COMPUTER SECURITY

PRINCIPLES AND PRACTICE

SECOND EDITION

William Stallings | Lawrie Brown

COMPUTER SECURITY
PRINCIPLES AND PRACTICE

Second Edition

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
Principle Security Program Manager, Microsoft Corporation

PEARSON

Boston Columbus Indianapolis New York San Francisco Upper Saddle River
Amsterdam Cape Town Dubai London Madrid Milan Munich Paris Montreal Toronto
Delhi Mexico City Sao Paulo Sydney Hong Kong Seoul Singapore Taipei Tokyo

Editorial Director, ECS: Marcia Horton
Editor-in-Chief: Michael Hirsch
Acquisitions Editor: Tracy Dunkelberger
Associate Editor: Carole Snyder
Editorial Assistant: Stephanie Sellinger
Vice President, Marketing: Patrice Jones
Marketing Manager: Yezan Alayan
Marketing Coordinator: Kathryn Ferranti
Marketing Assistant: Emma Snider
Vice President, Production: Vince O'Brien
Managing Editor: Jeff Holcomb
Production Project Manager: Kayla Smith-Tarbox
Senior Operations Supervisor: Alan Fischer
Manufacturing Buyer: Lisa McDowell
Art Director: Anthony Gemmellaro/Jayne Conte
Cover Designer: Bruce Kenselaar
Cover Image: Bodiam Castle © Lance Bellers
Media Editor: Daniel Sandin
Full-Service Project Management: Integra
Composition: Integra
Printer/Binder: Courier/Westford
Cover Printer: Lehigh-Phoenix Color/ Hagerstown
Text Font: Times Roman, 10/12

Credits and acknowledgments borrowed from other sources and reproduced, with permission, in this textbook appear on the appropriate page within text on page 787.

Library of Congress Cataloging-in-Publication Data
Stallings, William.
Computer security : principles and practice / William Stallings, Lawrie Brown.—2nd ed.
p. cm.
ISBN-13: 978-0-13-277506-9 (alk. paper)
ISBN-10: 0-13-277506-9 (alk. paper)
1. Computer security. 2. Computer security—Examinations—Study guides.
3. Computer networks—Security measures—Examinations—Study guides. 4. Electronic data processing personnel—Certification—Study guides. I. Brown, Lawrie. II. Title.
QA76.9.A25S685 2012
005.8—dc23

2011029651

15 14 13 12 11—CW—10 9 8 7 6 5 4 3 2 1

PEARSON

ISBN-10: 0-13-277506-9
ISBN-13: 978-0-13-277506-9

For my loving wife, A. T. S.

—WS

To my extended family, who helped
make this all possible

—LB

This page intentionally left blank

CONTENTS

APPENDICES

ONLINE CHAPTERS AND APPENDICES[1]

[1] Online chapters, appendices, and other documents are Premium Content, available via the access card at the front of this book.

Online Resources

Site	Location	Description
Companion Website	WilliamStallings.com/Computer Security	*Student Resources* link: Useful links and documents for students. *Instructor Resources* links: Useful links and documents for instructors.
Premium Content	Click on *Premium Content* link at Companion Website or at pearson highered.com/stallings and enter the student access code found on the card in the front of the book.	Online chapters, appendices, and other documents that supplement the book.
Instructor Resource Center (IRC)	Click on *Pearson Resources for Instructors* link at Companion Website or on *Instructor Resource* link at pearsonhighered.com/stallings.	Solutions manual, projects manual, slides, and other useful documents
Computer Science Student Resource Site	ComputerScienceStudent.com	Useful links and documents for computer science students.

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
$+$	$x + y$	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
$\vert$, X	$\vert X(C) \vert$	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 $X(D)$
$\Vert$	$x \Vert y$	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 include 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 Computer ScienceStudent.com. 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.

PREFACE

WHAT'S NEW IN THE SECOND EDITION

In the four and a half years since the first edition of this book was published, the field has seen continued innovations and improvements. In this new edition, we try to capture these changes while maintaining a broad and comprehensive coverage of the entire field. To begin the process of revision, the first edition of this book was extensively reviewed by a number of professors who teach the subject and by professionals working in the field. The result is that in many places the narrative has been clarified and tightened, and illustrations have been improved.

