Hannes Federrath, Oliver Berthold, Marit Köhntopp, Stefan Köpsell

c't 16/2000

Tarnkappe für das Internet

Verfahren zur anonymen und unbeobachtbaren Kommunikation

Anonymitätsdienste wie Anonymizer, Rewebber oder Freedom erfreuen sich immer größerer Beliebtheit bei Surfern, die dem Datensammeln kommerzieller Dienste wie DoubleClick ein Schnippchen schlagen wollen. Dabei verwenden die Anonymisierer Verfahren, die sehr unterschiedlich in ihrem erreichbaren Schutz gegen Datensammeln und Überwachung sind. Es lohnt sich also, etwas genauer hinzuschauen, wenn man sich ernsthaft gegen neugierige Blicke aus dem Internet schützen will.

Ich habe nichts zu verbergen

Ein oft gehörte Aussage ist, man »habe ja nichts zu verbergen«. Warum also E-Mails verschlüsseln oder in Formularen auf Webseiten falsche Angaben machen? »Gut, Sie haben nichts zu verbergen. Aber warum hat Ihr Bad dann eine Tür, wo doch jeder weiß, was Sie dahinter wahrscheinlich tun?« Dass es so etwas wie Privatheit tatsächlich geben sollte, ist unbestritten und zudem in vielen Ländern der Erde gesetzlich verankert. Diese Regeln gelten natürlich auch im Internet, nur scheinen das die professionellen Datensammler entweder noch nicht bemerkt zu haben, oder die Gesetze sind für sie nicht anwendbar, z.B. weil sie in einem anderen Staat auf anderen rechtlichen Grundlagen arbeiten.

In diesem Beitrag geht es darum, wie sich ein Benutzer vor Beobachtung schützen kann: Manche Internet-Dienste möchte man anonym benutzen, ohne seine Identität preiszugeben. Kommunikationsereignisse, die von einem Benutzer ausgehen oder ihn erreichen, sollen vor anderen unbeobachtbar bleiben (zu den Begriffen Anonymität und Unbeobachtbarkeit siehe Kasten 1). Mögliche Beobachter können andere Benutzer des Internet sein, der eigene Internet Service Provider (ISP), Betreiber von Routern, die die jeweiligen Datenpakete durchleiten, oder auch externe Beobachter. Selbst wenn der Benutzer keine weiteren Erkennungsmerkmale (z.B. Cookies) akzeptiert oder selbst preisgibt, sind zumindest alle Datenpakete zu seiner IP-Nummer verkettbar. Bei fest zugewiesenen IP-Nummern kann jeder Beobachter, der die Zuordnung zwischen Benutzername und IP-Nummer kennt, exakte Benutzungsprofile erstellen. Um diese Zuordnung festzustellen, genügt es dem Beobachter bereits, eine E-Mail vom beobachteten Benutzer empfangen zu haben, da diese die IP-Nummer seines Rechners enthält. Hat der Beobachter dann noch Zugriff auf die Logdateien eines Web- oder Terminalservers, kann er diese nach der IP-Nummer durchsuchen, um das genaue Surfverhalten des Benutzers festzustellen. Bei dynamisch zugewiesenen IP-Nummern, wie sie für den Privatanwender heute bei den meisten ISPs üblich sind, reduziert sich die Beobachtbarkeit zunächst auf den eigenen ISP. Dieser weiß natürlich genau, welchem Benutzer er welche IP-Nummer zugewiesen hat, und er wird in der Regel auch eine Logdatei darüber führen. Solange der Benutzer seinem eigenen Provider vertraut, dass dieser die Daten gegen unbefugte Zugriffe schützt, nicht weitergibt und nicht selbst zur Beobachtung verwendet, der Benutzer Cookies abschaltet und auch sonst keine identifizierenden Daten an fremde Server übergibt, kann Entspannung eintreten. Die hierfür erforderliche Disziplin und Vorsicht ist aber selbst für hart gesottene Nutzer auf Dauer nicht durchzuhalten. Zudem erkennen die Datensammler gerade die ISPs mehr und mehr als Zielgruppe für ihre Sammelsoftware.

Mit Produkten wie Predictive Networks (http://www.predictivenetworks.com/) kann die Sammelwut zukünftig »vor Ort« [1] betrieben werden, was dem ISP auf alle Fälle Nebeneinnahmen beschert. Natürlich können die Kunden stets widersprechen, dass ihre Kommunikationsprofile erstellt und ausgewertet werden. Zumindest europäische Provider dürften dies dann nicht in Verbindung mit identifizierenden Kundendaten tun. Es ist bereits gesetzlich vorgesehen, daß jeder Provider den staatlichen Stellen eine Abhörschnittstelle zur Verfügung stellen muß: § 88 Telekommunikationsgesetz (TKG). Niemand kann jedoch garantieren, das diese Möglichkeit, die Leitungen zu belauschen, nicht mißbraucht wird (z.B. von der organisierten Kriminalität). Es gibt jedoch Verfahren, die trotzdem die

im Teledienstedatenschutzgesetz (TDDSG) geforderte anonyme Nutzung von Telediensten ermöglichen. Aus Benutzersicht sollte man daher lieber gleich Prävention betreiben — Vertrauen ist gut, Vorsorge ist besser.

