

# Inhaltsverzeichnis

## Vorwort

v

<b>1</b>	<b>Einführung</b>	<b>1</b>
1.1	Grundlegende Begriffe . . . . .	3
1.2	Schutzziele . . . . .	7
1.3	Schwachstellen, Bedrohungen, Angriffe . . . . .	16
1.3.1	Bedrohungen . . . . .	16
1.3.2	Angriffs- und Angreifer-Typen . . . . .	19
1.3.3	Rechtliche Rahmenbedingungen . . . . .	28
1.4	Computer Forensik . . . . .	33
1.5	Sicherheitsrichtlinie . . . . .	35
1.6	Sicherheitsinfrastruktur . . . . .	37
<b>2</b>	<b>Spezielle Bedrohungen</b>	<b>45</b>
2.1	Einführung . . . . .	45
2.2	Buffer-Overflow . . . . .	47
2.2.1	Einführung . . . . .	48
2.2.2	Angriffe . . . . .	50
2.2.3	Gegenmaßnahmen . . . . .	53
2.3	Computerviren . . . . .	56
2.3.1	Eigenschaften . . . . .	56
2.3.2	Viren-Typen . . . . .	58
2.3.3	Gegenmaßnahmen . . . . .	65
2.4	Würmer . . . . .	68
2.5	Trojanisches Pferd . . . . .	73
2.5.1	Eigenschaften . . . . .	73
2.5.2	Gegenmaßnahmen . . . . .	75
2.6	Bot-Netze und Spam . . . . .	77
2.6.1	Bot-Netze . . . . .	77
2.6.2	Spam . . . . .	79
2.7	Mobiler Code . . . . .	81
2.7.1	Eigenschaften . . . . .	82
2.7.2	Sicherheitsbedrohungen . . . . .	82

2.7.3	Gegenmaßnahmen . . . . .	84
2.7.4	Mobile Apps . . . . .	86
<b>3</b>	<b>Internet-(Un-)Sicherheit</b>	<b>91</b>
3.1	Einführung . . . . .	91
3.2	Internet-Protokollfamilie . . . . .	93
3.2.1	ISO/OSI-Referenzmodell . . . . .	93
3.2.2	Das TCP/IP-Referenzmodell . . . . .	100
3.2.3	Das Internet-Protokoll IP . . . . .	102
3.2.4	Das Transmission Control Protokoll TCP . . . . .	107
3.2.5	Das User Datagram Protocol UDP . . . . .	110
3.2.6	DHCP und NAT . . . . .	112
3.3	Sicherheitsprobleme . . . . .	115
3.3.1	Sicherheitsprobleme von IP . . . . .	115
3.3.2	Sicherheitsprobleme von ICMP . . . . .	121
3.3.3	Sicherheitsprobleme von ARP . . . . .	123
3.3.4	Sicherheitsprobleme von UDP und TCP . . . . .	127
3.4	Sicherheitsprobleme von Netzdiensten . . . . .	131
3.4.1	Domain Name Service (DNS) . . . . .	131
3.4.2	Network File System (NFS) . . . . .	141
3.4.3	Weitere Dienste . . . . .	146
3.5	Web-Anwendungen . . . . .	151
3.5.1	World Wide Web (WWW) . . . . .	152
3.5.2	Sicherheitsprobleme . . . . .	158
3.5.3	OWASP Top-Ten Sicherheitsprobleme . . . . .	166
3.6	Analysetools und Systemhärtung . . . . .	175
<b>4</b>	<b>Security Engineering</b>	<b>183</b>
4.1	Entwicklungsprozess . . . . .	184
4.1.1	Allgemeine Konstruktionsprinzipien . . . . .	184
4.1.2	Phasen . . . . .	185
4.1.3	BSI-Sicherheitsprozess . . . . .	186
4.2	Strukturanalyse . . . . .	190
4.3	Schutzbedarfsermittlung . . . . .	192
4.3.1	Schadensszenarien . . . . .	192
4.3.2	Schutzbedarf . . . . .	195
4.4	Bedrohungsanalyse . . . . .	197
4.4.1	Bedrohungsmatrix . . . . .	197
4.4.2	Bedrohungsbaum . . . . .	199
4.5	Risikoanalyse . . . . .	204
4.5.1	Attributierung . . . . .	205
4.5.2	Penetrationstests . . . . .	210

