

INTRODUCTION TO

Computer Security



Michael T. Roberto
GOODRICH & TAMASSIA

Editorial Director: Marcia Horton
Editor-in-Chief: Michael Hirsch
Acquisitions Editor: Matt Goldstein
Editorial Assistant: Chelsea Bell
Marketing Manager: Yezan Alayan
Marketing Coordinator: Kathryn Ferranti
Managing Editor: Jeff Holcomb
Senior Operations Supervisor: Alan Fischer
Art Director: Linda Knowles
Cover Designer: Joyce Cosentino Wells
Cover Photograph: © Fotolia
Media Editor: Daniel Sandin
Copyeditor: Jeri Warner
Proofreader: Richard Camp
Printer/Binder: Edwards Brothers
Cover Printer: Lehigh-Phoenix Color/Hagerstown

Credits and acknowledgments borrowed from other sources and reproduced, with permission, in this textbook appear on pages iii and iv of this book.

Copyright © 2011 Michael T. Goodrich and Roberto Tamassia. All rights reserved.
Manufactured in the United States of America. This publication is protected by Copyright, and permission should be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise. To obtain permission(s) to use material from this work, please submit a written request to Pearson Education, Inc., Permissions Department, 501 Boylston Street, Suite 900, Boston, Massachusetts 02116.

Many of the designations by manufacturers and seller to distinguish their products are claimed as trademarks. Where those designations appear in this book, and the publisher was aware of a trademark claim, the designations have been printed in initial caps or all caps.

Library of Congress Cataloging-in-Publication Data

Goodrich, Michael T.
Introduction to computer security / Michael T. Goodrich, Roberto Tamassia.
p. cm.
Includes bibliographical references and index.
ISBN-13: 978-0-321-51294-9 (alk. paper)
ISBN-10: 0-321-51294-4 (alk. paper)
1. Computer security. I. Tamassia, Roberto, 1960- II. Title.
QA76.9.A25G655 2011
005.8--dc22

2010028536

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



Contents

1	Introduction	1
1.1	Fundamental Concepts	2
1.1.1	Confidentiality, Integrity, and Availability	3
1.1.2	Assurance, Authenticity, and Anonymity	9
1.1.3	Threats and Attacks	14
1.1.4	Security Principles	15
1.2	Access Control Models	19
1.2.1	Access Control Matrices	19
1.2.2	Access Control Lists	20
1.2.3	Capabilities	22
1.2.4	Role-Based Access Control	23
1.3	Cryptographic Concepts	25
1.3.1	Encryption	25
1.3.2	Digital Signatures	31
1.3.3	Simple Attacks on Cryptosystems	32
1.3.4	Cryptographic Hash Functions	35
1.3.5	Digital Certificates	37
1.4	Implementation and Usability Issues	39
1.4.1	Efficiency and Usability	39
1.4.2	Passwords	41
1.4.3	Social Engineering	43
1.4.4	Vulnerabilities from Programming Errors	44
1.5	Exercises	46

2	Physical Security	55
2.1	Physical Protections and Attacks	56
2.2	Locks and Safes	57
2.2.1	Lock Technology	57
2.2.2	Attacks on Locks and Safes	62
2.2.3	The Mathematics of Lock Security	68
2.3	Authentication Technologies	71
2.3.1	Barcodes	71
2.3.2	Magnetic Stripe Cards	72
2.3.3	Smart Cards	74
2.3.4	RFIDs	79
2.3.5	Biometrics	83
2.4	Direct Attacks Against Computers	88
2.4.1	Environmental Attacks and Accidents	88
2.4.2	Eavesdropping	89
2.4.3	TEMPEST	94
2.4.4	Live CDs	96
2.4.5	Computer Forensics	96
2.5	Special-Purpose Machines	99
2.5.1	Automated Teller Machines	99
2.5.2	Voting Machines	101
2.6	Physical Intrusion Detection	103
2.6.1	Video Monitoring	103
2.6.2	Human Factors and Social Engineering	105
2.7	Exercises	106
3	Operating Systems Security	113
3.1	Operating Systems Concepts	114
3.1.1	The Kernel and Input/Output	115
3.1.2	Processes	116
3.1.3	The Filesystem	121
3.1.4	Memory Management	124
3.1.5	Virtual Machines	128
3.2	Process Security	130
3.2.1	Inductive Trust from Start to Finish	130
3.2.2	Monitoring, Management, and Logging	132
3.3	Memory and Filesystem Security	136
3.3.1	Virtual Memory Security	136
3.3.2	Password-Based Authentication	137
3.3.3	Access Control and Advanced File Permissions	140
3.3.4	File Descriptors	146
3.3.5	Symbolic Links and Shortcuts	148

