HZ BOOKS
华章教育

PEARSON

经典原版书库

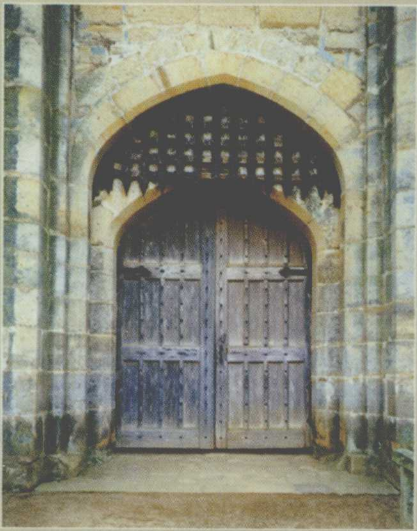
计算机安全

原理与实践

（英文版）

COMPUTER SECURITY

Principles and Practice



William Stallings
新南威尔士大学
Lawrie Brown
新南威尔士大学
等著

机械工业出版社
China Machine Press

经　典　原　版　书　库

计算机安全

原理与实践

（英文版）

William Stallings
新南威尔士大学
Lawrie Brown
新南威尔士大学
等著

机械工业出版社
China Machine Press

本书版权登记号：图字：01-2009-7320

图书在版编目（CIP）数据

计算机安全：原理与实践（英文版）/ 斯托林斯（Stallings，W.），布朗（Brown，L.）等著．—北京：机械工业出版社，2010.1
（经典原版书库）
书名原文：Computer Security：Principles and Practice

ISBN 978-7-111-29247-0

Ⅰ．计…　Ⅱ．①斯…　②布…　Ⅲ．电子计算机－安全技术－英文　Ⅳ.TP309

中国版本图书馆 CIP 数据核字（2009）第 226912 号

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：迟振春
北京京师印务有限公司印刷
2010 年 1 月第 1 版第 1 次印刷
150mm×214mm·25.625 印张
标准书号：ISBN 978-7-111-29247-0
定价：69.00 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；88361066
购书热线：（010）68326294；88379649；68995259
投稿热线：（010）88379604
读者信箱：hzjsj@hzbook.com

出版者的话

文艺复兴以降，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；也正是这样的传统，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分社较早意识到“出版要为教育服务”。自 1998 年开始，华章分社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，从他们现有的数百种教材中甄选出 Andrew S. Tanenbaum，Bjarne Stroustrup，Brain 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襄助，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，有的还专程为其书的中译本

作序。迄今，“计算机科学丛书”已经出版了近两百个品种，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。华章分社欢迎老师和读者对我们的工作提出建议或给予指正，我们的联系方法如下：

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南街1号
邮政编码：100037

HZ BOOKS
华章教育

华章科技图书出版中心

PREFACE

BACKGROUND

Interest in education in computer security and related topics has been growing at a dramatic rate in recent years. This interest has been spurred by a number of factors, two of which stand out:

1. As information systems, databases, and Internet-based distributed systems and communication have become pervasive in the commercial world, coupled with the increased intensity and sophistication of security-related attacks, organizations now recognize the need for a comprehensive security strategy. This strategy encompasses the use of specialized hardware and software and trained personnel to meet that need.
2. Computer security education, often termed *information security education* or *information assurance education* has emerged as a national goal in the United States and other countries, with national defense and homeland security implications. Organizations such as the Colloquium for Information System Security Education and the National Security Agency's (NSA's) Information Assurance Courseware Evaluation (IACE) Program are spearheading a government role in the development of standards for computer security education.

Accordingly, the number of courses in universities, community colleges, and other institutions in computer security and related areas is growing.

OBJECTIVES

The objective of this book is to provide an up-to-date survey of developments in computer security. Central problems that confront security designers and security administrators include defining the threats to computer and network systems, evaluating the relative risks of these threats, and developing cost-effective and user-friendly countermeasures.

