GLOBAL EDITION

Computer Security

Principles and Practice

THIRD EDITION

William Stallings • Lawrie Brown

ALWAYS LEARNING

PEARSON

ONLINE ACCESS

Thank you for purchasing a new copy of ***Computer Security: Principles and Practice,* Third Edition, Global Edition**. Your textbook includes twelve months of prepaid access to the book's Premium Website. This prepaid subscription provides you with full access to the following student support areas:

- Online Chapters
- Online Appendices
- Practice Problem Set with Solutions

Use a coin to scratch off the coating and reveal your student access code.
Do not use a knife or other sharp object as it may damage the code.

To access the ***Computer Security: Principles and Practice*, Third Edition, Global Edition,** Premium Website for the first time, you will need to register online using a computer with an Internet connection and a web browser. The process takes just a couple of minutes and only needs to be completed once.

1. Go to **www.pearsonglobaleditions.com/Stallings**
2. Click on **Premium Website**.
3. Click on the **Register** button.
4. On the registration page, enter your student access code* found beneath the scratch-off panel. Do not type the dashes. You can use lower- or uppercase.
5. Follow the on-screen instructions. If you need help at any time during the online registration process, simply click the **Need Help?** icon.
6. Once your personal Login Name and Password are confirmed, you can begin using the *Computer Security: Principles and Practice* Premium Website!

To log in after you have registered:

You only need to register for this Premium Website once. After that, you can log in any time at **www.pearsonglobaleditions.com/Stallings** by providing your Login Name and Password when prompted.

*Important: The access code can only be used once. This subscription is valid for twelve months upon activation and is not transferable. If this access code has already been revealed, it may no longer be valid. If this is the case, you can purchase a subscription by going to **www.pearsonglobaleditions.com/Stallings** and following the on-screen instructions.

COMPUTER SECURITY
PRINCIPLES AND PRACTICE

Third Edition
Global Edition

William Stallings

Lawrie Brown
UNSW Canberra at the Australian Defence Force Academy

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 São Paulo Sydney Hong Kong Seoul Singapore Taipei Tokyo

Editorial Director, ECS: Marcia Horton
Head of Learning Asset Acquisition, Global Edition: Laura Dent
Executive Editor: Tracy Johnson (Dunkelberger)
Editorial Assistant: Kelsey Loanes
Acquisitions Editor, Global Edition: Karthik Subramanian
Associate Project Editor, Global Edition: Uttaran Das Gupta
Director of Marketing: Christy Lesko
Marketing Manager: Yez Alayan
Marketing Assistant: Jon Bryant
Director of Program Management: Erin Gregg
Program Management - Team Lead: Scott Disanno
Program Manager: Carole Snyder
Project Manager: Robert Engelhardt
Senior Manufacturing Controller, Production, Global Edition: Trudy Kimber
Procurement Specialist: Linda Sager
Cover Designer: Lumina Datamatics
Managing Project Editor: Dr. Priyadharshini Dhanagopal
Production Project Manager: Jennifer Sargunar
Permissions Supervisor: Rachel Youdelman
Permissions Administrator: William Opaluch
Cover Art: Bildagentur Zoonar GmbH/Shutterstock
Associate Web Developer: Barry Offringa

Credits and acknowledgments borrowed from other sources and reproduced, with permission, in this textbook appear on page 835.

Pearson Education Limited
Edinburgh Gate
Harlow
Essex CM 20 2JE
England and Associated Companies throughout the world

Visit us on the World Wide Web at: www.pearsonglobaleditions.com

Authorized adaptation from the United States edition, entitled Computer Security: Principles and Practice, 4th Edition, ISBN 978-0-133-77392-7, by William Stallings and Lawrie Brown, published by Pearson Education © 2015.

ISBN 10: 1-292-06617-2
ISBN 13: 978-1-292-06617-2
British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

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

Typeset by Mahalatchoumy Saravanan, Jouve India in 10/12 Times Ten LT Std.
Printed and bound by Courier Westford in the United States of America.

For my loving wife, Tricia

—WS

To my extended family, who helped
make this all possible

—LB

Contents

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.

PREFACE

WHAT'S NEW IN THE THIRD EDITION

Since the second 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 second 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.

