国外计算机科学教材系列

PEARSON

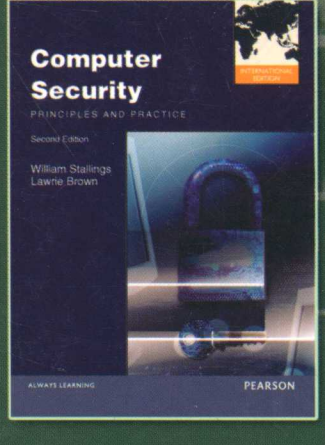
William Stallings

计算机安全

——原理与实践（第二版）

Computer Security

Principles and Practice, Second Edition



英文版

[美] William Stallings
[澳] Lawrie Brown
著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

CONTENTS

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

ONLINE CHAPTERS AND APPENDICES [1]

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 Recommended Reading and Web Sites
25.9 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 Recommended Reading and Web Sites
26.8 Key Terms, Review Questions, Problems, and Projects

Appendix B Some Aspects of Number Theory

B.1 Prime and Relatively Prime Numbers
B.2 Modular Arithmetic
B.3 Fermat's and Euler's Theorems

Appendix C Standards and Standard-Setting Organizations

C.1 The Importance of Standards
C.2 Internet Standards and the Internet Society
C.3 National Institute of Standards and Technology
C.4 The International Telecommunication Union
C.5 The International Organization for Standardization
C.6 Significant Security Standards and Documents

Appendix D Random and Pseudorandom Number Generation

D.1 The Use of Random Numbers
D.2 Pseudorandom Number Generators (PRNGs)
D.3 True Random Number Generators
D.4 References

Appendix E Message Authentication Codes Based on Block Ciphers

E.1 Cipher-Based Message Authentication Code (CMAC)
E.2 Counter with Cipher Block Chaining-Message Authentication Code

① 本书的补充章节及附录可登录华信教育资源网（www.hxedu.com.cn）注册下载。

Appendix F TCP/IP Protocol Architecture

F.1 TCP/IP Layers
F.2 TCP and UDP
F.3 Operation of TCP/IP
F.4 TCP/IP Applications

Appendix G Radix-64 Conversion

Appendix H Security Policy-Related Documents

H.1 A Company's Physical and Environmental Security Policy
H.2 Security Policy Standard of Good Practice
H.3 Security Awareness Standard of Good Practice
H.4 Information Privacy Standard of Good Practice
H.5 Incident Handling Standard of Good Practice

Appendix I The Domain Name System

I.1 Domain Names
I.2 The DNS Database
I.3 DNS Operation

Appendix J The Base-Rate Fallacy

J.1 Conditional Probability and Independence
J.2 Bayes' Theorem
J.3 The Base-Rate Fallacy Demonstrated

Appendix K Glossary

国外计算机科学教材系列

计算机安全

——原理与实践

（第二版）（英文版）

Computer Security: Principles and Practice

Second Edition

［美］ William Stallings
［澳］ Lawrie Brown 著

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

内容简介

本书在上一版的基础上进行了修订与更新，全面覆盖了计算机安全领域的相关主题。全书共分为五个部分：第一部分——计算机安全技术与原理，概述了支持有效安全策略所必需的技术领域；第二部分——软件安全与可信系统，讲解了软件开发和运行中的安全问题；第三部分——管理问题，主要讨论信息与计算机安全在管理方面的问题；第四部分——密码学算法，给出了各种类型的加密算法和其他类型的密码算法；第五部分——网络安全，重点分析了为网络通信提供安全保障的协议和标准。本书思路清晰、结构严谨，并且提供了大量精心设计的实践问题。

本书可作为高等院校计算机科学、计算机工程、电子工程等相关专业计算机安全课程的本科生双语教材，同时也是一本有关密码学和计算机网络安全方面的非常有价值的参考书。

版权贸易合同登记号　图字：01-2013-1499

图书在版编目（CIP）数据

计算机安全：原理与实践 = Computer Security: Principles and Practice：第 2 版：英文 /（美）斯托林斯（Stallings, W.），（澳）布朗（Brown, L.）著；—北京：电子工业出版社，2013.4