Anon-Proxies

Die einfachste, schnellste, leider aber auch stark eingeschränkte Möglichkeit, sich vor Beobachtung seiner Kommunikationsbeziehungen zu schützen, sind so genannte Anon-Proxies [2]. Für das World Wide Web haben solche Systeme, z.B. Anonymizer (http://www.anonymizer.com) oder Rewebber (http://www.rewebber.com), bereits einen recht hohen Bekanntheitsgrad erlangt. Ihr größter Vorteil besteht darin, dass auf dem eigenen PC keine zusätzlichen Programme installiert werden müssen: Es wird im Web-Browser einfach die URL des Anon-Proxy aufgerufen und in das angezeigte Formularfeld die gewünschte Adresse eingetragen. Der Proxy ruft die Daten in seinem eigenen Namen ab, so als wäre er der Benutzer. Damit der Surfer alle Links, die auf der gewünschten Webseite vorhanden sind, bequem anklicken kann, ohne dabei beobachtet zu werden, analysiert der Anon-Proxy die Seite nach allen Links und Bildern, lädt die Bilder ebenfalls in seinem eigenen Namen und ersetzt die Links durch einen kryptischen Link, der wieder auf den Anon-Proxy verweist. Zusätzlich werden teilweise Cookies, JavaScript, ActiveX und andere »gefährliche Inhalte« gefiltert, die die IP-Adresse des Benutzers über Umwege enttarnen könnten. Anon-Proxies haben drei strukturelle Nachteile. **Erstens** schützen sie nicht vor dem Betreiber des Anon-Proxies, d.h. dieser weiß genau, welche IP-Nummer sich hinter dem Request verbirgt. Es ist deshalb nur eine Frage der Zeit, bis die Datensammler die »Gratis-Sammelstelle« Anon-Proxy für sich entdecken und selbst solche »Anonymisierungsdienste« betreiben. **Zweitens**, und spätestens hier trennt sich die Spreu vom Weizen, müssen Anon-Proxies beim Analysieren und Filtern der Webseiten eine Abwägung zwischen Erscheinungsbild und Sicherheit vornehmen: Werden zu viele Inhalte, Tags und Formate gefiltert, wirkt die Seite langweilig wie aus den Anfangszeiten des Web, sozusagen reduziert auf ihren textuellen Inhalt. Erlaubt man mehr Inhalte, Tags und Formate, kann dem Analyseprogramn schonmal ein gefährlicher Inhalt durch die Lappen gehen, der dann dazu führt, dass der PC dem Server doch seine IP-Nummer preisgibt [3,4]. **Drittens** helfen Anon-Proxies nichts gegen professionelle Überwacher. Warum, soll am Beispiel eines Big Brothers erklärt werden.

Big Brother und die Unbeobachtbarkeit

Gegen einen Big Brother bieten Anon-Proxies keinen ausreichenden Schutz: Ein Überwacher, der große Teile des Netzes beobachtet, weiß (zumindest theoretisch) genau, zu welchem Zeitpunkt ein Request in den Anon-Proxy eingegangen ist. Da der Proxy den eingehenden Request sofort bearbeitet, d.h. den Zugriff auf die gewünschte Adresse ausführt, kann der Big Brother beides leicht miteinander verketten.

Gegen diese Beobachtung hilft selbst Verschlüsselung nicht, da die zeitliche Zusammengehörigkeit nach wie vor beobachtbar bleibt. Eine Verschlüsselung zwischen Benutzer und Proxy sowie zwischen Proxy und Zielserver verbirgt zwar vor fremden Blicken, für welche Inhalte (z.B. welche Webseiten) sich der Benutzer interessiert. Aber die Kommunikationsbeziehung, d.h. welcher Webserver aufgerufen wird, ist trotzdem beobachtbar. Das ist nicht unbedingt ein Grund zur Resignation, denn es gibt Verfahren, die es auch dem Big Brother schwer machen. Um es vorweg zu schicken: Diese Systeme sind heute ausgenommen für E-Mail noch nicht komfortabel und zuverlässig benutzbar, da sie gerade erst entwickelt werden. Dabei basieren die Verfahren, mit denen Kommunikationsbeziehungen verschleiert werden, auf wissenschaftlichen Erkenntnissen, die teilweise knapp 20 Jahre zurückliegen.

Anonymität und Unbeobachtbarkeit

Für einen Benutzer des Internet sollte es — wie im »wirklichen Leben« — die Möglichkeit geben, wann immer er es wünscht, seine Identität vor Anderen zu verbergen, d.h. seine Anonymität zu wahren. Wer einen Laden betritt, um sich nur zu informieren, stellt sich dem Verkaufspersonal auch nicht mit vollem Namen und Adresse vor, sondern bleibt zunächst anonym. Ein Besuch eines Internet-Shops beginnt meist mit dem Übermitteln eines Cookies. Auf jeden Fall aber hinterlässt der Besucher bereits mit dem ersten Klick seine Internet-Adresse.
Bei *anonymer* Kommunikation verbirgt ein Kommunikationspartner seine Identität vor den anderen Kommunikationspartnern. Bei *unbeobachtbarer* Kommunikation kennen sich möglicherweise die Kommunikationspartner, allerdings kann niemand, nicht einmal die Betreiber des Kommunikationsnetzes, feststellen, dass die Kommunikationspartner tatsächlich miteinander kommunizieren.
Auch für Unbeobachtbarkeit findet man Anwendungen im wirklichen Leben: Firmen möchten möglichst unbeobachtbar Patentrecherchen betreiben, um eigene Forschungen und Entwicklungen vor der Konkurrenz geheimzuhalten. Beratungsstellen sollten aufgesucht werden können, ohne dabei Datenspuren beim Netzbetreiber zu hinterlassen.

Mixe für Internetverbindungen

Eines der ersten Verfahren für das unbeobachtbare Versenden und Empfangen von E-Mails sind die Mixe, die auf den amerikanischen Kryptographen David Chaum [5] zurückgehen. Mixe sind eine Art hintereinander geschaltete Anon-Proxies. Viele verschlüsselt ankommende E-Mails werden im Mix verwürfelt, in ihrem Aussehen verändert und schließlich wieder ausgegeben. Selbst wenn Big Brother alle Ein- und Ausgänge eines Mix beobachtet, verliert er die Zuordnung, welche ausgehende Mail zu welcher eingehenden Mail gehört. Die Funktionsweise eines Mix gleicht einem Postamt, das jeden eingehenden Brief öffnet und darin wieder einen verschlossenen Briefumschlag vorfindet, den es an die darauf stehende Adresse, meist wieder ein Postamt, weiterleitet. Das nächste Postamt verfährt ebenso, bis der Brief entsprechend verzögert schließlich beim Empfänger landet. In der Welt des Internet sind die Briefe die Datenpakete und die Postämter die Mixe. Damit diese Weiterleitung klappt, muss der Absender natürlich die Datenpakete entsprechend vorbereiten, d.h. sie verpacken (verschlüsseln), adressieren (mit der Adresse des Empfängers), frankieren, wieder verpacken, adressieren (diesmal mit der Adresse des letzen Postamts), frankieren usw. Dies muss unbedingt auf dem PC des Benutzers geschehen, damit niemand sonst mitbekommt, welche Adressen auf den inneren Datenpaketen steht.

