

Inhaltsverzeichnis

1	Das Internet	1
1.1	TCP/IP-Schichtenmodell	1
1.1.1	Netzzugangsschicht	3
1.1.2	IP-Schicht	4
1.1.3	Transportschicht	5
1.1.4	Anwendungsschicht	6
1.2	Bedrohungen im Internet	7
1.2.1	Passive Angriffe	7
1.2.2	Aktive Angriffe	7
1.3	Kryptographie im Internet	10
2	Kryptographie: Vertraulichkeit	13
2.1	Notation	14
2.2	Symmetrische Verschlüsselung	14
2.2.1	Blockchiffren	16
2.2.2	Stromchiffren	19
2.3	Asymmetrische Verschlüsselung	21
2.4	RSA-Verschlüsselung	22
2.4.1	Textbook RSA	22
2.4.2	PKCS#1	23
2.4.3	OAEP	24
2.5	Diffie-Hellman-Schlüsselvereinbarung	25
2.5.1	Diffie-Hellman-Protokoll	26
2.5.2	Komplexitätsannahmen	27
2.6	ElGamal-Verschlüsselung	31
2.6.1	ElGamal-Verschlüsselung	32
2.6.2	Key Encapsulation Mechanism (KEM)	33
2.7	Hybride Verschlüsselung von Nachrichten	33
2.8	Sicherheitsziel Vertraulichkeit	34

3	Kryptographie: Integrität und Authentizität	39
3.1	Hashfunktionen	39
3.1.1	Hashfunktionen in der Praxis	40
3.1.2	Sicherheit von Hashfunktionen	41
3.2	Message Authentication Codes und Pseudozufallsfunktionen	44
3.3	Authenticated Encryption	47
3.4	Digitale Signaturen	47
3.4.1	RSA-Signatur	49
3.4.2	ElGamal-Signatur	50
3.4.3	DSS und DSA	51
3.5	Sicherheitsziel Integrität	52
3.6	Sicherheitsziel Vertraulichkeit und Integrität	53
4	Kryptographische Protokolle	55
4.1	Passwörter	55
4.1.1	Username/Password-Protokoll	55
4.1.2	Wörterbuchangriffe	57
4.1.3	Rainbow Tables	59
4.2	Authentifikationsprotokolle	61
4.2.1	One-Time-Password-Protokoll (OTP)	61
4.2.2	Challenge-and-Response-Protokoll	63
4.2.3	Certificate/Verify-Protokoll	63
4.2.4	Beidseitige Authentifikation	64
4.3	Schlüsselvereinbarung	65
4.3.1	Public-Key-Schlüsselvereinbarung	65
4.3.2	Symmetrische Schlüsselvereinbarung	65
4.4	Authentische Schlüsselvereinbarung	66
4.5	Angriffe und Sicherheitsmodelle	67
4.5.1	Sicherheitsmodelle für Protokolle	67
4.5.2	Generische Angriffe auf Protokolle	68
4.6	Zertifikate	69
4.6.1	X.509	69
4.6.2	Public-Key-Infrastruktur (PKI)	71
4.6.3	Gültigkeit von Zertifikaten	73
4.6.4	Angriffe auf Zertifikate	74
5	Point-to-Point-Sicherheit	77
5.1	Point-to-Point-Protokoll	78
5.2	PPP-Authentifizierung	79
5.3	Authentication, Authorization und Accounting (AAA)	79
5.3.1	RADIUS	80
5.3.2	Diameter und TACACS+	81

