



Contents

Preface to the Second Edition	xxv
Foreword by Bruce Schneier	xxvii
Preface	xxix
Acknowledgments	xxxv
Part I	
Chapter 1 What Is Security Engineering?	3
Introduction	3
A Framework	4
Example 1–A Bank	6
Example 2–A Military Base	7
Example 3–A Hospital	9
Example 4–The Home	10
Definitions	11
Summary	15
Chapter 2 Usability and Psychology	17
Introduction	17
Attacks Based on Psychology	18
Pretexting	19
Phishing	21
Insights from Psychology Research	22
What the Brain Does Worse Than the Computer	23
Perceptual Bias and Behavioural Economics	24
Different Aspects of Mental Processing	26
Differences Between People	27
Social Psychology	28
What the Brain Does Better Than Computer	30

Passwords	31
Difficulties with Reliable Password Entry	32
Difficulties with Remembering the Password	33
Naive Password Choice	34
User Abilities and Training	35
Design Errors	37
Operational Issues	39
Social-Engineering Attacks	40
Trusted Path	42
Phishing Countermeasures	43
Password Manglers	43
Client Certs or Specialist Apps	44
Using the Browser's Password Database	44
Soft Keyboards	45
Customer Education	45
Microsoft Passport	46
Phishing Alert Toolbars	47
Two-Factor Authentication	47
Trusted Computing	48
Fortified Password Protocols	49
Two-Channel Authentication	49
The Future of Phishing	50
System Issues	52
Can You Deny Service?	53
Protecting Oneself or Others?	53
Attacks on Password Entry	54
Interface Design	54
Eavesdropping	55
Technical Defeats of Password Retry Counters	55
Attacks on Password Storage	56
One-Way Encryption	56
Password Cracking	57
Absolute Limits	57
CAPTCHAs	59
Summary	60
Research Problems	61
Further Reading	61
Chapter 3 Protocols	63
Introduction	63
Password Eavesdropping Risks	65
Who Goes There? — Simple Authentication	66
Challenge and Response	70
The MIG-in-the-Middle Attack	73
Reflection Attacks	76
Manipulating the Message	78
Changing the Environment	79

Chosen Protocol Attacks	80
Managing Encryption Keys	82
Basic Key Management	83
The Needham-Schroeder Protocol	84
Kerberos	85
Practical Key Management	86
Getting Formal	87
A Typical Smartcard Banking Protocol	87
The BAN Logic	88
Verifying the Payment Protocol	89
Limitations of Formal Verification	90
Summary	91
Research Problems	92
Further Reading	92
Chapter 4 Access Control	93
Introduction	93
Operating System Access Controls	96
Groups and Roles	98
Access Control Lists	99
Unix Operating System Security	100
Apple's OS/X	101
Windows — Basic Architecture	102
Capabilities	103
Windows — Added Features	104
Middleware	107
Database Access Controls	107
General Middleware Issues	108
ORBs and Policy Languages	109
Sandboxing and Proof-Carrying Code	110
Virtualization	111
Trusted Computing	111
Hardware Protection	113
Intel Processors, and 'Trusted Computing'	114
ARM Processors	116
Security Processors	116
What Goes Wrong	117
Smashing the Stack	118
Other Technical Attacks	119
User Interface Failures	121
Why So Many Things Go Wrong	122
Remedies	124
Environmental Creep	125
Summary	126
Research Problems	127
Further Reading	127

Chapter 5	Cryptography	129
	Introduction	129
	Historical Background	130
	An Early Stream Cipher — The Vigenère	131
	The One-Time Pad	132
	An Early Block Cipher — Playfair	134
	One-Way Functions	136
	Asymmetric Primitives	138
	The Random Oracle Model	138
	Random Functions — Hash Functions	140
	Properties	141
	The Birthday Theorem	142
	Random Generators — Stream Ciphers	143
	Random Permutations — Block Ciphers	144
	Public Key Encryption and Trapdoor One-Way Permutations	146
	Digital Signatures	147
	Symmetric Crypto Primitives	149
	SP-Networks	149
	Block Size	150
	Number of Rounds	150
	Choice of S-Boxes	151
	Linear Cryptanalysis	151
	Differential Cryptanalysis	152
	Serpent	153
	The Advanced Encryption Standard (AES)	153
	Feistel Ciphers	155
	The Luby-Rackoff Result	157
	DES	157
	Modes of Operation	160
	Electronic Code Book	160
	Cipher Block Chaining	161
	Output Feedback	161
	Counter Encryption	162
	Cipher Feedback	163
	Message Authentication Code	163
	Composite Modes of Operation	164
	Hash Functions	165
	Extra Requirements on the Underlying Cipher	166
	Common Hash Functions and Applications	167
	Asymmetric Crypto Primitives	170
	Cryptography Based on Factoring	170
	Cryptography Based on Discrete Logarithms	173
	Public Key Encryption — Diffie Hellman and ElGamal	174
	Key Establishment	175
	Digital Signature	176
	Special Purpose Primitives	178

