

Inhaltsverzeichnis

1	Einführung	1
1.1	Motivation	1
1.2	Kapitelüberblick	2
1.3	Für wen dieses Buch geschrieben wurde	3
1.4	Über den Autor	3
	Literatur	3

Teil I Grundlagen

2	Grundlagen der Netzwerktechnik	7
2.1	Einführung	7
2.1.1	Reichweite von Netzwerken	8
2.1.2	Netzwerktopologien	9
2.2	Datenpakete, Einkapselung und die Entwicklung von TCP/IP	10
2.2.1	Einige Worte zum OSI-Modell	12
2.2.2	OSI- vs. TCP/IP-Modell	13
2.3	Grundzüge des TCP/IP-Modells	13
2.3.1	Link Layer	13
2.3.2	Internet Layer	23
2.3.3	Transport Layer	24
2.3.4	Application Layer	26
2.3.5	Zusammenfassung	26
2.4	Die wichtigsten Protokolle	26
2.5	Link Layer: ARP	27
2.5.1	Reverse-ARP	28
2.5.2	Proxy-ARP	28
2.6	Internet Layer: IPv4	29
2.6.1	IP-Adressen	32
2.6.2	Fragmentierung	33

2.7	Internet Layer: ICMPv4	35
2.7.1	ICMP-Types 0 und 8	35
2.7.2	ICMP-Type 3	36
2.7.3	ICMP-Type 4	37
2.7.4	ICMP-Type 5	37
2.7.5	ICMP-Types 9 und 10.....	37
2.7.6	ICMP-Type 11.....	38
2.7.7	ICMP-Type 12.....	38
2.7.8	Weitere ICMP-Typen	38
2.8	Internet Layer: IGMP	39
2.8.1	Der IGMPv2-Header	39
2.9	Internet Layer: IPv6.....	40
2.9.1	IPv6-Adressen	41
2.9.2	IPv6 Header Extensions.....	42
2.10	Internet Layer: ICMPv6	43
2.11	Transport Layer: UDP	45
2.11.1	Der UDP-Header	45
2.12	Transport Layer: TCP.....	46
2.12.1	TCP-Reliability.....	46
2.12.2	Sende- und Empfangspuffer	48
2.12.3	Flusskontrolle (Flow-Control)	48
2.12.4	Header	49
2.12.5	Kommunikationsphasen	50
2.13	Application Layer: DHCP	53
2.14	Application Layer: HTTP	54
2.14.1	Aufbau des HTTP-Headers	55
2.14.2	HTTP/2	58
2.15	Application Layer: DNS	58
2.15.1	Resource Records	60
2.15.2	Resolving	60
2.15.3	Der DNS-Header	61
2.15.4	DNS-Tools.....	63
2.16	Application Layer: E-Mail- und Usenetprotokolle	65
2.16.1	POP3	66
2.16.2	IMAP	67
2.16.3	SMTP	69
2.16.4	NNTP (Usenet).....	70
2.17	Application Layer: sonstige Protokolle	73
2.18	Zusammenfassung	74
2.19	Weiterführende Literatur	74
2.20	Übungsaufgaben	74
	Literatur	76

3	Grundlagen der IT-Sicherheit	79
3.1	Einführung	79
3.2	Schutzziele der IT-Sicherheit	83
3.3	Schwachstellen, Verwundbarkeiten und Co.	84
3.4	Zugriffskontrolle	85
	3.4.1 Discretionary Access Control (DAC)	86
	3.4.2 DAC-Erweiterungen	86
	3.4.3 MAC und DAC: Das Bell-LaPadula-Modell	87
3.5	Authentifizierung	89
3.6	Privatsphäre	91
	3.6.1 Anonymität und Pseudonymität	91
	3.6.2 Verkettbarkeit und Verfolgbarkeit	92
	3.6.3 Überwachung	93
3.7	Schadsoftware	95
	3.7.1 Arten von Schadsoftware	95
	3.7.2 Schadsoftware-Mechanismen	98
3.8	IT-Sicherheit: ein Trade-off samt Vorschriften	99
3.9	Science of Security	100
3.10	Zusammenfassung	101
3.11	Weiterführende Literatur	101
3.12	Übungsaufgaben	102
	Literatur	102

Teil II Kryptografie

4	Einführung in die Kryptografie	107
4.1	Einführung und Grundbegriffe	107
4.2	Grundlegende Begriffe	109
	4.2.1 Verschlüsselung und Entschlüsselung als Abbildungen	109
	4.2.2 Kryptografische Schlüssel	110
	4.2.3 Kryptosysteme	111
	4.2.4 Symmetrische und Asymmetrische Kryptografie	111
	4.2.5 Grundlegendes Angreifermodell	112
4.3	Historische Verfahren	113
	4.3.1 Transpositionschiffre	113
	4.3.2 Die Caesar-Chiffre	113
	4.3.3 Die Vigenère-Chiffre	115
	4.3.4 Die Vernam-Chiffre (One-Time-Pad)	115
4.4	Kryptoanalyse für historische Chiffren	116
	4.4.1 Skytale-Chiffre	116
	4.4.2 Caesar-Chiffre	116
	4.4.3 Kryptoanalyse der Vigenère-Chiffre	118

