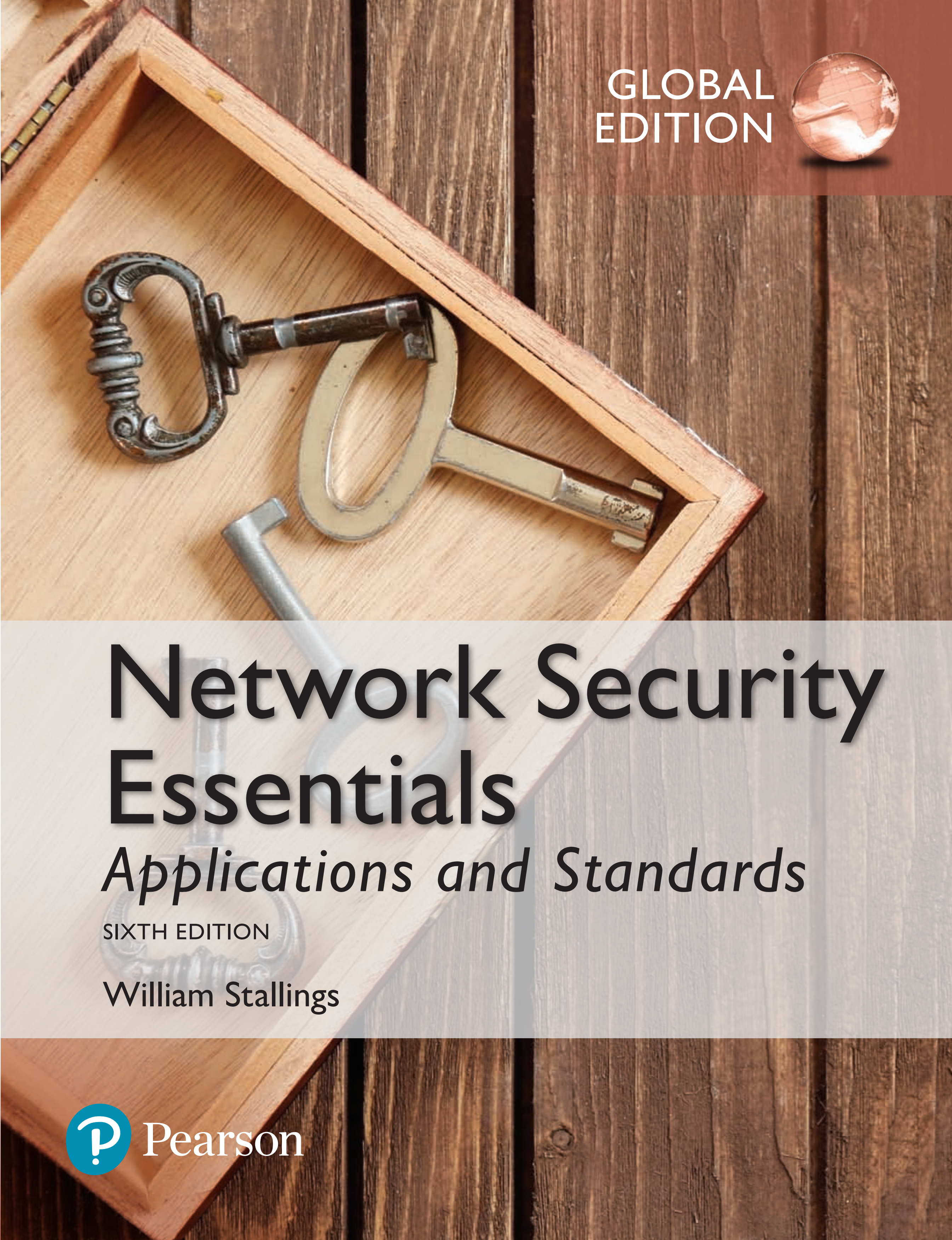

GLOBAL EDITION

Network Security Essentials

Applications and Standards

SIXTH EDITION

William Stallings

Pearson

Network Security Essentials:

Applications and Standards

Sixth Edition

Global Edition

William Stallings

Pearson

Harlow, England • London • New York • Boston • San Francisco • Toronto • Sydney • Dubai • Singapore • Hong Kong
Tokyo • Seoul • Taipei • New Delhi • Cape Town • Sao Paulo • Mexico City • Madrid • Amsterdam • Munich • Paris • Milan

Vice President and Editorial Director, ECS: Marcia J. Horton
Executive Editor: Tracy Johnson (Dunkelberger)
Editorial Assistant: Kristy Alaura
Program Manager: Carole Snyder
Project Manager: Robert Engelhardt
Media Team Lead: Steve Wright
Acquisitions Editor, Global Edition: Sourabh Maheshwari
Assistant Project Editor, Global Edition: Shaoni Mukherjee
Manager, Media Production, Global Edition: Vikram Kumar
Senior Manufacturing Controller, Production, Global Edition: Trudy Kimber
R&P Manager: Rachel Youdelman
R&P Senior Project Manager: William Opaluch
Senior Operations Specialist: Maura Zaldivar-Garcia
Inventory Manager: Meredith Maresca
Marketing Manager: Demetrius Hall
Product Marketing Manager: Bram Van Kempen
Marketing Assistant: Jon Bryant
Cover Designer: Marta Samsel
Cover Art: Africa Studio
Full-Service Project Management: Chandrasekar Subramanian, SPi Global

Credits and acknowledgments borrowed from other sources and reproduced, with permission, in this textbook appears on page 448.