One obvious change to the book is a revision in the organization, which makes for a clearer presentation of related topics. There is a new chapter on operating system security and a new chapter on wireless security. The material in Part Three has been reallocated to chapters in a way that presents it more systematically.

Beyond these refinements to improve pedagogy and user-friendliness, there have been major substantive changes throughout the book. Highlights include:

- **Operating system security:** This chapter reflects the focus in NIST SP800-123. The chapter also covers the important topic of virtual machine security.
- **Cloud security:** A new section covers the security issues relating to the exciting new area of cloud computing.
- **Application-based denial-of-service attacks:** A new section deals with this prevalent form of DoS attack.
- **Malicious software:** This chapter provides a different focus than that of the first edition. Increasingly, we see backdoor/rootkit type malware installed by social engineering attacks, rather than more classic virus/worm direct infection. And phishing is even more prominent than ever. These trends are reflected in the coverage.
- **Internet security protocol and standards:** This chapter has been expanded to include two additional important protocols and services: HTTPS and DKIM.
- **Wireless security:** A new chapter on wireless security has been added.
- **Computer security incident response:** The section on CSIR has been updated and expanded.
- **Student study aid:** Each chapter now begins with a list of learning objectives.
- **Sample syllabus:** The text contains more material than can be conveniently covered in one semester. Accordingly, instructors are provided with several sample syllabi that guide the use of the text within limited time (e.g., 16 weeks or 12 weeks). These samples are based on real-world experience by professors with the first edition.
- **Practice problem set:** A set of homework problems, plus solutions, is provided for student use.
- **Test bank:** A set of review questions, including yes/no, multiple choice, and fill in the blank, is provided for each chapter.

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) 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 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 *OS Security and Protection*, which is one of the core subject areas in the *IEEE/ACM Computer Curriculum 2008: An Interim Revision to CS 2001*, as well as a number of other topics. The book covers the core area *IAS Information Assurance and Security* in the *IEEE/ACM Curriculum Guidelines for Undergraduate Degree Programs in Information Technology 2008*; and *CE-OPS6 Security and Protection* from the *IEEE/ACM 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 five parts (see Chapter 0):

- Computer Security Technology and Principles
- Software Security and Trusted Systems
- Management Issues
- Cryptographic Algorithms
- Network Security

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 Websites.

COVERAGE OF CISSP SUBJECT AREAS

This book provides coverage of all the subject areas specified for CISSP (Certified Information Systems Security Professional) certification. The CISSP designation from the International Information Systems Security Certification Consortium (ISC)^2 is often referred to as the "gold standard" when it comes to information security certification. It is the only universally recognized certification in the security industry. Many organizations, including the U.S. Department of Defense and many financial institutions, now require that cyber security personnel have the CISSP certification. In 2004, CISSP became the first IT program to earn accreditation under the international standard ISO/IEC 17024 (*General Requirements for Bodies Operating Certification of Persons*).

The CISSP examination is based on the Common Body of Knowledge (CBK), a compendium of information security best practices developed and maintained by (ISC)^2, a nonprofit organization. The CBK is made up of 10 domains that comprise the body of knowledge that is required for CISSP certification. See Chapter 0 for details of this book's coverage of CBK.

STUDENT RESOURCES

For this new edition, a tremendous amount of original supporting material for students has been made available online, at two Web locations. The **Companion Website**, at William Stallings.com/ComputerSecurity (click on Student Resources link), includes a list of relevant links organized by chapter and an errata sheet for the book.

Purchasing this textbook new grants the reader six months of access to the **Premium Content Site**, which includes the following materials:

- **Online chapters:** To limit the size and cost of the book, two chapters of the book are provided in PDF format. The chapters are listed in this book's table of contents.
- **Online appendices:** There are numerous interesting topics that support material found in the text but whose inclusion is not warranted in the printed text. A total of nine appendices cover these topics for the interested student. The appendices are listed in this book's table of contents.
- **Homework problems and solutions:** To aid the student in understanding the material, a separate set of homework problems with solutions are available. These enable the students to test their understanding of the text.
- **Key papers:** Several dozen papers from the professional literature, many hard to find, are provided for further reading.
- **Supporting documents:** A variety of other useful documents are referenced in the text and provided online.

