Der Förderalismus stößt nicht nur wegen der dinglicher werdenden Entbürokratisierung an seine Grenzen. Die Bundesländer werden aus übergeordneten Gründen in einem stärker zusammenwachsenden Europa nicht darum herumkommen, sich übergreifend zu größeren verwaltungsorganisatorischen Einheiten zu verbinden.

Der Umfang der Aufgabenstellung wird wenigstens die nächsten zwei Legislaturperioden in Anspruch nehmen. Wer seriöse Ergebnisse will, muß den Datenschutz aus der kurzatmigen Tagespolitik heraushalten. Das ist unsere abschließende Forderung an die politisch Verantwortlichen.

Technischer Datenschutz in diensteintegrierenden Digitalnetzen – Warum und wie?

Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner

Stichwörter: Technischer Datenschutz, überprüfbarer Datenschutz, vorbeugender Datenschutz, Personenkennzeichen, (Un-)Beobachtbarkeit, Anonymität, Verhinderung der Datenerfassungsmöglichkeit, Individualüberwachung, Massenüberwachung, Fernmeldenetze, ISDN, IBFN, Trojanische Pferde, Verkehrsanalyse, Nutzdaten, Vermittlungsdaten, Inhaltsdaten, Interessensdaten, Verkehrsdaten, Verbindungs-Verschlüsselung, Ende-zu-Ende-Verschlüsselung, öffentliche Anschlüsse, zeitlich entkoppelte Verarbeitung, lokale Auswahl, Verteilung, implizite Adressierung, MIX-Netz, überlagerndes Senden, RING-Netz, Vermittlungs-/Verteilnetz

Zusammenfassung: Immer mehr kommunizieren Menschen und Maschinen über öffentliche Vermittlungsnetze. Personenbezogene Daten können dabei sowohl aus den eigentlichen Nutzdaten als auch aus den Vermittlungsdaten, z.B. Ziel- und Herkunftsadresse, Datenumfang und Zeit, gewonnen werden.

Wir untersuchen, wie sie vor illegalen und legalen Netzbenutzern, dem Betreiber des Netzes und seinen Angestellten und den Herstellern der Vermittlungszentralen 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 geplanten Netzstruktur diensteintegrierender Digitalnetze erlauben auch juristische Datenschutzvorschriften und Verschlüsselung keinen ausreichenden und mit vernünftigem Aufwand *überprüfbaren* Datenschutz.

Deshalb werden die zur Abhilfe geeigneten bekannten Grundverfahren zusammen mit einigen Überlegungen zu ihrer Implementierung dargestellt und gezeigt, wie diese Grundverfahren zur Gestaltung eines Datenschutz garantierenden breitbandigen diensteintegrierenden Digitalnetzes verwendet werden können.

Dies ist eine stark überarbeitete und erweiterte Fassung von [Pfit_85].

Gliederung

1 Problemanalyse

1.1 Heutige und geplante Kommunikationsnetze

Immer mehr benutzen wir öffentliche Kommunikationsnetze:

- Hörfunk, Fernsehen, Videotext z.B. sind Dienste, die (genauer: deren Informationen) heute vorwiegend über das Rundfunksendernetz der Deutschen Bundespost, mehr und mehr aber über das entstehende Breitbandkabelverteilnetz *verteilt* werden. Zweck des Breitbandkabelverteilnetzes ist die Verbesserung der Dienstqualität durch Erhöhung der verfügbaren Bandbreite: mehr empfangbare Fernsehprogramme heißt dann Kabelfernsehen, größeres Informationsangebot bei Videotext heißt dann Kabeltext.
- Fernsprechen, Bildschirmtext, elektronisches Postfach (TELEBOX) für elektronische Brief- und Sprachpost, Fernschreiben (TELEX, TELETEX), Fernkopieren (TELEFAX) und Fernwirken (TEMEX) sind Dienste, die heute über das analoge Telefonnetz bzw. das digitale Text- und Datennetz der Deutschen Bundespost, beginnend ab 1988 mit höherer Dienstqualität über das dann digitale „Telefonnetz" *vermittelt* werden.

  Das heutige analoge Telefonnetz und das dieselben Teilnehmeranschlußleitungen benutzende digitale „Telefonnetz", das ab 1988 in einigen Ortsnetzen und ab etwa 1993 in der ganzen Bundesrepublik entstehen wird, sind *schmalbandige* Netze, d.h. sie sind im Gegensatz zu *breitbandigen* Netzen nicht in der Lage, Bewegtbilder (z.B. Fernsehen) zu übertragen.

Zur Zeit benutzen wir also zwei grundsätzlich verschiedene Typen von Netzen:

- *Verteilnetze,* in denen alle Teilnehmerstationen vom Netz dasselbe erhalten und jeder Teilnehmer lokal auswählt, ob und, wenn ja, was er tatsächlich empfangen will, und
- *Vermittlungsnetze,* in denen jede Teilnehmerstation vom Netz individuell nur das erhält, was der Teilnehmer angefordert oder ein anderer Teilnehmer an ihn gesendet hat.

In den realisierten und geplanten öffentlichen Verteilnetzen findet Kommunikation nur in einer Richtung, vom Netz zum Teilnehmer, statt; in Vermittlungsnetzen wird in beiden Richtungen kommuniziert.

Da langfristig ein Netz für alle Dienste, ein sogenanntes *diensteintegrierendes* Netz, zumindest im Teilnehmeranschlußbereich preiswerter als mehrere verschiedene Netze ist, und da alle verteilten Dienste auch vermittelt werden können, strebt die Deutsche Bundespost an, beginnend ab 1992 alle Dienste in einem Netz zu vermitteln [Schö_84, ScSc_84, ScS1_84, Rose_85].

Damit auch breitbandige Dienste vermittelt zum Teilnehmer übertragen werden können, müssen neue Teilnehmeranschlußleitungen (Glasfaser) verlegt werden. Nach und nach wird dadurch ein Breitbandkabelverteilnetz überflüssig. Über ein breitbandiges diensteintegrierendes Vermittlungsnetz können nicht nur alle Dienste angeboten werden, die über ein Breitbandkabelverteilnetz und ein schmalbandiges Vermittlungsnetz zusammen angeboten werden können, sondern auch noch zusätzlich Dienste, die breitbandige Kommunikation zwischen Teilnehmern erfordern, z.B. Bildfernsprechen.

Da digitale Werte in modernen technischen Systemen nicht nur leichter übertragen, sondern auch leichter verarbeitet werden können, wird das diensteintegrierende Netz ein *digitales* Netz sein, abgekürzt ISDN (Integrated Services Digital Network). Ersetzt das breitbandige ISDN (abgekürzt Breitband-ISDN oder B-ISDN [Steg_85]) das Breitbandkabelverteilnetz, nennt es die Deutsche Bundespost Integriertes Breitbandfernmeldenetz (IBFN) [ScS1_84]. Pilotversuche zur Erprobung des IBFN sind unter der Abkürzung BIGFON (breitbandiges integriertes Glasfaser-Fernmeldeortsnetz) bekannt [Brau_82, Brau_83].

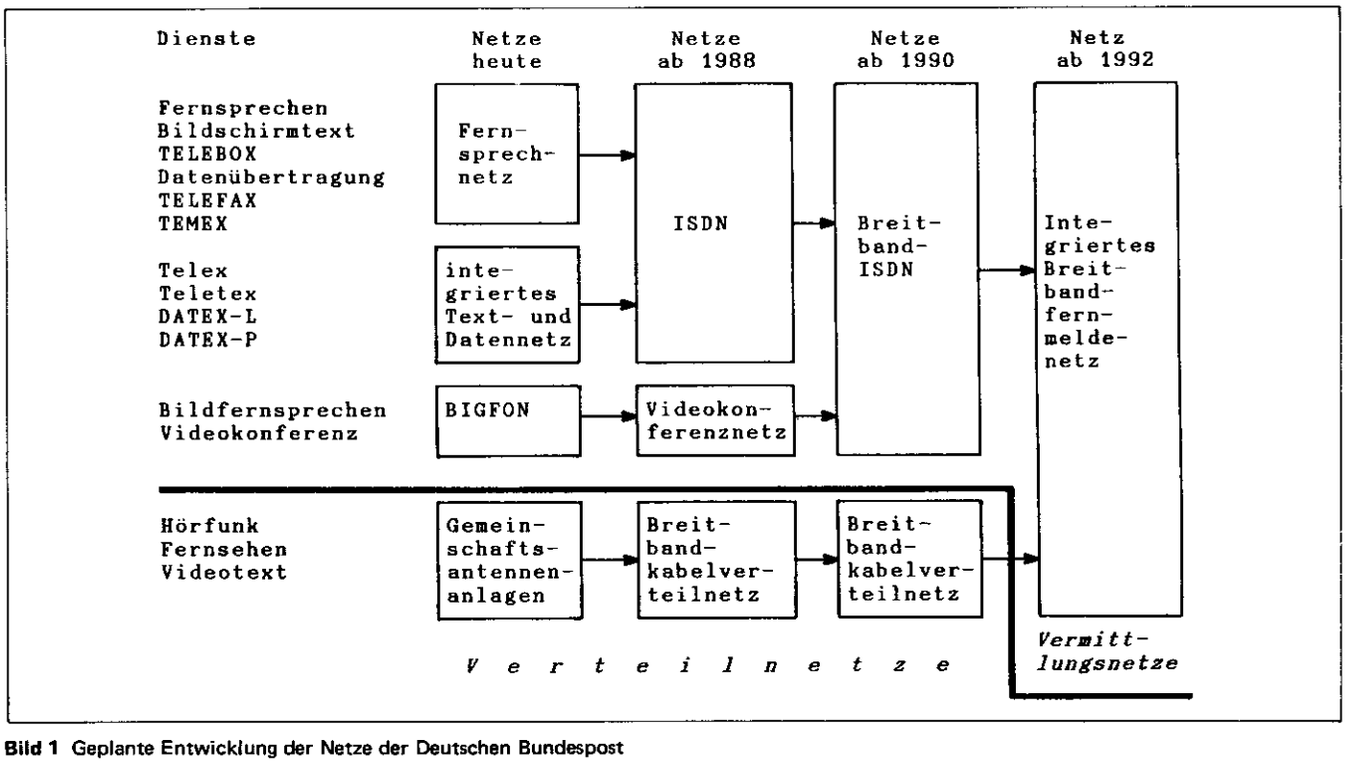


Bild 1 Geplante Entwicklung der Netze der Deutschen Bundespost

Die geschilderte Entwicklung ist in Bild 1 etwas detaillierter dargestellt.

Nicht dargestellt und im folgenden auch nicht explizit behandelt sind Funknetze, die als Anschlußnetz für ortsbewegte Teilnehmer, als Ersatznetz in Katastrophenfällen und als Garanten grenzüberschreitender Informationsfreiheit bleibende Bedeutung haben.

Nachdem nun die geplante Entwicklung dargestellt ist, können wir uns der Frage zuwenden: Welche Auswirkungen hat sie auf den Datenschutz?

1.2 Welche Beobachtungsmöglichkeiten bieten diese Netze?

In Bild 2 ist die Endsituation der geschilderten Entwicklung dargestellt: Alle Dienste, z.B. Fernsehen, Radio, Telefon, Bildschirmtext, werden über eine Glasfaser von der Vermittlungszentrale der Deutschen Bundespost zum Netzabschluß eines Teilnehmers vermittelt.

Die Glasfaser ist diesem Teilnehmer (bzw. seiner Familie o.ä.) eindeutig zugeordnet und über sie wird, da es sich um ein Vermittlungsnetz handelt, nur übertragen, was von ihm oder speziell für ihn bestimmt ist. Folglich stellt die physikalische Netzadresse eine Art Personenkennzeichen dar, unter dem Daten über diesen Teilnehmer gesammelt werden können.

Die dafür auf der Glasfaser und in den Vermittlungszentralen anfallenden Informationen bestehen technisch gesehen aus

- den transportierten *Nutzdaten* (Bild, Ton, Text) und
- den *Vermittlungsdaten* (Adressen und Absender der Kommunikationspartner, Datenumfang, Dienstart, Zeit).

