Fassung vom 29.10.90, erscheint in Datenschutz und Datensicherung 14/12 (1990)

Entwicklungslinien der Informationstechnik und Informatik und ihre Auswirkungen auf rechtliche Beherrschung*

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

Zusammenfassung

Ich möchte den Leser anregen, sich eine eigene Meinung zu bilden, inwieweit und wie informationstechnische Systeme der Zukunft rechtlich beherrscht werden können. Hierzu beschreibe ich den heutigen Entwicklungsstand der Informationstechnik und Informatik. Aus ihm und der Entwicklung der letzten drei Jahrzehnte lassen sich Trends der technischen Entwicklung erkennen, die ich hervorhebe. Wo angebracht, streue ich Bemerkungen über Auswirkungen auf die rechtliche Beherrschung, insbesondere den Datenschutz, ein.

Gliederung

Einleitungsfrage 2
1 Informationstechnik 2
1.1 Massenspeicher 2
1.1.1 Fest eingebautes Speichermedium 3
1.1.2 Wechselbares Speichermedium 3
1.1.3 Beispiel: Volkszählung 1987 3
1.1.4 Trend der technischen Entwicklung und Auswirkungen 4
1.2 Rechner 4
1.2.1 Trend und Stand der technischen Entwicklung 4
1.2.2 Auswirkungen 5
1.3 Kommunikationsnetze 5
1.3.1 Übertragung 6
1.3.2 Vermittlung 6
1.3.3 Auswirkungen 6
1.4 Datenerfassungs-Peripherie 7
1.5 Gegen ihre Benutzer sichere Geräte 8
2 Informatik 8
2.1 Programmierwerkzeuge: Transformation 8
2.1.1 Hilfe zur Realisierung 8
2.1.2 Hilfe für Angriffe 8
2.2 Systemtypen und Korrektheit 10
2.2.1 Präzis definierte Systeme: Verifikation 10
2.2.2 Vage definierte Systeme: Validierung 11
2.2.3 Sozio-technische Systeme: Hoffnung 11
2.3 Kompatibilität 11
2.4 Erweiterte Einsatzbereiche 11
3 Informationstechnik und Informatik fördern sich gegenseitig 12
Versuch einer Ausblicksantwort 12
Ein Dankeschön 13
Literatur 13
Stichwörter 15

---

* Schriftliche Fassung des den Teilnehmern am GRVI / GDD / DVD / DGIR / GI-Diskursprojekt „Rechtliche Beherrschung der Informationstechnik“, insbesondere den Nicht-Informatikern, am 23.4.1990 in Hamburg gehaltenen Vortrags

Einleitungsfrage

Um den Leser für Wachstumsvorgänge zu sensibilisieren, möge er für sich folgendes bekannte Problem lösen, auf das ich am Ende zurückkommen werde:

Eine Seerose verdoppele jedes Jahr die Fläche ihrer Blätter. Sie wird in einen See gesetzt. Nach 30 Jahren sei der See vollständig mit Seerosenblättern bedeckt. Nach wie vielen Jahren ist der See zur Hälfte bedeckt?

1 Informationstechnik

Aus dem Bereich Informationstechnik habe ich die fünf Gebiete Massenspeicher, Rechner, Kommunikationsnetze, Datenerfassungs-Peripherie und gegen ihre Benutzer sichere Geräte ausgewählt, die ich der Reihe nach abhandle. Diese fünf Gebiete scheinen mir für Fragen der rechtlichen Beherrschung, insbesondere Datenschutz und Rechtssicherheit, besonders wichtig zu sein.

Bei Datenschutz und Rechtssicherheit handelt es sich um durch Informationstechnik üblicherweise subtil verletzbare und deshalb schwierig zu schützende Rechtsgüter. Verletzungen anderer Rechtsgüter, etwa „körperliche Unversehrtheit“, dürften wohl eher offensichtlich sein. (Man denke etwa an autonome Roboter, die Menschen umrennen oder -fahren.) Bezüglich dieser hier ausgeklammerten Aspekte, insbesondere solche der Verletzlichkeit der „Informationsgesellschaft“, sei auf [RWHP_89] verwiesen.

1.1 Massenspeicher

Unter Massenspeichern versteht man diejenigen Speicher, die zur längerfristigen und preiswerten Aufbewahrung größerer Datenmengen geeignet sind. Hierbei reicht „längerfristig“ von einigen Sekunden bis zu vielen Jahrzehnten.

Bei Massenspeichern unterscheidet man, ob das eigentliche Speichermedium fest in das Schreib-/Lesegerät eingebaut ist oder ein Wechsel durch den Benutzer möglich und vorgesehen ist. Letzteres ermöglicht die Verwendung vieler „billiger“ Speichermedien mittels eines „teuren“ Schreib-/Lesegerätes und etwas physischer Arbeit, die ein Mensch oder ein Roboter zu verrichten hat.

Bild 1 gibt einen Überblick über die verfügbaren Massenspeicher, die in den folgenden Unterabschnitten ausführlicher behandelt werden.

		magnetische Festplatte	*Diskette*	*optische Platte*	*Streamer*
Kapazität		600 MByte	1,4 MByte	600 MByte	2300 MByte
Zugriffszeit		0,02 s	0,1 s	0,08 s	20 s
Abmessungen	*Gerät*	Schuhkarton	Zigarrenkiste	Schuhkarton	Schuhkarton
	Speichermedium	(fest eingebaut)	90•94•3 mm	CD	Video-8
Preis	*Gerät*	6000 DM	200 DM	9000 DM	8000 DM
	Speichermedium	(fest eingebaut)	4 DM	900 DM	50 DM

Bild 1: 1990 verfügbare kleine Massenspeicher

1.1.1 Fest eingebautes Speichermedium

Als Massenspeicher mit fest eingebautem Speichermedium werden heutzutage fast ausschließlich **magnetische Festplatten** (Winchester-Laufwerke, hard-disk drive) verwendet. Für etwa 6000 DM erhält man schuhkartongroße Geräte, die 600 MByte (in Zahlen ausgeschrieben: 600 000 000 Byte) speichern und auf beliebige Datenblöcke in etwa 20 ms (in Zahlen ausgeschrieben: in 0,02 Sekunden) zugreifen können. Als Transferrate zwischen Festplatte und Rechner sind mehr als 1 MByte/s üblich (in Zahlen ausgeschrieben: 1 000 000 Bytes pro Sekunde).

Für den Einbau in tragbare Geräte gibt es physisch sehr kleine Festplatten, z.B. eine 21-MByte-Festplatte mit nur 181 g Masse, 15•71•102 mm Größe und weniger als 1 W Energieverbrauch [Voel_90 Seite 29].

1.1.2 Wechselbares Speichermedium

Als Massenspeicher mit wechselbarem Speichermedium werden heutzutage vor allem Disketten (floppy disks), optische Platten (optical disks) und Streamer verwendet.