Beyond these refinements to improve pedagogy and user-friendliness, there have been major substantive changes throughout the book. The most noteworthy changes are as follows:

- **Fundamental security design principles:** Chapter 1 includes a new section discussing the security design principles listed as fundamental by the National Centers of Academic Excellence in Information Assurance/Cyber Defense, which is jointly sponsored by the U.S. National Security Agency and the U.S. Department of Homeland Security.
- **Attack surfaces and attack trees:** Chapter 1 includes a new section describing these two concepts, which are useful in evaluating and classifying security threats.
- **User authentication model:** Chapter 3 includes a new description of a general model for user authentication, which helps to unify the discussion of the various approaches to user authentication.
- **Attribute-based access control (ABAC):** Chapter 4 has a new section devoted to ABAC, which is becoming increasingly widespread.
- **Identity, credential, and access management (ICAM):** Chapter 4 includes a new section on ICAM, which is a comprehensive approach to managing and implementing digital identities (and associated attributes), credentials, and access control.
- **Trust frameworks:** Chapter 4 includes a new section on the Open Identity Trust Framework, which is an open, standardized approach to trustworthy identity and attribute exchange that is becoming increasingly widespread.
- **SQL injection attacks:** Chapter 5 includes a new section on the SQL injection attack, which is one of the most prevalent and dangerous network-based security threats.
- **Cloud security:** The material on cloud security in Chapter 5 has been updated and expanded to reflect its importance and recent developments.
- **Malware:** The material on Malware, and on categories of intruders, has been revised to reflect the latest developments, including details of Advanced Persistent Threats, which are most likely due to nation state actors.
- **Intrusion detection/intrusion prevention systems:** The material on IDS/IPS has been updated to reflect new developments in the field, including the latest developments in Host-Based Intrusion Detection Systems that assist in implementing a defense-in-depth strategy.

- **Human resources:** Security lapses due to human factors and social engineering are of increasing concern, including several recent cases of massive data exfiltration by insiders. Addressing such lapses requires a complex mix of procedural and technical controls, which we review in several significantly revised sections.
- **Mobile device security:** Mobile device security has become an essential aspect of enterprise network security, especially for devices in the category known as bring your own device (BYOD). A new section in Chapter 24 covers this important topic.
- **SHA-3:** This recently adopted cryptographic hash standard is covered in a new appendix.

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. The NSA/DHS National Center of Academic Excellence in Information Assurance/Cyber Defense is 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.

SUPPORT OF ACM/IEEE COMPUTER SCIENCE CURRICULA 2013

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. This edition is designed to support the recommendations of the ACM/IEEE Computer Science Curricula 2013 (CS2013). The CS2013 curriculum recommendation includes, for the first time, Information Assurance and Security (IAS) as one of the Knowledge Areas in the Computer Science Body of Knowledge. CS2013 divides all course work into three categories: Core-Tier 1 (all topics should be included in the curriculum), Core-Tier 2 (all or almost all topics should be included), and Elective (desirable to provide breadth and depth). In the IAS area, CS2013 includes three Tier 1 topics, five Tier 2 topics, and numerous Elective topics, each of which has a number of subtopics. This text covers all of the Tier 1 and Tier 2 topics and subtopics listed by CS2013, as well as many of the elective topics.

See Chapter 0 for details of this book's coverage of CS2013.

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.

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 chapters and 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, and suggestions for further reading.

INSTRUCTOR SUPPORT MATERIALS

The major goal of this text is to make it as effective a teaching tool for this exciting and fast-moving subject as possible. This goal is reflected both in the structure of the book and in the supporting material. The text is accompanied by the following supplementary material to aid the instructor:

- **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.

All of these support materials are available at the **Instructor Resource Center (IRC)** for this textbook, which can be reached through the publisher's Web site www.pearsonglobaledition.com/Stallings or by clicking on the link labeled *Pearson Resources for Instructors* at this book's Companion Web site at www.pearsonglobaledition.com/Stallings. To gain access to the IRC, please contact your local Pearson sales representative.

The **Companion Web Site**, at www.pearsonglobaledition.com/Stallings (click on the 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.

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 Web Site**, at www.pearsonglobaledition.com/Stallings (click on the Student Resources link), includes a list of relevant links organized by chapter and an errata sheet for the book.

Purchasing this textbook now grants the reader 12-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 is available. These enable the students to test their understanding of the text.

To access the Premium Content site, click on the *Premium Content* link at the Companion Web site or at www.pearsonglobaledition.com/Stallings and enter the student access code found on the card in the front of the book.

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 Pearson not only include guidance on how to assign and structure the projects but also include 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.
- **Security education (SEED) projects:** The SEED projects are a set of hands-on exercises, or labs, covering a wide range of security topics.
- **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.

- **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.
- **Webcasts for teaching computer security:** A catalog of webcast sites that can be used to enhance the course. An effective way of using this catalog is to select, or allow the student to select, one or a few videos to watch, and then to write a report/analysis of the video.

