
IT-Sicherheit

Konzept – Verfahren – Protokolle

von
Prof. Dr. Claudia Eckert
Technische Universität Darmstadt

3., überarbeitete und erweiterte Auflage

Oldenbourg Verlag München Wien

Inhaltsverzeichnis

1	Einführung	1
1.1	Grundlegende Begriffe	1
1.2	Schutzziele	6
1.3	Schwachstellen, Bedrohungen, Angriffe	13
1.4	Computer Forensik	24
1.5	Sicherheitsstrategie	26
1.6	Sicherheitsinfrastruktur	29
2	Spezielle Bedrohungen	33
2.1	Einführung	33
2.2	Buffer-Overflow	35
2.2.1	Einführung	35
2.2.2	Angriffe	38
2.2.3	Gegenmaßnahmen	41
2.3	Computerviren	43
2.3.1	Eigenschaften	43
2.3.2	Viren-Typen	45
2.3.3	Gegenmaßnahmen	51
2.4	Würmer	55
2.5	Trojanisches Pferd	61
2.5.1	Eigenschaften	61
2.5.2	Gegenmaßnahmen	63
2.6	Mobiler Code	67
2.6.1	Eigenschaften	67
2.6.2	Sicherheitsbedrohungen	68
2.6.3	Gegenmaßnahmen	70
3	Internet-(Un)Sicherheit	73
3.1	Einführung	73
3.2	Internet-Protokollfamilie	75
3.2.1	ISO/OSI-Referenzmodell	75
3.2.2	Das TCP/IP-Referenzmodell	81
3.2.3	Das Internet-Protokoll IP	83

3.2.4	Das Transport-Kontrollprotokoll TCP	86
3.2.5	Das User Datagram Protocol UDP	88
3.2.6	DHCP und NAT	90
3.3	Sicherheitsprobleme	93
3.3.1	Sicherheitsprobleme von IP	93
3.3.2	Sicherheitsprobleme von ICMP	99
3.3.3	Sicherheitsprobleme von ARP	101
3.3.4	Sicherheitsprobleme von UDP und TCP	102
3.4	Sicherheitsprobleme von Netzdiensten	106
3.4.1	Domain Name Service (DNS)	106
3.4.2	Network File System (NFS)	111
3.4.3	Network Information System (NIS)	117
3.4.4	World Wide Web (WWW)	119
3.4.5	Weitere Dienste	132
3.4.6	Angriffsszenario	137
3.5	Analysetools und Systemhärtung	138
4	Security Engineering	149
4.1	Entwicklungsprozess	150
4.1.1	Allgemeine Konstruktionsprinzipien	150
4.1.2	Phasen	151
4.1.3	BSI-Sicherheitsprozess	152
4.2	Strukturanalyse	155
4.3	Schutzbedarfsermittlung	157
4.3.1	Schadensszenarien	158
4.3.2	Schutzbedarf	160
4.4	Bedrohungsanalyse	161
4.4.1	Bedrohungsmatrix	162
4.4.2	Bedrohungsbaum	163
4.5	Risikoanalyse	169
4.5.1	Attributierung	170
4.5.2	Penetrationstests	175
4.6	Sicherheitsstrategie und -modell	177
4.7	Systemarchitektur und Validierung	178
4.8	Aufrechterhaltung im laufenden Betrieb	179
4.8.1	Dynamische Überwachung	179
4.8.2	Der elektronische Sicherheitsinspektor (eSI)	179
4.9	Sicherheitsgrundfunktionen	187
4.10	Realisierung der Grundfunktionen	191
4.11	Beispiel: Elektronische Shopping Mall	193
4.11.1	Systemanforderungen und Einsatzumgebung	193
4.11.2	Bedrohungsanalyse	194

4.11.3	Risikoanalyse	199
4.11.4	Sicherheitsstrategie	205
4.11.5	Sicherheitsarchitektur	207
5	Bewertungskriterien	209
5.1	TCSEC-Kriterien	209
5.1.1	Sicherheitsstufen	209
5.1.2	Kritik am Orange Book	212
5.1.3	Erkennen verdeckter Informationskanäle	213
5.2	IT-Kriterien	213
5.2.1	Mechanismen	214
5.2.2	Funktionsklassen	215
5.2.3	Qualität und Zertifikat	216
5.3	ITSEC-Kriterien	217
5.3.1	Evaluationsstufen	218
5.3.2	Qualität und Bewertung	219
5.4	Zertifizierung	220
5.5	Common Criteria	222
5.5.1	Einführung	222
5.5.2	Überblick über die CC	223
5.5.3	CC-Funktionsklassen	228
5.5.4	Schutzprofile	229
5.5.5	Vertrauenswürdigkeitsklassen	232
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
6.1.5	Klassifikationsschema	244
6.2	Zugriffskontrollmodelle	245
6.2.1	Zugriffsmatrix-Modell	245
6.2.2	Rollenbasierte Modelle	254
6.2.3	Chinese-Wall Modell	261
6.2.4	Bell-LaPadula Modell	266
6.3	Informationsflussmodelle	273
6.3.1	Verbands-Modell	273
6.4	Einsatz-Leitlinien	277
7	Kryptografische Verfahren	281
7.1	Einführung	281
7.2	Steganografie	283

