问控制	142
1.6 计算机安全策略	46	4.6 基于属性的访问控制	148
1.7 标准	48	4.7 身份、凭证和访问管理	154
1.8 关键术语、复习题和习题	49	4.8 信任框架	158
第一部分 计算机安全技术与原理		4.9 案例学习：银行的 RBAC 系统	162
第 2 章 密码编码工具	52	4.10 关键术语、复习题和习题	164
2.1 用对称加密实现机密性	53	第 5 章 数据库与云安全	169
2.2 消息认证和散列函数	59	5.1 数据库安全需求	170
2.3 公钥加密	67	5.2 数据库管理系统	171
2.4 数字签名和密钥管理	72	5.3 关系数据库	173
2.5 随机数和伪随机数	77	5.4 SQL 注入攻击	177
2.6 实际应用：存储数据的加密	79	5.5 数据库访问控制	183
2.7 关键术语、复习题和习题	80	5.6 推理	188
第 3 章 用户认证	85	5.7 数据库加密	190
3.1 数字用户认证方法	86	5.8 数据中心安全	194
3.2 基于口令的认证	92	5.9 关键术语、复习题和习题	200
3.3 基于令牌的认证	104	第 6 章 恶意软件	205
3.4 生物特征认证	109	6.1 恶意软件的类型	207
3.5 远程用户认证	114	6.2 高级持续性威胁	209
3.6 用户认证中的安全问题	117	6.3 传播 - 感染内容 - 病毒	210
3.7 实际应用：虹膜生物特征认证 系统	119	6.4 传播 - 漏洞利用 - 蠕虫	215
3.8 案例学习：ATM 系统的安全 问题	121	6.5 传播 - 社会工程学 - 垃圾电子 邮件、木马	224
3.9 关键术语、复习题和习题	124	6.6 载荷 - 系统损坏	227
		6.7 载荷 - 攻击代理 - zombie、bot	229

6.8 载荷 - 信息窃取 - 键盘记录器、 网络钓鱼、间谍软件	231
6.9 载荷 - 隐蔽 - 后门、rootkit	233
6.10 对抗手段	236
6.11 关键术语、复习题和习题	242

第 7 章 拒绝服务攻击

7.1 拒绝服务攻击	247
7.2 洪泛攻击	255
7.3 分布式拒绝服务攻击	256
7.4 基于应用的带宽攻击	258
7.5 反射攻击与放大攻击	261
7.6 拒绝服务攻击防范	265
7.7 对拒绝服务攻击的响应	269
7.8 关键术语、复习题和习题	270

第 8 章 入侵检测

8.1 入侵者	274
8.2 入侵检测	278
8.3 分析方法	281
8.4 基于主机的入侵检测	284
8.5 基于网络的入侵检测	289
8.6 分布式或混合式入侵检测	295
8.7 入侵检测交换格式	297
8.8 蜜罐	300
8.9 实例系统: Snort	302
8.10 关键术语、复习题和习题	306

第 9 章 防火墙与入侵防御系统

9.1 防火墙的必要性	311
9.2 防火墙的特征和访问策略	312
9.3 防火墙的类型	314
9.4 防火墙的布置	320
9.5 防火墙的部署和配置	323
9.6 入侵防御系统	328
9.7 实例: 一体化威胁管理产品	332

9.8 关键术语、复习题和习题	336
-----------------------	-----

第二部分 软件和系统安全

第 10 章 缓冲区溢出

10.1 栈溢出	343
10.2 针对缓冲区溢出的防御	364
10.3 其他形式的溢出攻击	370
10.4 关键术语、复习题和习题	377

第 11 章 软件安全

11.1 软件安全问题	380
11.2 处理程序输入	384
11.3 编写安全程序代码	395
11.4 与操作系统和其他程序进行交互	400
11.5 处理程序输出	413
11.6 关键术语、复习题和习题	415

第 12 章 操作系统安全

12.1 操作系统安全简介	421
12.2 系统安全规划	422
12.3 操作系统加固	422
12.4 应用安全	426
12.5 安全维护	428
12.6 Linux/UNIX 安全	429
12.7 Windows 安全	433
12.8 虚拟化安全	435
12.9 关键术语、复习题和习题	443

第 13 章 云和 IoT 安全

13.1 云计算	446
13.2 云安全的概念	454
13.3 云安全方法	457
13.4 物联网	466
13.5 IoT 安全	470
13.6 关键术语和复习题	478

第三部分 管理问题

第 14 章 IT 安全管理与风险评估480

- 14.1 IT 安全管理481
- 14.2 组织的情境和安全方针484
- 14.3 安全风险评估487
- 14.4 详细的安全风险分析490
- 14.5 案例学习：银星矿业502
- 14.6 关键术语、复习题和习题507

