

X . media . press



Christoph Meinel · Harald Sack

Digitale Kommunikation

Vernetzen, Multimedia, Sicherheit

 Springer

Prof. Dr. Christoph Meinel
Hasso-Plattner-Institut für
Softwaresystemtechnik GmbH
Prof.-Dr.-Helmert-Str. 2–3
14482 Potsdam
Germany
meinel@hpi.uni-potsdam.de

Dr. Harald Sack
Hasso-Plattner-Institut für
Softwaresystemtechnik GmbH
Prof.-Dr.-Helmert-Str. 2–3
14482 Potsdam
Germany
harald.sack@hpi.uni-potsdam.de

ISSN 1439-3107

ISBN 978-3-540-92922-2

e-ISBN 978-3-540-92923-9

DOI 10.1007/978-3-540-92923-9

Springer Dordrecht Heidelberg London New York

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

© Springer-Verlag Berlin Heidelberg 2009

Dieses Werk ist urheberrechtlich geschützt. Die dadurch begründeten Rechte, insbesondere die der Übersetzung, des Nachdrucks, des Vortrags, der Entnahme von Abbildungen und Tabellen, der Funksendung, der Mikroverfilmung oder der Vervielfältigung auf anderen Wegen und der Speicherung in Datenverarbeitungsanlagen, bleiben, auch bei nur auszugsweiser Verwertung, vorbehalten. Eine Vervielfältigung dieses Werkes oder von Teilen dieses Werkes ist auch im Einzelfall nur in den Grenzen der gesetzlichen Bestimmungen des Urheberrechtsgesetzes der Bundesrepublik Deutschland vom 9. September 1965 in der jeweils geltenden Fassung zulässig. Sie ist grundsätzlich vergütungspflichtig. Zuwiderhandlungen unterliegen den Strafbestimmungen des Urheberrechtsgesetzes.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Einbandabbildung: KüenkelLopka GmbH, Heidelberg

Printed on acid-free paper

Springer ist Teil der Fachverlagsgruppe Springer Science+Business Media (www.springer.com)

Vorwort

Was eigentlich immer noch zum Staunen ist, scheint heute im Alltag vielen schon ganz selbstverständlich: Der alte, die ganze Menschheitsentwicklung antreibende Traum von einer Mobilität über die Grenzen von Zeit und Raum hinweg hat sich in den letzten Jahrzehnten in einem Maße verwirklicht, wie nie zuvor in der Menschheitsgeschichte. Und dabei wurde kein einziges physikalisches Gesetz gebrochen. Der Mensch hat vielmehr gelernt, mit unerwartet vielen Dingen des Lebens in einer entmaterialisierten, virtuellen Form umzugehen. Entmaterialisiert in dem Sinne, dass anstelle mit den Dingen selbst lediglich mit ihren digitalen „Schatten“ umgegangen wird, also mit Beschreibungen, kodiert in Form von Nullen und Einsen, die über elektromagnetische Signale mit Lichtgeschwindigkeit transportiert und an jedem Computer bearbeitet werden können. Zwei technologische Entwicklungen machen das möglich: *Computer* bieten den Kosmos, in dem diese digitalen Schatten ihr Dasein entfalten, in dem sie neu geschöpft, bearbeitet, verknüpft und abgelegt werden können; das *Internet* bietet die Möglichkeit, diese digitalen Schatten fast mit Lichtgeschwindigkeit an jeden Ort der Welt zu transportieren, damit sie in einem Computer am anderen Ende der Welt ihre Wirkung entfalten können.

Tatsächlich zählen Computer und Internet zu den ganz wenigen technologischen Entwicklungen in der Geschichte der Menschheit, die das Leben und Handeln der Menschen wirklich grundlegend verändert haben. Nachdem die industrielle Revolution des 19. und 20. Jahrhunderts unsere physische Mobilität dramatisch steigern konnte – Autos, Flugzeuge, Raumschiffe erweiterten den körperlichen Aktionsradius des Menschen beträchtlich –, so erweitern Computer- und Internet-Technologien als Treiber der *digitalen Revolution* unsere gedankliche Mobilität in einem bisher unvorstellbaren Maße und befreien unseren geistigen Aktionsradius von (fast) jeglicher körperlicher Beschränkung. Während selbst modernste Fortbewegungsmittel wohl immer viele Stunden brauchen werden, um einen Menschen von einem Kontinent zum anderen zu bringen, kann er diese Entfernung mit Hilfe des Internets fast augenblicklich überwinden. Empfindungen, Gedanken und Anweisungen lassen sich unmittelbar übermitteln, sekundenschnell kann auf die Wünsche und Anforderungen weit Entfernter reagiert werden – und das anders als im Bereich der physischen Mobilität ohne nennenswerte Kosten.

