

Inhaltsverzeichnis

1	Einführung	1
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	Sicherheitsstrategie	34
1.6	Sicherheitsinfrastruktur	38
2	Spezielle Bedrohungen	45
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	55
2.3.1	Eigenschaften	55
2.3.2	Viren-Typen	57
2.3.3	Gegenmaßnahmen	64
2.4	Würmer	67
2.5	Trojanisches Pferd	72
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	81
2.7.2	Sicherheitsbedrohungen	82
2.7.3	Gegenmaßnahmen	85
2.7.4	Mobile Apps	87
3	Internet-(Un)Sicherheit	93
3.1	Einführung	93
3.2	Internet-Protokollfamilie	95
3.2.1	ISO/OSI-Referenzmodell	95
3.2.2	Das TCP/IP-Referenzmodell	102
3.2.3	Das Internet-Protokoll IP	104
3.2.4	Das Transmission Control Protokoll TCP	109
3.2.5	Das User Datagram Protocol UDP	112
3.2.6	DHCP und NAT	114
3.3	Sicherheitsprobleme	117
3.3.1	Sicherheitsprobleme von IP	117
3.3.2	Sicherheitsprobleme von ICMP	123
3.3.3	Sicherheitsprobleme von ARP	125
3.3.4	Sicherheitsprobleme von UDP und TCP	129
3.4	Sicherheitsprobleme von Netzdiensten	133
3.4.1	Domain Name Service (DNS)	134
3.4.2	Network File System (NFS)	143
3.4.3	Network Information System (NIS)	148
3.4.4	Weitere Dienste	150
3.5	Web-Anwendungen	155
3.5.1	World Wide Web (WWW)	155
3.5.2	Sicherheitsprobleme	161
3.5.3	OWASP Top-Ten Sicherheitsprobleme	170
3.6	Analysetools und Systemhärtung	179
4	Security Engineering	187
4.1	Entwicklungsprozess	188
4.1.1	Allgemeine Konstruktionsprinzipien	188
4.1.2	Phasen	189
4.1.3	BSI-Sicherheitsprozess	190
4.2	Strukturanalyse	194
4.3	Schutzbedarfsermittlung	196
4.3.1	Schadensszenarien	196
4.3.2	Schutzbedarf	198

4.4	Bedrohungsanalyse	200
4.4.1	Bedrohungsmatrix	201
4.4.2	Bedrohungsbaum	202
4.5	Risikoanalyse	208
4.5.1	Attributierung	209
4.5.2	Penetrationstests	214
4.6	Sicherheitsarchitektur und Betrieb	216
4.6.1	Sicherheitsstrategie und Sicherheitsmodell	216
4.6.2	Systemarchitektur und Validierung	217
4.6.3	Aufrechterhaltung im laufenden Betrieb	218
4.7	Sicherheitsgrundfunktionen	218
4.8	Realisierung der Grundfunktionen	222
4.9	Security Development Lifecycle (SDL)	224
4.9.1	Die Entwicklungsphasen	225
4.9.2	Bedrohungs- und Risikoanalyse	226
5	Bewertungskriterien	231
5.1	TCSEC-Kriterien	231
5.1.1	Sicherheitsstufen	232
5.1.2	Kritik am Orange Book	233
5.2	IT-Kriterien	235
5.2.1	Mechanismen	235
5.2.2	Funktionsklassen	236
5.2.3	Qualität	236
5.3	ITSEC-Kriterien	237
5.3.1	Evaluationsstufen	238
5.3.2	Qualität und Bewertung	239
5.4	Common Criteria	240
5.4.1	Überblick über die CC	241
5.4.2	CC-Funktionsklassen	245
5.4.3	Schutzprofile	247
5.4.4	Vertrauenswürdigkeitsklassen	250
5.5	Zertifizierung	257
6	Sicherheitsmodelle	259
6.1	Modell-Klassifikation	259
6.1.1	Objekte und Subjekte	260
6.1.2	Zugriffsrechte	261
6.1.3	Zugriffsbeschränkungen	262
6.1.4	Sicherheitsstrategien	262

