

Security Engineering

A Guide to Building
Dependable Distributed Systems

Ross J Anderson

To Shireen

DRAFT
book to be published by Wiley,
February 2001
ISBN 0-471-38922-6

Version: September 2000

Contents

1	What is security engineering?	8
1.1	Example 1 – a Bank	9
1.2	Example 2 – an Air Force Base	10
1.3	Example 3 – a Hospital	11
1.4	Example 4 – the Home	12
1.5	Definitions	13
2	Protocols	18
2.1	Password Eavesdropping Risks	19
2.2	Who goes there? – simple authentication	20
2.2.1	Challenge and response	22
2.2.2	The MIG-in-the-Middle Attack	24
2.2.3	Reflection Attacks	26
2.3	Manipulating the Message	27
2.4	Changing the Environment	28
2.5	Chosen Protocol Attacks	29
2.6	Managing encryption keys	30
2.6.1	Basic key management	30
2.6.2	The Needham-Schroeder protocol	31
2.6.3	Kerberos	32
2.7	Getting Formal	33
2.7.1	A typical smartcard banking protocol	34
2.7.2	The BAN logic	34
2.7.3	Verifying the payment protocol	35
2.7.4	Limitations of formal verification	36
2.8	Summary	37

3	Passwords	39
3.1	Basics	40
3.2	Applied Psychology Issues	40
3.2.1	Social Engineering	40
3.2.2	Difficulties with Reliable Password Entry	41
3.2.3	Difficulties with Remembering the Password	42
3.2.3.1	Design errors	42
3.2.3.2	Operational issues	44
3.3	System Issues	45
3.3.1	Protecting oneself or others?	46
3.3.2	Intrusion detection issues	46
3.3.3	Can the users be trained?	47
3.3.4	The growing famine for security data	48
3.4	Technical Protection of Passwords	49
3.4.1	Attacks on password entry	49
3.4.1.1	Interface design	49
3.4.1.2	Eavesdropping	50
3.4.1.3	The need for trusted path	50
3.4.1.4	Technical defeats of password retry counters	51
3.4.1.5	Attacks via the audit trail	51
3.4.1.6	Bugs and blunders	51
3.4.1.7	One-way encryption	52
3.4.1.8	Password cracking	52
3.4.1.9	Absolute limits	53
3.4.2	Military systems	54
3.5	Summary	54
4	Access Control	56
4.1	Introduction	56
4.2	Operating system access controls	58
4.2.1	Groups and Roles	59
4.2.2	Access control lists	60
4.2.3	Unix operating system security	61
4.2.4	Windows NT	62
4.2.5	Capabilities	63
4.2.6	Added features in Windows 2000	64

4.2.7	Granularity	65
4.2.8	Sandboxing and proof-carrying code	66
4.2.9	Object request brokers	67
4.3	Hardware Protection	67
4.3.1	Intel 80x86/Pentium processors	68
4.3.2	ARM processors	69
4.3.3	Security processors	69
4.3.4	Other processors	70
4.4	What Goes Wrong	70
4.4.1	Smashing the stack	71
4.4.2	Other technical attacks	72
4.4.3	User interface failures	73
4.4.4	Why so many things go wrong	74
4.4.5	Remedies	74
4.4.6	Environmental creep	75
4.5	Summary	76
5	Cryptography	79
5.1	Introduction	79
5.2	Historical Background	80
5.2.1	An early stream cipher – the Vigenère	81
5.2.2	The One-time Pad	82
5.2.3	An early block cipher – Playfair	83
5.2.4	One-way functions	85
5.2.5	Asymmetric primitives	86
5.3	The Random Oracle Model	87
5.3.1	Random functions – hash functions	88
5.3.1.1	Properties	89
5.3.1.2	The birthday theorem	90
5.3.2	Random generators – stream ciphers	91
5.3.3	Random permutations – block ciphers	92
5.3.4	Public key encryption and trapdoor one-way permutations	94
5.3.5	Digital signatures	95
5.4	Symmetric crypto primitives	96
5.4.1	SP-networks	96
5.4.1.1	Block size	97