Die daraus zu gewinnenden personenbezogenen Daten des Teilnehmers kann man inhaltlich gesehen einteilen in:

- *Inhaltsdaten,* d.h. Inhalte persönlicher Nachrichten, z.B. von Telefongesprächen oder elektronischer Post.
- *Interessensdaten,* d.h. Informationen über das Interesse des Teilnehmers an Nachrichten, deren Inhalt nicht persönlich ist. Hierzu zählen die Beobachtungen, welche Zeitungsartikel sich der Teilnehmer schicken läßt, welche Auskünfte er aus Datenbanken, z.B. Bildschirmtext, einholt und was genau er im Fernsehen sieht bzw. im Radio hört:

  Will der Teilnehmer z.B. das Fernsehprogramm wechseln, teilt er dies über seinen Fernseher und seinen Netzabschluß der Vermittlungszentrale mit. Diese überträgt dann statt des bisher gesehenen das angeforderte Fernsehprogramm über die Glasfaser.

  Diese Daten waren bisher in Netzen überhaupt nicht zu gewinnen.
- *Verkehrsdaten,* also z.B. wann der Teilnehmer wie lange mit wem kommuniziert. Diese können allein aus den Vermittlungsdaten gewonnen werden. Daß auch sie sensitiv sein können, zeigt:

  > *Fast täglich kommuniziert Teilnehmer A mit einem kommunistischen oder (der politischen Ausgewogenheit des Beispiels wegen) rechtsradikalen Zeitungsverlag...*

  Aber auch für einen Teilnehmer, der in dieser Hinsicht „nichts zu verbergen hat", ergeben die Verkehrsdaten bereits interessante Bausteine für ein Persönlichkeitsbild, z.B. Konsumgewohnheiten, Freundeskreis, Tagesablauf, Kontakte mit Polizei und Gesundheitsamt.

Eine Möglichkeit, an diese Daten zu gelangen, ist das Abhören der Glasfaser. Glasfasern sind zwar etwas abhörsicherer als elektrische Leitungen, aber auch ihr Abhören stellt kein schwieriges technisches Problem dar [Horg_85 Seite 36].

Noch einfacher und zudem für viele Teilnehmer auf einmal erhalten diejenigen die Daten, die sie sich direkt aus der Vermittlungszentrale beschaffen können.

Zunächst einmal *kann* die Post (und damit der Staat, genauer seine Geheimdienste) als Betreiber die Vermittlungsanlagen beliebig Daten speichern und auswerten lassen. Innerhalb weiter Grenzen *darf* sie dies auch, wie dem Bericht der Landesbeauftragten für den Datenschutz in Baden-Württemberg, Dr. Ruth Leuze, zu entnehmen ist [Leuz_83 Seite 114, vgl. auch Leuz_84 Seite 24, 25]:

> *„... der Betreiber von Bildschirmtext darf über jeden Teilnehmer speichern, wann, wie lange und wie oft er auf welche Weise den Bildschirmtext in Anspruch nahm."*

Weiter können Personen (z.B. Postangestellte, Wartungstechniker) oder Organisationen (z.B. Hersteller), die Zugang

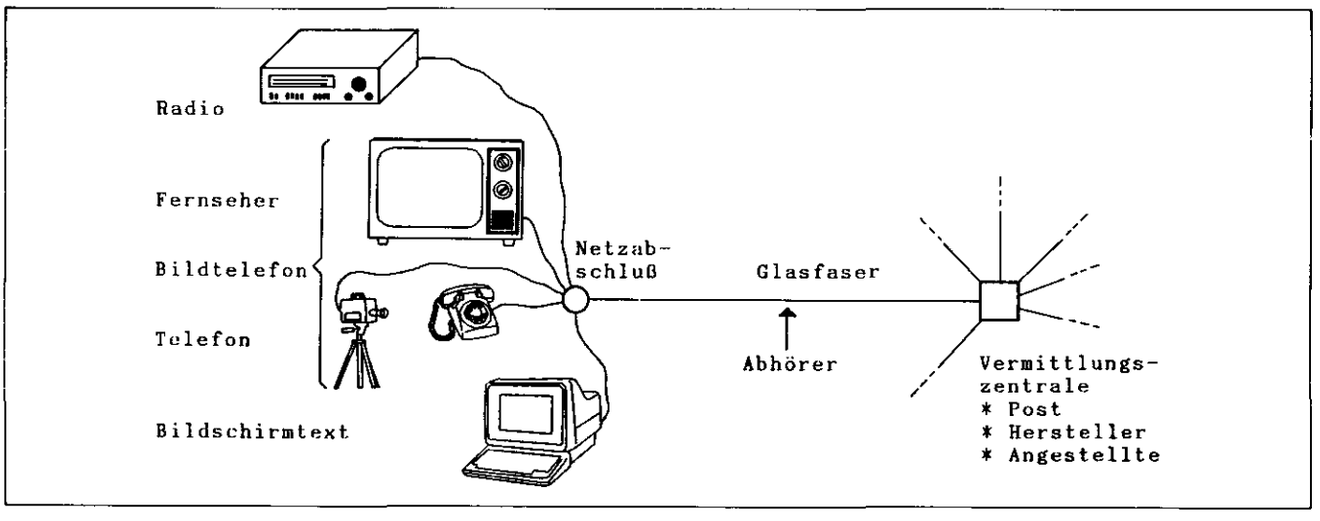


Bild 2 Beobachtbarkeit von Benutzern im sternförmigen ISDN

zur Vermittlungszentrale haben oder hatten, beliebige Informationen erhalten: Vermittlungszentralen sind heute komplexe Rechensysteme mit vielfältigen Möglichkeiten zum Installieren „Trojanischer Pferde" [Home_??], d.h. von Systemteilen, die Information auf verborgenen Kanälen einem nicht empfangsberechtigten Empfänger zukommen lassen [PoKl_78, Loep_85]. Das Finden „Trojanischer Pferde" ist äußerst schwierig [Thom_84] und, da eine diesbezügliche Systemüberprüfung auch nach jeder Wartungsmaßnahme nötig ist, sehr aufwendig.

Das Erschreckende ist, daß die Deutsche Bundespost anscheinend nicht einmal den Versuch unternehmen will, nach „Trojanischen Pferden" zu suchen, wie das folgende Beispiel der Bildschirmtextzentrale in Ulm zeigt:

Der Hersteller der Bildschirmtextzentrale muß den Systemaufbau der Deutschen Bundespost nicht offenlegen, was das Aufspüren „Trojanischer Pferde" vollends unmöglich macht. Der Bundesbeauftragte für den Datenschutz, Dr. Reinhold Baumann, schreibt darüber [BfD_85 Seite 25]:

> *„Wer Daten verarbeitet, muß die Wirkung der dafür eingesetzten Programme genau kennen. Deshalb hat es überrascht, daß der Deutschen Bundespost als Betreiber des Bildschirmtext-Systems keine umfassende Dokumentation aller eingesetzten Programme vorliegt. Zur Begründung dafür hat sie auf ihre vertraglichen Regelungen mit der Lieferfirma IBM hingewiesen. Dadurch ist es der Deutschen Bundespost verwehrt, sich genaue Kenntnis der Programme in allen Details ohne Hilfe Dritter zu verschaffen. Vor diesem Hintergrund erscheint schwer vorstellbar, wie die Deutsche Bundespost ihrer Verantwortung für die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme (§ 15 Nr. 2 BDSG) gerecht werden kann."*

Da der Personenkreis, der an die im Netz, insbesondere in den Vermittlungszentralen, anfallenden Daten gelangen kann, so groß ist, wird es auch ausländischen Geheimdiensten möglich sein, die Daten zu erhalten.

Interessensdaten können außer durch Abhören der Glasfaser oder über die Vermittlungszentralen auch noch von großen Kommunikationspartnern, etwa Datenbanken oder Zeitungsverlagen, gesammelt werden, sofern diese die Identitäten der Dienstnutzer erfahren.

1.3 Notwendigkeit vorbeugenden Datenschutzes als Gegenmaßnahme

Außer durch vorbeugende technische Datenschutzmaßnahmen kann man auf den geschilderten Sachverhalt auf folgende Weisen reagieren:

- Man verdrängt, bagatellisiert oder bestreitet ihn.
- Man verbietet per Gesetz das Erfassen dieser Daten oder das Erstellen von Persönlichkeitsprofilen aus ihnen (was für einen Teil der oben genannten Daten durch das Fernmeldegeheimnis bereits der Fall ist). Aber ein Verbot ist nur dann wirkungsvoll, wenn seine Einhaltung mit angemessenem Aufwand *überprüft* und durch Strafverfolgung gesichert und der ursprüngliche Zustand durch Schadensersatz *wiederhergestellt* werden kann. Beides ist in der geschilderten Situation leider nicht gegeben:

  „Datendiebstahl" allgemein, speziell das direkte Abhören von Leitungen oder Kopieren von Daten aus Vermittlungsrechnern ist kaum feststellbar, da sich an den Originaldaten nichts ändert. Ebenso ist, wie oben erwähnt, das Installieren „Trojanischer Pferde" kaum festzustellen und erst recht nicht die unerlaubte Weiterverarbeitung von Daten, die man legal (oder auch illegal) erhalten hat. Dies bedeutet, daß auch dann, wenn die Post sich an der Durchsetzung des Gesetzes zu beteiligen versucht, nicht einmal entdeckt werden kann, wenn Angestellte, Hersteller von Vermittlungszentralen oder Datenbanken, die die Identitäten der Dienstnutzer erfahren, es übertreten.

  Die Wiederherstellung des ursprünglichen Zustands müßte vor allem darin bestehen, alle entstandenen Daten zu löschen. Man ist aber nie sicher, ob nicht noch weitere Kopien existieren. Außerdem können sich Daten im Gedächtnis von Menschen festsetzen, wo das Löschen besser nicht angestrebt werden sollte.
- Man versucht, die Weiterentwicklung der Kommunikationsnetze zu verhindern, insbesondere die Errichtung diensteintegrierender Digitalnetze mit ihren gegen Angriffe anfälligen komplizierten Vermittlungszentralen. Sofern aber an den durch solche Netze ermöglichten neuen Diensten und Qualitätsverbesserungen für schon existierende Dienste Interesse besteht, wird man ihre Einführung nicht verhindern können und wollen.

So bleibt nur die Möglichkeit, zu untersuchen, ob durch *vorbeugende (größtenteils technische) Datenschutzmaßnahmen* in solchen Netzen das Erstellen von Persönlichkeitsprofilen verhindert werden kann. Dies bedeutet, daß man die Benutzung der Netze, die auf den Netzen angebotenen Dienste oder gar die Netze selbst soweit anders gestaltet, daß von vornherein im Netz keine Möglichkeit besteht, ohne explizite Einwilligung des Teilnehmers über ihn Daten zu erfassen [Pfit_83, Riha_85].

1.4 Diskussion möglicher Einwände

Ein oft gehörter Einwand gegen vorbeugende (und deshalb nicht unterlaufbare) technische Datenschutzmaßnahmen ist, daß sie gesellschaftlich nicht wünschenswert seien, da ein Interesse bestehe, bei begründetem Verdacht das Verhalten Einzelner beobachten zu können (G 10-Gesetz).

Hier kann man entgegnen, daß der technische Fortschritt auch auf anderen Gebieten als Kommunikationsnetzen eine Fülle neuer Überwachungstechniken hervorbringt:

- Immer kleinere und perfektere Abhörmikrofone [Horg_85 Seite 31] oder die Abtastung von Fensterscheiben mittels Laserstrahl durch mehrere hundert Meter entfernte Geräte [Hor2_85] erlauben die Wiedergabe aller Geräusche, z.B. aller Gespräche im Zimmer und am Telefon sowie des gewählten Fernseh- oder Radioprogramms.
- Die Arbeit auf Bildschirmen kann mit einem handelsüblichen Gerät im Wert von rund fünfzig US-Dollar über Entfernungen von 1000 m aufgefangen und auf einem Fernsehgerät dargestellt werden [Eck_85].
- Optische Überwachung ist durch immer bessere und billigere Kameras möglich (neben der klassischen Methode der persönlichen Verfolgung). In Zukunft erlauben vielleicht auch Aufklärungssatelliten nicht nur die Beob-

achtung militärischer Operationen, sondern auch die Erstellung von Bewegungsprofilen privater Bürger.

