

Inhaltsverzeichnis

I	Grundlagen der Datensicherheitstechnik	1
1	Einleitung	3
1.1	Inhalt und Aufbau dieses Buches	4
1.2	Bedrohungen und Sicherheitsziele	6
1.3	Sicherheitsanalyse für Netze	10
1.4	Maßnahmen der Informationssicherheit	14
1.5	Zentrale Begriffe der Kommunikationssicherheit	15
2	Grundbegriffe der Kryptologie	19
2.1	Kryptologie, Kryptografie und Kryptanalyse	19
2.2	Klassifizierung kryptografischer Algorithmen	20
2.3	Kryptanalyse	21
2.4	Einschätzung des Aufwandes kryptografischer Analysen	24
2.5	Eigenschaften und Klassifizierung von Chiffrieralgorithmen	27
2.6	Schlüsselverwaltung	29
2.7	Zusammenfassung	31
2.8	Weiterführende Literatur	33
2.9	Übungen	33
3	Symmetrische Chiffrierverfahren	35
3.1	Betriebsarten von Blockchiffren	35
3.2	Der Data Encryption Standard	42
3.3	Der Advanced Encryption Standard	49
3.4	Der RC4-Algorithmus	54
3.5	Der KASUMI-Algorithmus	57
3.6	Zusammenfassung	60
3.7	Weiterführende Literatur	61
3.8	Übungen	62
4	Asymmetrische kryptografische Verfahren	63
4.1	Grundidee asymmetrischer kryptografischer Verfahren	63
4.2	Mathematische Grundlagen	67
4.3	Der RSA-Algorithmus	76

4.4	Das Problem des diskreten Logarithmus	79
4.5	Das Diffie-Hellman-Schlüsselaustauschverfahren	83
4.6	Der ElGamal-Algorithmus	85
4.7	Sicherheit herkömmlicher asymmetrischer Kryptografie	88
4.8	Grundlagen der Kryptografie auf elliptischen Kurven	90
4.9	Zusammenfassung	102
4.10	Weiterführende Literatur	103
4.11	Übungen	105
5	Kryptografische Prüfwerte	107
5.1	Anforderungen und Klassifikation	107
5.2	Modifikationserkennungswerte	109
5.3	Nachrichtenauthentisierungswerte	125
5.4	Authentisierte Verschlüsselung	130
5.5	Zusammenfassung	135
5.6	Weiterführende Literatur	136
5.7	Übungen	136
6	Erzeugung sicherer Zufallszahlen	139
6.1	Zufallszahlen und Pseudozufallszahlen	139
6.2	Kryptografisch sichere Zufallszahlen	140
6.3	Statistische Tests für Zufallszahlen	142
6.4	Erzeugung von Zufallszahlen	143
6.5	Erzeugung kryptografisch sicherer Pseudozufallszahlen	145
6.6	Implementierungssicherheit	148
6.7	Zusammenfassung	149
6.8	Weiterführende Literatur	150
6.9	Übungen	151
7	Kryptografische Protokolle	153
7.1	Eigenschaften und Notation kryptografischer Protokolle	153
7.2	Nachrichten- und Instanzenauthentisierung	156
7.3	Das Needham-Schroeder-Protokoll	161
7.4	Kerberos	165
7.5	Der internationale Standard X.509	175
7.6	Sicherheit ausgehandelter Sitzungsschlüssel	180
7.7	Fortgeschrittene Verfahren zur Passwortauthentisierung	182
7.8	Formale Betrachtung kryptografischer Protokolle	187
7.9	Zusammenfassung	198
7.10	Weiterführende Literatur	199
7.11	Übungen	200

8	Sichere Gruppenkommunikation	203
8.1	Spezifische Anforderungen sicherer Gruppenkommunikation .	203
8.2	Aushandlung von Gruppenschlüsseln	205
8.3	Quellenauthentisierung	214
8.4	Zusammenfassung	219
8.5	Weiterführende Literatur	220
8.6	Übungen	220
9	Zugriffskontrolle	223
9.1	Begriffsdefinitionen und Konzepte	223
9.2	Security Labels	225
9.3	Spezifikation von Zugriffskontrollrichtlinien	227
9.4	Kategorien von Zugriffskontrollmechanismen	228
9.5	Zusammenfassung	231
9.6	Weiterführende Literatur	231
9.7	Übungen	232
II	Netzsicherheit	233
10	Integration von Sicherheitsdiensten	235
10.1	Motivation	235
10.2	Ein pragmatisches Modell	237
10.3	Überlegungen zur Platzierung von Sicherheitsdiensten	239
10.4	Integration in untere Protokollschichten vs. Anwendungen ..	243
10.5	Integration in End- oder Zwischensysteme	245
10.6	Zusammenfassung	246
10.7	Weiterführende Literatur	247
10.8	Übungen	247
11	Sicherheitsprotokolle der Datensicherungsschicht	249
11.1	Virtuelle Separation von Datenverkehr mit IEEE 802.1Q ...	250
11.2	Sicherung der lokalen Netzinfrastruktur mit IEEE 802.1X ...	252
11.3	Verschlüsselung des Datenverkehrs mit IEEE 802.1AE	255
11.4	Point-to-Point Protocol	256
11.5	Point-to-Point Tunneling Protocol	266
11.6	Virtuelle private Netze	272
11.7	Zusammenfassung	274
11.8	Weiterführende Literatur	276
11.9	Übungen	278

