

Inhaltsverzeichnis Sicherheit im WWW

1. Introduction	6
1.1. Internet.....	7
1.2. WWW.....	15
1.3. Vulnerabilities, threats, and countermeasures.....	20
1.4. Generic security model.....	23
2. HTTP Security	25
2.1. HTTP.....	26
2.2. User authentication authorization, and access control.....	28
2.3. Basic authentication.....	31
2.4. Digest access authentication.....	35
2.5. Certificate-based authentication.....	39
2.6. Server configuration.....	40
2.7. Conclusions.....	41
3. Proxy Servers and Firewalls	42
3.1. Introduction.....	43
3.2. Static packet filtering.....	48
3.3. Dynamic packet filtering or stateful inspection.....	50
3.4. Circuit-level gateways.....	52
3.5. Application-level gateways.....	53
3.6. Firewall configurations.....	54
3.7. Network address translation.....	56
3.8. Configuring the browser.....	57
3.9. Conclusions.....	59
4. Cryptographic Techniques	61
4.1. Introduction.....	62
4.2. Cryptographic hash functions.....	64
4.3. Secret key cryptography.....	66
4.4. Public key cryptography.....	68
4.5. Digital envelopes.....	71
4.6. Protection of cryptographic keys.....	72
4.7. Generation of pseudorandom bit sequences.....	73
4.8. Legal issues.....	74
5. Internet Security Protocols	75
5.1. Introduction.....	76
5.2. Network access layer security protocols.....	77
5.3. Internet layer security protocols.....	84
5.4. Transport layer security protocols.....	98
5.5. Application layer security protocols.....	99
5.6. Conclusions.....	100
6. SSL and TLS Protocols	101
6.1. SSL Protocol.....	102
6.2. TLS Protocol.....	111
6.3. SSL and TLS certificates.....	112
6.4. Firewall traversal.....	113
6.5. Conclusions.....	114
7. Certificate Management and Public Key Infrastructures	115
7.1. Introduction.....	116
7.2. Public key certificates.....	121
7.3. IETF PKIX WG.....	128
7.4. Certificate revocation.....	130
7.5. Certificates for the WWW.....	132
7.6. Conclusions.....	133
8. Authentication and Authorization Infrastructures	136
8.1. Introduction.....	137
8.2. Microsoft .NET Passport.....	140
8.3. Kerberos -based AAls.....	142
8.4. PKI-based AAls.....	145
8.5. Conclusions.....	149
9. Electronic Payment Systems	150
9.1. Introduction.....	151
9.2. Electronic cash systems.....	155
9.3. Electronic checks.....	156
9.4. Electronic credit-card payments.....	157
9.5. Micropayment systems.....	158
9.6. Conclusions.....	159
10. Client-side Security	160
10.1. Introduction.....	161
10.2. Binary mail attachments.....	166
10.3. Helper applications and plug-ins.....	168
10.4. Scripting languages.....	173
10.5. Java applets.....	177
10.6. ActiveX controls.....	182
10.7. Security zones.....	186
10.8. Implications for firewalls.....	187
10.9. Conclusions.....	188
11. Server-side Security	189
11.1. Introduction.....	190
11.2. CGI.....	198
11.3. Server APIs.....	206
11.4. FastCGI.....	208
11.5. Server-side includes.....	210
11.6. ASP.....	212
11.7. JSP.....	213
11.8. Conclusions.....	214
12. Privacy Protection and Anonymity Services	216
12.1. Introduction.....	217
12.2. Early work.....	221
12.3. Cookies.....	224
12.4. Anonymous browsing.....	229
12.5. Anonymous publishing.....	230
12.6. Voluntary privacy standards.....	231
12.7. Conclusions.....	233
13. Intellectual Property Protection	234
13.1. Introduction.....	235
13.2. Usage control.....	239
13.3. Digital copyright labeling.....	240
13.4. Digital Millenium Copyright Act.....	244
13.5. Conclusions.....	246
14. Censorship on the WWW	247
14.1. Introduction.....	248
14.2. Content blocking.....	249
14.3. Content rating and self-determination.....	250
14.4. Conclusions.....	255
15. Risk Management	256
15.1. Introduction.....	257
15.2. Formal risk analysis.....	258
15.3. Alternative approaches and technologies.....	260
15.4. Conclusions.....	261
16. Conclusions and Outlook	262

Inhaltsverzeichnis Alphabetisch Sicherheit im WWW

ActiveX controls	182
Alternative approaches and technologies	260
Anonymous browsing	229
Anonymous publishing	230
Application layer security protocols	99
Application-level gateways	53
ASP	212
Authentication and Authorization Infrastructures	136
Basic authentication	31
Binary mail attachments	166
Censorship on the WWW	247
Certificate Management and Public Key Infrastructures	115
Certificate revocation	130
Certificate-based authentication	39
Certificates for the WWW	132
CGI	198
Circuit-level gateways	52
Client-side Security	160
Conclusions and Outlook	262
Configuring the browser	57
Content blocking	249
Content rating and self-determination	250
Cookies	224
Cryptographic hash functions	64
Cryptographic Techniques	61
Digest access authentication	35
Digital copyright labeling	240
Digital envelopes	71
Digital Millenium Copyright Act	244
Dynamic packet filtering or stateful inspection	50
Early work	221
Electronic cash systems	155
Electronic checks	156
Electronic credit-card payments	157
Electronic Payment Systems	150
FastCGI	208
Firewall configurations	54
Firewall traversal	113
Formal risk analysis	258
Generation of pseudorandom bit sequences	73
Generic security model	23

Helper applications and plug-ins	168
HTTP Security	25
HTTP	26
IETF PKIX WG	128
Implications for firewalls	187
Intellectual Property Protection	234
Internet layer security protocols	84
Internet Security Protocols	75
Internet	7
Introduction	6
Java applets	177
JSP	213
Kerberos-based AAls	142
Legal issues	74
Micropayment systems	158
Microsoft .NET Passport	140
Network access layer security protocols	77
Network address translation	56
PKI-based AAls	145
Privacy Protection and Anonymity Services	216
Protection of cryptographic keys	72
Proxy Servers and Firewalls	42
Public key certificates	121
Public key cryptography	68
Risk Management	256
Scripting languages	173
Secret key cryptography	66
Security zones	186
Server APIs	206
Server configuration	40
Server-side includes	210
Server-side Security	189
SSL and TLS certificates	112
SSL and TLS Protocols	101
SSL Protocol	102
Static packet filtering	48
TLS Protocol	111
Transport layer security protocols	98
Usage control	239
User authentication authorization, and access control	28
Voluntary privacy standards	231
Vulnerabilities, threats, and countermeasures	20
WWW	15