Informatik-Fachberichte 234

Herausgeber: W. Brauer
im Auftrag der Gesellschaft für Informatik (GI)

Andreas Pfitzmann

# Diensteintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz

Springer-Verlag
Berlin Heidelberg New York
London Paris Tokyo Hong Kong

**Autor**

Andreas Pfitzmann
Universität Karlsruhe
Institut für Rechnerentwurf und Fehlertoleranz
Postfach 6980, D-7500 Karlsruhe 1

CR Subject Classifications (1987): C.2, D.4.6, E.3, H.4.3, K.4.1

ISBN-13: 978-3-540-52327-7 e-ISBN-13: 978-3-642-75544-6
DOI: 10.1007/978-3-642-75544-6

CIP-Titelaufnahme der Deutschen Bibliothek.
Pfitzmann, Andreas:
Diensteintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz / Andreas Pfitzmann. - Berlin; Heidelberg; New York; London; Paris; Tokyo; Hong Kong: Springer, 1990
(Informatik-Fachberichte; 234)

NE: GT



2145/3140 - 543210 - Gedruckt auf säurefreiem Papier

# Vorwort

Menschen und Maschinen kommunizieren immer mehr über öffentliche *Vermittlungsnetze*. *Sensitive Daten* (z. B. personenbezogene Daten, Geschäftsgeheimnisse) können dabei sowohl aus den eigentlichen *Nutzdaten* als auch aus den *Vermittlungsdaten*, z. B. Ziel- und Herkunftsadresse, Datenumfang und Zeit, gewonnen werden.

Deshalb wird in dieser Arbeit untersucht, wie sensitive Daten vor illegalen und legalen Netzbenutzern, dem Betreiber des Netzes und den Herstellern der Vermittlungszentralen sowie ihren Mitarbeitern geschützt werden können. Manche Vermittlungsdaten, z. B. die genauen Netzadressen der Teilnehmer, müssen auch vor Kommunikationspartnern, etwa Datenbanken, geschützt werden, damit sie nicht als Personenkennzeichen verwendbar werden.

Bei der heute üblichen und von der Deutschen Bundespost auch für die Zukunft, nämlich für das **diensteintegrierende** Digitalnetz (ISDN), geplanten Netzstruktur erlauben auch juristische Datenschutzvorschriften und Verschlüsselung allein keinen ausreichenden und mit vernünftigem Aufwand **überprüfbaren** Datenschutz. Die Nutzdaten können zwar durch Ende-zu-Ende-Verschlüsselung in Digitalnetzen effizient, überprüfbar und umfassend geschützt werden. Bei der im Teilnehmeranschlußbereich üblichen vollvermittelten Sternstruktur der Kommunikationsnetze erlauben diese Maßnahmen jedoch keinen überprüfbaren Schutz der Vermittlungsdaten vor dem Betreiber des Netzes. Werden – wie vorgesehen – komplexe und zusätzlich frei speicherprogrammierbare Vermittlungszentralen verwendet, die für „Trojanische Pferde" anfällig sind, können vor ihren Herstellern, deren Mitarbeitern und damit grundsätzlich auch fremden Geheimdiensten die Vermittlungsdaten ebenfalls nicht überprüfbar geschützt werden. Derart strukturierte öffentliche Vermittlungsnetze – insbesondere also das geplante ISDN – gewähren ihrem Benutzer nicht das im Volkszählungsurteil des Bundesverfassungsgerichts vom Dezember 1983 formulierte „Recht auf informationelle Selbstbestimmung ..., grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen". Zusammen mit dem faktischen Benutzungszwang, der durch immer stärkere Nutzung und das Fernmeldemonopol verursacht wird, wirft dies die Frage auf, ob die Beibehaltung dieser Netzstruktur verfassungsrechtlich zulässig ist.

Nach dieser Problemanalyse werden zunächst die zur Abhilfe geeigneten bekannten Grundverfahren – sie machen **Datenschutz** weitgehend sogar **teilnehmerüberprüfbar** – zusammen mit einigen Überlegungen zu ihrer effizienten Realisierung dargestellt. In reiner Form sind sie beim in den nächsten zwei Jahrzehnten zu erwartenden Stand der Technik nur als Spezialnetze für geringe Teilnehmerzahlen oder Leistungsanforderungen zu vertretbaren, aber bezogen auf die Kommunikationsleistung hohen Kosten realisierbar. Um die bezüglich Teilnehmerzahl, Zuverlässigkeit und Verkehrslast hohen Anforderungen eines diensteintegrierenden Kommunikationsnetzes zu erfüllen und damit teilnehmerüberprüfbaren Datenschutz auch in offenen Kommunikationsnetzen – durch die Diensteintegration sogar preiswert – zur Verfügung stellen zu können, werden die Grundverfahren durch Implementierung verschieden geschützter Verkehrsklassen, hierarchische Unterteilung des Kommunikationsnetzes sowie mit Datenschutz verträgliche Fehlertoleranztechniken praktikabel gemacht. Anschließend wird gezeigt, wie diese praktikablen Grundverfahren zur (ausgehend von den heutigen Kommunikationsnetzen) evolutionären Gestaltung eines Datenschutz garantierenden offenen, zunächst schmalbandigen, später breitbandigen diensteintegrierenden Digitalnetzes verwendet werden können. Überlegungen zur Netzbetreiberschaft und Verantwortung für die Dienstqualität sowie

