

IT-Sicherheit

Konzept -Verfahren - Protokolle

von

Dr. habil. Claudia Eckert

Technische Universität München

Oldenbourg Verlag München Wien

Inhaltsverzeichnis

Vorwort	V
1 Einführung	1
1.1 Grundlegende Begriffe	1
1.2 Sicherheitseigenschaften.	4
1.3 Bedrohungen und Angriffe.	9
1.4 Sicherheitsinfrastruktur	13
2 Software-Anomalien und mobiler Code	17
2.1 Einführung	17
2.2 Computerviren.	18
2.2.1 Eigenschaften.	18
2.2.2 Viren-Typen.	20
2.2.3 Gegenmaßnahmen.	24
2.3 Würmer.	27
2.4 Trojanisches Pferd.	30
2.4.1 Eigenschaften.	31
2.4.2 Gegenmaßnahmen.	32
2.5 Mobiler Code.	34
2.5.1 Eigenschaften.	34
2.5.2 Sicherheitsbedrohungen.	34
2.5.3 Gegenmaßnahmen.	37
3 Internet-(Un)Sicherheit	39
3.1 Einführung.	39
3.2 Internet-Protokollfamilie.	41
3.2.1 ISO/OSI-Referenzmodell.	41
3.2.2 Das TCP/IP-Referenzmodell.	44
3.2.3 Das Internet-Protokoll IP.	45
3.2.4 Das Transport-Kontrollprotokoll TCP.	48
3.2.5 Das User Datagram Protocol UDP.	50
3.3 Sicherheitsprobleme.	50
3.3.1 Sicherheitsprobleme von IP.	51
3.3.2 Sicherheitsprobleme von ICMP.	55

3.3.3	Sicherheitsprobleme von ARP.	57
3.3.4	Sicherheitsprobleme von UDP und TCP.	58
3.4	Sicherheitsprobleme von Netzdiensten.	62
3.4.1	Domain Name Service (DNS).	63
3.4.2	Network File System (NFS).	65
3.4.3	Network Information System (NIS).	70
3.4.4	World Wide Web (WWW).	71
3.4.5	Weitere Dienste.	76
3.4.6	Angriffsszenario	78
4	Konstruktion sicherer Systeme	81
4.1	Entwicklungsprozess.	81
4.1.1	Allgemeines Vorgehen.	81/
4.1.2	Entwicklungsphasen.	82
4.1.3	Allgemeine Konstruktionsprinzipien.	90
4.2	Sicherheitsgrundfunktionen.	91
4.3	Realisierung der Grundfunktionen	94
4.4	Beispiel: Elektronische Shopping Mall.	96
4.4.1	Systemanforderungen und Einsatzumgebung.	96
4.4.2	Bedrohungsanalyse.	97
4.4.3	Risikoanalyse.	102
4.4.4	Sicherheitsstrategie.	107
4.4.5	Sicherheitsarchitektur.	109
4.5	Sicherheitskriterien.	110
4.5.1	TCSEC-Kriterien.	111
4.5.2	IT-Kriterien.	115
4.5.3	(JTSEC-Kriterien.	118
4.5.4	Zertifizierung.	121
4.5.5	Fazit und Ausblick.	123
5	Sicherheitsmodelle	125
5.1	Modell-Klassifikation.	125
5.1.1	Objekte und Subjekte.	126
5.1.2	Zugriffsrechte	127
5.1.3	Zugriffsbeschränkungen.	128
5.1.4	Sicherheitsstrategien.	128
5.1.5	Klassifikationsschema	130
5.2	Zugriffskontrollmodelle.	131
5.2.1	Zugriffsmatrix-Modell.	131
5.2.2	Rollenbasierte Modelle.	140
5.2.3	Chinese-Wall Modell.	146
5.2.4	Bell-LaPadula Modell.	152

5.3	Informationsflussmodelle.	158
5.3.1	Verbands-Modell.	159
5.4	Einsatz-Leitlinien.	162
6	Kryptographische Verfahren	165
6.1	Einführung.	165
6.2	Steganographie.	167
6.2.1	Linguistische Steganographie.	168
6.2.2	Technische Steganographie.	169
6.3	Grundlagen kryptographischer Verfahren.	171
6.3.1	Kryptographische Systeme.	171
6.3.2	Anforderungen.	175
6.4	Informationstheorie.	178
6.4.1	Stochastische und kryptographische Kanäle.	178
6.4.2	Entropie und Redundanz.	180
6.4.3	Sicherheit kryptographischer Systeme.	181
6.5	Symmetrische Verfahren.	187
6.5.1	Permutation und Substitution.	187
6.5.2	Block-und Stromchiffren.	188
6.5.3	Betriebsmodi von Blockchiffren.	191
6.5.4	Data Encryption Standard.	196
6.5.5	International Data Encryption Algorithm.	205
6.6	Asymmetrische Verfahren.	207
6.6.1	Eigenschaften.	207
6.6.2	Das RSA-Verfahren.	211
6.7	Kryptoanalyse.	222
6.7.1	Klassen kryptographischer Angriffe.	223
6.7.2	Substitutionschiffren.	224
6.7.3	Differentielle Kryptoanalyse.	226
6.7.4	Lineare Kryptoanalyse.	228
6.8	Kryptoregulierung.	229
6.8.1	Hintergrund.	229
6.8.2	Internationale Regelungen.	231
6.8.3	Kryptopolitik in Deutschland.	233
7	Hashfunktionen und digitale Signaturen	235
7.1	Hashfunktionen.	235
7.1.1	Grundlagen.	236
7.1.2	Blockchiffren-basierte Hashfunktionen.	241
7.1.3	Dedizierte Hashfunktionen.	243
7.1.4	Message Authentication Code.	247
7.2	Digitale Signaturen.	251

