

Rechnernetze und Datensicherheit

Steffen Kaup
Burkard Neumayer

17. Oktober 2003

Angewandte Informatik

**Steffen Kaup
Burkard Neumayer**

Rechnernetze und Datensicherheit

Shaker Verlag
Aachen 2003

Bibliografische Information der Deutschen Bibliothek

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.ddb.de> abrufbar.

Copyright Shaker Verlag 2003

Alle Rechte, auch das des auszugsweisen Nachdruckes, der auszugsweisen oder vollständigen Wiedergabe, der Speicherung in Datenverarbeitungsanlagen und der Übersetzung, vorbehalten.

Printed in Germany.

ISBN 3-8322-2136-0

ISSN 0945-0807

Shaker Verlag GmbH • Postfach 101818 • 52018 Aachen

Telefon: 02407 / 95 96 - 0 • Telefax: 02407 / 95 96 - 9

Internet: www.shaker.de • eMail: info@shaker.de

Inhaltsverzeichnis

A	Rechnertechnik und Betriebssysteme	5
1	Rechnertechnik	7
1.1	Klassifizierung von Rechnersystemen	7
1.2	Rechnerarchitektur	9
1.2.1	Von-Neumann-Architektur	9
1.2.2	Zusammenspiel der Komponenten	9
1.3	Periphere Schnittstellen	13
1.4	Mehrprozessorsysteme	15
1.4.1	Parallelrechner	15
1.4.2	Verteilte Systeme	16
1.4.3	Realzeitsysteme	17
1.5	Betriebsarten der Kommunikation	18
1.6	Vom Abakus zum Avatar - eine Historie	19
1.7	Rechner-Vernetzung	24
1.7.1	Ausdehnung von Netzwerken	24
1.7.2	Arten der Adressierung	25
1.7.3	Netzwerkarten	26
1.7.3.1	Peer-to-Peer-Netzwerk	26
1.7.3.2	Client/Server-Netzwerk	27
1.8	Physikalische Topologien	28
1.8.1	Bus-Topologie	28
1.8.2	Stern-Topologie	32
1.8.3	Ring-Topologie	34
1.9	Übertragungsmedien	36
1.9.1	Twisted-Pair	37
1.9.2	Koaxialkabel	39
1.9.3	Lichtwellenleiter	40
1.9.4	Überblick über die gebräuchlichen Standardkabel	42
1.10	Zugriffsverfahren	43
1.10.1	CSMA/CD	43
1.10.2	CSMA/CA	44

1.10.3	Token Passing	45
2	Betriebssysteme	47
2.1	Definition und Aufgaben eines Betriebssystems	47
2.1.1	Betriebsmittelverwaltung	49
2.1.2	Aufgabenverwaltung	49
2.1.3	Datenverwaltung	50
2.2	Aufgabenabarbeitung (Tasking)	51
2.3	Schnittstellen zum Benutzer	53
2.4	Wichtige Betriebssysteme	54
2.4.1	Microsoft-Betriebssysteme	54
2.4.1.1	Windows 95/98	56
2.4.1.2	Windows NT	56
2.4.1.3	Windows XP	58
2.4.2	UNIX	59
2.4.3	Linux	61
2.4.4	OS/2	62
2.4.5	Vergleich von Befehlssätzen	63
3	Übungsaufgaben Teil A	65
3.1	Rechnertechnik	65
3.2	Betriebssysteme	67
3.3	Anwendungsprogramme	68
B	Internet: Dienste, Recherchen und Programmierung	71
4	Dienste im Internet/Intranet	73
4.1	Historie und Einführung	73
4.2	Begriffsabgrenzung Internet/Intranet	74
4.2.1	Internet	74
4.2.2	Intranet	74
4.3	Die wichtigsten Dienste im Überblick	75
4.3.1	Telnet	75
4.3.2	FTP	75
4.3.3	eMail	76
4.3.4	Gopher	77
4.3.5	LDAP	77
4.4	Zugang zu den Diensten mittels eines Browsers	78
4.4.1	Uniform Resource Locator	78
4.4.2	Bookmarks	79