Pearson Education Limited
Edinburgh Gate
Harlow
Essex CM20 2JE
England

and Associated Companies throughout the world

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

© Pearson Education Limited 2017

The right of William Stallings to be identified as the author of this work has been asserted by him in accordance with the Copyright, Designs and Patents Act 1988.

Authorized adaptation from the United States edition, entitled Network Security Essentials: Applications and Standards, 6th Edition, ISBN 978-0-134-52733-8, by William Stallings published by Pearson Education © 2017.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without either the prior written permission of the publisher or a license permitting restricted copying in the United Kingdom issued by the Copyright Licensing Agency Ltd, Saffron House, 6–10 Kirby Street, London EC1N 8TS.

All trademarks used herein are the property of their respective owners. The use of any trademark in this text does not vest in the author or publisher any trademark ownership rights in such trademarks, nor does the use of such trademarks imply any affiliation with or endorsement of this book by such owners.

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: 1-292-15485-3
ISBN 13: 978-1-292-15485-5

Typeset by SPi Global
Printed and bound in Malaysia.

For Tricia never
dull never boring
the smartest
and bravest
person I know

This page intentionally left blank

CONTENTS

Preface 10

About the Author 16

Chapter 1 Introduction 17

1.1 Computer Security Concepts 20
1.2 The OSI Security Architecture 24
1.3 Security Attacks 25
1.4 Security Services 27
1.5 Security Mechanisms 31
1.6 Fundamental Security Design Principles 32
1.7 Attack Surfaces and Attack Trees 36
1.8 A Model for Network Security 39
1.9 Standards 42
1.10 Key Terms, Review Questions, and Problems 42

PART ONE: CRYPTOGRAPHY 45

Chapter 2 Symmetric Encryption and Message Confidentiality 45

2.1 Symmetric Encryption Principles 46
2.2 Symmetric Block Encryption Algorithms 52
2.3 Random and Pseudorandom Numbers 59
2.4 Stream Ciphers and RC4 63
2.5 Cipher Block Modes of Operation 68
2.6 Key Terms, Review Questions, and Problems 73

Chapter 3 Public-Key Cryptography and Message Authentication 78

3.1 Approaches to Message Authentication 79
3.2 Secure Hash Functions 84
3.3 Message Authentication Codes 91
3.4 Public-Key Cryptography Principles 96
3.5 Public-Key Cryptography Algorithms 100
3.6 Digital Signatures 109
3.7 Key Terms, Review Questions, and Problems 112

PART TWO: NETWORK SECURITY APPLICATIONS 119

Chapter 4 Key Distribution and User Authentication 119

4.1 Remote User Authentication Principles 120
4.2 Symmetric Key Distribution Using Symmetric Encryption 123
4.3 Kerberos 124
4.4 Key Distribution Using Asymmetric Encryption 137
4.5 X.509 Certificates 139
4.6 Public-Key Infrastructure 146

4.7 Federated Identity Management 149
4.8 Key Terms, Review Questions, and Problems 155
Chapter 5 Network Access Control and Cloud Security 160
5.1 Network Access Control 161
5.2 Extensible Authentication Protocol 164
5.3 IEEE 802.1X Port-Based Network Access Control 168
5.4 Cloud Computing 170
5.5 Cloud Security Risks and Countermeasures 176
5.6 Data Protection in the Cloud 178
5.7 Cloud Security as a Service 182
5.8 Addressing Cloud Computing Security Concerns 185
5.9 Key Terms, Review Questions, and Problems 186
Chapter 6 Transport-Level Security 187
6.1 Web Security Considerations 188
6.2 Transport Layer Security 190
6.3 HTTPS 207
6.4 Secure Shell (SSH) 208
6.5 Key Terms, Review Questions, and Problems 220
Chapter 7 Wireless Network Security 222
7.1 Wireless Security 223
7.2 Mobile Device Security 226
7.3 IEEE 802.11 Wireless LAN Overview 230
7.4 IEEE 802.11i Wireless LAN Security 236
7.5 Key Terms, Review Questions, and Problems 251
Chapter 8 Electronic Mail Security 253
8.1 Internet Mail Architecture 254
8.2 E-mail Formats 258
8.3 E-mail Threats and Comprehensive E-mail Security 266
8.4 S/MIME 268
8.5 Pretty Good Privacy 279
8.6 DNSSEC 280
8.7 DNS-Based Authentication of Named Entities 285
8.8 Sender Policy Framework 286
8.9 DomainKeys Identified Mail 289
8.10 Domain-Based Message Authentication, Reporting, and Conformance 295
8.11 Key Terms, Review Questions, and Problems 300
Chapter 9 IP Security 302
9.1 IP Security Overview 303
9.2 IP Security Policy 309
9.3 Encapsulating Security Payload 314
9.4 Combining Security Associations 322
9.5 Internet Key Exchange 325
9.6 Cryptographic Suites 333
9.7 Key Terms, Review Questions, and Problems 335

