

Inhaltsverzeichnis

Vorwort	vii
1 Kryptographie und das Internet	1
1.1 Was ist das Internet	2
1.2 Bedrohungen im Internet	5
1.2.1 Passive Angriffe	5
1.2.2 Aktive Angriffe	6
1.3 Kryptographie	7
1.4 Symmetrische Kryptographie	8
1.4.1 Symmetrische Verschlüsselung	9
1.4.2 Blockchiffren	10
1.4.3 Stromchiffren	12
1.4.4 Hashfunktionen	14
1.4.5 Message Authentication Codes (MAC) und Pseudozufallsfunktionen	14
1.5 Public-Key Kryptographie	15
1.5.1 Asymmetrische Verschlüsselung	16
1.5.2 Digitale Signatur	17
1.5.3 Diffie-Hellman Schlüsselvereinbarung	17
1.5.4 RSA	19
1.5.5 ElGamal	20
1.5.6 DSS und DSA	21
1.5.7 Hybride Verschlüsselung von Nachrichten	23
1.6 Kryptographische Protokolle	23
1.6.1 Username/Password	24
1.6.2 One Time Password	25
1.6.3 Challenge-and-Response	25
1.6.4 Certificate/Verify	25
1.7 Angriffe auf Kryptographische Verfahren	26
1.7.1 Angriffe auf Verschlüsselung	26
1.7.2 Padding Oracle-Angriffe auf den CBC-Modus von Blockchiffren	26
1.7.3 Angriffe auf Hashfunktionen	29
1.7.4 Angriffe auf MAC und digitale Signaturen	29
1.7.5 Angriffe auf Protokolle	29
1.8 Zertifikate	30
1.8.1 X.509	30
1.8.2 Public Key Infrastrukturen (PKI)	32
1.8.3 Gültigkeit von Zertifikaten	34
2 Point-To-Point Sicherheit	37
2.1 PPP-Sicherheit	37
2.2 PPP	38
2.3 PPP-Authentisierung	39

2.4	PPP-Verlängerungen	40
2.5	Der PPTP-Angriff von Mudge und Schneier	43
2.5.1	Wörterbuchangriffe	43
2.5.2	Übersicht PPTP-Authentifizierungsoptionen	45
2.5.3	Angriff auf Option 2	46
2.5.4	Angriff auf Option 3	46
2.6	PPTPv2	48
2.7	EAP-Protokolle	50
2.7.1	Lightweight Extensible Authentication Protocol (LEAP)	51
2.7.2	EAP-TLS	51
2.7.3	EAP-TTLS	51
2.7.4	EAP-FAST	51
2.7.5	Weitere EAP-Methoden	52
2.8	AAA: Authentication, Authorization and Accounting	52
2.8.1	RADIUS	52
2.8.2	Diameter	53
3	Drahtlose Netzwerke (WLAN)	55
3.1	Local Area Networks (LAN)	55
3.1.1	Ethernet und andere LAN-Technologien	56
3.1.2	LAN-spezifische Angriffe	57
3.1.3	Nicht-kryptographische Sicherungsmechanismen	57
3.2	Wireless LAN	58
3.2.1	Nichtkryptographische Sicherheitsfeatures von IEEE 802.11	58
3.3	Wired Equivalent Privacy (WEP)	59
3.3.1	Funktionsweise von WEP	59
3.3.2	RC4	60
3.3.3	Sicherheitsprobleme von WEP	61
3.3.4	Der Angriff von Fluhrer, Mantin und Shamir	63
3.4	Wi-Fi Protected Access (WPA)	66
3.5	IEEE 802.1X	67
3.6	IEEE 802.11i	68
4	Mobilfunk	71
4.1	GSM und GPRS	71
4.2	UMTS und LTE	74
4.3	Einbindung ins Internet: EAP	78
4.3.1	EAP-SIM	78
4.3.2	EAP-AKA	78
5	IP Sicherheit (IPSec)	79
5.1	Internet Protocol (IP)	80
5.1.1	Datenstrukturen	81
5.1.2	Routing	83
5.2	Erste Ansätze	84