5.4	Point-to-Point Tunneling Protocol (PPTP)	81
5.4.1	PPP-basierte VPN	81
5.4.2	PPTP	82
5.5	Der PPTP-Angriff von Schneier und Mudge	82
5.5.1	Übersicht PPTP-Authentifizierungsoptionen	82
5.5.2	Angriff auf Option 2	83
5.5.3	Angriff auf Option 3	84
5.6	PPTPv2	86
5.7	EAP-Protokolle	87
5.7.1	Lightweight Extensible Authentication Protocol (LEAP) ...	88
5.7.2	EAP-TLS	88
5.7.3	EAP-TTLS	88
5.7.4	EAP-FAST	88
5.7.5	Weitere EAP-Methoden	89
6	Drahtlose Netzwerke (WLAN)	91
6.1	Local Area Network (LAN)	91
6.1.1	Ethernet und andere LAN-Technologien	91
6.1.2	LAN-spezifische Angriffe	93
6.1.3	Nichtkryptographische Sicherungsmechanismen	93
6.2	Wireless LAN	94
6.2.1	Nichtkryptographische Sicherheitsfeatures von IEEE 802.11	94
6.3	Wired Equivalent Privacy (WEP)	95
6.3.1	Funktionsweise von WEP	95
6.3.2	RC4	96
6.3.3	Sicherheitsprobleme von WEP	97
6.3.4	Der Angriff von Fluhrer, Mantin und Shamir	99
6.4	Wi-Fi Protected Access (WPA)	102
6.5	IEEE 802.1X	104
6.6	Enterprise WPA/IEEE 802.11i mit EAP	105
6.7	Key Reinstallation Attack (KRACK) gegen WPA2	107
6.8	WPA3	108
7	Mobilfunk	111
7.1	Architektur von Mobilfunksystemen	112
7.2	GSM	113
7.3	UMTS und LTE	116
7.4	Einbindung ins Internet: EAP	120
7.4.1	EAP-SIM	121
7.4.2	EAP-AKA	121

8	IP-Sicherheit (IPsec)	123
8.1	Internet Protocol (IP)	124
8.1.1	IP-Pakete	125
8.1.2	IPv6	128
8.1.3	Routing	128
8.1.4	Round-Trip Time (RTT)	129
8.1.5	Private IP-Adressen und Network Address Translation (NAT)	130
8.1.6	Virtual Private Network (VPN)	131
8.2	Erste Ansätze	133
8.2.1	Hybride Verschlüsselung	133
8.2.2	Simple Key Management for Internet Protocols (SKIP)	133
8.3	IPsec: Überblick	134
8.3.1	SPI und SA	134
8.3.2	Softwaremodule	135
8.3.3	Senden eines verschlüsselten IP-Pakets	136
8.4	IPsec-Datenformate	137
8.4.1	Transport und Tunnel Mode	137
8.4.2	Authentication Header	139
8.4.3	Encapsulation Security Payload (ESP)	140
8.4.4	ESP und AH in IPv6	142
8.5	IPsec-Schlüsselmanagement: Entwicklung	142
8.5.1	Station-to-Station Protocol	143
8.5.2	Photuris	143
8.5.3	SKEME	146
8.5.4	OAKLEY	146
8.6	Internet Key Exchange Version 1 (IKEv1)	152
8.6.1	Phasenstruktur IKE	152
8.6.2	Datenstruktur ISAKMP	154
8.6.3	Phase 1	154
8.6.4	Phase 2	160
8.7	IKEv2	161
8.7.1	Phasenstruktur	162
8.7.2	Phase 1	162
8.7.3	Aushandlung weiterer IPsec SAs	167
8.8	NAT Traversal	168
8.9	Angriffe auf IPsec	169
8.9.1	Angriffe auf Encryption-Only-Modi in ESP	169
8.9.2	Wörterbuchangriffe auf die PSK-Modi	169
8.9.3	Bleichenbacher-Angriff auf IKEv1 und IKEv2	172

