

# Inhaltsverzeichnis

<b>1</b>	<b>Einführung</b>	<b>1</b>
1.1	Grundlegende Begriffe . . . . .	1
1.2	Schutzziele . . . . .	6
1.3	Schwachstellen, Bedrohungen, Angriffe . . . . .	13
1.4	Computer Forensik . . . . .	25
1.5	Sicherheitsstrategie . . . . .	27
1.6	Sicherheitsinfrastruktur . . . . .	30
<b>2</b>	<b>Spezielle Bedrohungen</b>	<b>35</b>
2.1	Einführung . . . . .	35
2.2	Buffer-Overflow . . . . .	37
2.2.1	Einführung . . . . .	37
2.2.2	Angriffe . . . . .	40
2.2.3	Gegenmaßnahmen . . . . .	43
2.3	Computerviren . . . . .	45
2.3.1	Eigenschaften . . . . .	45
2.3.2	Viren-Typen . . . . .	47
2.3.3	Gegenmaßnahmen . . . . .	53
2.4	Würmer . . . . .	57
2.5	Trojanisches Pferd . . . . .	63
2.5.1	Eigenschaften . . . . .	63
2.5.2	Gegenmaßnahmen . . . . .	65
2.6	Mobiler Code . . . . .	69
2.6.1	Eigenschaften . . . . .	69
2.6.2	Sicherheitsbedrohungen . . . . .	70
2.6.3	Gegenmaßnahmen . . . . .	72
<b>3</b>	<b>Internet-(Un)Sicherheit</b>	<b>75</b>
3.1	Einführung . . . . .	75
3.2	Internet-Protokollfamilie . . . . .	77
3.2.1	ISO/OSI-Referenzmodell . . . . .	77
3.2.2	Das TCP/IP-Referenzmodell . . . . .	83
3.2.3	Das Internet-Protokoll IP . . . . .	85

3.2.4	Das Transmission Control Protokoll TCP . . . . .	88
3.2.5	Das User Datagram Protocol UDP . . . . .	90
3.2.6	DHCP und NAT . . . . .	92
3.3	Sicherheitsprobleme . . . . .	95
3.3.1	Sicherheitsprobleme von IP . . . . .	95
3.3.2	Sicherheitsprobleme von ICMP . . . . .	101
3.3.3	Sicherheitsprobleme von ARP . . . . .	103
3.3.4	Sicherheitsprobleme von UDP und TCP . . . . .	104
3.4	Sicherheitsprobleme von Netzdiensten . . . . .	108
3.4.1	Domain Name Service (DNS) . . . . .	109
3.4.2	Network File System (NFS) . . . . .	114
3.4.3	Network Information System (NIS) . . . . .	120
3.4.4	World Wide Web (WWW) . . . . .	121
3.4.5	Weitere Dienste . . . . .	135
3.4.6	Angriffsszenario . . . . .	139
3.5	Analysetools und Systemhärtung . . . . .	141
<b>4</b>	<b>Security Engineering</b>	<b>151</b>
4.1	Entwicklungsprozess . . . . .	152
4.1.1	Allgemeine Konstruktionsprinzipien . . . . .	152
4.1.2	Phasen . . . . .	153
4.1.3	BSI-Sicherheitsprozess . . . . .	154
4.2	Strukturanalyse . . . . .	157
4.3	Schutzbedarfsermittlung . . . . .	159
4.3.1	Schadensszenarien . . . . .	160
4.3.2	Schutzbedarf . . . . .	162
4.4	Bedrohungsanalyse . . . . .	163
4.4.1	Bedrohungsmatrix . . . . .	164
4.4.2	Bedrohungsbaum . . . . .	165
4.5	Risikoanalyse . . . . .	171
4.5.1	Attributierung . . . . .	172
4.5.2	Penetrationstests . . . . .	177
4.6	Sicherheitsstrategie und -modell . . . . .	179
4.7	Systemarchitektur und Validierung . . . . .	180
4.8	Aufrechterhaltung im laufenden Betrieb . . . . .	181
4.8.1	Dynamische Überwachung . . . . .	181
4.8.2	Der elektronische Sicherheitsinspektor (eSI) . . . . .	182
4.9	Sicherheitsgrundfunktionen . . . . .	189
4.10	Realisierung der Grundfunktionen . . . . .	193
4.11	Beispiel: Elektronische Shopping Mall . . . . .	195
4.11.1	Systemanforderungen und Einsatzumgebung . . . . .	196
4.11.2	Bedrohungsanalyse . . . . .	196

