



Contents

	Preface	xix
	About the Author	xxii
	Foreword	xxiii
	Acknowledgments	xxv
	Legal Notice	xxvii
Part One		1
1	What Is Security Engineering?	3
	1.1 Example 1: A Bank	4
	1.2 Example 2: An Air Force Base	5
	1.3 Example 3: A Hospital	6
	1.4 Example 4: The Home	7
	1.5 Definitions	8
	1.6 Summary	11
2	Protocols	13
	2.1 Password Eavesdropping Risks	14
	2.2 Who Goes There? Simple Authentication	15
	2.2.1 Challenge and Response	17
	2.2.2 The MIG-in-the-Middle Attack	19
	2.2.3 Reflection Attacks	20

2.3	Manipulating the Message	22
2.4	Changing the Environment	23
2.5	Chosen Protocol Attacks	24
2.6	Managing Encryption Keys	25
2.6.1	Basic Key Management	25
2.6.2	The Needham-Schroeder Protocol	26
2.6.3	Kerberos	27
2.7	Getting Formal	28
2.7.1	A Typical Smartcard Banking Protocol	29
2.7.2	The BAN Logic	29
2.7.3	Verifying the Payment Protocol	30
2.7.4	Limitations of Formal Verification	31
2.8	Summary	32
	Research Problems	32
	Further Reading	33
3	Passwords	35
3.1	Basics	36
3.2	Applied Psychology Issues	36
3.2.1	Social Engineering	37
3.2.2	Difficulties with Reliable Password Entry	37
3.2.3	Difficulties with Remembering the Password	38
3.3	System Issues	41
3.3.1	Protecting Oneself or Others?	41
3.3.2	Intrusion Detection Issues	42
3.3.3	Can Users Be Trained?	42
3.3.4	The Growing Famine for Security Data	44
3.4	Technical Protection of Passwords	45
3.4.1	Attacks on Password Entry	45
3.4.2	Attacks on Password Storage	47
3.4.3	Absolute Limits	48
3.5	Summary	49
	Research Problems	50
	Further Reading	50
4	Access Control	51
4.1	Introduction	51
4.2	Operating System Access Controls	53
4.2.1	Groups and Roles	54
4.2.2	Access Control Lists	55
4.2.3	Unix Operating System Security	55
4.2.4	Windows NT	57

4.2.5 Capabilities	58
4.2.6 Added Features in Windows 2000	59
4.2.7 Granularity	60
4.2.8 Sandboxing and Proof-Carrying Code	61
4.2.9 Object Request Brokers	61
4.3 Hardware Protection	62
4.3.1 Intel 80x86/Pentium Processors	63
4.3.2 ARM Processors	63
4.3.3 Security Processors	64
4.3.4 Other Processors	64
4.4 What Goes Wrong	65
4.4.1 Smashing the Stack	65
4.4.2 Other Technical Attacks	66
4.4.3 User Interface Failures	67
4.4.4 Why So Many Things Go Wrong	68
4.4.5 Remedies	69
4.4.6 Environmental Creep	69
4.5 Summary	70
Research Problems	71
Further Reading	71
5 Cryptography	73
5.1 Introduction	73
5.2 Historical Background	74
5.2.1 An Early Stream Cipher: The Vigenère	75
5.2.2 The One-Time Pad	76
5.2.3 An Early Block Cipher: Playfair	77
5.2.4 One-Way Functions	78
5.2.5 Asymmetric Primitives	80
5.3 The Random Oracle Model	80
5.3.1 Random Functions: Hash Functions	82
5.3.2 Random Generators: Stream Ciphers	84
5.3.3 Random Permutations: Block Ciphers	85
5.3.4 Public Key Encryption and Trapdoor One-Way Permutations	87
5.3.5 Digital Signatures	88
5.4 Symmetric Crypto Primitives	89
5.4.1 SP-Networks	89
5.4.2 The Advanced Encryption Standard (AES)	93
5.4.3 Feistel Ciphers	95
5.5 Modes of Operation	98
5.5.1 Electronic Code Book	98
5.5.2 Cipher Block Chaining	98