INSTRUCTOR SUPPORT MATERIALS

Support materials for instructors are available at the **Instructor Resource Center (IRC)** for this textbook, which can be reached through the Publisher's Web site www.pearsonhighered.com/stallings or by clicking on the link labeled "Pearson Resources for Instructor" at this book's Companion Website at WilliamStallings.com/ComputerSecurity. To gain access to the IRC, please contact your local Pearson sales representative via pearsonhighered.com/educator/replocator/requestSalesRep.page or call Pearson Faculty Services at 1-800-526-0485. The IRC provides the following materials:

- **Projects manual:** Project resources including documents and portable software, plus suggested project assignments for all of the project categories listed in the following section.
- **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
- **Test bank:** A chapter-by-chapter set of questions.

- **Sample syllabuses:** The text contains more material than can be conveniently covered in one semester. Accordingly, instructors are provided with several sample syllabuses that guide the use of the text within limited time. These samples are based on real-world experience by professors with the first edition.

The **Companion Website**, at WilliamStallings.com/ComputerSecurity (click on Instructor Resources link), includes the following:

- Links to Web sites for other courses being taught using this book
- Sign-up information for an Internet mailing list for instructors using this book to exchange information, suggestions, and questions with each other and with the author

PROJECTS AND OTHER 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 support materials available through Prentice Hall 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:

- **Hacking exercises**: Two projects that enable students to gain an understanding of the issues in intrusion detection and prevention.
- **Laboratory exercises:** A series of projects that involve programming and experimenting with concepts from the book.
- **Research projects:** A series of research assignments that instruct the student to research a particular topic on the Internet and write a report.
- **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.
- **Practical security assessments:** A set of exercises to examine current infrastructure and practices of an existing organization.
- **Firewall projects:** A portable network firewall visualization simulator is provided, together with exercises for teaching the fundamentals of firewalls.
- **Case studies:** A set of real-world case studies, including learning objectives, case description, and a series of case discussion questions.
- **Writing assignments:** A list of writing assignments to facilitate learning the material.
- **Reading/report assignments:** A list of papers that can be assigned for reading and writing a report, plus suggested assignment wording.

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 A in this book for details.

ACKNOWLEDGMENTS

This new edition 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: Bob Brown (Southern Polytechnic State University), Leming Zhou (University of Pittsburgh), Yosef Sherif (Mihaylo College of Business and Economics), Nazrul Islam (Farmingdale State University), Qinghai Gao (Farmingdale State University), Wei Li (Nova Southeastern University), Jeffrey Kane (Nova Southeastern University), Philip John Lunsford II (East Carolina University), Jeffrey H. Peden (Longwood University), Ratan Guha (University of Central Florida), Sven Dietrich (Stevens Institute of Technology), and David Liu (Purdue University, Fort Wayne).

Thanks also to the many people who provided detailed technical reviews of one or more chapters: Paymon Yamini Sharif, Umair Manzoor (UmZ), Adewumi Olatunji (FAG-OSI Systems, Nigeria), Rob Meijer, Robin Goodchil, Greg Barnes (Inviolate Security LLC), Arturo Busleiman (Buanzo Consulting), Ryan M. Speers (Dartmouth College), Wynand van Staden (School of Computing, University of South Africa), Oh Sieng Chye, Michael Gromek, Samuel Weisberger, Brian Smithson (Ricoh Americas Corp, CISSP), Josef B. Weiss (CISSP), Robbert-Frank Ludwig (Veenendaal, ActStamp Information Security), William Perry, Daniela Zamfiroiu (CISSP), Rodrigo Ristow Branco, George Chetcuti (Technical Editor, TechGenix), Thomas Johnson (Director of Information Security at a banking holding company in Chicago, CISSP), Robert Yanus (CISSP), Rajiv Dasmohapatra (Wipro Ltd), Dirk Kotze, Ya'akov Yehudi, Stanley Wine (Adjunct Lecturer, Computer Information Systems Department, Zicklin School of Business, Baruch College).

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 our editor Tracy Dunkelberger, her assistant Carole Snyder, and production manager Kayla Smith-Tarbox. We also thank Shiny Rajesh and the production staff at Integra for another excellent and rapid job. Thanks also to the marketing and sales staffs at Pearson, without whose efforts this book would not be in your hands.

CHAPTER 0

READER'S AND INSTRUCTOR'S GUIDE

This book, with its accompanying Web site, covers a lot of material. Here we give the reader an overview.