Üblich sind heute 3,5"-**Disketten** (Abmessungen: 90•94•3 mm), die etwa 4 DM kosten. Auf ihnen können mittels zigarrenkistengroßer und wenige hundert DM teurer Laufwerke 1,4 MByte gespeichert werden. Ist eine Diskette in ein Laufwerk eingelegt, kann auf beliebige ihrer Datenblöcke in Sekundenbruchteilen zugegriffen werden. Im Labor erprobt und für den Markt angekündigt sind unwesentlich teurere Disketten und Laufwerke gleicher Abmessung, die 20 mal so viel speichern und in etwa 50 ms zugreifen können [Mora_90, hr_90]. Am Markt erhältlich sind bereits heute 2"-Disketten (Abmessungen etwa: 55•61•3 mm), die mehr als 1 MByte speichern können, sich am Markt aber wohl nur durchsetzen werden, wenn sie ein größerer Rechnerhersteller verwendet [Voel_90 Seite 30].

Wiederbeschreibbare **optische Platten** sind seit etwa Frühjahr 1989 verfügbar. Für etwa 9000 DM erhält man schuhkartongroße Geräte, die 600 MByte (je optische Platte) speichern und beliebige Datenblöcke in etwa 80 ms zugreifen können (natürlich nur bei bereits eingelegter Platte). Die Abmessungen des Speichermediums entsprechen genau denen der im HiFi-Bereich weitverbreiteten CDs. Eine optische Platte kostet etwa 900 DM, wobei mit einem drastischen Sinken des Preises zu rechnen ist, sobald größere Stückzahlen hergestellt werden.

Seit Mitte 1989 sind für etwa 8000 DM schuhkartongroße **Streamer** erhältlich, die auf einer für etwa 50 DM erhältlichen, gewöhnlichen Video-8-Kassette (Abmessungen inkl. Schutzbox: 102•67•20 mm) 2,3 GByte (in Zahlen ausgeschrieben: 2 300 000 000 Byte) speichern [Glas_90]. Auch hier kann man auf beliebige Blöcke zugreifen, muß dazu aber im schlimmsten Fall das Band einmal umspulen. Inzwischen wurde die Kapazität bei gleichem Speichermedium auf 5 GByte gesteigert, wobei der Gerätepreis sich allerdings ebenfalls gut verdoppelt hat [eh_90].

1.1.3 Beispiel: Volkszählung 1987

Da große Zahlen schwer einschätzbar sind, ein Beispiel: Selbst unter sehr defensiven Annahmen (redundante Codierung) benötigt ein vollständiger Datensatz der Volkszählung 1987, d.h. das Maximum dessen, was pro Person in die Rechner gelangen soll, nur 226 bit (Gemeinde, Personenbogen und Wohnungsbogen). Im Mittel könnte dies sicher auf 180 bit gedrückt werden. Dies ergibt bei 61 Millionen Personen 1,72325 GByte maximal und im Mittel wohl eher 1,3725 GByte. Selbst unter defensiven Annahmen passen somit alle Volkszählungsdaten seit 1989 auf eine zigarettenschachtelgroße Magnetbandkassette, dazu noch die Daten von 17 Millionen DDR-Einwohnern und ein paar Minuten Video – letzteres etwa zur Täuschung bei Kontrollen, z.B. am Ausgang der Behörde oder Firma. Seit 1990 kann der Video-Anteil im Beispiel sogar deutlich überwiegen. Das Risiko, entdeckt zu werden, sinkt damit weiter.

1.1.4 Trend der technischen Entwicklung und Auswirkungen

Einerseits werden insbesondere die wechselbaren Speichermedien so *klein*, daß eine Abgangskontrolle (vgl. Abschnitt 1.1.3) bereits heute eigentlich eine Leibesvisitation erfordert und demnächst ohne lückenlose Personenüberwachung wohl nicht mehr möglich ist. Die Datenträger werden so klein sein, daß sie z.B. geschluckt oder in Schuhabsätzen verborgen werden können.

Andererseits wuchs die *Speicherkapazität* in den letzten Jahrzehnten exponentiell: Sie wurde trotz sinkender Abmessungen und Preise im Mittel alle anderthalb bis zwei Jahre verdoppelt.

Für das Sinken der *Preise* ist eine hohe Stückzahl wesentlich. Dies führt bei den wechselbaren Speichermedien zu zweierlei: Einerseits setzen sich nur wenige Formate durch. Andererseits werden von der „Datentechnik“ Formate mitverwendet, die sich in anderen Bereichen, z.B. Video oder Audio, durchgesetzt haben oder deren baldige Durchsetzung erwartet wird. Dies Mitverwenden führt dazu, daß aus dem Datenträger nicht mehr auf die Art des Inhalts geschlossen werden kann.

Alle drei Eigenschaften zusammen haben dazu geführt, daß heute *keinerlei technisch oder ökonomisch bedingte Zwänge oder auch nur nennenswerte Anreize zum Löschen irgendwelcher Daten* mehr bestehen. Dies gilt insbesondere auch für den privaten Bereich.

1.2 Rechner

1.2.1 Trend und Stand der technischen Entwicklung

Bei gleichen Abmessungen und Preisen wird die Arbeitsgeschwindigkeit der **Zentraleinheiten** (CPUs) etwa alle 2 Jahre verdoppelt und zusätzlich durch Erhöhung der internen und externen Verarbeitungsbreite ($4 \rightarrow 8 \rightarrow 16 \rightarrow 32 \rightarrow 64 \rightarrow 128$ bit) gesteigert.

Innerhalb der Zentraleinheiten gibt es im wesentlichen zwei Klassen *Halbleiter-Speicher* zur kurzfristigen Aufbewahrung von Daten: Beim **Arbeitsspeicher** ist das primäre Optimierungsziel hohe Speicherkapazität, beim zwischen Prozessor und Arbeitsspeicher angeordneten **Cache(speicher)** ist es geringe Zugriffszeit. Auch die Arbeitsspeicher- und Cachekapazität wird etwa alle 18 Monate verdoppelt, die Zugriffszeit etwa alle 3 Jahre halbiert.

Zusammen mit Verbesserungen der Rechnerorganisation ergibt dies bei gleichen Abmessungen und Kosten mehr als eine Verdopplung der Rechenleistung pro Jahr.

1990 ist etwa folgender Stand erreicht: Für etwa 10000 DM kann jeder z.B. einen schuhkartongroßen Arbeitsplatzrechner (workstation) kaufen, der 10 Millionen Befehle pro Sekunde ausführt, 8 MByte Hauptspeicher besitzt und beliebige 4-Byte-Speicherwörter in 80 ns (in Zahlen ausgeschrieben: 0,000 000 08 s) zugreifen kann. Dies bedeutet, daß ein viele Millionen DM teures Rechenzentrum des Jahres 1980 im Jahre 1990 für einige tausend DM auf dem Schreibtisch steht. Es gibt allerdings eine wichtige Ausnahme: Während beim historischen Rechenzentrum die meisten Rechner via Speicherschutz und Betriebssystem Anwendungsprozesse voreinander wenigstens etwas schützten, ist dies bei den heutigen Schreibtischrechnern größtenteils nicht der Fall, obwohl die Bedrohungen heute weitaus größer sind, vgl. Kapitel 2.1.

Der PC des Jahres 1980 für viele tausend DM ist inzwischen ein nur noch zigarrenkistengroßer Taschencomputer für einige hundert DM, z.B. ATARI Portfolio (IBM PC kompatibel, Abmessungen: 180•100•27 mm; Preis etwa 500 DM [Quel_90]).