国外计算机科学教材系列

ISBN 978-7-121-20034-2

Ⅰ.①计…　Ⅱ.①斯…　②布…　Ⅲ.①计算机安全 - 高等学校 - 教材 - 英文　Ⅳ.①TP309

中国版本图书馆 CIP 数据核字（2013）第 060277 号

策划编辑：冯小贝

责任编辑：冯小贝

印　　刷：三河市鑫金马印装有限公司

装　　订：三河市鑫金马印装有限公司

出版发行：电子工业出版社

北京市海淀区万寿路 173 信箱　邮编：100036

开　　本：787 × 980　1/16　　印张：50.75　　字数：1520 千字

印　　次：2013 年 4 月第 1 次印刷

定　　价：99.00 元

凡所购买电子工业出版社的图书有缺损问题，请向购买书店调换；若书店售缺，请与本社发行部联系。联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

出 版 说 明

21世纪初的5至10年是我国国民经济和社会发展的重要时期，也是信息产业快速发展的关键时期。在我国加入WTO后的今天，培养一支适应国际化竞争的一流IT人才队伍是我国高等教育的重要任务之一。信息科学和技术方面人才的优劣与多寡，是我国面对国际竞争时成败的关键因素。

当前，正值我国高等教育特别是信息科学领域的教育调整、变革的重大时期，为使我国教育体制与国际化接轨，有条件的高等院校正在为某些信息学科和技术课程使用国外优秀教材和优秀原版教材，以使我国在计算机教学上尽快赶上国际先进水平。

电子工业出版社秉承多年来引进国外优秀图书的经验，翻译出版了“国外计算机科学教材系列”丛书，这套教材覆盖学科范围广、领域宽、层次多，既有本科专业课程教材，也有研究生课程教材，以适应不同院系、不同专业、不同层次的师生对教材的需求，广大师生可自由选择和自由组合使用。这些教材涉及的学科方向包括网络与通信、操作系统、计算机组织与结构、算法与数据结构、数据库与信息处理、编程语言、图形图像与多媒体、软件工程等。同时，我们也适当引进了一些优秀英文原版教材，本着翻译版本和英文原版并重的原则，对重点图书既提供英文原版又提供相应的翻译版本。

在图书选题上，我们大都选择国外著名出版公司出版的高校教材，如Pearson Education培生教育出版集团、麦格劳－希尔教育出版集团、麻省理工学院出版社、剑桥大学出版社等。撰写教材的许多作者都是蜚声世界的教授、学者，如道格拉斯·科默（Douglas E. Comer）、威廉·斯托林斯（William Stallings）、哈维·戴特尔（Harvey M. Deitel）、尤利斯·布莱克（Uyless Black）等。

为确保教材的选题质量和翻译质量，我们约请了清华大学、北京大学、北京航空航天大学、复旦大学、上海交通大学、南京大学、浙江大学、哈尔滨工业大学、华中科技大学、西安交通大学、国防科学技术大学、解放军理工大学等著名高校的教授和骨干教师参与了本系列教材的选题、翻译和审校工作。他们中既有讲授同类教材的骨干教师、博士，也有积累了几十年教学经验的老教授和博士生导师。

在该系列教材的选题、翻译和编辑加工过程中，为提高教材质量，我们做了大量细致的工作，包括对所选教材进行全面论证；选择编辑时力求达到专业对口；对排版、印制质量进行严格把关。对于英文教材中出现的错误，我们通过与作者联络和网上下载勘误表等方式，逐一进行了修订。

此外，我们还将与国外著名出版公司合作，提供一些教材的教学支持资料，希望能为授课老师提供帮助。今后，我们将继续加强与各高校教师的密切联系，为广大师生引进更多的国外优秀教材和参考书，为我国计算机科学教学体系与国际教学体系的接轨做出努力。

电子工业出版社

教材出版委员会

主　任	杨芙清	北京大学教授 中国科学院院士 北京大学信息与工程学部主任 北京大学软件工程研究所所长
委　员	王　珊	中国人民大学信息学院院长、教授
	胡道元	清华大学计算机科学与技术系教授 国际信息处理联合会通信系统中国代表
	钟玉琢	清华大学计算机科学与技术系教授、博士生导师 清华大学深圳研究生院信息学部主任
	谢希仁	中国人民解放军理工大学教授 全军网络技术研究中心主任、博士生导师
	尤晋元	上海交通大学计算机科学与工程系教授 上海分布计算技术中心主任
	施伯乐	上海国际数据库研究中心主任、复旦大学教授 中国计算机学会常务理事、上海市计算机学会理事长
	邹　鹏	国防科学技术大学计算机学院教授、博士生导师 教育部计算机基础课程教学指导委员会副主任委员
	张昆藏	青岛大学信息工程学院教授