7.2.1	Linguistische Steganografie	284
7.2.2	Technische Steganografie	285
7.3	Grundlagen kryptografischer Verfahren	287
7.3.1	Kryptografische Systeme	287
7.3.2	Anforderungen	291
7.4	Informationstheorie	294
7.4.1	Stochastische und kryptografische Kanäle	294
7.4.2	Entropie und Redundanz	296
7.4.3	Sicherheit kryptografischer Systeme	297
7.5	Symmetrische Verfahren	303
7.5.1	Permutation und Substitution	303
7.5.2	Block- und Stromchiffren	304
7.5.3	Betriebsmodi von Blockchiffren	309
7.5.4	Data Encryption Standard	313
7.5.5	AES	322
7.6	Asymmetrische Verfahren	325
7.6.1	Eigenschaften	325
7.6.2	Das RSA-Verfahren	329
7.7	Kryptoanalyse	340
7.7.1	Klassen kryptografischer Angriffe	341
7.7.2	Substitutionschiffren	342
7.7.3	Differentielle Kryptoanalyse	344
7.7.4	Lineare Kryptoanalyse	346
7.8	Kryptoregulierung	347
7.8.1	Hintergrund	347
7.8.2	Internationale Regelungen	349
7.8.3	Kryptopolitik in Deutschland	351
8	Hashfunktionen und elektronische Signaturen	353
8.1	Hashfunktionen	353
8.1.1	Grundlagen	354
8.1.2	Blockchiffren-basierte Hashfunktionen	359
8.1.3	Dedizierte Hashfunktionen	361
8.1.4	Message Authentication Code	365
8.2	Elektronische Signaturen	370
8.2.1	Anforderungen	370
8.2.2	Erstellung elektronischer Signaturen	371
8.2.3	Digitaler Signaturstandard (DSS)	378
8.2.4	Signaturgesetz	380
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	402
9.2.1	Schlüsselerzeugung	403
9.2.2	Schlüsselspeicherung und -vernichtung	405
9.3	Schlüsselaustausch	408
9.3.1	Schlüsselhierarchie	409
9.3.2	Naives Austauschprotokoll	410
9.3.3	Protokoll mit symmetrischen Verfahren	412
9.3.4	Protokoll mit asymmetrischen Verfahren	415
9.3.5	Leitlinien für die Protokollentwicklung	417
9.3.6	Diffie-Hellman Verfahren	420
9.4	Schlüsselerückgewinnung	426
9.4.1	Systemmodell	427
9.4.2	Grenzen und Risiken	432
10	Authentifikation	437
10.1	Einführung	438
10.2	Authentifikation durch Wissen	440
10.2.1	Passwortverfahren	440
10.2.2	Authentifikation in Unix	451
10.2.3	Challenge-Response-Verfahren	457
10.2.4	Zero-Knowledge-Verfahren	462
10.3	Smartcard	465
10.3.1	Architektur	466
10.3.2	Sicherheit	469
10.4	Biometrie	478
10.4.1	Einführung	478
10.4.2	Biometrische Techniken	480
10.4.3	Biometrische Authentifikation	484
10.4.4	Fallbeispiel: Fingerabdruckerkennung	486
10.4.5	Sicherheit biometrischer Techniken	489
10.5	Authentifikation in verteilten Systemen	493
10.5.1	RADIUS	494
10.5.2	Remote Procedure Call	499
10.5.3	Secure RPC	500
10.5.4	Kerberos-Authentifikationssystem	503
10.5.5	Microsoft Passport-Protokoll	514
10.5.6	Authentifikations-Logik	529