4.11.3	Risikoanalyse . . . . .	201
4.11.4	Sicherheitsstrategie . . . . .	206
4.11.5	Sicherheitsarchitektur . . . . .	209
<b>5</b>	<b>Bewertungskriterien</b>	<b>211</b>
5.1	TCSEC-Kriterien . . . . .	211
5.1.1	Sicherheitsstufen . . . . .	211
5.1.2	Kritik am Orange Book . . . . .	214
5.1.3	Erkennen verdeckter Informationskanäle . . . . .	215
5.2	IT-Kriterien . . . . .	215
5.2.1	Mechanismen . . . . .	216
5.2.2	Funktionsklassen . . . . .	217
5.2.3	Qualität und Zertifikat . . . . .	218
5.3	ITSEC-Kriterien . . . . .	219
5.3.1	Evaluationsstufen . . . . .	220
5.3.2	Qualität und Bewertung . . . . .	221
5.4	Zertifizierung . . . . .	222
5.5	Common Criteria . . . . .	224
5.5.1	Einführung . . . . .	224
5.5.2	Überblick über die CC . . . . .	225
5.5.3	CC-Funktionsklassen . . . . .	230
5.5.4	Schutzprofile . . . . .	231
5.5.5	Vertrauenswürdigkeitsklassen . . . . .	233
<b>6</b>	<b>Sicherheitsmodelle</b>	<b>241</b>
6.1	Modell-Klassifikation . . . . .	241
6.1.1	Objekte und Subjekte . . . . .	242
6.1.2	Zugriffsrechte . . . . .	243
6.1.3	Zugriffsbeschränkungen . . . . .	244
6.1.4	Sicherheitsstrategien . . . . .	244
6.1.5	Klassifikationsschema . . . . .	246
6.2	Zugriffskontrollmodelle . . . . .	247
6.2.1	Zugriffsmatrix-Modell . . . . .	248
6.2.2	Rollenbasierte Modelle . . . . .	256
6.2.3	Chinese-Wall Modell . . . . .	263
6.2.4	Bell-LaPadula Modell . . . . .	268
6.3	Informationsflussmodelle . . . . .	275
6.3.1	Verbands-Modell . . . . .	275
6.4	Einsatz-Leitlinien . . . . .	278
<b>7</b>	<b>Kryptografische Verfahren</b>	<b>281</b>
7.1	Einführung . . . . .	281
7.2	Steganografie . . . . .	283

7.2.1	Linguistische Steganografie . . . . .	284
7.2.2	Technische Steganografie . . . . .	285
7.3	Grundlagen kryptografischer Verfahren . . . . .	287
7.3.1	Kryptografische Systeme . . . . .	287
7.3.2	Anforderungen . . . . .	291
7.4	Informationstheorie . . . . .	294
7.4.1	Stochastische und kryptografische Kanäle . . . . .	294
7.4.2	Entropie und Redundanz . . . . .	296
7.4.3	Sicherheit kryptografischer Systeme . . . . .	297
7.5	Symmetrische Verfahren . . . . .	303
7.5.1	Permutation und Substitution . . . . .	303
7.5.2	Block- und Stromchiffren . . . . .	304
7.5.3	Betriebsmodi von Blockchiffren . . . . .	309
7.5.4	Data Encryption Standard . . . . .	313
7.5.5	AES . . . . .	322
7.6	Asymmetrische Verfahren . . . . .	325
7.6.1	Eigenschaften . . . . .	326
7.6.2	Das RSA-Verfahren . . . . .	329
7.7	Kryptoanalyse . . . . .	340
7.7.1	Klassen kryptografischer Angriffe . . . . .	341
7.7.2	Substitutionschiffren . . . . .	342
7.7.3	Differentielle Kryptoanalyse . . . . .	344
7.7.4	Lineare Kryptoanalyse . . . . .	346
7.8	Kryptoregulierung . . . . .	347
7.8.1	Hintergrund . . . . .	347
7.8.2	Internationale Regelungen . . . . .	349
7.8.3	Kryptopolitik in Deutschland . . . . .	351
<b>8</b>	<b>Hashfunktionen und elektronische Signaturen</b>	<b>353</b>
8.1	Hashfunktionen . . . . .	353
8.1.1	Grundlagen . . . . .	354
8.1.2	Blockchiffren-basierte Hashfunktionen . . . . .	359
8.1.3	Dedizierte Hashfunktionen . . . . .	361
8.1.4	Message Authentication Code . . . . .	365
8.2	Elektronische Signaturen . . . . .	370
8.2.1	Anforderungen . . . . .	370
8.2.2	Erstellung elektronischer Signaturen . . . . .	371
8.2.3	Digitaler Signaturstandard (DSS) . . . . .	378
8.2.4	Signaturgesetz . . . . .	380
<b>9</b>	<b>Schlüsselmanagement</b>	<b>389</b>
9.1	Zertifizierung . . . . .	389

