

THIRD EDITION

SECURITY ENGINEERING

.....

**A GUIDE TO
BUILDING DEPENDABLE
DISTRIBUTED SYSTEMS**

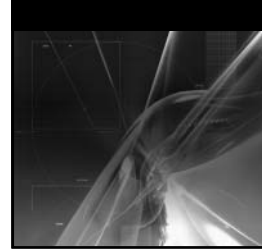
ROSS ANDERSON

.....

WILEY

Security Engineering

Third Edition



Security Engineering

**A Guide to Building Dependable
Distributed Systems
Third Edition**

Ross Anderson

WILEY

Copyright © 2020 by Ross Anderson
Published by John Wiley & Sons, Inc., Indianapolis, Indiana
Published simultaneously in Canada and the United Kingdom

ISBN: 978-1-119-64278-7
ISBN: 978-1-119-64283-1 (ebk)
ISBN: 978-1-119-64281-7 (ebk)

Manufactured in the United States of America

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, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at www.wiley.com/go/permissions.

Limit of Liability/Disclaimer of Warranty: The publisher and the author make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the publisher nor the author shall be liable for damages arising herefrom. The fact that an organization or Web site is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or website may provide or recommendations it may make. Further, readers should be aware that Internet websites listed in this work may have changed or disappeared between when this work was written and when it is read.

For general information on our other products and services please contact our Customer Care Department within the United States at (877) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may download this material at booksupport.wiley.com. For more information about Wiley products, visit www.wiley.com.

Library of Congress Control Number: 2020948679

Trademarks: Wiley and the Wiley logo are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates, in the United States and other countries, and may not be used without written permission. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc. is not associated with any product or vendor mentioned in this book.

For Shireen, Bavani, Nav, Ivan, Lily-Rani, Veddle and Bella



About the Author

I've worked with systems for over forty years. I graduated in mathematics and natural science from Cambridge in the 1970s, and got a qualification in computer engineering; my first proper job was in avionics; and after getting interested in cryptology and computer security, I worked in the banking industry in the 1980s. I then started working for companies who designed equipment for banks, and then on related applications such as prepayment electricity meters.

I moved to academia in 1992 but continued to consult to industry on security technology. During the 1990s, the number of applications that used cryptology rose rapidly: burglar alarms, car door locks, road toll tags and satellite TV systems all made their appearance. The first legal disputes about these systems came along, and I was lucky enough to be an expert witness in some of the important cases. The research team I lead had the good fortune to be in the right place at the right time when technologies such as peer-to-peer systems, tamper-resistance and digital watermarking became hot topics.

After I'd taught security and cryptology to students for a few years, it became clear to me that the existing textbooks were too narrow and theoretical: the security textbooks focused on the access control mechanisms in operating systems, while the cryptology books developed the theory behind cryptographic algorithms and protocols. These topics are interesting, and important. But they're only part of the story. Most working engineers are not overly concerned with crypto or operating system internals, but with getting good tools and learning how to use them effectively. The inappropriate use of protection mechanisms is one of the main causes of security failure. I was encouraged by the positive reception of a number of articles I wrote on security engineering (starting with 'Why Cryptosystems Fail' in 1993).

Finally, in 1999, I got round to rewriting my class lecture notes and a number of real-world case studies into a book for a general technical audience.

The first edition of the book, which appeared in 2001, helped me consolidate my thinking on the economics of information security, as I found that when I pulled my experiences about some field together into a narrative, the backbone of the story was often the incentives that the various players had faced. As the first edition of this book established itself as the standard textbook in the field, I worked on establishing security economics as a discipline. In 2002, we started the Workshop on the Economics of Information Security to bring researchers and practitioners together.

By the time the second edition came out in 2008, it was clear we'd not paid enough attention to the psychology of security either. Although we'd worked on security usability from the 1990s, there's much more to it than that. We need to understand everything from the arts of deception to how people's perception of risk is manipulated. So in 2008 we started the Workshop on Security and Human Behaviour to get security engineers talking to psychologists, anthropologists, philosophers and even magicians.

A sabbatical in 2011, which I spent partly at Google and partly at Carnegie Mellon University, persuaded me to broaden our research group to hire psychologists and criminologists. Eventually in 2015 we set up the Cambridge Cybercrime Centre to collect lots of data on the bad things that happen online and make them available to over a hundred researchers worldwide. This hasn't stopped us doing research on technical security; in fact it's helped us pick more relevant technical research topics.