Chaum ging bei der Entwicklung der Mixe davon aus, dass der Beobachter das gesamte Netz überwacht und zusätzlich einen Großteil der Mixe kontrolliert. Damit eine Nachricht unbeobachtbar durch das Kommunikationsnetz transportiert wird, muss lediglich ein einziger Mix vertrauenswürdig sein. Schließlich könnte Big Brother ja selbst viele Postämter betreiben. Würde der Benutzer nur einen Mix verwenden bzw. nur Mixe benutzen, die von genau einem Betreiber verwaltet werden, käme das wieder einer »frei Haus« Lieferung des persönlichen Benutzungsprofils gleich. Als Grundregel für ein praktisches System gilt: Es müssen wenigstens zwei Mixe verwendet werden, damit weder der eine noch der andere Mix alles über die Kommunikationsbeziehung erfährt: Der erste Mix weiß, welcher Benutzer einen Request absendet und dass er ihn an einen Mix weiterleiten muss. Der zweite bzw. letzte Mix weiß, wohin ein Request gesendet werden soll, aber nicht, bei welchem Benutzer er seinen Ursprung hat. Solange die beiden Mixe nicht zusammenarbeiten, bleibt die Kommunikationsbeziehung vor allen Außenstehenden und sogar vor den Betreibern der Mixe verborgen.

In der Praxis wird man natürlich mehr als zwei Mixe verwenden, wobei jeder Mix von einer anderen Institution betrieben wird, die möglichst wenig gemeinsame Interessen mit den anderen Betreibern hat, so dass eine Enttarnung der Benutzer unwahrscheinlich ist. Die Anzahl der Mixe, für die sich ein Benutzer entscheidet, hängt letztendlich von so genannten Vertrauensfaktoren ab. Diese sind aber sozialer Natur und entziehen sich daher einer technischen Beschreibung. Es spielt für die erreichbare Unbeobachtbarkeit aus technischer Sicht keine Rolle, ob in einer Mix-Kette mit 5 Mixen genau 0, 1, 2, 3 oder 4 Mixe korrupt sind, solange wenigstens ein Mix vertrauenswürdig ist. Viel hilft also nicht unbedingt viel; besser ist es, die Betreiber der Mixe sorgfältig auszuwählen, damit diese nicht mit vereinten Kräften an der Enttarnung ihrer Benutzer arbeiten.

Solche Mix-Betreiber könnten z.B. sein: Datenschutzbeauftragte des Bundes und der Länder, Bürgernetzvereine, kirchliche Organisationen und insbesondere Institutionen, deren Geschäftsfeld typischerweise Diskretion erfordert, z.B. Banken, Beratungsstellen oder die Post. Erste Ansätze hierzu gibt es bereits. In enger Zusammenarbeit zwischen der Technischen Universität Dresden und dem Landesbeauftragten für den Datenschutz Schleswig-Holstein wird derzeit am Aufbau eines Dienstes gearbeitet, mit dem sich der gewöhnliche Surfer vor dem Big Brother schützen kann (Kasten 2).

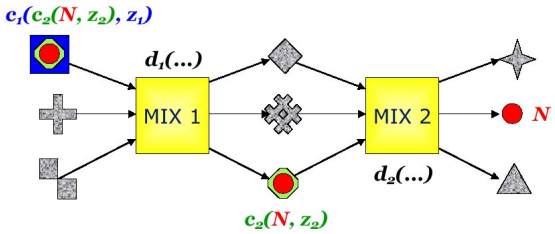
Da sich die Mixe an unterschiedlichen physischen Orten befinden und von unabhängigen Betreibern angeboten werden, ist die Chance, dass doch alle Mixe mit dem Beobachter zusammenarbeiten, sehr gering. In jedem Fall muss aber der Benutzer wesentlich weniger Vertrauen in den einzelnen Betreiber eines Mixes investieren, als dies bei den Anon-Proxies nötig ist. Schließlich kann nicht einmal ein Mix feststellen, welcher Benutzer mit welchem Server kommuniziert.

Im folgenden werden der Aufbau und das Funktionsprinzip des Mix-Netzes erklärt. Ein Mix-Netz besteht aus einer Folge von Rechnern, den Mixen, die beispielsweise über das Internet verbunden sind. Die Mixe verarbeiten Nachrichten dabei schubartig, wobei ein Schub aus allen von den Teilnehmern innerhalb einer bestimmten Zeit gesendeten Nachrichten besteht. Die Nutzer des Mix-Netzes senden ihre Nachrichten an den ersten Mix, dieser schickt alle Nachrichten an den zweiten Mix und so fort. Der letzte Mix der Folge sen-

det die Nachrichten dann jeweils an den eigentlichen Zielrechner. Damit verhindert wird, dass ein Beobachter, der die Datenleitungen abhören kann, den Weg einer Nachricht verfolgt, muss sie mehrfach verschlüsselt werden. Der Sender verschlüsselt jede zu sendende Nachricht so, dass sie nur dann entschlüsselt und damit der Empfänger ermittelt werden kann, wenn sie von allen zu verwendenden Mixen in der vom Sender vorgesehenen Reihenfolge entschlüsselt wurde.

