

Inhaltsverzeichnis

1	Einführung	1
1.1	Grundlegende Begriffe	1
1.2	Schutzziele	6
1.3	Schwachstellen, Bedrohungen, Angriffe	14
1.3.1	Bedrohungen	15
1.3.2	Angriffs- und Angreifer-Typen	17
1.3.3	Rechtliche Rahmenbedingungen	26
1.4	Computer Forensik	31
1.5	Sicherheitsstrategie	33
1.6	Sicherheitsinfrastruktur	36
2	Spezielle Bedrohungen	43
2.1	Einführung	43
2.2	Buffer-Overflow	45
2.2.1	Einführung	46
2.2.2	Angriffe	48
2.2.3	Gegenmaßnahmen	51
2.3	Computerviren	53
2.3.1	Eigenschaften	53
2.3.2	Viren-Typen	55
2.3.3	Gegenmaßnahmen	62
2.4	Würmer	65
2.5	Trojanisches Pferd	70
2.5.1	Eigenschaften	71
2.5.2	Gegenmaßnahmen	73
2.6	Bot-Netze und Spam	75
2.6.1	Bot-Netze	75
2.6.2	Spam	77
2.7	Mobiler Code	79
2.7.1	Eigenschaften	79
2.7.2	Sicherheitsbedrohungen	80
2.7.3	Gegenmaßnahmen	83

3	Internet-(Un)Sicherheit	85
3.1	Einführung	85
3.2	Internet-Protokollfamilie	87
3.2.1	ISO/OSI-Referenzmodell	87
3.2.2	Das TCP/IP-Referenzmodell	94
3.2.3	Das Internet-Protokoll IP	96
3.2.4	Das Transmission Control Protokoll TCP	98
3.2.5	Das User Datagram Protocol UDP	101
3.2.6	DHCP und NAT	103
3.3	Sicherheitsprobleme	106
3.3.1	Sicherheitsprobleme von IP	106
3.3.2	Sicherheitsprobleme von ICMP	112
3.3.3	Sicherheitsprobleme von ARP	114
3.3.4	Sicherheitsprobleme von UDP und TCP	115
3.4	Sicherheitsprobleme von Netzdiensten	119
3.4.1	Domain Name Service (DNS)	120
3.4.2	Network File System (NFS)	125
3.4.3	Network Information System (NIS)	131
3.4.4	Weitere Dienste	132
3.5	Web-Anwendungen	137
3.5.1	World Wide Web (WWW)	137
3.5.2	Sicherheitsprobleme	142
3.5.3	OWASP Top-Ten Sicherheitsprobleme	149
3.6	Analysertools und Systemhärtung	158
4	Security Engineering	167
4.1	Entwicklungsprozess	168
4.1.1	Allgemeine Konstruktionsprinzipien	168
4.1.2	Phasen	169
4.1.3	BSI-Sicherheitsprozess	170
4.2	Strukturanalyse	174
4.3	Schutzbedarfsermittlung	176
4.3.1	Schadensszenarien	176
4.3.2	Schutzbedarf	178
4.4	Bedrohungsanalyse	180
4.4.1	Bedrohungsmatrix	181
4.4.2	Bedrohungsbaum	182
4.5	Risikoanalyse	188
4.5.1	Attributierung	189
4.5.2	Penetrationstests	194
4.6	Sicherheitsarchitektur und Betrieb	196
4.6.1	Sicherheitsstrategie und Sicherheitsmodell	196

4.6.2	Systemarchitektur und Validierung	197
4.6.3	Aufrechterhaltung im laufenden Betrieb	197
4.7	Sicherheitsgrundfunktionen	198
4.8	Realisierung der Grundfunktionen	202
4.9	Security Development Lifecycle (SDL)	204
4.9.1	Die Entwicklungsphasen	205
4.9.2	Bedrohungs- und Risikoanalyse	206
5	Bewertungskriterien	211
5.1	TCSEC-Kriterien	211
5.1.1	Sicherheitsstufen	212
5.1.2	Kritik am Orange Book	213
5.2	IT-Kriterien	215
5.2.1	Mechanismen	215
5.2.2	Funktionsklassen	216
5.2.3	Qualität	216
5.3	ITSEC-Kriterien	217
5.3.1	Evaluationsstufen	218
5.3.2	Qualität und Bewertung	219
5.4	Common Criteria	220
5.4.1	Überblick über die CC	221
5.4.2	CC-Funktionsklassen	225
5.4.3	Schutzprofile	227
5.4.4	Vertrauenswürdigkeitsklassen	230
5.5	Zertifizierung	237
6	Sicherheitsmodelle	239
6.1	Modell-Klassifikation	239
6.1.1	Objekte und Subjekte	240
6.1.2	Zugriffsrechte	241
6.1.3	Zugriffsbeschränkungen	242
6.1.4	Sicherheitsstrategien	242
6.2	Zugriffskontrollmodelle	244
6.2.1	Zugriffsmatrix-Modell	244
6.2.2	Rollenbasierte Modelle	252
6.2.3	Chinese-Wall Modell	260
6.2.4	Bell-LaPadula Modell	265
6.3	Informationsflussmodelle	272
6.3.1	Verbands-Modell	272
6.4	Fazit und Ausblick	276
7	Kryptografische Verfahren	279
7.1	Einführung	279

