

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



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, Image Resource 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*



© 2008 Pearson Education, Inc.
Pearson Prentice Hall
Pearson Education, Inc.
Upper Saddle River, NJ 07458

All rights reserved. No part of this book may be reproduced in any form or by any means, without permission in writing from the publisher.

Pearson Prentice Hall™ is a trademark of Pearson Education, Inc.
All other trademarks or product names are the property of their respective owners.

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

Notation xii

About the Authors xiii

Preface xv

Chapter 0 Reader's and Instructor's Guide 1

- 0.1 Outline of the Book 2
- 0.2 A Roadmap for Readers and Instructors 3
- 0.3 Internet and Web Resources 3
- 0.4 Standards 5

Chapter 1 Overview 6

- 1.1 Computer Security Concepts 7
 - 1.2 Threats, Attacks, and Assets 14
 - 1.3 Security Functional Requirements 20
 - 1.4 A Security Architecture for Open Systems 22
 - 1.5 The Scope of Computer Security 27
 - 1.6 Computer Security Trends 28
 - 1.7 Computer Security Strategy 32
 - 1.8 Recommended Reading and Web Sites 34
 - 1.9 Key Terms, Review Questions, and Problems 36
- Appendix:1A Significant Security Standards and Documents 37

PART ONE COMPUTER SECURITY TECHNOLOGY AND PRINCIPLES 40

Chapter 2 Cryptographic Tools 41

- 2.1 Confidentiality with Symmetric Encryption 42
- 2.2 Message Authentication and Hash Functions 49
- 2.3 Public-Key Encryption 56
- 2.4 Digital Signatures and Key Management 61
- 2.5 Random and Pseudorandom Numbers 65
- 2.6 Practical Application: Encryption of Stored Data 67
- 2.7 Recommended Reading and Web Sites 68
- 2.8 Key Terms, Review Questions, and Problems 69

Chapter 3 User Authentication 74

- 3.1 Means of Authentication 75
- 3.2 Password-Based Authentication 76
- 3.3 Token-Based Authentication 88
- 3.4 Biometric Authentication 92
- 3.5 Remote User Authentication 97
- 3.6 Security Issues for User Authentication 99
- 3.7 Practical Application: An Iris Biometric System 101

3.8	Case Study: Security Problems for ATM Systems	103
3.9	Recommended Reading and Web Sites	106
3.10	Key Terms, Review Questions, and Problems	107
Chapter 4	Access Control	110
4.1	Access Control Principles	111
4.2	Subjects, Objects, and Access Rights	115
4.3	Discretionary Access Control	116
4.4	Example: UNIX File Access Control	122
4.5	Role-Based Access Control	125
4.6	Case Study: RBAC System for a Bank	134
4.7	Recommended Reading and Web Sites	137
4.8	Key Terms, Review Questions, and Problems	138
Chapter 5	Database Security	142
5.1	Database Management Systems	143
5.2	Relational Databases	144
5.3	Database Access Control	148
5.4	Inference	153
5.5	Statistical Databases	156
5.6	Database Encryption	166
5.7	Recommended Reading	170
5.8	Key Terms, Review Questions, and Problems	171
Chapter 6	Intrusion Detection	176
6.1	Intruders	177
6.2	Intrusion Detection	181
6.3	Host-Based Intrusion Detection	183
6.4	Distributed Host-Based Intrusion Detection	190
6.5	Network-Based Intrusion Detection	193
6.6	Distributed Adaptive Intrusion Detection	197
6.7	Intrusion Detection Exchange Format	200
6.8	Honeypots	202
6.9	Example System: Snort	204
6.10	Recommended Reading and Web Sites	208
6.11	Key Terms, Review Questions, and Problems	209
	Appendix 6A: The Base-Rate Fallacy	211
Chapter 7	Malicious Software	215
7.1	Types of Malicious Software	216
7.2	Viruses	220
7.3	Virus Countermeasures	226
7.4	Worms	231
7.5	Bots	240
7.6	Rootkits	242
7.7	Recommended Reading and Web Sites	245
7.8	Key Terms, Review Questions, and Problems	246

Chapter 8 Denial of Service 249

- 8.1 Denial of Service Attacks 250
- 8.2 Flooding Attacks 257
- 8.3 Distributed Denial of Service Attacks 259
- 8.4 Reflector and Amplifier Attacks 261
- 8.5 Defenses Against Denial of Service Attacks 265
- 8.6 Responding to a Denial of Service Attack 269
- 8.7 Recommended Reading and Web Sites 270
- 8.8 Key Terms, Review Questions, and Problems 271

