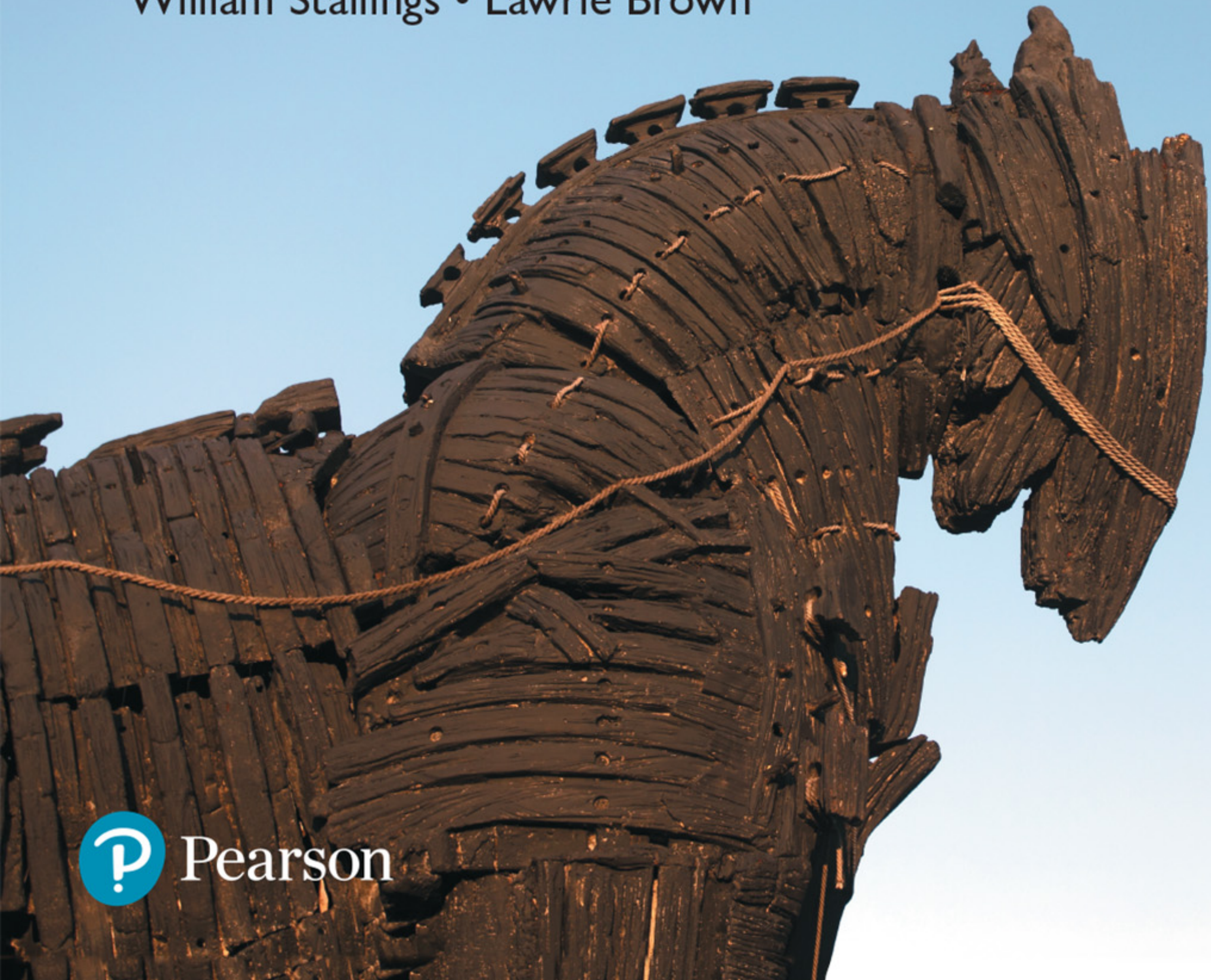
GLOBAL
EDITION

Computer Security

Principles and Practice

FOURTH EDITION

William Stallings • Lawrie Brown



Pearson

Digital Resources for Students

Your new textbook provides 12-month access to digital resources that may include VideoNotes (step-by-step video tutorials on programming concepts), source code, web chapters, quizzes, and more. Refer to the preface in the textbook for a detailed list of resources.