A medic needs to understand a whole series of subjects including anatomy, physiology, biochemistry, pharmacy and psychology, and then temper this knowledge with experience of working on hundreds of cases with experienced colleagues. So also a security engineer needs to understand technical subjects like crypto, access controls, protocols and side channels; but this knowledge also needs to be honed by studying real cases. My goal in my academic career has been to pull all this together. The result you now hold in your hands.

I have learned a lot in the process; writing down what you think you know is a good way of finding out what you don't. I have also had a lot of fun. I hope you have as much fun reading it!

Ross Anderson
Cambridge, November 2020



Acknowledgements

A great many people have helped in various ways with the third edition of this book. I put the chapters online for comment as I wrote them, and I owe thanks to the many people who read them and pointed out assorted errors and obscurities. They are: Mansoor Ahmed, Sam Ainsworth, Peter Allan, Amit Seal Ami, James Andrews, Tom Auger, Asokan, Maria Bada, Daniel Bates, Craig Bauer, Pilgrim Beart, Gerd Beuster, Johann Bezuidenhout, Fred Bone, Matt Brockman, Nick Bohm, Fred Bone, Phil Booth, Lorenzo Cavallaro, David Chaiken, Yi Ting Chua, Valerio Cini, Ben Collier, Hugo Connery, Lachlan Cooper, Franck Courbon, Christopher Cowan, Ot van Daalen, Ezra Darshan, Roman Dickmann, Saar Drimer, Charles Duffy, Marlena Erdos, Andy Farnell, Bob Fenichel, David Fernée, Alexis FitzGerald, Jean-Alain Fournier, Jordan Frank, Steve Friedl, Jerry Gamache, Alex Gantman, Ben Gardiner, Jon Geater, Stuart Gentry, Cam Gerlach, John Gilmore, Jan Goette, Ralph Gross, Cyril Guerin, Pedram Hayati, Chengying He, Matt Hermannson, Alex Hicks, Ross Hinds, Timothy Howell, Nick Humphrey, James Humphry, Duncan Hurwood, Gary Irvine, Erik Itland, Christian Jeschke, Gary Johnson, Doug Jones, Henrik Karlzen, Joud Khoury, Jon Kilian, Timm Korte, Ronny Kuckuck, Mart Kung, Jay Lala, Jack Lang, Susan Landau, Peter Landrock, Carl Landwehr, Peter Lansley, Jeff Leese, Jochen Leidner, Tom de Leon, Andrew Lewis, David Lewis, Steve Lipner, Jim Lippard, Liz Louis, Simon Luyten, Christian Mainka, Dhruv Malik, Ivan Marsa-Maestra, Phil Maud, Patrick McCorry, TJ McIntyre, Marco Mesturino, Luke Mewburn, Spencer Moss, Steven Murdoch, Arvind Narayanan, Lakshmi Narayanan, Kristi Nikolla, Greg Norcie, Stanislav Ochotnický, Andy Ozment, Deborah Peel, Stephen Perlmutter, Tony Plank, William Porquet, David Pottage, Mark Quevedo, Roderick Rees, Larry Reeves, Philipp Reisinger, Mark Richards, Niklas Rosencrantz, Andy Sayler, Philipp

Schaumann, Christian Schneider, Ben Scott, Jean-Pierre Seifert, Mark Shawyer, Adam Shostack, Ilia Shumailov, Barbara Simons, Sam Smith, Saija Sorsa, Michael Specter, Chris Tarnowski, Don Taylor, Andrew Thaeler, Kurt Thomas, Anthony Vance, Jonas Vautherin, Alex Vetterl, Jeffrey Walton, Andrew Watson, Debora Weber-Wulff, Nienke Weiland, David White, Blake Wiggs, Robin Wilton, Ron Woerner, Bruno Wolff, Stuart Wray, Jeff Yan, Tom Yates, Andrew Yeomans, Haarooun Yousaf, Tim Zander and Yiren Zhao. I am also grateful to my editors at Wiley, Tom Dinse, Jim Minatel and Pete Gaughan, and to my copyeditors Judy Flynn and Kim Wimpsett, who have all helped make the process run smoothly.