Chapter 9 Firewalls and Intrusion Prevention Systems 273

- 9.1 The Need for Firewalls 274
- 9.2 Firewall Characteristics 275
- 9.3 Types of Firewalls 276
- 9.4 Firewall Basing 283
- 9.5 Firewall Location and Configurations 286
- 9.6 Intrusion Prevention Systems 291
- 9.7 Example: Unified Threat Management Products 294
- 9.8 Recommended Reading and Web Sites 298
- 9.9 Key Terms, Review Questions, and Problems 299

Chapter 10 Trusted Computing and Multilevel Security 303

- 10.1 The Bell-LaPadula Model for Computer Security 304
- 10.2 Other Formal Models for Computer Security 314
- 10.3 The Concept of Trusted Systems 320
- 10.4 Application of Multilevel Security 323
- 10.5 Trusted Computing and the Trusted Platform Module 330
- 10.6 Common Criteria for Information Technology Security Evaluation 334
- 10.7 Assurance and Evaluation 340
- 10.8 Recommended Reading and Web Sites 345
- 10.9 Key Terms, Review Questions, and Problems 346

PART TWO SOFTWARE SECURITY 349**Chapter 11 Buffer Overflow 350**

- 11.1 Stack Overflows 352
- 11.2 Defending Against Buffer Overflows 373
- 11.3 Other Forms of Overflow Attacks 379
- 11.4 Recommended Reading and Web Sites 385
- 11.5 Key Terms, Review Questions, and Problems 386

Chapter 12 Other Software Security Issues 388

- 12.1 Software Security Issues 389
- 12.2 Handling Program Input 392
- 12.3 Writing Safe Program Code 403
- 12.4 Interacting with the Operating System and Other Programs 408
- 12.5 Handling Program Input 419
- 12.6 Recommended Reading and Web Sites 422
- 12.7 Key Terms, Review Questions, and Problems 423

PART THREE MANAGEMENT ISSUES 426

Chapter 13 Physical and Infrastructure Security 427

- 13.1 Overview 428
- 13.2 Physical Security Threats 429
- 13.3 Physical Security Prevention and Mitigation Measures 435
- 13.4 Recovery from Physical Security Breaches 438
- 13.5 Threat Assessment, Planning, and Plan Implementation 439
- 13.6 Example: A Corporate Physical Security Policy 440
- 13.7 Integration of Physical and Logical Security 441
- 13.8 Recommended Reading and Web Sites 446
- 13.9 Key Terms, Review Questions, and Problems 447

Chapter 14 Human Factors 449

- 14.1 Security Awareness, Training, and Education 450
- 14.2 Organizational Security Policy 455
- 14.3 Employment Practices and Policies 461
- 14.4 E-Mail and Internet Use Policies 464
- 14.5 Example: A Corporate Security Policy Document 465
- 14.6 Recommended Reading and Web Sites 467
- 14.7 Key Terms, Review Questions, and Problems 468
 - Appendix 14A: Security Awareness Standard of Good Practice 469
 - Appendix 14B: Security Policy Standard of Good Practice 473

Chapter 15 Security Auditing 475

- 15.1 Security Auditing Architecture 476
- 15.2 The Security Audit Trail 481
- 15.3 Implementing the Logging Function 486
- 15.4 Audit Trail Analysis 497
- 15.5 Example: An Integrated Approach 501
- 15.6 Recommended Reading and Web Sites 504
- 15.7 Key Terms, Review Questions, and Problems 505

Chapter 16 IT Security Management and Risk Assessment 508

- 16.1 IT Security Management 509
- 16.2 Organizational Context and Security Policy 512
- 16.3 Security Risk Assessment 515
- 16.4 Detailed Security Risk Analysis 518
- 16.5 Case Study: Silver Star Mines 530
- 16.6 Recommended Reading and Web Sites 534
- 16.7 Key Terms, Review Questions, and Problems 536

Chapter 17 IT Security Controls, Plans and Procedures 538

- 17.1 IT Security Management Implementation 539
- 17.2 Security Controls or Safeguards 539
- 17.3 IT Security Plan 547
- 17.4 Implementation of Controls 548
- 17.5 Implementation Followup 550
- 17.6 Case Study: Silver Star Mines 556

