

---

# Inhaltsverzeichnis

<b>1</b>	<b>Einleitung</b> .....	1
1.1	Motivation .....	1
1.2	Sicherheit im Internet .....	2
1.3	Abgrenzung .....	3
1.4	Faktor Mensch .....	4
1.5	Gliederung des Buches .....	5

---

## Teil I Grundlagen

---

<b>2</b>	<b>Systemsicherheit</b> .....	9
2.1	Sicherheit als Managementaufgabe .....	9
2.2	Sicherheitsrichtlinien .....	11
2.3	Robustheit und Fehlertoleranz .....	12
2.4	Allgemeine Bedrohungen und Sicherheitsziele .....	13
2.5	Bedrohungsszenarien und Angriffe .....	14
2.5.1	Abhören .....	14
2.5.2	Einfügen, Löschen oder Verändern von Daten .....	15
2.5.3	Verzögern und Wiedereinspielen von Daten .....	15
2.5.4	Maskerade .....	16
2.5.5	Autorisierungsverletzung .....	16
2.5.6	Abstreiten von Ereignissen .....	17
2.5.7	Sabotage .....	17
2.5.8	Kombination von Angriffen .....	18
2.6	Sicherheitsziele in Netzwerken .....	19
2.7	Schichtenmodell für Kommunikationssysteme .....	21
2.8	Endsystemsicherheit .....	23
2.9	Zusammenfassung .....	23
<b>3</b>	<b>Grundlagen zur Kryptographie</b> .....	25
3.1	Geschichte .....	26

3.2	Kryptoanalyse .....	27
3.3	Zufallszahlen .....	29
3.3.1	Qualität von Zufallszahlen .....	30
3.3.2	Aufbau eines Pseudozufallszahlengenerators .....	30
3.3.3	Zusammenfassung .....	33
3.4	Symmetrische Kryptographie .....	33
3.4.1	Blockchiffren .....	33
3.4.2	Stromchiffren .....	35
3.4.3	Betriebsmodi von symmetrischen Blockchiffren .....	39
3.4.4	DES .....	46
3.4.5	AES .....	51
3.4.6	RC4 .....	54
3.4.7	Zusammenfassung .....	55
3.5	Einwegfunktionen .....	56
3.5.1	Kryptographische Hash-Funktionen .....	57
3.5.2	Hash-Ketten .....	58
3.5.3	SHA-1 .....	59
3.5.4	MD5 .....	61
3.5.5	Zusammenfassung .....	63
3.6	Asymmetrische Kryptographie .....	63
3.6.1	Ablauf einer Verschlüsselung .....	64
3.6.2	RSA .....	66
3.6.3	Diffie-Hellman .....	69
3.6.4	El-Gamal .....	72
3.7	Digitale Signaturen .....	77
3.7.1	Elektronische Signaturen .....	78
3.7.2	DSS und DSA .....	83
3.8	Hybride Verschlüsselungssysteme .....	87
3.8.1	Schlüssellängen .....	88
3.8.2	Empfohlene Schlüssellängen .....	90

---

## Teil II Sicherheitsmechanismen für Netzwerke

---

4	Sicherungsmechanismen und -verfahren .....	95
4.1	Authentizität/Authentifizierung .....	95
4.1.1	Klartext-Passwörter .....	97
4.1.2	Passwort-Hashes .....	97
4.1.3	S/KEY und OTP .....	100
4.1.4	Asymmetrische Kryptographie .....	100
4.1.5	Bewertung .....	102
4.2	Integritätssicherung .....	103
4.2.1	Lineare Verfahren .....	103
4.2.2	HMAC .....	104
4.2.3	CBC-MAC .....	106