The people who contributed in various ways to the first and second editions included the late Anne Anderson, Adam Atkinson, Jean Bacon, Robin Ball, Andreas Bender, Alastair Beresford, Johann Bezuidenhout, Maximilian Blochberger, David Boddie, Kristof Boeynaems, Nick Bohm, Mike Bond, Richard Bondi, Robert Brady, Martin Brain, John Brazier, Ian Brown, Mike Brown, Nick Bohm, Richard Bondi, the late Caspar Bowden, Duncan Campbell, Piotr Carlson, Peter Chambers, Valerio Cini, Richard Clayton, Frank Clish, Jolyon Clulow, Richard Cox, Dan Cvrcek, George Danezis, James Davenport, Peter Dean, John Daugman, Whit Diffie, Roger Dingledine, Nick Drage, Austin Donnelly, Ben Dougall, Saar Drimer, Orr Dunkelman, Steve Early, Dan Eble, Mike Ellims, Jeremy Epstein, Rasit Eskicioğlu, Robert Fenichel, Fleur Fisher, Shawn Fitzgerald, Darren Foong, Shailendra Fuloria, Dan Geer, Gary Geldart, Paul Gillingwater, John Gilmore, Brian Gladman, Virgil Gligor, Bruce Godfrey, John Gordon, Gary Graunke, Rich Graveman, Wendy Grossman, Dan Hagon, Feng Hao, Tony Harminc, Pieter Hartel, David Häsäther, Bill Hey, Fay Hider, Konstantin Hyppönen, Ian Jackson, Neil Jenkins, Simon Jenkins, Roger Johnston, Oliver Jorns, Nikolaos Karapanos, the late Paul Karger, Ian Kelly, Grant Kelly, Alistair Kelman, Ronald De Keulenaer, Hyoungh Joong Kim, Patrick Koeberl, Oliver Kömmerling, Simon Kramer, Markus Kuhn, Peter Landrock, Susan Landau, Jack Lang, Jong-Hyeon Lee, the late Owen Lewis, Stephen Lewis, Paul Leyland, Jim Lippard, Willie List, Dan Lough, John McHugh, the late David MacKay, Garry McKay, Udi Manber, John Martin, Nick Mathewson, Tyler Moore, the late Bob Morris, Ira Moskowitz, Steven Murdoch, Shishir Nagaraja, Roger Nebel, the late Roger Needham, Stephan Neuhaus, Andrew Odlyzko, Mark Oeltjenbruns, Joe Osborne, Andy Ozment, Alexandros Papadopoulos, Roy Paterson, Chris Pepper, Oscar Pereira, Fabien Petitcolas, Raphael Phan, Mike Roe, Mark Rotenberg, Avi Rubin, Jerry Saltzer, Marv Schaefer, Denise Schmandt-Besserat, Gus Simmons, Sam Simpson, Sergei Skorobogatov, Matthew Slyman, Rick Smith, Sijbrand Spannenburg, the late Karen Spärck Jones, Mark Staples, Frank Stajano, Philipp Steinmetz, Nik Sultana, Don Taylor, Martin Taylor, Peter Taylor, Daniel Thomas, Paul Thomas,

Vlasios Tsiatsis, Marc Tobias, Hal Varian, Nick Volenec, Daniel Wagner-Hall, Randall Walker, Robert Watson, Keith Willis, Simon Wiseman, Stuart Wray, Jeff Yan and the late Stefek Zaba. I also owe a lot to my first publisher, Carol Long.

Through the whole process I have been supported by my family, and especially by my long-suffering wife Shireen. Each edition of the book meant over a year when I was constantly distracted. Huge thanks to all for putting up with me!



Contents at a Glance

Preface to the Third Edition	xxxvii
Preface to the Second Edition	xli
Preface to the First Edition	xlili
For my daughter, and other lawyers ...	xlvi
Foreword	xlix
Part I	
Chapter 1 What Is Security Engineering?	3
Chapter 2 Who Is the Opponent?	17
Chapter 3 Psychology and Usability	63
Chapter 4 Protocols	119
Chapter 5 Cryptography	145
Chapter 6 Access Control	207
Chapter 7 Distributed Systems	243
Chapter 8 Economics	275

Part II

Chapter 9	Multilevel Security	315
Chapter 10	Boundaries	341
Chapter 11	Inference Control	375
Chapter 12	Banking and Bookkeeping	405
Chapter 13	Locks and Alarms	471
Chapter 14	Monitoring and Metering	497
Chapter 15	Nuclear Command and Control	529
Chapter 16	Security Printing and Seals	549
Chapter 17	Biometrics	571
Chapter 18	Tamper Resistance	599
Chapter 19	Side Channels	639
Chapter 20	Advanced Cryptographic Engineering	667
Chapter 21	Network Attack and Defence	699
Chapter 22	Phones	737
Chapter 23	Electronic and Information Warfare	777
Chapter 24	Copyright and DRM	815
Chapter 25	New Directions?	865