4.6	Sicherheitsarchitektur und Betrieb . . . . .	212
4.6.1	Sicherheitsstrategie und Sicherheitsmodell . . . . .	212
4.6.2	Systemarchitektur und Validierung . . . . .	213
4.6.3	Aufrechterhaltung im laufenden Betrieb . . . . .	214
4.7	Sicherheitsgrundfunktionen . . . . .	214
4.8	Realisierung der Grundfunktionen . . . . .	218
4.9	Security Development Lifecycle (SDL) . . . . .	220
4.9.1	Die Entwicklungsphasen . . . . .	221
4.9.2	Bedrohungs- und Risikoanalyse . . . . .	222
<b>5</b>	<b>Bewertungskriterien</b>	<b>227</b>
5.1	TCSEC-Kriterien . . . . .	227
5.1.1	Sicherheitsstufen . . . . .	228
5.1.2	Kritik am Orange Book . . . . .	229
5.2	IT-Kriterien . . . . .	231
5.2.1	Mechanismen . . . . .	231
5.2.2	Funktionsklassen . . . . .	232
5.2.3	Qualität . . . . .	232
5.3	ITSEC-Kriterien . . . . .	233
5.3.1	Evaluationsstufen . . . . .	234
5.3.2	Qualität und Bewertung . . . . .	235
5.4	Common Criteria . . . . .	236
5.4.1	Überblick über die CC . . . . .	237
5.4.2	CC-Funktionsklassen . . . . .	241
5.4.3	Schutzprofile . . . . .	243
5.4.4	Vertrauenswürdigkeitsklassen . . . . .	246
5.5	Zertifizierung . . . . .	252
<b>6</b>	<b>Sicherheitsmodelle</b>	<b>255</b>
6.1	Modell-Klassifikation . . . . .	255
6.1.1	Objekte und Subjekte . . . . .	256
6.1.2	Zugriffsrechte . . . . .	257
6.1.3	Zugriffsbeschränkungen . . . . .	258
6.1.4	Sicherheitsstrategien . . . . .	258
6.2	Zugriffskontrollmodelle . . . . .	260
6.2.1	Zugriffsmatrix-Modell . . . . .	260
6.2.2	Rollenbasierte Modelle . . . . .	268
6.2.3	Chinese-Wall Modell . . . . .	276
6.2.4	Bell-LaPadula Modell . . . . .	281
6.3	Informationsflussmodelle . . . . .	288
6.3.1	Verbands-Modell . . . . .	288
6.4	Fazit und Ausblick . . . . .	292

<b>7</b>	<b>Kryptografische Verfahren</b>	<b>295</b>
7.1	Einführung . . . . .	295
7.2	Steganografie . . . . .	297
7.2.1	Linguistische Steganografie . . . . .	298
7.2.2	Technische Steganografie . . . . .	299
7.3	Grundlagen kryptografischer Verfahren . . . . .	301
7.3.1	Kryptografische Systeme . . . . .	301
7.3.2	Anforderungen . . . . .	306
7.4	Informationstheorie . . . . .	307
7.4.1	Stochastische und kryptografische Kanäle . . . . .	307
7.4.2	Entropie und Redundanz . . . . .	309
7.4.3	Sicherheit kryptografischer Systeme . . . . .	311
7.5	Symmetrische Verfahren . . . . .	316
7.5.1	Permutation und Substitution . . . . .	317
7.5.2	Block- und Stromchiffren . . . . .	318
7.5.3	Betriebsmodi von Blockchiffren . . . . .	323
7.5.4	Data Encryption Standard . . . . .	329
7.5.5	AES . . . . .	338
7.6	Asymmetrische Verfahren . . . . .	344
7.6.1	Eigenschaften . . . . .	345
7.6.2	Das RSA-Verfahren . . . . .	348
7.7	Elliptische Kurven Kryptografie (ECC) . . . . .	360
7.7.1	Grundlagen . . . . .	361
7.7.2	Einsatz elliptischer Kurven . . . . .	366
7.8	Kryptoanalyse . . . . .	371
7.8.1	Klassen kryptografischer Angriffe . . . . .	371
7.8.2	Substitutionschiffren . . . . .	373
7.8.3	Differentielle Kryptoanalyse . . . . .	375
7.8.4	Lineare Kryptoanalyse . . . . .	376
<b>8</b>	<b>Hashfunktionen und elektronische Signaturen</b>	<b>379</b>
8.1	Hashfunktionen . . . . .	379
8.1.1	Grundlagen . . . . .	380
8.1.2	Blockchiffren-basierte Hashfunktionen . . . . .	386
8.1.3	Dedizierte Hashfunktionen . . . . .	387
8.1.4	Message Authentication Code . . . . .	391
8.2	Elektronische Signaturen . . . . .	396
8.2.1	Anforderungen . . . . .	396
8.2.2	Erstellung elektronischer Signaturen . . . . .	398
8.2.3	Digitaler Signaturstandard (DSS) . . . . .	402
8.2.4	Signaturgesetz . . . . .	406
8.2.5	Fazit und Ausblick . . . . .	412