PART THREE: SYSTEM SECURITY 337

Chapter 10 Malicious Software 337

10.1 Types of Malicious Software (Malware) 338
10.2 Advanced Persistent Threat 341
10.3 Propagation—Infected Content—Viruses 342
10.4 Propagation—Vulnerability Exploit—Worms 347
10.5 Propagation—Social Engineering—Spam E-mail, Trojans 353
10.6 Payload—System Corruption 355
10.7 Payload—Attack Agent—Zombie, Bots 356
10.8 Payload—Information Theft—Keyloggers, Phishing, Spyware 357
10.9 Payload—Stealthing—Backdoors, Rootkits 359
10.10 Countermeasures 360
10.11 Distributed Denial of Service Attacks 367
10.12 Key Terms, Review Questions, and Problems 372

Chapter 11 Intruders 375

11.1 Intruders 376
11.2 Intrusion Detection 381
11.3 Password Management 396
11.4 Key Terms, Review Questions, and Problems 406

Chapter 12 Firewalls 410

12.1 The Need for Firewalls 411
12.2 Firewall Characteristics and Access Policy 412
12.3 Types of Firewalls 414
12.4 Firewall Basing 420
12.5 Firewall Location and Configurations 423
12.6 Key Terms, Review Questions, and Problems 428

APPENDICES 432

Appendix A Some Aspects of Number Theory 432

A.1 Prime and Relatively Prime Numbers 433
A.2 Modular Arithmetic 435

Appendix B Projects for Teaching Network Security 437

B.1 Research Projects 438
B.2 Hacking Project 439
B.3 Programming Projects 439
B.4 Laboratory Exercises 440
B.5 Practical Security Assessments 440
B.6 Firewall Projects 440
B.7 Case Studies 441
B.8 Writing Assignments 441
B.9 Reading/Report Assignments 441

References 442

Credits 448

Index 450

ONLINE CHAPTERS AND APPENDICES[1]

Chapter 13 Network Management Security

13.1 Basic Concepts of SNMP
13.2 SNMPv1 Community Facility
13.3 SNMPv3
13.4 Recommended Reading
13.5 Key Terms, Review Questions, and Problems

PART FIVE: LEGAL AND ETHICAL ISSUES

Chapter 14 Legal and Ethical Issues

14.1 Cybercrime and Computer Crime
14.2 Intellectual Property
14.3 Privacy
14.4 Ethical Issues
14.5 Recommended Reading
14.6 References
14.7 Key Terms, Review Questions, and Problems
14.A Information Privacy

Chapter 15 SHA-3

15.1 The Origins of SHA-3
15.2 Evaluation Criteria for SHA-3
15.3 The Sponge Construction
15.4 The SHA-3 Iteration Function *f*
15.5 Recommended Reading and Referencess
15.6 Key Terms, Review Questions, and Problems

Appendix C Standards and Standards-Setting Organizations

C.1 The Importance of Standards
C.2 Internet Standards and the Internet Society
C.3 The National Institute of Standards and Technology
C.4 The International Telecommunication Union
C.5 The International Organization for Standardization
C.6 Significant Security Standards and Documents

Appendix D TCP/IP and OSI

D.1 Protocols and Protocol Architectures
D.2 The TCP/IP Protocol Architecture
D.3 The Role of an Internet Protocol
D.4 IPv4
D.5 IPv6
D.6 The OSI Protocol Architecture

[1] Online chapters, appendices, and other documents are at the Companion Website, available via the access code on the inside front cover of this book.

Appendix E Pseudorandom Number Generation

E.1 Prng Requirements

E.2 Pseudorandom Number Generation Using a Block Cipher

E.3 Pseudorandom Number Generation Using Hash Functions and MACs

Appendix F Kerberos Encryption Techniques

F.1 Password-To-Key Transformation

F.2 Propagating Cipher Block Chaining Mode

Appendix G Data Compression Using ZIP

G.1 Compression Algorithm

G.2 Decompression Algorithm

Appendix H PGP

H.1 Notation

H.2 Operational Description

H.3 Cryptographic Keys and Key Rings

H.4 Public-Key Management

H.5 PGP Random Number Generation

Appendix I The International Reference Alphabet

Appendix J The Base-Rate Fallacy

J.1 Conditional Probability and Independence

J.2 Bayes' Theorem

J.3 The Base-Rate Fallacy Demonstrated

J.4 References

Appendix K Radix-64 Conversion