12	Die IPsec-Sicherheitsarchitektur	279
12.1	Kurze Einführung in die Internetprotokollfamilie	279
12.2	Überblick über die IPsec-Architektur	284
12.3	Einsatz des Transport- und des Tunnelmodus	293
12.4	IPsec-Protokollverarbeitung	297
12.5	Das ESP-Protokoll	300
12.6	Das AH-Protokoll	307
12.7	Das ISAKMP-Protokoll	313
12.8	Der Internet Key Exchange Version 1	321
12.9	Der Internet Key Exchange Version 2	329
12.10	Weitere Aspekte von IPsec	333
12.11	Zusammenfassung	336
12.12	Weiterführende Literatur	337
12.13	Übungen	339
13	Sicherheitsprotokolle der Transportschicht	341
13.1	Secure Socket Layer (SSL)	342
13.2	Transport Layer Security (TLS)	355
13.3	Datagram Transport Layer Security (DTLS)	363
13.4	Secure Shell (SSH)	364
13.5	Zusammenfassung	374
13.6	Weiterführende Literatur	375
13.7	Übungen	375
III	Sichere drahtlose und mobile Kommunikation	377
14	Sicherheitsaspekte der Mobilkommunikation	379
14.1	Bedrohungen in Mobilkommunikationsnetzen	379
14.2	Wahrung der Vertraulichkeit des Aufenthaltsortes	381
14.3	Zusammenfassung	386
14.4	Weiterführende Literatur	386
14.5	Übungen	387
15	Sicherheit in drahtlosen lokalen Netzen	389
15.1	Der Standard IEEE 802.11 für drahtlose lokale Netze	389
15.2	Instanzenauthentisierung	392
15.3	Wired Equivalent Privacy	397
15.4	Robust Secure Networks	404
15.5	Sicherheit in öffentlichen WLANs	411
15.6	Zusammenfassung	413
15.7	Weiterführende Literatur	415
15.8	Übungen	415

16	Sicherheit in funkbasierten Weitverkehrsnetzen	417
16.1	Global System for Mobile Communication (GSM)	417
16.2	Universal Mobile Telecommunications System (UMTS)	425
16.3	Long Term Evolution (LTE)	433
16.4	Zusammenfassung	438
16.5	Weiterführende Literatur	439
16.6	Übungen	440
IV	Schutz von Kommunikationsinfrastrukturen	441
17	Schutz von Kommunikation und Infrastruktur in offenen Netzen	443
17.1	Systematische Bedrohungsanalyse	444
17.2	Sicherheit von Endsystemen	448
17.3	Zusammenfassung	460
17.4	Weiterführende Literatur	461
17.5	Übungen	462
18	Verfügbarkeit des Datentransports	463
18.1	Sabotageangriffe	463
18.2	Verteilte Sabotageangriffe	471
18.3	Gegenmaßnahmen	473
18.4	Zusammenfassung	485
18.5	Weiterführende Literatur	486
18.6	Übungen	487
19	Routing-Sicherheit	489
19.1	Kryptografische Sicherung von BGP	493
19.2	Erkennung von Routing-Anomalien*	503
19.3	Zusammenfassung	508
19.4	Weiterführende Literatur	510
19.5	Übungen	511
20	Sichere Namensauflösung	513
20.1	Funktionsweise von DNS	513
20.2	Sicherheitsziele und Bedrohungen	515
20.3	Sicherer Einsatz von traditionellem DNS	522
20.4	Kryptografische Sicherung von DNS	524
20.5	Zusammenfassung	537
20.6	Weiterführende Literatur	538
20.7	Übungen	539

21	Internet-Firewalls	541
21.1	Aufgaben und Grundprinzipien einer Firewall	541
21.2	Firewall-relevante Internetdienste und Protokolle	544
21.3	Terminologie und Grundbausteine	546
21.4	Firewall-Architekturen	548
21.5	Paketfilterung	552
21.6	Bastion Hosts und Proxyserver	557
21.7	Weitere Aspekte moderner Firewall-Systeme	560
21.8	Zusammenfassung	561
21.9	Weiterführende Literatur	562
21.10	Übungen	563
22	Automatisierte Angriffserkennung und -reaktion	565
22.1	Arbeitsweise und Ziele von Intrusion-Detection-Systemen	566
22.2	Aufbau und Funktionsweise netzwerkbasierter IDS	570
22.3	Reaktion auf Angriffe und automatische Unterbindung	581
22.4	Techniken zur Umgehung von NIDS	583
22.5	Zusammenfassung	586
22.6	Weiterführende Literatur	587
22.7	Übungen	588
23	Verwaltung komplexer Kommunikationsinfrastrukturen*	589
23.1	Automatisches Zertifikatsmanagement	589
23.2	Automatische VPN-Konfiguration	597
23.3	Zusammenfassung	612
23.4	Weiterführende Literatur	614
23.5	Übungen	616
	Literaturverzeichnis	617
	Abkürzungsverzeichnis	647
	Index	656