6.2	Zugriffskontrollmodelle	264
6.2.1	Zugriffsmatrix-Modell	264
6.2.2	Rollenbasierte Modelle	272
6.2.3	Chinese-Wall Modell	280
6.2.4	Bell-LaPadula Modell	285
6.3	Informationsflussmodelle	292
6.3.1	Verbands-Modell	292
6.4	Fazit und Ausblick	296
7	Kryptografische Verfahren	299
7.1	Einführung	299
7.2	Steganografie	301
7.2.1	Linguistische Steganografie	302
7.2.2	Technische Steganografie	303
7.3	Grundlagen kryptografischer Verfahren	305
7.3.1	Kryptografische Systeme	305
7.3.2	Anforderungen	310
7.4	Informationstheorie	312
7.4.1	Stochastische und kryptografische Kanäle	313
7.4.2	Entropie und Redundanz	315
7.4.3	Sicherheit kryptografischer Systeme	316
7.5	Symmetrische Verfahren	322
7.5.1	Permutation und Substitution	322
7.5.2	Block- und Stromchiffren	323
7.5.3	Betriebsmodi von Blockchiffren	328
7.5.4	Data Encryption Standard	334
7.5.5	AES	343
7.6	Asymmetrische Verfahren	347
7.6.1	Eigenschaften	348
7.6.2	Das RSA-Verfahren	351
7.7	Kryptoanalyse	363
7.7.1	Klassen kryptografischer Angriffe	363
7.7.2	Substitutionschiffren	365
7.7.3	Differentielle Kryptoanalyse	367
7.7.4	Lineare Kryptoanalyse	369
7.8	Kryptoregulierung	370
7.8.1	Hintergrund	370
7.8.2	Internationale Regelungen	371
7.8.3	Kryptopolitik in Deutschland	374

8	Hashfunktionen und elektronische Signaturen	375
8.1	Hashfunktionen	375
8.1.1	Grundlagen	376
8.1.2	Blockchiffren-basierte Hashfunktionen	381
8.1.3	Dedizierte Hashfunktionen	382
8.1.4	Message Authentication Code	387
8.2	Elektronische Signaturen	391
8.2.1	Anforderungen	392
8.2.2	Erstellung elektronischer Signaturen	393
8.2.3	Digitaler Signaturstandard (DSS)	397
8.2.4	Signaturgesetz	400
8.2.5	Fazit und Ausblick	406
9	Schlüsselmanagement	409
9.1	Zertifizierung	409
9.1.1	Zertifikate	410
9.1.2	Zertifizierungsstelle	411
9.1.3	Public-Key Infrastruktur	415
9.2	Schlüsselerzeugung und -aufbewahrung	423
9.2.1	Schlüsselerzeugung	423
9.2.2	Schlüsselspeicherung und -vernichtung	426
9.3	Schlüsselaustausch	429
9.3.1	Schlüsselhierarchie	429
9.3.2	Naives Austauschprotokoll	431
9.3.3	Protokoll mit symmetrischen Verfahren	433
9.3.4	Protokoll mit asymmetrischen Verfahren	437
9.3.5	Leitlinien für die Protokollentwicklung	439
9.3.6	Diffie-Hellman Verfahren	441
9.4	Schlüsselrückgewinnung	447
9.4.1	Systemmodell	448
9.4.2	Grenzen und Risiken	453
10	Authentifikation	459
10.1	Einführung	459
10.2	Authentifikation durch Wissen	462
10.2.1	Passwortverfahren	462
10.2.2	Authentifikation in Unix	475
10.2.3	Challenge-Response-Verfahren	481
10.2.4	Zero-Knowledge-Verfahren	485

10.3	Biometrie	488
10.3.1	Einführung	488
10.3.2	Biometrische Techniken	491
10.3.3	Biometrische Authentifikation	494
10.3.4	Fallbeispiel: Fingerabdruckerkennung	496
10.3.5	Sicherheit biometrischer Techniken	500
10.4	Authentifikation in verteilten Systemen	504
10.4.1	RADIUS	504
10.4.2	Remote Procedure Call	510
10.4.3	Secure RPC	511
10.4.4	Kerberos-Authentifikationssystem	514
10.4.5	Authentifikations-Logik	524
11	Digitale Identität	533
11.1	Smartcards	533
11.1.1	Smartcard-Architektur	534
11.1.2	Betriebssystem und Sicherheitsmechanismen	537
11.1.3	Fallbeispiele	541
11.1.4	Smartcard-Sicherheit	544
11.2	Elektronische Identifikationsausweise	548
11.2.1	Elektronischer Reisepass (ePass)	549
11.2.2	Elektronischer Personalausweis (nPA)	569
11.3	Trusted Computing	593
11.3.1	Trusted Computing Platform Alliance	594
11.3.2	TCG-Architektur	596
11.3.3	TPM	601
11.3.4	Sicheres Booten	615
12	Zugriffskontrolle	627
12.1	Einleitung	627
12.2	Speicherschutz	628
12.2.1	Betriebsmodi und Adressräume	629
12.2.2	Virtueller Speicher	630
12.3	Objektschutz	634
12.3.1	Zugriffskontrolllisten	635
12.3.2	Zugriffsausweise	639
12.4	Zugriffskontrolle in Unix	645
12.4.1	Identifikation	645
12.4.2	Rechtevergabe	646
12.4.3	Zugriffskontrolle	651