0.1 OUTLINE OF THIS BOOK

Following an introductory chapter, Chapter 1, the book is organized into five parts:

Part One: Computer Security Technology and Principles: This part covers technical areas that must underpin any effective security strategy. Chapter 2 lists the key cryptographic algorithms, discusses their use, and discusses issues of strength. The remaining chapters in this part look at specific technical areas of computer security: authentication, access control, database security, malicious software, denial of service, intrusion detection, and firewalls.

Part Two: Software Security and Trusted Systems: This part covers issues concerning software development and implementation, including operating systems, utilities, and applications. Chapter 10 covers the perennial issue of buffer overflow, while Chapter 11 examines a number of other software security issues. Chapter 12 takes an overall look at operating system security. The final chapter in this part deals with trusted computing and multilevel security, which are both software and hardware issues.

Part Three: Management Issues: This part is concerned with management aspects of information and computer security. Chapters 14 and 15 focus specifically on management practices related to risk assessment, the setting up of security controls, and plans and procedures for managing computer security. Chapter 16 looks at physical security measures that must complement the technical security measures of Part One. Chapter 17 examines a wide range of human factors issues that relate to computer security. A vital management tool is security auditing, examined in Chapter 18. Finally, Chapter 19 examines legal and ethical aspects of computer security.

Part Four: Cryptographic Algorithms: Many of the technical measures that support computer security rely heavily on encryption and other types of cryptographic algorithms. Part Four is a technical survey of such algorithms.

Part Five: Internet Security: This part looks at the protocols and standards used to provide security for communications across the Internet. Chapter 22 discusses some of the most important security protocols for use over the Internet. Chapter 23 looks at various protocols and standards related to authentication over the Internet. Chapter 24 examines important aspects of wireless security.

A number of online appendices cover additional topics relevant to the book.

0.2 A ROADMAP FOR READERS AND INSTRUCTORS

This book covers a lot of material. For the instructor or reader who wishes a shorter treatment, there are a number of alternatives.

To thoroughly cover the material in the first two parts, the chapters should be read in sequence. If a shorter treatment in **Part One** is desired, the reader may choose to skip Chapter 5 (Database Security).

Although **Part Two** covers software security, it should be of interest to users as well as system developers. However, it is more immediately relevant to the latter category. Chapter 13 (Trusted Computing and Multilevel Security) may be considered optional.

The chapters in **Part Three** are relatively independent of one another, with the exception of Chapters 14 (IT Security Management and Risk Assessment) and 15 (IT Security Controls, Plans, and Procedures). The chapters can be read in any order and the reader or instructor may choose to select only some of the chapters.

Part Four provides technical detail on cryptographic algorithms for the interested reader.

Part Five covers Internet security and can be read at any point after Part One.

0.3 SUPPORT FOR CISSP CERTIFICATION

This book provides coverage of all the subject areas specified for CISSP (Certified Information Systems Security Professional) certification.

As employers have come to depend on in-house staff to manage and develop security policies and technologies, and to evaluate and manage outside security services and products, there is a need for methods for evaluating candidates. Increasingly, employers are turning to certification as a tool for guaranteeing that a potential employee has the required level of knowledge in a range of security areas.

The international standard ISO/IEC 17024 (*General Requirements for Bodies Operating Certification of Persons*) defines the following terms related to certification:

- **Certification process:** All activities by which a certification body establishes that a person fulfils specified competence requirements.
- **Certification scheme:** Specific certification requirements related to specified categories of persons to which the same particular standards and rules, and the same procedures apply.
- **Competence:** Demonstrated ability to apply knowledge and/or skills and, where relevant, demonstrated personal attributes, as defined in the certification scheme.

The CISSP designation from the International Information Systems Security Certification Consortium (ISC)^1, a nonprofit organization, is often referred to as the "gold standard" when it comes to information security certification. It is the only universally recognized certification in the security industry [SAVA03]. Many organizations, including the U.S. Department of Defense and many financial institutions, now require that cyber security personnel have the CISSP certification [DENN11]. In 2004, CISSP became the first IT program to earn accreditation under ISO/IEC 17024.

The CISSP examination is based on the Common Body of Knowledge (CBK), a compendium of information security best practices developed and maintained by (ISC)^1. The CBK is made up of 10 domains that comprise the body of knowledge that is required for CISSP certification. Table 0.1 shows the support for the CISSP body of knowledge provided in this textbook.