5.4.1.2	Number of rounds	98
5.4.1.3	Choice of S-boxes	98
5.4.1.4	Linear Cryptanalysis	98
5.4.1.5	Differential Cryptanalysis	98
5.4.1.6	Serpent	99
5.4.2	Feistel ciphers	100
5.4.2.1	The Luby-Rackoff result	102
5.4.2.2	DES	102
5.4.3	AES	104
5.5	Modes of Operation	104
5.5.1	Electronic code book	105
5.5.2	Cipher block chaining	105
5.5.3	Output feedback	106
5.5.4	Counter encryption	107
5.5.5	Cipher feedback	107
5.5.6	Message Authentication Code	108
5.6	Hash Functions	109
5.6.1	Extra requirements on the underlying cipher	109
5.6.2	Common hash functions and applications	111
5.7	Asymmetric crypto primitives	112
5.7.1	Cryptography based on factoring	112
5.7.2	Cryptography based on discrete logarithms	114
5.7.2.1	Digital signature	114
5.7.2.2	Public key encryption – Diffie Hellman and El-Gamal	115
5.7.2.3	Key establishment	116
5.7.3	Special purpose primitives	117
5.7.4	Certification	118
5.7.5	The strength of asymmetric cryptographic primitives	120
5.8	Summary	120
6	Distributed Systems	123
6.1	Concurrency	123
6.1.1	Using old data versus paying to propagate state	124
6.1.2	Locking to prevent inconsistent updates	125
6.1.3	The order of updates	125

6.1.4	Deadlock	126
6.1.5	Non-convergent state	126
6.1.6	Secure time	127
6.2	Fault Tolerance and Failure Recovery	128
6.2.1	Failure models	129
6.2.1.1	Byzantine Failure	129
6.2.1.2	Interaction with fault tolerance	129
6.2.2	What is resilience for?	130
6.2.3	At what level is the redundancy?	131
6.2.4	Service denial attacks	132
6.3	Naming	133
6.3.1	The distributed systems view of naming	133
6.3.2	What else goes wrong	136
6.3.2.1	Naming and identity	136
6.3.2.2	Cultural assumptions	137
6.3.2.3	Semantic content of names	138
6.3.2.4	Uniqueness of names	139
6.3.2.5	Stability of names and addresses	139
6.3.2.6	Restrictions on the use of names	140
6.3.3	Types of name	140
6.4	Summary	141
7	Multilevel Security	145
7.1	Introduction	145
7.2	What is a Security Policy Model?	146
7.3	The Bell-LaPadula Security Policy Model	147
7.3.1	Classifications and clearances	148
7.3.2	Information flow control	150
7.3.3	The standard criticisms of Bell-LaPadula	151
7.3.4	Alternative formulations	152
7.3.5	The Biba model	154
7.4	Examples of Multilevel Secure Systems	155
7.4.1	SCOMP	155
7.4.2	Blacker	156
7.4.3	MLS Unix, CMWs and Trusted Windowing	156
7.4.4	The NRL Pump	157

7.4.5	Logistics systems	158
7.4.6	Purple Penelope	158
7.4.7	Future MLS systems	159
7.5	What Goes Wrong	160
7.5.1	Composability	160
7.5.2	The cascade problem	161
7.5.3	Covert channels	162
7.5.4	The threat from viruses	163
7.5.5	Polyinstantiation	164
7.5.6	Other practical problems	165
7.6	Broader Implications of MLS	167
7.7	Summary	168
8	Multilateral Security	170
8.1	Introduction	170
8.2	Compartmentation, the Chinese Wall and the BMA model	171
8.2.1	Compartmentation and the lattice model	172
8.2.2	The Chinese Wall	175
8.2.3	The BMA model	176
8.2.3.1	The threat model	177
8.2.3.2	The security policy	179
8.2.3.3	Pilot implementations	181
8.2.4	Comparative analysis	181
8.3	Inference Control	182
8.3.1	Basic problems of inference control in medicine	182
8.3.2	Other applications of inference control	183
8.3.3	The theory of inference control	184
8.3.3.1	Query set size control	185
8.3.3.2	Trackers	185
8.3.3.3	More sophisticated query controls	186
8.3.3.4	Cell suppression	186
8.3.3.5	Maximum order control and the lattice model	187
8.3.3.6	Audit based control	187
8.3.3.7	Randomization	188
8.3.4	Limitations of generic approaches	189
8.3.4.1	Active attacks	190

