

Inhaltsverzeichnis

1	Einführung	1
1.1	Grundlegende Begriffe	3
1.2	Schutzziele	7
1.3	Schwachstellen, Bedrohungen, Angriffe	15
1.3.1	Bedrohungen	17
1.3.2	Angriffs- und Angreifer-Typen	18
1.3.3	Rechtliche Rahmenbedingungen	25
1.4	Computer Forensik	30
1.5	Sicherheitsrichtlinie	31
1.6	Sicherheitsinfrastruktur	34
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	54
2.3.1	Eigenschaften	54
2.3.2	Viren-Typen	56
2.3.3	Gegenmaßnahmen	63
2.4	Würmer	65
2.5	Trojanisches Pferd	71
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	Mobile Apps	79
2.7.1	Sicherheitsbedrohungen	80
2.7.2	Gegenmaßnahmen	82
2.8	Meltdown- und Spectre-Angriffsklassen	83
2.8.1	Einführung	83

2.8.2	Background	85
2.8.3	Angriffsklassen	88
3	Internet-(Un)Sicherheit	97
3.1	Einführung	97
3.2	Internet-Protokollfamilie	99
3.2.1	ISO/OSI-Referenzmodell	99
3.2.2	Das TCP/IP-Referenzmodell	105
3.2.3	Das Internet-Protokoll IP	107
3.2.4	Das Transmission Control Protokoll TCP	113
3.2.5	Das User Datagram Protocol UDP	115
3.2.6	DHCP und NAT	116
3.3	Sicherheitsprobleme	119
3.3.1	Sicherheitsprobleme von IP	119
3.3.2	Sicherheitsprobleme von ICMP	125
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	Network File System (NFS)	140
3.4.3	Weitere Dienste	146
3.5	Web-Anwendungen	150
3.5.1	World Wide Web (WWW)	151
3.5.2	Sicherheitsprobleme	157
3.5.3	OWASP Top-Ten Sicherheitsprobleme	163
4	Security Engineering	171
4.1	Entwicklungsprozess	172
4.1.1	Allgemeine Konstruktionsprinzipien	172
4.1.2	Phasen	173
4.1.3	BSI-Sicherheitsprozess	174
4.2	Strukturanalyse	177
4.3	Schutzbedarfsermittlung	179
4.3.1	Schadensszenarien	179
4.3.2	Schutzbedarf	182
4.4	Bedrohungsanalyse	184
4.4.1	Bedrohungsmatrix	184
4.4.2	Bedrohungsbaum	186
4.5	Risikoanalyse	191
4.5.1	Attributierung	192
4.5.2	Penetrationstests	197

4.6	Sicherheitsarchitektur und Betrieb	199
4.6.1	Sicherheitsstrategie und Sicherheitsmodell	199
4.6.2	Systemarchitektur und Validierung	200
4.6.3	Aufrechterhaltung im laufenden Betrieb	200
4.7	Sicherheitsgrundfunktionen	201
4.8	Realisierung der Grundfunktionen	205
4.9	Security Development Lifecycle (SDL)	207
4.9.1	Die Entwicklungsphasen	208
4.9.2	Bedrohungs- und Risikoanalyse	209
5	Bewertungskriterien	213
5.1	TCSEC-Kriterien	213
5.1.1	Sicherheitsstufen	214
5.1.2	Kritik am Orange Book	215
5.2	IT-Kriterien	216
5.2.1	Mechanismen	217
5.2.2	Funktionsklassen	218
5.2.3	Qualität	218
5.3	ITSEC-Kriterien	219
5.3.1	Evaluationsstufen	220
5.3.2	Qualität und Bewertung	221
5.4	Common Criteria	222
5.4.1	Überblick über die CC	223
5.4.2	CC-Funktionsklassen	227
5.4.3	Schutzprofile	229
5.4.4	Vertrauenswürdigkeitsklassen	232
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	275