	Elliptic Curve Cryptography	179
	Certification	179
	The Strength of Asymmetric Cryptographic Primitives	181
	Summary	182
	Research Problems	183
	Further Reading	183
Chapter 6	Distributed Systems	185
	Introduction	185
	Concurrency	186
	Using Old Data Versus Paying to Propagate State	186
	Locking to Prevent Inconsistent Updates	188
	The Order of Updates	188
	Deadlock	189
	Non-Convergent State	190
	Secure Time	191
	Fault Tolerance and Failure Recovery	192
	Failure Models	193
	Byzantine Failure	193
	Interaction with Fault Tolerance	194
	What Is Resilience For?	195
	At What Level Is the Redundancy?	197
	Service-Denial Attacks	198
	Naming	200
	The Distributed Systems View of Naming	200
	What Else Goes Wrong	204
	Naming and Identity	204
	Cultural Assumptions	206
	Semantic Content of Names	207
	Uniqueness of Names	207
	Stability of Names and Addresses	208
	Adding Social Context to Naming	209
	Restrictions on the Use of Names	210
	Types of Name	211
	Summary	211
	Research Problems	212
	Further Reading	213
Chapter 7	Economics	215
	Introduction	215
	Classical Economics	216
	Monopoly	217
	Public Goods	219
	Information Economics	220
	The Price of Information	220
	The Value of Lock-In	221
	Asymmetric Information	223

Game Theory	223
The Prisoners' Dilemma	225
Evolutionary Games	226
The Economics of Security and Dependability	228
Weakest Link, or Sum of Efforts?	229
Managing the Patching Cycle	229
Why Is Windows So Insecure?	230
Economics of Privacy	232
Economics of DRM	233
Summary	234
Research Problems	235
Further Reading	235

Part II

Chapter 8	Multilevel Security	239
	Introduction	239
	What Is a Security Policy Model?	240
	The Bell-LaPadula Security Policy Model	242
	Classifications and Clearances	243
	Information Flow Control	245
	The Standard Criticisms of Bell-LaPadula	246
	Alternative Formulations	248
	The Biba Model and Vista	250
	Historical Examples of MLS Systems	252
	SCOMP	252
	Blacker	253
	MLS Unix and Compartmented Mode Workstations	253
	The NRL Pump	254
	Logistics Systems	255
	Sybard Suite	256
	Wiretap Systems	256
	Future MLS Systems	257
	Vista	257
	Linux	258
	Virtualization	260
	Embedded Systems	261
	What Goes Wrong	261
	Composability	261
	The Cascade Problem	262
	Covert Channels	263
	The Threat from Viruses	265
	Polyinstantiation	266
	Other Practical Problems	267
	Broader Implications of MLS	269