7.2	Steganografie	281
7.2.1	Linguistische Steganografie	282
7.2.2	Technische Steganografie	283
7.3	Grundlagen kryptografischer Verfahren	285
7.3.1	Kryptografische Systeme	285
7.3.2	Anforderungen	290
7.4	Informationstheorie	292
7.4.1	Stochastische und kryptografische Kanäle	293
7.4.2	Entropie und Redundanz	295
7.4.3	Sicherheit kryptografischer Systeme	296
7.5	Symmetrische Verfahren	302
7.5.1	Permutation und Substitution	302
7.5.2	Block- und Stromchiffren	303
7.5.3	Betriebsmodi von Blockchiffren	308
7.5.4	Data Encryption Standard	314
7.5.5	AES	323
7.6	Asymmetrische Verfahren	327
7.6.1	Eigenschaften	327
7.6.2	Das RSA-Verfahren	331
7.7	Kryptoanalyse	343
7.7.1	Klassen kryptografischer Angriffe	343
7.7.2	Substitutionschiffren	345
7.7.3	Differentielle Kryptoanalyse	347
7.7.4	Lineare Kryptoanalyse	349
7.8	Kryptoregulierung	350
7.8.1	Hintergrund	350
7.8.2	Internationale Regelungen	351
7.8.3	Kryptopolitik in Deutschland	354
8	Hashfunktionen und elektronische Signaturen	355
8.1	Hashfunktionen	355
8.1.1	Grundlagen	356
8.1.2	Blockchiffren-basierte Hashfunktionen	361
8.1.3	Dedizierte Hashfunktionen	362
8.1.4	Message Authentication Code	367
8.2	Elektronische Signaturen	371
8.2.1	Anforderungen	372
8.2.2	Erstellung elektronischer Signaturen	373
8.2.3	Digitaler Signaturstandard (DSS)	377
8.2.4	Signaturgesetz	379
8.2.5	Fazit und Ausblick	386

9	Schlüsselmanagement	389
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	403
9.2.1	Schlüsselerzeugung	403
9.2.2	Schlüsselspeicherung und -vernichtung	406
9.3	Schlüsselaustausch	409
9.3.1	Schlüsselhierarchie	410
9.3.2	Naives Austauschprotokoll	412
9.3.3	Protokoll mit symmetrischen Verfahren	414
9.3.4	Protokoll mit asymmetrischen Verfahren	417
9.3.5	Leitlinien für die Protokollentwicklung	419
9.3.6	Diffie-Hellman Verfahren	422
9.4	Schlüsselerückgewinnung	428
9.4.1	Systemmodell	429
9.4.2	Grenzen und Risiken	434
10	Authentifikation	439
10.1	Einführung	439
10.2	Authentifikation durch Wissen	442
10.2.1	Passwortverfahren	442
10.2.2	Authentifikation in Unix	455
10.2.3	Challenge-Response-Verfahren	461
10.2.4	Zero-Knowledge-Verfahren	465
10.3	Biometrie	468
10.3.1	Einführung	468
10.3.2	Biometrische Techniken	471
10.3.3	Biometrische Authentifikation	474
10.3.4	Fallbeispiel: Fingerabdruckerkennung	476
10.3.5	Sicherheit biometrischer Techniken	480
10.4	Authentifikation in verteilten Systemen	484
10.4.1	RADIUS	484
10.4.2	Remote Procedure Call	489
10.4.3	Secure RPC	491
10.4.4	Kerberos-Authentifikationssystem	494
10.4.5	Microsoft Passport-Protokoll	504
10.4.6	Authentifikations-Logik	520
11	Digitale Identität	529
11.1	Smartcards	529

