

Inhaltsverzeichnis

1	Kryptographie im Internet.....	1
1.1	Was ist das „Internet“.....	1
1.2	Bedrohungen im Internet.....	4
1.3	Kryptographie.....	6
1.4	Symmetrische Kryptographie.....	7
1.5	Public-Key Kryptographie	13
1.6	Kryptographische Protokolle.....	19
1.7	Zertifikate	22
2	Datenverschlüsselung: PGP	29
2.1	PGP - Die Legende.....	30
2.2	PGP - Das Produkt	37
2.3	OpenPGP – Der Standard.....	43
2.4	PGP – Die Angriffe	49
2.5	Ausblick	57
3	Sichere E-Mail.....	59
3.1	E-Mail nach RFC 822	59
3.2	Multipurpose Internet Mail Extensions (MIME)	60
3.3	S/MIME.....	63
3.4	PKCS#7 und CMS	74
3.5	PEM.....	78
3.6	PGP und OpenPGP.....	80
3.7	POP3 und IMAP.....	80
4	WWW-Sicherheit mit SSL.....	83
4.1	Das Hypertext Transfer Protocol (HTTP).....	84
4.2	HTTP-Sicherheitsmechanismen.....	86
4.3	Erste Versuche: SSL 2.0 und PCT	90
4.4	SSL 3.0: Sicherheitsschicht über TCP	92
4.5	TLS: Der Internet-Sicherheitsstandard.....	105
4.6	Angriffe auf SSL	111
4.7	Praktische Aspekte.....	117
5	IP Security (IPSec).....	124
5.1	Internet Protocol (IP).....	124
5.2	Erste Ansätze.....	126
5.3	IPSec: Überblick	128
5.4	IPSec Datenformate.....	132
5.5	IPSec: Schlüsselmanagement.....	139
5.6	Die Zukunft von IPSec.....	155
6	Multicast-Netzwerke.....	158
6.1	IP Multicast	159
6.2	IPSec und IP Multicast.....	160
6.3	Schlüsselvereinbarung für Gruppen.....	161
6.4	Multicast-Sicherheit im Internet.....	175
7	Link Layer-Sicherheit	176
7.1	PPP-Sicherheit.....	176
7.2	Wireless LAN.....	186
7.3	Mobilfunk	189
8	DNS Security.....	195
8.1	Einführung Domain Name System	195
8.2	Angriffe auf das Domain Name System	201

8.3	DNSSEC.....	205
8.4	Probleme mit DNSSEC.....	213
8.5	TSIG.....	215
9	XML- und Webservice-Security.....	216
9.1	eXtensible Markup Language.....	216
9.2	Microsoft Passport.....	225
9.3	Webservice Security.....	236
10	Malware und Kryptographie.....	242
10.1	Malware.....	242
10.2	Code-Signatur.....	245
10.3	Trusted Computing.....	249
10.4	Fazit.....	250
11	Literatur.....	251
12	Index.....	261