	Summary	272
	Research Problems	272
	Further Reading	272
Chapter 9	Multilateral Security	275
	Introduction	275
	Compartmentation, the Chinese Wall and the BMA Model	277
	Compartmentation and the Lattice Model	277
	The Chinese Wall	281
	The BMA Model	282
	The Threat Model	284
	The Security Policy	287
	Pilot Implementations	289
	Current Privacy Issues	290
	Inference Control	293
	Basic Problems of Inference Control in Medicine	293
	Other Applications of Inference Control	296
	The Theory of Inference Control	297
	Query Set Size Control	298
	Trackers	298
	More Sophisticated Query Controls	298
	Cell Suppression	299
	Maximum Order Control and the Lattice Model	300
	Audit Based Control	300
	Randomization	301
	Limitations of Generic Approaches	302
	Active Attacks	304
	The Value of Imperfect Protection	305
	The Residual Problem	306
	Summary	309
	Research Problems	310
	Further Reading	310
Chapter 10	Banking and Bookkeeping	313
	Introduction	313
	The Origins of Bookkeeping	315
	Double-Entry Bookkeeping	316
	A Telegraphic History of E-commerce	316
	How Bank Computer Systems Work	317
	The Clark-Wilson Security Policy Model	319
	Designing Internal Controls	320
	What Goes Wrong	324
	Wholesale Payment Systems	328
	SWIFT	329
	What Goes Wrong	331
	Automatic Teller Machines	333
	ATM Basics	334

What Goes Wrong	337
Incentives and Injustices	341
Credit Cards	343
Fraud	344
Forgery	345
Automatic Fraud Detection	346
The Economics of Fraud	347
Online Credit Card Fraud — the Hype and the Reality	348
Smartcard-Based Banking	350
EMV	351
Static Data Authentication	352
Dynamic Data Authentication	356
Combined Data Authentication	356
RFID	357
Home Banking and Money Laundering	358
Summary	361
Research Problems	362
Further Reading	363
Chapter 11 Physical Protection	365
Introduction	365
Threats and Barriers	366
Threat Model	367
Deterrence	368
Walls and Barriers	370
Mechanical Locks	372
Electronic Locks	376
Alarms	378
How not to Protect a Painting	379
Sensor Defeats	380
Feature Interactions	382
Attacks on Communications	383
Lessons Learned	386
Summary	387
Research Problems	388
Further Reading	388
Chapter 12 Monitoring and Metering	389
Introduction	389
Prepayment Meters	390
Utility Metering	392
How the System Works	393
What Goes Wrong	395
Taxi Meters, Tachographs and Truck Speed Limiters	397
The Tachograph	398
What Goes Wrong	399
How Most Tachograph Manipulation Is Done	400

Tampering with the Supply	401
Tampering with the Instrument	401
High-Tech Attacks	402
The Digital Tachograph Project	403
System Level Problems	404
Other Problems	405
The Resurrecting Duckling	407
Postage Meters	408
Summary	412
Research Problems	413
Further Reading	414
Chapter 13 Nuclear Command and Control	415
Introduction	415
The Evolution of Command and Control	417
The Kennedy Memorandum	418
Authorization, Environment, Intent	419
Unconditionally Secure Authentication	420
Shared Control Schemes	422
Tamper Resistance and PALs	424
Treaty Verification	426
What Goes Wrong	427
Secrecy or Openness?	429
Summary	430
Research Problems	430
Further Reading	430
Chapter 14 Security Printing and Seals	433
Introduction	433
History	434
Security Printing	435
Threat Model	436
Security Printing Techniques	437
Packaging and Seals	443
Substrate Properties	443
The Problems of Glue	444
PIN Mailers	445
Systemic Vulnerabilities	446
Peculiarities of the Threat Model	447
Anti-Gundecking Measures	448
The Effect of Random Failure	449
Materials Control	450
Not Protecting the Right Things	451
The Cost and Nature of Inspection	451
Evaluation Methodology	453
Summary	454
Research Problems	454
Further Reading	455

Chapter 15	Biometrics	457
	Introduction	457
	Handwritten Signatures	458
	Face Recognition	461
	Bertillonage	464
	Fingerprints	464
	Verifying Positive or Negative Identity Claims	466
	Crime Scene Forensics	469
	Iris Codes	472
	Voice Recognition	475
	Other Systems	476
	What Goes Wrong	477
	Summary	481
	Research Problems	482
	Further Reading	482
Chapter 16	Physical Tamper Resistance	483
	Introduction	483
	History	485
	High-End Physically Secure Processors	486
	Evaluation	492
	Medium Security Processors	494
	The iButton	494
	The Dallas 5000 Series	495
	FPGA Security, and the Clipper Chip	496
	Smartcards and Microcontrollers	499
	History	500
	Architecture	501
	Security Evolution	501
	The State of the Art	512
	Defense in Depth	513
	Stop Loss	513
	What Goes Wrong	514
	The Trusted Interface Problem	514
	Conflicts	515
	The Lemons Market, Risk Dumping and Evaluation	516
	Security-By-Obscurity	517
	Interaction with Policy	517
	Function Creep	518
	So What Should One Protect?	518
	Summary	520
	Research Problems	520
	Further Reading	520
Chapter 17	Emission Security	523
	Introduction	523
	History	524