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	291
7.4.1	Stochastische und kryptografische Kanäle	291
7.4.2	Entropie und Redundanz	293
7.4.3	Sicherheit kryptografischer Systeme	295
7.5	Symmetrische Verfahren	300
7.5.1	Permutation und Substitution	300
7.5.2	Block- und Stromchiffren	302
7.5.3	Betriebsmodi von Blockchiffren	308
7.5.4	Data Encryption Standard	317
7.5.5	AES	326
7.6	Asymmetrische Verfahren	331
7.6.1	Eigenschaften	331
7.6.2	Das RSA-Verfahren	335
7.7	Elliptische Kurven Kryptografie (ECC)	347
7.7.1	Grundlagen	348
7.7.2	Einsatz elliptischer Kurven	353
7.8	Kryptoanalyse	358
7.8.1	Klassen kryptografischer Angriffe	358
7.8.2	Substitutionschiffren	360
7.8.3	Differentielle Kryptoanalyse	362
7.8.4	Lineare Kryptoanalyse	363
8	Hashfunktionen und elektronische Signaturen	365
8.1	Hashfunktionen	365
8.1.1	Grundlagen	366
8.1.2	Blockchiffren-basierte Hashfunktionen	372
8.1.3	Dedizierte Hashfunktionen	373
8.1.4	Message Authentication Code	376
8.2	Elektronische Signaturen	380
8.2.1	Anforderungen	381
8.2.2	Erstellung elektronischer Signaturen	382
8.2.3	Digitaler Signaturstandard (DSS)	386
8.2.4	Rechtliche Rahmen	390

9	Schlüsselmanagement	397
9.1	Zertifizierung	397
9.1.1	Zertifikate	398
9.1.2	Zertifizierungsstelle	399
9.1.3	Public-Key Infrastruktur	403
9.2	Schlüsselerzeugung und -aufbewahrung	410
9.2.1	Schlüsselerzeugung	410
9.2.2	Schlüsselspeicherung und -vernichtung	412
9.3	Schlüsselaustausch	415
9.3.1	Schlüsselhierarchie	416
9.3.2	Naives Austauschprotokoll	418
9.3.3	Protokoll mit symmetrischen Verfahren	420
9.3.4	Protokoll mit asymmetrischen Verfahren	423
9.3.5	Leitlinien für die Protokollentwicklung	425
9.3.6	Diffie-Hellman Verfahren	428
9.4	Schlüsselerückgewinnung	435
9.4.1	Systemmodell	436
9.4.2	Grenzen und Risiken	439
10	Authentifikation	443
10.1	Einführung	443
10.2	Authentifikation durch Wissen	445
10.2.1	Passwortverfahren	446
10.2.2	Authentifikation in Unix	459
10.2.3	Challenge-Response-Verfahren	465
10.2.4	Zero-Knowledge-Verfahren	469
10.3	Biometrie	472
10.3.1	Einführung	472
10.3.2	Biometrische Techniken	474
10.3.3	Biometrische Authentifikation	477
10.3.4	Fallbeispiel: Fingerabdruckerkennung	480
10.3.5	Sicherheit biometrischer Techniken	482
10.4	Authentifikation in verteilten Systemen	486
10.4.1	RADIUS	486
10.4.2	Kerberos-Authentifikationssystem	491
11	Digitale Identität	503
11.1	Smartcards	503
11.1.1	Smartcard-Architektur	504
11.1.2	Betriebssystem und Sicherheitsmechanismen	507
11.1.3	Smartcard-Sicherheit	510

11.2	Elektronische Identifikationsausweise	515
11.2.1	Elektronischer Reisepass (ePass)	515
11.2.2	Personalausweis	535
11.3	Universal Second Factor Authentication	554
11.3.1	Registrierung eines U2F-Devices	556
11.3.2	Login beim Web-Dienst	559
11.3.3	Sicherheitsbetrachtungen	563
11.3.4	U2F-Protokoll versus eID-Funktion	570
11.4	Trusted Computing	573
11.4.1	Trusted Computing Platform Alliance	574
11.4.2	TCG-Architektur	575
11.4.3	TPM 1.2	580
11.4.4	Sicheres Booten	594
11.5	Physically Unclonable Functions (PUF)	604
11.5.1	Einführung	605
11.5.2	Einsatz von PUFs in Sicherheitsprotokollen	610
11.5.3	Sicherheitsuntersuchungen von PUFs	613
12	Zugriffskontrolle	615
12.1	Einleitung	615
12.2	Speicherschutz	616
12.2.1	Betriebsmodi und Adressräume	616
12.2.2	Virtueller Speicher	618
12.3	Objektschutz	622
12.3.1	Zugriffskontrolllisten	623
12.3.2	Zugriffsausweise	627
12.4	Zugriffskontrolle in Unix	632
12.4.1	Identifikation	632
12.4.2	Rechtevergabe	633
12.4.3	Zugriffskontrolle	638
12.5	Systembestimmte Zugriffskontrolle	642
12.6	Service-orientierte Architektur	644
12.6.1	Konzepte und Sicherheitsanforderungen	644
12.6.2	Web-Services	647
12.6.3	Web-Service Sicherheitsstandards	649
12.6.4	SAML	656
13	Fallstudien: iOS-Ecosystem und Windows10	663
13.1	iOS-Ecosystem	663
13.1.1	iOS-Sicherheitsarchitektur im Überblick	664
13.1.2	Sichere Enklave	666
13.1.3	Touch ID	667

