

# Inhaltsverzeichnis

<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 . . . . .	32
1.5	Sicherheitsrichtlinie . . . . .	34
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 . . . . .	78
2.6.2	Spam . . . . .	80
2.7	Mobiler Code . . . . .	82
2.7.1	Eigenschaften . . . . .	82
2.7.2	Sicherheitsbedrohungen . . . . .	83
2.7.3	Gegenmaßnahmen . . . . .	85
2.7.4	Mobile Apps . . . . .	88

<b>3</b>	<b>Internet-(Un)Sicherheit</b>	<b>95</b>
3.1	Einführung . . . . .	95
3.2	Internet-Protokollfamilie . . . . .	97
3.2.1	ISO/OSI-Referenzmodell . . . . .	97
3.2.2	Das TCP/IP-Referenzmodell . . . . .	104
3.2.3	Das Internet-Protokoll IP . . . . .	106
3.2.4	Das Transmission Control Protokoll TCP . . . . .	111
3.2.5	Das User Datagram Protocol UDP . . . . .	114
3.2.6	DHCP und NAT . . . . .	116
3.3	Sicherheitsprobleme . . . . .	119
3.3.1	Sicherheitsprobleme von IP . . . . .	119
3.3.2	Sicherheitsprobleme von ICMP . . . . .	125
3.3.3	Sicherheitsprobleme von ARP . . . . .	127
3.3.4	Sicherheitsprobleme von UDP und TCP . . . . .	131
3.4	Sicherheitsprobleme von Netzdiensten . . . . .	135
3.4.1	Domain Name Service (DNS) . . . . .	136
3.4.2	Network File System (NFS) . . . . .	145
3.4.3	Network Information System (NIS) . . . . .	150
3.4.4	Weitere Dienste . . . . .	152
3.5	Web-Anwendungen . . . . .	157
3.5.1	World Wide Web (WWW) . . . . .	157
3.5.2	Sicherheitsprobleme . . . . .	163
3.5.3	OWASP Top-Ten Sicherheitsprobleme . . . . .	172
3.6	Analysetools und Systemhärtung . . . . .	181
<b>4</b>	<b>Security Engineering</b>	<b>189</b>
4.1	Entwicklungsprozess . . . . .	190
4.1.1	Allgemeine Konstruktionsprinzipien . . . . .	190
4.1.2	Phasen . . . . .	191
4.1.3	BSI-Sicherheitsprozess . . . . .	192
4.2	Strukturanalyse . . . . .	196
4.3	Schutzbedarfsermittlung . . . . .	198
4.3.1	Schadensszenarien . . . . .	199
4.3.2	Schutzbedarf . . . . .	201
4.4	Bedrohungsanalyse . . . . .	203
4.4.1	Bedrohungsmatrix . . . . .	203
4.4.2	Bedrohungsbaum . . . . .	205
4.5	Risikoanalyse . . . . .	210
4.5.1	Attributierung . . . . .	211
4.5.2	Penetrationstests . . . . .	216
4.6	Sicherheitsarchitektur und Betrieb . . . . .	218
4.6.1	Sicherheitsstrategie und Sicherheitsmodell . . . . .	218