4.2.4	Digitale Signaturen .....	106
4.2.5	Bewertung .....	106
4.3	Schutz gegen Wiedereinspielungsangriffe .....	107
4.3.1	Zeitstempel .....	108
4.3.2	Sequenznummern .....	110
4.3.3	Bewertung .....	112
4.4	Vertraulichkeit .....	112
4.4.1	Symmetrische Verschlüsselung .....	112
4.4.2	Asymmetrische Verschlüsselung .....	113
4.4.3	Hybride Krypto-Systeme .....	114
4.4.4	Steganographie .....	115
4.5	Dynamische Schlüsselerzeugung .....	115
4.5.1	Unabhängigkeit von Schlüsseln .....	116
4.5.2	Erneuerung von Schlüsseln .....	117
4.5.3	Schutz der Identitäten .....	117
4.6	Aushandlung der Sicherungsverfahren .....	118
4.7	Erhöhung der Resistenz gegen DoS-Angriffe .....	119
4.7.1	Cookies und Puzzles .....	120
4.7.2	Reihenfolge von Operationen .....	121
4.8	Nachweisbarkeit/Nichtabstreitbarkeit .....	122
4.8.1	Problemanalyse .....	122
4.8.2	Einsatz digitaler Signaturen .....	123
4.9	Anonymität/Abstreitbarkeit .....	125
4.9.1	Pseudonymität .....	125
4.9.2	Verstecken in der Masse .....	125
4.9.3	Chaum-Mixes .....	126
4.10	VPN .....	126
4.10.1	MPLS-VPNs .....	127
4.10.2	VPNs mit kryptographischen Schutzmechanismen ...	128
<b>5</b>	<b>Netzzugangsschicht .....</b>	<b>131</b>
5.1	Punkt-zu-Punkt-Verbindungen .....	132
5.1.1	PPP .....	132
5.1.2	Bewertung .....	138
5.1.3	PPTP und L2TP .....	138
5.2	LAN .....	141
5.2.1	Ethernet .....	142
5.2.2	PPPoE .....	148
5.2.3	802.1x .....	151
5.2.4	PANA .....	152
5.2.5	Bewertung .....	154
5.3	WLAN .....	155
5.3.1	Übertragungsreichweite und Sicherheit .....	155
5.3.2	Mögliche Angriffe auf WLANs .....	157
5.3.3	WEP .....	158

5.3.4	Werkzeuge zur Sicherheitsüberprüfung	163
5.3.5	Steigerung der Sicherheit eines WLANs	165
5.3.6	WPA, RSN und 802.11i	166
5.3.7	EAP-TLS	173
5.3.8	PEAP	176
5.3.9	EAP-TTLS	177
5.3.10	Bewertung	180
5.4	Bluetooth	180
5.4.1	Sicherheit	181
5.4.2	Link Keys	181
5.4.3	Authentifizierung	185
5.4.4	Encryption Keys	186
5.4.5	Verschlüsselung	186
5.4.6	Bewertung	187
5.5	Ausblick: ZigBee	190
<b>6</b>	<b>Netzwerkschicht</b>	<b>193</b>
6.1	IP	193
6.1.1	IP Version 4	194
6.1.2	IP Version 6	202
6.1.3	Bewertung	206
6.1.4	DHCP	207
6.2	IPsec	210
6.2.1	Sicherheitskonzept	211
6.2.2	Übertragungsmodi	211
6.2.3	Sicherheitsprotokolle	213
6.2.4	Einsatz	218
6.2.5	Probleme	220
6.2.6	Implementierung	223
6.2.7	Bewertung	224
6.3	IKE	226
6.3.1	Authentifizierung	227
6.3.2	Aufbau des sicheren Kanals	228
6.3.3	Aushandlung von IPsec-SAs	233
6.3.4	Bewertung	236
6.3.5	IKEv2	237
6.4	Photuris	243
6.4.1	Cookie-Austausch	243
6.4.2	Wertaustausch	244
6.4.3	Identitätenaustausch	245
6.4.4	Bewertung	245
6.5	NAT	246
6.5.1	Private Adressen und Intranets	246
6.5.2	Adressenumsetzung	247
6.5.3	NAT-Varianten	249