第 15 章 IT 安全控制、计划和 规程510

- 15.1 IT 安全管理的实施511
- 15.2 安全控制或保障措施511
- 15.3 IT 安全计划520
- 15.4 控制的实施521
- 15.5 监视风险522
- 15.6 案例学习：银星矿业524
- 15.7 关键术语、复习题和习题527

第 16 章 物理和基础设施安全529

- 16.1 概述530
- 16.2 物理安全威胁531
- 16.3 物理安全的防御和减缓措施538
- 16.4 物理安全破坏的恢复541
- 16.5 实例：某公司的物理安全策略541
- 16.6 物理安全和逻辑安全的集成542
- 16.7 关键术语、复习题和习题548

第 17 章 人力资源安全550

- 17.1 安全意识、培训和教育551
- 17.2 雇用实践和策略557
- 17.3 电子邮件和 Internet 使用策略560
- 17.4 计算机安全事件响应团队561
- 17.5 关键术语、复习题和习题568

第 18 章 安全审计570

- 18.1 安全审计体系结构572
- 18.2 安全审计迹576
- 18.3 实现日志功能581
- 18.4 审计迹分析592
- 18.5 安全信息和事件管理596
- 18.6 关键术语、复习题和习题598

第 19 章 法律与道德问题600

- 19.1 网络犯罪和计算机犯罪601
- 19.2 知识产权605
- 19.3 隐私611
- 19.4 道德问题618
- 19.5 关键术语、复习题和习题624

第四部分 密码编码算法

第 20 章 对称加密和消息机密性627

- 20.1 对称加密原理628
- 20.2 数据加密标准633
- 20.3 高级加密标准635
- 20.4 流密码和 RC4641
- 20.5 分组密码的工作模式644
- 20.6 密钥分发650
- 20.7 关键术语、复习题和习题652

第 21 章 公钥密码和消息认证656

- 21.1 安全散列函数657
- 21.2 HMAC663
- 21.3 认证加密666
- 21.4 RSA 公钥加密算法669
- 21.5 Diffie-Hellman 和其他非对称
算法675
- 21.6 关键术语、复习题和习题679

第五部分 网络安全

第 22 章 Internet 安全协议和

标准682

22.1 安全 E-mail 和 S/MIME683

22.2 域名密钥识别邮件标准686

22.3 安全套接层和传输层安全690

22.4 HTTPS697

22.5 IPv4 和 IPv6 的安全性698

22.6 关键术语、复习题和习题703

第 23 章 Internet 认证应用706

23.1 Kerberos707

23.2 X.509713

23.3 公钥基础设施716

23.4 关键术语、复习题和习题719

第 24 章 无线网络安全722

24.1 无线安全723

24.2 移动设备安全726

24.3 IEEE 802.11 无线局域网概述730

24.4 IEEE 802.11i 无线局域网安全736

24.5 关键术语、复习题和习题751

附录 A 计算机安全教学项目和

学生练习754

缩略语761

NIST 和 ISO 文件列表762

参考文献764

在线章节和附录^①

第 25 章 Linux 安全

第 26 章 Windows 安全

第 27 章 可信计算与多级安全

附录 B 数论的相关内容

附录 C 标准和标准制定组织

附录 D 随机数与伪随机数的生成

附录 E 基于分组密码的消息认证码

附录 F TCP/IP 协议体系结构

附录 G Radix-64 转换

附录 H 域名系统

附录 I 基率谬误

附录 J SHA-3

附录 K 术语

① 关于这些在线资源，读者可在华章图书官网 <http://www.hzbook.com> 上获得。——编辑注

Contents

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 Exchange Format	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	

PART THREE MANAGEMENT ISSUES 480**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

- 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

ONLINE CHAPTERS AND APPENDICES[⊖]

Chapter 25 Linux Security

Chapter 26 Windows and Windows Vista Security

Chapter 27 Trusted Computing and Multilevel Security

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

⊖ 关于这些在线资源，读者可在华章图书官网 <http://www.hzbook.com> 上获得。——编辑注

经典原版书库

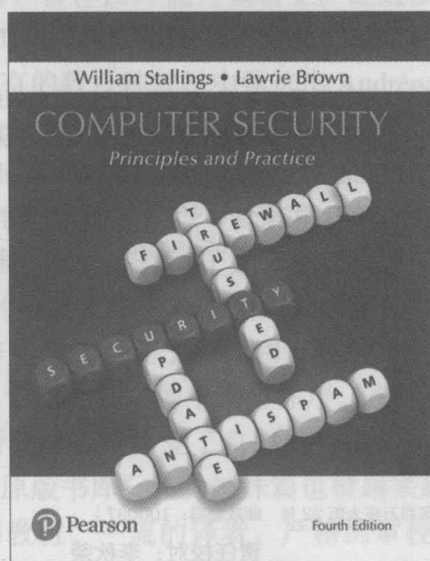
计算机安全

原理与实践

(英文版·原书第4版)

