

Inhalt

1	Gefahren, Angriffe, Risiken *	1
1.1	Der Begriff der IT-Sicherheit *	2
1.2	Gefahren und Ursachen – im Internet und anderswo *	8
1.3	Grundlegende Mechanismen für die IT-Sicherheit *	15
1.4	Die Unsicherheit des Internet: TCP/IP *	16
1.5	Die Unsicherheit des Internet: Dienste *	21
1.6	Gefahren durch Viren und aktive Inhalte *	23
1.7	Security Awareness *	24
1.8	Konstruktion sicherer Systeme *	26
1.8.1	Box: Sicherheitsgrundfunktionen *	29
1.8.2	Box: Sicherheitskriterien *	31
1.8.3	Box: Sicherheitsmodelle *	33
2	Kryptologische Verfahren und Protokolle *	37
2.1	Verschlüsselung *	37
2.2	Symmetrische Verschlüsselungsverfahren *	41
2.2.1	Block- und Stromverschlüsselung *	42
2.2.2	Das DES-Verfahren *	45
2.2.3	3DES: Der verbesserte DES **	49
2.2.4	Das AES-Verfahren *	51
2.2.5	Box: Betriebsmodi von Blockchiffren **	55
2.2.6	Stromchiffren mit linearen Schieberegistern *	58
2.2.6.1	Box: Der Algorithmus A5 ***	65
2.2.7	Box: Der Algorithmus RC4 **	67
2.3	Asymmetrische Kryptosysteme *	69
2.3.1	Einwegfunktionen *	73
2.3.2	Das RSA-Verfahren *	75
2.3.3	Elliptische Kurven ***	78
2.3.4	Die Digitale Unterschrift *	82
2.3.4.1	Box: Archivierung digitaler Dokumente *	87
2.3.4.2	Box: Blinde Signaturen **	89
2.3.5	Hashfunktionen *	91
2.3.5.1	Box: Secure Hash Algorithm **	93
2.3.6	Der Digital Signature Algorithm **	96
2.4	Box: Kryptographische Terminologie *	99
2.5	Zero-Knowledge-Protokolle *	101
2.5.1	Box: Der Fiat-Shamir-Algorithmus **	104
2.6	Schlüsselmanagement *	105
2.6.1	Schlüsselerzeugung und -aufbewahrung *	106
2.6.2	Schlüsselaustausch *	109
2.6.2.1	Box: Protokolle von Needham-Schroeder **	111
2.6.2.2	Box: Diffie-Hellman-Schlüsselaustausch **	113
2.6.3	Zertifizierung von Schlüsseln *	115

2.7	Zertifikate *	116
2.8	Kryptoanalyse *	118
2.8.1	Box: Kryptographische Angriffe *	120
2.9	Steganographie *	122
2.10	Digitale Wasserzeichen *	123
3	Computersicherheit *	127
3.1	Zugangskontrolle: Ansätze *	127
3.1.1	Authentifikation durch Wissen *	129
3.1.1.1	Box: Wie sicher ist mein Passwort? *	133
3.1.1.2	Box: Authentifikation in UNIX ***	136
3.1.2	Authentifikation durch Besitz *	137
3.1.2.1	Box: Technik von Smart-Cards ***	141
3.1.2.2	Box: Authentifikation bei GSM ***	144
3.1.3	Biometrie *	146
3.1.4	Authentifikation in verteilten Systemen *	149
3.1.4.1	Kerberos *	151
3.2	Zugriffskontrolle *	156
3.2.1	Box: Zugriffskontrolle in UNIX ***	160
3.3	Sicherheit von Betriebssystemen *	162
3.3.1	Trusted Computing *	167
3.4	Softwaregesteuerte Angriffe *	169
3.4.1	Viren und Co. *	171
3.4.2	Schutz vor Viren und aktiven Inhalten *	177
3.5	Sichere Software *	180
3.6	Sicherheit eingebetteter Systeme *	184
4	Sicherheit in Netzen *	189
4.1	Firewalls *	189
4.1.1	Aufgaben von Firewalls *	189
4.1.2	Firewall-Systeme *	193
4.1.2.1	Box: Einsatz eines Paketfilters **	198
4.1.2.2	Box: Wie kann man Angreifer identifizieren? ***	199
4.1.3	Box: Intrusion-Detection-Systeme *	202
4.2	Sicherheit der Internet-Schichten *	203
4.2.1	Sicherheit auf der Netzzugangsschicht *	205
4.2.2	Sicherheit auf der IP-Schicht *	207
4.2.2.1	Eine Übersicht zu IPSec *	208
4.2.2.2	Die Architektur von IPSec *	211
4.2.2.3	Encapsulating Security Payload **	213
4.2.2.4	Authentication Header ****	216
4.2.2.5	Einsatzbeispiele IPSec **	217
4.2.3	Sicherheit auf der TCP-Schicht *	220
4.2.3.1	Secure Shell *	220
4.2.3.2	Secure Socket Layer *	223
4.2.4	Sicherheit der Anwendungsschicht *	228

4.2.4.1	Sicherheit bei Remote Terminal Access, File Transfer und Network File System *	229
4.2.4.2	Sicherheit von E-Mail *	232
4.3	Sicherheit im Web *	242
4.3.1	Web-Sicherheit: Clients *	244
4.3.1.1	Aktive Inhalte *	246
4.3.2	Web-Sicherheit: Server *	250
4.3.3	Sichere Webanwendungen **	255
4.4	Sicherheit in GSM-Netzen *	259
4.5	Smartphones und Appstores *	262
4.5.1	Box: Appstore-Sicherheit *	266
4.5.2	Box: Sichere Entwicklung von Apps **	269
4.6	Anonymität in Netzen *	270
4.6.1	Box: Das Mix-Konzept **	273
4.7	Sicherheit im Intranet *	275
4.7.1	Box: ARP Poisoning **	276
4.7.2	WLAN, Bluetooth und VoIP *	278
Glossar		285
Literatur		303
Sachindex		304