

Inhaltsverzeichnis

1	Einführung	1
1.1	Grundlegende Begriffe	3
1.2	Schutzziele	7
1.3	Schwachstellen, Bedrohungen, Angriffe	17
1.3.1	Bedrohungen	18
1.3.2	Angriffs- und Angreifer-Typen	20
1.3.3	Rechtliche Rahmenbedingungen	28
1.4	Computer Forensik	32
1.5	Sicherheitsrichtlinie	34
1.6	Sicherheitsinfrastruktur	36
2	Spezielle Bedrohungen	47
2.1	Einführung	47
2.2	Buffer-Overflow	49
2.2.1	Einführung	50
2.2.2	Angriffe	53
2.2.3	Gegenmaßnahmen	55
2.3	Computerviren	58
2.3.1	Eigenschaften	58
2.3.2	Viren-Typen	60
2.3.3	Gegenmaßnahmen	66
2.4	Würmer	69
2.5	Trojanisches Pferd	74
2.5.1	Eigenschaften	75
2.5.2	Gegenmaßnahmen	76
2.6	Bot-Netze und Spam	78
2.6.1	Bot-Netze	78
2.6.2	Spam	80
2.7	Apps	82
2.7.1	Sicherheitsbedrohungen	83
2.7.2	Gegenmaßnahmen	84
2.8	Meltdown- und Spectre-Angriffsklassen	86
2.8.1	Einführung	86

2.8.2	Background	88
2.8.3	Angriffsklassen	91
3	Internet-(Un)Sicherheit	99
3.1	Einführung	99
3.2	Internet-Protokollfamilie	101
3.2.1	ISO/OSI-Referenzmodell	102
3.2.2	Das TCP/IP-Referenzmodell	107
3.2.3	Das Internet-Protokoll IP	109
3.2.4	Das Transmission Control Protokoll TCP	115
3.2.5	Das User Datagram Protocol UDP	117
3.2.6	DHCP und NAT	118
3.3	Sicherheitsprobleme	120
3.3.1	Sicherheitsprobleme von IP	120
3.3.2	Sicherheitsprobleme von ICMP	124
3.3.3	Sicherheitsprobleme von ARP	127
3.3.4	Sicherheitsprobleme mit IPv6	128
3.3.5	Sicherheitsprobleme von UDP und TCP	130
3.4	Sicherheitsprobleme von Netzdiensten	134
3.4.1	Domain Name Service (DNS)	135
3.4.2	SMTP, FTP, Telnet	140
3.5	Web-Anwendungen	144
3.5.1	World Wide Web (WWW)	144
3.5.2	Sicherheitsprobleme	151
3.5.3	OWASP Top-Ten Sicherheitsprobleme	155
3.5.4	Ausgewählte Beispiele aus der Top-Ten Liste	159
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	173
4.3	Schutzbedarfsermittlung	175
4.3.1	Schadensszenarien	175
4.3.2	Schutzbedarf	177
4.4	Bedrohungsanalyse	179
4.4.1	Bedrohungsmatrix	179
4.4.2	Bedrohungsbaum	181
4.5	Risikoanalyse	187
4.5.1	Attributierung	188
4.5.2	Penetrationstests	192