8.10	Alternativen zu IPsec	177
8.10.1	OpenVPN	177
8.10.2	Neue Entwicklungen	179
9	Sicherheit von HTTP	181
9.1	TCP und UDP	181
9.1.1	User Datagram Protocol (UDP)	182
9.1.2	Transmission Control Protocol (TCP)	183
9.1.3	UDP und TCP Proxies	184
9.2	Hypertext Transfer Protokoll (HTTP)	184
9.3	HTTP-Sicherheitsmechanismen	186
9.3.1	Basic Authentication für HTTP	187
9.3.2	Digest Access Authentication für HTTP	187
9.3.3	HTML-Formulare mit Passwordeingabe	188
9.4	HTTP/2	189
10	Transport Layer Security	191
10.1	TLS-Ökosystem	191
10.1.1	Versionen	191
10.1.2	Architektur	192
10.1.3	Aktivierung von TLS	193
10.1.4	Weitere Handshake-Komponenten	195
10.2	TLS Record Layer	195
10.3	TLS-Handshake	198
10.3.1	Übersicht	198
10.3.2	TLS-Ciphersuites	201
10.3.3	Abgleich der Fähigkeiten: ClientHello und ServerHello	205
10.3.4	Schlüsselaustausch: Certificate und ClientKeyExchange	207
10.3.5	Erzeugung des Schlüsselmaterials	210
10.3.6	Synchronisation: ChangeCipherSpec und Finished	211
10.3.7	Optionale Authentifizierung des Client: CertificateRequest, Certificate und CertificateVerify	212
10.3.8	TLS-DHE-Handshake im Detail	213
10.3.9	TLS-RSA-Handshake im Detail	215
10.4	TLS-Hilfsprotokolle: Alert und ChangeCipherSec	216
10.5	TLS Session Resumption	217
10.6	TLS-Renegotiation	219
10.7	TLS Extensions	221
10.8	HTTP-Header mit Auswirkungen auf TLS	222
10.9	Datagram TLS (DTLS)	224
10.9.1	Warum TLS über UDP nicht funktioniert	224
10.9.2	Anpassungen DTLS	225

11	Eine kurze Geschichte von TLS	229
11.1	Erste Versuche: SSL 2.0 und PCT	229
11.1.1	SSL 2.0: Records	230
11.1.2	SSL 2.0: Handshake	230
11.1.3	SSL 2.0: Schlüsselableitung	232
11.1.4	SSL 2.0: Probleme	232
11.1.5	Private Communication Technology	233
11.2	SSL 3.0	234
11.2.1	Record Layer	234
11.2.2	Handshake	235
11.2.3	Schlüsselableitung	236
11.2.4	FORTEZZA: Skipjack und KEA	236
11.3	TLS 1.0	237
11.3.1	Record Layer	237
11.3.2	Die PRF-Funktion von TLS 1.0 und 1.1	237
11.4	TLS 1.1	239
11.5	TLS 1.3	239
11.5.1	TLS-1.3-Ökosystem	239
11.5.2	Record Layer	240
11.5.3	Regular Handshake: Beschreibung	242
11.5.4	TLS 1.3: Schlüsselableitung	244
11.5.5	PSK-Handshake und 0-RTT-Modus	246
11.6	Wichtige Implementierungen	248
11.7	Fazit	249
12	Angriffe auf SSL und TLS	251
12.1	Übersicht	251
12.2	Angreifermodelle	253
12.2.1	Web Attacker Model	253
12.2.2	Man-in-the-Middle Attack	254
12.3	Angriffe auf den Record Layer	255
12.3.1	Wörterbuch aus Chiffretextlängen	255
12.3.2	BEAST	256
12.3.3	Padding-Oracle-Angriffe	259
12.3.4	Kompressionsbasierte Angriffe	272
12.4	Angriffe auf den Handshake	280
12.4.1	Angriffe auf SSL 2.0	280
12.4.2	Bleichenbacher-Angriff	280
12.4.3	Weiterentwicklung des Bleichenbacher-Angriffs	286
12.4.4	Signaturfälschung mit Bleichenbacher	287
12.4.5	ROBOT	288
12.4.6	Synchronisationsangriff auf TLS-RSA	288