8.3.5	The value of imperfect protection	190
8.4	The residual problem	191
8.5	Summary	193
9	Banking and Bookkeeping	195
9.1	Introduction	195
9.1.1	The origins of bookkeeping	196
9.1.2	Double entry bookkeeping	196
9.2	How bank computer systems work	197
9.2.1	The Clark-Wilson Security Policy Model	198
9.2.2	Separation of duties	199
9.2.3	What goes wrong	202
9.3	Wholesale Payment Systems	204
9.3.1	SWIFT	204
9.3.2	What goes wrong	206
9.4	Automatic Teller Machines	208
9.4.1	ATM basics	208
9.4.2	What goes wrong	211
9.4.3	Practical Implications	214
9.5	Summary	215
10	Monitoring Systems	218
10.1	Introduction	218
10.2	Alarms	219
10.2.1	Threat model	220
10.2.2	How not to protect a painting	221
10.2.3	Sensor defeats	222
10.2.4	Feature interactions	224
10.2.5	Attacks on communications	225
10.2.6	Lessons learned	227
10.3	Prepayment Meters	228
10.3.1	Example – utility metering	230
10.3.2	How the system works	231
10.3.3	What goes wrong	232
10.4	Taxi meters, tachographs and truck speed limiters	234
10.4.1	What goes wrong	235

10.4.1.1	How most tachograph manipulation is done . . .	235
10.4.1.2	Tampering with the supply	236
10.4.1.3	Tampering with the instrument	236
10.4.1.4	High-tech attacks	237
10.4.2	Countermeasures	237
10.4.2.1	Tachosmart	238
10.4.2.2	System level problems	238
10.4.2.3	Other problems	239
10.4.2.4	The resurrecting duckling	240
10.5	Summary	240
11	Nuclear Command and Control	242
11.1	Introduction	242
11.2	The Kennedy Memorandum	243
11.3	Unconditionally Secure Authentication Codes	244
11.4	Shared Control Schemes	246
11.5	Tamper Resistance and PALs	247
11.6	Treaty Verification	249
11.7	What Goes Wrong	250
11.8	Secrecy or Openness?	251
11.9	Summary	252
12	Security Printing and Seals	254
12.1	Introduction	254
12.2	History	255
12.3	Security Printing	256
12.3.1	Threat model	256
12.3.2	Security printing techniques	257
12.4	Packaging and Seals	262
12.4.1	Substrate properties	263
12.4.2	The problems of glue	263
12.5	Systemic Vulnerabilities	264
12.5.1	Peculiarities of the threat model	265
12.5.2	Staff diligence	266
12.5.3	The effect of random failure	266
12.5.4	Materials control	267

12.5.5	Not protecting the right things	268
12.5.6	The cost and nature of inspection	268
12.6	Evaluation Methodology	269
12.7	Summary	270
13	Biometrics	272
13.1	Introduction	272
13.2	Handwritten signatures	273
13.3	Face Recognition	275
13.4	Fingerprints	277
13.5	Iris codes	280
13.6	Voice recognition	282
13.7	Other systems	283
13.8	What Goes Wrong	284
13.9	Summary	286
14	Physical Tamper Resistance	288
14.1	Introduction	288
14.2	History	289
14.3	High-End Physically Secure Processors	290
14.4	Evaluation	295
14.5	Medium Security Processors	296
14.5.1	The iButton	296
14.5.2	The Dallas 5002	297
14.5.3	The Capstone/Clipper Chip	298
14.6	Smartcards and Microcontrollers	299
14.6.1	Architecture	301
14.6.2	Security evolution	301
14.6.3	The state of the art	307
14.6.3.1	Defense in depth	308
14.6.3.2	Tamper resistance versus tamper evidence	308
14.6.3.3	Stop loss	309
14.7	What Goes Wrong	309
14.7.1	Protecting the wrong things – architectural errors	309
14.7.2	Protecting the wrong things – security-by-obscurity and evaluation errors	310

14.7.3	Protecting things wrongly – protocol failure	311
14.7.4	Function creep	313
14.8	So What Should One Protect?	313
14.9	Summary	315
15	Emission Security	317
15.1	Introduction	317
15.2	History	318
15.3	Technical Surveillance and Countermeasures	319
15.4	Passive attacks	322
15.4.1	Leakage through power and signal cables	322
15.4.1.1	Red/black separation	323
15.4.1.2	Power analysis	323
15.4.2	Leakage through RF signals	325
15.5	Active Attacks	327
15.5.1	Tempest viruses	328
15.5.2	Nonstop	329
15.5.3	Glitching	329
15.5.4	Differential fault analysis	329
15.5.5	Combination attacks	330
15.5.6	Commercial exploitation	330
15.5.7	Defenses	330
15.6	How serious are Emsec attacks?	331
15.6.1	Governments	331
15.6.2	Businesses	331
15.7	Summary	332
16	Electronic and Information Warfare	334
16.1	Introduction	334
16.2	Basics	335
16.3	Communications Systems	336
16.3.1	Signals intelligence techniques	337
16.3.2	Attacks on communications	339
16.3.3	Protection techniques	340
16.3.3.1	Frequency hopping	341
16.3.3.2	DSSS	341