4.6	Sicherheitsarchitektur und Betrieb	194
4.6.1	Sicherheitsstrategie und Sicherheitsmodell	194
4.6.2	Systemarchitektur und Validierung	195
4.6.3	Aufrechterhaltung im laufenden Betrieb	196
4.7	Sicherheitsgrundfunktionen	196
4.8	Realisierung der Grundfunktionen	200
4.9	Security Development Lifecycle (SDL)	202
4.9.1	Die Entwicklungsphasen	203
4.9.2	Bedrohungs- und Risikoanalyse	204
5	Bewertungskriterien	209
5.1	TCSEC-Kriterien	209
5.1.1	Sicherheitsstufen	210
5.1.2	Kritik am Orange Book	211
5.2	IT-Kriterien	213
5.2.1	Mechanismen	213
5.2.2	Funktionsklassen	214
5.2.3	Qualität	214
5.3	ITSEC-Kriterien	215
5.3.1	Evaluationsstufen	216
5.3.2	Qualität und Bewertung	217
5.4	Common Criteria	218
5.4.1	Überblick über die CC	219
5.4.2	CC-Funktionsklassen	222
5.4.3	Schutzprofile	225
5.4.4	Vertrauenswürdigkeitsklassen	227
5.5	Zertifizierung	232
6	Sicherheitsmodelle	235
6.1	Modell-Klassifikation	235
6.1.1	Objekte und Subjekte	236
6.1.2	Zugriffsrechte	237
6.1.3	Zugriffsbeschränkungen	238
6.1.4	Sicherheitsstrategien	238
6.2	Zugriffskontrollmodelle	239
6.2.1	Zugriffsmatrix-Modell	240
6.2.2	Rollenbasierte Modelle	248
6.2.3	Chinese-Wall Modell	256
6.2.4	Bell-LaPadula Modell	261
6.3	Informationsflussmodelle	266
6.3.1	Verbands-Modell	266
6.4	Fazit	270

7	Kryptografische Verfahren	273
7.1	Einführung	273
7.2	Steganografie	275
7.2.1	Linguistische Steganografie	276
7.2.2	Technische Steganografie	277
7.3	Grundlagen kryptografischer Verfahren	279
7.3.1	Kryptografisches System	279
7.3.2	Anforderungen	284
7.4	Informationstheorie	287
7.4.1	Stochastische und kryptografische Kanäle	287
7.4.2	Entropie und Redundanz	289
7.4.3	Sicherheit kryptografischer Systeme	290
7.5	Symmetrische Verfahren	296
7.5.1	Permutation und Substitution	296
7.5.2	Block- und Stromchiffren	297
7.5.3	Betriebsmodi von Blockchiffren	304
7.5.4	Data Encryption Standard	313
7.5.5	AES	320
7.6	Asymmetrische Verfahren	325
7.6.1	Eigenschaften	325
7.6.2	Das RSA-Verfahren	329
7.7	Elliptische Kurven Kryptografie (ECC)	341
7.7.1	Grundlagen	342
7.7.2	Einsatz elliptischer Kurven	347
7.8	Kryptoanalyse	352
7.8.1	Klassen kryptografischer Angriffe	352
7.8.2	Substitutionschiffren	354
7.8.3	Differentielle Kryptoanalyse	356
7.8.4	Lineare Kryptoanalyse	357
7.8.5	Quanten-Computer basierte Krypto-Analyse	359
7.9	Empfohlene Sicherheitsniveaus	361
8	Hashfunktionen und elektronische Signaturen	363
8.1	Hashfunktionen	363
8.1.1	Grundlagen	364
8.1.2	Blockchiffren-basierte Hashfunktionen	370
8.1.3	Dedizierte Hashfunktionen	371
8.1.4	Message Authentication Code	375
8.2	Elektronische Signaturen	380
8.2.1	Anforderungen	380
8.2.2	Erstellung elektronischer Signaturen	381
8.2.3	Digitaler Signaturstandard (DSS)	386