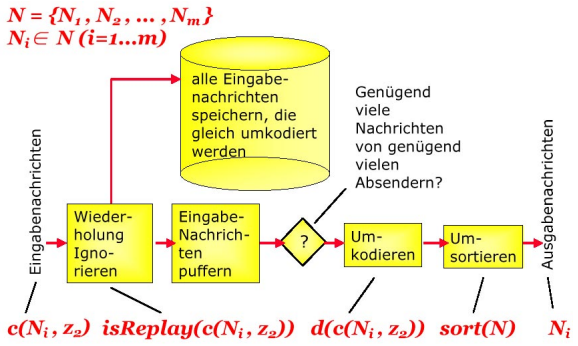
Dies geschieht nach folgendem Schema (siehe Postamtbeispiel oben): Der Sender verschlüsselt die Nachricht zunächst für den letzten Mix, so dass nur dieser sie lesen kann. Das Ergebnis dieser Verschlüsselung wird nun erneut verschlüsselt, diesmal jedoch für den vorletzten Mix. Nun wird das Ergebnis für den vorvorletzten Mix verschlüsselt und so fort, bis letztendlich eine Verschlüsselung für den ersten Mix durchgeführt wird.

Die so vorbereitete Nachricht wird an den ersten Mix gesendet. Nur er kann sie entschlüsseln und verschickt das Ergebnis dieser Entschlüsselung an den zweiten Mix. Dabei handelt es sich um eine Nachricht, die nur der zweite Mix entschlüsseln kann. Die entschlüsselte Botschaft schickt er weiter an den dritten Mix und so weiter.



Ein Beobachter, der alle Leitungen eines Mixes belauscht, sieht, wie verschlüsselte Nachrichten den Mix erreichen und wieder verlassen. Da der Mix aber eine Umkodierung (Entschlüsselung) durchgeführt hat, ist es dem Beobachter nicht möglich, eine Beziehung zwischen eingehenden und ausgehenden Nachrichten herzustellen. Eine Zuordnung der Nachricht ist insbesondere deshalb nicht möglich, da immer mehrere Nachrichten von unterschiedlichen Teilnehmern schubweise bearbeitet und im Mix *umsortiert* werden. Daher die Bezeichnung »Mix«. Ein Beobachter kann also nicht davon ausgehen, das z.B. die dritte eingehende Nachricht zu der dritten vom Mix gesendeten Nachricht gehört.

Die mehrfache Verschlüsselung und die Umsortierung reichen jedoch noch nicht aus. So müssen alle von den Teilnehmern eines Mix-Netzes gesendeten Nachrichten die *gleiche Länge* haben. Ansonsten wäre es einem Beobachter möglich, den Weg der Nachricht durch das Netz nur aufgrund ihrer Größe zu bestimmen, da er sie anhand dieses Merkmals von allen anderen Nachrichten unterscheiden kann.

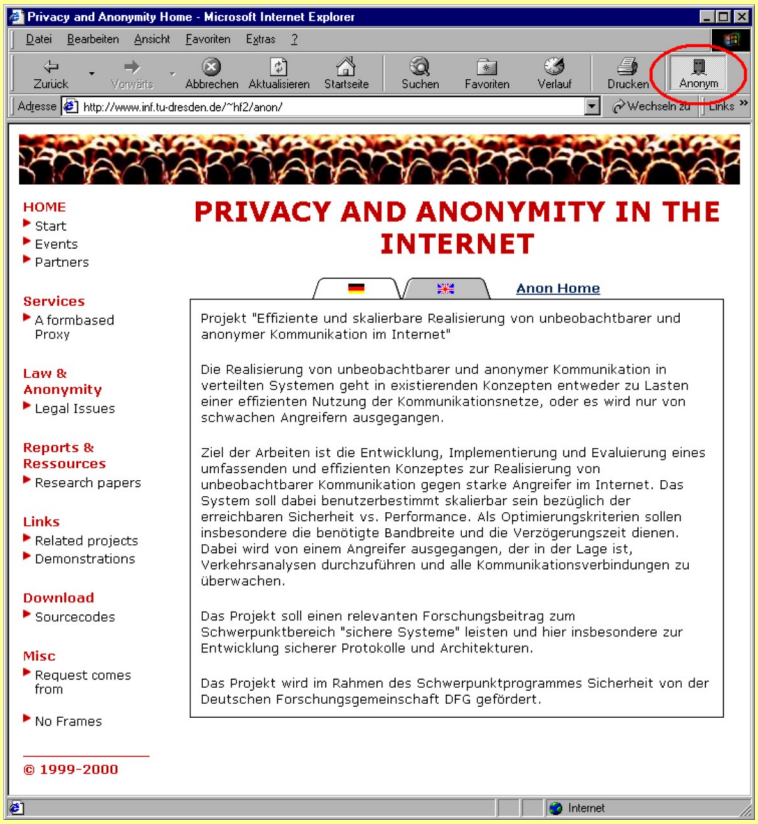


Es ist außerdem wichtig, dass die Teilnehmer eines Mix-Netzes auch dann Daten senden, wenn sie eigentlich keine Nachrichten übermitteln wollen. Diese Leernachrichten werden als *Dummy-Traffic* bezeichnet. Ohne ihn wäre es einem Beobachter ebenfalls möglich, die Kommunikationsbeziehung aufzudecken: Da er das Netz überwacht, bemerkt er, wenn ein Teilnehmer aufhört zu senden und gleichzeitig ein vom letzten Mix adressierter Rechner keine Daten mehr empfängt.