Aufgrund der noch sehr jungen Geschichte – das Internet ist gerade einmal Vierzig, das WWW vor kurzem volljährig geworden – und da die rasante Entwicklung der Computer- und Netzwerk-Technologien ungebrochen anhält, lassen sich die durch die digitale Revolution ausgelösten Veränderungen in Gesellschaft, Wirtschaft und im privaten Bereich erst in allerersten Umrissen absehen. Um so interessanter ist es daher, hinter die Kulissen dieser Entwicklung zu schauen und die technischen Grundlagen zu verstehen, wie Internet und WWW eigentlich funktionieren. Genau dazu will das vorliegende Buch „Digitale Kommunikation“ zusammen mit den beiden nachfolgenden Bänden, „Internetworking“ und „Web-Technologien“, ein

verständiger, umfassender und vertrauenswürdiger, lehr- und detailreicher Führer sein.

Der vorliegende Band ist den Grundlagen der digitalen Kommunikation gewidmet und bietet einen ausführlichen Rückblick auf die Geschichte der Kommunikation und ihre technischen Hilfsmittel. Er behandelt die Grundlagen der Kommunikation in Rechnernetzen, stellt die Vielfalt der digitalen Medien, ihre Ausprägungen und Kodierung dar, und gibt einen Überblick zur Sicherheitsproblematik in der neuen digitalen Welt. Die mehrdimensionale Gliederung des Materials – allgemeinverständliche Beschreibungen werden durch zahlreiche ins technische Detail gehende Exkurse ergänzt, Glossare bieten kapitelbezogene, kommentierte Indizes, und Literaturhinweise laden zum Nachschlagen und Weiterlesen ein – soll dem geneigten Leser den Zugang zur Fülle des behandelten Stoffes soweit wie möglich erleichtern und ihm eine interessen- bzw. themenbezogene Auswahl ermöglichen.

Auf Basis dieses Buches werden dann in den beiden nachfolgenden Bänden „Internetworking“ und „Web-Technologien“ die Internet- und Web-Technologien umfassend und im Detail vorgestellt, also die aktuellen Rechnernetzwerktechnologien, die verschiedenen Schichten des Internets, die TCP/IP-Protokollsuite, das WWW, sowie die verschiedenen Web-Technologien, wie URL, HTTP, HTML, CSS, XML, Web-Programmierung, Suchmaschinen, Web2.0 und Semantic Web.

Wir haben uns große Mühe gegeben, um Sie, verehrte Leser, als interessierte Laien durch die Lektüre unseres Buches anzustecken mit der Faszination der neuen digitalen Welt, um Ihnen als fleißige und Anstrengungen nicht scheuende Studenten ein brauchbares und umfassendes Lehrbuch vorzulegen, und Ihnen als gestandene Profis ein zuverlässiges Nachschlagewerk an die Hand zu geben, mit dem Sie Ihre Spezialgebiete leicht und sicher in den Kontext des riesigen Gesamtkomplexes der digitalen Kommunikation einordnen können.

Dank zu sagen gilt es dem Springer-Verlag in Person von Hermann Engesser und Dorothea Glaunsinger für das Vertrauen in das Gelingen dieses Buchprojekts und die Unterstützung bei seiner Realisierung, und bei Euch, Ivana und Anja, für den Langmut und die Toleranz, mit der ihr uns habt während zahlloser Wochenenden und Ferientage in unsere Arbeitszimmer verschwinden lassen, und die uns auch dabei begleitende Liebe.

Potsdam, im Januar 2009

*Christoph Meinel
Harald Sack*

Inhaltsverzeichnis

1	Prolog	1
1.1	Digitale Güter	1
1.2	Digitale Kommunikation und ihre Grundlagen	8
1.3	Wegweiser durch die digitale Kommunikation	13
1.4	Glossar	15
2	Geschichtlicher Rückblick	19
2.1	Entwicklung der Schrift	19
	Exkurs 1: Die Entwicklung der Sprache	21
2.2	Erste Kommunikationsnetzwerke	28
2.3	Die Entwicklung des Buchdrucks	34
2.4	Entstehung des Zeitungswesen	41
2.5	Telekommunikationssysteme und Elektrizität	44
	2.5.1 Optische Telegrafie	44
	2.5.2 Elektrische Telegrafie	47
2.6	Der Vormarsch der Individual-Telekommunikation	50
	2.6.1 Telefon	50
	2.6.2 Vom Phonograph zum Grammophon	52
	2.6.3 Fotografie	54
2.7	Drahtlose Telekommunikation - Rundfunk und Fernsehen	57
	2.7.1 Funktelegrafie	57
	2.7.2 Rundfunk	59
	2.7.3 Film und Kino	61
	2.7.4 Fernsehen	63
	2.7.5 Analoge und digitale Aufzeichnungsverfahren	66
2.8	Der Computer als universeller persönlicher Kommunikationsmanager	68
2.9	Die untrennbare Geschichte von Internet und WWW	75
	2.9.1 Das ARPANET – wie alles begann...	75
	2.9.2 The Internet goes public	79
	2.9.3 Das WWW revolutioniert das Internet	81