The following basic themes unify the discussion:

- **Principles:** Although the scope of this book is broad, there are a number of basic principles that appear repeatedly as themes and that unify this field. Examples are issues relating to authentication and access control. The book highlights these principles and examines their application in specific areas of computer security.
- **Design approaches:** The book examines alternative approaches to meeting specific computer security requirements.
- **Standards:** Standards have come to assume an increasingly important, indeed dominant, role in this field. An understanding of the current status and future direction of technology requires a comprehensive discussion of the related standards.
- **Real-world examples:** A number of the chapters include a section that shows the practical application of that chapter's principles in a real-world environment.

INTENDED AUDIENCE

The book is intended for both an academic and a professional audience. As a textbook, it is intended as a one- or two-semester undergraduate course for computer science, computer engineering, and electrical engineering majors. It covers all the topics in *OS7 Security and Protection,* which is one of the core subject areas in the *IEEE/ACM Computer Curricula 2001,* as well as a number of other topics. The book covers the core area *IAS Information Assurance and Security in the Computer Curricula 2005 Information Technology Volume;* and *CE-OPS6 Security and Protection from the Computer Engineering Curriculum Guidelines, 2004.*

For the professional interested in this field, the book serves as a basic reference volume and is suitable for self-study.

PLAN OF THE TEXT

The book is divided into six parts (see Chapter 0):

- Computer Security Technology and Principles
- Software Security
- Management Issues
- Cryptographic Algorithms
- Internet Security
- Operating System Security

The section on OS security covers two real-world examples in detail: Linux and Windows Vista. There are also a number of appendices in the book to provide additional background. The book is also accompanied by a number of online appendices that provide more detail on selected topics.

The book includes an extensive glossary, a list of frequently used acronyms, and a bibliography. Each chapter includes homework problems, review questions, a list of key words, suggestions for further reading, and recommended Web sites.

HACKING EXERCISES

The instructor's support materials include two Web related hacking exercises: (1) Cross site scripting attacks (2) Server side SQL injection type attacks For both of the above the instructor needs a Linux system with a web server installed (Apache is freely available and could work as a web server) as well as PhP installed (again, its freely available). You simply download the files from the instructor support site and save them in the public_html directory, and unpack them for the projects to be ready to use. You would of course also need to change the permissions on the folders and the files after you unpack it but that's easy. Also included is a short step-by-step instruction manual that tells the instructor exactly what to do with this package of files in order to create the environment for the student exercises.

These projects have been used in computer security courses and have been the highlight of the courses; students felt the most excited because of them and they are very rewarding indeed.

An additional hacking exercise is included that involves attempting to reverse engineer an application-level protocol. This is a sockets programming exercise.

See Appendix C in this book for more details.

OTHER PROJECTS AND STUDENT EXERCISES

For many instructors, an important component of a computer security course is a project or set of projects by which the student gets hands-on experience to reinforce concepts from the text. This book provides an unparalleled degree of support for including a projects component in the course. The instructor's supplement not only includes guidance on how to assign and structure the projects but also includes a set of user's manuals for various project types plus specific assignments, all written especially for this book. Instructors can assign work in the following areas:

- **Programming projects:** A series of programming projects that cover a broad range of topics and that can be implemented in any suitable language on any platform
- **Research projects:** A series of research assignments that instruct the student to research a particular topic on the Internet and write a report
- **Laboratory exercises:** A series of projects that involve programming and experimenting with concepts from the book
- **Practical security assessments:** A set of exercises to examine current infrastructure and practices of an existing organization
- **Reading/report assignments:** A list of papers that can be assigned for reading and writing a report, plus suggested assignment wording
- **Writing assignments:** A list of writing assignments to facilitate learning the material

This diverse set of projects and other student exercises enables the instructor to use the book as one component in a rich and varied learning experience and to tailor a course plan to meet the specific needs of the instructor and students. See Appendix C in this book for details.

INSTRUCTIONAL SUPPORT MATERIALS

To support instructors, the following materials are provided:

- **Solutions Manual:** Solutions to end-of-chapter Review Questions and Problems
- **PowerPoint slides:** A set of slides covering all chapters, suitable for use in lecturing.
- **PDF files:** Reproductions of all figures and tables from the book
- **Projects manual:** Suggested project assignments for all of the project categories listed below

Instructors may contact their Pearson Education or Prentice Hall representative for access to these materials.

