

Horst Langendörfer
Bettina Schnor

Verteilte Systeme



Carl Hanser Verlag München Wien

Inhalt

1	Grundlegende Definitionen, Klassifikation der Hardware, Architekturkonzepte	1
1.1	Betriebssysteme im Wandel	1
1.2	Klassifikation der Hardware	3
1.3	Netzwerke	5
1.4	Hypercubes	12
1.5	Transputer = TRANSfer + comPUTER	15
1.6	Lokale Netze	17
1.7	Verteilte Betriebssysteme: Entwicklungsziele und Architekturkonzepte .	18
2	Interprozeßkommunikation	27
2.1	Netzkommunikation	29
2.2	Message Passing versus Distributed Shared Memory	36
2.3	Remote Procedure Call	38
2.4	Beispiel Sun RPC	42
2.5	RPC-Protokolle	47
2.6	Gruppenkommunikation	52
2.6.1	Broadcast im LAN	53
2.6.2	Broadcast für Mehrprozessorarchitekturen	54
2.7	Mach-Interprozeßkommunikation	59
3	Synchronisation	69
3.1	Formale Beschreibung	69
3.2	Der zentrale Ansatz	72
3.3	Synchronisation mittels Zeitmarken	76
3.4	Tokenverfahren	83
3.4.1	Logischer Ring	83
3.4.2	Tokenwechsel auf Anforderung	84

4	Verteilte Dateisysteme	87
4.1	Motivation	87
4.2	Konzepte	90
4.3	Caching	96
4.4	Network-File-System	98
4.5	Andrew File System	102
4.6	Sprite	105
4.7	Vergleich der besprochenen Systeme	106
4.8	Replikation	108
4.8.1	Master-Slave-Strategie	109
4.8.2	Votierungsverfahren	110
5	Prozeßverwaltung	115
5.1	Gruppenscheduling	115
5.1.1	Strategien für deterministisches Gruppenscheduling	118
5.1.2	Dynamisches Gruppenscheduling	125
5.1.3	Wave Scheduling	127
5.1.4	Mapping und Scheduling unter Mach	131
5.1.5	Überblick über kommerzielle Systeme	133
5.2	Lastverteilung	135
5.2.1	Lastverteilungssysteme	137
5.2.2	Condor - A Hunter of idle Workstations	143
6	Verklemmungen	149
6.1	Modellbildung und Verklemmungserkennung	151
6.2	Zentraler Ansatz	153
6.3	Verteilte Verklemmungserkennung	155
7	Sichere Kommunikation	157
7.1	Grundlagen	158
7.1.1	Eine kurze Einführung in die Kryptologie	159
7.1.2	Die Ausgangssituation in Rechnernetzen und verteilten Systemen	162
7.1.3	Eine Logik zur Authentizität	164
7.2	Das Protokoll von Needham und Schroeder	173
7.3	Der Netzwerk-Authentifizierungsservice Kerberos	180
7.3.1	Arbeitsweise von Kerberos Version 4	180
7.3.2	Untersuchung des Authentifizierungsprotokolls in Kerberos 4	184

7.3.3	Ein Überblick über Kerberos Version 5	187
7.4	KryptoKnight – Ein System zur Authentifizierung und Schlüsselverteilung	189
7.4.1	Verwendete Verfahren	189
7.4.2	Angriffe auf einfache Protokolle	196
7.5	Ein Protokoll mit geringer Nachrichtenanzahl	198
7.6	Ein Protokoll für einen Authentifizierungsservice ohne synchronisierte Uhren	202
7.6.1	Das initiale Protokoll	202
7.6.2	Wiederholung der Authentifizierung	204
7.7	Standards der ISO/CCITT	206
7.7.1	CCITT X.509: The Directory - Authentication Framework	208
7.8	Der Authentifizierungsservice SPX	211
7.9	Authentizität in verteilten Betriebssystemen und RPCs	214
7.9.1	Amoeba	215
7.9.2	Mach	217
7.9.3	Sichere RPCs	218
7.9.4	SUN RPC	221
7.10	Authentifizierter Nachrichtenaustausch ohne Verschlüsselung	225
7.10.1	Nachteile und Probleme bei der Verwendung von Verschlüsselungsverfahren	225
7.10.2	Verwendung von Einweg-Hash-Funktionen	226
7.11	Ein Zero-Knowledge Protokoll zur Identifizierung	228
7.12	Automatische Protokollanalyse und Benutzeridentifikation	233
7.12.1	INTERROGATOR	233
7.12.2	KEYMEX	240
7.12.3	MINOS	242
8	Leistungsaspekte bei verteilten Systemen	249
8.1	Grundlegende Definitionen und Vorbemerkungen	249
8.2	Das Gesetz von Amdahl	252
8.3	Die Benchmarks der EuroBen Gruppe – Die Genesis Benchmarks	256
8.4	Benchmarks für verteilte Dateisysteme	258
8.5	Durchführung eines Benchmarktests	260
8.6	RAPS-Benchmark	262
9	Verteilte Verarbeitung	265
9.1	LINDA	265

9.2	ISIS	268
9.2.1	Grundlagen des ISIS-Systems	268
9.2.2	System-Architektur	271
9.2.3	Das Drilling-Programm: Ein Beispiel für eine fehlertolerante verteilte Anwendung	273
9.3	Effizienz von parallelen Make-Programmen auf Workstation-Clustern	287
10	Beispiele für verteilte Betriebssysteme	295
10.1	Amoeba	295
10.2	Mach und OSF/1	301
10.3	DCE	305
10.3.1	Komponenten	306
10.3.2	Bewertung	311
10.4	Plan 9	313
	FTP-Adressen	319
	Literaturverzeichnis	321
	Index	341