4.4.4	Kryptoanalyse der Vernam-Chiffre	120
4.4.5	Weitere Anmerkungen zu historischen Chiffren	120
4.5	Stromchiffren und Zufallszahlengeneratoren	121
4.5.1	Zufallszahlengeneratoren (PRNG)	121
4.5.2	Der RC4-Algorithmus	122
4.5.3	Die A5/1- und A5/2-Algorithmen	123
4.6	Blockchiffren	124
4.6.1	Der Data Encryption Standard (DES)	125
4.6.2	Der Advanced Encryption Standard (AES)	130
4.6.3	Blockchiffren-Betriebsmodi	132
4.7	Informationstheorie und Kryptografie	133
4.7.1	Grundzüge der Informationstheorie	134
4.7.2	Informationstheorie in der Kryptografie	137
4.7.3	Redundanz	138
4.7.4	Sicherheit eines Kryptosystems	138
4.7.5	Spurious Keys	139
4.7.6	Unizitätsdistanz	140
4.8	Kryptografische Hashfunktionen	141
4.8.1	Einweg-Hashfunktionen	141
4.8.2	Kollisionsresistenz	142
4.8.3	Geburtsstagsangriff und Substitutionsattacke	143
4.8.4	Hashwertlänge im Kontext von Angriffen	144
4.8.5	Wörterbuchangriff (Brute-Force-Angriff)	145
4.8.6	Hashwerttabellen und Regenbogentabellen	145
4.8.7	Sicherheit von Hashfunktionen	148
4.8.8	Aufbau einer typischen Hashfunktion	148
4.8.9	Message Authentication Codes (MAC)	149
4.8.10	Hashfunktionen und Unix-Passwortdateien	150
4.8.11	Hashfunktionen und Filesystem Intrusion Detection	150
4.8.12	Hashfunktionen und Software Ports	151
4.8.13	Hashfunktionen und Hashbäume	152
4.9	Asymmetrische Kryptografie	152
4.9.1	Schlüsselaustausch	153
4.9.2	Rivest-Shamir-Adleman-Algorithmus (RSA)	155
4.10	Digitale Signaturen	157
4.11	Zusammenfassung	157
4.12	Weiterführende Literatur	158
4.13	Übungsaufgaben	159
	Literatur	162

5	Weiterführende Themen der Kryptografie	165
5.1	Einführung	165
5.2	Public Key Infrastructure	166
5.2.1	Digitale Zertifikate und PKI-Bestandteile.....	166
5.2.2	Vertrauensmodelle.....	168
5.3	Virtuelle Private Netzwerke	171
5.3.1	IPSec	172
5.3.2	Transport Layer Security (TLS)	177
5.4	Anonymität und Onion-Routing	179
5.4.1	Grundzüge der Mixe	179
5.4.2	Angriffe gegen Anonymisierungssysteme	181
5.5	Visuelle Kryptografie	181
5.6	Secure Multi-Party Computation und homomorphe Verschlüsselung	182
5.6.1	Dining Cryptographers.....	183
5.7	Geteilte Geheimnisse	183
5.8	Zusammenfassung	184
5.9	Weiterführende Literatur	185
5.10	Übungsaufgaben	185
	Literatur	186

Teil III Netzwerksicherheit

6	Einführung in die Netzwerksicherheit	191
6.1	Einführung	191
6.2	Angriff.....	191
6.2.1	Scanning	192
6.2.2	Wireless Wardriving.....	192
6.2.3	Protocol Fuzzing	192
6.2.4	Sniffer und Promiscuous Mode.....	193
6.2.5	Man-in-the-Middle- und Spoofing-Angriffe	193
6.2.6	Redirects (Routing-Angriffe)	194
6.2.7	Denial-of-Service (DoS)	195
6.2.8	Exploits	196
6.2.9	Social Engineering und Advanced Persistent Threats	197
6.3	Verteidigung.....	198
6.3.1	Firewalls	198
6.3.2	Intrusion Detection und Prevention	199
6.3.3	Honeypots und Honeynets	202