5.5.3	Output Feedback	99
5.5.4	Counter Encryption	100
5.5.5	Cipher Feedback	100
5.5.6	Message Authentication Code	100
5.6	Hash Functions	101
5.6.1	Extra Requirements on the Underlying Cipher	102
5.6.2	Common Hash Functions and Applications	103
5.7	Asymmetric Crypto Primitives	104
5.7.1	Cryptography Based on Factoring	105
5.7.2	Cryptography Based on Discrete Logarithms	106
5.7.3	Special-Purpose Primitives	110
5.7.4	Certification	110
5.7.5	The Strength of Asymmetric Cryptographic Primitives	112
5.8	Summary	112
	Research Problems	113
	Further Reading	113
6	Distributed Systems	115
6.1	Concurrency	115
6.1.1	Using Old Data versus Paying to Propagate State	116
6.1.2	Locking to Prevent Inconsistent Updates	117
6.1.3	Order of Updates	117
6.1.4	Deadlock	118
6.1.5	Non-convergent State	118
6.1.6	Secure Time	119
6.2	Fault Tolerance and Failure Recovery	120
6.2.1	Failure Models	120
6.2.2	What Is Resilience For?	122
6.2.3	At What Level Is the Redundancy?	123
6.2.4	Service Denial Attacks	124
6.3	Naming	124
6.3.1	The Distributed Systems View of Naming	125
6.3.2	What Else Goes Wrong	127
6.3.3	Types of Name	131
6.4	Summary	132
	Research Problems	133
	Further Reading	133
	Part Two	135
7	Multilevel Security	137
7.1	Introduction	137

7.2	What Is a Security Policy Model?	138
7.3	The Bell-LaPadula Security Policy Model	139
7.3.1	Classifications and Clearances	140
7.3.2	Information Flow Control	142
7.3.3	Standard Criticisms of Bell-LaPadula	143
7.3.4	Alternative Formulations	143
7.3.5	The Biba Model	145
7.4	Examples of Multilevel Secure Systems	146
7.4.1	SCOMP	146
7.4.2	Blacker	147
7.4.3	MLS Unix, CMWs, and Trusted Windowing	147
7.4.4	The NRL Pump	148
7.4.5	Logistics Systems	149
7.4.6	Purple Penelope	149
7.4.7	Future MLS Systems	150
7.5	What Goes Wrong	151
7.5.1	Composability	151
7.5.2	The Cascade Problem	152
7.5.3	Covert Channels	153
7.5.4	The Threat from Viruses	154
7.5.5	Polyinstantiation	154
7.5.6	Other Practical Problems	155
7.6	Broader Implications of MLS	157
7.7	Summary	159
	Research Problems	159
	Further Reading	160
8	Multilateral Security	161
8.1	Introduction	161
8.2	Compartmentation, the Chinese Wall, and the BMA Model	162
8.2.1	Compartmentation and the Lattice Model	162
8.2.2	The Chinese Wall	165
8.2.3	The BMA Model	166
8.2.4	Comparative Analysis	171
8.3	Inference Control	172
8.3.1	Basic Problems of Inference Control in Medicine	172
8.3.2	Other Applications of Inference Control	173
8.3.3	The Theory of Inference Control	174
8.3.4	Limitations of Generic Approaches	179
8.3.5	The Value of Imperfect Protection	180
8.4	The Residual Problem	181