Bild 2 gibt eine Gegenüberstellung.

	PC	*Taschen-computer*	*Verdopplungs Halbierungszeit* } *zeit*
Befehlsbreite	32 bit	8 bit	5 Jahre
Befehle / s	10 000 000	1 000 000	2 Jahre
Speicherkapazität	8 MByte	1/8 MByte	1,5 Jahre
Zugriffszeit	0,000 000 08 s	0,000 000 3 s	3 Jahre
Cachekapazität	1/32 MByte	–	1,5 Jahre
Zugriffszeit	0,000 000 025 s	–	3 Jahre
Abmessungen	Schuhkarton	180•100•27 mm	
Preis	10 000 DM	500 DM	

Bild 2: 1990 verfügbare kleine Rechner

1.2.2 Auswirkungen

Dank immer leistungsfähigerer „universeller“ Maschinen kann immer mehr durch Programmierung erledigt werden.

Alle vorhandenen Daten können universell (und im privaten Bereich: völlig *unkontrollierbar*) *ausgewertet* werden. Angesichts der oben beschriebenen Massenspeicher, die ein massenhaftes Erfassen, Austauschen und Entwenden (= Kopieren) von Daten sowie ihr Speichern auch im privaten Bereich sehr erleichtern, ist es sehr verwunderlich, daß zwar weit vor 1980 versucht wurde, die Datenverarbeitung in Rechenzentren juristisch zu regeln (u.a. BDSG), entsprechendes heute aber für den privaten Bereich nicht einmal ernsthaft erwogen wird. Ebensowenig wird jedoch heute die Nichtdurchsetzbarkeit juristischer Maßnahmen als Defizit öffentlich zugegeben. Das Dilemma ist klar: Zur Durchsetzung der Regelung müßte entweder der Verkauf von PCs an private Personen verboten werden (aus Durchsetzbarkeitsgründen vermutlich auch die Produktion und Einfuhr von PCs) oder die Datenverarbeitung müßte in jeder Wohnung überwacht werden. Glücklicherweise gibt es für viele Anwendungen einen dritten Ausweg: Personenbezogene Daten können ohne Einschränkung der Nutzfunktionen und Rechtssicherheit so gut wie vollständig vermieden werden, vgl. die nächsten Zeilen.

Neben den genannten Problemen schaffen immer leistungsfähigere „universelle“ Maschinen aber auch qualitativ neue Möglichkeiten. *Jeder kann seine Rechte selbst sichern und wahrnehmen*: Verschlüsselung und digitale Signaturen können in Software realisiert werden [PfAß_90, PWP_90, BoRu_89], ebenfalls umrechenbare Dokumente [Chau_87, PWP_90]. Dadurch wird u.a. *Rechtssicherheit trotz Anonymität* (und damit ohne Sammelmöglichkeit personenbezogener Daten) möglich, was vielen paradox erscheint. Beispielsweise können digitale Zahlungssysteme effizient so gestaltet werden, daß selbst alle Banken zusammen nicht wissen, wer an wen welche Zahlung geleistet hat. Trotzdem können einzelne Bankkunden bei Bedarf nachweisen, daß sie und ggf. auch an wen sie gezahlt haben. Ebenso ist sichergestellt, daß auch alle Bankkunden zusammen die Geldmenge im digitalen Zahlungssystem nicht vermehren können [Chau_89, PWP_90]. Es gibt also keinen Grund, Zahlungssysteme so zu gestalten wie von den Banken geplant.

1.3 Kommunikationsnetze

Kommunikationsnetze unterscheiden sich darin, wie und wieviel Information sie übertragen können und wie sie Information vom Sender zum Empfänger vermitteln.

1.3.1 Übertragung

Die Übertragung findet entweder leitungsgebunden oder nicht leitungsgebunden statt. Nur letzteres ermöglicht ortsbewegliche Endgeräte. Unter anderem weil bei **digitaler Übertragung** (im Gegensatz zu analoger) ein Qualitätsverlust vollständig vermieden werden kann, werden seit einigen Jahren zunehmend digitale Übertragungssysteme eingesetzt.

Als Übertragungsleitungen dienen üblicherweise

- verdrillte Kupferkabel (twisted pair), z.B. „normale“ Telefonkabel, bei ISDN für die Übertragung von 144 kbit/s (= 144 000 bit pro Sekunde) genutzt,
- Koaxialkabel, z.B. bei Kabelfernsehen für die analoge Übertragung von etwa 30 Fernsehkanälen genutzt, bei dem lokalen Netz (LAN) Ethernet für die Übertragung von nur 10 Mbit/s, in Weitverkehrsnetzen für bis zu 800 Mbit/s,
- Glasfasern, über die fast beliebig viel übertragen werden kann. Die nutzbare Bandbreite wird heutzutage durch die Sende- und Empfangselektronik auf etwa 8000 Mbit/s begrenzt und bei gleichen Kosten etwa alle zwei Jahre verdoppelt.

Nicht leitungsgebundene Übertragung findet üblicherweise als

- (Erd-) Funk,
- Satellitenfunk

statt. Da bei Funk in jedem durch die Senderstärke und die frequenzabhängigen Ausbreitungseigenschaften definierten lokalen Bereich das Frequenzspektrum nur einmal zur Verfügung steht, ist die Gesamtbandbreite bei nicht leitungsgebundener Übertragung im Gegensatz zu leitungsgebundener stark beschränkt.

1.3.2 Vermittlung

Um die vorhandenen Leitungen möglichst gut zu nutzen, insbesondere das Verlegen neuer Leitungen zu vermeiden, planen die Postverwaltungen, immer mehr Dienste zu **vermitteln** [ScS1_84, ScSc_84, Kade_88]. Hierbei fallen prinzipiell eine Menge personenbezogener Daten an. Zudem wird die Vermittlung zunehmend **von frei speicherprogrammierbaren Rechnern** vorgenommen, so daß niemand mehr prüfen kann, welche Daten, z.B. durch ein universelles transitives Trojanisches Pferd (vgl. Kap. 2.1.2), an wen weitergegeben werden.

Entsprechendes gilt für Zellularfunk. Hier besteht nicht nur wie in jedem Funknetz das Problem, daß Sender gepeilt werden können, sondern die Teilnehmer werden bei Verlassen kleiner lokaler Bereiche im nächsten an- und dann im vorherigen abgemeldet. Der Durchmesser dieser sogenannten (Funk-)Zellen liegt zwischen einigen hundert Meter in Ballungsgebieten und vielen Kilometern im ländlichen Raum [Stee_89]. Das An- und Abmelden geschieht selbst dann, wenn kein Dienst in Anspruch genommen wird und deshalb ansonsten eine Peilung unmöglich wäre. Komfortabler kann man umfassende Bewegungsbilder der Bevölkerung kaum erhalten.

1.3.3 Auswirkungen

Es werden immer mehr und immer sensitivere Daten über offene Kommunikationsnetze übertragen. Diese Daten können vor Veränderung und Verlust (etwa durch physische Angriffe auf Netzkomponenten) prinzipiell nicht geschützt werden. Dies macht die Gesellschaft zunehmend verletzlich, vgl. [RWHP_89]. Zur Zeit sind die Daten auch vor unbefugter Kenntnisnahme, *unerkannter* Veränderung und *unerkanntem* Verlust nicht geschützt, obwohl hiergegen Verfahren bekannt sind:

Im Gegensatz zu analoger ermöglicht digitale Übertragung ohne Verlust an Nutzleistung sichere Verschlüsselung [VoKe_83, PfPW_88, Pfit_89], deren Einsatz die Geheimdienste aber zu verhindern suchen [WaPP_87].