5.2.1	Hybride Verschlüsselung	84
5.2.2	Simple Key Management for Internet Protocols (SKIP)	85
5.3	IPSec: Überblick	87
5.3.1	SPI und SA	87
5.3.2	Software-Module	88
5.3.3	Senden eines verschlüsselten IP-Pakets von A nach B	88
5.3.4	Einsatzmöglichkeiten	89
5.4	IPSec Datenformate	91
5.4.1	Transport und Tunnel Mode	91
5.4.2	Authentication Header	93
5.4.3	Encapsulation Security Payload (ESP)	95
5.4.4	Kryptographische Algorithmen	97
5.4.5	IPv6	98
5.5	IPSec Schlüsselmanagement	98
5.5.1	Station-to-Station Protocol	99
5.5.2	Photuris	100
5.5.3	SKEME	102
5.5.4	OAKLEY	103
5.5.5	ISAKMP	109
5.5.6	IKE	111
5.6	Neuere Entwicklungen bei IPSec	118
5.6.1	IKEv2	118
5.6.2	Private IP-Adressen und Network Address Translation (NAT)	120
5.6.3	NAT Traversal	121
5.7	Angriffe auf IPSec	121
6	IP Multicast	123
6.1	IP Multicast	124
6.2	Zentralisierte Schlüsselvereinbarung für Gruppen	127
6.2.1	Pay-TV Schlüsselmanagement	127
6.2.2	Die Logical Key Hierarchy (LKH)	131
6.3	Diffie-Hellman-basierte Schlüsselvereinbarungsverfahren für Gruppen	133
6.3.1	Das Konferenzschlüsselsystem von Ingemarsson, Tang und Wong [ITW82]	134
6.3.2	Das Burmester-Desmedt-Protokoll [BD94]	135
6.3.3	Protokolle zur Aufnahme und zum Ausschluss von Mitgliedern	137
6.3.4	Iterierter Diffie-Hellman	139
7	WWW-Sicherheit mit SSL	145
7.1	Das Hypertext Transfer Protokoll (HTTP)	147
7.2	HTTP-Sicherheitsmechanismen	150
7.2.1	Basic Authentication für HTTP	150
7.2.2	Digest Access Authentication für HTTP	151
7.2.3	HTML-Formulare mit Passworтеingabe	152

7.3	Secure HTTP	152
7.4	Erste Versuche: SSL 2.0 und PCT	156
7.4.1	SSL 2.0	156
7.4.2	Private Communication Technology	157
7.5	SSL 3.0: Sicherheitsschicht über TCP	158
7.6	SSL Record Layer	159
7.7	SSL Handshake	160
7.7.1	Übersicht	161
7.7.2	Authentisierung des Client.	163
7.7.3	Verkürzter SSL-Handshake.	163
7.7.4	Die Nachrichten im SSL - Handshake.....	164
7.7.5	Abgleich der Fähigkeiten: ClientHello und ServerHello.	165
7.7.6	Schlüsselaustausch: Certificate und ClientKeyExchange.	167
7.7.7	Synchronisation: [ChangeCipherSpec] und Finished.....	169
7.7.8	Optionale Authentisierung des Clients: CertificateRequest, Certificate und Verify.	171
7.8	SSL Alert Protocol	172
7.9	TLS: Der Internet-Sicherheitsstandard	172
7.9.1	Neue Alert-Nachrichten	173
7.9.2	Konsequenter Einsatz von HMAC	174
7.9.3	Die PRF-Funktion von TLS	174
7.9.4	Erzeugung des Schlüsselmaterials	176
7.9.5	CertificateVerify	176
7.9.6	Finished	177
7.9.7	TLS Ciphersuites	177
7.10	Angriffe auf SSL	178
7.10.1	Angriffe auf den Handshake	179
7.10.2	Angriffe auf den Handshake: Der Bleichenbacher-Angriff	181
7.10.3	Angriffe auf den Record Layer	185
7.10.4	Angriffe auf Zertifikate und ihre Validierung	186
7.10.5	Angriffe auf die GUI des Browsers	187
7.11	Formale Analysen von TLS	190
7.11.1	Formale Sicherheitsmodelle für Authentische Schlüsselvereinbarung (AKE)	191
7.11.2	Authenticated and Confidential Channel Establishment (ACCE)....	192
7.11.3	Logische Analysen	192
7.12	Praktische Aspekte	192
7.12.1	Sourcecode	193
7.12.2	Die PKI für SSL.....	193
7.12.3	Extended Validation-Zertifikate.....	193
7.12.4	Client Zertifikate	194
7.12.5	SSL ohne PKI.....	194
7.12.6	TLS 1.1 und TLS 1.2	195

