

Inhaltsverzeichnis

1	Einführung	1
1.1	Grundlegende Begriffe	1
1.2	Schutzziele	6
1.3	Schwachstellen, Bedrohungen, Angriffe	13
1.3.1	Bedrohungen	15
1.3.2	Angriffs- und Angreifer-Typen	16
1.3.3	Rechtliche Rahmenbedingungen	25
1.4	Computer Forensik	28
1.5	Sicherheitsstrategie	30
1.6	Sicherheitsinfrastruktur	34
2	Spezielle Bedrohungen	41
2.1	Einführung	41
2.2	Buffer-Overflow	43
2.2.1	Einführung	43
2.2.2	Angriffe	46
2.2.3	Gegenmaßnahmen	49
2.3	Computerviren	51
2.3.1	Eigenschaften	51
2.3.2	Viren-Typen	53
2.3.3	Gegenmaßnahmen	60
2.4	Würmer	63
2.5	Trojanisches Pferd	68
2.5.1	Eigenschaften	68
2.5.2	Gegenmaßnahmen	70
2.6	Bot-Netze und Spam	72
2.6.1	Bot-Netze	72
2.6.2	Spam	74
2.7	Mobiler Code	76
2.7.1	Eigenschaften	77
2.7.2	Sicherheitsbedrohungen	77
2.7.3	Gegenmaßnahmen	80

3	Internet-(Un)Sicherheit	83
3.1	Einführung	83
3.2	Internet-Protokollfamilie	85
3.2.1	ISO/OSI-Referenzmodell	85
3.2.2	Das TCP/IP-Referenzmodell	91
3.2.3	Das Internet-Protokoll IP	93
3.2.4	Das Transmission Control Protokoll TCP	96
3.2.5	Das User Datagram Protocol UDP	98
3.2.6	DHCP und NAT	101
3.3	Sicherheitsprobleme	104
3.3.1	Sicherheitsprobleme von IP	104
3.3.2	Sicherheitsprobleme von ICMP	110
3.3.3	Sicherheitsprobleme von ARP	112
3.3.4	Sicherheitsprobleme von UDP und TCP	113
3.4	Sicherheitsprobleme von Netzdiensten	117
3.4.1	Domain Name Service (DNS)	117
3.4.2	Network File System (NFS)	123
3.4.3	Network Information System (NIS)	129
3.4.4	World Wide Web (WWW)	130
3.4.5	Weitere Dienste	145
3.5	Analysetools und Systemhärtung	149
4	Security Engineering	157
4.1	Entwicklungsprozess	158
4.1.1	Allgemeine Konstruktionsprinzipien	158
4.1.2	Phasen	159
4.1.3	BSI-Sicherheitsprozess	160
4.2	Strukturanalyse	164
4.3	Schutzbedarfsermittlung	166
4.3.1	Schadensszenarien	166
4.3.2	Schutzbedarf	168
4.4	Bedrohungsanalyse	170
4.4.1	Bedrohungsmatrix	171
4.4.2	Bedrohungsbaum	172
4.5	Risikoanalyse	178
4.5.1	Attributierung	180
4.5.2	Penetrationstests	184
4.6	Sicherheitsarchitektur und Betrieb	186
4.6.1	Sicherheitsstrategie und Sicherheitsmodell	186
4.6.2	Systemarchitektur und Validierung	187
4.6.3	Aufrechterhaltung im laufenden Betrieb	188
4.7	Sicherheitsgrundfunktionen	188

4.8	Realisierung der Grundfunktionen	192
4.9	Security Development Lifecycle (SDL)	194
4.9.1	Die Entwicklungsphasen	195
4.9.2	Bedrohungs- und Risikoanalyse	196
5	Bewertungskriterien	201
5.1	TCSEC-Kriterien	201
5.1.1	Sicherheitsstufen	202
5.1.2	Kritik am Orange Book	203
5.2	IT-Kriterien	205
5.2.1	Mechanismen	205
5.2.2	Funktionsklassen	206
5.2.3	Qualität	206
5.3	ITSEC-Kriterien	207
5.3.1	Evaluationsstufen	208
5.3.2	Qualität und Bewertung	209
5.4	Common Criteria	210
5.4.1	Überblick über die CC	211
5.4.2	CC-Funktionsklassen	215
5.4.3	Schutzprofile	217
5.4.4	Vertrauenswürdigkeitsklassen	220
5.5	Zertifizierung	227
6	Sicherheitsmodelle	229
6.1	Modell-Klassifikation	229
6.1.1	Objekte und Subjekte	230
6.1.2	Zugriffsrechte	231
6.1.3	Zugriffsbeschränkungen	232
6.1.4	Sicherheitsstrategien	232
6.2	Zugriffskontrollmodelle	234
6.2.1	Zugriffsmatrix-Modell	234
6.2.2	Rollenbasierte Modelle	243
6.2.3	Chinese-Wall Modell	250
6.2.4	Bell-LaPadula Modell	255
6.3	Informationsflussmodelle	262
6.3.1	Verbands-Modell	262
6.4	Fazit und Ausblick	266
7	Kryptografische Verfahren	269
7.1	Einführung	269
7.2	Steganografie	271
7.2.1	Linguistische Steganografie	272
7.2.2	Technische Steganografie	273