Part III

Chapter 26	Surveillance or Privacy?	909
Chapter 27	Secure Systems Development	965
Chapter 28	Assurance and Sustainability	1015
Chapter 29	Beyond “Computer Says No”	1059
Bibliography		1061
Index		1143



Contents

Preface to the Third Edition	xxxvii
Preface to the Second Edition	xli
Preface to the First Edition	xlili
For my daughter, and other lawyers ...	xlvii
Foreword	xlix
Part I	
Chapter 1 What Is Security Engineering?	3
1.1 Introduction	3
1.2 A framework	4
1.3 Example 1 – a bank	6
1.4 Example 2 – a military base	7
1.5 Example 3 – a hospital	8
1.6 Example 4 – the home	10
1.7 Definitions	11
1.8 Summary	16
Chapter 2 Who Is the Opponent?	17
2.1 Introduction	17
2.2 Spies	19
2.2.1 The Five Eyes	19
2.2.1.1 Prism	19
2.2.1.2 Tempora	20
2.2.1.3 Muscular	21
2.2.1.4 Special collection	22

	2.2.1.5	Bullrun and Edgehill	22
	2.2.1.6	Xkeyscore	23
	2.2.1.7	Longhaul	24
	2.2.1.8	Quantum	25
	2.2.1.9	CNE	25
	2.2.1.10	The analyst's viewpoint	27
	2.2.1.11	Offensive operations	28
	2.2.1.12	Attack scaling	29
	2.2.2	China	30
	2.2.3	Russia	35
	2.2.4	The rest	38
	2.2.5	Attribution	40
2.3	Crooks		41
	2.3.1	Criminal infrastructure	42
	2.3.1.1	Botnet herders	42
	2.3.1.2	Malware devs	44
	2.3.1.3	Spam senders	45
	2.3.1.4	Bulk account compromise	45
	2.3.1.5	Targeted attackers	46
	2.3.1.6	Cashout gangs	46
	2.3.1.7	Ransomware	47
	2.3.2	Attacks on banking and payment systems	47
	2.3.3	Sectoral cybercrime ecosystems	49
	2.3.4	Internal attacks	49
	2.3.5	CEO crimes	49
	2.3.6	Whistleblowers	50
2.4	Geeks		52
2.5	The swamp		53
	2.5.1	Hacktivism and hate campaigns	54
	2.5.2	Child sex abuse material	55
	2.5.3	School and workplace bullying	57
	2.5.4	Intimate relationship abuse	57
2.6	Summary		59
	Research problems		60
	Further reading		61
Chapter 3	Psychology and Usability		63
	3.1	Introduction	63
	3.2	Insights from psychology research	64
	3.2.1	Cognitive psychology	65
	3.2.2	Gender, diversity and interpersonal variation	68

3.2.3	Social psychology	70
3.2.3.1	Authority and its abuse	71
3.2.3.2	The bystander effect	72
3.2.4	The social-brain theory of deception	73
3.2.5	Heuristics, biases and behavioural economics	76
3.2.5.1	Prospect theory and risk misperception	77
3.2.5.2	Present bias and hyperbolic discounting	78
3.2.5.3	Defaults and nudges	79
3.2.5.4	The default to intentionality	79
3.2.5.5	The affect heuristic	80
3.2.5.6	Cognitive dissonance	81
3.2.5.7	The risk thermostat	81
3.3	Deception in practice	81
3.3.1	The salesman and the scamster	82
3.3.2	Social engineering	84
3.3.3	Phishing	86
3.3.4	Opsec	88
3.3.5	Deception research	89
3.4	Passwords	90
3.4.1	Password recovery	92
3.4.2	Password choice	94
3.4.3	Difficulties with reliable password entry	94
3.4.4	Difficulties with remembering the password	95
3.4.4.1	Naïve choice	96
3.4.4.2	User abilities and training	96
3.4.4.3	Design errors	98
3.4.4.4	Operational failures	100
3.4.4.5	Social-engineering attacks	101
3.4.4.6	Customer education	102
3.4.4.7	Phishing warnings	103
3.4.5	System issues	104
3.4.6	Can you deny service?	105
3.4.7	Protecting oneself or others?	105
3.4.8	Attacks on password entry	106
3.4.8.1	Interface design	106
3.4.8.2	Trusted path, and bogus terminals	107
3.4.8.3	Technical defeats of password retry counters	107
3.4.9	Attacks on password storage	108
3.4.9.1	One-way encryption	109
3.4.9.2	Password cracking	109
3.4.9.3	Remote password checking	109