Technical Surveillance and Countermeasures	526
Passive Attacks	530
Leakage Through Power and Signal Cables	530
Red/Black Separation	530
Timing Analysis	531
Power Analysis	531
Leakage Through RF Signals	534
Active Attacks	538
Tempest Viruses	538
Nonstop	539
Glitching	540
Differential Fault Analysis	540
Combination Attacks	540
Commercial Exploitation	541
Defenses	541
Optical, Acoustic and Thermal Side Channels	542
How Serious are Emsec Attacks?	544
Governments	544
Businesses	545
Summary	546
Research Problems	546
Further Reading	546
Chapter 18 API Attacks	547
Introduction	547
API Attacks on Security Modules	548
The XOR-To-Null-Key Attack	549
The Attack on the 4758	551
Multiparty Computation, and Differential Protocol Attacks	552
The EMV Attack	553
API Attacks on Operating Systems	554
Summary	555
Research Problems	557
Further Reading	557
Chapter 19 Electronic and Information Warfare	559
Introduction	559
Basics	560
Communications Systems	561
Signals Intelligence Techniques	563
Attacks on Communications	565
Protection Techniques	567
Frequency Hopping	568
DSSS	569
Burst Communications	570
Combining Covertiness and Jam Resistance	571
Interaction Between Civil and Military Uses	572

Surveillance and Target Acquisition	574
Types of Radar	574
Jamming Techniques	575
Advanced Radars and Countermeasures	577
Other Sensors and Multisensor Issues	578
IFF Systems	579
Improvised Explosive Devices	582
Directed Energy Weapons	584
Information Warfare	586
Definitions	587
Doctrine	588
Potentially Useful Lessons from Electronic Warfare	589
Differences Between E-war and I-war	591
Summary	592
Research Problems	592
Further Reading	593
Chapter 20 Telecom System Security	595
Introduction	595
Phone Phreaking	596
Attacks on Metering	596
Attacks on Signaling	599
Attacks on Switching and Configuration	601
Insecure End Systems	603
Feature Interaction	605
Mobile Phones	606
Mobile Phone Cloning	607
GSM Security Mechanisms	608
Third Generation Mobiles — 3gpp	617
Platform Security	619
So Was Mobile Security a Success or a Failure?	621
VOIP	623
Security Economics of Telecomms	624
Frauds by Phone Companies	625
Billing Mechanisms	627
Summary	630
Research Problems	631
Further Reading	632
Chapter 21 Network Attack and Defense	633
Introduction	633
Vulnerabilities in Network Protocols	635
Attacks on Local Networks	636
Attacks Using Internet Protocols and Mechanisms	638
SYN Flooding	638
Smurfing	639
Distributed Denial of Service Attacks	640

Spam	642
DNS Security and Pharming	643
Trojans, Viruses, Worms and Rootkits	644
Early History of Malicious Code	644
The Internet Worm	645
How Viruses and Worms Work	646
The History of Malware	647
Countermeasures	650
Defense Against Network Attack	652
Configuration Management and Operational Security	652
Filtering: Firewalls, Spam Filters, Censorware and Wiretaps	654
Packet Filtering	654
Circuit Gateways	655
Application Relays	655
Ingress Versus Egress Filtering	657
Architecture	657
Intrusion Detection	660
Types of Intrusion Detection	661
General Limitations of Intrusion Detection	662
Specific Problems Detecting Network Attacks	664
Encryption	665
SSH	665
WiFi	666
Bluetooth	668
HomePlug	668
IPsec	669
TLS	670
PKI	672
Topology	675
Summary	676
Research Problems	677
Further Reading	678
Chapter 22 Copyright and DRM	679
Introduction	679
Copyright	680
Software	681
Books	688
Audio	689
Video and Pay-TV	690
Typical System Architecture	690
Video Scrambling Techniques	691
Attacks on Hybrid Scrambling Systems	693
DVB	697
DVD	698
HD-DVD and Blu-ray	701
AACS — Broadcast Encryption and Traitor Tracing	701