Es gibt alternative „Vermittlungskonzepte“, die auch die Verkehrsdaten (wer kommuniziert wann mit wem?) und Interessensdaten (wer interessiert sich wofür?) schützen. Dies geht für leitungs-

gebundene Netze unter Inanspruchnahme großer Übertragungsleistung perfekt [Chau_88, Pfit_89, Waid_90, WaPf_89] (hier hilft die Weiterentwicklung der Technik dem Datenschutz), und selbst mit den vorhandenen Leitungen und Übertragungssystemen des ISDN befriedigend gut [PfPW1_89]. Selbst bei Funknetzen sind wesentliche Verbesserungen möglich [Pfit_89].

Die in Abschnitt 1.2.2 erwähnten privaten Datensammlungen können über Kommunikationsnetze bequem ausgetauscht werden, so daß die Gefahr besteht, daß viele „Kleine Brüder“ zusammen einen verteilt realisierten „Großen Bruder“ bilden.

1.4 Datenerfassungs-Peripherie

Zunächst werde ich die offensichtliche, danach die subtile Datenerfassungs-Peripherie behandeln.

Dabei bedeutet *offensichtlich* lediglich, daß es sich um Peripherie-Geräte handelt, die zum primären Zweck der Datenerfassung geschaffen wurden. Offensichtlich bedeutet nicht: „immer leicht zu sehen“, denn diese Peripherie kann sehr klein und versteckt montiert sein.

- **Mikrophone** kombiniert mit **Sprecher**- und zunehmend auch **Spracherkennung**: Erkennung von dem System bekannten Sprechern gelingt gut, ebenso Einzelworterkennung bei begrenztem Wortschatz und dem System bekanntem Sprecher. Erkennung fließend gesprochener Sprache oder unbekannter Sprecher gelingt bei großen Wortschätzen trotz riesigen Aufwands nur mittelmäßig; Erkennung von Sprache, die ein unbekannter Sprecher fließend spricht, liegt wohl noch in der Zukunft [PeGr_90, UeRe_87].
- **optische Scanner**: durch sie und **Zeichenerkennung** werden alle Akten maschinenlesbar; Scanner, die DIN A 4 Vorlagen selbständig erfassen, kosten etwa 2000 DM pro Gerät und sind schuhkartongroß; billiger sind zigarettenschachtelgroße Handgeräte, mit denen man die Vorlage ggf. streifenweise überstreichen muß. Solche Handgeräte, die mit einer Auflösung von etwa 15 Punkten pro mm arbeiten, kosten etwa 400 DM.

  Optische Scanner haben nicht nur Auswirkungen im Bereich Datenschutz, sondern zusammen mit den in Abschnitt 1.1 beschriebenen Massenspeichern auch im Bereich *Urheberrecht*: In einigen Jahren wird optisches Abtasten und digitales Abspeichern von Büchern dem Fotokopieren wohl den Rang ablaufen, da das Weiterverbreiten digital abgespeicherter Bücher nahezu ohne Aufwand erfolgen kann.
- **Videoüberwachung**, die durch Menschen oder zunehmend maschinell ausgewertet wird. Bei genügender Anzahl könnten dank ihrer mittlerweile hinreichend hohen Auflösung von vermutlich weniger als 10 cm auch militärische **Aufklärungssatelliten** zur Überwachung der Bevölkerung verwendet werden [Adam_86].

Es ist unmöglich, alle *subtile* Datenerfassungs-Peripherie aufzuzählen. Besonders wichtig sind drei Gerätegruppen.

- **Kommunikationsnetze** (vgl. Abschnitt 1.3.2), insbesondere auch neue Dienste wie Fernwirken **(TEMEX)** [ScS1_84, Pete_87, Pfit_89].
- **Zahlungssysteme**: bei umfangreichem Einsatz der geplanten elektronischen Zahlungssysteme können auch Banken detaillierte Konsum-, Interessens- und Bewegungsprofile erstellen, aber auch hier gibt es Abhilfe, vgl. Abschnitt 1.2.2.
- **Verkehrsleitsysteme**, mit deren Hilfe Bewegungsprofile erstellt werden können [FO_87, Pfit_89].

Bei allen drei Gerätegruppen ist *Anonymität der Systembenutzer* (und damit Verhinderung der Sammelmöglichkeit personenbezogener Daten) die einzige bekannte Maßnahme, die die überprüfbare Realisierung von Datenschutz ermöglicht.

1.5 Gegen ihre Benutzer sichere Geräte

Die sichere Gestaltung von Informationstechnik würde viel weniger Nachdenken erfordern, gäbe es überprüfbar gegen ihre Benutzer sichere Geräte. Diese Eigenschaft wird beispielsweise Chipkarten von den meisten Autoren zugeschrieben, teilweise ohne jede Einschränkung [Beu1_87]. Letzteres ist mit Sicherheit unverantwortlich. Aber auch ersterem kann ich mich nicht anschließen, da es meines Wissens keine überzeugenden Begründungen gibt.

Es ist deshalb vorsichtig und nötig davon auszugehen, daß es keine Daten gibt, auf die nicht mindestens eine Person physischen Zugriff hat. Glücklicherweise kann für viele Anwendungen Sicherheit (Rechtssicherheit, Schutz personenbezogener Daten vor unbefugter Kenntnisnahme, usw.) trotzdem erreicht werden [Chau_87, PWP_90].

2 Informatik

Ich behandle der Reihe nach den Einfluß von Programmierwerkzeugen, Korrektheitsprobleme, die Bestrebungen nach Kompatibilität und die Erweiterung der Einsatzbereiche für Systeme der Informatik.

2.1 Programmierwerkzeuge: Transformation

2.1.1 Hilfe zur Realisierung

Den größten Fortschritt hat die Informatik in den letzten 25 Jahren durch die Entwicklung und weitgehend portable Implementierung höherer algorithmischer Universalsprachen sowie von Sprachen für spezielle Anwendungen gemacht. Genannt seien syntaxgesteuerte Editoren, Compiler, Interpreter, Konfigurierungs- und Versionenkontrollsysteme, kurzum Programmierumgebungen im weiteren Sinne.

Da sich der Programmierer durch diese Werkzeuge immer weniger um die Eigenheiten seines Entwicklungs- und Zielrechners kümmern muß, ist die Zahl derjenigen, die „programmieren“, und ihre Produktivität deutlich gewachsen. Es ist deshalb heutzutage noch naiver als vor 10 Jahren zu glauben, alle Programmierer würden sich loyal verhalten.

Außerdem werden Programmierwerkzeuge benutzt, um Programmierwerkzeuge zu generieren, usw. Die „Innereien“ generierter Werkzeuge schaut sich normalerweise niemand an, da dies einerseits nicht nötig sein sollte und andererseits den Menschen meist vor schier unlösbare Verständnisschwierigkeiten stellt: Umfang und insbesondere Komplexität der Werkzeuge sind in den letzten Jahrzehnten exponentiell gewachsen, aber die automatisierten Analysemethoden haben hiermit bei weitem nicht Schritt gehalten.