9.1.1	Zertifikate . . . . .	390
9.1.2	Zertifizierungsstelle . . . . .	391
9.1.3	Public-Key Infrastruktur . . . . .	395
9.2	Schlüsselerzeugung und -aufbewahrung . . . . .	402
9.2.1	Schlüsselerzeugung . . . . .	403
9.2.2	Schlüsselspeicherung und -vernichtung . . . . .	405
9.3	Schlüsselaustausch . . . . .	408
9.3.1	Schlüsselhierarchie . . . . .	409
9.3.2	Naives Austauschprotokoll . . . . .	411
9.3.3	Protokoll mit symmetrischen Verfahren . . . . .	412
9.3.4	Protokoll mit asymmetrischen Verfahren . . . . .	416
9.3.5	Leitlinien für die Protokollentwicklung . . . . .	418
9.3.6	Diffie-Hellman Verfahren . . . . .	420
9.4	Schlüsselrückgewinnung . . . . .	426
9.4.1	Systemmodell . . . . .	427
9.4.2	Grenzen und Risiken . . . . .	432
<b>10</b>	<b>Authentifikation</b>	<b>437</b>
10.1	Einführung . . . . .	438
10.2	Authentifikation durch Wissen . . . . .	440
10.2.1	Passwortverfahren . . . . .	440
10.2.2	Authentifikation in Unix . . . . .	451
10.2.3	Challenge-Response-Verfahren . . . . .	457
10.2.4	Zero-Knowledge-Verfahren . . . . .	462
10.3	Smartcard . . . . .	465
10.3.1	Architektur . . . . .	466
10.3.2	Sicherheit . . . . .	469
10.4	Biometrie . . . . .	478
10.4.1	Einführung . . . . .	478
10.4.2	Biometrische Techniken . . . . .	480
10.4.3	Biometrische Authentifikation . . . . .	484
10.4.4	Fallbeispiel: Fingerabdruckerkennung . . . . .	486
10.4.5	Sicherheit biometrischer Techniken . . . . .	489
10.5	Authentifikation in verteilten Systemen . . . . .	493
10.5.1	RADIUS . . . . .	494
10.5.2	Remote Procedure Call . . . . .	499
10.5.3	Secure RPC . . . . .	500
10.5.4	Kerberos-Authentifikationssystem . . . . .	503
10.5.5	Microsoft Passport-Protokoll . . . . .	514
10.5.6	Authentifikations-Logik . . . . .	529

<b>11</b>	<b>Zugriffskontrolle</b>	<b>539</b>
11.1	Einleitung . . . . .	539
11.2	Speicherschutz . . . . .	540
11.2.1	Betriebsmodi und Adressräume . . . . .	541
11.2.2	Virtueller Speicher . . . . .	542
11.3	Objektschutz . . . . .	546
11.3.1	Zugriffskontrolllisten . . . . .	548
11.3.2	Zugriffsausweise . . . . .	555
11.4	Zugriffskontrolle in Unix . . . . .	559
11.4.1	Identifikation . . . . .	560
11.4.2	Rechtevergabe . . . . .	561
11.4.3	Zugriffskontrolle . . . . .	566
11.5	Zugriffskontrolle unter Windows 2000 . . . . .	569
11.5.1	Architektur-Überblick . . . . .	570
11.5.2	Sicherheitssystem . . . . .	572
11.5.3	Datenstrukturen zur Zugriffskontrolle . . . . .	575
11.5.4	Zugriffskontrolle . . . . .	580
11.6	Verschlüsselnde Dateisysteme . . . . .	583
11.6.1	Einführung . . . . .	583
11.6.2	Klassifikation . . . . .	584
11.6.3	Encrypting File System (EFS) . . . . .	586
11.7	Systembestimmte Zugriffskontrolle . . . . .	592
11.8	Sprachbasierter Schutz . . . . .	595
11.8.1	Programmiersprache . . . . .	595
11.8.2	Übersetzer und Binder . . . . .	599
11.9	Java-Sicherheit . . . . .	604
11.9.1	Die Programmiersprache . . . . .	605
11.9.2	Sicherheitsarchitektur . . . . .	606
11.9.3	Sicherheitsmodelle . . . . .	611
11.9.4	Fazit . . . . .	616
11.10	Trusted Computing . . . . .	617
11.10.1	Einführung . . . . .	618
11.10.2	TCG-Architektur-Überblick . . . . .	620
11.10.3	TPM . . . . .	626
11.10.4	TPM-Schlüssel . . . . .	630
11.10.5	Sicheres Booten . . . . .	639
11.10.6	Einsatzmöglichkeiten für TCG-Plattformen . . . . .	644
11.10.7	Fazit und offene Probleme . . . . .	645
<b>12</b>	<b>Sicherheit in Netzen</b>	<b>651</b>
12.1	Firewall-Technologie . . . . .	652
12.1.1	Einführung . . . . .	652

