

Contents

Preface		xvii
Chapter 1.	Security Concepts	1
1.1	Introduction	1
1.2	The Internet Threat Model	1
1.3	The Players	2
1.4	The Goals of Security	3
1.5	Tools of the Trade	5
1.6	Putting It All Together	15
1.7	A Simple Secure Messaging System	16
1.8	A Simple Secure Channel	17
1.9	The Export Situation	24
1.10	Real Cryptographic Algorithms	25
1.11	Symmetric Encryption: Stream Ciphers	26
1.12	Symmetric Encryption: Block Ciphers	27
1.13	Digest Algorithms	32
1.14	Key Establishment	32
1.15	Digital Signature	36
1.16	MACs	38
1.17	Key Length	39
1.18	Summary	40

Chapter 2.	Introduction to SSL	43
2.1	Introduction	43
2.2	Standards and Standards Bodies	43
2.3	SSL Overview	44
2.4	SSL/TLS Design Goals	44
2.5	SSL and the TCP/IP Suite	46
2.6	SSL History	47
2.7	SSL for the Web	51
2.8	Everything over SSL	52
2.9	Getting SSL	53
2.10	Summary	55
Chapter 3.	Basic SSL	57
3.1	Introduction	57
3.2	SSL Overview	57
3.3	Handshake	58
3.4	SSL Record Protocol	61
3.5	Putting the Pieces Together	62
3.6	A Real Connection	63
3.7	Some More Connection Details	65
3.8	SSL Specification Language	68
3.9	Handshake Message Structure	70
3.10	Handshake Messages	71
3.11	Key Derivation	82
3.12	Record Protocol	88
3.13	Alerts and Closure	91
3.14	Summary	94
Chapter 4.	Advanced SSL	95
4.1	Introduction	95
4.2	Session Resumption	96
4.3	Client Authentication	96
4.4	Ephemeral RSA	97
4.5	Rehandshake	99
4.6	Server Gated Cryptography	100
4.7	DSS and DH	102
4.8	Elliptic Curve Cipher Suites	103
4.9	Kerberos	104
4.10	FORTEZZA	104
4.11	The Story So Far	106

4.12	Session Resumption Details	106
4.13	Client Authentication Details	108
4.14	Ephemeral RSA Details	112
4.15	SGC Details	115
4.16	DH/DSS Details	124
4.17	FORTEZZA Details	126
4.18	Error Alerts	128
4.19	SSLv2 Backward Compatibility	135
4.20	Summary	137
Chapter 5.	SSL Security	139
5.1	Introduction	139
5.2	What SSL Provides	139
5.3	Protect the master_secret	140
5.4	Protect the Server's Private Key	140
5.5	Use Good Randomness	140
5.6	Check the Certificate Chain	141
5.7	Algorithm Selection	142
5.8	The Story So Far	142
5.9	Compromise of the master_secret	142
5.10	Protecting Secrets in Memory	145
5.11	Securing the Server's Private Key	146
5.12	Random Number Generation	154
5.13	Certificate Chain Verification	156
5.14	Partial Compromise	162
5.15	Known Attacks	166
5.16	Timing Cryptanalysis	167
5.17	Million Message Attack	168
5.18	Small-Subgroup Attack	170
5.19	Downgrade to Export	171
5.20	Summary	173
Chapter 6.	SSL Performance	175
6.1	Introduction	175
6.2	SSL Is Slow	175
6.3	Performance Principles	176
6.4	Cryptography Is Expensive	179
6.5	Session Resumption	181
6.6	Handshake Algorithm and Key Choice	182
6.7	Bulk Data Transfer	183
6.8	Basic SSL Performance Rules	184

6.9	The Story So Far	184
6.10	Handshake Time Allocation	184
6.11	Normal RSA Mode	186
6.12	RSA with Client Authentication	188
6.13	Ephemeral RSA	189
6.14	DSS/DHE	191
6.15	DSS/DHE with Client Authentication	194
6.16	Performance Improvements with DH	195
6.17	Record Processing	197
6.18	Java	199
6.19	SSL Servers under Load	202
6.20	Hardware Acceleration	204
6.21	Inline Hardware Accelerators	206
6.22	Network Latency	209
6.23	The Nagle Algorithm	212
6.24	Handshake Buffering	214
6.25	Advanced SSL Performance Rules	216
6.26	Summary	217
Chapter 7.	Designing with SSL	219
7.1	Introduction	219
7.2	Know What You Want to Secure	220
7.3	Client Authentication Options	221
7.4	Reference Integrity	222
7.5	Inappropriate Tasks	224
7.6	Protocol Selection	224
7.7	Reducing Handshake Overhead	227
7.8	Design Strategy	227
7.9	The Story So Far	228
7.10	Separate Ports	228
7.11	Upward Negotiation	229
7.12	Downgrade Attacks	230
7.13	Reference Integrity	233
7.14	Username/Password Authentication	235
7.15	SSL Client Authentication	236
7.16	Mutual Username/Password Authentication	238
7.17	Rehandshake	242
7.18	Secondary Channels	244
7.19	Closure	244
7.20	Summary	247