4.6.2	Systemarchitektur und Validierung . . . . .	219
4.6.3	Aufrechterhaltung im laufenden Betrieb . . . . .	219
4.7	Sicherheitsgrundfunktionen . . . . .	220
4.8	Realisierung der Grundfunktionen . . . . .	224
4.9	Security Development Lifecycle (SDL) . . . . .	226
4.9.1	Die Entwicklungsphasen . . . . .	227
4.9.2	Bedrohungs- und Risikoanalyse . . . . .	228
<b>5</b>	<b>Bewertungskriterien</b>	<b>233</b>
5.1	TCSEC-Kriterien . . . . .	233
5.1.1	Sicherheitsstufen . . . . .	234
5.1.2	Kritik am Orange Book . . . . .	235
5.2	IT-Kriterien . . . . .	237
5.2.1	Mechanismen . . . . .	237
5.2.2	Funktionsklassen . . . . .	238
5.2.3	Qualität . . . . .	238
5.3	ITSEC-Kriterien . . . . .	239
5.3.1	Evaluationsstufen . . . . .	240
5.3.2	Qualität und Bewertung . . . . .	241
5.4	Common Criteria . . . . .	242
5.4.1	Überblick über die CC . . . . .	243
5.4.2	CC-Funktionsklassen . . . . .	247
5.4.3	Schutzprofile . . . . .	249
5.4.4	Vertrauenswürdigkeitsklassen . . . . .	252
5.5	Zertifizierung . . . . .	258
<b>6</b>	<b>Sicherheitsmodelle</b>	<b>261</b>
6.1	Modell-Klassifikation . . . . .	261
6.1.1	Objekte und Subjekte . . . . .	262
6.1.2	Zugriffsrechte . . . . .	263
6.1.3	Zugriffsbeschränkungen . . . . .	264
6.1.4	Sicherheitsstrategien . . . . .	264
6.2	Zugriffskontrollmodelle . . . . .	266
6.2.1	Zugriffsmatrix-Modell . . . . .	266
6.2.2	Rollenbasierte Modelle . . . . .	274
6.2.3	Chinese-Wall Modell . . . . .	282
6.2.4	Bell-LaPadula Modell . . . . .	287
6.3	Informationsflussmodelle . . . . .	294
6.3.1	Verbands-Modell . . . . .	294
6.4	Fazit und Ausblick . . . . .	298
<b>7</b>	<b>Kryptografische Verfahren</b>	<b>301</b>
7.1	Einführung . . . . .	301

7.2	Steganografie . . . . .	303
7.2.1	Linguistische Steganografie . . . . .	304
7.2.2	Technische Steganografie . . . . .	305
7.3	Grundlagen kryptografischer Verfahren . . . . .	307
7.3.1	Kryptografische Systeme . . . . .	307
7.3.2	Anforderungen . . . . .	312
7.4	Informationstheorie . . . . .	314
7.4.1	Stochastische und kryptografische Kanäle . . . . .	315
7.4.2	Entropie und Redundanz . . . . .	317
7.4.3	Sicherheit kryptografischer Systeme . . . . .	318
7.5	Symmetrische Verfahren . . . . .	324
7.5.1	Permutation und Substitution . . . . .	324
7.5.2	Block- und Stromchiffren . . . . .	325
7.5.3	Betriebsmodi von Blockchiffren . . . . .	330
7.5.4	Data Encryption Standard . . . . .	336
7.5.5	AES . . . . .	346
7.6	Asymmetrische Verfahren . . . . .	352
7.6.1	Eigenschaften . . . . .	352
7.6.2	Das RSA-Verfahren . . . . .	356
7.7	Kryptoanalyse . . . . .	368
7.7.1	Klassen kryptografischer Angriffe . . . . .	368
7.7.2	Substitutionschiffren . . . . .	370
7.7.3	Differentielle Kryptoanalyse . . . . .	372
7.7.4	Lineare Kryptoanalyse . . . . .	374
7.8	Kryptoregulierung . . . . .	375
7.8.1	Hintergrund . . . . .	375
7.8.2	Internationale Regelungen . . . . .	376
7.8.3	Kryptopolitik in Deutschland . . . . .	379
<b>8</b>	<b>Hashfunktionen und elektronische Signaturen</b>	<b>381</b>
8.1	Hashfunktionen . . . . .	381
8.1.1	Grundlagen . . . . .	382
8.1.2	Blockchiffren-basierte Hashfunktionen . . . . .	388
8.1.3	Dedizierte Hashfunktionen . . . . .	389
8.1.4	Message Authentication Code . . . . .	393
8.2	Elektronische Signaturen . . . . .	398
8.2.1	Anforderungen . . . . .	398
8.2.2	Erstellung elektronischer Signaturen . . . . .	400
8.2.3	Digitaler Signaturstandard (DSS) . . . . .	404
8.2.4	Signaturgesetz . . . . .	408
8.2.5	Fazit und Ausblick . . . . .	414