Dadurch ist eine umfassendere Überwachung *weniger Einzelner* möglich als durch die bisherige Telefonüberwachung. Gegen manche dieser Techniken gibt es Gegenmaßnahmen, z.B. sehr schmutzige Fensterscheiben gegen die Laserüberwachung oder Abschirmung von Terminals (Verfahren und Normen für letzteres sind unter den Kürzeln COMSEC und TEMPEST bekannt [Horg_85]). Da aber auch bisher niemand gezwungen war, am Telefon Belastendes von sich zu geben, ergibt sich nur dasselbe Problem wie mit der bisherigen Telefonüberwachung: gerade diejenigen, die wirklich Gesetze übertreten, greifen vermutlich zu Schutzmaßnahmen, während jemand, der sich keines Unrechts bewußt ist, beobachtbar ist.

Die geplanten Kommunikationsnetze hingegen würden nicht nur eine viel umfassendere Beobachtung Einzelner, sondern auch ohne großen Aufwand das Beobachten der *gesamten Bevölkerung* ermöglichen, und zwar nicht nur durch den eigenen Staat (Geheimdienst), sondern auch durch Fernmeldefirmen, Systemprogrammierer, fremde Staaten (Geheimdienste) usw.

Dieser Aufwandsunterschied zwischen Beobachtung über diensteintegrierende Digitalnetze und anderen Überwachungstechniken beantwortet auch den umgekehrten Einwand, ob es sich überhaupt lohne, Daten in Netzen zu schützen, ohne gleichzeitig Gegenmaßnahmen gegen alle anderen Überwachungsmöglichkeiten anzugeben und zu ergreifen.

In entfernterer Zukunft könnten aber einige der anderen Überwachungsmöglichkeiten zu ebenso großen Datenschutzproblemen führen. Außerdem werden einige der Daten, die in Kommunikationsnetzen geschützt werden sollen, über Personalinformationssysteme, maschinenlesbare Personalausweise u.ä. ebenfalls in Rechenanlagen gelangen. Hier ergibt sich (wie bei den Vermittlungszentralen) das Problem, daß die Einhaltung von Datenschutzgesetzen und -vereinbarungen nicht mit vernünftigem Aufwand überprüfbar ist.

1.5 Was kann man durch Verschlüsselung erreichen?

Kommunikation wird technisch üblicherweise durch Verschlüsselung der Daten geschützt [VoKe_83]. Hier hat man zwei Strategien zur Auswahl, die leider beide Nachteile haben:

Die erste Strategie besteht darin, alle Daten jeweils zwischen benachbarten Netzknoten, d.h. Teilnehmerstationen und Vermittlungszentralen, zu verschlüsseln (*Verbindungs-Verschlüsselung*, link-by-link encryption). Dadurch erhält man durch das Abhören der Glasfaser keine Information mehr. Die Nachteile sind:

- In den Vermittlungszentralen liegen alle Daten unverschlüsselt vor, von allen oben genannten möglichen Angreifern werden also nur diejenigen ausgeschlossen, die die Glasfaser abhören.

  (Wir verwenden „Angreifer" als kurze Bezeichnung für jemanden, der versucht, personenbezogene Daten ohne Einwilligung des Betroffenen zu sammeln.)
- Auf der Glasfaser werden etwa 560 Mbit/s übertragen. Dies ist eher oberhalb dessen, was heute mit Kryptogeräten, die auf einem für halbwegs sicher gehaltenen Kryptosystem beruhen und halbwegs preiswert sind, verschlüsselt werden kann. So verschlüsseln die schnellsten auf dem Data Encryption Standard (DES) beruhenden, auf einem Chip implementierten Geräte 14 Mbit/s [Abbr_84, DESi_84, Hors_85, KaRS_85]. Es wäre zumindest von Vorteil, wenn man Fernsehen als breitbandigen Dienst, bei dem es nicht um den Schutz von Inhalts-, sondern von Interessensdaten geht, nicht verschlüsseln müßte.

Die zweite Strategie ist, die Daten zwischen Teilnehmerstationen verschlüsselt zu übertragen (*Ende-zu-Ende-Verschlüsselung*, end-to-end encryption), damit sie in der Vermittlungszentrale nicht interpretiert werden können. Die Nachteile hiervon sind:

- Durch Ende-zu-Ende-Verschlüsselung können nur die Nutzdaten, nicht die Vermittlungsdaten geschützt werden. Verkehrsdaten (vgl. 1.2) lassen sich also weiterhin gewinnen.
- Vor jemandem, der die Nutzdaten schon vorher kannte und nun die Vermittlungsdaten erhält, sind damit auch die Interessensdaten (vgl. 1.2) ungeschützt.

  Insbesondere kann dieses Verfahren also nicht als Schutz vor der Post und anderen, die Zugriff auf Postrechner haben, dienen, wenn diese gleichzeitig Kommunikationspartner sind oder wenn sich die Nutzdaten in Form einer Datenbank in einem Postrechner (z.B. Bildschirmtext-Zentrale in Ulm) befinden. Die Nutzdaten können zwar in verschlüsselter Form in der Datenbank abgespeichert werden, dies nützt jedoch nur etwas, wenn der Angreifer (Post bzw. andere mit Zugriff auf Postrechner) die zugehörigen Schlüssel nicht kennt und auch nicht in Erfahrung bringen kann. Letzteres erscheint außer bei kleinen geschlossenen Benutzergruppen unrealistisch, da der Angreifer in große geschlossene Benutzergruppen einen Strohmann einschleusen und bei offenen Benutzergruppen als normaler Nutzdateninteressent auftreten kann.

  Daneben ist auch eine Zusammenarbeit von jemandem, der an Daten in der Vermittlungszentrale gelangen kann, und dem Kommunikationspartner denkbar. Dies könnte z.B. vom Geheimdienst ausgehen, der über die Post die Vermittlungsdaten erhält und Kommunikationspartner, z.B. Datenbanken, Zeitungsverlage, veranlaßt, ihm die Nutzdaten offenzulegen, aber auch vom Kommunikationspartner, der über Angestellte o.ä. Zugang zu den Vermittlungsdaten erhält.

  Außerdem ist es trivialerweise sinnlos, sich mit Ende-zu-Ende-Verschlüsselung vor Kommunikationspartnern schützen zu wollen, die die Identitäten der Dienstnutzer im normalen Verlauf der Dienstnutzung erfahren.
- Wie bei Verbindungs-Verschlüsselung ist es auch hier recht umständlich, auch Fernsehen verschlüsseln zu müssen, um die Interessensdaten vor den Angreifern in den Vermittlungszentralen zu schützen.

1.6 Was bleibt zu tun?

Auch die üblichen kryptographischen Techniken erlauben also auf der heute üblichen und von der Deutschen Bundespost auch für die Zukunft geplanten Netzstruktur diensteintegrierender Netze keinen ausreichenden und mit vernünftigem Aufwand *überprüfbaren* Datenschutz für Ver-

kehrs- und Interessensdaten vor vielen möglichen Angreifern in den Vermittlungszentralen und Kommunikationspartnern.

Die folgenden Kapitel untersuchen, wie der noch fehlende Schutz durch andere Maßnahmen erreicht werden kann. Dabei muß darauf geachtet werden, daß nicht jemand, der bisher als möglicher Angreifer gar nicht auftrat, z.B. Nachbarn, plötzlich Beobachtungsmöglichkeiten erhält.

Technisch gesehen ist dabei das Hauptziel, die Verkehrsdaten vor dem Betreiber der Vermittlungseinrichtungen zu schützen und sich auch gegenüber dem Kommunikationspartner nicht identifizieren zu müssen. Damit sind Verkehrs- und Interessensdaten nicht nur vor diesen geschützt, sondern (und das ohne zusätzliche Verschlüsselung von nicht personenbezogenen Nutzdaten wie Fernsehen) erst recht vor anderen Angreifern in den Vermittlungseinrichtungen oder Abhörern, da alle diese höchstens genausoviel Information erhalten können wie der Betreiber selbst. Der Schutz der Inhaltsdaten wird dann zusätzlich durch Ende-zu-Ende-Verschlüsselung personenbezogener Nutzdaten erreicht.

In Kapitel 2 werden Grundverfahren mit einigen Überlegungen zu ihrer Implementierung dargestellt, und in Kapitel 3 wird untersucht, wie diese Verfahren für eine Anwendung in breitbandigen diensteintegrierenden Digitalnetzen abgeändert und ergänzt werden müssen.

2 Grundverfahren

In diesem Kapitel werden grundlegende Verfahren zum Schutz von Verkehrs- und Interessensdaten vor Angreifern in Vermittlungszentralen und Kommunikationspartnern dargelegt.

Zunächst werden Schutzmaßnahmen dargestellt, die außerhalb des Netzes angesiedelt sind, d.h. die jeder Benutzer für sich trifft. Diese werden sich als nicht ausreichend erweisen.

Danach werden solche Schutzmaßnahmen dargestellt, die innerhalb des Netzes angesiedelt sind, d.h. die Benutzung des Netzes nicht verändern, jedoch den Transport innerhalb des Netzes.

2.1 Schutz außerhalb des Netzes

Bei Schutzmaßnahmen außerhalb des Netzes sind Ziel- und Herkunftsadresse einer Nachricht weiterhin im Netz als Vermittlungsdaten sichtbar. Dazu sind natürlich die Zeit, zu der eine Nachricht im Netz ist, und zumindest für den Kommunikationspartner die Nutzdaten sichtbar. Man muß verhindern, daß daraus Schlüsse auf Verkehrs- und Interessensdaten gezogen werden können.

2.1.1 Öffentliche Anschlüsse

Die Herkunftsadresse und Zieladresse einer Nachricht werden weitgehend bedeutungslos, wenn man verschiedene öffentliche Anschlüsse benutzt, z.B. Telefonzellen. Dies gilt natürlich nur, wenn man sich nicht zu Zwecken der Zugangskontrolle oder der Zahlung von Gebühren identifizieren muß, d.h. anonym bleibt.

Die Anwendung und Wirkung dieser Maßnahme ist stark eingeschränkt: Wer etwa will in (Bild-)Telefonzellen fernsehen?

2.1.2 Zeitlich entkoppelte Verarbeitung

Die Zeit, zu der sich eine Nachricht im Netz befindet, wird weitgehend bedeutungslos, wenn man Teilnehmerstationen (z.B. Personal Computer) Informationen nicht erst dann anfordern läßt, wenn der Teilnehmer sie benötigt, sondern zu einem beliebigen Zeitpunkt vorher:

> *Will man eine Zeitung lesen, so kann die Teilnehmerstation sie bereits zum Erscheinungszeitpunkt oder einem Zeitpunkt mit besonders geringen Übertragungskosten (z.B. Nachttarif) anfordern und zum späteren Lesen abspeichern.*

Diese Schutzmaßnahme verhindert, daß der Netzbetreiber allein aus dem Vermittlungsdatum „Zeit" und Kontextwissen schließen kann, wer mit wem kommuniziert:

> *Wenn tagsüber eine Zeitung angefordert wird und 10 Leute als Anforderer in Frage kommen, von denen bekanntlich 9 in Tag- und einer in Nachtschicht arbeiten, wäre ohne zeitliche Entkopplung klar, daß sie der Nachtarbeiter liest.*

Kann der Netzbetreiber auf andere Art erkennen, wer mit wem kommuniziert, so erschwert diese Maßnahme doch zumindest das Erstellen von Persönlichkeitsbildern über den Tagesablauf.

Natürlich greift diese Maßnahme nicht bei Kommunikationsformen mit Realzeitanforderungen.