	8.5 Summary	183
	Research Problems	183
	Further Reading	184
9	Banking and Bookkeeping	185
	9.1 Introduction	185
	9.1.1 The Origins of Bookkeeping	186
	9.1.2 Double-entry Bookkeeping	187
	9.2 How Bank Computer Systems Work	187
	9.2.1 The Clark-Wilson Security Policy Model	188
	9.2.2 Separation of Duties	189
	9.2.3 What Goes Wrong	191
	9.3 Wholesale Payment Systems	194
	9.3.1 SWIFT	194
	9.3.2 What Goes Wrong	196
	9.4 Automatic Teller Machines	197
	9.4.1 ATM Basics	198
	9.4.2 What Goes Wrong	200
	9.4.3 Practical Implications	203
	9.5 Summary	204
	Research Problems	205
	Further Reading	205
10	Monitoring Systems	207
	10.1 Introduction	207
	10.2 Alarms	208
	10.2.1 Threat Model	208
	10.2.2 How Not to Protect a Painting	210
	10.2.3 Sensor Defeats	211
	10.2.4 Feature Interactions	212
	10.2.5 Attacks on Communications	213
	10.2.6 Lessons Learned	216
	10.3 Prepayment Meters	217
	10.3.1 Utility Metering	218
	10.3.2 How the System Works	219
	10.3.3 What Goes Wrong	220
	10.4 Taximeters, Tachographs, and Truck Speed Limiters	222
	10.4.1 What Goes Wrong	224
	10.4.2 Countermeasures	225
	10.5 Summary	229
	Research Problems	229
	Further Reading	230

11	Nuclear Command and Control	231
	11.1 Introduction	231
	11.2 The Kennedy Memorandum	232
	11.3 Unconditionally Secure Authentication Codes	233
	11.4 Shared Control Schemes	234
	11.5 Tamper Resistance and PALs	236
	11.6 Treaty Verification	237
	11.7 What Goes Wrong	238
	11.8 Secrecy or Openness?	240
	11.9 Summary	240
	Research Problem	241
	Further Reading	241
12	Security Printing and Seals	243
	12.1 Introduction	243
	12.2 History	244
	12.3 Security Printing	245
	12.3.1 Threat Model	245
	12.3.2 Security Printing Techniques	246
	12.4 Packaging and Seals	251
	12.4.1 Substrate Properties	251
	12.4.2 The Problems of Glue	252
	12.5 Systemic Vulnerabilities	252
	12.5.1 Peculiarities of the Threat Model	253
	12.5.2 Staff Diligence	254
	12.5.3 The Effect of Random Failure	255
	12.5.4 Materials Control	255
	12.5.5 Not Protecting the Right Things	256
	12.5.6 The Cost and Nature of Inspection	256
	12.6 Evaluation Methodology	257
	12.7 Summary	258
	Research Problems	259
	Further Reading	259
13	Biometrics	261
	13.1 Introduction	261
	13.2 Handwritten Signatures	262
	13.3 Face Recognition	264
	13.4 Fingerprints	265

13.5	Iris Codes	270
13.6	Voice Recognition	271
13.7	Other Systems	272
13.8	What Goes Wrong	273
13.9	Summary	275
	Research Problems	276
	Further Reading	276
14	Physical Tamper Resistance	277
14.1	Introduction	277
14.2	History	278
14.3	High-End Physically Secure Processors	279
14.4	Evaluation	284
14.5	Medium-Security Processors	285
14.5.1	The iButton	285
14.5.2	The Dallas 5002	286
14.5.3	The Capstone/Clipper Chip	287
14.6	Smartcards and Microcontrollers	288
14.6.1	Architecture	289
14.6.2	Security Evolution	290
14.6.3	The State of the Art	296
14.7	What Goes Wrong	298
14.7.1	Protecting the Wrong Things: Architectural Errors	298
14.7.2	Protecting the Wrong Things: Security-by-Obscurity and Evaluation Errors	299
14.7.3	Protecting Things Wrongly: Protocol Failure	299
14.7.4	Function Creep	301
14.8	What Should Be Protected?	302
14.9	Summary	303
	Research Problems	304
	Further Reading	304
15	Emission Security	305
15.1	Introduction	305
15.2	History	306
15.3	Technical Surveillance and Countermeasures	307
15.4	Passive Attacks	310
15.4.1	Leakage through Power and Signal Cables	310
15.4.2	Leakage through RF Signals	313
15.5	Active Attacks	315
15.5.1	Tempest Viruses	315

