

Contents

Preface	xiii
Acknowledgments	xxi
1 Introduction	1
1.1 Internet	1
1.2 WWW	4
1.3 Vulnerabilities, Threats, and Countermeasures	10
1.4 Generic Security Model	11
1.4.1 Security Policy	13
1.4.2 Host Security	14
1.4.3 Network Security	15
1.4.4 Organizational Security	17
1.4.5 Legal Security	18
2 HTTP User Authentication and Authorization	21
2.1 Introduction	21
2.2 HTTP Basic Authentication	24
2.3 HTTP Digest Authentication	27
2.4 Certificate-Based Authentication	33
2.5 Authorization and Access Control	34
2.6 Conclusions	39

3	Proxy Servers and Firewalls	41
3.1	Introduction	42
3.2	Packet Filtering and Stateful Inspection	47
3.3	Circuit-Level Gateways	51
3.4	Application-Level Gateways and Proxy Servers	55
3.5	Firewall Configurations	57
	3.5.1 Screened Subnet Firewalls	58
	3.5.2 Dual-Homed Firewalls	59
3.6	Configuring the Browser	61
	3.6.1 Netscape Navigator	62
	3.6.2 Microsoft Internet Explorer	65
3.7	Conclusions	67
4	Cryptographic Techniques	73
4.1	Introduction	74
4.2	One-Way Hash Functions	77
4.3	Secret Key Cryptography	79
4.4	Public Key Cryptography	80
4.5	Legal Issues	87
	4.5.1 Patent Claims	88
	4.5.2 Regulations	89
	4.5.3 Electronic and Digital Signature Legislation	90
4.6	Notation	91
5	Internet Security Protocols	95
5.1	Introduction	95
5.2	Network Access Layer Security Protocols	96
	5.2.1 Layer 2 Forwarding Protocol	99
	5.2.2 Point-to-Point Tunneling Protocol	99
	5.2.3 Layer 2 Tunneling Protocol	106
5.3	Internet Layer Security Protocols	107
	5.3.1 IP Security Architecture	108
	5.3.2 IP Security Protocol	110
	5.3.3 Internet Key Management Protocol	114
	5.3.4 Implementations	116
5.4	Transport Layer Security Protocols	117
	5.4.1 Secure Shell	118
	5.4.2 Secure Sockets Layer and Transport Layer Security Protocols	119

5.5	Application Layer Security Protocols	119
5.5.1	Security-Enhanced Application Protocols	120
5.5.2	Authentication and Key Distribution Systems	123
5.6	Conclusions	124
6	SSL and TLS Protocols	131
6.1	Introduction	131
6.2	SSL Protocol	133
6.2.1	SSL Record Protocol	136
6.2.2	SSL Handshake Protocol	139
6.2.3	Implementations	147
6.2.4	Performance Considerations	149
6.3	TLS Protocol	149
6.4	SSL and TLS Certificates	154
6.4.1	Personal Certificates	156
6.4.2	Site and CA Certificates	161
6.5	Firewall Tunneling	162
6.6	Conclusions	166
7	Electronic Payment Systems	171
7.1	Introduction	171
7.2	Electronic Cash Systems	177
7.2.1	eCash	179
7.2.2	CAFE	180
7.2.3	NetCash	182
7.2.4	CyberCoin	184
7.2.5	Mondex	184
7.2.6	EMV Cash Cards	185
7.3	Electronic Checks	185
7.3.1	NetBill	187
7.3.2	NetCheque	188
7.3.3	PayNow	188
7.4	Electronic Credit Card Payments	189
7.4.1	CyberCash	191
7.4.2	iKP	192
7.4.3	SEPP and STT	192
7.4.4	SET	193
7.5	Micropayment Systems	195

7.5.1	Millicent	196
7.5.2	SubScrip	198
7.5.3	PayWord	198
7.5.4	μ -iKP and MiniPay	201
7.5.5	MicroMint	201
7.6	Conclusions	203
8	Managing Certificates	207
8.1	Introduction	207
8.1.1	IETF PKIX WG	209
8.1.2	IETF SPKI WG	211
8.1.3	Attribute Certificates	214
8.2	Establishing a Public Key Infrastructure	218
8.3	Certification Service Providers	222
8.3.1	VeriSign	222
8.3.2	Swisskey	223
8.4	Certificate Revocation	224
8.4.1	CRLs	226
8.4.2	OCSP	227
8.4.3	Alternative Certificate Revocation Schemes	227
8.5	Authorization	234
8.6	Conclusions	236
9	Executable Content	241
9.1	Introduction	241
9.2	Binary Mail Attachments	245
9.3	Helper Applications and Plug-ins	245
9.4	Scripting Languages	248
9.4.1	JavaScript	248
9.4.2	VBScript	251
9.5	Java Applets	251
9.6	ActiveX Controls	263
9.7	Implications for Firewalls	268
9.8	Conclusions	269
10	CGI and API Scripts	273
10.1	Introduction	273
10.2	Safe CGI and API Programming	279

10.3	Configuring CGI and API Scripts	283
10.4	Server-Side Includes	285
10.5	Conclusions	287
11	Mobile Code and Agent-Based Systems	289
11.1	Introduction	289
11.2	Protecting the Execution Environment	293
11.2.1	Sandboxing	294
11.2.2	Digital “Shrink-Wrap”	294
11.2.3	PCC	295
11.3	Protecting the Mobile Code	297
11.3.1	Time-Limited Blackbox Security	299
11.3.2	Computing with Encrypted Functions	300
11.3.3	Cryptographic Traces	302
11.4	Conclusions and Outlook	302
12	Copyright Protection	307
12.1	Introduction	307
12.2	Watermarking	310
12.2.1	Watermark Insertion	313
12.2.2	Watermark Extraction and Detection	314
12.2.3	Possible Attacks	315
12.3	Fingerprinting	316
12.4	Conclusions	317
13	Privacy Protection and Anonymity Services	321
13.1	Introduction	322
13.2	Cookies	327
13.3	Anonymous Browsing	332
13.3.1	The Anonymizer	332
13.3.2	Onion Routing	334
13.3.3	Lucent Personalized Web Assistant	337
13.3.4	Crowds	339
13.4	Anonymous Publishing	342
13.4.1	JANUS	342
13.4.2	TAZ Servers and the Rewebber Network	345
13.5	Conclusions	348

14 Censorship on the WWW	353
14.1 Introduction	353
14.2 Content Blocking	354
14.2.1 IP Address Blocking	355
14.2.2 URL Blocking	357
14.3 Content Rating and Self-Determination	360
14.4 Conclusions	368
15 Conclusions and Outlook	371
Glossary	375
Abbreviations and Acronyms	397
About the Author	409
Index	411