7.3	Grundlagen kryptografischer Verfahren	275
7.3.1	Kryptografische Systeme	275
7.3.2	Anforderungen	280
7.4	Informationstheorie	282
7.4.1	Stochastische und kryptografische Kanäle	283
7.4.2	Entropie und Redundanz	284
7.4.3	Sicherheit kryptografischer Systeme	286
7.5	Symmetrische Verfahren	291
7.5.1	Permutation und Substitution	292
7.5.2	Block- und Stromchiffren	293
7.5.3	Betriebsmodi von Blockchiffren	298
7.5.4	Data Encryption Standard	304
7.5.5	AES	313
7.6	Asymmetrische Verfahren	317
7.6.1	Eigenschaften	317
7.6.2	Das RSA-Verfahren	321
7.7	Kryptoanalyse	333
7.7.1	Klassen kryptografischer Angriffe	333
7.7.2	Substitutionschiffren	335
7.7.3	Differentielle Kryptoanalyse	337
7.7.4	Lineare Kryptoanalyse	339
7.8	Kryptoregulierung	340
7.8.1	Hintergrund	340
7.8.2	Internationale Regelungen	341
7.8.3	Kryptopolitik in Deutschland	344
8	Hashfunktionen und elektronische Signaturen	345
8.1	Hashfunktionen	345
8.1.1	Grundlagen	346
8.1.2	Blockchiffren-basierte Hashfunktionen	351
8.1.3	Dedizierte Hashfunktionen	352
8.1.4	Message Authentication Code	357
8.2	Elektronische Signaturen	361
8.2.1	Anforderungen	362
8.2.2	Erstellung elektronischer Signaturen	363
8.2.3	Digitaler Signaturstandard (DSS)	367
8.2.4	Signaturgesetz	370
8.2.5	Fazit und Ausblick	376
9	Schlüsselmanagement	379
9.1	Zertifizierung	379
9.1.1	Zertifikate	380

9.1.2	Zertifizierungsstelle	381
9.1.3	Public-Key Infrastruktur	385
9.2	Schlüsselerzeugung und -aufbewahrung	393
9.2.1	Schlüsselerzeugung	393
9.2.2	Schlüsselspeicherung und -vernichtung	395
9.3	Schlüsselaustausch	399
9.3.1	Schlüsselhierarchie	400
9.3.2	Naives Austauschprotokoll	402
9.3.3	Protokoll mit symmetrischen Verfahren	404
9.3.4	Protokoll mit asymmetrischen Verfahren	407
9.3.5	Leitlinien für die Protokollentwicklung	409
9.3.6	Diffie-Hellman Verfahren	412
9.4	Schlüsselrückgewinnung	418
9.4.1	Systemmodell	419
9.4.2	Grenzen und Risiken	424
10	Authentifikation	429
10.1	Einführung	429
10.2	Authentifikation durch Wissen	432
10.2.1	Passwortverfahren	432
10.2.2	Authentifikation in Unix	445
10.2.3	Challenge-Response-Verfahren	451
10.2.4	Zero-Knowledge-Verfahren	455
10.3	Smartcard	458
10.3.1	Architektur	459
10.3.2	Sicherheit	462
10.4	Biometrie	472
10.4.1	Einführung	473
10.4.2	Biometrische Techniken	475
10.4.3	Biometrische Authentifikation	478
10.4.4	Fallbeispiel: Fingerabdruckerkennung	481
10.4.5	Sicherheit biometrischer Techniken	484
10.5	Authentifikation in verteilten Systemen	488
10.5.1	RADIUS	488
10.5.2	Remote Procedure Call	494
10.5.3	Secure RPC	495
10.5.4	Kerberos-Authentifikationssystem	498
10.5.5	Microsoft Passport-Protokoll	508
10.5.6	Authentifikations-Logik	524
11	Zugriffskontrolle	535
11.1	Einleitung	535