Table 0.1 Coverage of CISSP Domains

CISSP Domain	Key Topics in Domain	Chapter Coverage
Access Control	• Identification, authentication, and authorization technologies • Discretionary versus mandatory access control models • Rule-based and role-based access control	4—Access Control
Application Development Security	• Software development models • Database models • Relational database components	5—Database Security 10—Buffer Overflow 11—Software Security
Business Continuity and Disaster Recovery Planning	• Planning • Roles and responsibilities • Liability and due care issues • Business impact analysis	16—Physical and Infrastructure Security 17—Human Resources Security
Cryptography	• Block and stream ciphers • Explanation and uses of symmetric algorithms • Explanation and uses of asymmetric algorithms	2—Cryptographic Tools 20—Symmetric Encryption and Message Confidentiality 21—Public-Key Cryptography and Message Authentication
Information Security Governance and Risk Management	• Types of security controls • Security policies, standards, procedures, and guidelines • Risk management and analysis	14—IT Security Management and Risk Assessment 15—IT Security Controls, Plans, and Procedures
Legal, Regulations, Investigations and Compliance	• Privacy laws and concerns • Computer crime investigation • Types of evidence	19—Legal and Ethical Aspects
Operations Security	• Operations department responsibilities • Personnel and roles • Media library and resource protection	15—IT Security Controls, Plans, and Procedures 17—Human Resources Security 18—Security Auditing
Physical (Environmental) Security	• Facility location and construction issues • Physical vulnerabilities and threats • Perimeter protection	16—Physical and Infrastructure Security
Security Architecture and Design	• Critical components • Access control models • Certification and accreditation	13—Trusted Computing and Multilevel Security
Telecommunications and Network Security	• TCP/IP protocol suite • LAN, MAN, and WAN technologies • Firewall types and architectures	Appendix F—TCP/IP Protocol Architecture 22—Internet Security Protocols and Standards 24—Wireless Network Security

The 10 domains are as follows:

- **Access control:** A collection of mechanisms that work together to create a security architecture to protect the assets of the information system.
- **Application development security:** Addresses the important security concepts that apply to application software development. It outlines the environment where software is designed and developed and explains the critical role software plays in providing information system security.
- **Business continuity and disaster recovery planning:** For the preservation and recovery of business operations in the event of outages.
- **Cryptography:** The principles, means, and methods of disguising information to ensure its integrity, confidentiality, and authenticity.
- **Information security governance and risk management:** The identification of an organization's information assets and the development, documentation, and implementation of policies, standards, procedures, and guidelines. Management tools such as data classification and risk assessment/analysis are used to identify threats, classify assets, and to rate system vulnerabilities so that effective controls can be implemented.
- **Legal, regulations, investigations and compliance:** Computer crime laws and regulations. The measures and technologies used to investigate computer crime incidents.
- **Operations security:** Used to identify the controls over hardware, media, and the operators and administrators with access privileges to any of these resources. Audit and monitoring are the mechanisms, tools, and facilities that permit the identification of security events and subsequent actions to identify the key elements and report the pertinent information to the appropriate individual, group, or process.
- **Physical (environmental) security:** Provides protection techniques for the entire facility, from the outside perimeter to the inside office space, including all of the information system resources.
- **Security architecture and design:** Contains the concepts, principles, structures, and standards used to design, monitor, and secure operating systems, equipment, networks, applications, and those controls used to enforce various levels of availability, integrity, and confidentiality.
- **Telecommunications and network security:** Covers network structures; transmission methods; transport formats; security measures used to provide availability, integrity, and confidentiality; and authentication for transmissions over private and public communications networks and media.

In this book, we cover each of these domains in some depth.

0.4 INTERNET AND WEB RESOURCES

There are a number of resources available on the Internet and the Web to support this book and to help one keep up with developments in this field.

Web Sites for This Book

Three Web sites provide additional resources for students and instructors. We maintain a **Companion Web site** for this book at WilliamStallings.com/ComputerSecurity. For students, this Web site includes a list of relevant links, organized by chapter, and an errata sheet for the book. For instructors, this Web site provides links to course pages by professors teaching from this book.