2.1.3 Lokale Auswahl

Um Interessensdaten zu schützen, kann man Information in großen Einheiten anfordern und lokal auswählen (lassen), was einen wirklich interessiert:

> *Bestellt man sich statt eines bestimmten Zeitungsartikels mehrere Zeitungen verschiedener politischer Richtungen, so können aus der Bestellung keinerlei Rückschlüsse auf die Interessen und Meinungen des Bestellers gezogen werden.*
>
> *Zusätzlich ließe sich durch „intelligente" Teilnehmerstationen die Dienstleistung sogenannter Ausschnittsbüros, die einem Kunden auf Wunsch zu einem bestimmten Thema Artikel aus mehreren Zeitungen zusammenstellen, jedem Teilnehmer bieten.*

Durch die lokale Auswahl verschleiert man selbst gegenüber dem Kommunikationspartner, was einen wirklich interessiert.

Das Anfordern von großen Informationseinheiten vom Kommunikationspartner ist folglich als Schutz bei solchen Informationsarten sinnvoll, die unverschlüsselt übertragen werden oder bei denen Netzbetreiber und Kommunikationspartner identisch sind oder als zusammenarbeitend angenommen werden können.

In zukünftigen Netzen, in denen (zumindest für schmalbandiges Senden) reichlich Bandbreite zur Verfügung steht, verursacht diese Maßnahme bei Diensten, bei denen der Benutzer nur bereits bereitgestellte Information abruft, real beinahe keine Kosten. Es ist jedoch eine Frage des Abrechnungsmodus, ob dies auch dem Anwender dieser Maßnahme zugutekommt (vgl. 3.4).

2.2 Schutz innerhalb des Netzes

Im Gegensatz zu den oben genannten Schutzmaßnahmen sollen in diesem Kapitel Maßnahmen vorgestellt werden, die die im Netz anfallenden Vermittlungsdaten selbst verringern.

Dadurch soll für den Teilnehmer unsichtbar, aber nachprüfbar Senden und Empfangen, zumindest aber die Kommunikationsbeziehungen zwischen Teilnehmern vor möglichen Angreifern (bösen Nachbarn, dem Netzbetreiber, großen Organisationen und Konzernen usw.) verborgen werden, so daß das Erfassen von Verkehrs- oder Interessensdaten unmöglich wird.

Da Schutz vor einem allmächtigen Angreifer, der alle Leitungen, alle Vermittlungszentralen, alle Teilnehmerstationen außer der eigenen und den Kommunikationspartner kontrolliert, nicht möglich ist, sind alle folgenden Maßnahmen nur Annäherungen an den perfekten Schutz der Teilnehmer vor jedem möglichen Angreifer. Die Annäherung wird im allgemeinen durch Angabe des unterstellten Angreifermodelles (Was wird von ihm kontrolliert; wie stark ist er maximal?) beschrieben.

Verbirgt ein Kommunikationsnetz Senden und Empfangen oder zumindest die Kommunikationsbeziehung vor dem unterstellten Angreifer, so nennen wir es anonym und sprechen dann von anonymer Kommunikation.

2.2.1 Schutz des Empfängers

Indem das Netz alle Informationen an alle Teilnehmer sendet (Verteilung, broadcast), kann man den Empfänger der Information vor dem Netz und dem Kommunikationspartner schützen.

Will man dies auch bei bisher vermittelten Diensten tun, so muß jede Teilnehmerstation anhand eines Merkmals (*implizite Adresse*) entscheiden können, welche Nachrichten wirklich für sie bestimmt sind.

Kann eine Adresse nur vom Empfänger ausgewertet werden, so spricht man von *verdeckter Adressierung.* Kann eine Adresse von jedem ausgewertet, d.h. auf Gleichheit mit anderen Adressen getestet werden, so nennt man dies *offene Adressierung* [Waid_85].

Die übliche Implementierung von verdeckter Adressierung verwendet Redundanz innerhalb des Nachrichteninhalts und ein Kryptosystem mit öffentlichen Schlüsseln [Denn_82]. Jede Nachricht wird mit dem öffentlichen Schlüssel des adressierten Teilnehmers verschlüsselt (wodurch gleichzeitig Ende-zu-Ende-verschlüsselt wird). Nach der Entschlüsselung mit dem zugehörigen privaten Schlüssel kann die Teilnehmerstation des adressierten Teilnehmers anhand der Redundanz feststellen, daß die Nachricht für sie bestimmt ist. Da die Implementierungen von Kryptosystemen mit öffentlichen Schlüsseln langsam sind und jede Teilnehmerstation alle Nachrichten entschlüsseln muß, ist dieses Verfahren im allgemeinen viel zu aufwendig. Es kann durch Austausch eines geheimen Schlüssels und Verwendung eines schnelleren konventionellen Kryptosystems (statt eines Kryptosystems mit öffentlichen Schlüsseln) nach Aufnahme der Kommunikationsbeziehung jedoch etwas effizienter gestaltet werden.

Offene Adressierung läßt sich einfacher realisieren, indem man z.B. Nachrichten mit einem Adreßfeld versieht und die Teilnehmer(stationen) beliebige Zahlen als Adressen erzeugen. Eine Teilnehmerstation muß dann nur bei allen erhaltenen Nachrichten dieses Adreßfeld mit ihren Adressen vergleichen.

Hinsichtlich der Adreßverwaltung kann man bei beiden Formen der impliziten Adressierung öffentliche und private Adressen unterscheiden: *Offentliche Adressen* stehen in allgemein zugänglichen Adreßverzeichnissen (z.B. in einem „Telefonbuch") und dienen meist einer ersten Kontaktaufnahme. *Private Adressen* werden an einzelne Kommunikationspartner gegeben. Dies kann entweder außerhalb des Netzes oder innerhalb als Absenderangabe in Nachrichten geschehen.

Bei offener Adressierung, im Gegensatz zur verdeckten, kann das Netz Informationen über die Empfänger von Nachrichten gewinnen. Dies kann bei Verwendung privater Adressen geschehen, wenn man dieselbe Adresse mehrfach verwendet, weil dann erkennbar wird, daß diese Nachrichten an denselben Empfänger gerichtet sind. Die mehrmalige Verwendung muß also durch fortlaufendes Generieren und Mitübertragen oder durch Vereinbarung eines Generieralgorithmus (Pseudozufallszahlengenerator) vermieden werden. Bei Verwendung öffentlicher offener Adressen kann sogar festgestellt werden, unter welcher Bezeichnung der Empfänger im Adreßverzeichnis eingetragen ist. Die Verwendung solcher Adressen sollte also möglichst vermieden werden.

Die Datenschutz- und Aufwandseigenschaften der Kombinationen von Adressierungsart und Adreßverwaltung sind in Bild 3 zusammengefaßt.

Gegenüber expliziter Adressierung, bei der die Adreßinformation vom Netz interpretiert und zur Wegwahl und damit zur Minimierung der Netzbelastung verwendet wird, hat implizite Adressierung bezüglich der effizienten Nutzung des Netzes einen leichten Vorteil und einen schweren Nachteil: Das Wegwahl-Problem (routing) im Netz vereinfacht sich, wenn man z.B. Überflutung (flooding [Tane_81]) einsetzt: jede Station überträgt jede Nachricht an alle Nachbarstationen, von denen sie diese Nachricht (noch) nicht empfangen hat. Je nach Netz kann jedoch die nutzbare Leistung sehr stark absinken.

Durch Verteilung und geeignete implizite Adressierung kann der Empfänger einer Nachricht also vollständig geschützt werden.

			Adreßverwaltung	
			öffentliche Adresse	private Adresse
Adressierungsart	implizite Adresse	verdeckt	sehr aufwendig, für Kontaktaufnahme nötig	aufwendig
		offen	abzuraten	nach Kontaktaufnahme ständig wechseln
	explizite Adresse		sehr abzuraten	sehr abzuraten

Bild 3 Bewertung der Kombinationen von Adressierungsart und Adreßverwaltung

2.2.2 Schutz der Kommunikationsbeziehung

Statt zusätzlich zum Empfänger auch den Sender verborgen zu halten, kann man zunächst versuchen, nur deren Verbindung geheimzuhalten und so die Anonymität der Kommunikation herzustellen.

Diese Idee wird durch das Verfahren der umkodierenden MIXe verwirklicht [Chau_81].

Bei diesem von David Chaum 1981 für elektronische Post vorgeschlagenen Verfahren werden Nachrichten nicht notwendigerweise auf dem kürzesten Weg zum Empfänger geschickt, sondern über mehrere möglichst unabhängige, umkodierende und umsortierende Zwischenstationen, sogenannte MIXe, geleitet. Der Absender einer Nachricht verschlüsselt sie so mit Schlüsseln eines Kryptosystems mit öffentlichen Schlüsseln, daß sie nacheinander von einer von ihm gewählten Folge von MIXen mit deren zugehörigen privaten Schlüsseln entschlüsselt werden muß. Dadurch ändert sich das Erscheinungsbild der Nachricht auf jedem Stück ihres Weges, so daß ihr Weg (außer wenn alle MIXe, die sie durchläuft, zusammenarbeiten) nicht verfolgt werden kann.

Um ein Verfolgen von Nachrichten nicht durch zeitliche Zusammenhänge oder ihre Längen zu ermöglichen, muß jeder MIX eine Reihe von Nachrichten gleicher Länge abwarten und dann diese umsortiert wieder ausgeben. Gegebenenfalls müssen Teilnehmer oder MIXe bedeutungslose Nachrichten erzeugen.

Um nicht über Nachrichtenhäufigkeiten Entsprechungen zwischen Ein- und Ausgabe des MIXes entstehen zu lassen, bearbeitet der MIX (solange er sein Schlüsselpaar beibehält) nur unterschiedliche Eingabenachrichten. Erhält der MIX eine Eingabenachricht mehrmals, ignoriert er ihr wiederholtes Eintreffen.

Das Verfahren ist in Bild 4 anhand zweier MIXe dargestellt.

Die schlimmste Folge eines Angriffs (oder Fehlers) durch einen MIX wäre dann der Verlust einer Nachricht, nicht jedoch der Verlust der Anonymität. Durch öffentlichen Zugriff auf die von MIXen gesendeten Nachrichten ist ein Verlust jedoch feststellbar und beweisbar. Durch geeignete Fehlertoleranzmaßnahmen ist zudem die Wahrscheinlichkeit des Verlustes von Nachrichten durch Ausfall eines MIXes (ein ausgefallener MIX reicht, um eine Nachricht zu verlieren!) zu vermindern [Pfi1_85, PfWa_85].

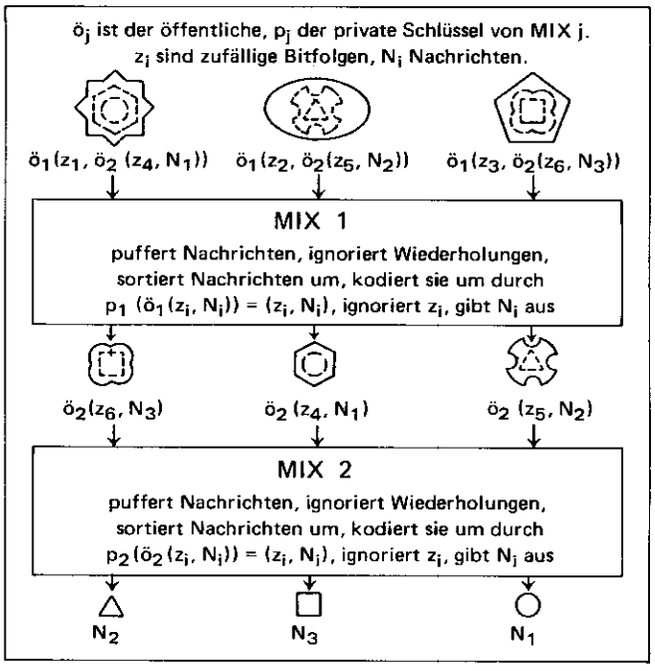


Bild 4 MIXe verbergen den Zusammenhang zwischen ein- und auslaufenden Nachrichten

Wegen der Zeitverzögerung durch Umsortieren der Nachrichten und des Zeitaufwandes für die Entschlüsselungen in einem Kryptosystem mit öffentlichen Schlüsseln ist dieses Verfahren nicht für Anwendungen geeignet, die kurze Übertragungszeiten fordern.