17.7	Recommended Reading 559
17.8	Key Terms, Review Questions, and Problems 559
Chapter 18	Legal and Ethical Aspects 562
18.1	Cybercrime and Computer Crime 563
18.2	Intellectual Property 567
18.3	Privacy 574
18.4	Ethical Issues 580
18.5	Recommended Reading and Web Sites 586
18.6	Key Terms, Review Questions, and Problems 587
	Appendix 18A: Information Privacy Standard of Good Practice 590
PART FOUR CRYPTOGRAPHIC ALGORITHMS 592	
Chapter 19	Symmetric Encryption and Message Confidentiality 593
19.1	Symmetric Encryption and Message Confidentiality 594
19.2	Data Encryption Standard 598
19.3	Advanced Encryption Standard 600
19.4	Stream Ciphers and RC4 607
19.5	Cipher Block Modes of Operation 610
19.6	Location of Symmetric Encryption Devices 616
19.7	Key Distribution 618
19.8	Recommended Reading and Web Sites 620
19.9	Key Terms, Review Questions, and Problems 620
Chapter 20	Public-Key Cryptography and Message Authentication 625
20.1	Secure Hash Functions 626
20.2	HMAC 632
20.3	The RSA Public-Key Encryption Algorithm 635
20.4	Diffie-Hellman and Other Asymmetric Algorithms 641
20.5	Recommended Reading and Web Sites 646
20.6	Key Terms, Review Questions, and Problems 646
PART FIVE INTERNET SECURITY 650	
Chapter 21	Internet Security Protocols and Standards 651
21.1	Secure Sockets Layer (SSL) and Transport Layer Security (TLS) 652
21.2	IPv4 and IPv6 Security 656
21.3	Secure Email and S/MIME 662
21.4	Recommended Reading and Web Sites 665
21.5	Key Terms, Review Questions, and Problems 666
	Appendix 21A: Radix-64 Conversion 668
Chapter 22	Internet Authentication Applications 671
22.1	Kerberos 672
22.2	X.509 678
22.3	Public-Key Infrastructure 680
22.4	Federated Identity Management 683
22.5	Recommended Reading and Web Sites 687
22.6	Key Terms, Review Questions, and Problems 688

PART SIX OPERATING SYSTEM SECURITY 689

Chapter 23 Linux Security 690

- 23.1 Introduction 691
- 23.2 Linux's Security Model 691
- 23.3 The Linux DAC in Depth: Filesystem Security 693
- 23.4 Linux Vulnerabilities 699
- 23.5 Linux System Hardening 701
- 23.6 Application Security 709
- 23.7 Mandatory Access Controls 711
- 23.8 Recommended Reading and Web Sites 711
- 23.9 Key Terms, Review Questions, and Problems 718

Chapter 24 Windows and Windows Vista Security 720

- 24.1 Windows Security Architecture 721
- 24.2 Windows Vulnerabilities 728
- 24.3 Windows Security Defenses 729
- 24.4 Browser Defenses 737
- 24.5 Cryptographic Services 737
- 24.6 Common Criteria 738
- 24.7 Recommended Reading and Web Sites 739
- 24.8 Key Terms, Review Questions, Problems, and Projects 740

APPENDICES

Appendix A Some Aspects of Number Theory 742

- A.1 Prime and Relatively Prime Numbers 743
- A.2 Modular Arithmetic 744
- A.3 Fermat's and Euler's Theorems 746

Appendix B Random and Pseudorandom Number Generation 750

- B.1 The Use of Random Numbers 751
- B.2 Pseudorandom Number Generators (PRNGs) 752
- B.3 True Random Number Generators 757

Appendix C Projects for Teaching Computer Security 759

- C.1 Research Projects 760
- C.2 Hacking Projects 761
- C.3 Programming Projects 761
- C.4 Laboratory Exercises 762
- C.5 Practical Security Assessments 762
- C.6 Writing Assignments 762
- C.7 Reading/Report Assignments 763

References 765

Index 783

ONLINE APPENDICES**Appendix D Standards and Standard-Setting Organizations**

- D.1** The Importance of Standards
- D.2** Internet Standards and the Internet Society
- D.3** National Institute of Standards and Technology
- D.4** The International Telecommunication Union
- D.5** The International Organization for Standardization

Appendix E TCP/IP Protocol Architecture

- E.1** TCP/IP Layers
- E.2** TCP and UDP
- E.3** Operation of TCP/IP
- E.4** TCP/IP Applications

Appendix F Glossary

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
\sim	$\sim x$	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 $X(C)$
\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 (aacompssec.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 (Independent 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.