COMPUTER SECURITY:
PRINCIPLES AND PRACTICE

William Stallings

Lawrie Brown
University of New South Wales, Australian Defence Force Academy

With Contributions by

Mick Bauer
Security Editor, Linux Journal
Dir. of Value-Subtracted Svcs., Wiremonkeys.org

Michael Howard
Principal Security Program Manager, Microsoft Corporation

PEARSON
Prentice
Hall

Upper Saddle River, New Jersey 07458

Library of Congress Cataloging-in-Publication Data on File

Vice President and Editorial Director, ECS: *Marcia J. Horton*
Executive Editor: *Tracy Dunkelberger*
Assistant Editor: *Carole Snyder*
Editorial Assistants: *Christianna Lee and ReeAnne Davis*
Managing Editor: *Camille Trentacoste*
Production Editor: *Rose Kernan*
Director of Creative Services: *Paul Belfanti*
Creative Director: *Juan Lopez*
Cover Designer: *Kenny Beck*
Managing Editor, AV Management and Production: *Patricia Burns*
Art Editor: *Gregory Dulles*
Director, Imange Resouce Center: *Melinda Reo*
Manager, Rights and Permissions: *Zina Arabia*
Manager, Visual Research: *Beth Brenzel*
Manager, Cover Visual Research and Permissions: *Karen Sanatar*
Manufacturing Manager, ESM: *Alexis Heydt-Long*
Manufacturing Buyer: *Lisa McDowell*
Marketing Manager: *Mack Patterson*

Pearson Prentice Hall
Pearson Education, Inc.
Upper Saddle River, NJ 07458

The author and publisher of this book have used their best efforts in preparing this book. These efforts include the development, research, and testing of the theories and programs to determine their effectiveness. The author and publisher make no warranty of any kind, expressed or implied, with regard to these programs or the documentation contained in this book. The author and publisher shall not be liable in any event for incidental or consequential damages in connection with, or arising out of, the furnishing, performance, or use of these programs.

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

ISBN: 0-13-600424-5
978-0-13-600424-0

Pearson Education Ltd., *London*
Pearson Education Australia Pty. Ltd., *Sydney*
Pearson Education Singapore, Pte. Ltd.
Pearson Education North Asia Ltd., *Hong Kong*
Pearson Education Canada, Inc., *Toronto*
Pearson Educación de Mexico, S.A. de C.V.
Pearson Education—Japan, *Tokyo*
Pearson Education Malaysia, Pte. Ltd.
Pearson Education, Inc., *Upper Saddle River, New Jersey*

For my loving wife, A. T. S.

—WS

To my extended family, who helped
make this all possible

—LB

CONTENTS

ONLINE APPENDICES

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
$\bullet$	$x \bullet y$	Logical AND: x AND y
~	~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 $X(C)$
$\cap$	$X(C) \cap X(D)$	Set intersection: the number of records in both $X(C)$ and $X(D)$
$\|\|$	$x \,\|\|\, y$	x concatenated with y

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 Lifecycle, 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.

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.