<b>9</b>	<b>Schlüsselmanagement</b>	<b>417</b>
9.1	Zertifizierung . . . . .	417
9.1.1	Zertifikate . . . . .	418
9.1.2	Zertifizierungsstelle . . . . .	419
9.1.3	Public-Key Infrastruktur . . . . .	423
9.2	Schlüsselerzeugung und -aufbewahrung . . . . .	431
9.2.1	Schlüsselerzeugung . . . . .	431
9.2.2	Schlüsselspeicherung und -vernichtung . . . . .	434
9.3	Schlüsselaustausch . . . . .	437
9.3.1	Schlüsselhierarchie . . . . .	437
9.3.2	Naives Austauschprotokoll . . . . .	439
9.3.3	Protokoll mit symmetrischen Verfahren . . . . .	441
9.3.4	Protokoll mit asymmetrischen Verfahren . . . . .	445
9.3.5	Leitlinien für die Protokollentwicklung . . . . .	447
9.3.6	Diffie-Hellman Verfahren . . . . .	449
9.4	Schlüsselerückgewinnung . . . . .	455
9.4.1	Systemmodell . . . . .	456
9.4.2	Grenzen und Risiken . . . . .	461
<b>10</b>	<b>Authentifikation</b>	<b>465</b>
10.1	Einführung . . . . .	465
10.2	Authentifikation durch Wissen . . . . .	468
10.2.1	Passwortverfahren . . . . .	468
10.2.2	Authentifikation in Unix . . . . .	482
10.2.3	Challenge-Response-Verfahren . . . . .	488
10.2.4	Zero-Knowledge-Verfahren . . . . .	492
10.3	Biometrie . . . . .	495
10.3.1	Einführung . . . . .	495
10.3.2	Biometrische Techniken . . . . .	498
10.3.3	Biometrische Authentifikation . . . . .	501
10.3.4	Fallbeispiel: Fingerabdruckerkennung . . . . .	503
10.3.5	Sicherheit biometrischer Techniken . . . . .	507
10.4	Authentifikation in verteilten Systemen . . . . .	511
10.4.1	RADIUS . . . . .	511
10.4.2	Remote Procedure Call . . . . .	516
10.4.3	Secure RPC . . . . .	518
10.4.4	Kerberos-Authentifikationssystem . . . . .	521
10.4.5	Authentifikations-Logik . . . . .	531
<b>11</b>	<b>Digitale Identität</b>	<b>541</b>
11.1	Smartcards . . . . .	541
11.1.1	Smartcard-Architektur . . . . .	542

11.1.2	Betriebssystem und Sicherheitsmechanismen . . . . .	545
11.1.3	Fallbeispiele . . . . .	549
11.1.4	Smartcard-Sicherheit . . . . .	552
11.2	Elektronische Identifikationsausweise . . . . .	556
11.2.1	Elektronischer Reisepass (ePass) . . . . .	557
11.2.2	Elektronischer Personalausweis (nPA) . . . . .	577
11.3	Trusted Computing . . . . .	601
11.3.1	Trusted Computing Platform Alliance . . . . .	602
11.3.2	TCG-Architektur . . . . .	604
11.3.3	TPM . . . . .	609
11.3.4	Sicheres Booten . . . . .	623
<b>12</b>	<b>Zugriffskontrolle</b>	<b>635</b>
12.1	Einleitung . . . . .	635
12.2	Speicherschutz . . . . .	636
12.2.1	Betriebsmodi und Adressräume . . . . .	637
12.2.2	Virtueller Speicher . . . . .	638
12.3	Objektschutz . . . . .	642
12.3.1	Zugriffskontrolllisten . . . . .	643
12.3.2	Zugriffsausweise . . . . .	647
12.4	Zugriffskontrolle in Unix . . . . .	653
12.4.1	Identifikation . . . . .	653
12.4.2	Rechtevergabe . . . . .	654
12.4.3	Zugriffskontrolle . . . . .	659
12.5	Zugriffskontrolle unter Windows . . . . .	663
12.5.1	Architektur-Überblick . . . . .	663
12.5.2	Sicherheitssystem . . . . .	665
12.5.3	Datenstrukturen zur Zugriffskontrolle . . . . .	668
12.5.4	Zugriffskontrolle . . . . .	673
12.6	Verschlüsselnde Dateisysteme . . . . .	676
12.6.1	Klassifikation . . . . .	678
12.6.2	Encrypting File System (EFS) . . . . .	680
12.7	Systembestimmte Zugriffskontrolle . . . . .	686
12.8	Sprachbasierter Schutz . . . . .	689
12.8.1	Programmiersprache . . . . .	689
12.8.2	Übersetzer und Binder . . . . .	692
12.9	Java-Sicherheit . . . . .	698
12.9.1	Die Programmiersprache . . . . .	699
12.9.2	Sicherheitsarchitektur . . . . .	700
12.9.3	Java-Sicherheitsmodelle . . . . .	705