Mixe müssen sich auch gegen sogenannte *Replay-Attacken* schützen. Dabei zeichnet der Beobachter eine Nachricht auf und spielt sie später noch einmal ein, so dass dem Mix eine bereits versendete Nachricht zur erneuten Bearbeitung vorgelegt wird. Der Mix führt die Entschlüsselung durch und sendet das Ergebnis weiter. Dabei entsteht eine zur ursprünglichen Verarbeitung identische Nachricht. Vergleicht ein Beobachter nun die Ausgaben des Mixes, kann er die wiederholt gesendete Nachricht entdecken, da nur sie in beiden Ausgaben vorhanden ist. Er hat somit diesen Mix überbrückt. Um solche Replay-Angriffe zu verhindern, besitzt jeder Mix eine Datenbank, in der er bereits bearbeitete Nachrichten speichert. Genau genommen speichert er nicht die Nachricht selbst, sondern nur einen aus der Nachricht berechneten »Fingerabdruck«, der diese Nachricht eindeutig identifiziert. Wird dem Mix nun eine Nachricht zur Bearbeitung vorgelegt, überprüft er zunächst, ob sie nicht bereits bearbeitet wurde. In diesem Fall ignoriert er die Nachricht. Um ein unbegrenztes Anwachsen der Datenbank zu verhindern, besitzt jede Nachricht einen Zeitstempel. Der Mix bearbeitet dabei nur Nachrichten, die innerhalb einer vorgegebenen Zeitschranke liegen, z.B. Nachrichten, die nicht älter als eine Minute sind.

Dem Big Brother den Kampf angesagt — Web-Mixe

Die bisher in der Praxis eingesetzten Systeme zeigen alle Schwächen gegenüber starken Angreifern, die in der Lage sind, das gesamte Kommunikationsnetz zu überwachen. Spätestens seit dem Bekanntwerden von »Echelon« [9] stellt sich aber nicht mehr die Frage, ob es einen solchen Angreifer auch tatsächlich gibt, sondern vielmehr, ob es möglich ist, ein praktikables System zu entwickeln, das auch vor solchen Angreifern die Anonymität gewährleistet. Die Forschungsgruppe der TU Dresden um Prof. Andreas Pfitzmann und Dr. Hannes Federrath hat es sich deshalb zum Ziel gesetzt, einen sicheren, einfach zu benutzenden und gleichzeitig praktikablen Anonymitätsdienst zu entwickeln. Dieser beruht auf den Chaumschen Mixen. Dieses Verfahren ist zwar schon seit 1981 bekannt, die Schwierigkeit besteht jedoch darin, alle möglichen Angriffe zu erkennen und entsprechende Lösungen zu entwickeln. Gleichzeitig muss das System möglichst sparsam mit den vorhandenen Ressourcen wie Rechenzeit, Speicher, Bandbreite etc. umgehen. Niemand würde wohl ein System nutzen, bei dem er zwar perfekte Anonymität hat, aber auf jede Web-Seite mehrere Minuten (oder gar Stunden) warten muss.



Zunächst wurden im Rahmen von Diplomarbeiten prinzipielle Realisierungsmöglichkeiten und Angriffe auf Mixe untersucht. Dabei entstand eine Implementierung eines Mix-Netzes in der Programmiersprache Java, die es dem Nutzer ermöglicht, anonym zu surfen oder E-Mails zu verschicken. Durch die Wahl von Java lässt sich das Programm auf fast allen Rechnerplattformen und Betriebssystemen einsetzen. Allerdings ist das System nicht praktikabel im oben beschriebenen Sinne, da die Ausführung der benötigten kryptographischen Algorithmen in Java zu langsam für ein ordentliches Surfen ist. Wer Interesse am Ausprobieren hat, kann sich die Software unter http://www.inf.tu-dresden.de/~hf2/anon/PGA2000/ herunterladen.

Im nächsten Schritt sollen nun die bei diesem Projekt gesammelten Erfahrungen in einem neuen Mix umgesetzt werden. Durch die Entwicklung in der Programmiersprache C++ lässt sich eine akzeptable Ausführungsgeschwindigkeit erreichen. Gleichzeitig wird bei der Entwicklung darauf geachtet, dass eine Vielzahl von Plattformen (Windows NT, Linux, Solaris etc.) unterstützt wird, damit die Mixe auch wirklich von verschiedenen, unabhängigen Institutionen betrieben werden können. Ebenso wird die beim Benutzer zu installierende Software verbessert. Gedacht ist dabei an eine für den Anwender völlig transparente Integration in z.B. den WWW-Browser (siehe Abbildung). Weitere Informationen über den Fortschritt des Projektes und den Download der Software findet man unter http://www.inf.tu-dresden.de/~hf2/anon/. Derzeit ist ein erstes Release der Software für Ende August geplant. Sie soll als OpenSource-Software allen Interessierten zur Verfügung stehen.

Somit muss sich der Mix auch nur diese Nachrichten merken. Ältere Nachrichten kann er aus der Datenbank löschen, da sie sowieso nicht mehr bearbeitet würden.

Die sogenannten »*n* -1«-*Angriffe* stellen eine weitere Gefahr für die Anonymität der Nutzer dar. Die Größe *n* meint dabei die Anzahl der Teilnehmer eines Mix-Netzes (genauer: die Schubgröße). Das Prinzip des Angriffs beruht darauf, dass man von den *n* zu einem Zeitpunkt verarbeiteten Nachrichten *n*-1 kennt und deren Weg bestimmen kann. Als einzige unbekannte bleibt somit die Nachricht des angegriffenen und nun enttarnten Teilnehmers übrig. Durchführbar ist dieser Angriff z.B., indem ein Teilnehmer alleine *n*-1 Nachrichten generiert oder *n*-1 Teilnehmer zusammenarbeiten. Dass mehrere Nachrichten eines Schubes vom selben Teilnehmer stammen, lässt sich mittels kryptographischer Verfahren verhindern. Technisch nicht kontrollierbar ist natürlich, ob Teilnehmer zusammenarbeiten (z.B. weil sie alle mit dem Big Brother zusammenarbeiten), um andere zu enttarnen.