Computer Security

Principles and Practice (Fourth Edition)



[美] 威廉·斯托林斯 [澳] 劳里·布朗 著
William Stallings Lawrie Brown

华章网站: www.hzbook.com
电子邮件: hzjsj@hzbook.com

联系电话: (010) 88379614

联系地址: 北京市西城区百万庄大街24号

邮政编码: 100037



机械工业出版社
China Machine Press

华章科技图书出版中心

图书在版编目 (CIP) 数据

计算机安全: 原理与实践 (英文版·原书第4版) / (美) 威廉·斯托林斯 (William Stallings) 等著.
—北京: 机械工业出版社, 2019.3

(经典原版书库)

书名原文: Computer Security: Principles and Practice, Fourth Edition

ISBN 978-7-111-62228-4

I. 计… II. 威… III. 计算机安全—教材—英文 IV. TP309

中国版本图书馆 CIP 数据核字 (2019) 第 046070 号

本书版权登记号: 图字 01-2018-7389

Authorized Reprint from the English language edition, entitled *Computer Security: Principles and Practice*, Fourth Edition, William Stallings, Lawrie Brown, published by Pearson Education, Inc., Copyright © Pearson Education Limited 2018.

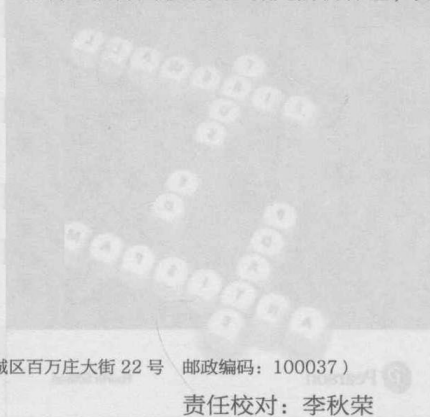
All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without permission from Pearson Education, Inc.

English language edition published by China Machine Press, Copyright © 2019.

本书英文影印版由 Pearson Education Inc. 授权机械工业出版社独家出版。未经出版者书面许可, 不得以任何方式复制或抄袭本书内容。

此影印版仅限于中华人民共和国境内 (不包括香港、澳门特别行政区及台湾地区) 销售发行。

本书封面贴有 Pearson Education (培生教育出版集团) 激光防伪标签, 无标签者不得销售。



出版发行: 机械工业出版社 (北京市西城区百万庄大街 22 号 邮政编码: 100037)

责任编辑: 曲 熠

责任校对: 李秋荣

印 刷: 中国电影出版社印刷厂

版 次: 2019 年 4 月第 1 版第 1 次印刷

开 本: 186mm×240mm 1/16

印 张: 48.5

书 号: ISBN 978-7-111-62228-4

定 价: 139.00 元

凡购本书, 如有缺页、倒页、脱页, 由本社发行部调换

客服热线: (010) 88378991 88379833

投稿热线: (010) 88379604

购书热线: (010) 68326294

读者信箱: hzsj@hzbook.com

版权所有·侵权必究

封底无防伪标均为盗版

本书法律顾问: 北京大成律师事务所 韩光/邹晓东

出版者的话

文艺复兴以来,源远流长的科学精神和逐步形成的学术规范,使西方国家在自然科学的各个领域取得了垄断性的优势;也正是这样的优势,使美国在信息技术发展的六十多年间名家辈出、独领风骚。在商业化的进程中,美国的产业界与教育界越来越紧密地结合,计算机学科中的许多泰山北斗同时身处科研和教学的最前线,由此而产生的经典科学著作,不仅擘划了研究的范畴,还揭示了学术的源变,既遵循学术规范,又自有学者个性,其价值并不会因年月的流逝而减退。

近年,在全球信息化大潮的推动下,我国的计算机产业发展迅猛,对专业人才的需求日益迫切。这对计算机教育界和出版界都既是机遇,也是挑战;而专业教材的建设在教育战略上显得举足轻重。在我国信息技术发展时间较短的现状下,美国等发达国家在其计算机科学发展的几十年间积淀和发展的经典教材仍有许多值得借鉴之处。因此,引进一批国外优秀计算机教材将对我国计算机教育事业的发展起到积极的推动作用,也是与世界接轨、建设真正的世界一流大学的必由之路。