12.4.7	Triple Handshake Attack	289
12.5	Angriffe auf den privaten Schlüssel	290
12.5.1	Timing-basierte Angriffe	291
12.5.2	Heartbleed	291
12.5.3	Invalid-Curve-Angriffe	293
12.6	Cross-Protocol-Angriffe	294
12.6.1	Cross-Ciphersuite-Angriffe für TLS	295
12.6.2	TLS und QUIC	295
12.6.3	TLS 1.2 und TLS 1.3	296
12.6.4	TLS und IPsec	298
12.6.5	DROWN	298
12.7	Angriffe auf die GUI des Browsers	301
12.7.1	Die PKI für TLS	301
12.7.2	Phishing, Pharming und Visual Spoofing	302
12.7.3	Warnmeldungen	303
12.7.4	SSLStrip	303
13	Secure Shell (SSH)	305
13.1	Einführung	305
13.1.1	Was ist eine „Shell“?	305
13.1.2	SSH-Schlüsselmanagement	306
13.1.3	Kurze Geschichte von SSH	307
13.2	SSH-1	308
13.3	SSH 2.0	310
13.3.1	Handshake	311
13.3.2	Binary Packet Protocol	312
13.4	Angriffe auf SSH	313
13.4.1	Angriff von Albrecht, Paterson und Watson	313
14	Kerberos	317
14.1	Symmetrisches Schlüsselmanagement	317
14.2	Das Needham-Schroeder-Protokoll	319
14.3	Kerberos-Protokoll	320
14.4	Sicherheit von Kerberos v5	323
14.5	Kerberos v5 und Microsofts Active Directory	324
14.5.1	Windows-Domänen	325
14.5.2	Active Directory und Kerberos	325
15	DNS Security	327
15.1	Domain Name System (DNS)	327
15.1.1	Kurze Geschichte des DNS	328
15.1.2	Domainnamen und DNS-Hierarchie	329
15.1.3	Resource Records	330

15.1.4	Auflösung von Domainnamen	332
15.1.5	DNS-Query und DNS-Response	334
15.2	Angriffe auf das DNS	336
15.2.1	DNS Spoofing	336
15.2.2	DNS Cache Poisoning	336
15.2.3	Name Chaining und In-Bailiwick-RRs	339
15.2.4	Kaminski-Angriff.	340
15.3	DNSSEC	341
15.3.1	Neue RR-Datentypen	343
15.3.2	Sichere Namensauflösung mit DNSSEC	346
15.4	Probleme mit DNSSEC	347
16	Datenverschlüsselung: PGP	349
16.1	PGP – Die Legende	349
16.1.1	Die Anfänge	349
16.1.2	Die Anklage	351
16.1.3	PGP 2.62 und PGP International	351
16.1.4	Freeware auf dem Weg zum IETF-Standard	352
16.2	Das PGP-Ökosystem	352
16.2.1	Schlüsselverwaltung in PGP	353
16.2.2	Verschlüsselung	355
16.2.3	Digitale Signaturen	356
16.2.4	Vertrauensmodell: Web of Trust.	356
16.3	Open PGP: Der Standard	357
16.3.1	Struktur eines OpenPGP-Pakets.	358
16.3.2	Verschlüsselung und Signatur einer Testnachricht.	359
16.3.3	OpenPGP Packets.	361
16.3.4	Radix-64-Konvertierung	362
16.4	Angriffe auf PGP	362
16.4.1	Additional Decryption Keys	363
16.4.2	Manipulation des privaten Schlüssel	364
16.5	PGP: Implementierungen.	369
16.5.1	Kryptobibliotheken mit OpenPGP-Unterstützung	370
16.5.2	OpenPGP-GUIs für verschiedene Betriebssysteme.	371
16.5.3	Paketmanager mit OpenPGP-Signaturen.	372
16.5.4	Software-Downloads	372
17	S/MIME	373
17.1	E-Mail nach RFC 822	374
17.2	Privacy Enhanced Mail (PEM)	377
17.3	Multipurpose Internet Mail Extensions (MIME).	379
17.4	ASN.1, PKCS#7 und CMS	383