Wandelt man dieses Verfahren aber ab, so kann man anonyme Kanäle schalten, die z.B. den Realzeitanforderungen des Telefonverkehrs genügen könnten. Hierzu wird zum Kanalaufbau eine spezielle Nachricht nach dem oben beschriebenen Verfahren übertragen, die jedem gewählten MIX einen Schlüssel eines schnelleren Kryptosystems mit privaten Schlüsseln übergibt, den dieser MIX von da an für die Entschlüsselung des Verkehrs auf diesem Kanal verwendet [Pfi1_85]. Das Umkodieren bei Kanälen nützt natürlich nur dann etwas, wenn mindestens zwei Kanäle durch denselben MIX gleichzeitig auf- und abgebaut werden.

Will man durch umkodierende MIXe nicht nur Kommunikationsbeziehungen, sondern auch das Senden und Empfangen von Teilnehmerstationen schützen, muß jede Teilnehmerstation ein MIX sein oder sehr viele bedeutungslose Nachrichten senden, wie dies im folgenden Abschnitt beschrieben ist. Ersteres erfordert bei geringer Verkehrsdichte große Wartezeiten auf mehrere Nachrichten bzw. auf Auf- oder Abbau von mehreren Kanälen. Bei hoher Verkehrsdichte erfordert es Teilnehmerstationen, die sehr viele Nachrichten und breitbandige Kanäle umkodieren und vermitteln können. Derartige Teilnehmerstationen sind sehr aufwendig und in der überschaubaren Zukunft zu teuer.

2.2.3 Schutz des Senders

Der Sender einer Nachricht kann sich schützen, indem er *bedeutungslose Nachrichten* (dummy traffic) sendet. Werden diese mit nicht existenten impliziten Adressen versehen, können sie von allen Teilnehmerstationen weggeworfen werden. Werden auch bedeutungslose Nachrichten gesendet, kann das Netz nicht mehr entscheiden, wann genau und wieviele bedeutungsvolle Nachrichten ein Teilnehmer sendet [Chau_81].

Dieses Verfahren verursacht stets einen sehr hohen Aufwand und erfüllt zugleich nicht die Forderung nach Anonymität auch bei Angriffen, an denen sich der Empfänger bedeutungsvoller Nachrichten beteiligt.

Die beiden folgenden Verfahren haben diese Nachteile nicht; sie sind in gewisser Weise effizient und es ist bewiesen, daß der Sender selbst bei Identität oder Zusammenarbeit von Empfänger und Netzbetreiber anonym ist.

2.2.3.1 Überlagerndes Senden

In [Cha3_85, Cha8_85] gibt David Chaum folgende Möglichkeit zum anonymen Senden (und Empfangen) an:

Alle Teilnehmerstationen erzeugen für jedes zu sendende Nutzbit ein oder mehrere Schlüsselbits, von denen sie jedes genau einer anderen Teilnehmerstation auf einem (noch zu diskutierenden) geheimen Kanal zukommen lassen. Jede

Teilnehmerstation *überlagert* (bildet die Summe modulo 2) lokal alle ihr bekannten Schlüsselbits und, sofern sie ein Nutzbit senden will, ihr Nutzbit. Jede Teilnehmerstation sendet das Ergebnis ihrer lokalen Überlagerung. Alle gesendeten Bits werden global überlagert und die entstehende Summe (modulo 2) aller Bits an alle Teilnehmerstationen verteilt.

Wollte keine senden, ist die Summe 0, da jedes Schlüsselbit genau zweimal addiert wurde. Wollte eine senden, ist die Summe gleich dem gesendeten Nutzbit.

Natürlich können Kollisionen auftreten, falls mehrere Teilnehmerstationen gleichzeitig senden wollen. Dies ist ein übliches Problem bei Verteil-Kanälen mit Mehrfachzugriff, zu dessen Lösung es eine große Zahl von Zugriffsverfahren gibt. Man darf aber nur solche verwenden, die die Anonymität des Senders wahren. Daneben sollten sie bei zu erwartender Verkehrsverteilung den zur Verfügung stehenden Kanal günstig nutzen [Pfi1_85]. Beispiele anonymer Zugriffsverfahren sind das einfache, aber nicht sehr effiziente Verfahren slotted ALOHA und eine für Kanäle mit großer Verzögerungszeit entworfene, effiziente Reservierungstechnik [Tane_81 Seite 272, Cha3_85].

Vereinbart man, daß ein Teilnehmer einen Übertragungsrahmen, in dem er ohne Kollision gesendet hat, weiterbenutzen darf und andere Teilnehmer in diesem Rahmen erst wieder senden dürfen, wenn er einmal nicht benutzt wurde, so kann man durch die Verwendung mehrerer Übertragungsrahmen (slots) Kanäle schalten [Höck_85, HöPf_85].

David Chaum beweist in [Cha3_85], daß, solange eine Gruppe von Teilnehmerstationen Schlüssel nur in der beschriebenen Form weitergibt und solange diese Gruppe bezüglich der ausgetauschten Schlüssel zusammenhängend ist, andere an diesem Verfahren Beteiligte auch durch Zusammentragen all ihrer Information keine Information darüber erhalten, wer innerhalb der Gruppe sendet. „Bezüglich der ausgetauschten Schlüssel zusammenhängend" bedeutet, daß für je zwei beliebige Teilnehmerstationen T_0, T_1 der Gruppe es eine möglicherweise leere Folge von Teilnehmerstationen T_2 bis T_n der Gruppe gibt, so daß für $1 \leqq i \leqq n$ gilt: T_i hat mit $T_{(i+1) \bmod (n+1)}$ einen Schlüssel ausgetauscht.

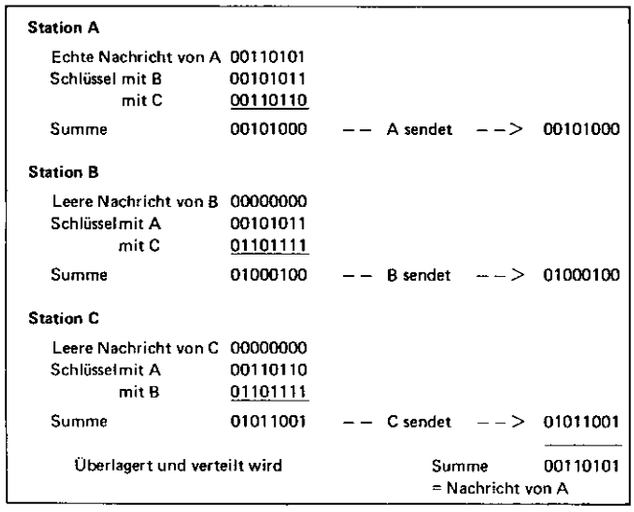


Bild 5 Überlagerndes Senden

Der Einsatz dieses Verfahrens ist sehr aufwendig, weil man große Mengen an Schlüsseln geheim austauschen muß: Für jedes Paar von Teilnehmerstationen, das Schlüssel miteinander austauscht, benötigt man dazu einen geheimen Kanal mit derselben Bandbreite, wie sie das Netz allen Benutzern zusammen zum Austausch ihrer Nachrichten bereitstellt.

Diesen Aufwand beim Schlüsselaustausch kann man reduzieren, indem man Pseudozufallszahlengeneratoren verwendet. Man muß dann nur relativ kurze Schlüssel geheim austauschen und kann aus diesen sehr lange Schlüssel, die äußeren Betrachtern zufällig erscheinen, erzeugen.

Das Verfahren ist dann nicht mehr informationstheoretisch sicher, sondern nur noch kryptographisch mehr oder weniger sicher.

Leider sind die uns bekannten schnellen Pseudozufallszahlengeneratoren alle leicht brechbar oder zumindest von zweifelhafter Sicherheit (z.B. rückgekoppelte Schieberegister), während die bisherigen kryptographisch starken Pseudozufallszahlengeneratoren [VaVa_85, BlMi_84] sehr aufwendig und sehr, sehr langsam sind. Dabei heißt ein Pseudozufallszahlengenerator kryptographisch stark, wenn bewiesen werden kann, daß durch das Brechen zugleich ein effizienter Algorithmus zur Lösung eines wohluntersuchten, aber bislang nicht effizient lösbaren mathematischen Problems (z.B. Faktorisierung, diskreter Logarithmus) angegeben werden kann.

David Chaum schlägt in [Cha3_85] vor, das überlagernde Senden auf einem Ring zu implementieren. Dadurch wird einem Angreifer das Brechen von schnellen (und vielleicht leicht brechbaren) Pseudozufallszahlengeneratoren erschwert, weil er die Ausgaben von aufeinanderfolgenden Teilnehmerstationen im Ring nur durch sehr aufwendige physikalische Maßnahmen, also realistischerweise nicht erfährt (vgl. 2.2.3.2).

Bei dieser Implementierung kreist jedes Bit einmal zum Zwecke des Sendens durch sukzessives Überlagern und einmal zum Zwecke des Empfangens um den Ring.

Da diese Implementierung im Mittel nur den vierfachen Übertragungsaufwand verursacht wie ein übliches Sendeverfahren auf einem Ring, während eine Implementierung auf einem sternförmigen Netz den N-fachen Übertragungsaufwand gegenüber einem gewöhnlichen Sendeverfahren auf einem Stern verursacht, wirkt sie recht effizient.

Da aber die Übertragungsmenge auf jeder einzelnen Leitung, also die geforderte Bandbreite, bei allen Implementierungen gleich ist, könnte die Implementierung auf einem Stern (oder allgemeiner: Baum) trotzdem effizienter sein. Die Implementierung eines Kanals ist um so besser, je kürzer die Verzögerungszeit ist, also die Zeit, die zwischen Sendeversuch und der Rückmeldung, ob eine Kollision auftrat, verstreicht. Für dieses Verfahren können die Knoten von Stern- und Baumnetzen wesentlich einfacher als übliche Vermittlungszentralen sein und so entworfen werden, daß die Summe der Schaltzeiten nur logarithmisch mit der Teilnehmeranzahl wächst. Die reine Laufzeit wächst ungefähr mit der Wurzel der Teilnehmeranzahl, während beide bei Ringnetzen stets proportional zur Teilnehmeranzahl wachsen [Pfi1_85].

2.2.3.2 RING-Netz

Das aufwendige Generieren, ggf. Verteilen und Überlagern von Schlüsseln und Nutzdaten im vorherigen Abschnitt ist nötig, da davon ausgegangen wird, daß ein Angreifer die Ausgänge und Eingänge aller Teilnehmerstationen abhört.

Die Idee für ein weit weniger aufwendiges Verfahren, das *RING-Netz*, besteht darin, das Netz bereits physikalisch so zu gestalten, daß es für einen Angreifer nicht einfacher ist, alle Ein- und Ausgänge einer Teilnehmerstation abzuhören, als den Teilnehmer bzw. die Teilnehmerstation direkt zu beobachten (vgl. 1.4).

Die praktischste Möglichkeit hierzu ist, die Teilnehmerstationen ringförmig anzuordnen, wie dies im Bereich lokaler Netze seit langem praktiziert wird. Um hier das Senden einer Station zu überwachen, müssen entweder ihre beiden Nachbarn zusammenarbeiten oder die Leitungen müssen abgehört werden. Durch bauliche Maßnahmen, z.B. direkte Verkabelung von Wohnungen in Mehrfamilienhäusern sowie direkte Verkabelung aneinandergrenzender privater Grundstücke [Pfi1_83 Seite 18], kann man erreichen, daß letzteres ebenso aufwendige physikalische Maßnahmen erfordert wie das direkte Abhören des Teilnehmers oder der Teilnehmerstation innerhalb der Wohnung. Damit verspricht es keinen zusätzlichen Vorteil. Versuchen die zwei Ringnachbarn eines Teilnehmers, diesen ohne Auftrag Dritter (d.h. hier ohne Zusammenarbeit mit großen Kommunikationspartnern) zu beobachten, so erfahren sie beinahe nichts, da alle ausgehenden Nachrichten verschlüsselt und die Adressen bei geeigneter Verwendung impliziter Adressierung für sie nicht interpretierbar sind.