3.4	Application Program Security	149
3.4.1	Compiling and Linking	149
3.4.2	Simple Buffer Overflow Attacks	150
3.4.3	Stack-Based Buffer Overflow	152
3.4.4	Heap-Based Buffer Overflow Attacks	159
3.4.5	Format String Attacks	162
3.4.6	Race Conditions	163
3.5	Exercises	166
4	Malware	173
4.1	Insider Attacks	174
4.1.1	Backdoors	174
4.1.2	Logic Bombs	177
4.1.3	Defenses Against Insider Attacks	180
4.2	Computer Viruses	181
4.2.1	Virus Classification	182
4.2.2	Defenses Against Viruses	185
4.2.3	Encrypted Viruses	186
4.2.4	Polymorphic and Metamorphic Viruses	187
4.3	Malware Attacks	188
4.3.1	Trojan Horses	188
4.3.2	Computer Worms	190
4.3.3	Rootkits	195
4.3.4	Zero-Day Attacks	199
4.3.5	Botnets	200
4.4	Privacy-Invasive Software	202
4.4.1	Adware	202
4.4.2	Spyware	204
4.5	Countermeasures	208
4.5.1	Best Practices	208
4.5.2	The Impossibility of Detecting All Malware	211
4.5.3	The Malware Detection Arms Race	213
4.5.4	Economics of Malware	214
4.6	Exercises	215
5	Network Security I	221
5.1	Network Security Concepts	222
5.1.1	Network Topology	222
5.1.2	Internet Protocol Layers	223
5.1.3	Network Security Issues	227
5.2	The Link Layer	229
5.2.1	Ethernet	229

5.2.2	Media Access Control (MAC) Addresses	232
5.2.3	ARP Spoofing	233
5.3	The Network Layer	236
5.3.1	IP	236
5.3.2	Internet Control Message Protocol	240
5.3.3	IP Spoofing	242
5.3.4	Packet Sniffing	244
5.4	The Transport Layer	246
5.4.1	Transmission Control Protocol (TCP)	246
5.4.2	User Datagram Protocol (UDP)	250
5.4.3	Network Address Translation (NAT)	251
5.4.4	TCP Session Hijacking	253
5.5	Denial-of-Service Attacks	256
5.5.1	ICMP Attacks	256
5.5.2	SYN Flood Attacks	258
5.5.3	Optimistic TCP ACK Attack	260
5.5.4	Distributed Denial-of-Service	261
5.5.5	IP Traceback	262
5.6	Exercises	264
6	Network Security II	269
6.1	The Application Layer and DNS	270
6.1.1	A Sample of Application-Layer Protocols	270
6.1.2	The Domain Name System (DNS)	271
6.1.3	DNS Attacks	278
6.1.4	DNSSEC	285
6.2	Firewalls	287
6.2.1	Firewall Policies	288
6.2.2	Stateless and Stateful Firewalls	289
6.3	Tunneling	292
6.3.1	Secure Shell (SSH)	293
6.3.2	IPsec	294
6.3.3	Virtual Private Networking (VPN)	297
6.4	Intrusion Detection	299
6.4.1	Intrusion Detection Events	302
6.4.2	Rule-Based Intrusion Detection	305
6.4.3	Statistical Intrusion Detection	306
6.4.4	Port Scanning	308
6.4.5	Honeypots	312
6.5	Wireless Networking	313
6.5.1	Wireless Technologies	314
6.5.2	Wired Equivalent Privacy (WEP)	315

6.5.3	Wi-Fi Protected Access (WPA)	318
6.6	Exercises	322
7	Web Security	327
7.1	The World Wide Web	328
7.1.1	HTTP and HTML	328
7.1.2	HTTPS	334
7.1.3	Dynamic Content	339
7.1.4	Sessions and Cookies	342
7.2	Attacks on Clients	347
7.2.1	Session Hijacking	347
7.2.2	Phishing	349
7.2.3	Click-Jacking	351
7.2.4	Vulnerabilities in Media Content	352
7.2.5	Privacy Attacks	356
7.2.6	Cross-Site Scripting (XSS)	357
7.2.7	Cross-Site Request Forgery (CSRF)	364
7.2.8	Defenses Against Client-Side Attacks	366
7.3	Attacks on Servers	368
7.3.1	Server-Side Scripting	368
7.3.2	Server-Side Script Inclusion Vulnerabilities	370
7.3.3	Databases and SQL Injection Attacks	372
7.3.4	Denial-of-Service Attacks	378
7.3.5	Web Server Privileges	379
7.3.6	Defenses Against Server-Side Attacks	380
7.4	Exercises	382
8	Cryptography	387
8.1	Symmetric Cryptography	388
8.1.1	Attacks	389
8.1.2	Substitution Ciphers	391
8.1.3	One-Time Pads	393
8.1.4	Pseudo-Random Number Generators	395
8.1.5	The Hill Cipher and Transposition Ciphers	397
8.1.6	The Advanced Encryption Standard (AES)	399
8.1.7	Modes of Operation	402
8.2	Public-Key Cryptography	406
8.2.1	Modular Arithmetic	406
8.2.2	The RSA Cryptosystem	410
8.2.3	The Elgamal Cryptosystem	413
8.2.4	Key Exchange	415
8.3	Cryptographic Hash Functions	417