zur datenschutzgerechten Abrechnung der Netznutzung schließen die Betrachtung diensteintegrierender Kommunikationsnetze im engeren Sinne ab.

Um einen Ausblick auf die Nutzung solcher Kommunikationsnetze zu geben, skizziere ich, wie die wichtigsten Transaktionsprotokolle, nämlich solche für *Zahlungen*, *Warentransfer* (d. h. digitale Ware gegen Geld) und *Dokumente* (z. B. Nachweis einer Qualifikation), und *statistische Erhebungen* so gestaltet werden können, daß teilnehmerüberprüfbarer Datenschutz und Rechtssicherheit gewährleistet werden. Um die Anwendbarkeit der Verfahren für teilnehmerüberprüfbaren Datenschutz in diensteintegrierenden Kommunikationsnetzen auf andere Problemstellungen zu demonstrieren, gebe ich einen Ausblick auf eine datenschutzgerechte Gestaltung von *öffentlichem mobilem Funk* (z. B. Autotelefon, Verkehrsleitsysteme) und *Fernwirken* (TEMEX) sowie auf eine Lösung des *Einschränkungsproblems* in verteilten Systemen, d. h. die Frage, wie ein Programm, das ein „Trojanisches Pferd" enthält, daran gehindert werden kann, Information über verdeckte Kanäle weiterzugeben.

# Danksagung

Diese von der Fakultät für Informatik der Universität Karlsruhe (Technische Hochschule) genehmigte Dissertation entstand am Institut für Rechnerentwurf und Fehlertoleranz (früher: Institut für Informatik IV). Sie wurde der Fakultät am 20. Mai 1988 vom Autor zur Erlangung des akademischen Grades eines Doktors der Naturwissenschaften vorgelegt. Die mündliche Prüfung fand am 1. Februar 1989 statt.

Prof. Dr.-Ing. *Winfried Görke* übernahm das Referat, Prof. Dr. *Otto Spaniol* (RWTH Aachen) nach intensiven und sehr anregenden Gesprächen, der Lektüre der bis dahin geschriebenen Arbeiten und einem in Aachen gehaltenen Kolloquiumsvortrag das Korreferat. Als dritter Gutachter wurde Prof. Dr.-Ing. *Paul J. Kühn* (Univ. Stuttgart) bestimmt. Für die viele investierte Zeit danke ich ihnen sehr.

Den Anstoß zu dieser Arbeit verdanke ich Dipl.-Ing. *Peter Mahnkopf*, der am 31. Januar 1983 im Informatik-Kolloquium der Karlsruher Fakultät voller Begeisterung über „Neue bildschirmorientierte Telekommunikationsformen – eine Darstellung der neuen Medien" vortrug und auf meine Frage, ob er jemals über die durch das von ihm angepriesene BIGFON-Konzept (Vermittlung von allen Diensten, auch von Fernsehen) verursachten Datenschutz-Probleme und deren technische Lösung nachgedacht habe, klar antwortete: „Nein, und ich kenne auch niemand, der bisher darüber nachgedacht hat." Dies und die durch die damals bevorstehende Volkszählung verursachte, sehr lebhafte Diskussion über Datenschutz brachten mich dazu, mich nicht nur um Fehlertoleranz, sondern nebenbei auch etwas um Datenschutz zu kümmern. Darin bestärkt wurde ich dadurch, daß Dr. *Ruth Leuze* im Sommersemester 1983 in Karlsruhe eine vielbesuchte und eindrucksvolle Vorlesung über (juristischen) „Datenschutz" hielt. Dankenswerterweise verschwieg sie nicht, wie wenig sie und ihre Mitarbeiter von technischem Datenschutz verstünden und wie dringend erforderlich originäre Lösungen in diesem Bereich seien.