8.2.4	Rechtliche Rahmen	389
9	Schlüsselmanagement	397
9.1	Zertifizierung	397
9.1.1	Zertifikate	398
9.1.2	Zertifizierungsstelle	399
9.1.3	Public-Key Infrastruktur	402
9.1.4	Zertifikatsmanagement	407
9.2	Schlüsselerzeugung und -aufbewahrung	414
9.2.1	Schlüsselerzeugung	414
9.2.2	Schlüsselspeicherung und -vernichtung	416
9.3	Schlüsselaustausch	420
9.3.1	Schlüsselhierarchie	421
9.3.2	Naives Austauschprotokoll	423
9.3.3	Protokoll mit symmetrischen Verfahren	425
9.3.4	Protokoll mit asymmetrischen Verfahren	429
9.3.5	Leitlinien für die Protokollentwicklung	431
9.3.6	Diffie-Hellman Verfahren	433
9.4	Schlüsselrückgewinnung	441
9.4.1	Systemmodell	442
9.4.2	Grenzen und Risiken	445
10	Authentifikation	449
10.1	Einführung	449
10.2	Authentifikation durch Wissen	451
10.2.1	Passwortverfahren	452
10.2.2	Authentifikation in Unix	465
10.2.3	Challenge-Response-Verfahren	471
10.2.4	Zero-Knowledge-Verfahren	475
10.3	Biometrie	479
10.3.1	Einführung	479
10.3.2	Biometrische Techniken	481
10.3.3	Biometrische Authentifikation	483
10.3.4	Fallbeispiel: Fingerabdruckerkennung	486
10.3.5	Sicherheit biometrischer Techniken	489
10.4	Authentifikation in verteilten Systemen	493
10.4.1	RADIUS	494
10.4.2	Kerberos-Authentifikationssystem	499
10.4.3	Shibboleth	508
10.4.4	OAuth und OpenID Connect	510
11	Digitale Identität	523
11.1	Smartcards	523

11.1.1	Smartcard-Architektur	524
11.1.2	Betriebssystem und Sicherheitsmechanismen	527
11.1.3	Smartcard-Sicherheit	530
11.2	Elektronische Identifikationsausweise	534
11.2.1	Elektronischer Reisepass (ePass)	535
11.2.2	Personalausweis	553
11.3	Universal Second Factor Authentication	572
11.3.1	Registrierung eines U2F-Devices	573
11.3.2	Login beim Web-Dienst	577
11.3.3	Sicherheitsbetrachtungen	581
11.3.4	U2F-Protokoll versus eID-Funktion	588
11.4	Trusted Computing	591
11.4.1	Trusted Computing Platform Alliance	592
11.4.2	TCG-Architektur	593
11.4.3	TPM 1.2	598
11.4.4	Sicheres Booten	612
11.5	Physical Unclonable Functions (PUF)	621
11.5.1	Einführung	622
11.5.2	Einsatz von PUFs in Sicherheitsprotokollen	628
11.5.3	Sicherheitsuntersuchungen von PUFs	631
12	Zugriffskontrolle	633
12.1	Einleitung	633
12.2	Speicherschutz	634
12.2.1	Betriebsmodi und Adressräume	634
12.2.2	Virtueller Speicher	636
12.3	Objektschutz	640
12.3.1	Zugriffskontrolllisten	640
12.3.2	Zugriffsausweise	645
12.4	Zugriffskontrolle in Unix	650
12.4.1	Identifikation	650
12.4.2	Rechtevergabe	651
12.4.3	Zugriffskontrolle	656
12.5	Systembestimmte Zugriffskontrolle	659
12.6	Service-orientierte Architektur	661
12.6.1	Konzepte und Sicherheitsanforderungen	661
12.6.2	Web-Services	664
12.6.3	Web-Service Sicherheitsstandards	667
12.6.4	SAML2.0	673
13	Fallstudien: iOS-Ecosystem und Windows 10	681
13.1	iOS-Ecosystem	681