11.2	Speicherschutz	536
11.2.1	Betriebsmodi und Adressräume	537
11.2.2	Virtueller Speicher	538
11.3	Objektschutz	542
11.3.1	Zugriffskontrolllisten	543
11.3.2	Zugriffsausweise	548
11.4	Zugriffskontrolle in Unix	553
11.4.1	Identifikation	553
11.4.2	Rechtevergabe	554
11.4.3	Zugriffskontrolle	559
11.5	Zugriffskontrolle unter Windows 2000	563
11.5.1	Architektur-Überblick	563
11.5.2	Sicherheitssystem	565
11.5.3	Datenstrukturen zur Zugriffskontrolle	568
11.5.4	Zugriffskontrolle	573
11.6	Verschlüsselnde Dateisysteme	576
11.6.1	Klassifikation	578
11.6.2	Encrypting File System (EFS)	580
11.7	Systembestimmte Zugriffskontrolle	586
11.8	Sprachbasierter Schutz	589
11.8.1	Programmiersprache	589
11.8.2	Übersetzer und Binder	592
11.9	Java-Sicherheit	598
11.9.1	Die Programmiersprache	599
11.9.2	Sicherheitsarchitektur	600
11.9.3	Java-Sicherheitsmodelle	604
11.10	Trusted Computing	611
11.10.1	Trusted Computing Platform Alliance	612
11.10.2	TCG-Architektur	614
11.10.3	TPM	620
11.10.4	TPM-Schlüssel	625
11.10.5	Sicheres Booten	634
11.10.6	Einsatzmöglichkeiten für TCG-Plattformen	639
11.10.7	Fazit und offene Probleme	640
12	Sicherheit in Netzen	645
12.1	Firewall-Technologie	646
12.1.1	Einführung	646
12.1.2	Paketfilter	649
12.1.3	Proxy-Firewall	663
12.1.4	Applikationsfilter	667
12.1.5	Architekturen	671

12.1.6	Risiken und Grenzen	674
12.2	OSI-Sicherheitsarchitektur	680
12.2.1	Sicherheitsdienste	680
12.2.2	Sicherheitsmechanismen	683
12.3	Sichere Kommunikation	688
12.3.1	Verschlüsselungs-Layer	690
12.3.2	Virtual Private Network (VPN)	697
12.4	IPSec	702
12.4.1	Überblick	704
12.4.2	Security Association und Policy-Datenbank	706
12.4.3	AH-Protokoll	711
12.4.4	ESP-Protokoll	715
12.4.5	Schlüsselaustauschprotokoll IKE	718
12.4.6	Sicherheit von IPSec	723
12.5	Secure Socket Layer (SSL)	729
12.5.1	Überblick	730
12.5.2	Handshake-Protokoll	733
12.5.3	Record-Protokoll	736
12.5.4	Sicherheit von SSL	739
12.6	Sichere Anwendungsdienste	742
12.6.1	Elektronische Mail	742
12.6.2	Elektronischer Zahlungsverkehr	760
12.7	Service-orientierte Architektur	768
12.7.1	Konzepte und Sicherheitsanforderungen	769
12.7.2	Web-Services	771
12.7.3	Web-Service Sicherheitsstandards	777
12.7.4	Offene Fragen	783
13	Sichere mobile und drahtlose Kommunikation	785
13.1	Einleitung	785
13.1.1	Heterogenität der Netze	786
13.1.2	Entwicklungsphasen	787
13.2	GSM	790
13.2.1	Grundlagen	790
13.2.2	GSM-Grobarchitektur	791
13.2.3	Identifikation und Authentifikation	793
13.2.4	Gesprächsverschlüsselung	797
13.2.5	Sicherheitsprobleme	799
13.2.6	Weiterentwicklungen	803
13.2.7	GPRS	804
13.3	UMTS	807
13.3.1	UMTS-Sicherheitsarchitektur	807

13.3.2	Authentifikation und Schlüsselvereinbarung	809
13.3.3	Vertraulichkeit und Integrität	814
13.3.4	Fazit	814
13.4	Funk-LAN (WLAN)	816
13.4.1	Einführung	816
13.4.2	Technische Grundlagen	818
13.4.3	WLAN-Sicherheitsprobleme	823
13.4.4	Einbindung eines WLAN in die Netztopologie	827
13.4.5	WEP im Überblick	828
13.4.6	WEP-Authentifikation	830
13.4.7	WEP-Integrität	832
13.4.8	WEP-Vertraulichkeit	836
13.4.9	Zusätzliche Sicherheitsmaßnahmen	840
13.4.10	WPA und 802.11i	842
13.4.11	Schlüsselmanagement in WPA und 802.11i	845
13.4.12	802.1X-Framework und EAP	847
13.4.13	TKIP	852
13.4.14	AES-CCMP	855
13.5	Bluetooth	857
13.5.1	Einordnung und Abgrenzung	858
13.5.2	Technische Grundlagen	861
13.5.3	Sicherheitsarchitektur	866
13.5.4	Schlüsselmanagement	871
13.5.5	Authentifikation	876
13.5.6	Bluetooth-Sicherheitsprobleme	879
13.5.7	Secure Simple Pairing	881
13.6	Ausblick	886
Literaturverzeichnis		889
Glossar		905
Index		915