Chapter 8.	Coding with SSL	249
8.1	Introduction	249
8.2	SSL Implementations	249
8.3	Sample Programs	250
8.4	Context Initialization	252
8.5	Client Connect	258
8.6	Server Accept	263
8.7	Simple I/O Handling	265
8.8	Multiplexed I/O Using Threads	269
8.9	Multiplexed I/O with <code>select()</code>	274
8.10	Closure	282
8.11	Session Resumption	285
8.12	What's Missing?	286
8.13	Summary	288
Chapter 9.	HTTP over SSL	291
9.1	Introduction	291
9.2	Securing the Web	291
9.3	HTTP	293
9.4	HTML	295
9.5	URLs	298
9.6	HTTP Connection Behavior	300
9.7	Proxies	301
9.8	Virtual Hosts	302
9.9	Protocol Selection	302
9.10	Client Authentication	303
9.11	Reference Integrity	303
9.12	HTTPS	304
9.13	HTTPS Overview	304
9.14	URLs and Reference Integrity	307
9.15	Connection Closure	314
9.16	Proxies	316
9.17	Virtual Hosts	320
9.18	Client Authentication	322
9.19	Referrer	327
9.20	Substitution Attacks	327
9.21	Upgrade	328
9.22	Programming Issues	331
9.23	Proxy <code>CONNECT</code>	331
9.24	Handling Multiple Clients	336
9.25	Summary	341

Chapter 10.	SMTP over TLS	343
10.1	Introduction	343
10.2	Internet Mail Security	343
10.3	Internet Messaging Overview	345
10.4	SMTP	346
10.5	RFC 822 and MIME	349
10.6	E-Mail Addresses	351
10.7	Mail Relaying	352
10.8	Virtual Hosts	355
10.9	MX Records	356
10.10	Client Mail Access	357
10.11	Protocol Selection	357
10.12	Client Authentication	357
10.13	Reference Integrity	357
10.14	Connection Semantics	358
10.15	STARTTLS	358
10.16	STARTTLS Overview	358
10.17	Connection Closure	363
10.18	Requiring TLS	364
10.19	Virtual Hosts	364
10.20	Security Indicators	365
10.21	Authenticated Relaying	366
10.22	Originator Authentication	367
10.23	Reference Integrity Details	367
10.24	Why Not CONNECT?	371
10.25	What's STARTTLS Good For?	372
10.26	Programming Issues	373
10.27	Implementing STARTTLS	373
10.28	Server Startup	374
10.29	Summary	375
Chapter 11.	Contrasting Approaches	377
11.1	Introduction	377
11.2	The End-to-End Argument	378
11.3	The End-to-End Argument and SMTP	378
11.4	Other Protocols	379
11.5	IPsec	380
11.6	Security Associations	381
11.7	ISAKMP and IKE	381
11.8	AH and ESP	384
11.9	Putting It All Together: IPsec	386
11.10	IPsec versus SSL	386

11.11	Secure HTTP	389
11.12	CMS	390
11.13	Message Format	391
11.14	Cryptographic Options	392
11.15	Putting It All Together: S-HTTP	393
11.16	S-HTTP versus HTTPS	397
11.17	S/MIME	400
11.18	Basic S/MIME Formatting	401
11.19	Signing Only	401
11.20	Algorithm Choice	403
11.21	Putting It All Together: S/MIME	405
11.22	Implementation Barriers	406
11.23	S/MIME versus SMTP/TLS	407
11.24	Choosing the Appropriate Solution	408
11.25	Summary	410
Appendix A. Example Code		411
A.1	Chapter 8	411
A.1.1	C Examples	411
A.1.2	Java Examples	425
A.2	Chapter 9	431
A.2.1	HTTPS Examples	431
A.2.2	mod_ssl Session Caching	436
Appendix B. SSLv2		455
B.1	Introduction	455
B.2	SSLv2 Overview	455
B.3	Missing Features	457
B.4	Security Problems	458
B.5	PCT	461
B.6	What about SSLv1?	463
Bibliography		465
Index		475