	15.5.2 Nonstop	316
	15.5.3 Glitching	317
	15.5.4 Differential Fault Analysis	317
	15.5.5 Combination Attacks	317
	15.5.6 Commercial Exploitation	318
	15.5.7 Defenses	318
	15.6 How Serious Are Emsec Attacks?	318
	15.6.1 Governments	319
	15.6.2 Businesses	319
	15.7 Summary	320
	Research Problems	320
	<i>Further Reading</i>	320
16	Electronic and Information Warfare	321
	16.1 Introduction	321
	16.2 Basics	322
	16.3 Communications Systems	323
	16.3.1 Signals Intelligence Techniques	324
	16.3.2 Attacks on Communications	326
	16.3.3 Protection Techniques	327
	16.3.4 Interaction Between Civil and Military Uses	331
	16.4 Surveillance and Target Acquisition	332
	16.4.1 Types of Radar	333
	16.4.2 Jamming Techniques	333
	16.4.3 Advanced Radars and Countermeasures	335
	16.4.4 Other Sensors and Multisensor Issues	336
	16.5 IFF Systems	337
	16.6 Directed Energy Weapons	338
	16.7 Information Warfare	339
	16.7.1 Definitions	340
	16.7.2 Doctrine	341
	16.7.3 Potentially Useful Lessons from Electronic Warfare	342
	16.7.4 Differences Between E-War and I-War	343
	16.8 Summary	344
	Research Problems	344
	<i>Further Reading</i>	344
17	Telecom System Security	345
	17.1 Introduction	345
	17.2 Phone Phreaking	345
	17.2.1 Attacks on Metering	346
	17.2.2 Attacks on Signalling	348
	17.2.3 Attacks on Switching and Configuration	348

17.2.4	Insecure End Systems	350
17.2.5	Feature Interaction	351
17.3	Mobile Phones	352
17.3.1	Mobile Phone Cloning	352
17.3.2	GSM System Architecture	353
17.3.3	Communications Security Mechanisms	354
17.3.4	The Next Generation: 3gpp	358
17.3.5	GSM Security: A Success or Failure?	362
17.4	Corporate Fraud	363
17.5	Summary	365
	Research Problems	365
	Further Reading	366
18	Network Attack and Defense	367
18.1	Introduction	367
18.1.1	The Most Common Attacks	367
18.1.2	Skill Issues: Script Kiddies and Packaged Defense	369
18.2	Vulnerabilities in Network Protocols	370
18.2.1	Attacks on Local Networks	370
18.2.2	Attacks Using Internet Protocols and Mechanisms	371
18.3	Defense against Network Attack	374
18.3.1	Configuration Management	374
18.3.2	Firewalls	375
18.3.3	Strengths and Limitations of Firewalls	376
18.3.4	Encryption	378
18.4	Trojans, Viruses, and Worms	379
18.4.1	Early History of Malicious Code	379
18.4.2	The Internet Worm	380
18.4.3	How Viruses and Worms Work	381
18.4.4	The Arms Race	382
18.4.5	Recent History	382
18.4.6	Antivirus Measures	383
18.5	Intrusion Detection	384
18.5.1	Types of Intrusion Detection	385
18.5.2	General Limitations of Intrusion Detection	385
18.5.3	Specific Problems Detecting Network Attacks	387
18.6	Summary	388
	Research Problems	389
	Further Reading	390
19	Protecting E-Commerce Systems	391
19.1	Introduction	391
19.2	A Telegraphic History of E-Commerce	392

