

Inhalt

1	Gefahren, Angriffe, Risiken *	1
1.1	Der Begriff der IT-Sicherheit *	3
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 *	17
1.5	Die Unsicherheit des Internet: Dienste *	21
1.6	Gefahren durch Viren und aktive Inhalte *	24
1.7	Konstruktion sicherer Systeme *	25
1.7.1	Box: Sicherheitsgrundfunktionen *	28
1.7.2	Box: Sicherheitskriterien *	30
1.7.3	Box: Sicherheitsmodelle *	32
2	Kryptologische Verfahren und Protokolle *	35
2.1	Verschlüsselung *	35
2.2	Symmetrische Verschlüsselungsverfahren *	39
2.2.1	Block- und Stromverschlüsselung *	40
2.2.2	Das DES-Verfahren *	43
2.2.3	3DES: Der verbesserte DES **	47
2.2.4	Das AES-Verfahren *	49
2.2.5	Box: Betriebsmodi von Blockchiffren **	53
2.2.6	Stromchiffren mit linearen Schieberegistern *	55
2.2.6.1	Box: Der Algorithmus A5 ***	62
2.2.7	Box: Der Algorithmus RC4 **	65
2.3	Asymmetrische Kryptosysteme *	67
2.3.1	Einwegfunktionen *	71
2.3.2	Das RSA-Verfahren *	73
2.3.3	Elliptische Kurven ***	76
2.3.4	Die Digitale Unterschrift *	79
2.3.4.1	Box: Archivierung digitaler Dokumente *	85
2.3.4.2	Box: Blinde Signaturen **	86
2.3.5	Hashfunktionen *	88
2.3.5.1	Box: Secure Hash Algorithm **	90
2.3.6	Der <i>Digital Signature Algorithm</i> **	93
2.4	Box: Kryptographische Terminologie *	95
2.5	Zero-Knowledge-Protokolle *	97
2.5.1	Box: Der Fiat-Shamir-Algorithmus **	100
2.6	Schlüsselmanagement *	101
2.6.1	Schlüsselerzeugung und -aufbewahrung *	102
2.6.2	Schlüsselaustausch *	105
2.6.2.1	Box: Protokolle von Needham-Schroeder **	107
2.6.2.2	Box: Diffie-Hellman-Schlüsselaustausch **	110
2.6.3	Zertifizierung von Schlüsseln *	112
2.7	Zertifikate *	112



Inhalt

2.8	Kryptoanalyse *	115
2.8.1	Box: Kryptographische Angriffe *	117
2.9	Steganographie *	118
2.10	Digitale Wasserzeichen *	120
3	Computersicherheit *	123
3.1	Zugangskontrolle: Ansätze *	123
3.1.1	Authentifikation durch Wissen *	125
3.1.1.1	Box: Wie sicher ist mein Passwort? *	129
3.1.1.2	Box: Authentifikation in UNIX ***	132
3.1.2	Authentifikation durch Besitz *	133
3.1.2.1	Box: Technik von Smart-Cards ***	136
3.1.2.2	Box: Authentifikation bei GSM ***	139
3.1.3	Biometrie *	141
3.1.4	Authentifikation in verteilten Systemen *	144
3.1.4.1	Kerberos *	146
3.2	Zugriffskontrolle *	151
3.2.1	Box: Zugriffskontrolle in UNIX ***	155
3.3	Sicherheit von Betriebssystemen *	157
3.3.1	Trusted Computing *	159
3.4	Softwaregesteuerte Angriffe *	161
3.4.1	Viren und Co. *	163
3.4.2	Schutz vor Viren und aktiven Inhalten *	169
3.5	Sichere Software *	172
4	Sicherheit in Netzen *	175
4.1	Firewalls *	175
4.1.1	Aufgaben von Firewalls *	175
4.1.2	Firewall-Systeme *	179
4.1.2.1	Box: Einsatz eines Paketfilters **	184
4.1.2.2	Box: Windows-Firewall **	185
4.1.2.3	Box: Norton Personal Firewall ***	188
4.1.2.4	Box: Wie kann man Angreifer identifizieren? ***	192
4.1.3	Box: Intrusion-Detection-Systeme *	195
4.2	Sicherheit der Internet-Schichten *	196
4.2.1	Sicherheit auf der Netzzugangsschicht *	198
4.2.2	Sicherheit auf der IP-Schicht *	200
4.2.2.1	Eine Übersicht zu IPSec *	201
4.2.2.2	Die Architektur von IPSec *	204
4.2.2.3	<i>Encapsulating Security Payload</i> **	206
4.2.2.4	<i>Authentication Header</i> ****	209
4.2.2.5	Einsatzbeispiele IPSec **	210
4.2.3	Sicherheit auf der TCP-Schicht *	213
4.2.3.1	<i>Secure Shell</i> *	213
4.2.3.2	<i>Secure Socket Layer</i> *	216
4.2.4	Sicherheit der Anwendungsschicht *	221

4.2.4.1	Sicherheit bei Remote Terminal Access, File Transfer und Network File System *	222
4.2.4.2	Sicherheit von E-Mail *	225
4.2.4.3	Box: E-Mail-Sicherheit mit PGP ***	235
4.3	Sicherheit im Web *	242
4.3.1	Web-Sicherheit: Clients *	244
4.3.1.1	Aktive Inhalte *	246
4.3.1.2	Box: Sicherheitseinstellungen des Internet Explorer ***	250
4.3.1.3	Box: Sicherheitseinstellungen des Firefox ***	255
4.3.2	Web-Sicherheit: Server *	261
4.3.2.1	Box: Sichere Webanwendungen **	266
4.4	Anonymität in Netzen *	268
4.4.1	Box: Das Mix-Konzept **	270
4.5	Sicherheit in GSM-Netzen *	272
4.6	Sicherheit im Intranet *	275
4.6.1	Box: ARP Poisoning **	277
4.6.2	WLAN, Bluetooth und VoIP *	279
Glossar		285
Literatur		303
Sachindex		304