In addition, the book's Web site supports instructors with

- Links to Webs sites for other courses being taught using this book
- Sign-up information for an Internet mailing list for instructors

INTERNET SERVICES FOR INSTRUCTORS AND STUDENTS

There is a Web site for this book that provides support for students and instructors. The site includes links to other relevant sites. The Web page is at WilliamStallings.com/CompSec/CompSec1e.html; see Chapter 0 for more information. An Internet mailing list has been set up so that instructors using this book can exchange information, suggestions, and questions with each other and with the author. As soon as typos or other errors are discovered, an errata list for this book will be available at WilliamStallings.com.

ACKNOWLEDGMENTS

This book has benefited from review by a number of people, who gave generously of their time and expertise. The following professors and instructors reviewed all or a large part of the manuscript: James Bret Michael (Naval Postgraduate School), Scott Campbell (Miami University), Jim Alves-Foss (University of Idaho), Gregory B. White (University of Texas—San Antonio), Corey D. Shou (Idaho State University), Weining Zhang (University of Texas—San Antonio), Sreekanth Malladi (Dakota State University), Breno Fonseca De Medeiros (Florida State University), Kent E. Seamons (Brigham Young University), Krishna M. Sivalingam (University of Maryland, Baltimore County), and Alec Yasinsac (Florida State University).

Thanks also to the many people who provided detailed technical reviews of one or more chapters: Pradeep Navalkar (TechTonics Group Limited); Manish Gupta (M&T Bank Corporation, Buffalo); Scott W. DeVault (CISSP, MCP, The AEgis Technologies Group, Inc.); Arturo 'Buanzo' Busleiman (Independent Security Consultant, Buenos Aires); David Grant (MICDDS, Group Security Manager, Halcrow Group Ltd); Spike Quatrone; Jaspreet Singh (Senior Consultant, Ernst and Young, India); Jean-Charles Demarque (IT Consultant in France); Steve Fletcher; David Gillett (CISSP, CCNP, CCSE, MCSE); Robert Slade (author and prolific book reviewer); Rob J. Meijer (Dutch National Police Agency); Marc Blitz (aacompsec.com); Kevin Sanchez-Cherry (IT security and assurance specialist); Don Munro; Edward Lewis (Australian Defence Force Academy, University of New South Wales); and Jerome Athias (Independant Security Researcher).

Sreekanth Malladi of Dakota State University developed the Web hacking projects. Arnold Patton of Bradley University developed the reverse engineering hacking project.

We also thank Ricky Magalhaes of Fastennet Security, who developed a series of Windows security projects for this book.

The following people provided homework problems: Zubair Baig (Monash University); Spike Quatrone; Edward Lewis (University of New South Wales), and Rob J Meijer.

Dr Lawrie Brown would first like to thank Bill Stallings for the pleasure of working with him to produce this text. I would also like to thank my colleagues in the School of Information Technology and Electrical Engineering, University of New South Wales at the Australian Defence Force Academy in Canberra, Australia for their encouragement and support. I particularly wish to acknowledge the insightful comments and critiques by Ed Lewis and Don Munro, who I believe have helped produce a more accurate and succinct text.

Finally, we would like to thank the many people responsible for the publication of the book, all of whom did their usual excellent job. This includes the staff at Prentice Hall, particularly my editor, Tracy Dunkelberger, her assistants, Christianna Lee and Carole Snyder, and production manager, Rose Kernan. Thanks also to Patricia M. Daly, who did the copy editing.

ABOUT THE AUTHORS

Dr. William Stallings has authored 17 titles, and counting revised editions, over 40 books on computer security, computer networking, and computer architecture. In over 20 years in the field, he has been a technical contributor, technical manager, and an executive with several high-technology firms. Currently he is an independent consultant whose clients have included computer and networking manufacturers and customers, software development firms, and leading-edge government research institutions. He has nine times received the award for the best Computer Science textbook of the year from the Text and Academic Authors Association.

He created and maintains the Computer Science Student Resource Site at WilliamStallings.com/StudentSupport.html. This site provides documents and links on a variety of subjects of general interest to computer science students (and professionals). He is a member of the editorial board of Cryptologia, a scholarly journal devoted to all aspects of cryptology.