3.4.10	Absolute limits	110
3.4.11	Using a password manager	111
3.4.12	Will we ever get rid of passwords?	113
3.5	CAPTCHAs	115
3.6	Summary	116
	Research problems	117
	Further reading	118
Chapter 4	Protocols	119
4.1	Introduction	119
4.2	Password eavesdropping risks	120
4.3	Who goes there? – simple authentication	122
4.3.1	Challenge and response	124
4.3.2	Two-factor authentication	128
4.3.3	The MITM-in-the-middle attack	129
4.3.4	Reflection attacks	132
4.4	Manipulating the message	133
4.5	Changing the environment	134
4.6	Chosen protocol attacks	135
4.7	Managing encryption keys	136
4.7.1	The resurrecting duckling	137
4.7.2	Remote key management	137
4.7.3	The Needham-Schroeder protocol	138
4.7.4	Kerberos	139
4.7.5	Practical key management	141
4.8	Design assurance	141
4.9	Summary	143
	Research problems	143
	Further reading	144
Chapter 5	Cryptography	145
5.1	Introduction	145
5.2	Historical background	146
5.2.1	An early stream cipher – the Vigenère	147
5.2.2	The one-time pad	148
5.2.3	An early block cipher – Playfair	150
5.2.4	Hash functions	152
5.2.5	Asymmetric primitives	154
5.3	Security models	155
5.3.1	Random functions – hash functions	157
5.3.1.1	Properties	157
5.3.1.2	The birthday theorem	158
5.3.2	Random generators – stream ciphers	159
5.3.3	Random permutations – block ciphers	161

5.3.4	Public key encryption and trapdoor one-way permutations	163
5.3.5	Digital signatures	164
5.4	Symmetric crypto algorithms	165
5.4.1	SP-networks	165
5.4.1.1	Block size	166
5.4.1.2	Number of rounds	166
5.4.1.3	Choice of S-boxes	167
5.4.1.4	Linear cryptanalysis	167
5.4.1.5	Differential cryptanalysis	168
5.4.2	The Advanced Encryption Standard (AES)	169
5.4.3	Feistel ciphers	171
5.4.3.1	The Luby-Rackoff result	173
5.4.3.2	DES	173
5.5	Modes of operation	175
5.5.1	How not to use a block cipher	176
5.5.2	Cipher block chaining	177
5.5.3	Counter encryption	178
5.5.4	Legacy stream cipher modes	178
5.5.5	Message authentication code	179
5.5.6	Galois counter mode	180
5.5.7	XTS	180
5.6	Hash functions	181
5.6.1	Common hash functions	181
5.6.2	Hash function applications – HMAC, commitments and updating	183
5.7	Asymmetric crypto primitives	185
5.7.1	Cryptography based on factoring	185
5.7.2	Cryptography based on discrete logarithms	188
5.7.2.1	One-way commutative encryption	189
5.7.2.2	Diffie-Hellman key establishment	190
5.7.2.3	ElGamal digital signature and DSA	192
5.7.3	Elliptic curve cryptography	193
5.7.4	Certification authorities	194
5.7.5	TLS	195
5.7.5.1	TLS uses	196
5.7.5.2	TLS security	196
5.7.5.3	TLS 1.3	197
5.7.6	Other public-key protocols	197
5.7.6.1	Code signing	197
5.7.6.2	PGP/GPG	198
5.7.6.3	QUIC	199
5.7.7	Special-purpose primitives	199

5.7.8	How strong are asymmetric cryptographic primitives?	200
5.7.9	What else goes wrong	202
5.8	Summary	203
	Research problems	204
	Further reading	204
Chapter 6	Access Control	207
6.1	Introduction	207
6.2	Operating system access controls	209
6.2.1	Groups and roles	210
6.2.2	Access control lists	211
6.2.3	Unix operating system security	212
6.2.4	Capabilities	214
6.2.5	DAC and MAC	215
6.2.6	Apple's macOS	217
6.2.7	iOS	217
6.2.8	Android	218
6.2.9	Windows	219
6.2.10	Middleware	222
	6.2.10.1 Database access controls	222
	6.2.10.2 Browsers	223
6.2.11	Sandboxing	224
6.2.12	Virtualisation	225
6.3	Hardware protection	227
6.3.1	Intel processors	228
6.3.2	Arm processors	230
6.4	What goes wrong	231
6.4.1	Smashing the stack	232
6.4.2	Other technical attacks	234
6.4.3	User interface failures	236
6.4.4	Remedies	237
6.4.5	Environmental creep	238
6.5	Summary	239
	Research problems	240
	Further reading	240
Chapter 7	Distributed Systems	243
7.1	Introduction	243
7.2	Concurrency	244
7.2.1	Using old data versus paying to propagate state	245
7.2.2	Locking to prevent inconsistent updates	246
7.2.3	The order of updates	247
7.2.4	Deadlock	248