4.5	Organisationen und Gremien	80
4.5.1	Definition und Eigenschaften von Domänen	80
4.5.2	Gremienstruktur im Internet	81
5	Informationsrecherche im Web	83
5.1	Einführung in die Informationsrecherche	83
5.2	Begriffsabgrenzung Kataloge/Suchmaschinen	84
5.2.1	Kataloge	85
5.2.2	Suchmaschinen	86
5.2.2.1	Vorgehensweise zur Wissenserhebung	86
5.2.2.2	Bewertung von Suchergebnissen	87
5.2.2.3	Metasuchmaschinen	88
6	Protokolle und Adressen im Web	91
6.1	Modell: Open Systems Interconnection	91
6.2	IP-Adressierung	95
6.2.1	Notwendigkeit von Adressierung	95
6.2.2	Ethernet-Adressen	95
6.2.3	IP-Adressen und deren Klassifizierung	95
6.2.4	Spezielle IP-Adressen	98
6.2.5	Subnetzmasken	99
6.2.6	Subnetting	101
6.3	Protokolle	102
6.3.1	Internet Protocol (IP)	103
6.3.2	Transmission Control Protocol (TCP)	104
6.4	Der Routing-Prozess	106
6.4.1	Einführung in den Routing-Prozess	106
6.4.2	Ermitteln der Netzwerkkonfiguration	108
7	Internet-Programmierung	109
7.1	HTML	109
7.1.1	Einführung in HTML	109
7.1.2	Aufbau von HTML-Seiten	110
7.1.3	Steueranweisungen (Tags)	111
7.1.4	Fenstertitel und Meta-Tags	112
7.1.4.1	Titel des Browserfensters	112
7.1.4.2	Angabe von Meta-Tags	113
7.1.5	Schriftmanipulation	114
7.1.5.1	Darstellende Tags	114
7.1.5.2	Logische Tags	116
7.1.6	Sonderzeichen	117
7.1.7	Listen	119

7.1.8	Tabellen	120
7.1.8.1	Gerüst einer Tabelle	120
7.1.8.2	Vordefinieren von Spalten	121
7.1.8.3	Rahmen und Trennlinien	124
7.1.8.4	Zellenfusion	125
7.1.9	Dimensionierung und Ausrichtung	126
7.1.9.1	Verweise (Hyperlinks)	127
7.1.10	Farbgestaltung	128
7.1.11	Bildschirmaufteilung (Frames)	131
7.1.11.1	Das Frameset	131
7.1.11.2	Horizontale Aufteilung	133
7.1.11.3	Vertikale Aufteilung	135
7.1.11.4	Kombinierte Aufteilung	136
7.1.12	Formatvorlagen (Style Sheets)	139
7.1.12.1	Aufbau von Style Sheets	139
7.1.12.2	Integration von Style Sheets in eine HTML-Seite	140
7.2	Einführung in JavaScript	142
7.2.1	Einbindung von JavaScript in HTML	142
7.2.2	Kommentare	144
7.2.3	Alternativer Text	144
7.2.4	Funktionen	145
7.2.4.1	Funktionsaufruf beim Start	145
7.2.4.2	Ereignisorientierter Funktionsaufruf	146
7.2.5	Variablen in JavaScript	149
7.2.5.1	Variablendeklaration und -initialisierung	149
7.2.6	Operatoren	150
7.2.6.1	Arithmetische Operatoren	151
7.2.6.2	Vergleichende Operatoren	152
7.2.6.3	Logische Operatoren	152
7.2.7	Bedingte Abfragen	154
7.2.7.1	Eingabe von Variablen	154
7.2.7.2	IF-Abfrage	155
7.2.7.3	SWITCH-Abfrage	157
7.2.8	Schleifen	159
7.2.8.1	Do-WHILE-Schleife	159
7.2.8.2	WHILE-Schleife	160
7.2.8.3	FOR-Schleife	161
7.2.9	Versions-Handling	162

