

Contents

Preface	xv
References.	xx
Acknowledgments.	xxiii

1 Introduction	1
1.1 Internet.	1
1.2 WWW.	5
1.3 Vulnerabilities, threats, and countermeasures	8
1.4 Generic security model.	10
1.4.1 Security policy	12
1.4.2 Host security.	13
1.4.3 Network security.	13
1.4.4 Organizational security	16
1.4.5 Legal security.	17
References.	17

2 HTTP Security	21
2.1 HTTP.	21
2.2 User authentication, authorization, and access control	26

2.3	Basic authentication	29
2.4	Digest access authentication	34
2.5	Certificate-based authentication	41
2.6	Server configuration	42
2.6.1	<i>Configuring HTTP basic authentication</i>	42
2.6.2	<i>Configuring HTTP digest access authentication</i>	45
2.7	Conclusions	46
	References	48

3**Proxy Servers and Firewalls 49**

3.1	Introduction	49
3.2	Static packet filtering	54
3.3	Dynamic packet filtering or stateful inspection	57
3.4	Circuit-level gateways	58
3.5	Application-level gateways	64
3.6	Firewall configurations	68
3.6.1	<i>Dual-homed firewall</i>	69
3.6.2	<i>Screened host firewall</i>	71
3.6.3	<i>Screened subnet firewall</i>	72
3.7	Network address translation	74
3.8	Configuring the browser	76
3.9	Conclusions	80
	References	83

4**Cryptographic Techniques 87**

4.1	Introduction	87
4.2	Cryptographic hash functions	90
4.3	Secret key cryptography	92
4.3.1	<i>DES</i>	93
4.3.2	<i>Triple-DES</i>	93
4.3.3	<i>IDEA</i>	95
4.3.4	<i>SAFER</i>	95
4.3.5	<i>Blowfish</i>	95

4.3.6	CAST-128	95
4.3.7	RC2, RC4, RC5, and RC6.	95
4.3.8	AES	96
4.4	Public key cryptography	96
4.4.1	RSA	100
4.4.2	Diffie-Hellman	101
4.4.3	ElGamal	102
4.4.4	DSS	102
4.4.5	ECC	102
4.5	Digital envelopes	103
4.6	Protection of cryptographic keys	105
4.7	Generation of pseudorandom bit sequences.	107
4.8	Legal issues	107
4.8.1	Patent claims	108
4.8.2	Regulations	109
4.8.3	Electronic and digital signature legislation.	110
4.9	Notation	111
	References.	113

5

	Internet Security Protocols	117
5.1	Introduction	117
5.2	Network access layer security protocols.	118
5.2.1	Layer 2 Forwarding Protocol	121
5.2.2	Point-to-Point Tunneling Protocol.	122
5.2.3	Layer 2 Tunneling Protocol	124
5.2.4	Virtual private networking.	124
5.3	Internet layer security protocols	125
5.3.1	IP security architecture	128
5.3.2	IPsec protocols	131
5.3.3	IKE Protocol	136
5.3.4	Implementations	141
5.4	Transport layer security protocols	143
5.5	Application layer security protocols.	143
5.5.1	Security-enhanced application protocols	144

5.5.2	<i>Authentication and key distribution systems</i>	144
5.5.3	<i>Layering security protocols above the application layer</i>	145
5.6	Conclusions	146
	References	148

6**SSL and TLS Protocols 153**

6.1	SSL Protocol	153
6.1.1	<i>History</i>	153
6.1.2	<i>Architecture</i>	155
6.1.3	<i>SSL Record Protocol</i>	159
6.1.4	<i>SSL Handshake Protocol</i>	161
6.1.5	<i>Security analysis</i>	167
6.1.6	<i>Implementations</i>	169
6.2	TLS Protocol	171
6.3	SSL and TLS certificates	175
6.4	Firewall traversal	178
6.4.1	<i>SSL/TLS tunneling</i>	179
6.4.2	<i>SSL/TLS proxy servers</i>	181
6.5	Conclusions	182
	References	183