	7.2.5	Non-convergent state	249
	7.2.6	Secure time	250
	7.3	Fault tolerance and failure recovery	251
	7.3.1	Failure models	252
		7.3.1.1 Byzantine failure	252
		7.3.1.2 Interaction with fault tolerance	253
	7.3.2	What is resilience for?	254
	7.3.3	At what level is the redundancy?	255
	7.3.4	Service-denial attacks	257
	7.4	Naming	259
	7.4.1	The Needham naming principles	260
	7.4.2	What else goes wrong	263
		7.4.2.1 Naming and identity	264
		7.4.2.2 Cultural assumptions	265
		7.4.2.3 Semantic content of names	267
		7.4.2.4 Uniqueness of names	268
		7.4.2.5 Stability of names and addresses	269
		7.4.2.6 Restrictions on the use of names	269
	7.4.3	Types of name	270
	7.5	Summary	271
		Research problems	272
		Further reading	273
Chapter 8	Economics		275
	8.1	Introduction	275
	8.2	Classical economics	276
		8.2.1 Monopoly	278
	8.3	Information economics	281
		8.3.1 Why information markets are different	281
		8.3.2 The value of lock-in	282
		8.3.3 Asymmetric information	284
		8.3.4 Public goods	285
	8.4	Game theory	286
		8.4.1 The prisoners' dilemma	287
		8.4.2 Repeated and evolutionary games	288
	8.5	Auction theory	291
	8.6	The economics of security and dependability	293
		8.6.1 Why is Windows so insecure?	294
		8.6.2 Managing the patching cycle	296
		8.6.3 Structural models of attack and defence	298
		8.6.4 The economics of lock-in, tying and DRM	300
		8.6.5 Antitrust law and competition policy	302
		8.6.6 Perversely motivated guards	304

8.6.7	Economics of privacy	305
8.6.8	Organisations and human behaviour	307
8.6.9	Economics of cybercrime	308
8.7	Summary	310
	Research problems	311
	Further reading	311

Part II

Chapter 9	Multilevel Security	315
9.1	Introduction	315
9.2	What is a security policy model?	316
9.3	Multilevel security policy	318
9.3.1	The Anderson report	319
9.3.2	The Bell-LaPadula model	320
9.3.3	The standard criticisms of Bell-LaPadula	321
9.3.4	The evolution of MLS policies	323
9.3.5	The Biba model	325
9.4	Historical examples of MLS systems	326
9.4.1	SCOMP	326
9.4.2	Data diodes	327
9.5	MAC: from MLS to IFC and integrity	329
9.5.1	Windows	329
9.5.2	SELinux	330
9.5.3	Embedded systems	330
9.6	What goes wrong	331
9.6.1	Composability	331
9.6.2	The cascade problem	332
9.6.3	Covert channels	333
9.6.4	The threat from malware	333
9.6.5	Polyinstantiation	334
9.6.6	Practical problems with MLS	335
9.7	Summary	337
	Research problems	338
	Further reading	339
Chapter 10	Boundaries	341
10.1	Introduction	341
10.2	Compartmentation and the lattice model	344
10.3	Privacy for tigers	346
10.4	Health record privacy	349
10.4.1	The threat model	351
10.4.2	The BMA security policy	353
10.4.3	First practical steps	356