12.1.2	Paketfilter . . . . .	655
12.1.3	Proxy-Firewall . . . . .	670
12.1.4	Applikationsfilter . . . . .	674
12.1.5	Architekturen . . . . .	678
12.1.6	Risiken und Grenzen . . . . .	681
12.2	OSI-Sicherheitsarchitektur . . . . .	687
12.2.1	Sicherheitsdienste . . . . .	687
12.2.2	Sicherheitsmechanismen . . . . .	690
12.3	Sichere Kommunikation . . . . .	696
12.3.1	ISO/OSI-Einordnung . . . . .	697
12.3.2	Virtual Private Network (VPN) . . . . .	704
12.4	IPSec . . . . .	708
12.4.1	Überblick . . . . .	710
12.4.2	Security Association und Policy-Datenbank . . . . .	712
12.4.3	AH-Protokoll . . . . .	717
12.4.4	ESP-Protokoll . . . . .	721
12.4.5	Schlüsselaustauschprotokoll IKE . . . . .	725
12.4.6	Sicherheit von IPSec . . . . .	730
12.5	Secure Socket Layer (SSL) . . . . .	736
12.5.1	Überblick . . . . .	736
12.5.2	Handshake-Protokoll . . . . .	739
12.5.3	Record-Protokoll . . . . .	743
12.5.4	Sicherheit von SSL . . . . .	745
12.6	Sichere Anwendungsdienste . . . . .	748
12.6.1	Elektronische Mail . . . . .	748
12.6.2	Elektronischer Zahlungsverkehr . . . . .	767
<b>13</b>	<b>Sichere mobile und drahtlose Kommunikation</b>	<b>777</b>
13.1	Einleitung . . . . .	778
13.1.1	Heterogenität der Netze . . . . .	778
13.1.2	Entwicklungsphasen . . . . .	779
13.2	GSM . . . . .	783
13.2.1	Grundlagen . . . . .	783
13.2.2	GSM-Grobarchitektur . . . . .	784
13.2.3	Identifikation und Authentifikation . . . . .	785
13.2.4	Gesprächsverschlüsselung . . . . .	789
13.2.5	Sicherheitsprobleme . . . . .	792
13.2.6	Weiterentwicklungen . . . . .	795
13.2.7	GPRS . . . . .	797
13.3	UMTS . . . . .	799
13.3.1	UMTS-Sicherheitsarchitektur . . . . .	800
13.3.2	Authentifikation und Schlüsselvereinbarung . . . . .	802

13.3.3	Vertraulichkeit und Integrität . . . . .	806
13.3.4	Fazit . . . . .	807
13.4	Funk-LAN (WLAN) . . . . .	808
13.4.1	Einführung . . . . .	808
13.4.2	Technische Grundlagen . . . . .	811
13.4.3	WLAN-Sicherheitsprobleme . . . . .	815
13.4.4	Einbindung eines WLAN in die Netztopologie . . . . .	820
13.4.5	WEP im Überblick . . . . .	821
13.4.6	WEP-Authentifikation . . . . .	823
13.4.7	WEP-Integrität . . . . .	826
13.4.8	WEP-Vertraulichkeit . . . . .	829
13.4.9	Zusätzliche Sicherheitsmaßnahmen . . . . .	833
13.4.10	Weiterentwicklungen des 802.11-Standards . . . . .	835
13.4.11	802.1X-Framework und EAP . . . . .	837
13.4.12	TKIP . . . . .	842
13.5	Bluetooth . . . . .	848
13.5.1	Einordnung und Abgrenzung . . . . .	849
13.5.2	Technische Grundlagen . . . . .	851
13.5.3	Sicherheitsarchitektur . . . . .	856
13.5.4	Schlüsselmanagement . . . . .	862
13.5.5	Authentifikation . . . . .	866
13.5.6	Bluetooth-Sicherheitsprobleme . . . . .	870
13.6	Future Net . . . . .	874
13.6.1	Entwicklungsstufen . . . . .	874
13.6.2	Vom Informations- zum Wissensmanagement . . . . .	876
13.6.3	Next Generation Networks . . . . .	877
<b>Literaturverzeichnis</b>		<b>883</b>
<b>Glossar</b>		<b>899</b>
<b>Index</b>		<b>909</b>