16.3.3.3	Burst communications	343
16.3.3.4	Combining covertness and jam resistance	343
16.3.4	Interaction between civil and military uses	345
16.4	Surveillance and Target Acquisition	346
16.4.1	Types of radar	346
16.4.2	Jamming techniques	346
16.4.3	Advanced radars and countermeasures	349
16.4.4	Other sensors and multisensor issues	350
16.5	IFF Systems	351
16.6	Directed Energy Weapons	351
16.7	Information warfare	352
16.7.1	Definitions	353
16.7.2	Doctrine	354
16.7.3	Potentially useful lessons from electronic warfare	355
16.7.4	Differences between e-war and i-war	356
16.8	Summary	357
17	Telecom System Security	358
17.1	Introduction	358
17.2	Phone Phreaking	358
17.2.1	Attacks on metering	359
17.2.2	Attacks on signaling	361
17.2.3	Attacks on switching and configuration	362
17.2.4	Insecure end systems	363
17.2.5	Feature interaction	364
17.3	Mobile Phones	365
17.3.1	Mobile phone cloning	366
17.3.2	GSM system architecture	367
17.3.3	Communications security mechanisms	367
17.3.4	The next generation – 3gpp	372
17.3.5	So was GSM security a success or a failure?	376
17.4	Corporate Fraud	377
17.5	Summary	379
18	Network Attack and Defense	381
18.1	Introduction	381

18.1.1	The most common attacks	381
18.1.2	Skill issues – script kiddies and packaged defense	383
18.2	Vulnerabilities in Network Protocols	384
18.2.1	Attacks on local networks	384
18.2.2	Attacks using internet protocols and mechanisms	385
18.2.2.1	SYN flooding	386
18.2.2.2	Smurfing	386
18.2.2.3	Distributed denial of service attacks	386
18.2.2.4	Spam and address forgery	387
18.2.2.5	Spoofing attacks	387
18.2.2.6	Routing attacks	388
18.3	Defense against network attack	388
18.3.1	Configuration Management	388
18.3.2	Firewalls	389
18.3.2.1	Packet filtering	389
18.3.2.2	Circuit gateways	390
18.3.2.3	Application relays	390
18.3.2.4	Ingress versus egress filtering	390
18.3.2.5	Combinations	391
18.3.3	Strengths and limitations of firewalls	391
18.3.4	Encryption	392
18.4	Trojans, Viruses and Worms	393
18.4.1	Early history of malicious code	394
18.4.2	The Internet Worm	394
18.4.3	How viruses and worms work	395
18.4.4	The arms race	396
18.4.5	Recent history	397
18.4.6	Antivirus measures	398
18.5	Intrusion Detection	399
18.5.1	Types of intrusion detection	399
18.5.2	General limitations of intrusion detection	400
18.5.3	Specific problems detecting network attacks	402
18.6	Summary	403
19	Protecting E-commerce Systems	405
19.1	Introduction	405

19.2	A Telegraphic History of E-commerce	406
19.3	An Introduction to Credit Cards	407
19.3.1	Fraud	408
19.3.2	Forgery	408
19.3.3	Automatic fraud detection	409
19.3.4	Economics	410
19.4	Online credit card fraud – the hype and the reality	411
19.5	Cryptographic protection mechanisms	412
19.5.1	SSL	412
19.5.2	SET	414
19.5.3	PKI	416
19.5.4	EDI and business-to-business systems	418
19.5.5	E-purses and micropayments	419
19.6	Network Economics	420
19.7	Competitive applications and corporate warfare	423
19.8	What Else Goes Wrong	424
19.9	What Can a Merchant Do?	425
19.10	Summary	426
20	Copyright and Privacy Protection	427
20.1	Introduction	427
20.2	Copyright	429
20.2.1	Software	429
20.2.2	Books	435
20.2.3	Audio	435
20.2.4	Video and pay-TV	437
20.2.4.1	Typical system architecture	438
20.2.4.2	Video scrambling techniques	439
20.2.4.3	Subscriber management techniques	441
20.2.4.4	What went wrong	441
20.2.4.5	How it was fixed	442
20.2.5	DVD	444
20.3	Information Hiding	447
20.3.1	The DVD marking concept	448
20.3.2	General information hiding techniques	448
20.3.3	Attacks on copyright marking schemes	450