机械工业出版社华章公司较早意识到“出版要为教育服务”。自1998年开始,我们就将工作重点放在了遴选、移译国外优秀教材上。经过多年的不懈努力,我们与Pearson、McGraw-Hill、Elsevier、MIT、John Wiley & Sons、Cengage等世界著名出版公司建立了良好的合作关系,从它们现有的数百种教材中甄选出Andrew S. Tanenbaum、Bjarne Stroustrup、Brian W. Kernighan、Dennis Ritchie、Jim Gray、Afred V. Aho、John E. Hopcroft、Jeffrey D. Ullman、Abraham Silberschatz、William Stallings、Donald E. Knuth、John L. Hennessy、Larry L. Peterson等大师名家的一批经典作品,以“计算机科学丛书”为总称出版,供读者学习、研究及珍藏。大理石纹理的封面,也正体现了这套丛书的品位和格调。

“计算机科学丛书”的出版工作得到了国内外学者的鼎力相助,国内的专家不仅提供了中肯的选题指导,还不辞劳苦地担任了翻译和审校的工作;而原书的作者也相当关注其作品在中国的传播,有的还专门为其书的中译本作序。迄今,“计算机科学丛书”已经出版了近500个品种,这些书籍在读者中树立了良好的口碑,并被许多高校采用为正式教材和参考书籍。其影印版“经典原版书库”作为姊妹篇也被越来越多实施双语教学的学校所采用。

权威的作者、经典的教材、一流的译者、严格的审校、精细的编辑,这些因素使我们的图书有了质量的保证。随着计算机科学与技术专业学科建设的不断完善和教材改革的逐渐深化,教育界对国外计算机教材的需求和应用都将步入一个新的阶段,我们的目标是尽善尽美,而反馈的意见正是我们达到这一终极目标的重要帮助。华章公司欢迎老师和读者对我们的工作提出建议或给予指正,我们的联系方式如下:

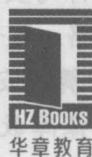
华章网站: www.hzbook.com

电子邮件: hzsj@hzbook.com

联系电话: (010) 88379604

联系地址: 北京市西城区百万庄南街1号

邮政编码: 100037



华章科技图书出版中心

前言

第4版新增内容

自本书第3版出版以来, 计算机安全领域又持续出现了一些改进和创新。在新版本中, 我们试图展现这些改进和创新, 同时, 力求在深度和广度上涵盖整个计算机安全领域。在第4版修订之初, 许多讲授该领域课程的教授和从事该领域工作的专业人士又重新仔细地审查了本书的第3版。第4版修订和完善了其中多处描述, 并对相关的图表进行了改进。

除了这些适用于教学和便于阅读方面的改进外, 本书也对一些实质性的内容进行了修订。下面列出的是其中一些较显著的修订:

- **数据中心安全:** 第5章增加了一节有关数据中心安全的内容, 其中包括有关可靠性等级的 TIA-942 标准的内容。
- **恶意软件:** 在第6章中, 对有关恶意软件的内容进行了修订, 包含了宏病毒及其结构的相关内容, 因为现在它们是病毒恶意软件的最为常见的形式。
- **虚拟化安全:** 考虑到组织和云计算环境中对虚拟化系统的使用越来越多, 在第12章中对有关虚拟化安全的内容进行了扩展, 增加了用于增强这些环境安全的虚拟防火墙的讨论。
- **云安全:** 第13章新增了有关云安全的讨论, 包括云计算的介绍、云安全的关键概念、云安全方法的分析和一个开源的示例。
- **IoT 安全:** 第13章新增了有关物联网 (Internet of Things, IoT) 安全的讨论, 包括 IoT 介绍、IoT 安全问题综述和一个开源的示例。
- **SEIM:** 第18章更新了有关安全信息和事件管理 (SIME) 系统的讨论。
- **隐私:** 第19章针对隐私问题及其管理增加了有关道德和法律方法的讨论, 以及与大数据相关的隐私问题。
- **认证加密:** 认证加密已经成为各种应用和协议中日益广泛使用的加密工具。第21章新增了有关认证描述的讨论, 并描述了一个重要的认证加密算法——分支编码本 (Offset CodeBook, OCB) 模式。

背景

近年来, 在高等教育中对计算机安全及相关主题的关注程度与日俱增。导致这一状况的因素很多, 以下是其中两个突出的因素:

1) 随着信息系统、数据库和基于 Internet 的分布式系统与通信广泛应用于商业领域, 再加上各种与安全相关的攻击愈演愈烈, 各类组织机构开始意识到必须拥有一个全面的信息安全策略。这个策略包括使用特定的软硬件和培训专业人员等。

2) 计算机安全教育, 也就是通常所说的信息安全教育 (Information Security Education) 或者信息保障教育 (Information Assurance Education), 由于与国防和国土安全密切相关,