

Rolf Oppliger

Computersicherheit

Eine Einführung

Technische Hochschule Darmstadt
FACHBEREICH INFORMATIK
BIBLIOTHEK

Inventar-Nr.: 20555

Sachgebiete: E.6

Standort: 19.92



Inhaltsverzeichnis

1	Einleitung	11
1.1	Motivation	11
1.2	Terminologie	12
1.3	Bedrohungen	15
1.3.1	Computerkriminalität	15
1.3.2	Physikalische Ereignisse	19
1.4	Risikomanagement	21
1.4.1	Risikoanalyse	21
1.4.2	Sicherheitsplanung	23
2	Kryptologie	27
2.1	Terminologie	27
2.1.1	Kryptographie	28
2.1.2	Block- und Flusschiffrierungen	30
2.1.3	Kryptoanalysis und -analyse	30
2.2	Substitutionsmethoden	32
2.2.1	Monoalphabetische Substitutionsmethoden	32
2.2.2	Homophonische Substitutionsmethoden	33
2.2.3	Polyalphabetische Substitutionsmethoden	33
2.2.4	“Sichere” Substitutionsmethoden	36
2.3	Transpositionsmethoden	37

3 Sichere Kryptosysteme	39
3.1 Symmetrische Kryptosysteme	39
3.1.1 DES	40
3.2 Asymmetrische Kryptosysteme	46
3.2.1 Merkle-Hellman-Rucksack	46
3.2.2 RSA	47
3.3 Schlüsselverwaltung	48
3.4 Elektronische Unterschriften	50
3.5 Schlussfolgerungen	51
4 Allgemeine Sicherheitsmassnahmen	55
4.1 Physikalische Schutzmassnahmen	55
4.1.1 Bauliche Schutzmassnahmen	55
4.1.2 Ergänzende Schutzmassnahmen	58
4.2 Zugangskontrollen	60
4.2.1 Konstante Passwörter	62
4.2.2 Dynamische Passwörter	65
5 Betriebssysteme	67
5.1 Terminologie	67
5.2 Zugriffskontrollen	68
5.2.1 Diskrete Zugriffskontrollen	69
5.2.2 Regelbasierte Zugriffskontrollen	71
5.3 Betriebssystementwurf	74
5.3.1 Speicherschutz	75
5.3.2 Architekturkonzepte	76
5.3.3 Evaluation und Zertifikation	78
5.4 Beispiele	83
5.4.1 UNIX	84
5.4.2 VMS	87
5.4.3 Scomp	89

6	Software	91
6.1	Einführung	91
6.2	Softwareanomalien und -manipulationen	93
6.2.1	Wanzen	93
6.2.2	Hintertüren	94
6.2.3	Trojanische Pferde	94
6.2.4	Würmer	97
6.2.5	Software-Bomben	99
6.2.6	Computerviren	99
6.3	Schutzmassnahmen	106
6.3.1	Virenschutzmassnahmen	106
6.3.2	Programmentwicklungsverfahren	110
6.3.3	Strafrecht	111
7	Personalcomputer und LAN	115
7.1	Sicherheitsprobleme	115
7.1.1	Lack of Sensitivity	116
7.1.2	Lack of Tools	116
7.2	Schutzmassnahmen	117
7.3	Lokale Netze	117
7.4	Kopierschutz	119
8	Computernetze	121
8.1	Angriffsformen	121
8.2	OSI-Sicherheitsarchitektur	123
8.2.1	Sicherheitsdienste	123
8.2.2	Sicherheitsmechanismen	126
8.3	Öffentliche Netze	131
8.3.1	Mietleitungsnetze	132
8.3.2	Wählleitungsnetze	133
8.3.3	X.25-Netze	135

9 Datenbanksysteme	139
9.1 Datenschutz	139
9.2 Inferenzproblem	140
9.2.1 Statistisches Datenbankmodell	141
9.2.2 Angriffsformen	142
9.2.3 Inferenzprävention	144
A Abkürzungen	147