Zu erwarten sind also im wesentlichen Angreifer, die nur eine Gruppe von mehreren zusammenhängenden Stationen eingekreist haben. Sie können durch Vergleich der ein- und auslaufenden Bitmuster nur feststellen, welche davon von den Mitgliedern dieser Gruppe gesendet bzw. vom Ring entfernt wurden, nicht aber von welchem Mitglied genau. Ein Angreifer hat allerdings nicht nur die Möglichkeit, ein- und auslaufende Bitmuster zu vergleichen, sondern kann auch seine Kenntnis des Ringzugriffsverfahrens verwenden, um Schlüsse zu ziehen, wer gerade senden darf. Man kann aber zeigen, daß bei geeigneten Ringzugriffsverfahren ein Angreifer, der eine Station nicht direkt eingekreist hat, tatsächlich das Senden dieser Station nie feststellen kann [HöPf_85, Höck_85]. Geeignet und effizient sind gewisse bekannte Verfahren (slotted ring, token ring), die dahingehend abgewandelt wurden, daß Senderecht zeitlich unbefristet vergeben wird und daß jede Nachricht einmal ganz um den Ring läuft, d.h. nicht vom Empfänger, sondern erst vom Sender wieder vom Ring entfernt wird (Bild 6). Da durch sie bereits Verteilung realisiert ist, wird neben dem Sender auch der Empfänger geschützt.

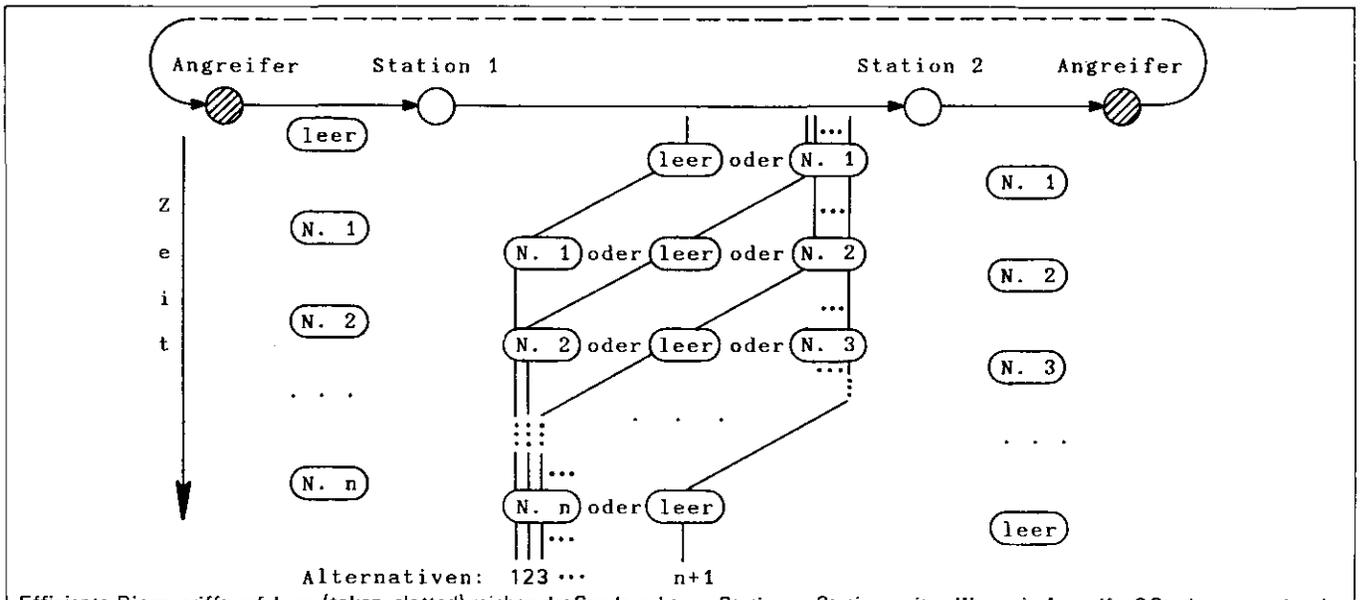
Sowohl das Senden von Nachrichten als auch das Schalten von Kanälen ist mit Hilfe dieser Zugriffsverfahren möglich. Bei Duplexkanälen kann man aber ohne große Anonymitätseinbußen auch wieder darauf verzichten, daß alle Information einmal ganz um den Ring läuft. Statt dessen nimmt der Empfänger die Information vom Ring und ersetzt sie sofort durch Information in Gegenrichtung. Dadurch ist die Kapazität des Rings doppelt so gut nutzbar.

3 Gestaltung eines Anonymität garantierenden breitbandigen diensteintegrierenden Digitalnetzes

In Kapitel 2 wurden Grundverfahren beschrieben, die es den Teilnehmern eines Digitalnetzes ermöglichen, anonym voreinander wie auch vor dem Netz Nachrichten auszutauschen. Dieses Kapitel setzt diese Lösungsansätze in Beziehung zur Gesamtheit der Forderungen, die an ein Anonymität garantierendes breitbandiges diensteintegrierendes Digitalnetz gestellt werden.

3.1 Physikalische Ebene: Vermittlungs-/ Verteilnetz

In diesem Abschnitt wird nach Implementierungen für die Verfahren aus Kapitel 2.2 gesucht, die die hohen Leistungs-



Effiziente Ringzugriffsverfahren (token, slotted) reichen das Senderecht von Station zu Station weiter. Wenn ein Angreifer 2 Stationen umzingelt hat, die nach Erhalt des Senderechts insgesamt n Nachrichten senden und dann das Sendrecht weiterreichen, gibt es n+1 Alternativen, welche Station welche Nachricht (N.) gesendet haben kann. Für jede Nachricht gibt es mindestens eine Alternative, bei der Station i (i = 1,2) die Nachricht sendet.
Das Beispiel kann auf g umzingelte Stationen verallgemeinert werden. Es gibt $\binom{n+g-1}{n}$ Alternativen und zumindest eine Alternative für jede Nachricht, bei der Station i (i = 1,2,...,g) die Nachricht sendet.

Bild 6 Ein anonymes Zugriffsverfahren für RING-Netze garantiert: ein Angreifer, der eine Folge von Stationen umzingelt hat, kann nicht entscheiden, welche was sendet.

anforderungen (nach großem Durchsatz und kurzen Verzögerungszeiten) eines breitbandigen diensteintegrierenden Digitalnetzes erfüllen.

Die genauen Forderungen sind zwar bei verschiedenen Diensten verschieden, da es aber mit dem Bildfernsprechen mindestens einen Dienst gibt, der alle Forderungen zusammen stellt, muß man ein Netz entwerfen, das alle diese Forderungen gleichzeitig hinreichend gut erfüllt.

Zumindest im Teilnehmeranschlußbereich sollten aus Kostengründen auch alle anderen Dienste auf derselben physischen Netzstruktur abgewickelt werden. Dabei kann man aber Dienste, die weniger hohe Leistungsanforderungen stellen, mit anderen Protokollen behandeln, um noch stärkeren Datenschutz zu garantieren.

Beschränkt man sich darauf, ein Netz für die Bundesrepublik Deutschland, also einen Staat mit Fernmeldemonopol, zu konstruieren, so ist der Lösungsansatz der umkodierenden MIXe kaum zu verwirklichen: Da erforderlich ist, daß die MIXe nicht zusammen gegen die Benutzer arbeiten, sollten sie verschiedene Betreiber haben. Dies bedeutet, daß jede Nachricht das öffentliche Netz mehrmals durchläuft, da nicht einfach dessen Vermittlungsstellen allein als MIXe eingesetzt werden können. Dadurch wird das Verfahren für ein breitbandiges Netz sehr übertragungsaufwendig. Dabei müßte auch noch die Verantwortung für die Dienstqualität zwischen der Post und den MIX-Betreibern geregelt werden.

Außerdem kann es, um die Summe der Kosten aller MIXe und die durch ihr gleichzeitiges Ausgeben von Nachrichten bzw. Schalten von Kanälen bedingten Verzögerungszeiten erträglich zu halten, nur relativ wenige MIXe geben, die dann sehr leistungsfähig, aber auch sehr komplex sind [Pfi1_85]. Die große Mehrzahl der Teilnehmer ist damit gezwungen, ihren Datenschutz in wenige „fremde Hände" zu legen und genießt daneben keinen oder nur sehr ineffizienten Schutz ihres Sendens.

Man benötigt also die Verfahren aus 2.2.3 zum Schutz des Senders und Verteilung (2.2.1) zum Schutz des Empfängers.

Aus Leistungsgründen ist ein breitbandiges diensteintegrierendes Digitalnetz, in dem alle Nachrichten an alle Teilnehmerstationen verteilt werden, jedoch undenkbar. So ist es z.B. nicht nur aus Leistungs-, sondern auch aus Zuverlässigkeits- und Kostengründen nicht sinnvoll, Ringe mit mehr als 10000 Teilnehmerstationen zu bauen. Da das überlagernde Senden aufwendiger ist als das RING-Netz, dürfte die maximale Teilnehmerzahl dieses Verfahrens erst recht unter 10000 liegen. Ein breitbandiges diensteintegrierendes Digitalnetz muß folglich ab einer gewissen Größe hierarchisch unterteilt werden. Die Nachrichten werden dabei nicht an alle, sondern nur an hinreichend viele Teilnehmerstationen verteilt (multicast).

Eine mögliche effiziente Realisierung einer solchen Hierarchie ist ein *Vermittlungs-/Verteilnetz* [Pfit_83, Pfi1_83, Pfit_84]. Es besteht aus Verteilnetzen im Teilnehmeranschlußbereich und einem Vermittlungsnetz, das diese Verteilnetze verbindet (Bild 7, links).

Das Vermittlungsnetz kann dabei ohne Rücksicht auf den Datenschutz nach Leistungsgesichtspunkten gebaut werden. (In Staaten ohne Fernmeldemonopol könnten MIXe eine Alternative sein.)

Die Verteilnetze müssen somit die Hauptlast der Anonymisierungsmaßnahmen tragen. Sie können entsprechend den gegebenen Anforderungen hinsichtlich Leistung und Kosten und in Abhängigkeit von (bei der Bebauungsart des zu verkabelnden Gebietes) zu erwartenden Angreifern durch physikalische Ringe als RING-Netz oder durch überlagerndes Senden in einer dafür geeigneten Topologie realisiert werden.

Hält man das in Abschnitt 2.2.3.2 für das RING-Netz beschriebene Angreifermodell für realistisch, ist also die in Bild 7 rechts dargestellte Topologie (Ringstruktur im Teilnehmeranschlußbereich) günstig.

Genügend schnelle Übertragungssysteme zur Implementierung von Ringstrukturen sind im Laborstadium verfügbar [BeEn_85], die Realisierung eines Vermittlungs-/Verteilnetzes mit dem Verfahren des RING-Netzes also möglich. Die Ergebnisse erster Übertragungsleistungs-, Zuverlässigkeits- und Kostenuntersuchungen [Pfi1_83, Bürl_84, Bürl_85, Mann_85, Papa_84] lassen für diese Netze ein in etwa gleichgroßes Leistung/Kosten-Verhältnis wie für die üblichen reinen Vermittlungsnetze erwarten.