12.5	Zugriffskontrolle unter Windows 2000	655
12.5.1	Architektur-Überblick	655
12.5.2	Sicherheitssubsystem	657
12.5.3	Datenstrukturen zur Zugriffskontrolle	660
12.5.4	Zugriffskontrolle	665
12.6	Verschlüsselnde Dateisysteme	668
12.6.1	Klassifikation	670
12.6.2	Encrypting File System (EFS)	672
12.7	Systembestimmte Zugriffskontrolle	678
12.8	Sprachbasierter Schutz	681
12.8.1	Programmiersprache	681
12.8.2	Übersetzer und Binder	684
12.9	Java-Sicherheit	690
12.9.1	Die Programmiersprache	690
12.9.2	Sicherheitsarchitektur	691
12.9.3	Java-Sicherheitsmodelle	696
13	Sicherheit in Netzen	705
13.1	Firewall-Technologie	706
13.1.1	Einführung	706
13.1.2	Paketfilter	709
13.1.3	Proxy-Firewall	723
13.1.4	Applikationsfilter	727
13.1.5	Architekturen	731
13.1.6	Risiken und Grenzen	734
13.2	OSI-Sicherheitsarchitektur	740
13.2.1	Sicherheitsdienste	740
13.2.2	Sicherheitsmechanismen	743
13.3	Sichere Kommunikation	749
13.3.1	Verschlüsselungs-Layer	750
13.3.2	Virtual Private Network (VPN)	757
13.4	IPSec	762
13.4.1	Überblick	764
13.4.2	Security Association und Policy-Datenbank	766
13.4.3	AH-Protokoll	771
13.4.4	ESP-Protokoll	775
13.4.5	Schlüsselaustauschprotokoll IKE	778
13.4.6	Sicherheit von IPSec	783
13.5	Secure Socket Layer (SSL)	789
13.5.1	Überblick	789

13.5.2	Handshake-Protokoll	793
13.5.3	Record-Protokoll	796
13.5.4	Sicherheit von SSL	799
13.6	Sichere Anwendungsdienste	802
13.6.1	Elektronische Mail	802
13.6.2	Elektronischer Zahlungsverkehr	820
13.7	Service-orientierte Architektur	828
13.7.1	Konzepte und Sicherheitsanforderungen	829
13.7.2	Web-Services	832
13.7.3	Web-Service Sicherheitsstandards	837
13.7.4	SAML	843
13.7.5	Offene Fragen	848
14	Sichere mobile und drahtlose Kommunikation	851
14.1	Einleitung	851
14.1.1	Heterogenität der Netze	852
14.1.2	Entwicklungsphasen	853
14.2	GSM	856
14.2.1	Grundlagen	856
14.2.2	GSM-Grobarchitektur	857
14.2.3	Identifikation und Authentifikation	858
14.2.4	Gesprächsverschlüsselung	863
14.2.5	Sicherheitsprobleme	865
14.2.6	GPRS	869
14.3	UMTS	871
14.3.1	UMTS-Sicherheitsarchitektur	872
14.3.2	Authentifikation und Schlüsselvereinbarung	874
14.3.3	Vertraulichkeit und Integrität	878
14.4	Funk-LAN (WLAN)	880
14.4.1	Grundlagen	880
14.4.2	WLAN-Sicherheitsprobleme	887
14.4.3	WEP	893
14.4.4	WPA und 802.11i	907
14.5	Bluetooth	921
14.5.1	Einordnung und Abgrenzung	922
14.5.2	Technische Grundlagen	925
14.5.3	Sicherheitsarchitektur	930
14.5.4	Schlüsselmanagement	936
14.5.5	Authentifikation	941
14.5.6	Bluetooth-Sicherheitsprobleme	944
14.5.7	Secure Simple Pairing	946

14.6	Long Term Evolution (LTE) und SAE	951
14.6.1	EPC und LTE	952
14.6.2	Interworking	955
14.6.3	Sicherheitsarchitektur und Sicherheitsdienste	957
14.6.4	Sicheres Interworking	962
Literaturverzeichnis		967
Glossar		983
Index		993