6.5.4	Bewertung	251
6.6	Firewalls	253
6.6.1	Komponenten einer Firewall	254
6.6.2	Erstellen von Filterregeln	254
6.6.3	Klassifikationsregeln	256
6.6.4	ICMP	258
6.6.5	Zusammenspiel mit Application-Level Gateways	259
6.6.6	Angriffsmöglichkeiten – DoS	261
6.6.7	Platzierung von Firewalls	261
6.6.8	Personal Firewalls	263
6.6.9	Port Knocking	264
6.6.10	Bewertung	266
<b>7</b>	<b>Transportschicht</b>	<b>269</b>
7.1	UDP	270
7.1.1	Bedrohungen	270
7.1.2	Sicherheitsmechanismen	271
7.1.3	Bewertung	271
7.2	TCP	271
7.2.1	Bedrohungen	272
7.2.2	Sicherheitsmechanismen	276
7.2.3	Bewertung	276
7.3	TLS	276
7.3.1	Motivation	277
7.3.2	Historie	277
7.3.3	Überblick über das TLS-Protokoll	278
7.3.4	Cipher-Suites	279
7.3.5	Authentifizierung des Kommunikationspartners	280
7.3.6	Aufbau des sicheren Kanals	281
7.3.7	Datenübertragung	286
7.3.8	Signalisierung in TLS	287
7.3.9	Erneuerung des Schlüsselmaterials	288
7.3.10	Verbindungsabbau	289
7.3.11	Schlüsselerzeugung	289
7.3.12	TLS-VPN	289
7.3.13	Hybrid-Variante: OpenVPN	290
7.3.14	Bewertung	291
7.3.15	Vergleich mit IPsec	292
7.4	SCTP	294
7.4.1	Bedrohungen	294
7.4.2	Sicherheitsmechanismen	294
7.4.3	Bewertung	295
7.5	DCCP	296
7.5.1	Bedrohungen	296
7.5.2	Sicherheitsmechanismen	296

7.5.3	Bewertung	296
<b>8</b>	<b>Netzwerkinfrastruktursicherheit</b>	<b>297</b>
8.1	Motivation	297
8.2	Allgemeine Schutzmaßnahmen	298
8.3	AAA	299
8.3.1	RADIUS	300
8.3.2	Diameter	307
8.4	Routing-Sicherheit	317
8.4.1	Einleitung	317
8.4.2	Sicherheit von Routing-Protokollen	319
8.4.3	Routing-Sicherheit für Endsysteme	321
8.4.4	Redundanzprotokolle	322
8.4.5	Dynamisches Routing	323
8.5	MPLS	326
8.5.1	Einleitung	326
8.5.2	Sicherheitsaspekte	330
8.5.3	Sicherheit von RSVP	330
8.5.4	Sicherheit von LDP	332
8.5.5	Bewertung	333
8.6	SNMP	334
8.6.1	Protokollversion v1	334
8.6.2	Sicherheit von SNMPv1	335
8.6.3	Protokollversion v2	337
8.6.4	Protokollversion v3	337
8.6.5	Bewertung	339
8.7	DDoS	339
8.7.1	Reflektorenangriffe	340
8.7.2	Gegenmaßnahmen	342
8.8	IDS	345
8.8.1	Klassifikation	346
8.8.2	Snort	347
8.8.3	Zusammenfassung	348
<b>9</b>	<b>Digitale Zertifikate, PKI und PMI</b>	<b>349</b>
9.1	Motivation: Authentifizierung	349
9.2	Motivation: Autorisierung	350
9.3	Digitale Zertifikate	351
9.3.1	Grundproblem	352
9.3.2	Definition	352
9.3.3	Vertrauensanker	353
9.3.4	Klassifikation	353
9.3.5	Vertrauen	354
9.3.6	Konsistenz bei Zertifikaten	357
9.3.7	Anforderungen an eine Infrastruktur	358