Im nächsten Abschnitt beschreibe ich, wieso gerade der größte Fortschritt der Informatik die Grundlage für die gefährlichste Angriffsform schafft.

2.1.2 Hilfe für Angriffe

Seit mehr als zwei Jahrtausenden ist die Angriffsform **Trojanisches Pferd** [Home_??] bekannt. Ein Trojanisches Pferd ist ein Systemteil, der unter Ausnutzung der ihm anvertrauten Daten und Rechte *mehr* als das von ihm Erwartete oder auch von ihm Erwartetes *nicht* oder *falsch* tut. Etwa könnte ein Editor die ihm eingegebenen Daten nicht nur in einer Datei seines Benutzers abspeichern, sondern noch an den Programmierer des Editors weitergeben. Hierzu benötigt das Trojanische Pferd einen **verborgenen Kanal** (covert channel) [Cove_90, Denn_82, Lamp_73, Pfit_89 Seite 7, 18]. Kann in unserem Beispiel der Editor als verborgenen Kanal keine zweite Datei benutzen (in vielen Rechnern könnte er das), so kann er etwa seinen Verbrauch an Betriebsmitteln (Speicherbelegung, CPU-Zeit) modulieren, was von anderen Prozessen wahrgenommen werden kann.

Leider sind keine brauchbaren Verfahren bekannt, alle Trojanischen Pferde zu finden oder deren Existenz im untersuchten Systemteil auszuschließen. Im wesentlichen ist man hier auf das „Hinschauen mit bloßem Auge“ angewiesen, was bei der heutigen Komplexität von Rechnern fast genausogut mit geschlossenen Augen geschehen kann.

Leider läßt sich die Bandbreite selbst mancher bekannter verborgener Kanäle ohne drastischen Mehraufwand nicht beliebig verkleinern. Die höchste Qualitätsanforderung der IT–Sicherheitskriterien läßt ohne Begrenzung der Anzahl der bekannten verborgenen Kanäle eine Bandbreite pro verborgenen Kanal von 1 bit/s zu [ZSI_89 Seite 96]. Auch dies möchte ich am Beispiel der Volkszählung 1987 (vgl. Abschnitt 1.1.3) veranschaulichen: Nehmen wir an, ein Angreifer kann sich von einem Trojanischen Pferd „nur“ 1 bit/s übertragen lassen. Dann erhält er innerhalb eines Jahres 31,536 Mbit, was 139 539 vollständigen Personendatensätzen entspricht.

Glücklicherweise kann durch den Einsatz von Diversität unter plausiblen Annahmen die Bandbreite auf exakt 0 bit/s verkleinert werden [Cles_88]. Allerdings ist der Aufwand hierfür beträchtlich.

Die sehr weite Definition Trojanischer Pferde läßt viele Spielarten zu, die teilweise mit eigenen martialischen Namen versehen sind, z.B. logische Bomben etc. Für eine grundsätzliche Betrachtung sind jedoch nur die beiden folgenden Eigenschaften universell und/oder transitiv wichtig.

Üblicherweise stellt man sich vor, daß der von einem Trojanischen Pferd anzurichtende Schaden (genauer: seine Schadensfunktion) beim *Entwurf* des Trojanischen Pferdes festgelegt wird. Damit wäre das Trojanische Pferd ein relativ unflexibler und ungerichteter Angreifer, bei Entdeckung wäre die Schädigungsabsicht seines Urhebers (sofern dieser identifizierbar ist) nachweisbar. Es ist aber auch möglich, zum Entwurfszeitpunkt nur einen Handlungsrahmen zu schaffen, der durch Eingaben während des *Betriebs* mit Leben gefüllt wird. Die Eingaben an den schädlichen Teil werden in zulässigen – und harmlos scheinenden – Eingaben an das ihn umfassende System verdeckt codiert. Die Codierung wird zweckmäßigerweise so redundant gewählt, daß die Wahrscheinlichkeit, daß ein Uneingeweihter durch seine Eingaben an das System auch Eingaben für den schädlichen Teil übermittelt, verschwindend gering ist. Im allgemeinsten Fall kann man während des Betriebs das Trojanische Pferd beliebig programmieren. Dorothy Denning hat diese Trojanischen Pferde **universell** (universal) genannt [Denn_85]. Die gezielte Verwendung universeller Trojanischer Pferde ist natürlich nur solchen Personen möglich, die während des Betriebes Zugriff auf das System haben. Dies ist insbesondere bei *offenen* Systemen aber fast jedem möglich. Mit Hilfe universeller Trojanischer Pferde sind sehr flexible und gerichtete Angriffe möglich. In unserem Volkszählungsbeispiel bräuchte der Benutzer des Trojanischen Pferdes nicht zu warten, bis ein ihn seit kurzem interessierender Datensatz nach vielen Jahren endlich übertragen wird, sondern er kann das universelle Trojanische Pferd diesen Datensatz sofort übertragen lassen.

Üblicherweise stellt man sich auch vor, daß ein Trojanisches Pferd vom Täter direkt dort untergebracht werden muß, wo es subversiv wirken soll. Auch diese Vorstellung ist falsch: Werden beim Entwurf Hilfsmittel verwendet (z.B. Compiler), so kann sowohl der Entwerfer als auch das Entwurfshilfsmittel ein Trojanisches Pferd im Entwurf unterbringen. Da mit Entwurfshilfsmitteln weitere Entwurfshilfsmittel entworfen werden, gilt dies rekursiv, so daß sich ein Trojanisches Pferd in der transitiven Hülle aller Entwürfe ausbreiten kann, an denen sein Gastgebersystem direkt oder indirekt beteiligt war [Thom_84, Pfit_89]. Ich spreche deshalb von **transitiven** Trojanischen Pferden.

Leider ist also bei den bisher verwendeten Entwurfs- und Dokumentationsrichtlinien (und erst recht in der Praxis) für alle in Abschnitt 2.2 beschriebenen Systemtypen (insbesondere auch die eigentlich am besten beherrschbaren) völlig unklärbar, wer welche Entscheidung getroffen hat und damit moralische Verantwortung trägt. Trotzdem wird in jedem Falle irgendjemand die juristische Verantwortung tragen müssen.

Anmerkung:

Die in aller Munde und Zeitschriften befindlichen **„Computer-Viren“** sind spezielle, durch ihren Ausbreitungsmechanismus definierte Trojanische Pferde: Hat ein ausgeführtes Programm, in dem

sich ein Computer-Virus befindet, Schreibzugriff auf ein beliebiges anderes Programm, so kann er dieses Programm so ändern, daß bei dessen Ausführung eine (optional veränderte) Kopie des Virus mit ausgeführt wird. Computer-Viren können sich in der transitiven Hülle der (meist üppig gewährten) Schreibzugriffsrechte ausbreiten.