17.4.1	Plattformunabhängigkeit: ASN.1	383
17.4.2	Public Key Cryptography Standards (PKCS)	384
17.4.3	PKCS#7 und Cryptographic Message Syntax (CMS)	387
17.5	S/MIME	390
17.6	S/MIME: Verschlüsselung	393
17.7	S/MIME: Signatur	398
17.7.1	Schlüsselmanagement	403
17.8	PGP/MIME	404
18	Angriffe auf S/MIME und OpenPGP	405
18.1	EFAIL 1: Verschlüsselung	405
18.1.1	Angreifermodell	406
18.1.2	Backchannels	407
18.1.3	Crypto Gadgets	408
18.1.4	Direct Exfiltration	409
18.2	EFAIL 2: Digitale Signaturen	412
18.2.1	Angreifermodell	412
18.2.2	GUI Spoofing	413
18.2.3	FROM Spoofing	413
18.2.4	MIME Wrapping	414
18.2.5	CMS Wrapping	415
18.3	EFAIL 3: Reply Attacks	416
19	E-Mail: Weitere Sicherheitsmechanismen	419
19.1	POP3 und IMAP	419
19.1.1	POP3	420
19.1.2	IMAP	421
19.2	SMTP-over-TLS	422
19.3	SPAM und SPAM-Filter	423
19.4	E-Mail-Absender	425
19.5	Domain Key Identified Mail (DKIM)	426
19.6	Sender Policy Framework (SPF)	431
19.7	DMARC	433
20	Web Security und Single-Sign-On-Protokolle	437
20.1	Bausteine von Webanwendungen	438
20.1.1	Architektur von Webanwendungen	438
20.1.2	Hypertext Markup Language (HTML)	439
20.1.3	Uniform Resource Locators (URLs) und Uniform Resource Identifiers (URIs)	440
20.1.4	JavaScript und das Document Object Model (DOM)	441
20.1.5	Same Origin Policy (SOP)	442
20.1.6	Cascading Style Sheets	444

20.1.7	Web 2.0 und AJAX.	445
20.1.8	HTTP-Cookies.	446
20.1.9	HTTP-Redirect und Query-Strings	447
20.1.10	HTML-Formulare	448
20.2	Sicherheit von Webanwendungen	449
20.2.1	Cross-Site Scripting (XSS)	449
20.2.2	Cross-Site Request Forgery (CSRF)	452
20.2.3	SQL-Injection (SQLi)	454
20.2.4	UI-Redressing	456
20.3	Single-Sign-On-Verfahren	458
20.3.1	Microsoft Passport	460
20.3.2	Security Assertion Markup Language (SAML).....	464
20.3.3	OpenID.	465
20.3.4	OAuth.	467
20.3.5	OpenID Connect	469
21	Kryptographische Datenformate im Internet	471
21.1	eXtensible Markup Language (XML)	471
21.1.1	XML Namespaces	472
21.1.2	DTD und XML-Schema.	473
21.1.3	XPath	475
21.1.4	XSLT	476
21.1.5	XML Signature	477
21.1.6	XML Encryption	479
21.1.7	Sicherheit von XML Parsern, XML Signature und XML Encryption	481
21.2	JavaScript Object Notation (JSON).....	483
21.2.1	Syntax.	483
21.2.2	JSON Web Signature	484
21.2.3	JSON Web Encryption	485
21.2.4	Sicherheit von JSON Signing und Encryption.	486
22	Ausblick: Herausforderungen der Internetsicherheit	487
22.1	Herausforderungen der Internetsicherheit	487
Literatur.		491
Stichwortverzeichnis.		513