13.1.4	Systemsicherheit	669
13.1.5	Passcode	671
13.1.6	Dateischutz	671
13.1.7	Keybags	680
13.1.8	Keychain	682
13.1.9	App-Sicherheit	683
13.1.10	Apple Pay	686
13.1.11	HomeKit-Framework	691
13.2	Windows 10	695
13.2.1	Architektur-Überblick	695
13.2.2	Sicherheits-Subsystem	699
13.2.3	Datenstrukturen zur Zugriffskontrolle	702
13.2.4	Zugriffskontrolle	707
13.2.5	Encrypting File System (EFS)	709
14	Sicherheit in Netzen	715
14.1	Firewall-Technologie	716
14.1.1	Einführung	716
14.1.2	Paketfilter	719
14.1.3	Proxy-Firewall	728
14.1.4	Applikationsfilter	731
14.1.5	Architekturen	734
14.2	Sichere Kommunikation	740
14.2.1	Verschlüsselungs-Layer	741
14.2.2	Virtual Private Network (VPN)	747
14.3	IPSec	751
14.3.1	Überblick	753
14.3.2	Security Association und Policy-Datenbank	755
14.3.3	AH-Protokoll	760
14.3.4	ESP-Protokoll	763
14.3.5	Schlüsselaustauschprotokoll IKE	767
14.3.6	Sicherheit von IPSec	772
14.4	TLS/SSL	778
14.4.1	Überblick	779
14.4.2	Handshake-Protokoll	781
14.4.3	Record-Protokoll	784
14.4.4	Sicherheit von TLS	787
14.5	DNSSEC	796
14.5.1	DNS-Schlüssel und -Schlüsselmanagement	796
14.5.2	DNS-Anfrage unter DNSSEC	799
14.6	Elektronische Mail	801
14.6.1	S/MIME	801

14.6.2	Pretty Good Privacy (PGP)	806
14.7	Signal-Protokoll für Messaging-Dienste	814
14.7.1	Extended Triple Diffie-Hellman (X3DH)	815
14.7.2	Double Ratchet-Protokoll	819
14.8	Blockchain	826
14.8.1	Technische Grundlagen	828
14.8.2	Smart Contracts	836
14.8.3	Sicherheit von Blockchains	838
14.8.4	Fallbeispiel: Bitcoin	841
14.8.5	Fazit und kritische Einordnung	846
15	Sichere mobile und drahtlose Kommunikation	851
15.1	GSM	852
15.1.1	Grundlagen	852
15.1.2	GSM-Grobarchitektur	853
15.1.3	Identifikation und Authentifikation	854
15.1.4	Gesprächsverschlüsselung	858
15.1.5	Sicherheitsprobleme	861
15.1.6	GPRS	865
15.2	UMTS	867
15.2.1	UMTS-Sicherheitsarchitektur	868
15.2.2	Authentifikation und Schlüsselvereinbarung	870
15.2.3	Vertraulichkeit und Integrität	874
15.3	Long Term Evolution (LTE) und SAE	876
15.3.1	EPC und LTE	878
15.3.2	Interworking	881
15.3.3	Sicherheitsarchitektur und Sicherheitsdienste	882
15.3.4	Sicheres Interworking	888
15.4	Funk-LAN (WLAN)	891
15.4.1	Einführung	891
15.4.2	Technische Grundlagen	893
15.4.3	WLAN-Sicherheitsprobleme	897
15.4.4	WEP und WPA	899
15.4.5	802.11i Sicherheitsdienste (WPA2)	903
15.4.6	802.1X-Framework und EAP	914
15.5	Bluetooth	920
15.5.1	Einordnung und Abgrenzung	921
15.5.2	Technische Grundlagen	922
15.5.3	Sicherheitsarchitektur	927
15.5.4	Schlüsselmanagement	932
15.5.5	Authentifikation	937
15.5.6	Bluetooth-Sicherheitsprobleme	940
15.5.7	Secure Simple Pairing	943

15.6	ZigBee	949
15.6.1	Überblick	949
15.6.2	Sicherheitsarchitektur	952
15.6.3	Schlüsseltypen	953
15.6.4	Netzzutritt und Schlüsselmanagement	956
15.6.5	ZigBee 3.0	958
15.6.6	Sicherheitsbetrachtungen	963
Literaturverzeichnis		969
Abkürzungsverzeichnis		983
Index		993