Bereits vor Erfindung der Computer-Viren waren grundsätzliche *Schutzmechanismen* zur Verhinderung ihrer Ausbreitung bekannt [Denn_82 Seite 317f]: *Programme werden vom Generierer digital unterschrieben. Vor der Ausführung jedes Programms wird geprüft, daß es nicht unautorisiert verändert wurde. Zusätzlich wird jedem Programm bei seiner Ausführung nur das ermöglicht, was es können muß (Prinzip der geringstmöglichen Privilegierung, principle of least privilege).*

Da diese Schutzmechanismen die Bedrohung durch Computer-Viren genau auf die durch transitive Trojanische Pferde reduzieren [Pfit_89 Seite 7, 17], sind Computer-Viren kein zusätzliches Problem der Informatik. Leider wurden diese grundsätzlichen Schutzmechanismen jedoch aus Denkfaulheit und zu einem geringeren Teil auch Aufwands- und damit Kostengründen bisher nicht eingesetzt. Daraus resultiert ein schwerwiegendes gesellschaftliches Problem, da gegen Viren weitgehend ungeschützte Rechner weit verbreitet sind und auch in lebenswichtigen Gebieten eingesetzt werden.

2.2 Systemtypen und Korrektheit

Für den Grad an Vertrauenswürdigkeit (genauer: technischer Beherrschung), den man bei einem System der Informatik prinzipiell erreichen kann, ist wesentlich, wieweit man weiß, was man von ihm fordert. Die folgende Einteilung in drei Systemtypen ist nach abnehmender technischer Beherrschbarkeit geordnet. Präzis definierte Systeme besitzen eine formale äußere Spezifikation (top-level specification), vage definierte nicht. Bei sozio-technischen Systemen wird der Mensch als Teil des Systems (nicht nur als separater Benutzer) betrachtet. In größeren Systemen kommen als Subsysteme meist alle drei Systemtypen vor. Im folgenden werden auch diese Subsysteme einfach als Systeme bezeichnet.

Deutliche Fortschritte wurden im Bereich Spezifikation und Verifikation erzielt. Beides bezieht sich aber, meist stillschweigend, nur auf präzis definierte Systeme. Damit sind vage definierte Systeme und solche, die Menschen einschließen, sogenannte sozio-technische Systeme, ausgeschlossen. Trotzdem werden auch die beiden letzteren zunehmend in kritischen Bereichen eingesetzt.

2.2.1 Präzis definierte Systeme: Verifikation

Unter Verifikation wird üblicherweise der Nachweis der **totalen Korrektheit** eines Systems bzgl. seiner Spezifikation verstanden. Dabei heißt ein System total korrekt bzgl. seiner Spezifikation (kurz: es *erfüllt* seine Spezifikation), wenn es *alles tut, was die Spezifikation fordert*. Die Spezifikation bezieht sich aber heutzutage meist nur auf die geplante Nutzleistung eines Systems. Es ist daher möglich, daß ein System zwar total korrekt bzgl. seiner Spezifikation ist, aber *darüberhinaus Unerwünschtes* tut, beispielsweise Daten nicht nur (richtig) verarbeitet, sondern zusätzlich nach außen gibt, vgl. Abschnitt 2.1.2. Spezifikationen, die dies bereits ausschließen, sind schwierig: Erstens ist man nie sicher, alle verborgenen Kanäle gefunden zu haben. Zweitens muß man, um bekannte verborgene Kanäle zu schließen, das Verhalten eines Systems oft schon so genau festlegen wie sonst erst bei der Implementierung. Drittens erlauben viele heute übliche Spezifikationsmethoden, die für formale Korrektheitsbeweise geeignet sind, nicht das Betrachten realer Zeitbedingungen. Aber gerade reale Zeitbedingungen werden häufig für verborgene Kanäle benutzt.

Der Nachweis der totalen Korrektheit ist heute für kleine Systeme automatisch möglich, auch bei größeren kann er vom Rechner unterstützt werden und sollte während des Entwurfs erfolgen. In der Praxis begnügt man sich oft (oder muß sich auch begnügen) damit nachzuweisen, daß das System zumindest manche sicherheitskritische Dinge so wie spezifiziert tut, bzw. so wie spezifiziert nicht tut (software safety) [Leve_86].

2.2.2 Vage definierte Systeme: Validierung

Unter diesen Systemtyp fällt vieles, was allgemein mit Schlagworten wie künstliche Intelligenz (KI, artificial intelligence, AI), Expertensysteme, Sprecher- und Spracherkennung, Sprachverständnis, Mustererkennung etc. beschrieben wird.

Einerseits sind die Fortschritte in manchen Gebieten beachtlich, weswegen solche Systeme immer weitere Verbreitung finden.

Andererseits gibt es für diesen Systemtyp keinen formalen Korrektheitsbegriff, so daß Verantwortung noch schwerer zurechenbar ist.

2.2.3 Sozio-technische Systeme: Hoffnung

Ist der Mensch Teil des Systems, so kann man noch weniger Gewißheit über das Systemverhalten gewinnen. Oftmals werden auch die Menschen, die als Teil des Systems betrachtet werden, nicht die alleinigen Träger der Verantwortung sein, selbst wenn dies auf den ersten Blick manchen so erscheinen mag. Man denke nur an die Steuerung von Chemiewerken oder Kernkraftwerken, wo Rechner dem Betriebspersonal einen anderen Prozeßzustand darstellen könnten als den, der wirklich vorliegt. Selbst wenn sich im eigentlichen Steuerkanal, d.h. dem Systemteil, der die Stellglieder ansteuert, kein Rechner befindet, können so von Rechnern immense Schäden verursacht werden.

2.3 Kompatibilität

Ein Hauptziel der Informatik ist, technisch offene, d.h. miteinander kompatible Systeme zu schaffen. Dies wird einerseits durch „vorbeugende“ Normung (Schlagwort: Open Systems Interconnection = OSI), andererseits durch „heilende“ Emulation erreicht. Unter Emulation wird verstanden, daß sich ein System vom Typ X (etwa ein PC) wie ein System vom Typ Y (etwa ein Terminal) verhält. Dies kann zunehmend durch Programmierung erreicht werden, vgl. Abschnitt 1.2.2, was die Flexibilität und damit potentielle Kompatibilität drastisch erhöht. Auch im Bereich vorbeugender Normung wurden in den letzten Jahren deutliche Fortschritte erzielt.

Sosehr Kompatibilität innerhalb der Informatik ein Ziel und für viele Anwendungen auch wünschenswert ist, muß man sich doch klarmachen, daß damit eine natürliche Abschottungsgrenze zwischen informationstechnischen Systemen fällt. Ich halte es allerdings nicht für sinnvoll, diese Abschottungsgrenze beibehalten zu wollen (energisch gefordert unter anderen von Dr. Ruth Leuze [Leuz_85]), da sich ein Angreifer dennoch stets der Emulation bedienen kann. Es gibt sicherere Abschottung. Ich möchte nur an Verschlüsselung und umrechenbare Dokumente erinnern, vgl. Abschnitt 1.2.2.

2.4 Erweiterte Einsatzbereiche

Die Informatik erschließt der Informationstechnik und sich selbst ständig neue Einsatzbereiche. Hierdurch steigen auch die qualitativen Anforderungen, etwa an Verläßlichkeit, Sicherheit, Datenschutz, Sozialverträglichkeit etc. [RWHP_89]. Diesen Anforderungen begegnen Informationstechnik und Informatik bisher fast ausschließlich quantitativ: mehr Speicherkapazität, Rechenleistung, Bandbreite, Flexibilität. Dies *kann* erheblich zur Verbesserung der Situation beitragen, verbessert die Situation jedoch nicht automatisch, sondern verschlechtert sie bei gedankenloser Fortschreibung der bisherigen technischen Entwicklung und der bisherigen Anwendungen.