Neben den hier kurz vorgestellten klassischen Angriffen auf das Mix-Netz gibt es eine Reihe weiterer Probleme, die die Anonymität gefährden. Berücksichtigt man diese jedoch, ist es möglich, ein System zu entwickeln, das auch gegen starke Angreifer (Big Brother) einen sicheren Schutz vor Beobachtung gewährleistet.

Broadcast

Das Mix-Konzept kommt in Vermittlungsnetzen wie dem Internet zum Einsatz. Zweifellos gehört den Vermittlungsnetzen die Zukunft. Es existieren jedoch »Kommunikationsnetze«, die zumindest für das unbeobachtbare Empfangen von Nachrichten ideal geeignet sind — die Breitbandkabel-Verteilnetze und die Sendeantennen zur Verteilung von Rundfunk und Fernsehen. Diese Art der Verbreitung von Nachrichten ermöglicht es dem Benutzer, lokal aus dem Informationsangebot das auszuwählen, wofür er sich interessiert, ohne dabei Datenspuren zu hinterlassen.

Da erst im Endgerät ein bestimmter Kanal bzw. eine bestimmte Information (z.B. im Videotext) ausgewählt wird, ist deren Empfang vollständig unbeobachtbar. Vorausgesetzt wird dabei immer, dass das verwendete Endgerät sich im Vertrauensbereich des jeweiligen Teilnehmers befindet, da dieses natürlich »weiß«, welche Daten es gerade anzeigt. Ein Vertrauensbereich des Teilnehmers ist deshalb die Grundvoraussetzung für alle Anonymitätsverfahren.

Wahrscheinlich ist es den heutigen Radiohörern und Fernsehzuschauern nicht wirklich bewusst, dass das größte unbeobachtbare Medium über kurz oder lang abgelöst werden wird durch die benutzergesteuerte und individualisierte Zusammenstellung des eigenen Unterhaltungsprogramms. Die Folge ist, dass die Überwachung des Medienkonsums von Haushalten perfekt möglich ist, wenn dies nicht von vornherein durch entsprechende technische Vorkehrungen ausgeschlossen wird. Gesetze könnten zwar den Missbrauch einschränken. Aber auch hier ist technische Vorsorge besser, zumal es dafür sogar eine gesetzliche Grundlage gäbe. Das Teledienstedatenschutzgesetz (TDDSG) enthält nämlich einen Paragraphen, der die Bereitstellung anonymer und pseudonymer Dienste ausdrücklich bekräftigt: § 4 Abs. 1 TDDSG: »Der Diensteanbieter hat dem Nutzer die Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeiten zu informieren.« Insofern dürfte die oft gehörte Begründung, dass anonyme und unbeobachtbare Verfahren viel zu aufwändig und daher nicht zumutbar sind, eigentlich ins Leere laufen, wenn die Kabelnetze jahrelang auch ohne Beobachtbarkeit der Benutzer ihren Dienst verrichtet haben. Zumindest sollten die existierenden Kabelnetze weiterbestehen und keinesfalls ein Nutzungszwang für vermitteltes Radio und Fernsehen entstehen.

Will man erreichen, dass ein spezieller Teilnehmer unbeobachtbar Informationen empfängt, die nur für ihn bestimmt sind, muss man ihn adressieren können. Dies geschieht bei Broadcast unter Nutzung von *impliziten Adressen*. Im einfachsten Fall ist dies eine sehr lange Zufallszahl, die nur dem Sender und dem »anonymen« Empfänger bekannt ist. Jede Teilnehmerstation durchsucht den empfangenen Datenstrom nach den für sie gültigen Zufallszahlen und zeigt dem Nutzer nur die so adressierten Daten an. Da diese Adressen unverschlüsselt übertragen werden und außerdem jeweils zwischen Sender und Empfänger vereinbart werden müssen, spricht man von *offen impliziten Adressen*. Soll verhindert werden, dass die anderen Teilnehmer die Nachricht ebenfalls lesen können, muss zusätzlich ein Schlüssel vereinbart werden, mit dem die Nachricht verschlüsselt wird. Der Nachteil von offen impliziten Adressen ist, dass alle Teilnehmer erkennen, welche Nachrichten an dieselbe Adresse und somit an denselben Empfänger gesendet werden.

Derartige Systeme werden z.B. bei Pagerdiensten der Telekommunikationsunternehmen eingesetzt. Dabei

werden alle Funkrufe in einem bestimmten Gebiet (z.B. in Deutschland oder ganz Europa) jeweils mit der Funkrufnummer des adressierten Teilnehmers ausgestrahlt. Der Pager sucht diesen Datenstrom nach seiner eigenen Adresskennung ab und speichert die zugehörigen Daten. Die völlig unbeobachtbare Nutzung dieser Dienst ist zumindest bei Diensten wie Scall (http://www.scall.de) oder TeLMI (http://www.telmi.de/) möglich, da man diese Geräte ohne Angabe der eigenen Identität kaufen kann und alle weiteren Kosten der Anrufer bezahlt.

Das DC-Netz: Schutz des Senders

Broadcast ermöglicht unbeobachtbares Empfangen von Nachrichten, indem alle Benutzer alle Nachrichten erhalten und lokal aus den empfangenen Daten auswählen, wofür sie sich interessieren. Das DC-Netz erreicht genau das Umgekehrte: Eine Gruppe von Benutzern möchte miteinander Nachrichten austauschen, ohne dass auch nur irgendein Gruppenmitglied erfährt, wer welche Nachricht gesendet hat. Das Verfahren wurde 1988 von David Chaum vorgestellt [6] und lässt sich sehr gut am folgenden Beispiel, den »*Dining Cryptographers*«, erklären: Drei Kryptographen (A, B, C) gehen essen. Als sie den Kellner nach der Rechnung fragen, antwortet er, dass bereits bezahlt sei, der Wohltäter wolle jedoch anonym bleiben. A, B und C fragen sich, wer von ihnen wohl bezahlt haben könnte oder ob es gar jemand anderes war (z.B. der Restaurantbesitzer oder einer der Geheimdienste, die sich ja traditionell für Kryptofragen interessieren). Sie respektieren zwar den Wunsch des Spenders, anonym bleiben zu wollen, sind aber neugierig, ob es einer von ihnen war, und erfinden folgendes Protokoll:

- A und B werfen eine Münze, ohne dass C das Ergebnis sieht: z(AB)
- B und C werfen eine Münze, ohne dass A das Ergebnis sieht: z(BC)
- A und C werfen eine Münze, ohne dass B das Ergebnis sieht: z(AC)

Kopf bedeutet »1«; Wappen bedeutet »0«. Die drei Kryptographen besitzen jetzt jeweils zwei Zahlen, die sie mit jeweils einem Partner ausgetauscht haben. Jeder Kryptograph berechnet still die **XOR-Verknüpfung** ⊕ der beiden Zahlen, d.h.

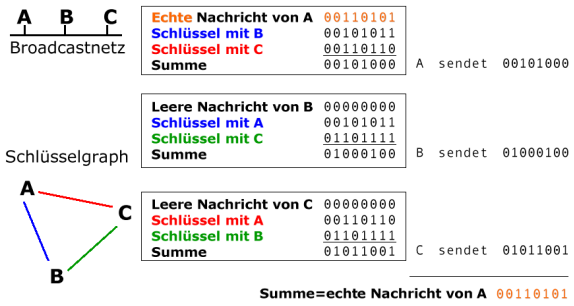
$$1 \oplus 0 = 0 \oplus 1 = 1 \text{ und } 0 \oplus 0 = 1 \oplus 1 = 0$$

und merken sich ihr Ergebnis (»lokale Summe«).

Hat einer von den dreien bezahlt, soll dieser sein Ergebnis noch einmal mit einer »1« XOR-verknüpfen, d.h. hat er eine »1« berechnet, merkt er sich jetzt eine »0« und umgekehrt. Schließlich nennen die drei Kryptographen die gemerkte Zahl. Die drei Zahlen werden wieder XOR verknüpft (»globale Summe«).

Ist das Ergebnis der XOR-Verknüpfung der drei Zahlen »1«, hat einer von den dreien bezahlt, andernfalls war es ein fremder Spender. Die Sicherheit des Verfahrens kommt dadurch zustande, dass keiner entscheiden kann, *welcher* Kryptograph noch die »1« zu den beiden Zahlen XOR-verknüpft hat, da er nur eine Zahl des anderen kennt.

Will man längere Nachrichten senden, muss das Verfahren einfach für jede Bitstelle der Nachricht wiederholt werden, wobei für jedes Bit die Münzen wieder neu geworfen werden müssen. Dies erledigt heutzutage natürlich der Computer, und die Nachrichten können direkt über die Tastatur eingegeben werden. Hat man keine Nachricht zu übertragen, sendet man einfach eine leere Nachricht, d.h. »0«-Bits. Die Berechnung der lokalen und globalen Summe erfolgt bitweise. Das Beispiel im Bild zeigt, wie A eine Nachricht senden möchte. B und C senden Leernachrichten.



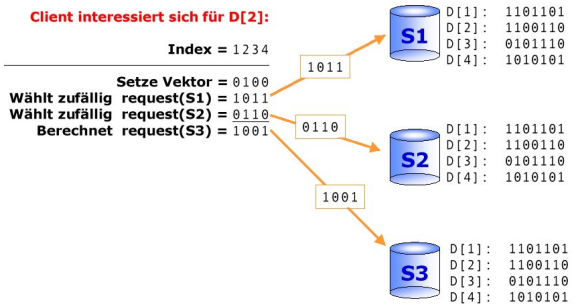
Zwei Nachteile hat das DC-Netz allerdings: Erstens wächst mit der Gruppengröße die Anzahl der Nachrichten, die übermittelt werden müssen. Schließlich muss jedes Gruppenmitglied die lokale Summe übermitteln, und alle müssen wieder die globale Summe, d.h. die Nachricht erfahren, was topologisch gesehen auf ein Broadcastnetz hinausläuft. Zweitens muß jeder »mitspielen«, damit das DC-Netz funktioniert. Sobald sich ein Gruppenmitglied nicht an die vorgeschriebenen Regeln hält und z.B. unsinnige lokale Summen übermittelt, ist zwar die Anonymität eines Senders nicht gefährdet; die Nachricht des Absenders »entsteht« aber auch gar nicht erst und kann daher nicht beim Empfänger ankommen. DC-Netze sind deshalb sehr empfindlich gegen Denial-of-Service-Angriffe.

Unbeobachtbarer Message Service

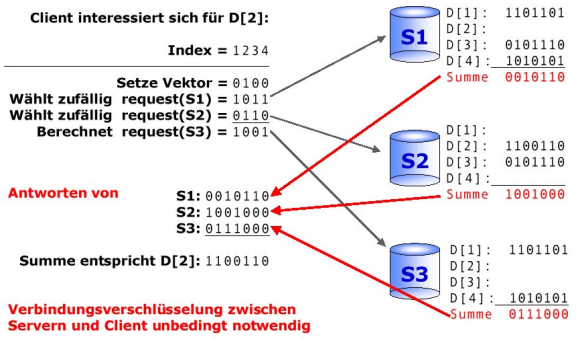
Man kann Broadcast auch auf Vermittlungsnetzen »simulieren«. So sind z.B. die Newsgruppen des Internet so etwas wie Broadcast-Kanäle. Allerdings kann aufgrund der IP-Nummern ein News-Server, von dem ein Benutzer sich seine News herunterlädt, wieder beobachten, wer sich für welche Inhalte interessiert. Theoretisch könnte sich der Benutzer zwar alle News auf seinen Rechner herunterladen und wieder lokal auswählen, allerdings würde das, wenn alle Benutzer so vorgehen würden, den News-Server überfordern, ganz abgesehen von der riesigen Datenmenge, die über eine gewöhnliche Modemverbindung einfach nicht transportierbar wäre.