前　言

第二版中的新内容

自本书第一版出版的5年多以来，该领域也在不断创新和改进。在这个新版本中，我们试图捕捉到这些变化，同时保持对整个领域广泛而全面的覆盖。修订过程从对本书第一版的广泛审阅开始，由一些从事该领域教学的教授或者在该领域工作的专业人士进行，新版本中很多地方的叙述更加简洁清晰，插图也得到了改进。

本书的一个明显的变化是组织结构的修订，这样一来可以更清晰地介绍相关主题。增加了新的两章“操作系统安全性”及“无线安全”。第三部分的内容进行了章节重新安排，因此更加系统化。

除了这些提高教学和用户友好性的改进之外，还有一些贯穿全书的主要实质性变化，重点包括：

- **操作系统安全性**：本章重点反映了NIST SP800-123中的内容。本章还介绍了虚拟机安全性的重要论题。
- **云安全**：一个新的小节，覆盖了与令人兴奋的新领域——云计算相关的安全问题。
- **基于应用程序的拒绝服务攻击**：一个有关拒绝服务攻击的普遍形式的新小节。
- **恶意软件**：本章与第一版相比有不同的重点。我们越来越多地看到通过社会工程学攻击安装后门/rootkit类型的恶意软件，而不是更经典的病毒/蠕虫直接感染。网络钓鱼甚至比以往任何时候都更加突出。这些趋势都体现在本书的内容中。
- **Internet安全协议及标准**：本章已扩展到包括另外两个重要的协议和服务：HTTPS和DKIM。
- **无线安全**：已经添加了新的一章“无线安全”。
- **计算机安全事件响应**：CSIR一节已进行了更新和扩充。
- **学生学习辅助**：现在每章以一个学习目标的列表开始。
- **教学大纲示例**：教材包含的材料超过了一个学期可以覆盖的内容。因此，为教师提供了几个教学大纲示例以帮助大家在有限的时间（例如16周或12周）使用教材。这些示例基于参与第一版编写的教师的实际经验。
- **实践问题集**：一组课外习题并附有答案，以供学生使用。
- **试题库**：每章都设置了一组复习题，包括判断题、多项选择题和填空题。

写作背景

近几年来，计算机安全及相关主题的教学兴趣呈现出飞速般的增长。若干因素导致了这一兴趣，列举其中两个：

1. 随着信息系统、数据库和基于Internet的分布式系统与通信在商业界的普及，再加上安全相关的攻击强度和复杂性的增加，组织机构现在已经认识到需要一个全面的安全策略。该策略包括使用专门的硬件和软件与经过培训的人员以满足这种需求。
2. 计算机安全教育，通常称为信息安全教育或信息保障教育，已成为美国及其他国家的国家目标，其中包含国防及国土安全的含义。信息系统安全教育讨论会和美国国家安全局（NSA）的信息保障课件评估（IACE）计划等组织机构，在发展计算机安全教育标准方面扮演着政府的带头角色。

因此，大学、社区学院及其他机构的计算机安全及相关领域的课程数目也越来越多。

写作目标

本书的写作目标是提供一个计算机安全发展的最新调查。安全设计和安全管理员面临的核心的问题包括确定计算机和网络系统的威胁，评价这些威胁的相对风险，以及开发用户友好和经济有效的对策。

讨论的内容涉及以下基本主题：

- **原理：**虽然本书范围广泛，但是一些基本原理在讨论主题中反复出现，统一了全书内容。例如有关身份鉴别和访问控制的问题，本书强调了这些基本原理，并探讨了它们在计算机安全具体领域的应用。
- **设计方法：**本书探讨了符合特定计算机安全要求的不同方法。
- **标准：**标准在这一领域承担着越来越重要的责任，实际上成为了占统治地位的角色。了解技术的现况及未来的发展方向，要求对相关标准进行全面的讨论。
- **真实世界的例子：**一些章包括展示本章基本原理在真实世界环境中实际应用的小节。