Dr. Lawrie Brown is a senior lecturer in the School of Information Technology and Electrical Engineering, at the Australian Defence Force Academy (UNSW@ADFA) in Canberra, Australia. His professional interests include cryptography, communications and computer systems security, and most recently, the design of safe mobile code environments using the functional language Erlang. He has previously worked on the design and implementation of private key block ciphers, in particular the LOKI family of encryption algorithms. He currently teaches courses in computer security, cryptography, data communications and java programming, and conducts workshops in security risk assessment and firewall design.

Michael Howard is a senior security program manager in the Security Engineering group at Microsoft. He is an architect of the security process improvements at Microsoft and co-author of numerous security books including Writing Secure Code for Windows Vista, The Security Development Lıᴗᴗycle, 19 Deadly Sins of Software Development and the award-winning Writing Secure Code.

Michael D. (Mick) Bauer, CISSP, is Network Security Architect for a large financial services provider. He is also Security Editor for Linux Journal Magazine, and author of its monthly "Paranoid Penguin" security column. Mick's areas of expertise include Linux security and general Unix security, network (TCP/IP) security, security assessment, and the development of security policies and awareness programs. He has been a Linux system administrator and user since 1995, and a Linux writer and educator since 2000. Mick is the author of over 40 articles on Linux security, network security, and hacker culture. Many of these were incorporated into his book Linux Server Security (O'Reilly Media, 2005), the first edition of which was translated into eight languages. Mick is a frequent lecturer and presenter at information security conferences.

NOTATION

Symbol	Expression	Meaning
D, K	D(K, Y)	Symmetric decryption of ciphertext Y using secret key K
D, PR_a	D(PR_a, Y)	Asymmetric decryption of ciphertext Y using A's private key PR_a
D, PU_a	D(PU_a, Y)	Asymmetric decryption of ciphertext Y using A's public key PU_a
E, K	E(K, X)	Symmetric encryption of plaintext X using secret key K.
E, PR_a	E(PR_a, X)	Asymmetric encryption of plaintext X using A's private key PR_a
E, PU_a	E(PU_a, X)	Asymmetric encryption of plaintext X using A's public key PU_a
K		Secret key
PR_a		Private key of user A
PU_a		Public key of user A
H	H(X)	Hash function of message X
		Logical OR: x OR y
•	$x \bullet y$	Logical AND: x AND y
~	$\sim x$	Logical NOT: NOT x
C		A characteristic formula, consisting of a logical formula over the values of attributes in a database
X	$X(C)$	Query set of C, the set of records satisfying C
|, X	$\|X(C)\|$	Magnitude of $X(C)$: the number of records in $X(C)$
∩	$X(C) \cap X(D)$	Set intersection: the number of records in both $X(C)$ and $X(D)$
||	$x \| y$	x concatenated with y

Acronyms

3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
AH	Authentication Header
ANSI	American National Standards Institute
ATM	Automatic Teller Machine
CBC	Cipher Block Chaining
CC	Common Criteria
CFB	Cipher Feedback
CMAC	Cipher-Based Message Authentication Code
DAC	Discretionary Access Control
DBMS	Database Management System
DDoS	Distributed Denial of Service
DES	Data Encryption Standard
DMZ	Demilitarized Zone
DoS	Denial of Service
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
ECB	Electronic Codebook
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standard
IAB	Internet Architecture Board
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPSec	IP Security
ISO	International Organization for Standardization
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
IV	Initialization Vector
KDC	Key Distribution Center
MAC	Mandatory Access Control
MAC	Message Authentication Code
MIC	Message Integrity Code
MIME	Multipurpose Internet Mail Extension
MLS	Multilevel Security
MTU	Maximum Transmission Unit
NIDA	Network-Based IDS
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OFB	Output Feedback
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PRNG	Pseudorandom Number Generator
RDBMS	Relational Database Management System
RBAC	Role-Based Access Control
RFC	Request for Comments
RNG	Random Number Generator
RSA	Rivest-Shamir-Adelman
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
S/MIME	Secure MIME
SQL	Structured Query Language
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS.	Transport Layer Security
TPM	Trusted Platform Module
UDP	User Datagram Protocol
VPN	Virtual Private Network

CONTENTS