9.3.8	Überblick über Standards	359
9.4	PKI	360
9.4.1	Definition	360
9.4.2	PKI-Modell	361
9.4.3	Anforderungen an eine PKI	361
9.4.4	Widerruf von Zertifikaten	362
9.4.5	Vertrauensmodelle	363
9.5	PKI auf X.509-Basis	370
9.5.1	Profile	370
9.5.2	Namensschema	370
9.5.3	Struktur eines ID-Zertifikats	371
9.5.4	Erweiterungen des ID-Zertifikats	372
9.5.5	Struktur von CRLs	374
9.5.6	Erweiterungen	375
9.5.7	CRL-Varianten	375
9.5.8	Prüfung eines Zertifikats	377
9.5.9	PKI-Unfälle	378
9.6	PKIX Working Group	379
9.6.1	OCSP	379
9.6.2	SCVP	381
9.6.3	Vergleich	382
9.7	PMI	382
9.7.1	Grundproblem	382
9.7.2	Überblick über Autorisierungsmodelle	383
9.7.3	Definition	384
9.7.4	PMI-Modell	384
9.7.5	PMI und Rollen	386
9.7.6	Widerruf von Zertifikaten	386
9.7.7	Vertrauensmodelle	386
9.8	PMI auf X.509-Basis	387
9.8.1	Struktur eines Attributzertifikats	388
9.8.2	Überblick	389
9.8.3	Erweiterungen von Attributzertifikaten	390
9.8.4	Zertifikatsvalidierung	392
9.8.5	Autorisierungsmodelle	394
9.9	PMIX Working Group	394
9.10	Bewertung	394
<b>10</b>	<b>Anwendungsschicht</b>	<b>397</b>
10.1	HTTP	397
10.1.1	Sicherheit	397
10.1.2	Bewertung	399
10.2	SSH	400
10.2.1	Historie	400
10.2.2	Remote Shell, Remote Login und Telnet	401

10.2.3	Authentifikation bei SSH	402
10.2.4	Weitere Funktionen mit Sicherheitsimplikationen	404
10.2.5	SSH mit verteilten Dateisystemen	407
10.2.6	SSH im Detail	408
10.2.7	SSH-VPN	415
10.2.8	Bewertung	415
10.3	Kerberos	416
10.3.1	Historie	416
10.3.2	Ablauf von Kerberos im Überblick	417
10.3.3	Anmeldung	419
10.3.4	Ticket und Authenticator	420
10.3.5	Ressourcen-Zugriff	422
10.3.6	Replizierung der Server	423
10.3.7	Domänen	424
10.3.8	Rechteweitergabe	425
10.3.9	Erweiterung der Gültigkeitsdauer	426
10.3.10	Bewertung	427
10.4	SASL	428
10.4.1	Motivation	428
10.4.2	Authentifizierungsmechanismen	428
10.4.3	Protokollablauf	432
10.4.4	Beispielabläufe	433
10.4.5	Bewertung	435
10.5	BEEP	436
10.5.1	Sicherheit	438
10.6	DNS	438
10.6.1	Beschreibung des DNS	439
10.6.2	Angriffe auf DNS	441
10.6.3	TSIG	442
10.6.4	DNS Security Extensions	443
10.6.5	Ausblick auf die Überarbeitung von DNSsec	447
10.6.6	Bewertung	448
10.7	LDAP	449
10.7.1	Historie	449
10.7.2	Verzeichniszugriff	449
10.7.3	Authentifizierung	450
10.7.4	Autorisierung	451
10.8	VoIP	452
10.8.1	Signalisierungsprotokoll	452
10.8.2	Transportprotokoll	456
10.8.3	Sicherheit	456
10.8.4	Bewertung	458
10.9	PGP und S/MIME	459
10.9.1	Das E-Mail-Datenformat	460
10.9.2	MIME	461

10.9.3	Sicherheitsanforderungen und Probleme .....	464
10.9.4	PGP .....	465
10.9.5	S/MIME .....	470
10.9.6	Bewertung .....	473
10.10	Spam .....	474
10.10.1	Historie und Ursachen .....	474
10.10.2	Gegenmaßnahmen .....	476
10.10.3	Bewertung .....	478
10.11	Instant Messaging .....	478
10.11.1	IRC .....	479
10.11.2	OSCAR/ICQ .....	480
10.11.3	XMPP/Jabber .....	482
10.11.4	Bewertung .....	483
10.12	Malware .....	484
10.12.1	Kategorisierung .....	484
10.12.2	Verbreitung von Malware .....	485
10.12.3	Schutzmechanismen gegen Malware .....	486
10.12.4	Hoax .....	488
10.12.5	Bewertung .....	489