3 Informationstechnik und Informatik fördern sich gegenseitig

Bisher habe ich Informationstechnik und Informatik getrennt behandelt. Für die Einschätzung der bisherigen, mehr aber noch für die der zukünftigen Entwicklung ist wichtig, daß sich Informationstechnik und Informatik gegenseitig fördern: Entwurfswerkzeuge der Informatik werden für den Entwurf der Informationstechnik eingesetzt und sind dort mittlerweile unverzichtbar. Sie erlauben die Entwicklung immer leistungsfähigerer Informationstechnik. Andererseits wird die Informatik von der Informationstechnik dadurch gefördert, daß Informatik-Systeme immer leistungsfähigere informationstechnische Trägersysteme benutzen können.

Das Zusammenspiel von Informationstechnik und Informatik birgt die Möglichkeit, das bisherige – über mehr als 3 Jahrzehnte exponentielle – Wachstum noch eine ganze Weile fortzusetzen. Natürlich sind exponentielle Wachstumsprozesse auf einer endlichen und in ihrem Materieaufbau diskreten Erde nur zeitlich begrenzt möglich. Solange aber keine harten Grenzen oder Trendbrüche belegt sind, ist es ein Gebot der Vorsicht, eine Fortsetzung des bisherigen zu erwarten. Rechtliche Beherrschung der Informationstechnik und Informatik muß also mit einem exponentiellen Wachstumsprozeß fertig werden, dessen Ende (vorerst) nicht absehbar ist.

Versuch einer Ausblicksantwort

Die Antwort auf die Einleitungsfrage lautet 29 Jahre. Wenn die Seeanwohner warten, bis Baden und Schwimmen massiv behindert werden, haben sie also nur ein Jahr Zeit, angemessen zu reagieren.

Falls uns die Informatisierung unserer Gesellschaft und unseres Lebens jemals über den Kopf wachsen sollte, dürften wir dies also für eine überlegte Reaktion zu spät bemerken. Bei exponentiellen Wachstumsvorgängen ist Rückholbarkeit von Entwicklungen besonders schwierig. Ich fürchte, daß sich dessen nicht allzu viele Beteiligte bewußt sind. Sonst, hoffe ich, würde nicht vergleichsweise unbesorgt weitergearbeitet.

Dieses Über-den-Kopf-wachsen ist zumindest im Bereich „Schutz personenbezogener Daten vor unbefugter Kenntnisnahme und Verarbeitung etc.“ meiner Meinung nach gerade zu erleben, s.o. Dies würde selbst dann gelten, wenn keinerlei informationstechnischer Fortschritt mehr erzielt und nur der geschilderte heutige Stand der Technik noch vermarktet würde: Es bleiben hier nur die Alternativen eines großen Rückschritts (so gut wie keine Informationstechnik) oder eines in der Richtung genau geplanten (und in der Richtung ggf. genau vorgeschriebenen) Fortschritts.

Für die Beherrschung der Informationstechnik und Informatik durch Recht sehe ich persönlich größte Probleme:

Die informationstechnischen Systeme sind heutzutage nicht so beschaffen, daß sich irgendwer davon überzeugen könnte, was in ihnen wirklich geschieht. Recht kann nur dann informationstechnische Systeme wirklich beherrschen, wenn eine gänzlich andere Gestaltung und weit strengere Qualitätsmaßstäbe vorgeschrieben werden. Solche Vorschriften kollidieren mit kurzfristigen Interessen und wohl auch langfristig mit manchen Partikularinteressen, etwa beliebige informationstechnische Systeme entwickeln und vermarkten zu dürfen.

Informatik als Wissenschaft läßt sich wie jede Wissenschaft durch Recht wohl nicht regeln. Alle historischen Versuche, den Forscherdrang einzuschränken, sind gescheitert.

Neben einer Weiterentwicklung des Rechts halte ich als Ergänzung zwei Dinge für hilfreich:

Die Informatiker sollten als Berufsgruppe von sich aus akzeptieren, daß sie ihre Systeme so bauen müssen, daß vorzugsweise die Systeme in allen Phasen von Entwurf und Betrieb vollständig kontrollierbar sind. Ersatzweise kann versucht werden, die Entwerfer zu kontrollieren. Dies ist aber immer nur unvollständig möglich. Gegenüber Qualitätsforderungen wie Verläßlichkeit, Sicherheit,

Datenschutz, Sozialverträglichkeit haben Herstellerinteressen (Geschäftsgeheimnisse, z.B. „mein Betriebssystem ist sicher, aber ich gebe nur den Objektcode heraus“) zurückzutreten.

Wenn es schon schwierig, vielleicht unmöglich ist, die relevanten Dinge rechtzeitig rechtlich zu regeln (Fremdkontrolle), so sollten die Informatiker sich dringend einen ethischen Codex als persönliche Richtschnur und zur gegenseitigen Eigenkontrolle zulegen. Hier ist insbesondere die GI gefordert.

Ein Dankeschön

Für Kritik an und Anregungen zu diesem Text danke ich Gerrit Bleumer, Manfred Böttger, Prof. Winfried Görke, Sabine Lugert, Jörg Lukat, Kai Rannenberg und insbesondere Birgit Pfitzmann herzlich.

Literatur

Adam_86 John A. Adam: Counting the weapons; 1. Part of Special report "Verification: Peacekeeping by technical means"; IEEE spectrum 23/7 (1986) 46-56.

Beu1_87 Albrecht Beutelspacher: Die SICRYPT-Chipkarte - ein Sicherheitswerkzeug der Zukunft; Siemens-Zeitschrift 61/7 (1987) 6-7.

BoRu_89 Dieter Bong, Christoph Ruland: Optimized Software Implementations of the Modular Exponentiation on General Purpose Microprocessors; Computers & Security 8 (1989) 621-630.

Chau_87 David Chaum: Sicherheit ohne Identifizierung; Scheckkartencomputer, die den Großen Bruder der Vergangenheit angehören lassen; Informatik-Spektrum 10/5 (1987) 262-277; Datenschutz und Datensicherung DuD /1 (1988) 26-41.

Chau_88 David Chaum: The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability; Journal of Cryptology 1/1 (1988) 65-75.

Chau_89 David Chaum: Privacy Protected Payments – Unconditional Payer and/or Payee Untraceability; SMART CARD 2000: The Future of IC Cards, Proceedings of the IFIP WG 11.6 International Conference; Laxenburg (Austria), 19.-20. 10. 1987, North-Holland, Amsterdam 1989, 69-93.

Cles_88 Wolfgang Clesle: Schutz auch vor Herstellern und Betreibern von Informationssystemen; Diplomarbeit am Institut für Rechnerentwurf und Fehlertoleranz, Universität Karlsruhe, Juni 1988.

Cove_90 First Workshop on Covert Channel Analysis; CIPHER Newsletter of the TC on Security & Privacy, IEEE Computer Society (Special Issue, July 1990) 1-35.