---

<b>9</b>	<b>Schlüsselmanagement</b>	<b>415</b>
9.1	Zertifizierung . . . . .	415
9.1.1	Zertifikate . . . . .	416
9.1.2	Zertifizierungsstelle . . . . .	417
9.1.3	Public-Key Infrastruktur . . . . .	421
9.2	Schlüsselerzeugung und -aufbewahrung . . . . .	428
9.2.1	Schlüsselerzeugung . . . . .	428
9.2.2	Schlüsselspeicherung und -vernichtung . . . . .	431
9.3	Schlüsselaustausch . . . . .	434
9.3.1	Schlüsselhierarchie . . . . .	434
9.3.2	Naives Austauschprotokoll . . . . .	437
9.3.3	Protokoll mit symmetrischen Verfahren . . . . .	439
9.3.4	Protokoll mit asymmetrischen Verfahren . . . . .	442
9.3.5	Leitlinien für die Protokollentwicklung . . . . .	444
9.3.6	Diffie-Hellman Verfahren . . . . .	446
9.4	Schlüsselrückgewinnung . . . . .	454
9.4.1	Systemmodell . . . . .	455
9.4.2	Grenzen und Risiken . . . . .	460
<b>10</b>	<b>Authentifikation</b>	<b>465</b>
10.1	Einführung . . . . .	465
10.2	Authentifikation durch Wissen . . . . .	467
10.2.1	Passwortverfahren . . . . .	468
10.2.2	Authentifikation in Unix . . . . .	481
10.2.3	Challenge-Response-Verfahren . . . . .	487
10.2.4	Zero-Knowledge-Verfahren . . . . .	492
10.3	Biometrie . . . . .	495
10.3.1	Einführung . . . . .	495
10.3.2	Biometrische Techniken . . . . .	497
10.3.3	Biometrische Authentifikation . . . . .	499
10.3.4	Fallbeispiel: Fingerabdruckerkennung . . . . .	502
10.3.5	Sicherheit biometrischer Techniken . . . . .	505
10.4	Authentifikation in verteilten Systemen . . . . .	508
10.4.1	RADIUS . . . . .	509
10.4.2	Kerberos-Authentifikationssystem . . . . .	514
<b>11</b>	<b>Digitale Identität</b>	<b>525</b>
11.1	Smartcards . . . . .	525
11.1.1	Smartcard-Architektur . . . . .	526
11.1.2	Betriebssystem und Sicherheitsmechanismen . . . . .	530
11.1.3	Fallbeispiele . . . . .	533
11.1.4	Smartcard-Sicherheit . . . . .	535

11.2	Elektronische Identifikationsausweise . . . . .	540
11.2.1	Elektronischer Reisepass (ePass) . . . . .	540
11.2.2	Personalausweis . . . . .	561
11.3	Universal Second Factor Authentication . . . . .	583
11.3.1	Registrierung eines U2F-Devices . . . . .	584
11.3.2	Login beim Web-Dienst . . . . .	588
11.3.3	Sicherheitsbetrachtungen . . . . .	591
11.3.4	U2F-Protokoll versus eID-Funktion . . . . .	598
11.4	Trusted Computing . . . . .	602
11.4.1	Trusted Computing Platform Alliance . . . . .	603
11.4.2	TCG-Architektur . . . . .	604
11.4.3	TPM . . . . .	609
11.4.4	Sicheres Booten . . . . .	623
11.5	Physically Unclonable Functions (PUF) . . . . .	633
11.5.1	Einführung . . . . .	634
11.5.2	Einsatz von PUFs in Sicherheitsprotokollen . . . . .	639
11.5.3	Sicherheitsuntersuchungen von PUFs . . . . .	642
<b>12</b>	<b>Zugriffskontrolle</b>	<b>643</b>
12.1	Einleitung . . . . .	643
12.2	Speicherschutz . . . . .	644
12.2.1	Betriebsmodi und Adressräume . . . . .	645
12.2.2	Virtueller Speicher . . . . .	646
12.3	Objektschutz . . . . .	650
12.3.1	Zugriffskontrolllisten . . . . .	651
12.3.2	Zugriffsausweise . . . . .	656
12.4	Zugriffskontrolle in Unix . . . . .	661
12.4.1	Identifikation . . . . .	661
12.4.2	Rechtevergabe . . . . .	662
12.4.3	Zugriffskontrolle . . . . .	667
12.5	Zugriffskontrolle unter Windows . . . . .	671
12.5.1	Architektur-Überblick . . . . .	671
12.5.2	Sicherheitssubsystem . . . . .	673
12.5.3	Datenstrukturen zur Zugriffskontrolle . . . . .	676
12.5.4	Zugriffskontrolle . . . . .	682
12.6	Verschlüsselnde Dateisysteme . . . . .	684
12.6.1	Encrypting File System (EFS) . . . . .	686
12.7	Systembestimmte Zugriffskontrolle . . . . .	692
12.8	Sprachbasierter Schutz . . . . .	695
12.8.1	Programmiersprache . . . . .	695
12.8.2	Übersetzer und Binder . . . . .	698