8	Übungsaufgaben Teil B	163
8.1	Dienste im Internet	163
8.2	Informationsrecherche	164
8.3	Internet-Programmierung	165
C	Kryptologie und Datensicherheit	167
9	Kryptologie - was ist das?	169
9.1	Gründe für die Notwendigkeit von Kryptologie	169
9.2	Ziele und Ansprüche der Kryptologie	170
9.3	Kryptoanalyse/Krypto-Angriffe	173
10	Symmetrische Verschlüsselungsverfahren	175
10.1	Transpositionschiffren	177
10.2	Substitutionschiffren	179
10.2.1	Monoalphabetische Substitution	179
10.2.1.1	Additive Substitution	179
10.2.1.2	Cäsar-Chiffre	181
10.2.1.3	Multiplikative Substitution	181
10.2.1.4	Affine Substitution	182
10.2.2	Polyalphabetische Substitution	183
10.2.2.1	Vigenère-Chiffre	183
10.2.2.2	One-Time-Pad	184
10.3	Data Encryption Standard	185
10.3.1	Funktionsweise des DES	185
10.3.1.1	Die Funktion F	186
10.3.1.2	Die Schlüsselaufbereitung des DES	187
10.3.2	Double-DES	187
10.3.3	Triple-DES	188
10.3.4	Sicherheit und Verwundbarkeit des DES	189
10.4	International Data Encryption Algorithm	190
10.4.1	Funktionsweise des IDEA	191
10.5	Rivest Cipher Nr.4	192
11	Asymmetrische Verschlüsselungsverfahren	193
11.1	Diffie-Hellman-Schlüsseltausch	195
11.1.1	Funktionsweise von Diffie-Hellman	195
11.1.2	Sicherheit von Diffie-Hellman	196
11.2	Der RSA-Algorithmus	197
11.2.1	Sicherheit des RSA-Algorithmus	200

12 Digitale Signaturen	203
12.1 Was sind digitale Signaturen?	203
12.2 RSA als Signaturverfahren	203
12.3 Einsatz diskreter Logarithmen	205
12.3.1 Funktionsweise von El-Gamal	205
12.3.2 Data Signature Algorithm	205
12.4 Gegenüberstellung von RSA und DLSS	206
12.5 Einweg- und Falltürfunktionen	207
12.5.1 Der diskrete Logarithmus	207
12.5.2 Das Faktorisierungsproblem	207
12.6 Kryptographische Hashfunktionen	208
12.6.1 Die wichtigsten kryptographischen Hashfunktionen	209
13 Algorithmentheorie	211
13.1 Euklidischer Algorithmus	211
13.1.1 Erweiterter Euklidischer Algorithmus	213
13.2 Primalität	215
13.2.1 Überprüfung auf Primalität	215
13.2.2 Generierung von großen Primzahlen	217
14 Angewandte Standards	219
14.1 Secure Socket Layer	219
14.1.1 Funktionsweise von SSL	219
14.1.2 Sicherheit von SSL	222
14.2 Pretty Good Privacy	224
14.2.1 Funktionsweise von PGP	224
14.2.2 Vulnerabilität von PGP und abschließende Betrachtungen	225
15 Absicherung eines Konzernverbundnetzes	227
15.1 Firewalls	227
15.2 Proxy-Server	229
15.3 Viren, Würmer und sonstige Schädlinge	230
15.3.1 Viren	230
15.3.2 Würmer	232
15.3.3 Trojaner	232
15.3.4 Spyware	233
15.3.5 Hoaxes	233
15.3.6 Erkennung von Viren	234
16 Übungsaufgaben Teil C	235
16.1 Kryptologie allgemein	235
16.2 Symmetrische Kryptographie-Verfahren	235

16.3 Asymmetrische Kryptographie-Verfahren	236
16.4 Firewalls und Proxies	236
16.5 Viren und Würmer	237