10.4.4	What actually goes wrong	357
10.4.4.1	Emergency care	358
10.4.4.2	Resilience	359
10.4.4.3	Secondary uses	359
10.4.5	Confidentiality – the future	362
10.4.6	Ethics	365
10.4.7	Social care and education	367
10.4.8	The Chinese Wall	369
10.5	Summary	371
	Research problems	372
	Further reading	373
Chapter 11	Inference Control	375
11.1	Introduction	375
11.2	The early history of inference control	377
11.2.1	The basic theory of inference control	378
11.2.1.1	Query set size control	378
11.2.1.2	Trackers	379
11.2.1.3	Cell suppression	379
11.2.1.4	Other statistical disclosure control mechanisms	380
11.2.1.5	More sophisticated query controls	381
11.2.1.6	Randomization	382
11.2.2	Limits of classical statistical security	383
11.2.3	Active attacks	384
11.2.4	Inference control in rich medical data	385
11.2.5	The third wave: preferences and search	388
11.2.6	The fourth wave: location and social	389
11.3	Differential privacy	392
11.4	Mind the gap?	394
11.4.1	Tactical anonymity and its problems	395
11.4.2	Incentives	398
11.4.3	Alternatives	399
11.4.4	The dark side	400
11.5	Summary	401
	Research problems	402
	Further reading	402
Chapter 12	Banking and Bookkeeping	405
12.1	Introduction	405
12.2	Bookkeeping systems	406
12.2.1	Double-entry bookkeeping	408
12.2.2	Bookkeeping in banks	408
12.2.3	The Clark-Wilson security policy model	410

12.2.4	Designing internal controls	411
12.2.5	Insider frauds	415
12.2.6	Executive frauds	416
12.2.6.1	The post office case	418
12.2.6.2	Other failures	419
12.2.6.3	Ecological validity	420
12.2.6.4	Control tuning and corporate governance	421
12.2.7	Finding the weak spots	422
12.3	Interbank payment systems	424
12.3.1	A telegraphic history of E-commerce	424
12.3.2	SWIFT	425
12.3.3	What goes wrong	427
12.4	Automatic teller machines	430
12.4.1	ATM basics	430
12.4.2	What goes wrong	433
12.4.3	Incentives and injustices	437
12.5	Credit cards	438
12.5.1	Credit card fraud	439
12.5.2	Online card fraud	440
12.5.3	3DS	443
12.5.4	Fraud engines	444
12.6	EMV payment cards	445
12.6.1	Chip cards	445
12.6.1.1	Static data authentication	446
12.6.1.2	ICVVs, DDA and CDA	450
12.6.1.3	The No-PIN attack	451
12.6.2	The preplay attack	452
12.6.3	Contactless	454
12.7	Online banking	457
12.7.1	Phishing	457
12.7.2	CAP	458
12.7.3	Banking malware	459
12.7.4	Phones as second factors	459
12.7.5	Liability	461
12.7.6	Authorised push payment fraud	462
12.8	Nonbank payments	463
12.8.1	M-Pesa	463
12.8.2	Other phone payment systems	464
12.8.3	Sofort, and open banking	465
12.9	Summary	466
	Research problems	466
	Further reading	468

Chapter 13	Locks and Alarms	471
13.1	Introduction	471
13.2	Threats and barriers	472
13.2.1	Threat model	473
13.2.2	Deterrence	474
13.2.3	Walls and barriers	476
13.2.4	Mechanical locks	478
13.2.5	Electronic locks	482
13.3	Alarms	484
13.3.1	How not to protect a painting	485
13.3.2	Sensor defeats	486
13.3.3	Feature interactions	488
13.3.4	Attacks on communications	489
13.3.5	Lessons learned	493
13.4	Summary	494
	Research problems	495
	Further reading	495
 Chapter 14	 Monitoring and Metering	 497
14.1	Introduction	497
14.2	Prepayment tokens	498
14.2.1	Utility metering	499
14.2.2	How the STS system works	501
14.2.3	What goes wrong	502
14.2.4	Smart meters and smart grids	504
14.2.5	Ticketing fraud	508
14.3	Taxi meters, tachographs and truck speed limiters	509
14.3.1	The tachograph	509
14.3.2	What goes wrong	511
	14.3.2.1 How most tachograph manipulation is done	511
	14.3.2.2 Tampering with the supply	512
	14.3.2.3 Tampering with the instrument	512
	14.3.2.4 High-tech attacks	513
14.3.3	Digital tachographs	514
	14.3.3.1 System-level problems	515
	14.3.3.2 Other problems	516
14.3.4	Sensor defeats and third-generation devices	518
14.3.5	The fourth generation – smart tachographs	518
14.4	Curfew tags: GPS as policeman	519
14.5	Postage meters	522