20.3.4	Applications of copyright marking schemes	453
20.4	Privacy mechanisms	454
20.4.1	Content hiding – PGP	455
20.4.2	Content deniability – steganography	457
20.4.3	Association hiding – remailers and the dining cryptogra- phers	458
20.4.4	Association deniability – digital cash	460
20.4.5	Other applications and issues	461
20.4.5.1	The right to remain ignorant	461
20.4.5.2	Location security	462
20.4.5.3	Distributed systems that resist censorship	462
20.4.5.4	Subversive group computing	463
20.4.5.5	Abuse	464
20.5	Summary	465
21	E-Policy	469
21.1	Introduction	469
21.2	Cryptography Policy	470
21.2.1	The history of police wiretapping	471
21.2.2	The history of traffic analysis	473
21.2.3	Communications intelligence on foreign targets	476
21.2.4	The history of crypto policy	478
21.2.4.1	Export control	479
21.2.4.2	DES and crypto research	480
21.2.4.3	Clipper	480
21.2.4.4	European initiatives	481
21.2.4.5	Red threading and the Crypto AG case	482
21.2.5	Discussion	482
21.2.5.1	Law enforcement or intelligence?	483
21.2.5.2	Carnivore	485
21.2.5.3	Underlying policy problems	486
21.3	Copyright	487
21.3.1	DMCA	488
21.3.2	The forthcoming European Directive and UCITA	488
21.4	Data protection	490
21.4.1	European data protection	490

21.4.2	Differences between Europe and the USA	492
21.4.3	Current trends	492
21.5	Evidential issues	494
21.5.1	Admissibility of evidence	494
21.5.2	Reliability of evidence	495
21.5.3	Electronic signatures	496
21.5.4	Burden of proof	498
21.6	Other Public Sector Issues	499
21.6.1	Service delivery	499
21.6.2	Social exclusion and discrimination	500
21.6.3	Revenue protection	501
21.6.4	Elections	501
21.7	Summary	502
22	Management Issues	504
22.1	Introduction	504
22.2	Managing a Security Project	505
22.2.1	A tale of three supermarkets	505
22.2.2	Balancing risk and reward	506
22.2.3	Organizational issues	507
22.2.3.1	The complacency cycle	507
22.2.3.2	Interaction with reliability	508
22.2.3.3	Solving the wrong problem	508
22.2.3.4	Incompetent and inexperienced security managers	509
22.2.3.5	Moral hazard	510
22.3	Methodology	510
22.3.1	Top-down design	511
22.3.2	Iterative design	512
22.3.3	Lessons from safety-critical systems	514
22.4	Security Requirements Engineering	518
22.4.1	Managing requirements evolution	519
22.4.1.1	Bug fixing	519
22.4.1.2	Control tuning and corporate governance	520
22.4.1.3	Evolving environments and the tragedy of the commons	521
22.4.1.4	Organizational change	522

22.4.2	Managing project requirements	524
22.4.3	Parallelizing the process	525
22.5	Risk Management	526
22.6	Economic Issues	528
22.7	Summary	529
23	System Evaluation and Assurance	532
23.1	Introduction	532
23.2	Assurance	533
23.2.1	Perverse economic incentives	533
23.2.2	Project assurance	534
23.2.2.1	Security testing	535
23.2.2.2	Formal methods	535
23.2.2.3	Quis custodiet?	536
23.2.3	Process assurance	537
23.2.4	Assurance growth	539
23.2.5	Evolution and security assurance	541
23.3	Evaluation	541
23.3.1	Evaluations by the relying party	542
23.3.2	The Common Criteria	545
23.3.3	What goes wrong	547
23.3.3.1	Corruption, manipulation and inertia	548
23.3.3.2	Underlying problems	549
23.4	Ways Forward	550
23.4.1	Semi-open design	551
23.4.2	Open source	552
23.4.3	Penetrate-and-patch, CERTs, and bugtraq	553
23.4.4	Education	554
23.5	Summary	554
24	Conclusions	556
	Bibliography	561