Möchte man auch bei Umzingelung einzelner Teilnehmerstationen den Sender von Nachrichten verbergen, muß man das in Abschnitt 2.2.3.1 beschriebene überlagernde Senden mit Hilfe paarweise gemeinsamer Schlüssel verwenden, für das es möglicherweise günstigere Topologien als Ringstrukturen im Teilnehmeranschlußbereich gibt. Außerdem ist

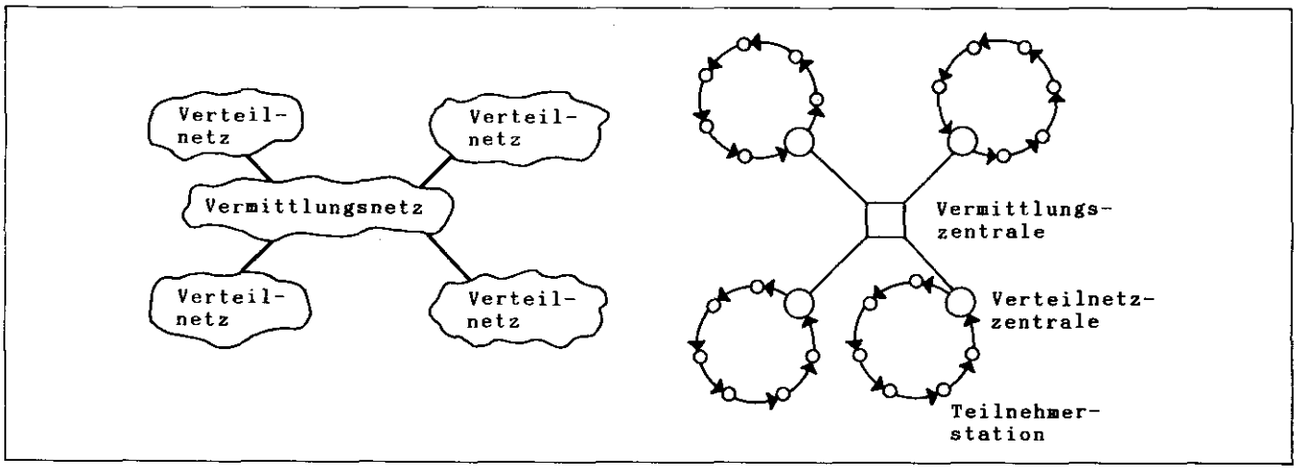


Bild 7 Allgemeine physikalische Struktur des Vermittlungs-/Verteilnetzes (links) und eine günstige Topologie (rechts)

es dann möglich, die Grenze zwischen Vermittlungsnetz und Verteilnetzen für verschieden sensitive und verschieden übertragungsaufwendige Verkehrsklassen verschieden zu wählen oder in Abhängigkeit von der Netzbelastung dynamisch zu verschieben [Pfi1_85].

Realisiert man im Teilnehmeranschlußbereich Ringe, so können die Verfahren aus Abschnitt 2.2.3 auch kombiniert werden, indem die Bandbreite jedes Ringes unter sie aufgeteilt wird.

3.2 Adressierung und Adreßverwaltung

Entsprechend der hierarchischen Struktur des Vermittlungs-/Verteilnetzes sind die verwendeten Adressen ebenfalls zweistufig: jede Nachricht enthält als Adresse eine explizite Adresse des Verteilnetzes des Empfängers und eine implizite Adresse des Empfängers innerhalb seines Verteilnetzes.

Verdeckte implizite Adressierung wird dabei nur bei öffentlichen Adressen verwendet, und diese wiederum bei breitbandigen Diensten und Telefon nur beim Kanalaufbau. Hierfür gibt es genügend schnelle Implementierungen von Kryptosystemen mit öffentlichen Schlüsseln [Rive_85]. Für die Übertragung von Folgenachrichten kann dann offene Adressierung mit privaten Adressen verwendet werden.

Es kann sinnvoll sein, die für das Vermittlungsnetz bestimmte explizite Adresse des Verteilnetzes des Empfängers für die übrigen Teilnehmerstationen des Verteilnetzes des Senders unkenntlich zu machen, etwa indem man die vollständige Adresse mit einem öffentlichen Schlüssel des Vermittlungsnetzes verschlüsselt.

3.3 Netzabschluß

Im Vermittlungs-/Verteilnetz muß jede Schutzmaßnahme, die innerhalb des Netzes angesiedelt ist, durch die Teilnehmerstationen und deren Netzabschlüsse realisiert werden. Zur Teilnehmerstation zählt man dabei die Teile, die ausschließlich unter Kontrolle der Teilnehmer stehen, während das, wofür die Post verantwortlich ist, zum Netzabschluß gerechnet wird.

Sofern die Post weiterhin für die Dienstqualität verantwortlich sein soll, bedeutet dies, daß neben dem Netzanschluß bei Verwendung des RING-Netzes auch das Zugriffsverfahren und beim überlagernden Senden zusätzlich noch die Pseudozufallszahlenerzeugung zum Netzabschluß gehören, denn sofern diese bei einem Teilnehmer Leistungs- oder Zuverlässigkeitsmängel aufweisen, sind auch alle anderen Teilnehmer desselben Verteilnetzes betroffen.

Wäre im Netzabschluß von der Post oder dem Hersteller ein „Trojanisches Pferd" untergebracht, so könnte dieses also das Senden der betroffenen Station registrieren. Man hat somit dieses Problem von den Vermittlungszentralen auf die Netzabschlüsse verlagert. Dennoch ist die Situation hier besser:

- Netzabschlüsse sind um einige Größenordnungen einfacher als Vermittlungsrechner, so daß eine Prüfung auf „Trojanische Pferde" möglich ist.
- Sie müssen nicht so häufig gewartet werden und können auch nicht so leicht ausgetauscht werden, so daß Kontrollen auf „Trojanische Pferde" nur selten nötig sind.

Um „Trojanische Pferde" ausschließen zu können, müßte man wohl die Netzabschlüsse unter öffentlicher Kontrolle nach geprüften Entwürfen herstellen.

3.4 Abrechnung

Ein diensteintegrierendes Digitalnetz muß auch die Abrechnung der Kosten für die Netzbenutzung mit dem Netzbetreiber und für die Dienstnutzung mit den Dienstanbietern ermöglichen. Bei der Organisation der Abrechnung muß darauf geachtet werden, daß durch Abrechnungsdaten die Anonymität im Netz nicht verloren geht.

Prinzipiell hat man dabei zwei Möglichkeiten: *Individuelle* Abrechnung nach Einzelnutzung (oder auch für Abonnements u.ä.) mit Verfahren, bei denen der bezahlende Teilnehmer (und ggf. auch der Zahlungsempfänger) anonym ist oder *generelle*, d.h. von allen Netzteilnehmern zu leistende, pauschale Bezahlung, die nicht anonym erfolgen muß, da dabei keine interessanten Abrechnungsdaten entstehen.

Für die erste Möglichkeit gibt es anonyme kryptographische Geldtransfersysteme, z.B. anonyme Bankschecks von David Chaum [Chau_83, Chau_84, Cha8_85, Bürk_86] und zwei auf anonymen Nummernkonten bzw. nicht manipulierbaren Zählern beruhende [Pfi1_83, Pfit_84]. Die genauen Abrechnungsprotokolle müssen dabei so entworfen werden, daß von vornherein niemand betrügen kann, da die Anonymität eine nachträgliche Strafverfolgung be- oder gar verhindert [WaPf_85].

Bei individueller Abrechnung gibt es ein von der Anonymität unabhängiges ungelöstes Problem: Da die Übertragung von Information in Zukunft sehr schnell und billig sein wird, kann man bei Diensten von hinreichend allgemeinem Interesse (z.B. Zeitungen) die Abrechnung mit dem Dienstерbringer für die Dienstbereitstellung, die für ihn nicht billiger sein wird als bisher, umgehen, indem man Information im Netz kopiert und weiterverteilt.

Dies gilt sogar für Information, die nicht im Netz angeboten wird. Alles, was ein Mensch sehen oder hören kann, kann er digital kopieren bzw. aufnehmen und dann über das Netz verteilen, z.B. gedruckte Zeitungen, Bücher oder Schallplatten. Dies verschärft das bisherige Urheberrechtsproblem mit Kopierern und Musikkassetten. Außerdem ist das Urheberrechtsproblem bezüglich für den Menschen sicht- oder hörbarer Werke schwerer zu lösen als das des Softwareschutzes, denn hier muß lediglich das Ergebnis eines Programmes wahrnehmbar sein, während man das Programm als solches oder Teile davon in einen sicheren Hardware-Modul einschließen kann.

Durch Verwendung von generellen Pauschalen vermeidet man alle Probleme bzgl. Betrugssicherheit.

Sobald genügend Bandbreite zur Verfügung steht, ist z.B. eine pauschale Gebühr an den Netzbetreiber für schmalbandiges Senden und Fernsehempfang möglich.

Wollte man jedoch, um das obige Problem des Weiterkopierens zu umgehen, auch für die gesamte Nutzung von Informationsdiensten eine generelle Pauschale erheben, so müßte man ein Verfahren finden, nach dem die von einer GEZ-ähnlichen Organisation eingezogenen Gebühren „gerecht" auf die verschiedenen Anbieter verteilt würden.

Dieses müßte die unterschiedlichen, von der Qualität, nicht aber von der Nachfrage abhängigen Bereitstellungs-

kosten der Anbieter von Diensten berücksichtigen, ohne jedoch Meinungszensur zu betreiben oder bestehende Märkte festzuschreiben und damit letztendlich den Informationspluralismus zu gefährden. Ein solches Verfahren ist uns nicht bekannt.

3.5 Weitere höhere Protokolle

Auf einem anonymen Netz sind beliebige, auch nicht anonyme Kommunikationsformen realisierbar. Fast alle Verfahren, sich über ein Netz einander zu erkennen zu geben (d.h. sich zu authentizieren), machen bereits heute keinen Gebrauch davon, daß man dem Netz gegenüber identifizierbar ist. Zum Beispiel erkennt man Telefonpartner an ihrer Stimme und Sprechweise sowie ihrem Wissen, Briefpartner an ihrer (Unter-)Schrift. Da es für beides digitale Entsprechungen gibt, können übliche Authentikationsprotokolle weiterverwendet werden [DaPr_84].

Es sei angemerkt, daß man auch bei vielen Kommunikationsarten (z.B. Bürger bei Ämtern), bei denen man heute namentlich auftreten muß, die Möglichkeit zur anonymen Kommunikation nutzen und unter verschiedenen Pseudonymen auftreten kann, wenn man ein Verfahren hat, um Dokumente, die auf eines dieser Pseudonyme lauten, in sicherer und anonymer Weise auf ein anderes eigenes Pseudonym umzuformen [Chau_84, Cha8_85].

4 Resümee

Breitbandige diensteintegrierende Digitalnetze, die auch Interessens- und Verkehrsdaten (vgl. 1.2) in überprüfbarer Weise schützen, benötigen auf jeden Fall eine passende physische Netzstruktur.

Ohne Verteilnetze im Teilnehmeranschlußbereich scheint ein Schutz der Empfänger unmöglich zu sein. Dies bedeutet, daß hier Leitungen mit sehr hoher Bandbreite benötigt werden. Verwendet man RING-Netze zum Schutz des Senders, so ist zusätzlich die Topologie des Netzes (Ringe im Teilnehmeranschlußbereich) vorgegeben.

Solche Netze sind realisierbar, und es ist ein etwa gleichgroßes Leistung/Kosten-Verhältnis wie für die üblichen reinen Vermittlungsnetze zu erwarten.

In gewissem Sinne ist das Problem, die Verkehrs- und Interessensdaten zu schützen, beim Entwurf eines Netzes also dringender als die Probleme des Schutzes der Nutzdaten und der Authentikation, mit denen sich die öffentliche Diskussion zur Zeit hauptsächlich beschäftigt. Letztere lassen sich auf jeder Netzstruktur im nachhinein durch kryptographische Verfahren lösen, während ersteres bereits beim Entwurf berücksichtigt werden muß.

Für ihre Kritik und Diskussionsbereitschaft danken wir Klaus Echtle, Prof. Winfried Görke und Prof. Detlef Schmid.