Ich danke Prof. Dr.-Ing. *Winfried Görke* für die mir gewährte Freiheit, in seiner bisher ausschließlich mit Zuverlässigkeit elektronischer Geräte, Fehlerdiagnose und Fehlertoleranz beschäftigten Arbeitsgruppe mich zunächst „nebenbei", und wie sich durch das lebhafte Echo nach und nach ergab, später „hauptsächlich" mit Technischem Datenschutz zu beschäftigen. Es war sehr angenehm, mit ihm und meinen Kollegen, insbesondere Dr. *Klaus Echtle*, über ein für uns alle neues Gebiet zu diskutieren und gemeinsam manches zu lernen.

Für meine Themenentscheidung fundierende Gespräche und menschliche Begleitung danke ich Dr. *Klaus Dittrich*, Dr. *Hermann Härtig* und Prof. Dr.-Ing. *Detlef Schmid*.

Zahlreiche Studenten haben durch fruchtbare Zusammenarbeit diese Arbeit gefördert: *Gabriele Bürle* durch Arbeiten über vergleichende Leistungsbewertung zwischen Ringnetzen mit verschiedenen Zugriffsverfahren und Sternnetzen, *Michael Waidner* durch eine grundlegende Arbeit über die Anonymitätserhaltung von Ringzugriffsverfahren sowie durch eine erste wichtige Systematisierung der Datenschutzmaßnahmen in Kommunikationsnetzen, *Gunter Höckel* durch eine mustergültige und weitgehend abschließende Arbeit über die Anonymitätserhaltung von Ringzugriffsverfahren, *Andreas Mann* durch Entwicklung und Bewertung von Datenschutz erhaltenden Fehlertoleranzmaßnahmen in Ringnetzen, *Holger Bürk* durch Programmieren der Formeln in Abschnitt 5.3.4, *Axel Burandt* durch Erfinden eines originellen Codes, *Eckhard Marchel* durch eine sehr sorgfältige Leistungsbewertung von überlagerndem Empfangen bei Mehrfachzugriffsverfahren mittels Kollisionsauflösung, *Arnold Niedermaier* durch die Bewertung von Zuverlässigkeit und Senderanonymität einer fehlertoleranten Kommunikationsstruktur für das DC-Netz, *Manfred Böttger* durch sorgfältige Untersuchungen zur Sicherheit von asymmetrischen Kryptosystemen und MIX-Implementierungen gegen aktive Angriffe und *Ralf Aßmann* durch die bei weitem effizienteste Implementierung von verallgemeinertem DES sowie das zuverlässige Realisieren, Integrieren und Pflegen von Programmen zur komfortableren Textbearbeitung und Literaturstellenverwaltung. *Manfred Böttger* und *Dirk Fox* lasen Teile dieser Arbeit; ihre Kritik führte zu zahlreichen Verbesserungen der Darstellung.

Ganz besonders anregend waren Artikel von sowie Begegnungen und Telefonate mit Dr. *David Chaum*, der mich seit 1985 über seine Arbeiten auf dem laufenden hält und an unseren kritischen Anteil nimmt.

Prof. *Herbert Kubicek* habe ich für über den Datenschutz hinausgehende Diskussionen über ISDN zu danken, *Michael Kühn* für beharrliches Fragen, was im Datenschutzkontext denn mit den Breitbandkabelverteilnetzen anzufangen sei.