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: Stefan Robila (Montclair State University), Weichao Wang (University of North Carolina, Charlotte), 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: Umair Manzoor (UmZ), Adewumi Olatunji (FAGOSI 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, and 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 Engineering and Information Technology, UNSW Canberra at the Australian Defence Force Academy for their encouragement and support.

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 Pearson, particularly our editor Tracy Dunkelberger, program manager Carole Snyder, and production manager Bob Engelhardt. We also thank the production staff at Jouve India for another excellent and rapid job. Thanks also to the marketing and sales staff at Pearson, without whose efforts this book would not be in your hands.

Notation

Symbol	Expression	Meaning
D, K	$\mathrm{D}(K, Y)$	Symmetric decryption of ciphertext Y using secret key K
D, PR_a	$\mathrm{D}(PR_a, Y)$	Asymmetric decryption of ciphertext Y using A's private key PR_a
D, PU_a	$\mathrm{D}(PU_a, Y)$	Asymmetric decryption of ciphertext Y using A's public key PU_a
E, K	$\mathrm{E}(K, X)$	Symmetric encryption of plaintext X using secret key K
E, PR_a	$\mathrm{E}(PR_a, X)$	Asymmetric encryption of plaintext X using A's private key PR_a
E, PU_a	$\mathrm{E}(PU_a, X)$	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	$\mathrm{H}(X)$	Hash function of message X
$+$	$x + y$	Logical OR: x OR y
$\bullet$	$x \bullet y$	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
$\vert, X$	$\vert X(C) \vert$	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 authored 18 textbooks, and, counting revised editions, a total of 70 books on various aspects of these subjects. His writings have appeared in numerous ACM and IEEE publications, including the *Proceedings of the IEEE and ACM Computing Reviews*. He has 11 times received the award for the best Computer Science textbook of the year from the Text and Academic Authors Association.

In over 30 years in the field, he has been a technical contributor, technical manager, and an executive with several high-technology firms. He has designed and implemented both TCP/IP-based and OSI-based protocol suites on a variety of computers and operating systems, ranging from microcomputers to mainframes. 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 created and maintains the Computer Science Student Resource Site at ComputerScienceStudent.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. His articles appear regularly at http://www.networking.answers.com, where he is the Networking Category Expert Writer.

Dr. Lawrie Brown is a senior lecturer in the School of Engineering and Information Technology, UNSW Canberra at the Australian Defence Force Academy.

His professional interests include communications and computer systems security and cryptography, including research on client authentication using proxy certificates, trust and security in eCommerce and Web environments, the design of secure remote code execution environments using the functional language Erlang, and on the design and implementation of the LOKI family of block ciphers.

He currently teaches courses on cyber-security and data structures, and has previously presented courses on cryptography, data communications, and programming in Java.

Pearson would like to thank the following persons for their contribution to the Global Edition:

Contributor:

Mohit Tahiliani (NITK Surathkal)

Reviewers:

B. R. Chandavarkar (NITK Surathkal), Somitra Kr. Sanadhya (Indraprastha Institute of Information Technology, Delhi), Sandeep Bhat (M.S. Ramaiah Institute of Technology, Bangalore)

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 and cloud 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 fulfills 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 $(ISC)^2$, 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 (Information Technology) 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)^2. 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	Textbook 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:** The types of 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 SUPPORT FOR NSA/DHS CERTIFICATION

The U.S. National Security Agency (NSA) and the U.S. Department of Homeland Security (DHS) jointly sponsor the National Centers of Academic Excellence in Information Assurance/Cyber Defense (IA/CD). The goal of these programs is to reduce vulnerability in our national information infrastructure by promoting higher education and research in IA and producing a growing number of professionals with IA expertise in various disciplines. To achieve that purpose, NSA/DHS have defined a set of Knowledge Units for 2- and 4-year institutions that must be supported in the curriculum to gain a designation as a NSA/DHS National Center of Academic Excellence in IA/CD. Each Knowledge Unit is composed of a minimum list of required topics to be covered and one or more outcomes or learning objectives. Designation is based on meeting a certain threshold number of core and optional Knowledge Units.

In the area of computer security, the 2014 Knowledge Units document [NCAE13] lists the following core Knowledge Units:

- **Cyber defense:** Includes access control, cryptography, firewalls, intrusion detection systems, malicious activity detection and countermeasures, trust relationships, and defense in depth.
- **Cyber threats:** Includes types of attacks, legal issues, attack surfaces, attack trees, insider problems, and threat information sources.
- **Fundamental security design principles:** A list of 12 principles, all of which are covered in Section 1.4 of this book.
- **Information assurance fundamentals:** Includes threats and vulnerabilities, intrusion detection and prevention systems, cryptography, access control models, identification/authentication, and audit.
- **Introduction to cryptography:** Includes symmetric cryptography, public-key cryptography, hash functions, and digital signatures.
- **Databases:** Includes an overview of databases, database access controls, and security issues of inference.