<b>12.9</b>	<b>Service-orientierte Architektur . . . . .</b>	<b>704</b>
12.9.1	Konzepte und Sicherheitsanforderungen . . . . .	704
12.9.2	Web-Services . . . . .	707
12.9.3	Web-Service Sicherheitsstandards . . . . .	712
12.9.4	SAML . . . . .	718
12.9.5	Offene Fragen . . . . .	723
<b>13</b>	<b>Sicherheit in Netzen . . . . .</b>	<b>727</b>
13.1	Firewall-Technologie . . . . .	728
13.1.1	Einführung . . . . .	728
13.1.2	Paketfilter . . . . .	731
13.1.3	Proxy-Firewall . . . . .	745
13.1.4	Applikationsfilter . . . . .	748
13.1.5	Architekturen . . . . .	752
13.1.6	Risiken und Grenzen . . . . .	755
13.2	OSI-Sicherheitsarchitektur . . . . .	760
13.2.1	Sicherheitsdienste . . . . .	761
13.2.2	Sicherheitsmechanismen . . . . .	764
13.3	Sichere Kommunikation . . . . .	769
13.3.1	Verschlüsselungs-Layer . . . . .	770
13.3.2	Virtual Private Network (VPN) . . . . .	777
13.4	IPSec . . . . .	782
13.4.1	Überblick . . . . .	784
13.4.2	Security Association und Policy-Datenbank . . . . .	786
13.4.3	AH-Protokoll . . . . .	791
13.4.4	ESP-Protokoll . . . . .	795
13.4.5	Schlüsselaustauschprotokoll IKE . . . . .	798
13.4.6	Sicherheit von IPSec . . . . .	804
13.5	SSL/TLS . . . . .	809
13.5.1	Überblick . . . . .	810
13.5.2	Handshake-Protokoll . . . . .	813
13.5.3	Record-Protokoll . . . . .	817
13.5.4	Sicherheit von SSL/TLS . . . . .	819
13.6	Sichere Anwendungsdienste . . . . .	829
13.6.1	Elektronische Mail . . . . .	829
13.6.2	Elektronischer Zahlungsverkehr . . . . .	847
<b>14</b>	<b>Sichere mobile und drahtlose Kommunikation . . . . .</b>	<b>857</b>
14.1	Einleitung . . . . .	857
14.1.1	Heterogenität der Netze . . . . .	858
14.1.2	Entwicklungsphasen . . . . .	859

14.2	GSM . . . . .	862
14.2.1	Grundlagen . . . . .	862
14.2.2	GSM-Grobarchitektur . . . . .	863
14.2.3	Identifikation und Authentifikation . . . . .	864
14.2.4	Gesprächsverschlüsselung . . . . .	868
14.2.5	Sicherheitsprobleme . . . . .	871
14.2.6	GPRS . . . . .	875
14.3	UMTS . . . . .	877
14.3.1	UMTS-Sicherheitsarchitektur . . . . .	878
14.3.2	Authentifikation und Schlüsselvereinbarung . . . . .	880
14.3.3	Vertraulichkeit und Integrität . . . . .	884
14.4	Long Term Evolution (LTE) und SAE . . . . .	886
14.4.1	EPC und LTE . . . . .	888
14.4.2	Interworking . . . . .	890
14.4.3	Sicherheitsarchitektur und Sicherheitsdienste . . . . .	892
14.4.4	Sicheres Interworking . . . . .	897
14.5	Funk-LAN (WLAN) . . . . .	900
14.5.1	Einführung . . . . .	901
14.5.2	Technische Grundlagen . . . . .	902
14.5.3	WLAN-Sicherheitsprobleme . . . . .	907
14.5.4	WEP und WPA . . . . .	909
14.5.5	802.11i Sicherheitsdienste (WPA2) . . . . .	912
14.5.6	802.1X-Framework und EAP . . . . .	921
14.6	Bluetooth . . . . .	926
14.6.1	Einordnung und Abgrenzung . . . . .	926
14.6.2	Technische Grundlagen . . . . .	927
14.6.3	Sicherheitsarchitektur . . . . .	932
14.6.4	Schlüsselmanagement . . . . .	937
14.6.5	Authentifikation . . . . .	942
14.6.6	Bluetooth-Sicherheitsprobleme . . . . .	945
14.6.7	Secure Simple Pairing . . . . .	948
	<b>Literaturverzeichnis</b>	<b>955</b>
	<b>Abkürzungsverzeichnis</b>	<b>969</b>
	<b>Index</b>	<b>979</b>