14.6	Summary	526
	Research problems	527
	Further reading	527
Chapter 15	Nuclear Command and Control	529
15.1	Introduction	529
15.2	The evolution of command and control	532
15.2.1	The Kennedy memorandum	532
15.2.2	Authorization, environment, intent	534
15.3	Unconditionally secure authentication	534
15.4	Shared control schemes	536
15.5	Tamper resistance and PALs	538
15.6	Treaty verification	540
15.7	What goes wrong	541
15.7.1	Nuclear accidents	541
15.7.2	Interaction with cyberwar	542
15.7.3	Technical failures	543
15.8	Secrecy or openness?	544
15.9	Summary	545
	Research problems	546
	Further reading	546
Chapter 16	Security Printing and Seals	549
16.1	Introduction	549
16.2	History	550
16.3	Security printing	551
16.3.1	Threat model	552
16.3.2	Security printing techniques	553
16.4	Packaging and seals	557
16.4.1	Substrate properties	558
16.4.2	The problems of glue	558
16.4.3	PIN mailers	559
16.5	Systemic vulnerabilities	560
16.5.1	Peculiarities of the threat model	562
16.5.2	Anti-gundecking measures	563
16.5.3	The effect of random failure	564
16.5.4	Materials control	564
16.5.5	Not protecting the right things	565
16.5.6	The cost and nature of inspection	566
16.6	Evaluation methodology	567
16.7	Summary	569
	Research problems	569
	Further reading	570

Chapter 17	Biometrics	571
	17.1 Introduction	571
	17.2 Handwritten signatures	572
	17.3 Face recognition	575
	17.4 Fingerprints	579
	17.4.1 Verifying positive or negative identity claims	581
	17.4.2 Crime scene forensics	584
	17.5 Iris codes	588
	17.6 Voice recognition and morphing	590
	17.7 Other systems	591
	17.8 What goes wrong	593
	17.9 Summary	596
	Research problems	597
	Further reading	597
Chapter 18	Tamper Resistance	599
	18.1 Introduction	599
	18.2 History	601
	18.3 Hardware security modules	601
	18.4 Evaluation	607
	18.5 Smartcards and other security chips	609
	18.5.1 History	609
	18.5.2 Architecture	610
	18.5.3 Security evolution	611
	18.5.4 Random number generators and PUFs	621
	18.5.5 Larger chips	624
	18.5.6 The state of the art	628
	18.6 The residual risk	630
	18.6.1 The trusted interface problem	630
	18.6.2 Conflicts	631
	18.6.3 The lemons market, risk dumping and evaluation games	632
	18.6.4 Security-by-obscurity	632
	18.6.5 Changing environments	633
	18.7 So what should one protect?	634
	18.8 Summary	636
	Research problems	636
	Further reading	636
Chapter 19	Side Channels	639
	19.1 Introduction	639
	19.2 Emission security	640
	19.2.1 History	641
	19.2.2 Technical surveillance and countermeasures	642

19.3	Passive attacks	645
19.3.1	Leakage through power and signal cables	645
19.3.2	Leakage through RF signals	645
19.3.3	What goes wrong	649
19.4	Attacks between and within computers	650
19.4.1	Timing analysis	651
19.4.2	Power analysis	652
19.4.3	Glitching and differential fault analysis	655
19.4.4	Rowhammer, CLKscrew and Plundervolt	656
19.4.5	Meltdown, Spectre and other enclave side channels	657
19.5	Environmental side channels	659
19.5.1	Acoustic side channels	659
19.5.2	Optical side channels	661
19.5.3	Other side-channels	661
19.6	Social side channels	663
19.7	Summary	663
	Research problems	664
	Further reading	664
Chapter 20	Advanced Cryptographic Engineering	667
20.1	Introduction	667
20.2	Full-disk encryption	668
20.3	Signal	670
20.4	Tor	674
20.5	HSMs	677
20.5.1	The xor-to-null-key attack	677
20.5.2	Attacks using backwards compatibility and time-memory tradeoffs	678
20.5.3	Differential protocol attacks	679
20.5.4	The EMV attack	681
20.5.5	Hacking the HSMs in CAs and clouds	681
20.5.6	Managing HSM risks	681
20.6	Enclaves	682
20.7	Blockchains	685
20.7.1	Wallets	688
20.7.2	Miners	689
20.7.3	Smart contracts	689
20.7.4	Off-chain payment mechanisms	691
20.7.5	Exchanges, cryptocrime and regulation	692
20.7.6	Permissioned blockchains	695
20.8	Crypto dreams that failed	695
20.9	Summary	696
	Research problems	698
	Further reading	698