6.3.4	Sandboxing	204
6.3.5	Threat Intelligence	204
6.4	Zusammenfassung	205
6.5	Weiterführende Literatur	206
6.6	Übungsaufgaben	206
	Literatur	207
7	Angriffe auf TCP/IP-Netzwerkprotokolle	209
7.1	Einführung	209
7.2	Angriffe auf der Netzzugangsschicht	210
7.2.1	Angriffe mit physikalischer Grobeinwirkung	210
7.2.2	Jamming	210
7.2.3	Eavesdropping (Sniffing)	210
7.2.4	Falsche Access Points	211
7.2.5	Sicherheit von ARP	212
7.3	Angriffe auf der Internetschicht	214
7.3.1	Reconnaissance (Aufklärung)	214
7.3.2	IP-Spoofing	217
7.3.3	Denial-of-Service-Angriffe	218
7.3.4	Angriffe auf Basis von IP-Fragmenten	220
7.3.5	Grundlegende Angriffe auf das IP-Routing	221
7.3.6	Weitere Anmerkungen zur Sicherheit von IPv6	224
7.3.7	Sicherheit von ICMPv6	224
7.4	Angriffe auf der Transportschicht	225
7.4.1	Sicherheitsaspekte von UDP	225
7.4.2	Sicherheit von TCP	226
7.4.3	Portscans mit TCP und UDP	227
7.5	Angriffe auf der Anwendungsschicht	230
7.5.1	Anmerkungen zur Reconnaissance	230
7.5.2	HTTP	231
7.5.3	DNS	232
7.5.4	E-Mail	234
7.5.5	Telnet, R-Dienste und SSH	235
7.5.6	NNTP	236
7.5.7	FTP	236
7.5.8	Sonstige historische Dienste	238
7.5.9	Zusammenspiel mehrerer Protokolle	238
7.6	Zusammenfassung	238
7.7	Weiterführende Literatur	239
7.8	Übungsaufgaben	239
	Literatur	241

8	Absicherung der Netzwerkschichten	243
8.1	Einführung	243
8.2	Absicherung auf der Netzzugangsschicht.....	243
8.2.1	Zutrittskontrolle und physikalischer Netzwerkzugang	244
8.2.2	Erwerb and Integration von Hardware	244
8.2.3	Verfügbarkeit	245
8.2.4	Komponentenverwaltung	246
8.2.5	MAC-Filter	247
8.2.6	Denial-of-Service-Eindämmung.....	247
8.2.7	Virtuelle LANs	248
8.2.8	Absicherung des ARP-Caches.....	249
8.2.9	IEEE 802.1X	250
8.2.10	WLAN-Verschlüsselung	250
8.3	Absicherung auf der Internetschicht	251
8.3.1	Härtung des IPv4/IPv6-Stacks.....	252
8.3.2	Firewalls für die IP-Kommunikation.....	252
8.3.3	SEND: Secure Neighbor Discovery Protocol.....	253
8.4	Absicherung der Transportschicht	254
8.4.1	Firewalls und Angriffserkennung für TCP und UDP.....	254
8.4.2	Portscan-Detektion.....	256
8.4.3	TCP-Härtung	257
8.5	Absicherung der Anwendungsschicht	258
8.5.1	Generelle Anmerkungen zur Anwendungsschicht.....	258
8.5.2	Proxyserver und Co.	261
8.5.3	HTTP	264
8.5.4	DNS	265
8.5.5	E-Mail-Protokolle: SMTP, IMAP und POP3	266
8.5.6	NNTP	268
8.6	Zusammenfassung	269
8.7	Weiterführende Literatur	270
8.8	Übungsaufgaben	270
	Literatur	271

Teil IV Vertiefung

9	Netzwerksteganografie	275
9.1	Einführung	275
9.2	Methoden der Netzwerksteganografie	278
9.2.1	Grundlegende Taxonomie.....	278
9.2.2	Versteckmuster	279
9.2.3	Spezifische Versteckmethoden.....	282

9.3	Gegenmaßnahmen zur Netzwerksteganografie	284
9.3.1	Detektion	286
9.3.2	Limitierung	288
9.3.3	Unterbindung	289
9.4	Exkurs: Linguistische Steganografie	290
9.5	Zusammenfassung	291
9.6	Weiterführende Literatur	292
9.7	Übungsaufgaben	292
	Literatur	293
10	Sicherheit im Internet der Dinge	295
10.1	Einführung	295
10.2	Schuld sind die anderen – der Cycle of Blame	301
10.3	Standardisierung (und Zertifizierung) im IoT	303
10.4	Patching	305
10.5	Smart Homes und Smart Buildings	306
10.5.1	Kommunikationsprotokolle	307
10.5.2	Angriffe	308
10.5.3	Angriffsdetektion und Härtung	310
10.6	Industriesteueranlagen (Industrial Control Systems)	312
10.6.1	Angriffe	313
10.6.2	Angriffsdetektion und Härtung	314
10.7	Stand der Verwendung von Kryptografie IoT-Protokollen	316
10.8	Generische IoT-Protokolle der Anwendungsschicht	319
10.8.1	CoAP	319
10.8.2	MQTT	324
10.9	IT-Sicherheit weiterer IoT-Domänen	325
10.9.1	Mobile IoT-Systeme (Smart Cars und Co.)	325
10.9.2	Electronic Healthcare (eHealth)	326
10.9.3	Landwirtschaft	327
10.9.4	Legacy-Equipment	328
10.10	Digitale Forensik für das IoT	329
10.11	Zusammenfassung	331
10.12	Weiterführende Literatur	332
10.13	Übungsaufgaben	332
	Literatur	333
	Anhang A: Wichtige wissenschaftliche Zeitschriften und Tagungen	339
	Sachverzeichnis	343