

Contents

Chapter 1: Introduction	1
1.1 Web Security and Electronic Commerce	2
1.2 History of ssl and tls	4
1.3 Approaches to Network Security	6
1.3.1 Separate Security Protocol	8
1.3.2 Application-Specific Security	9
1.3.3 Security within Core Protocols	10
1.3.4 Parallel Security Protocol	11
1.4 Protocol Limitations	12
1.4.1 Fundamental Protocol Limitations	12
1.4.2 Tool Limitations	13
1.4.3 Environmental Limitations	14
1.5 Organization of This Book	14
Chapter 2: Basic Cryptography	17
2.1 Using Cryptography	18
2.1.1 Keeping Secrets	18
2.1.2 Proving Identity	19
2.1.3 Verifying Information	20
2.2 Types of Cryptography	21
2.2.1 Secret Key Cryptography	22
2.2.2 Public Key Cryptography	24
2.2.3 Combining Secret & Public Key Cryptography	27
2.3 Key Management	29
2.3.1 Public Key Certificates	29
2.3.2 Certificate Authorities	31
2.3.3 Certificate Hierarchies	33
2.3.4 Certificate Revocation Lists	35

Chapter 3: SSL Operation	37
3.1 SSL Roles	37
3.2 SSL Messages	38
3.3 Establishing Encrypted Communications	39
3.3.1 ClientHello	41
3.3.2 ServerHello	43
3.3.3 ServerKeyExchange	45
3.3.4 ServerHelloDone	45
3.3.5 ClientKeyExchange	45
3.3.6 ChangeCipherSpec	46
3.3.7 Finished	51
3.4 Ending Secure Communications	52
3.5 Authenticating the Server's Identity	52
3.5.1 Certificate	55
3.5.2 ClientKeyExchange	56
3.6 Separating Encryption from Authentication	56
3.6.1 Certificate	59
3.6.2 ServerKeyExchange	59
3.6.3 ClientKeyExchange	59
3.7 Authenticating the Client's Identity	60
3.7.1 CertificateRequest	61
3.7.2 Certificate	62
3.7.3 CertificateVerify	63
3.8 Resuming a Previous Session	64
Chapter 4: Message Formats	67
4.1 Transport Requirements	68
4.2 Record Layer	69
4.3 ChangeCipherSpec Protocol	71
4.4 Alert Protocol	72
4.4.1 Severity Level	72
4.4.2 Alert Description	73
4.5 Handshake Protocol	74
4.5.1 HelloRequest	76
4.5.2 ClientHello	77

4.5.3	ServerHello	79
4.5.4	Certificate	80
4.5.5	ServerKeyExchange	81
4.5.6	CertificateRequest	84
4.5.7	ServerHelloDone	85
4.5.8	ClientKeyExchange	85
4.5.9	CertificateVerify	88
4.5.10	Finished	90
4.6	Securing Messages	92
4.6.1	Message Authentication Code	93
4.6.2	Encryption	95
4.6.3	Creating Cryptographic Parameters	96
4.7	Cipher Suites	102
4.7.1	Key Exchange Algorithms	103
4.7.2	Encryption Algorithms	104
4.7.3	Hash Algorithms	104
Chapter 5: Advanced SSL		105
5.1	Compatibility with Previous Versions	105
5.1.1	Negotiating ssl Versions	106
5.1.2	SSL Version 2.0 ClientHello	109
5.1.3	SSL Version 2.0 Cipher Suites	110
5.2	Netscape International Step-Up	111
5.2.1	Server Components	112
5.2.2	Client Components	112
5.2.3	Controlling Full-Strength Encryption	113
5.3	Microsoft Server Gated Cryptography	115
5.3.1	Server Gated Cryptography Certificates	115
5.3.2	Cipher Suite Renegotiation	115
5.4	The Transport Layer Security Protocol	117
5.4.1	TLS Protocol Version	118
5.4.2	Alert Protocol Message Types	118
5.4.3	Message Authentication	121
5.4.4	Key Material Generation	123
5.4.5	CertificateVerify	125
5.4.6	Finished	126

5.4.7	Baseline Cipher Suites	126
5.4.8	Interoperability with SSL	128
5.5	The Future of ssl and tls	128
Appendix A: X.509 Certificates		131
A.1	X.509 Certificate Overview	132
A.1.1	Version	132
A.1.2	Serial Number	133
A.1.3	Algorithm Identifier	133
A.1.4	Issuer	133
A.1.5	Period of Validity	133
A.1.6	Subject	134
A.1.7	Subject's Public Key	134
A.1.8	Issuer Unique Identifier	134
A.1.9	Subject Unique Identifier	134
A.1.10	Extensions	135
A.1.11	Signature	135
A.2	Abstract Syntax Notation One	135
A.2.1	Primitive Objects	136
A.2.2	Constructed Objects	136
A.2.3	The Object Identifier Hierarchy	137
A.2.4	Tagging	139
A.2.5	Encoding Rules	142
A.3	X.509 Certificate Definition	145
A.3.1	The Certificate Object	145
A.3.2	The Version Object	146
A.3.3	The CertificateSerialNumber Object	147
A.3.4	The AlgorithmIdentifier Object	147
A.3.5	The Validity Object	148
A.3.6	The SubjectPublicKeyInfo Object	148
A.3.7	The Time Object	149
A.3.8	The Extensions Object	149
A.3.9	The UniqueIdentifier Object	150
A.3.10	The Name Object	150
A.4	Example Certificate	152

Appendix B: SSL Security Checklist	161
B.1 Authentication Issues	161
B.1.1 Certificate Authority	162
B.1.2 Certificate Signature	163
B.1.3 Certificate Validity Times	163
B.1.4 Certificate Revocation Status	163
B.1.5 Certificate Subject	163
B.1.6 Diffie-Hellman Trapdoors	164
B.1.7 Algorithm Rollback	164
B.1.8 Dropped ChangeCipherSpec Messages	165
B.2 Encryption Issues	166
B.2.1 Encryption Key Size	166
B.2.2 Traffic Analysis	167
B.2.3 The Bleichenbacher Attack	168
B.3 General Issues	170
B.3.1 RSA Key Size	170
B.3.2 Version Rollback Attacks	171
B.3.3 Premature Closure	171
B.3.4 SessionID Values	172
B.3.5 Random Number Generation	172
B.3.6 Random Number Seeding	173
References	175
Protocol Standards	175
Certificate Formats	176
Cryptographic Algorithms	177
SSL Implementations	178
Glossary	179
Index	191