Follow the instructions below to register for the Companion Website for William Stallings/Lawrie Brown's *Computer Security: Principles and Practice,* Fourth Edition, Global Edition.

1. Go to www.pearsonglobaleditions.com/stallings.
2. Enter the title of your textbook or browse by author name.
3. Click Companion Website.
4. Click Register and follow the on-screen instructions to create a login name and password.

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

Use the login name and password you created during registration to start using the online resources that accompany your textbook.

IMPORTANT:

This access code can only be used once. This subscription is valid for 12 months upon activation and is not transferrable. If the access code has already been revealed it may no longer be valid.

For technical support go to https://support.pearson.com/getsupport/

Computer Security
Principles and Practice

Fourth Edition

Global Edition

William Stallings

Lawrie Brown
UNSW Canberra at the Australian Defence Force Academy

Pearson

330 Hudson Street, New York, NY 10013

Director, Portfolio Management: Engineering, Computer Science & Global Editions: Julian Partridge
Specialist, Higher Ed Portfolio Management: Tracy Johnson (Dunkelberger)
Acquisitions Editor, Global Edition: Sourabh Maheshwari
Portfolio Management Assistant: Meghan Jacoby
Managing Content Producer: Scott Disanno
Content Producer: Robert Engelhardt
Project Editor, Global Edition: K.K. Neelakantan
Web Developer: Steve Wright
Manager, Media Production, Global Edition: Vikram Kumar
Rights and Permissions Manager: Ben Ferrini
Manufacturing Buyer, Higher Ed, Lake Side Communications Inc (LSC): Maura Zaldivar-Garcia
Senior Manufacturing Controller, Global Edition: Angela Hawksbee
Inventory Manager: Ann Lam
Product Marketing Manager: Yvonne Vannatta
Field Marketing Manager: Demetrius Hall
Marketing Assistant: Jon Bryant
Cover Designer: Lumina Datamatics, Inc.
Cover Photo: Alex Kosev / Shutterstock
Full-Service Project Management: Kirthika Raj, SPi Global

Credits and acknowledgments borrowed from other sources and reproduced, with permission, in this textbook appear on page 777.

Pearson Education Limited
KAO Two
KAO Park
Harlow
CM17 9NA
United Kingdom

and Associated Companies throughout the world

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

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

ISBN 10: 1-292-22061-9
ISBN 13: 978-1-292-22061-1

Typeset by SPi Global
Printed and bound in Malaysia

For my loving wife, Tricia

—WS

To my extended family and friends, who helped
make this all possible

—LB

This page intentionally left blank

CONTENTS

ONLINE CHAPTERS AND APPENDICES[1]

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

PREFACE

WHAT'S NEW IN THE FOURTH EDITION

Since the third 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 third 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:

- **Data center security:** Chapter 5 includes a new discussion of data center security, including the TIA-492 specification of reliability tiers.
- **Malware:** The material on malware in Chapter 6 has been revised to include additional material on macro viruses and their structure, as they are now the most common form of virus malware.
- **Virtualization security:** The material on virtualization security in Chapter 12 has been extended, given the rising use of such systems by organizations and in cloud computing environments. A discussion of virtual firewalls, which may be used to help secure these environments, has also been added.
- **Cloud security:** Chapter 13 includes a new discussion of cloud security. The discussion includes an introduction to cloud computing, key cloud security concepts, an analysis of approaches to cloud security, and an open-source example.
- **IoT security:** Chapter 13 includes a new discussion of security for the Internet of Things (IoT). The discussion includes an introduction to IoT, an overview of IoT security issues, and an open-source example.
- **SEIM:** The discussion of Security Information and Event Management (SIEM) systems in Chapter 18 has been updated.
- **Privacy:** The section on privacy issues and its management in Chapter 19 has been extended with additional discussion of moral and legal approaches, and the privacy issues related to big data.
- **Authenticated encryption:** Authenticated encryption has become an increasingly widespread cryptographic tool in a variety of applications and protocols. Chapter 21 includes a new discussion of authenticated description and describes an important authenticated encryption algorithm known as offset codebook (OCB) mode.