11	Zugriffskontrolle	539
11.1	Einleitung	539
11.2	Speicherschutz	540
11.2.1	Betriebsmodi und Adressräume	541
11.2.2	Virtueller Speicher	542
11.3	Objektschutz	546
11.3.1	Zugriffskontrolllisten	548
11.3.2	Zugriffsausweise	555
11.4	Zugriffskontrolle in Unix	559
11.4.1	Identifikation	560
11.4.2	Rechtevergabe	561
11.4.3	Zugriffskontrolle	566
11.5	Zugriffskontrolle unter Windows 2000	569
11.5.1	Architektur-Überblick	570
11.5.2	Sicherheitssystem	572
11.5.3	Datenstrukturen zur Zugriffskontrolle	575
11.5.4	Zugriffskontrolle	580
11.6	Verschlüsselnde Dateisysteme	583
11.6.1	Einführung	583
11.6.2	Klassifikation	584
11.6.3	Encrypting File System (EFS)	586
11.7	Systembestimmte Zugriffskontrolle	592
11.8	Sprachbasierter Schutz	595
11.8.1	Programmiersprache	595
11.8.2	Übersetzer und Binder	599
11.9	Java-Sicherheit	604
11.9.1	Die Programmiersprache	605
11.9.2	Sicherheitsarchitektur	606
11.9.3	Sicherheitsmodelle	611
11.9.4	Fazit	616
11.10	Trusted Computing	617
11.10.1	Einführung	618
11.10.2	TCG-Architektur-Überblick	620
11.10.3	TPM	626
11.10.4	TPM-Schlüssel	630
11.10.5	Sicheres Booten	639
11.10.6	Einsatzmöglichkeiten für TCG-Plattformen	644
11.10.7	Fazit und offene Probleme	645
12	Sicherheit in Netzen	651
12.1	Firewall-Technologie	652
12.1.1	Einführung	652

12.1.2	Paketfilter	655
12.1.3	Proxy-Firewall	670
12.1.4	Applikationsfilter	674
12.1.5	Architekturen	678
12.1.6	Risiken und Grenzen	681
12.2	OSI-Sicherheitsarchitektur	687
12.2.1	Sicherheitsdienste	687
12.2.2	Sicherheitsmechanismen	690
12.3	Sichere Kommunikation	696
12.3.1	ISO/OSI-Einordnung	697
12.3.2	Virtual Private Network (VPN)	704
12.4	IPSec	708
12.4.1	Überblick	709
12.4.2	Security Association und Policy-Datenbank	711
12.4.3	AH-Protokoll	717
12.4.4	ESP-Protokoll	720
12.4.5	Schlüsselaustauschprotokoll IKE	724
12.4.6	Sicherheit von IPSec	729
12.5	Secure Socket Layer (SSL)	735
12.5.1	Überblick	735
12.5.2	Handshake-Protokoll	739
12.5.3	Record-Protokoll	742
12.5.4	Sicherheit von SSL	745
12.6	Sichere Anwendungsdienste	747
12.6.1	Elektronische Mail	748
12.6.2	Elektronischer Zahlungsverkehr	766
13	Sichere mobile und drahtlose Kommunikation	775
13.1	Einleitung	776
13.1.1	Heterogenität der Netze	776
13.1.2	Entwicklungsphasen	777
13.2	GSM	781
13.2.1	Grundlagen	781
13.2.2	GSM-Grobarchitektur	782
13.2.3	Identifikation und Authentifikation	783
13.2.4	Gesprächsverschlüsselung	787
13.2.5	Sicherheitsprobleme	790
13.2.6	Weiterentwicklungen	793
13.2.7	GPRS	795
13.3	UMTS	797
13.3.1	UMTS-Sicherheitsarchitektur	798
13.3.2	Authentifikation und Schlüsselvereinbarung	800

13.3.3	Vertraulichkeit und Integrität	804
13.3.4	Fazit	804
13.4	Funk-LAN (WLAN)	806
13.4.1	Einführung	806
13.4.2	Technische Grundlagen	808
13.4.3	WLAN-Sicherheitsprobleme	813
13.4.4	Einbindung eines WLAN in die Netztopologie	817
13.4.5	WEP im Überblick	819
13.4.6	WEP-Authentifikation	820
13.4.7	WEP-Integrität	823
13.4.8	WEP-Vertraulichkeit	826
13.4.9	Zusätzliche Sicherheitsmaßnahmen	831
13.4.10	Weiterentwicklungen des 802.11-Standards	833
13.4.11	802.11X-Framework und EAP	835
13.4.12	TKIP	840
13.5	Bluetooth	845
13.5.1	Einordnung und Abgrenzung	846
13.5.2	Technische Grundlagen	849
13.5.3	Sicherheitsarchitektur	854
13.5.4	Schlüsselmanagement	859
13.5.5	Authentifikation	864
13.5.6	Bluetooth-Sicherheitsprobleme	867
13.6	Future Net	871
13.6.1	Entwicklungsstufen	871
13.6.2	Vom Informations- zum Wissensmanagement	873
13.6.3	Next Generation Networks	875
	Literaturverzeichnis	881
	Glossar	897
	Index	905