13.1.1	iOS-Sicherheitsarchitektur im Überblick	682
13.1.2	Sichere Enklave	683
13.1.3	Touch ID	685
13.1.4	Systemsicherheit	687
13.1.5	Passcode	689
13.1.6	Dateischutz	689
13.1.7	Keybags	698
13.1.8	Keychain	699
13.1.9	App-Sicherheit	700
13.1.10	Apple Pay	704
13.1.11	HomeKit-Framework	709
13.2	Windows 10	713
13.2.1	Architektur-Überblick	713
13.2.2	Sicherheits-Subsystem	717
13.2.3	Datenstrukturen zur Zugriffskontrolle	720
13.2.4	Zugriffskontrolle	725
13.2.5	Encrypting File System (EFS)	727
14	Sicherheit in Netzen	733
14.1	Firewall-Technologie	734
14.1.1	Einführung	734
14.1.2	Paketfilter	737
14.1.3	Proxy-Firewall	745
14.1.4	Applikationsfilter	748
14.1.5	Architekturen	752
14.2	Sichere Kommunikation	757
14.2.1	Verschlüsselungs-Layer	759
14.2.2	Virtual Private Network (VPN)	764
14.3	IPSec	768
14.3.1	Überblick	770
14.3.2	Security Association und Policy-Datenbank	772
14.3.3	AH-Protokoll	777
14.3.4	ESP-Protokoll	781
14.3.5	Schlüsselaustauschprotokoll IKE	784
14.3.6	Sicherheit von IPSec	790
14.4	TLS/SSL	792
14.4.1	Überblick	793
14.4.2	Handshake-Protokoll	796
14.4.3	Record-Protokoll	799
14.4.4	Sicherheit von TLS1.2	801
14.4.5	TLS 1.3	809
14.5	DNSSEC	812

14.5.1	DNS-Schlüssel und -Schlüsselmanagement	812
14.5.2	DNS-Anfrage unter DNSSEC	815
14.6	Elektronische Mail	818
14.6.1	S/MIME	818
14.6.2	Pretty Good Privacy (PGP)	823
14.7	Instant Messaging Dienste	831
14.7.1	Signal-Protokoll	833
14.7.2	Extended Triple Diffie-Hellman (X3DH)	833
14.7.3	Double Ratchet-Protokoll	837
14.7.4	Telegram Messenger	844
14.8	Blockchain	848
14.8.1	Technische Grundlagen	850
14.8.2	Smart Contracts	858
14.8.3	Sicherheit von Blockchains	860
14.8.4	Fallbeispiel: Bitcoin	863
14.8.5	Fazit und kritische Einordnung	868
15	Sichere mobile und drahtlose Kommunikation	871
15.1	GSM	872
15.1.1	Grundlagen	872
15.1.2	GSM-Grobarchitektur	873
15.1.3	Identifikation und Authentifikation	874
15.1.4	Gesprächsverschlüsselung	879
15.1.5	Sicherheitsprobleme	880
15.2	UMTS	885
15.2.1	Erweiterte Sicherheitsarchitektur	885
15.3	Long Term Evolution (LTE) und SAE	891
15.3.1	EPC und LTE	892
15.3.2	Interworking	895
15.3.3	Sicherheitsarchitektur und Sicherheitsdienste	896
15.3.4	Sicheres Interworking	902
15.4	Funk-LAN (WLAN)	907
15.4.1	Einführung	907
15.4.2	Technische Grundlagen	909
15.4.3	WLAN-Sicherheitsprobleme	913
15.4.4	WEP und WPA	915
15.4.5	802.11i Sicherheitsdienste (WPA2)	918
15.4.6	WPA3	930
15.4.7	802.1X-Framework und EAP	934
15.5	Bluetooth	940
15.5.1	Einordnung und Abgrenzung	941
15.5.2	Technische Grundlagen	942

15.5.3	Sicherheitsarchitektur	947
15.5.4	Schlüsselmanagement	952
15.5.5	Authentifikation	957
15.5.6	Bluetooth-Sicherheitsprobleme	960
15.5.7	Secure Simple Pairing	962
15.6	ZigBee	969
15.6.1	Überblick	969
15.6.2	Sicherheitsarchitektur	972
15.6.3	Schlüsseltypen	973
15.6.4	Netzzutritt und Schlüsselmanagement	976
15.6.5	ZigBee 3.0	978
15.6.6	Sicherheitsbetrachtungen	983
Literaturverzeichnis		989
Abkürzungsverzeichnis		1001
Index		1011