Denn_82 Dorothy Denning: Cryptography and Data Security; Addison-Wesley Publishing Company, Reading 1982; Reprinted with corrections, January 1983.

Denn_85 Dorothy E. Denning: Commutative Filters for Reducing Inference Threats in Multilevel Database Systems; Proceedings of the 1985 Symposium on Security and Privacy, April 22-24, 1985, Oakland, California, IEEE Computer Society, 134-146.

eh_90 eh: Marktübersicht: Bandlaufwerke; Markt&Technik /27 (1990) 81-89.

FO_87 FO: Ein Fall für Prometheus; ADAC motorwelt /4 (1987) 50-53.

Glas_90 L. Brett Glass: Reeling in the Data; Byte 15/5 (1990) 299-306.

Home_?? Homer: Ilias; Diogenes Taschenbuch detebe 20779, übersetzt aus dem Altgriechischen von Heinrich Voß, herausgegeben von Peter Von der Mühll; Diogenes Verlag, Zürich 1980.

hr_90 hr: Durchbruch bei 20-MByte-Floppy; Markt&Technik /27 (1990) 11.

Kade_88 Firoz Kaderali: Entwicklungstrends und Entwicklungsaussichten für Telekommunikationsanlagen; Nachrichtentechnische Zeitschrift ntz 41/12 (1988) 690-693.

Lamp_73 Butler W. Lampson: A Note on the Confinement Problem; Communications of the ACM 16/10 (1973) 613-615.

Leuz_85 Ruth Leuze: Datenschutz für unsere Bürger; 6. Tätigkeitsbericht der Landesbeauftragten für den Datenschutz 1985; Herausgegeben von der Landesbeauftragten für den Datenschutz Dr. Ruth Leuze, Marienstraße 12, 7000 Stuttgart.

Leve_86 Nancy G. Leveson: Software Safety: Why, What, and How; ACM Computing Surveys 18/2 (1986) 125-163.

Mora_90 Chuck Moran: Die Wiedergeburt der Floppy: Floptical; mini Micro magazin /4 (1990) 106-108.

PeGr_90 Richard D. Peacocke, Daryl H. Graf: An Introduction to Speech and Speaker Recognition; Computer 23/8 (1990) 26-33.

Pete_87 Ulrich v. Petersdorff: "Weltneuheit" beim Berliner TEMEX-Versuch: Erprobung eines »intelligenten« Wasserzählers; Datenschutz und Datensicherung DuD /12 (1987) 575.

PfAß_90 Andreas Pfitzmann, Ralf Aßmann: Efficient Software Implementations of (Generalized) DES; SECURICOM 90, 8th Worldwide Congress on Computer and Communications Security and Protection, March 13-16, 1990, Paris, 139-158; Ausführlicher in Andreas Pfitzmann, Ralf Aßmann: More Efficient Software Implementations of (Generalized) DES; Interner Bericht 18/90, Fakultät für Informatik, Universität Karlsruhe 1990.

Pfit_89 Andreas Pfitzmann: Diensteintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz; Universität Karlsruhe, Fakultät für Informatik, Dissertation, IFB 234, Springer-Verlag, Heidelberg 1990.

PfPW_88 Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: Datenschutz garantierende offene Kommunikationsnetze; Informatik-Spektrum 11/3 (1988) 118-142.

PfPW1_89 Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: Telefon-MIXe: Schutz der Vermittlungsdaten für zwei 64-kbit/s-Duplexkanäle über den (2•64 + 16)-kbit/s-Teilnehmeranschluß; Datenschutz und Datensicherung DuD /12 (1989) 605-622.

PWP_90 Birgit Pfitzmann, Michael Waidner, Andreas Pfitzmann: Rechtssicherheit trotz Anonymität in offenen digitalen Systemen; Datenschutz und Datensicherung DuD 14/5-6 (1990) 243-253, 305-315.

Quel_90 Quelle: Katalog Herbst/Winter 90/91; Seite 1195.

RWHP_89 Alexander Roßnagel, Peter Wedde, Volker Hammer, Ulrich Pordesch: Die Verletzlichkeit der "Informationsgesellschaft"; Sozialverträgliche Technikgestaltung Band 5, Westdeutscher Verlag, Opladen 1989.

ScS1_84 Christian Schwarz-Schilling (ed.): ISDN - die Antwort der Deutschen Bundespost auf die Anforderungen der Telekommunikation von morgen; Herausgeber: Der Bundesminister für das Post- und Fernmeldewesen, Bonn, 1984.

ScSc_84 Christian Schwarz-Schilling (ed.): Konzept der Deutschen Bundespost zur Weiterentwicklung der Fernmeldeinfrastruktur; Herausgeber: Der Bundesminister für das Post- und Fernmeldewesen, Stab 202, Bonn, 1984.

Stee_89 Raymond Steele: The Cellular Environment of Lightweight Handheld Portables; IEEE Communications Magazine 27/7 (1989) 20-29.

Thom_84 Ken Thompson: Reflections on Trusting Trust; Communications of the ACM 27/8 (1984) 761-763.

UeRe_87 J. Uebler, H. E. Reinfelder: Ein Spracherkennungssystem für große Wortschätze; Siemens Forsch.- und Entwicklungs-Berichte, Springer- Verlag 16/2 (1987) 42-49.

Voel_90 John Voelcker: Peripherals; IEEE spectrum 27/2 (1990) 28-30.

VoKe_83 Victor L. Voydock, Stephen T. Kent: Security Mechanisms in High-Level Network Protocols; ACM Computing Surveys 15/2 (1983) 135-171.

Waid_90 Michael Waidner: Unconditional Sender and Recipient Untraceability in spite of Active Attacks; erscheint in Proceedings of Eurocrypt '89, LNCS, Springer-Verlag, Berlin 1990.

WaPf_89 Michael Waidner, Birgit Pfitzmann: Unconditional Sender and Recipient Untraceability in spite of Active Attacks – Some Remarks; Fakultät für Informatik, Universität Karlsruhe, Interner Bericht 5/89, März 1989.

WaPP_87 Michael Waidner, Birgit Pfitzmann, Andreas Pfitzmann: Über die Notwendigkeit genormter kryptographischer Verfahren; Datenschutz und Datensicherung DuD /6 (1987) 293-299.

ZSI_89 Zentralstelle für Sicherheit in der Informationstechnik (Hrsg.): IT–Sicherheitskriterien; Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (IT); 1. Fassung vom 11.1.1989; Köln, Bundesanzeiger 1989.

Stichwörter

Informationstechnik, Informatik, technische Entwicklung, rechtliche Beherrschung, Datenschutz, Rechtssicherheit, Massenspeicher, magnetische Festplatte, Diskette, optische Platte, Streamer, Volkszählung 1987, Rechner, Kommunikationsnetze, Übertragung, Vermittlung, Funknetze, Datenerfassungs-Peripherie, Sprechererkennung, Spracherkennung, optische Scanner, Zeichenerkennung, Videoüberwachung, Aufklärungssatelliten, Zahlungssysteme, Verkehrsleitsysteme, sichere Geräte, Spezifikation, Verifikation, totale Korrektheit, Validierung, Programmierwerkzeuge, universelles transitives Trojanisches Pferd, Viren, Kompatibilität, Wachstumsprozesse