Blu-ray and SPDC	703
General Platforms	704
Windows Media Rights Management	705
Other Online Rights-Management Systems	706
Peer-to-Peer Systems	707
Rights Management of Semiconductor IP	709
Information Hiding	710
Watermarks and Copy Generation Management	711
General Information Hiding Techniques	712
Attacks on Copyright Marking Schemes	714
Applications of Copyright Marking Schemes	718
Policy	718
The IP Lobby	720
Who Benefits?	722
Accessory Control	723
Summary	725
Research Problems	725
Further Reading	726
Chapter 23 The Bleeding Edge	727
Introduction	727
Computer Games	728
Types of Cheating	730
Aimbots and Other Unauthorized Software	732
Virtual Worlds, Virtual Economies	733
Web Applications	734
eBay	735
Google	736
Social Networking Sites	739
Privacy Technology	745
Anonymous Email — The Dining Cryptographers and Mixes	747
Anonymous Web Browsing — Tor	749
Confidential and Anonymous Phone Calls	751
Email Encryption	753
Steganography and Forensics Countermeasures	755
Putting It All Together	757
Elections	759
Summary	764
Research Problems	764
Further Reading	765
Part III	
Chapter 24 Terror, Justice and Freedom	769
Introduction	769
Terrorism	771
Causes of Political Violence	772

The Psychology of Political Violence	772
The Role of Political Institutions	774
The Role of the Press	775
The Democratic Response	775
Surveillance	776
The History of Government Wiretapping	776
The Growing Controversy about Traffic Analysis	779
Unlawful Surveillance	781
Access to Search Terms and Location Data	782
Data Mining	783
Surveillance via ISPs — Carnivore and its Offspring	784
Communications Intelligence on Foreign Targets	785
Intelligence Strengths and Weaknesses	787
The Crypto Wars	789
The Back Story to Crypto Policy	790
DES and Crypto Research	792
The Clipper Chip	793
Did the Crypto Wars Matter?	794
Export Control	796
Censorship	797
Censorship by Authoritarian Regimes	798
Network Neutrality	800
Peer-to-Peer, Hate Speech and Child Porn	801
Forensics and Rules of Evidence	803
Forensics	803
Admissibility of Evidence	806
Privacy and Data Protection	808
European Data Protection	809
Differences between Europe and the USA	810
Summary	812
Research Problems	813
Further Reading	813
Chapter 25 Managing the Development of Secure Systems	815
Introduction	815
Managing a Security Project	816
A Tale of Three Supermarkets	816
Risk Management	818
Organizational Issues	819
The Complacency Cycle and the Risk Thermostat	820
Interaction with Reliability	821
Solving the Wrong Problem	822
Incompetent and Inexperienced Security Managers	823
Moral Hazard	823
Methodology	824
Top-Down Design	826
Iterative Design	827

Lessons from Safety-Critical Systems	829
Security Requirements Engineering	834
Managing Requirements Evolution	835
Bug Fixing	836
Control Tuning and Corporate Governance	838
Evolving Environments and the Tragedy of the Commons	839
Organizational Change	841
Managing Project Requirements	842
Parallelizing the Process	844
Risk Management	846
Managing the Team	848
Summary	852
Research Problems	853
Further Reading	854
Chapter 26 System Evaluation and Assurance	857
Introduction	857
Assurance	858
Perverse Economic Incentives	858
Project Assurance	860
Security Testing	861
Formal Methods	862
Quis Custodiet?	862
Process Assurance	863
Assurance Growth	866
Evolution and Security Assurance	868
Evaluation	869
Evaluations by the Relying Party	870
The Common Criteria	873
What the Common Criteria Don't Do	876
Corruption, Manipulation and Inertia	878
Ways Forward	881
Hostile Review	882
Free and Open-Source Software	882
Semi-Open Design	884
Penetrate-and-Patch, CERTs, and Bugtraq	885
Education	886
Summary	887
Research Problems	887
Further Reading	887
Chapter 27 Conclusions	889
Bibliography	893
Index	997