读者对象

本书适用于学术和专业读者，可以作为一或两个学期的计算机科学、计算机工程和电子工程专业的本科生教材。它涵盖了OS安全和保护的所有主题，这是IEEE/ ACM计算机课程计划CC2008（CS2001的临时修订版本）的一个核心学科领域，此外还包括一些其他主题。本书涵盖了IEEE/ACM 2008信息技术学士学位课程中信息保障和安全（IAS）的课程纲要的核心内容，并且涵盖了IEEE/ACM 2004计算机工程专业CE-OPS6安全和保护的课程纲要。

这是一本对该领域感兴趣的读者的基本参考书，并且适合自学。

教材的组织

本书分为五个部分（见第0章）：

- 计算机安全技术与原理
- 软件安全与可信系统
- 管理问题
- 密码学算法
- 网络安全

本书配有相关的一些在线章节和附录，其中提供了更详细的主题。

本书包括一个广泛的词汇表、常用首字母缩写词表和参考文献。每一章都给出课外习题、复习题、关键词列表、进一步的阅读建议和推荐网站。

对 CISSP 学科领域的覆盖

本书覆盖了CISSP（国际注册信息系统安全专业人员）认证要求的所有学科领域。国际信息系统安全认证协会（ISC）指定的CISSP通常称为信息安全认证的“黄金标准”，它是安全行业唯一公认的认证。许多组织，包括美国国防部和许多金融机构，现在都要求网络安全人员获得CISSP认证。2004年，CISSP成为第一个获得国际标准ISO / IEC 17024（人员认证机构通用要求）认可的IT计划。

CISSP考试基于公共知识体系（CBK），它是由一个非盈利性组织（ISC）开发和维护的信息安全最佳实践纲要。CISSP认证要求的CBK由10个领域的知识组成，本书覆盖的CBK的详细信息请参阅第0章。

学生资源[①]

在这个新版本中，大量的原始辅助材料通过网络在线提供给学生。本书配套网站位于WilliamStallings.com/ComputerSecurity（点击Student Resources链接），其中包含按章组织的一系列相关链接和一份勘误表。

此外还将在线提供下列材料：

- **网络章节：**为了降低书本的厚度和成本，其中两章以PDF格式提供。本书的目录中列出了这些章节。
- **在线附录：**总共有10个附录，包含大量支持教材中内容的有趣主题，提供给感兴趣的学生阅读。本书的目录中给出了附录列表。

① 学习资源网站的一些资源可登录华信教育资源网（www.hxedu.com.cn）注册下载。

- **课外习题和答案**：为了帮助学生理解材料，有一组独立的课外习题，并附有答案。这使学生能够测试他们对教材的理解程度。
- **重要论文**：来自专业文献的几十个文件，许多都很难找到，可以提供进一步的阅读。
- **支持文件**：网上提供了许多教材中引用的其他有用文档。

教师支持材料[①]

为教师提供的支持材料包括：

- **项目手册**：列出了所有项目类别的项目资源，包括相关文档和简易软件，以及建议的项目作业指导。
- **解答手册**：每章末的复习题和习题的答案。
- **PowerPoint 幻灯片**：一组可用于授课的覆盖所有章节的幻灯片。
- **PDF 文件**：书中所有图表的副本。
- **试题库**：按章组织的问题集。
- **教学大纲示例**：本书的内容超过了一个学期课程可以覆盖的内容量，因此为教师提供了几个示例的教学大纲，以指导教师在有限的时间内使用教材。这些示例基于编辑第一版教材的教师的实践经验。

配套网站位于WilliamStallings.com/ComputerSecurity（点击Instructor Resources 链接），包括如下内容：

- 指向其他使用该教材的课程网站的链接。
- 互联网邮件列表的登录信息，方便使用本教材的教师之间及与作者相互交换信息、建议和问题。

项目及其他学生练习

对于许多教师，计算机安全课程的一个重要组成部分是提供一个项目或一组项目，可以让学生得到实际操作经验，以加强理解教材中学到的概念。本书对此提供了一个最新的支持，其中包含一个课程项目的组成部分。教师支持材料不但包括如何分配和安排项目的指导，还包括一组各种项目类型的用户手册，并加上具体的任务分配，都是专门为本书设计的。教师可以安排以下几个类型的项目：

- **黑客练习**：两个使学生理解入侵检测和预防问题的项目。
- **实验室练习**：一系列涉及本书概念的编程和实验。

① 相关的教辅申请方式请参见书末的“教学支持说明”。