This book provides extensive coverage in all of these areas. In addition, the book partially covers a number of the optional Knowledge Units.

0.5 SUPPORT FOR ACM/IEEE COMPUTER SOCIETY COMPUTER SCIENCE CURRICULA 2013

Computer Science Curricula 2013 (CS2013) is a joint effort of the Association for Computing Machinery (ACM) and the Computer Society of the Institute of Electrical and Electronics Engineers (IEEE-CS). ACM and IEEE-CS have collaborated on developing recommended computer science curricula starting with the publication of Curriculum 68. CS2013 is the first comprehensive revision of the recommendation since 2001. Hundreds of computer science professors, department chairs, and directors of undergraduate studies worldwide were involved in developing CS2013. There was a wide consensus that a strong need existed to add a new Knowledge Area on Information Assurance and Security (IAS).

IAS as a domain is the set of controls and processes, both technical and policy, intended to protect and defend information and information systems by ensuring their availability, integrity, authentication, and confidentiality and providing for non-repudiation. The concept of assurance also carries an attestation that current and past processes and data are valid. Both assurance and security concepts are needed to ensure a complete perspective.

CS2013 divides all course work into three categories: Core-Tier 1 (all topics should be included in the curriculum), Core-Tier-2 (all or almost all topics should be included), and Elective (desirable to provide breadth and depth). In the IAS area, CS2013 includes three Tier 1 topics, five Tier 2 topics, and numerous Elective topics, each of which has a number of subtopics. This text covers all of the Tier 1 and Tier 2 topics and subtopics listed by CS2013, as well as many of the elective topics. Table 0.2 shows the support for the ISA Knowledge Area provided in this textbook.

Table 0.2 **Coverage of CS2013 Information Assurance and Security (IAS) Knowledge Area**

IAS Knowledge Units	Topics	Textbook Coverage
Foundational Concepts in Security (Tier 1)	• CIA (Confidentiality, Integrity, Availability • Risk, threats, vulnerabilities, and attack vectors • Authentication and authorization, and access control (mandatory vs. discretionary) • Trust and trustworthiness • Ethics (responsible disclosure)	1—Overview 3—User Authentication 4—Access Control 19—Legal and Ethical Aspects
Principles of Secure Design (Tier 1)	• Least privilege and isolation • Fail-safe defaults • Open design • End-to-end security • Defense in depth • Security by design • Tensions between security and other design goals	1—Overview
Principles of Secure Design (Tier 2)	• Complete mediation • Use of vetted security components • Economy of mechanism (reducing trusted computing base, minimize attack surface) • Usable security • Security composability • Prevention, detection, and deterrence	1—Overview
Defensive Programming (Tier 1)	• Input validation and data sanitization • Choice of programming language and type-safe languages • Examples of input validation and data sanitization errors (buffer overflows, integer errors, SQL injection, and XSS vulnerability) • Race conditions • Correct handling of exceptions and unexpected behaviors	11—Software Security

(Continued)

Table 0.2 *(Continued)*

IAS Knowledge Units	Topics	Textbook Coverage
Defensive Programming (Tier 2)	• Correct usage of third-party components • Effectively deploying security updates	11—Software Security 12—OS Security
Threats and Attacks (Tier 2)	• Attacker goals, capabilities, and motivations • Malware • Denial of service and Distributed Denial of Service • Social engineering	6—Malicious Software 7—Denial-of-Service Attacks
Network Security (Tier 2)	• Network specific threats and attack types • Use of cryptography for data and network security • Architectures for secure networks • Defense mechanisms and countermeasures • Security for wireless, cellular networks	8—Intrusion Detection 9—Firewalls and Intrusion Prevention Systems Part 5—Network Security
Cryptography (Tier 2)	• Basic cryptography terminology • Cipher types • Overview of mathematical preliminaries • Public key I dnfrastructure	2—Cryptographic Tools Part 4—Cryptographic Algorithms

0.6 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, and a set of homework problems with solutions. See the card at the front of this book for access information.

Finally, additional material for instructors, including a solutions manual and a projects manual, 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

Numerous Web sites provide information related to the topics of this book. The Companion Website provides links to these sites, organized by chapter.

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

0.7 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)[1] is a worldwide federation of national standards bodies. 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.

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