There is also an access-controlled **Premium Content Web site** that provides a wealth of supporting material, including additional online chapters, additional online appendices, a set of homework problems with solutions, copies of a number of key papers in this field, and a number of other supporting documents. See the card at the front of this book for access information.

Finally, additional material for instructors is available at the **Instructor Resource Center (IRC)** for this book. See Preface for details and access information.

Computer Science Student Resource Site

William Stallings also maintains the Computer Science Student Resource Site, at ComputerScienceStudent.com. The purpose of this site is to provide documents, information, and links for computer science students and professionals. Links and documents are organized into five categories:

- **Math:** Includes a basic math refresher, a queuing analysis primer, a number system primer, and links to numerous math sites
- **How-to:** Advice and guidance for solving homework problems, writing technical reports, and preparing technical presentations
- **Research resources:** Links to important collections of papers, technical reports, and bibliographies
- **Other useful:** A variety of other useful documents and links
- **Computer science careers:** Useful links and documents for those considering a career in computer science.

Other Web Sites

There are numerous Web sites that provide information related to the topics of this book. In subsequent chapters, pointers to specific Web sites can be found in the *Recommended Reading and Web Sites* section. Because the addresses for Web sites tend to change frequently, we have not included URLs in the book. For all of the Web sites listed in the book, the appropriate link can be found at this book's Web site. Other links not mentioned in this book will be added to the Web site over time.

Online Groups

USENET NEWSGROUPS A number of USENET newsgroups are devoted to some aspect of computer security. As with virtually all USENET groups, there is a high noise-to-signal ratio, but it is worth experimenting to see if any meet your needs. The most relevant are as follows:

- **sci.crypt.research:** The best group to follow on cryptography. This is a moderated newsgroup that deals with research topics; postings must have some relationship to the technical aspects of cryptology.
- **sci.crypt:** A general discussion of cryptology and related topics.
- **alt.security:** A general discussion of security topics.
- **comp.security.misc:** A general discussion of computer security topics.
- **comp.security.firewalls:** A discussion of firewall products and technology.
- **comp.security.announce:** News and announcements from CERT (computer emergency response team).
- **comp.risks:** A discussion of risks to the public from computers and users.
- **comp.virus:** A moderated discussion of computer viruses.

FORUMS There are a number of worthwhile Web-based forums dealing with aspects of computer security. The companion Web site provides links to some of these.

0.5 STANDARDS

Many of the security techniques and applications described in this book have been specified as standards. Additionally, standards have been developed to cover management practices and the overall architecture of security mechanisms and services. Throughout this book, we describe the most important standards in use or that are being developed for various aspects of computer security. Various organizations have been involved in the development or promotion of these standards. The most important (in the current context) of these organizations are as follows:

- **National Institute of Standards and Technology:** NIST is a U.S. federal agency that deals with measurement science, standards, and technology related to U.S. government use and to the promotion of U.S. private-sector innovation. Despite its national scope, NIST Federal Information Processing Standards (FIPS) and Special Publications (SP) have a worldwide impact.
- **Internet Society:** ISOC is a professional membership society with worldwide organizational and individual membership. It provides leadership in addressing issues that confront the future of the Internet and is the organization home for the groups responsible for Internet infrastructure standards, including the Internet Engineering Task Force (IETF) and the Internet Architecture Board (IAB). These organizations develop Internet standards and related specifications, all of which are published as Requests for Comments (RFCs).
- **ITU-T:** The International Telecommunication Union (ITU) is an international organization within the United Nations System in which governments and the private sector coordinate global telecom networks and services. The ITU Telecommunication Standardization Sector (ITU-T) is one of the three sectors of the ITU. ITU-T's mission is the production of standards covering all fields of telecommunications. ITU-T standards are referred to as Recommendations.

- **ISO:** The International Organization for Standardization (ISO)[2] is a worldwide federation of national standards bodies from more than 140 countries, one from each country. ISO is a nongovernmental organization that promotes the development of standardization and related activities with a view to facilitating the international exchange of goods and services, and to developing cooperation in the spheres of intellectual, scientific, technological, and economic activity. ISO's work results in international agreements that are published as International Standards.

A more detailed discussion of these organizations is contained in Appendix C.

[2] ISO is not an acronym (in which case it would be IOS), but a word, derived from the Greek, meaning *equal*.