2.9.4	Web 2.0 und Semantic Web – Die Zukunft des WWW	85
2.10	Glossar	88
3	Grundlagen der Kommunikation in Rechnernetzen	93
3.1	Grundbegriffe und -konzepte	93
3.1.1	Kommunikation und Datenübertragung	93
3.1.2	Klassifikationen von Kommunikationssystemen	98
3.2	Rechnernetze und Paketvermittlung	103
3.2.1	Klassische Punkt-zu-Punkt Verbindung	103
3.2.2	Leitungsvermittelte Netzwerke	105
3.2.3	Von der Leitungsvermittlung zur Paketvermittlung	106
3.2.4	Das Prinzip der Paketvermittlung	107
3.2.5	Vorteile der Paketvermittlung	109
3.2.6	Paketheader	111
3.2.7	Nachteile der Paketvermittlung	112
3.2.8	Verbindungslose und verbindungsorientierte Netzwerk- dienste	113
3.2.9	Dienstparadigmen von Rechnernetzen	114
3.2.10	Fehlererkennung und Fehlerkorrektur	117
	Exkurs 2: Fehlererkennende und fehlerkorrigierende Codes	119
3.3	Leistungskennziffern von Rechnernetzen	125
3.3.1	Benutzerbezogene Kenngrößen	126
3.3.2	Qualitative Leistungskriterien	126
3.3.3	Quality of Service	128
	Exkurs 3: Verzögerung in paketvermittelten Netzwerken	131
3.4	Kommunikationsprotokolle	134
3.4.1	Protokollfamilien	136
3.4.2	Schichtenmodell	136
	Exkurs 4: Das ISO/OSI-Schichtenmodell	142
3.4.3	Das Internet und das TCP/IP-Schichtenmodell	146
3.4.4	Protokollfunktionen	152
3.5	Glossar	155
4	Multimediale Daten und ihre Kodierung	161
4.1	Medienvielfalt und Multimedia - eine Formatfrage	161
4.2	Information und Kodierung	164
4.2.1	Information und Entropie	164
4.2.2	Redundanz – Mehrwert oder Verschwendung?	166
4.3	Text - Datenformate und Komprimierung	168
4.3.1	Textkodierung	168
	Exkurs 5: Der Unicode Standard	174
4.3.2	Textkomprimierung	177
	Exkurs 6: Einfache Verfahren der Datenkomprimierung	179
4.4	Grafik - Datenformate und Komprimierung	182
	Exkurs 7: Was ist Farbe? – Farbe und Farbsysteme	185

4.4.1	Varianten der Lauflängenkodierung für Grafikdaten	191
4.4.2	LZW-Verfahren	192
4.4.3	GIF-Format	193
	Exkurs 8: GIF – Dateiaufbau	195
4.4.4	PNG-Format	199
4.4.5	JPEG-Format	200
	Exkurs 9: JPEG – Komprimierung und JPEG – Dateiformat	203
4.5	Audio – Datenformate und Komprimierung	213
4.5.1	Analog-Digital-Umwandlung	216
4.5.2	Unkomprimierte Audio-Datenformate	222
4.5.3	Audiokomprimierung	224
4.5.4	MPEG Audiokodierung	230
	Exkurs 10: MPEG-1 Audiokodierung	232
	Exkurs 11: MP3 – Dateiaufbau	238
4.5.5	Weitere Audio-Komprimierungsverfahren	244
4.5.6	Streamingtechniken	247
4.6	Video und Animation - Datenformate und Komprimierung	248
4.6.1	Digitale Videokodierung	249
4.6.2	Komprimierung von Videosignalen	255
4.6.3	Bewegungskompensation und Bewegungsvorhersage	258
4.6.4	MPEG Komprimierung: Schlüsselprobleme	260
4.6.5	MPEG Komprimierung: Prinzipielles Vorgehen	262
4.6.6	MPEG-2 Standard	269
	Exkurs 12: MPEG – Datenformat	273
4.6.7	MPEG-4 Standard	280
4.6.8	MPEG-7 Standard	287
4.6.9	MPEG-21 Standard	293
	Exkurs 13: Andere Videodatenformate und -komprimierungs- verfahren	296
4.7	Glossar	299
5	Digitale Sicherheit	307
5.1	Grundlagen der Sicherheit in Rechnernetzen	307
5.1.1	Sicherheitsziele	309
5.1.2	Kryptografische Grundbegriffe	313
5.2	Vertraulichkeit und Verschlüsselung	317
5.2.1	Symmetrische Verschlüsselungsverfahren	317
	Exkurs 14: Einfache historische Verschlüsselungsverfahren	318
	Exkurs 15: Data Encryption Standard (DES) und Advanced Encryption Standard (AES)	323
5.2.2	Asymmetrische Verschlüsselungsverfahren	327
	Exkurs 16: Das RSA Public-Key-Verfahren	330
5.2.3	Authentifikation	332
5.3	Digitale Signaturen	336
5.3.1	Datenintegrität und Authentizität	338

5.3.2	Message Digest	340
	Exkurs 17: Kryptografische Hashfunktionen	342
5.4	Public Key Infrastrukturen und Zertifikate	347
5.4.1	Zertifizierungsstelle (CA)	348
5.4.2	Vertrauensmodelle	351
5.5	Glossar	353
6	Epilog	359
	Personenregister	369
	Abkürzungen und Akronyme	391
	Bildnachweise	397
	Literaturverzeichnis	399
	Sachverzeichnis	409