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

This 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

Table P.1 **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, and Availability) • Risk, threats, vulnerabilities, and attack vectors • Authentication and authorization, 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
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 infrastructure	2—Cryptographic Tools Part 4—Cryptographic Algorithms

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. Table P.1 shows the support for the ISA Knowledge Area provided in this textbook.

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 8 domains that comprise the body of knowledge that is required for CISSP certification.

The 8 domains are as follows, with an indication of where the topics are covered in this textbook:

- **Security and risk management:** Confidentiality, integrity, and availability concepts; security governance principles; risk management; compliance; legal and regulatory issues; professional ethics; and security policies, standards, procedures, and guidelines. *(Chapter 14)*
- **Asset security:** Information and asset classification; ownership (e.g. data owners, system owners); privacy protection; appropriate retention; data security controls; and handling requirements (e.g., markings, labels, storage). *(Chapters 5, 15, 16, 19)*
- **Security engineering:** Engineering processes using secure design principles; security models; security evaluation models; security capabilities of information systems; security architectures, designs, and solution elements vulnerabilities; web-based systems vulnerabilities; mobile systems vulnerabilities; embedded devices and cyber-physical systems vulnerabilities; cryptography; and site and facility design secure principles; physical security. *(Chapters 1, 2, 13, 15, 16)*
- **Communication and network security:** Secure network architecture design (e.g., IP and non-IP protocols, segmentation); secure network components; secure communication channels; and network attacks. *(Part Five)*

- **Identity and access management:** Physical and logical assets control; identification and authentication of people and devices; identity as a service (e.g. cloud identity); third-party identity services (e.g., on-premise); access control attacks; and identity and access provisioning lifecycle (e.g., provisioning review). *(Chapters 3, 4, 8, 9)*
- **Security assessment and testing:** Assessment and test strategies; security process data (e.g., management and operational controls); security control testing; test outputs (e.g., automated, manual); and security architectures vulnerabilities. *(Chapters 14, 15, 18)*
- **Security operations:** Investigations support and requirements; logging and monitoring activities; provisioning of resources; foundational security operations concepts; resource protection techniques; incident management; preventative measures; patch and vulnerability management; change management processes; recovery strategies; disaster recovery processes and plans; business continuity planning and exercises; physical security; and personnel safety concerns. *(Chapters 11, 12, 15, 16, 17)*
- **Software development security:** Security in the software development lifecycle; development environment security controls; software security effectiveness; and acquired software security impact. *(Part Two)*

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 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 text.
- **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.

PLAN OF THE TEXT

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

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

The text is also accompanied by a number of online chapters and appendices that provide more detail on selected topics.

The text 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 Website www.pearsonglobaleditions.com/stallings . To gain access to the IRC, please contact your local Pearson sales representative.

The **Companion Website** 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 Website**, 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, three 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 eleven online 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 link at www.pearsonglobaleditions.com/stallings and enter the student access code found on the inside front cover.

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 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 students 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: Bernardo Palazzi (Brown University), Jean Mayo (Michigan Technological University), Scott Kerlin (University of North Dakota), Philip Campbell (Ohio University), Scott Burgess (Humboldt State University), Stanley Wine (Hunter College/CUNY), and E. Mauricio Angee (Florida International University).

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. In particular, thanks to Gideon Creech, Edward Lewis, and Ben Whitham for discussion and review of some of the chapter content.

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, her editorial assistant Kristy Alaura, and project manager Bob Engelhardt. Thanks also to the marketing and sales staffs at Pearson, without whose efforts this book would not be in front of you.

ACKNOWLEDGMENTS FOR THE GLOBAL EDITION

Pearson would like to thank and acknowledge Somitra Sanadhya (Indian Institute of Technology Ropar) for contributing to the Global Edition, and Arup Bhattacharya (RCC Institute of Technology), A. Kannammal (Coimbatore Institute of Technology), and Khyat Sharma for reviewing the Global Edition.