---

## Teil III Einsatzszenarien

---

<b>11</b>	<b>Einleitung zum Praxisbeispiel .....</b>	<b>493</b>
<b>12</b>	<b>Hauptstandort .....</b>	<b>497</b>
12.1	Bedrohungsanalyse .....	497
12.2	Schutzziele .....	498
12.3	Naiver Lösungsansatz .....	498
12.3.1	Fehler 1: Fehlender Schutz der Infrastruktur .....	500
12.3.2	Fehler 2: Keine Trennung von Rechnergruppen .....	501
12.3.3	Fehler 3: Keine Zugangssicherung zum LAN .....	504
12.3.4	Fehler 4: Implizites Filtern statt explizitem Filtern .....	506
12.3.5	Fehler 5: Schwache Absicherung in der Anwendungsebene .....	508
12.4	Verbesserter Lösungsansatz .....	509
<b>13</b>	<b>Nebenstandort .....</b>	<b>511</b>
13.1	Bedrohungsanalyse .....	511
13.2	Schutzziele .....	511
13.3	Naiver Lösungsansatz .....	512
13.3.1	Fehler 1: Direkter Zugriff auf Mitarbeiterrechner .....	512
13.3.2	Fehler 2: Ungeschützte Datenübertragung .....	513
13.3.3	Fehler 3: Keine redundante Anbindung .....	517
13.4	Verbesserter Lösungsansatz .....	518

<b>14 Zulieferer</b> .....	519
14.1 Bedrohungsanalyse .....	519
14.2 Schutzziele .....	520
14.3 Lösungsansätze für E-Mail-Sicherheit .....	520
14.4 Lösungsansätze für den Zugriff auf interne Ressourcen .....	522
14.4.1 VPN-Verbindung .....	522
14.4.2 Gesicherte Verbindungen zu ALGs .....	524
14.4.3 Autorisierungsprüfung .....	525
14.5 Empfohlener Lösungsansatz .....	525
<b>15 Außendienstmitarbeiter</b> .....	527
15.1 Analyse .....	527
15.2 Schutzziele .....	528
15.3 Schutz des Verkehrs .....	528
15.3.1 Einsatz von TLS .....	528
15.3.2 Einsatz eines VPNs .....	529
15.4 Schutz des mobilen Rechners .....	530
15.5 Zusammenfassung .....	531
<b>16 Drahtlose Infrastruktur</b> .....	533
16.1 Bedrohungsanalyse .....	533
16.2 Schutzziele .....	534
16.2.1 Mitarbeiter .....	534
16.2.2 Gäste .....	535
16.3 Naiver Ansatz fürs Mitarbeiter-WLAN .....	535
16.3.1 Fehler 1: Ungesicherter Zugriff .....	536
16.3.2 Fehler 2: Ungesicherte Datenübertragung .....	536
16.3.3 Fehler 3: Keine Zugriffskontrolle auf interne Ressourcen .....	537
16.3.4 Fehler 4: Direkter Zugriff auf Teilnehmer .....	537
16.4 Verbesserter Lösungsansatz fürs Mitarbeiter-WLAN .....	537
16.5 Einfacher Ansatz fürs Gäste-WLAN .....	538
16.5.1 Fehler 1: Unkontrollierte Nutzung .....	539
16.5.2 Fehler 2: Ungesicherter Zugriff auf Dienste .....	540
16.5.3 Fehler 3: Direkter Zugriff .....	541
16.6 Verbesserter Lösungsansatz fürs Gäste-WLAN .....	541
16.7 Gemeinsamer Lösungsansatz .....	542
16.7.1 Zusammenfassung .....	543
<b>Literatur</b> .....	545
<b>Abkürzungsverzeichnis</b> .....	569
<b>Index</b> .....	573