<b>13</b>	<b>Sicherheit in Netzen</b>	<b>713</b>
13.1	Firewall-Technologie . . . . .	714
13.1.1	Einführung . . . . .	714
13.1.2	Paketfilter . . . . .	717
13.1.3	Proxy-Firewall . . . . .	731
13.1.4	Applikationsfilter . . . . .	735
13.1.5	Architekturen . . . . .	739
13.1.6	Risiken und Grenzen . . . . .	742
13.2	OSI-Sicherheitsarchitektur . . . . .	748
13.2.1	Sicherheitsdienste . . . . .	748
13.2.2	Sicherheitsmechanismen . . . . .	751
13.3	Sichere Kommunikation . . . . .	756
13.3.1	Verschlüsselungs-Layer . . . . .	758
13.3.2	Virtual Private Network (VPN) . . . . .	765
13.4	IPSec . . . . .	770
13.4.1	Überblick . . . . .	772
13.4.2	Security Association und Policy-Datenbank . . . . .	774
13.4.3	AH-Protokoll . . . . .	779
13.4.4	ESP-Protokoll . . . . .	782
13.4.5	Schlüsselaustauschprotokoll IKE . . . . .	786
13.4.6	Sicherheit von IPSec . . . . .	791
13.5	SSL/TLS . . . . .	796
13.5.1	Überblick . . . . .	798
13.5.2	Handshake-Protokoll . . . . .	801
13.5.3	Record-Protokoll . . . . .	804
13.5.4	Sicherheit von SSL/TLS . . . . .	807
13.6	Sichere Anwendungsdienste . . . . .	812
13.6.1	Elektronische Mail . . . . .	813
13.6.2	Elektronischer Zahlungsverkehr . . . . .	831
13.7	Service-orientierte Architektur . . . . .	839
13.7.1	Konzepte und Sicherheitsanforderungen . . . . .	839
13.7.2	Web-Services . . . . .	842
13.7.3	Web-Service Sicherheitsstandards . . . . .	847
13.7.4	SAML . . . . .	854
13.7.5	Offene Fragen . . . . .	859
<b>14</b>	<b>Sichere mobile und drahtlose Kommunikation</b>	<b>863</b>
14.1	Einleitung . . . . .	863
14.1.1	Heterogenität der Netze . . . . .	864
14.1.2	Entwicklungsphasen . . . . .	865
14.2	GSM . . . . .	868
14.2.1	Grundlagen . . . . .	868

14.2.2	GSM-Grobarchitektur . . . . .	869
14.2.3	Identifikation und Authentifikation . . . . .	870
14.2.4	Gesprächsverschlüsselung . . . . .	875
14.2.5	Sicherheitsprobleme . . . . .	877
14.2.6	GPRS . . . . .	881
14.3	UMTS . . . . .	883
14.3.1	UMTS-Sicherheitsarchitektur . . . . .	884
14.3.2	Authentifikation und Schlüsselvereinbarung . . . . .	887
14.3.3	Vertraulichkeit und Integrität . . . . .	890
14.4	Funk-LAN (WLAN) . . . . .	892
14.4.1	Grundlagen . . . . .	893
14.4.2	WLAN-Sicherheitsprobleme . . . . .	900
14.4.3	WEP . . . . .	905
14.4.4	WPA und 802.11i . . . . .	919
14.5	Bluetooth . . . . .	934
14.5.1	Einordnung und Abgrenzung . . . . .	935
14.5.2	Technische Grundlagen . . . . .	938
14.5.3	Sicherheitsarchitektur . . . . .	943
14.5.4	Schlüsselmanagement . . . . .	948
14.5.5	Authentifikation . . . . .	953
14.5.6	Bluetooth-Sicherheitsprobleme . . . . .	956
14.5.7	Secure Simple Pairing . . . . .	959
14.6	Long Term Evolution (LTE) und SAE . . . . .	963
14.6.1	EPC und LTE . . . . .	965
14.6.2	Interworking . . . . .	967
14.6.3	Sicherheitsarchitektur und Sicherheitsdienste . . . . .	968
14.6.4	Sicheres Interworking . . . . .	975
<b>Literaturverzeichnis</b>		<b>979</b>
<b>Abkürzungsverzeichnis</b>		<b>995</b>
<b>Index</b>		<b>1005</b>