7.2.1	Anforderungen	251
7.2.2	Signaturgesetz	252
7.2.3	Erstellung digitaler Signaturen	255
7.2.4	Digitaler Signaturstandard (DSS).	262
8	Schlüsselmanagement	265
8.1	Zertifizierung	265
8.1.1	Zertifikate.	265
8.1.2	Zertifizierungsstelle.	267
8.1.3	Public-Key Infrastruktur.	271
8.2	Schlüsselerzeugung und -aufbewahrung	273
8.2.1	Schlüsselerzeugung	273
8.2.2	Schlüsselspeicherung und -Vernichtung	275-
8.3	Schlüsselaustausch	278
8.3.1	Schlüsselhierarchie.	279
8.3.2	Naives Austauschprotokoll	281
8.3.3	Protokoll mit symmetrischen Verfahren.	282
8.3.4	Protokoll mit asymmetrischen Verfahren.	285
8.3.5	Leitlinien für die Protokollentwicklung	287
8.3.6	Diffie-Hellman Verfahren.	290
8.4	Schlüssel-Rückgewinnung	296
8.4.1	Einführung	296
8.4.2	Systemmodell	297
8.4.3	Grenzen und Risiken.	301
9	Authentifikation	305
9.1	Einführung	305
9.2	Authentifikation durch Wissen	307
9.2.1	Passwortverfahren.	307
9.2.2	Authentifikation in Unix.	314
9.2.3	Challenge-Response Verfahren.	320
9.2.4	Zero-Knowledge Verfahren.	323
9.3	Chipkarte.	326
9.3.1	Architektur.	327
9.3.2	Sicherheit	330
9.3.3	Fallbeispiel GSM.	336
9.4	Biometrie.	344
9.4.1	Einführung	344
9.4.2	Biometrische Techniken.	346
9.4.3	Beispiele.	348
9.4.4	Sicherheit biometrischer Techniken	350
9.5	Authentifikation in verteilten Systemen.	354

9.5.1	Remote Procedure Call	354
9.5.2	SecureRPC	355
9.5.3	Kerberos-Authentifikationssystem.	358
9.5.4	Authentifikations-Logik.	366
10	Zugriffskontrolle	375
10.1	Einleitung	375
10.2	Speicherschutz	376
10.2.1	Betriebsmodi und Adressräume.	377
10.2.2	Virtueller Speicher.	378
10.3	Objektschutz	382
10.3.1	Zugriffskontrolllisten.	384
10.3.2	Zugriffsausweise.	390
10.3.3	Verschlüsselnde Dateisysteme.	398
10.4	Systembestimmte Zugriffskontrolle.	403
10.5	Zugriffskontrolle in Unix.	406
10.5.1	Rechtevergabe.	407
10.5.2	Implementierung der Zugriffskontrolle.	411
10.6	Sprachbasierter Schutz	414
10.6.1	Programmiersprache.	415
10.6.2	Übersetzer und Binder.	418
10.7	Java-Sicherheit	424
10.7.1	Die Programmiersprache.	425
10.7.2	Sicherheitsarchitektur.	426
10.7.3	Sicherheitsmodelle.	430
10.7.4	Fazit	435
11	Sicherheit in Netzen	437
11.1	Firewall-Technologie	438
11.1.1	Einführung.	438
11.1.2	Paketfilter.	441
11.1.3	Verbindungs-Gateway.	449
11.1.4	Applikationsfilter.	453
11.1.5	Architekturen.	456
11.1.6	Risiken und Grenzen.	459
11.2	OSI-Sicherheitsarchitektur.	463
11.2.1	Sicherheitsdienste.	463
11.2.2	Sicherheitsmechanismen.	466
11.3	Sichere Kommunikation.	471
11.3.1	ISO/OSI-Einordnung	472
11.3.2	Virtual Private Network (VPN).	479
11.3.3	IPsec.	481

11.3.4	Secure Socket Layer (SSL).	500
11.4	Sichere Anwendungsdienste.	508
11.4.1	Elektronische Mail.	509
11.4.2	Elektronischer Zahlungsverkehr.	517
11.4.3	Internet-Homebanking.	522
Literaturverzeichnis		529
Index		545