6.5.3	Wi-Fi Protected Access (WPA)	318
6.6	Exercises	322
7	Web Security	327
7.1	The World Wide Web	328
7.1.1	HTTP and HTML	328
7.1.2	HTTPS	334
7.1.3	Dynamic Content	339
7.1.4	Sessions and Cookies	342
7.2	Attacks on Clients	347
7.2.1	Session Hijacking	347
7.2.2	Phishing	349
7.2.3	Click-Jacking	351
7.2.4	Vulnerabilities in Media Content	352
7.2.5	Privacy Attacks	356
7.2.6	Cross-Site Scripting (XSS)	357
7.2.7	Cross-Site Request Forgery (CSRF)	364
7.2.8	Defenses Against Client-Side Attacks	366
7.3	Attacks on Servers	368
7.3.1	Server-Side Scripting	368
7.3.2	Server-Side Script Inclusion Vulnerabilities	370
7.3.3	Databases and SQL Injection Attacks	372
7.3.4	Denial-of-Service Attacks	378
7.3.5	Web Server Privileges	379
7.3.6	Defenses Against Server-Side Attacks	380
7.4	Exercises	382
8	Cryptography	387
8.1	Symmetric Cryptography	388
8.1.1	Attacks	389
8.1.2	Substitution Ciphers	391
8.1.3	One-Time Pads	393
8.1.4	Pseudo-Random Number Generators	395
8.1.5	The Hill Cipher and Transposition Ciphers	397
8.1.6	The Advanced Encryption Standard (AES)	399
8.1.7	Modes of Operation	402
8.2	Public-Key Cryptography	406
8.2.1	Modular Arithmetic	406
8.2.2	The RSA Cryptosystem	410
8.2.3	The Elgamal Cryptosystem	413
8.2.4	Key Exchange	415
8.3	Cryptographic Hash Functions	417

8.3.1	Properties and Applications	417
8.3.2	Birthday Attacks	419
8.4	Digital Signatures	421
8.4.1	The RSA Signature Scheme	422
8.4.2	The Elgamal Signature Scheme	423
8.4.3	Using Hash Functions with Digital Signatures	424
8.5	Details of AES and RSA Cryptography	425
8.5.1	Details for AES	425
8.5.2	Details for RSA	431
8.6	Exercises	439
9	Security Models and Practice	445
9.1	Policy, Models, and Trust	446
9.1.1	Security Policy	446
9.1.2	Security Models	447
9.1.3	Trust Management	448
9.2	Access-Control Models	450
9.2.1	The Bell-La Padula Model	450
9.2.2	Other Access-Control Models	454
9.2.3	Role-Based Access Control	456
9.3	Security Standards and Evaluation	460
9.3.1	Orange Book and Common Criteria	460
9.3.2	Government Regulations and Standards	462
9.4	Software Vulnerability Assessment	464
9.4.1	Static and Dynamic Analysis	465
9.4.2	Exploit Development and Vulnerability Disclosure	468
9.5	Administration and Auditing	470
9.5.1	System Administration	470
9.5.2	Network Auditing and Penetration Testing	473
9.6	Kerberos	475
9.6.1	Kerberos Tickets and Servers	475
9.6.2	Kerberos Authentication	476
9.7	Secure Storage	479
9.7.1	File Encryption	479
9.7.2	Disk Encryption	481
9.7.3	Trusted Platform Module	482
9.8	Exercises	484
10	Distributed-Applications Security	487
10.1	Database Security	488
10.1.1	Tables and Queries	489
10.1.2	Updates and the Two-Phase Commit Protocol	491

10.1.3 Database Access Control	493
10.1.4 Sensitive Data	497
10.2 Email Security	500
10.2.1 How Email Works	500
10.2.2 Encryption and Authentication	502
10.2.3 Spam	507
10.3 Payment Systems and Auctions	513
10.3.1 Credit Cards	513
10.3.2 Digital Cash	516
10.3.3 Online Auctions	518
10.4 Digital-Rights Management	519
10.4.1 Digital-Media Rights Techniques	520
10.4.2 Digital-Media Rights Practice	523
10.4.3 Software Licensing Schemes	525
10.4.4 Legal Issues	527
10.5 Social Networking	528
10.5.1 Social Networks as Attack Vectors	528
10.5.2 Privacy	529
10.6 Voting Systems	531
10.6.1 Security Goals	531
10.6.2 ThreeBallot	532
10.7 Exercises	535