5 Literatur

Abbr_84 C. R. Abbruscato: Data Encryption Equipment; IEEE Communications Magazine Vol. 22, No. 9, September 1984, Seite 15 bis 21

BeEn_85 Larry A. Bergman, Sverre T. Eng: A Synchronous Fiber Optic Ring Local Area Network for Multigigabit/s Mixed-Traffic Communication; IEEE Journal on Selected Areas in Communications Vol. SAC-3, No. 6, November 1985, Seite 842 bis 848

BfD_85 Dr. Reinhold Baumann: Siebter Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz, gemäß Par. 19 Absatz 2 Satz 2 Bundesdatenschutzgesetz dem Deutschen Bundestag vorgelegt zum 1. Januar 1985, als Bundestags-Drucksache 10/2777 veröffentlicht

BlMi_84 Manuel Blum, Silvio Micali: How to Generate Cryptographically Strong Sequences of Pseudo-Random Bits; SIAM J. Comput. Vol. 13, No. 4, November 1984, Seite 850 bis 864

Brau_82 Ewald Braun: BIGFON – der Start für die Kommunikationstechnik der Zukunft; telcom report Band 5, Heft 2, 1982, Seite 123 bis 129

Brau_83 Ewald Braun: BIGFON – Erprobung der optischen Breitbandübertragung im Ortsnetz; telcom report Band 6, Heft 2, April 1983, Seite 52 bis 53

Bürk_86 Holger Bürk: Digitale Zahlungssysteme und betrugssicherer, anonymer Wertetransfer; Studienarbeit am Institut für Informatik IV, Universität Karlsruhe, April 1986

Bürl_84 Gabriele Bürle: Leistungsvergleich von Sternnetz und Schieberegister-Ringnetz; Studienarbeit am Institut für Informatik IV, Universität Karlsruhe, 1984

Bürl_85 Gabriele Bürle: Leistungsbewertung von Vermittlungs-/Verteilnetzen; Diplomarbeit am Institut für Informatik IV, Universität Karlsruhe, Mai 1985

Chau_81 David Chaum: Untraceable Electronic Mail, Return Adresses, and Digital Pseudonyms; CACM Vol. 24, Nu. 2, February 1981, Seite 84 bis 88

Chau_83 David Chaum: Blind Signatures for Untraceable Payments; Advances in Cryptology, Proceedings of Crypto 82, A Workshop on the Theory and Application of Cryptographic Techniques, August 23–25, 1982, University of California, Santa Barbara, Edited by David Chaum, Ronald L. Rivest, and Alan T. Sherman, Plenum Press, New York, 1983, Seite 199 bis 203

Chau_84 David Chaum: A New Paradigm for Individuals in the Information Age; Proceedings of the 1984 Symposium on Security and Privacy, IEEE, April 29 – May 2 1984, Oakland, California, Seite 99 bis 103

Cha3_85 David Chaum: The Dining Cryptographers Problem. Unconditional Sender Anonymity; Draft, received May 13, 1985

Cha8_85 David Chaum: Security without Identification: Transaction Systems to make Big Brother Obsolete; CACM Vol. 28, Nu. 10, October 1985, Seite 1030 bis 1044

DaPr_84 D. W. Davies, W. L. Price: Security for Computer Networks, An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer; John Wiley & Sons, Chichester, New York, 1984

Denn_82 Dorothy E. Denning: Cryptography and Data Security; Addison-Wesley Publishing Company, Reading, Mass., 1982

DESi_84 Ein Schlüssel gegen Daten-Diebe; Peripherie-IC zur Ver- und Entschlüsselung von Daten für Massenspeicher und Übertragung; Markt&Technik Nr. 3 vom 20. Januar 1984, Seite 22 bis 26

Eck_85 Wim van Eck: Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?; Computers & Security Vol. 4, Nu. 4, December 1985, Seite 269 bis 286

Höck_85 Gunter Höckel: Untersuchung der Datenschutzeigenschaften von Ringzugriffsmechanismen; Diplomarbeit am Institut für Informatik IV, Universität Karlsruhe, August 1985

HöPf_85 Gunter Höckel, Andreas Pfitzmann: Untersuchung der Datenschutzeigenschaften von Ringzugriffsmechanismen; Proceedings der 1. GI Fachtagung Datenschutz und Datensicherung im Wandel der Informationstechnologien, München, Oktober 1985, herausgegeben von P. P. Spies, Informatik-Fachberichte Band 113, Springer-Verlag Heidelberg, Seite 113 bis 127

Home_?? Homer: Illias

Horg_85 John Horgan: Thwarting the information thieves; IEEE Spectrum Vol. 22, Nu. 7, July 1985, Seite 30 bis 41

Hors_85 Patrick Horster: Kryptologie; Reihe Informatik/47, herausgegeben von K. H. Böhling, U. Kulisch, H. Maurer, Bibliographisches Institut, Mannheim, 1985

Hor2_85 John Horgan: Inventor seeks to warn Government of threat from laser-based bug; The Institute, IEEE, October 1985, Seite 8

KaRS_85 Burt S. Kaliski, Ronald L. Rivest, Alan T. Sherman: Is the Data Encryption Standard a Group; Preliminary Draft, April 6, 1985, paper presented at Eurocrypt '85, Linz, Austria

Leuz_83 Ruth Leuze: Datenschutz für unsere Bürger; 4. Tätigkeitsbericht der Landesbeauftragten für den Datenschutz, 1983

Leuz_84 Ruth Leuze: Datenschutz für unsere Bürger; 5. Tätigkeitsbericht der Landesbeauftragten für den Datenschutz, 1984

Loep_85 Keith Loepere: Resolving Covert Channels Within a B2 Class Secure System; acm Operating Systems Review Vol. 19, Nu. 3, July 1985, Seite 9 bis 28

Mann_85 Andreas Mann: Fehlertoleranz und Datenschutz in Ringnetzen; Diplomarbeit am Institut für Informatik IV, Universität Karlsruhe, Oktober 1985

Papa_84 Petros Papadimitriou: Kürzeste Ringstrukturen und Kostenvergleich zu Sternstrukturen bei Kommunikationsnetzen; Studienarbeit am Institut für Informatik IV, Universität Karlsruhe, Dezember 1984

Pfit_83 Andreas Pfitzmann: Ein Vermittlungs-/Verteilnetz zur Erhöhung des Datenschutzes in Bildschirmtext-ähnlichen Neuen Medien; GI '83 13. Jahrestagung der Gesellschaft für Informatik, 3. bis 7. Oktober 1983, Universität Hamburg, Informatik-Fachberichte Band 73, Springer-Verlag Heidelberg, Seite 411 bis 418

Pfit_84 Andreas Pfitzmann: A switched/broadcast ISDN to decrease user observability; 1984 International Zurich Seminar on Digital Communications, Applications of Source Coding, Channel Coding and Secrecy Coding, March 6–8, 1984, Zurich, Switzerland, Swiss Federal Institute of Technology, Proceedings IEEE Catalog no. 84CH1998-4, Seite 183 bis 190

Pfit_85 Andreas Pfitzmann: Technischer Datenschutz in diensteintegrierenden Digitalnetzen – Problemanalyse, Lösungsansätze und eine angepaßte Systemstruktur; Proceedings der 1. GI Fachtagung Datenschutz und Datensicherung im Wandel der Informationstechnologien, München, Oktober 1985, herausgegeben von P. P. Spies, Informatik-Fachberichte Band 113, Springer-Verlag Heidelberg, Seite 96 bis 112

Pfi1_83 Andreas Pfitzmann: Ein dienstintegriertes digitales Vermittlungs-/Verteilnetz zur Erhöhung des Datenschutzes; Fakultät für Informatik, Universität Karlsruhe, Interner Bericht 18/83, Dezember 1983

Pfi1_85 Andreas Pfitzmann: How to implement ISDNs without user observability – Some remarks; Fakultät für Informatik, Universität Karlsruhe, Interner Bericht 14/85

PfWa_85 Andreas Pfitzmann, Michael Waidner: Networks without user observability – design options; Eurocrypt 85, A Workshop on the Theory and Application of Cryptographic Techniques, April 9–11, 1985, Johannes-Kepler-University, Linz, Austria, IACR – International Association for Cryptologic Research, Franz Pichler, Thomas Beth (eds.), LNCS Springer-Verlag; überarbeitete und erweiterte Fassung erscheint in Computers & Security, North Holland

PoKl_78 G. J. Popek, C.S. Kline: Issues in Kernel Design; Operating Systems, An Advanced Course, Edited by R. Bayer, R. M. Graham, G. Seegmüller; Lecture Notes in Computer Science LNCS 60, 1978; Nachgedruckt als Springer Study Edition, 1979; Springer-Verlag, Heidelberg, Seite 209 bis 227

Riha_85 Karl Rihaczek: Datenmißbrauch: Verhindern besser als verbieten; Proc. 1. GI Fachtagung Datenschutz und Datensicherung im Wandel der Informationstechnologien; München, Okt. 1985, IFB 113, Springer-Verlag Heidelberg, Seite 229 bis 236

Rive_85 Ronald L. Rivest: RSA Chips (Past/Present/Future); Advances in Cryptology, Proceedings of EUROCRYPT 84, A Workshop on the Theory and Application of Cryptographic Techniques, April 9–11, 1984, Paris, France, Edited by T. Beth, N. Cot and I. Ingemarsson, Lecture Notes in Computer Science LNCS 209, Springer-Verlag Heidelberg, 1985, Seite 159 bis 165

Rose_85 K. H. Rosenbrock: ISDN – Die folgerichtige Weiterentwicklung des digitalisierten Fernsprechnetzes für das künftige Dienstleistungsangebot der Deutschen Bundespost; GI/NTG-Fachtagung „Kommunikation in Verteilten Systemen – Anwendungen, Betrieb und Grundlagen –", 11.–15. März 1985, Tagungsband 1, D. Heger, G. Krüger, O. Spaniol, W. Zorn (Hrsg.), Informatik-Fachberichte IFB 95, Springer-Verlag Heidelberg, Seite 202 bis 221

Schö_84 Helmut Schön: Die Deutsche Bundespost auf ihrem Weg zum ISDN; The Deutsche Bundespost on its Way towards the ISDN; Zeitschrift für das Post- und Fernmeldewesen Heft 6 vom 27. Juni 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

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

Steg_85 H. Stegmeier: Einfluß der VLSI auf Kommunikationssysteme; GI/NTG-Fachtagung „Kommunikation in Verteilten Systemen – Anwendungen, Betrieb und Grundlagen –", 11.–15. März 1985, Tagungsband 1, D. Heger, G. Krüger, O. Spaniol, W. Zorn (Hrsg.), Informatik-Fachberichte IFB 95, Springer-Verlag Heidelberg, Seite 663 bis 672

Tane_81 Andrew S. Tanenbaum: Computer Networks; Prentice-Hall, Englewood Cliffs, N. J., 1981

Thom_84 Ken Thompson: Reflections on Trusting Trust; CACM, Vol. 27, No. 8, August 1984, Seite 761 bis 763

VaVa_85 Umesh V. Vazirani, Vijay V. Vazirani: Efficient and Secure Pseudo-Random Number Generation (extended abstract); Advances in Cryptology, Proceedings of Crypto 84, A Workshop on the Theory and Application of Cryptographic Techniques, August 19–22, 1984, University of California, Santa Barbara, Edited by G. R. Blakley and David Chaum, Lecture Notes in Computer Science LNCS 196, Springer-Verlag Heidelberg, 1985, Seite 193 bis 202

VoKe_83 Victor L. Voydock, Stephen T. Kent: Security Mechanisms in High-Level Network Protocols; acm computing surveys Vol. 15, No. 2, June 1983, Seite 135 bis 171

Waid_85 Michael Waidner: Datenschutz und Betrugssicherheit garantierende Kommunikationsnetze. Systematisierung der Datenschutzmaßnahmen und Ansätze zur Verifikation der Betrugssicherheit; Diplomarbeit am Institut für Informatik IV, Universität Karlsruhe, August 1985, Interner Bericht 19/85 der Fakultät für Informatik

WaPf_85 Michael Waidner, Andreas Pfitzmann: Betrugssicherheit trotz Anonymität. Abrechnung und Geldtransfer in Netzen; Proceedings der 1. GI Fachtagung Datenschutz und Datensicherung im Wandel der Informationstechnologien, München, Oktober 1985, herausgegeben von P. P. Spies, Informatik-Fachberichte Band 113, Springer-Verlag Heidelberg, Seite 128 bis 141; Überarbeitung erschien in „DuD, Datenschutz und Datensicherung, Informationsrecht, Kommunikationssysteme", Vieweg & Sohn, Braunschweig, Heft 1, Februar 1986, Seite 16 bis 22