19.3	An Introduction to Credit Cards	393
19.3.1	Fraud	394
19.3.2	Forgery	394
19.3.3	Automatic Fraud Detection	395
19.3.4	Economics	396
19.4	Online Credit Card Fraud: The Hype and the Reality	396
19.5	Cryptographic Protection Mechanisms	398
19.5.1	SSL	398
19.5.2	SET	400
19.5.3	PKI	401
19.5.4	EDI and Business-to-Business Systems	403
19.5.5	E-Purses and Micropayments	405
19.6	Network Economics	405
19.7	Competitive Applications and Corporate Warfare	408
19.8	What Else Goes Wrong	409
19.9	What Can a Merchant Do?	410
19.10	Summary	411
	Research Problems	411
	Further Reading	411
20	Copyright and Privacy Protection	413
20.1	Introduction	413
20.2	Copyright	415
20.2.1	Software	415
20.2.2	Books	420
20.2.3	Audio	421
20.2.4	Video and Pay-TV	423
20.2.5	DVD	430
20.3	Information Hiding	432
20.3.1	The DVD Marking Concept	433
20.3.2	General Information-Hiding Techniques	434
20.3.3	Attacks on Copyright-Marking Schemes	436
20.3.4	Applications of Copyright-Marking Schemes	439
20.4	Privacy Mechanisms	439
20.4.1	Content Hiding: PGP	440
20.4.2	Content Deniability—Steganography	442
20.4.3	Association Hiding—Remailers and the Dining Cryptographers	442
20.4.4	Association Deniability—Digital Cash	445
20.4.5	Other Applications and Issues	446
20.5	Summary	450
	Research Problems	451
	Further Reading	451

Part Three		453
21	E-Policy	455
	21.1 Introduction	455
	21.2 Cryptography Policy	456
	21.2.1 The History of Police Wiretapping	457
	21.2.2 The History of Traffic Analysis	459
	21.2.3 Communications Intelligence on Foreign Targets	461
	21.2.4 The History of Crypto Policy	464
	21.2.5 Discussion	468
	21.3 Copyright	472
	21.3.1 DMCA	473
	21.3.2 The Forthcoming European Directive and UCITA	474
	21.4 Data Protection	475
	21.4.1 European Data Protection: History	476
	21.4.2 Differences between Europe and the United States	477
	21.4.3 Current Trends	478
	21.5 Evidential Issues	480
	21.5.1 Admissibility of Evidence	480
	21.5.2 Reliability of Evidence	480
	21.5.3 Electronic Signatures	481
	21.5.4 Burden of Proof	483
	21.6 Other Public Sector Issues	484
	21.6.1 Service Delivery	484
	21.6.2 Social Exclusion and Discrimination	485
	21.6.3 Revenue Protection	486
	21.6.4 Elections	486
	21.7 Summary	486
	Research Problems	487
	Further Reading	487
22	Management Issues	489
	22.1 Introduction	489
	22.2 Managing a Security Project	490
	22.2.1 A Tale of Three Supermarkets	490
	22.2.2 Balancing Risk and Reward	491
	22.2.3 Organizational Issues	492
	22.3 Methodology	496
	22.3.1 Top-Down Design	497
	22.3.2 Iterative Design	498
	22.3.3 Lessons from Safety-Critical Systems	499
	22.4 Security Requirements Engineering	503
	22.4.1 Managing Requirements Evolution	504

	22.4.2 Managing Project Requirements	508
	22.4.3 Parallelizing the Process	510
	22.5 Risk Management	511
	22.6 Economic Issues	512
	22.7 Summary	514
	Research Problems	514
	Further Reading	515
23	System Evaluation and Assurance	517
	23.1 Introduction	517
	23.2 Assurance	518
	23.2.1 Perverse Economic Incentives	518
	23.2.2 Project Assurance	519
	23.2.3 Process Assurance	521
	23.2.4 Assurance Growth	523
	23.2.5 Evolution and Security Assurance	525
	23.3 Evaluation	526
	23.3.1 Evaluations by the Relying Party	527
	23.3.2 The Common Criteria	529
	23.3.3 What Goes Wrong	532
	23.4 Ways Forward	534
	23.4.1 Semi-Open Design	535
	23.4.2 Open Source	536
	23.4.3 Penetrate-and-Patch, CERTs, and bugtraq	537
	23.4.4 Education	538
	23.5 Summary	538
	Research Problems	539
	Further Reading	539
24	Conclusions	541
	Bibliography	545
	Index	595