7**Certificate Management and Public Key Infrastructures 185**

7.1	Introduction	185
7.2	Public key certificates	187
7.2.1	<i>PGP certificates</i>	188
7.2.2	<i>X.509 certificates</i>	190
7.3	IETF PKIX WG	193
7.4	Certificate revocation	196
7.4.1	<i>CRLs</i>	198
7.4.2	<i>OCSP</i>	199
7.4.3	<i>Alternative schemes</i>	200

7.5	Certificates for the WWW	201
7.5.1	CA certificates	201
7.5.2	Server or site certificates	203
7.5.3	Personal certificates	204
7.5.4	Software publisher certificates	205
7.6	Conclusions	207
	References	210

8

Authentication and Authorization Infrastructures 213

8.1	Introduction	213
8.2	Microsoft .NET Passport	216
8.2.1	Overview	217
8.2.2	.NET Passport user accounts	219
8.2.3	.NET Passport SSI service	222
8.2.4	Complementary services	228
8.2.5	Security analysis	230
8.3	Kerberos-based AAs	231
8.3.1	Kerberos	231
8.3.2	SESAME	240
8.3.3	Windows 2000	240
8.4	PKI-based AAs	241
8.5	Conclusions	245
	References	245

9

Electronic Payment Systems 249

9.1	Introduction	249
9.2	Electronic cash systems	255
9.3	Electronic checks	257
9.4	Electronic credit-card payments	259
9.5	Micropayment systems	261
9.6	Conclusions	262
	References	264

10	Client-side Security	267
	10.1 Introduction	267
	10.2 Binary mail attachments	271
	10.3 Helper applications and plug-ins	272
	10.4 Scripting languages	275
	10.5 Java applets	278
	10.5.1 <i>Security architecture</i>	279
	10.5.2 <i>Security policy</i>	281
	10.5.3 <i>Code signing</i>	281
	10.6 ActiveX controls	283
	10.7 Security zones	288
	10.8 Implications for firewalls	291
	10.9 Conclusions	293
	References	294
11	Server-side Security	297
	11.1 Introduction	297
	11.2 CGI	300
	11.3 Server APIs	309
	11.4 FastCGI	310
	11.5 Server-side includes	311
	11.6 ASP	312
	11.7 JSP	313
	11.8 Conclusions	314
	References	314
12	Privacy Protection and Anonymity Services	317
	12.1 Introduction	317
	12.2 Early work	321
	12.3 Cookies	324
	12.4 Anonymous browsing	328
	12.4.1 <i>Anonymizing HTTP proxy servers</i>	329
	12.4.2 <i>JAP</i>	330

12.4.3	<i>Crowds</i>	330
12.4.4	<i>Onion routing</i>	333
12.4.5	<i>Freedom network</i>	336
12.5	Anonymous publishing.	336
12.5.1	<i>JANUS and the rewebber service</i>	336
12.5.2	<i>TAZ servers and the rewebber network</i>	338
12.5.3	<i>Publius</i>	340
12.6	Voluntary privacy standards	341
12.6.1	<i>Privacy seals</i>	341
12.6.2	<i>P3P</i>	342
12.7	Conclusions	343
	References.	344

13

Intellectual Property Protection 347

13.1	Introduction	347
13.2	Usage control.	349
13.3	Digital copyright labeling	351
13.3.1	<i>Introduction.</i>	351
13.3.2	<i>Categories of watermarking techniques</i>	352
13.3.3	<i>Attacks</i>	355
13.4	Digital Millenium Copyright Act	356
13.5	Conclusions	357
	References.	358

14

Censorship on the WWW 359

14.1	Introduction	359
14.2	Content blocking	360
14.2.1	<i>IP address blocking.</i>	361
14.2.2	<i>URL blocking.</i>	363
14.3	Content rating and self-determination.	365
14.4	Conclusions	371
	References.	373

15

Risk Management 375

15.1 Introduction 375

15.2 Formal risk analysis 378

15.3 Alternative approaches and technologies 379

 15.3.1 Security Scanning 379

 15.3.2 Intrusion Detection 381

15.4 Conclusions 382

References 383

16

Conclusions and Outlook 385

Abbreviations and Acronyms 389

About the Author 403

Index 405