11.1.1	Smartcard-Architektur	530
11.1.2	Betriebssystem und Sicherheitsmechanismen	534
11.1.3	Fallbeispiele	537
11.1.4	Smartcard-Sicherheit	540
11.2	Elektronische Identifikationsausweise	544
11.2.1	Elektronischer Reisepass (ePass)	545
11.2.2	Elektronischer Personalausweis (ePA)	565
11.3	Trusted Computing	586
11.3.1	Trusted Computing Platform Alliance	587
11.3.2	TCG-Architektur	589
11.3.3	TPM	594
11.3.4	Sicheres Booten	608
12	Zugriffskontrolle	621
12.1	Einleitung	621
12.2	Speicherschutz	622
12.2.1	Betriebsmodi und Adressräume	623
12.2.2	Virtueller Speicher	624
12.3	Objektschutz	628
12.3.1	Zugriffskontrolllisten	629
12.3.2	Zugriffsausweise	633
12.4	Zugriffskontrolle in Unix	639
12.4.1	Identifikation	639
12.4.2	Rechtevergabe	640
12.4.3	Zugriffskontrolle	645
12.5	Zugriffskontrolle unter Windows 2000	649
12.5.1	Architektur-Überblick	649
12.5.2	Sicherheitssystem	651
12.5.3	Datenstrukturen zur Zugriffskontrolle	654
12.5.4	Zugriffskontrolle	659
12.6	Verschlüsselnde Dateisysteme	662
12.6.1	Klassifikation	664
12.6.2	Encrypting File System (EFS)	666
12.7	Systembestimmte Zugriffskontrolle	672
12.8	Sprachbasierter Schutz	675
12.8.1	Programmiersprache	675
12.8.2	Übersetzer und Binder	678
12.9	Java-Sicherheit	684
12.9.1	Die Programmiersprache	685
12.9.2	Sicherheitsarchitektur	686
12.9.3	Java-Sicherheitsmodelle	690

13	Sicherheit in Netzen	699
13.1	Firewall-Technologie	700
13.1.1	Einführung	700
13.1.2	Paketfilter	703
13.1.3	Proxy-Firewall	717
13.1.4	Applikationsfilter	721
13.1.5	Architekturen	725
13.1.6	Risiken und Grenzen	728
13.2	OSI-Sicherheitsarchitektur	734
13.2.1	Sicherheitsdienste	734
13.2.2	Sicherheitsmechanismen	737
13.3	Sichere Kommunikation	742
13.3.1	Verschlüsselungs-Layer	744
13.3.2	Virtual Private Network (VPN)	751
13.4	IPSec	756
13.4.1	Überblick	758
13.4.2	Security Association und Policy-Datenbank	760
13.4.3	AH-Protokoll	765
13.4.4	ESP-Protokoll	768
13.4.5	Schlüsselaustauschprotokoll IKE	772
13.4.6	Sicherheit von IPSec	777
13.5	Secure Socket Layer (SSL)	783
13.5.1	Überblick	783
13.5.2	Handshake-Protokoll	787
13.5.3	Record-Protokoll	790
13.5.4	Sicherheit von SSL	793
13.6	Sichere Anwendungsdienste	795
13.6.1	Elektronische Mail	796
13.6.2	Elektronischer Zahlungsverkehr	814
13.7	Service-orientierte Architektur	822
13.7.1	Konzepte und Sicherheitsanforderungen	822
13.7.2	Web-Services	825
13.7.3	Web-Service Sicherheitsstandards	830
13.7.4	Offene Fragen	836
14	Sichere mobile und drahtlose Kommunikation	839
14.1	Einleitung	839
14.1.1	Heterogenität der Netze	840
14.1.2	Entwicklungsphasen	841
14.2	GSM	844
14.2.1	Grundlagen	844
14.2.2	GSM-Grobarchitektur	845

14.2.3	Identifikation und Authentifikation	847
14.2.4	Gesprächsverschlüsselung	851
14.2.5	Sicherheitsprobleme	853
14.2.6	Weiterentwicklungen	857
14.2.7	GPRS	858
14.3	UMTS	861
14.3.1	UMTS-Sicherheitsarchitektur	861
14.3.2	Authentifikation und Schlüsselvereinbarung	863
14.3.3	Vertraulichkeit und Integrität	868
14.4	Funk-LAN (WLAN)	870
14.4.1	Grundlagen	870
14.4.2	WLAN-Sicherheitsprobleme	877
14.4.3	WEP	882
14.4.4	WPA und 802.11i	896
14.5	Bluetooth	911
14.5.1	Einordnung und Abgrenzung	912
14.5.2	Technische Grundlagen	915
14.5.3	Sicherheitsarchitektur	920
14.5.4	Schlüsselmanagement	925
14.5.5	Authentifikation	930
14.5.6	Bluetooth-Sicherheitsprobleme	933
14.5.7	Secure Simple Pairing	936
14.6	Ausblick	940
Literaturverzeichnis		945
Glossar		961
Index		971