8	Datenverschlüsselung: PGP	197
8.1	PGP - Die Legende	198
8.1.1	Die Anfänge	198
8.1.2	Die Anklage	199
8.1.3	Das MIT und PGP International	201
8.1.4	PGP mit Hintertür	202
8.1.5	Freeware auf dem Weg zum IETF-Standard	204
8.2	PGP - Die Implementierung	204
8.2.1	Dateiverschlüsselung und - signatur	204
8.2.2	Schlüsselverwaltung: GPG Schlüsselbund	205
8.2.3	Vertrauensmodell: Web of Trust	206
8.3	Open PGP: Der Standard	207
8.3.1	Struktur eines OpenPGP-Pakets	208
8.3.2	Verschlüsselung und Signatur einer Testnachricht	209
8.3.3	Literal Data Packet (Tag 11)	211
8.3.4	Signature Packet (Tag 2)	211
8.3.5	Compressed Data Packet (Tag 8)	214
8.3.6	Symmetrically Encrypted Data Packet (Tag 9)	214
8.3.7	Public-Key Encrypted Session Key Packet (Tag 1)	215
8.3.8	Radix-64-Konvertierung	216
8.4	Angriffe auf PGP	217
8.4.1	Additional Decryption Keys	217
8.4.2	Manipulation des privaten Schlüssel	220
9	S/MIME	225
9.1	E-Mail nach RFC 822	226
9.2	Multipurpose Internet Mail Extensions (MIME)	228
9.3	S/MIME	230
9.3.1	Vorbereitungen zum Verschlüsseln oder Signieren	233
9.3.2	Verschlüsselung	235
9.3.3	Signatur	237
9.3.4	Signatur und Verschlüsselung	240
9.3.5	Schlüsselmanagement	240
9.3.6	Inhalt eines S/MIME Zertifikats	241
9.4	PKCS#7 und CMS	242
9.4.1	Cryptographic Message Syntax (CMS)	242
9.4.2	Signed Data	244
9.4.3	Enveloped Data	245
9.5	PEM	246
9.6	POP3 und IMAP	248
9.6.1	POP3	249
9.6.2	IMAP	249
10	DNS Security	253

10.1	Das Domain Name System (DNS)	253
10.1.1	Geschichte des DNS	254
10.1.2	Domainnamen und die DNS-Hierarchie	254
10.1.3	Resource Records	255
10.1.4	DNS-Server und DNS-Resolver	259
10.1.5	Auflösung von Domainnamen	260
10.1.6	DNS Query und DNS Response	260
10.2	Angriffe auf das DNS	261
10.2.1	DNS Spoofing	261
10.2.2	DNS Cache Poisoning	263
10.2.3	Name Chaining	264
10.2.4	Der Kaminski-Angriff	265
10.3	DNSSEC	266
10.3.1	Neue RR-Datentypen	268
10.3.2	Sichere Namensauflösung mit DNSSEC	274
10.4	Probleme mit DNSSEC	275
11	Sicherheit von Webanwendungen	279
11.1	Bausteine von Webanwendungen	280
11.1.1	Architektur von Webanwendungen	280
11.1.2	Hypertext Markup Language (HTML)	281
11.1.3	Uniform Ressource Locators (URLs) und Uniform Ressource Identifiers (URI)	282
11.1.4	Javascript und das Document Object Model (DOM)	282
11.1.5	Die Same Origin Policy (SOP)	284
11.1.6	Cascading Stylesheets	285
11.1.7	Web 2.0 und AJAX	286
11.1.8	HTTP Cookies	286
11.1.9	HTTP Redirect	288
11.1.10	HTML Formulare	289
11.2	Sicherheit von Webanwendungen	290
11.2.1	Cross-Site Scripting (XSS)	290
11.2.2	Cross-Site Request Forgery (CSRF)	293
11.2.3	SQL-Injection (SQLi)	296
11.3	Das Kerberos-Protokoll	296
11.3.1	Funktionsweise	296
11.3.2	Kerberos v5 und Microsofts Active Directory	299
11.4	Single-Sign-On-Verfahren	299
11.4.1	Microsoft Passport	301
11.4.2	OpenID	304
12	XML- und Webservice-Sicherheit	307
12.1	eXtensible Markup Language	308
12.1.1	Was ist XML?	308

- 12.1.2 XML Namespaces. 312
 - 12.1.3 DTD und XML Schema. 313
 - 12.1.4 XPath 315
 - 12.1.5 XSLT 316
- 12.2 XML Signature 317
- 12.3 XML Encryption 319
- 12.4 Security Assertion Markup Language (SAML) 322
- 13 Ausblick: Herausforderungen der Internetsicherheit 325**
 - 13.1 Informierte Entscheidungen anstelle von Buzzwords 325
 - 13.2 SSL/TLS sicher konfigurieren 326
 - 13.3 HTML5 327
 - 13.4 Default-Verschlüsselung des gesamten Datenverkehrs 327
 - 13.5 Verständnis neuer Technologien 328
 - 13.6 Neue Einsatzszenarien 329
 - 13.7 Kryptographische Erkenntnisse müssen in die Praxis umgesetzt werden. 329
- Literaturverzeichnis 331**
- Index 349**