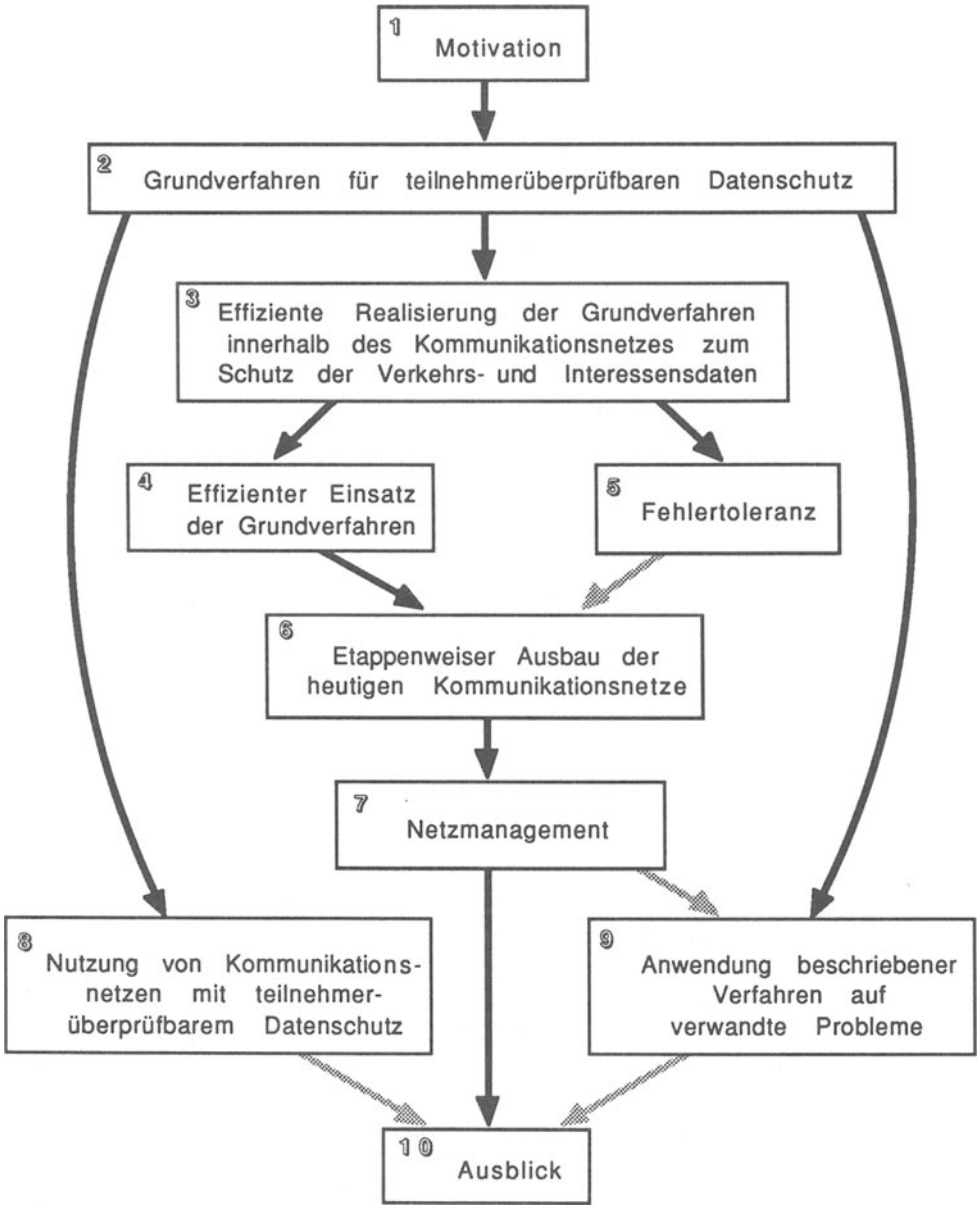
Ganz besonders danke ich meinen schärfsten, beharrlichsten, aber auch konstruktivsten Kritikern: Zuallererst meiner Frau *Birgit Pfitzmann*, dann dem Kollegen, mit dem ich die letzten Jahre am engsten zusammengearbeitet habe, Dipl.-Inform. *Michael Waidner*.

# Hinweise für den Leser

Literaturangaben mit Jahreszahl 89 wurden kurz vor Drucklegung und nur mit kurzem Hinweis auf ihren Inhalt nachträglich eingefügt. Entsprechendes gilt für alle Referenzen in Kapitel 8, das nur einen skizzenhaften Ausblick auf die Nutzung von Kommunikationsnetzen mit teilnehmerüberprüfbarem Datenschutz gibt. Alle anderen Referenzen stehen nach Sachverhalten, die für das Verständnis dieser Arbeit ausreichend ausführlich dargestellt sind. Dies gilt insbesondere für Arbeiten, deren Autor oder Koautor ich bin.

Diese Arbeit verdeutlicht einige der im fachlich sehr weit gespannten Bereich „Kommunikationsnetze" vorhandenen technischen Gefahren und weist Möglichkeiten zu ihrer Abwendung mit den Mitteln der „Telematik" (Telekommunikation und Informatik) nach. Sie bedient sich der in der Informatik üblichen Betrachtungsebenen und beschränkt sich auf sie. Das Erarbeiten und Darstellen von Lösungen setzt voraus, daß die zu lösenden Probleme klar und prägnant formuliert werden. Damit dies nicht mißverstanden wird: Wenn ich hervorhebe, daß jemand etwas tun *kann*, will ich damit nicht unterstellen, daß er es getan *hat* oder tun *wird*.

Das folgende Diagramm stellt die inhaltliche Abhängigkeit der Kapitel dar. Ein schwarzer bzw. grauer Pfeil von Kapitel $x$ zu Kapitel $y$ bedeutet, daß das Verständnis von $y$ das Verständnis von $x$ voraussetzt bzw. durch es erleichtert wird.



# Inhaltsverzeichnis