Es lässt sich aber trotzdem erreichen, dass niemand mitbekommt, welchen News-Artikel in welcher Newsgruppe ein Benutzer gerade liest. Leider existiert das Verfahren bisher nur auf dem Papier, weil sich noch niemand die Mühe gemacht hat, es für das Internet zu implementieren. Die Methode heißt Message Service [7] und beruht auf der Idee, dass mehrere Server mit exakt gleichen Datenbeständen nach einem raffinierten Verfahren abgefragt werden, um einen ganz bestimmten Datensatz abzurufen, ohne dass die Server herausfinden, für welchen Datensatz sich der Benutzer interessiert. Bedingung auch bei diesem Verfahren ist, dass mindestens ein Server nicht mit dem Beobachter zusammenarbeitet. Weltweit gibt es heute viele News-Server, die ihren Datenbestand ständig miteinander angleichen. Fehlt eigentlich nur noch jemand, der den Message Service auch dafür implementiert.

Die Funktionsweise erinnert etwas an das DC-Netz: Zum Abfragen eines Datenbankeintrages sendet der Teilnehmer parallel an alle Datenbanken so genannte Anfragevektoren. Der Anfragevektor hat genauso viele Bitstellen, wie es Datenbankeinträge gibt. Der Benutzer setzt alle Bitstellen des Anfragevektors auf Null bis auf jene Stelle, dessen Datenbankeintrag er anfordert. Enthält die Datenbank beispielsweise 4 Einträge und möchte der Benutzer die Nachricht Nr. 2 abrufen, setzt er den Anfragevektor auf den Wert 0100. Würde er diesen Anfragevektor an eine Datenbank senden, könnte die Datenbank sehr leicht feststellen, für welche Nachricht er sich interessiert. Statt dessen bildet er mehrere zufällige Vektoren, bei denen an jeder Bitstelle nach dem Zufallsprinzip eine 1 oder 0 steht. Aus diesen Vektoren und dem Anfragevektor wird mittels XOR-Verküpfung ein weiterer Vektor berechnet. Alle zufälligen Vektoren und der berechnete Vektor werden verschlüsselt an unterschiedliche Server geschickt. Das Bild zeigt ein Beispiel für drei Server.



Die Datenbanken entschlüsseln den jeweils empfangenen Vektor und berechnen die XOR-Verknüpfung aller Datenbankeinträge, deren Bitstelle im empfangenen Vektor 1 ist. Im Beispiel berechnet der Server S1, der den Vektor 1011 empfangen hat, die XOR-Verknüpfung aus den Datenbankeinträgen mit den Nummern 1, 3 und 4. Das Resultat wird wieder verschlüsselt und an den Benutzer zurückgeschickt. Hat der Benutzer die Antworten von allen angefragten Servern erhalten, entschlüsselt er die Resultate. Das Verfahren funktioniert, da die XOR-Verknüpfung aller entschlüsselten Antworten den gewünschten Datenbankeintrag ergibt. Das liegt daran, dass sich die Einsen all der Nachrichten, für die sich der Benutzer gerade nicht interessiert, durch die XOR-Verknüpfung gegenseitig aufheben, wie das Bild zeigt.



Der Message Service erzeugt natürlich mehr Verkehrsaufkommen als das unmittelbare und beobachtbare Abfragen des gewünschten Datenbankeintrags, wird aber im Vergleich zum Abruf aller Datenbankeinträge immer effizienter, je größer der Datenbestand wird, aus dem einzelne Nachrichten abgerufen werden sollen.

Theorie und Praxis

Dienste, die auch gegen die Beobachtung durch einen Big Brother schützen, sind recht aufwändig. Dementsprechend überschaubar ist der Markt an verfügbaren Diensten.

Für E-Mail stehen sogenannte Type-2-Remailer, wie z.B. der Mixmaster (http://www.obscura.com/) zur Verfügung. Sie verwenden das Mix-Konzept in abgewandelter Form. So werden in einem Remailer die eingehenden Nachrichten nicht etwa eine Zeit lang gesammelt und dann schubweise ausgegeben, sondern jede E-Mail wird um eine zufällige oder vom Sender bestimmte Zeit verzögert. Im Idealfall wartet im Remailer immer eine gewisse Anzahl Nachrichten, so dass die Reihenfolge der ankommenden E-Mails von der Reihenfolge der vom Remailer weitergesendeten unabhängig ist. Andere Grundkonzepte der Mixe wie gleiche Nachrichtenlängen, Replay-Erkennung und Umkodierung der Nachrichten werden wie bereits beschrieben angewendet.

Durch die hohen und für den Beobachter unvorhersehbaren Verzögerungszeiten werden auch sehr starke Angriffe wie der »*n*-1«-Angriff erschwert; schließlich müsste der Angreifer so lange alle Nachrichten blockieren, bis sich im Mix keine ihm unbekannte mehr befindet. Jedoch führen die unvorhersehbaren Verzögerungszeiten dazu, dass die Nachrichtenlaufzeiten sehr unterschiedlich sein können, weswegen sich das Konzept von Mixmaster nicht für Anwendungen wie WWW oder Chat eignen.

Ähnlich wie Mixmaster funktionieren die »Stop and Go«-Mixe [8], bei denen der Sender unter Verwendung einer Zufallsverteilung die Verzögerungszeit seiner Nachricht in jedem Mix festlegt. Damit ist es möglich, die Ankunftszeit der Nachricht beim folgenden Mix ziemlich genau auszurechnen, und in die Nachricht kann ein enges Gültigkeits-Zeitfenster hineincodiert werden. Da jeder vertrauenswürdige SG-Mix die Nachricht nur weiterleitet, wenn sie innerhalb des Zeitfensters eintrifft, hat der Angreifer mit hoher Wahrscheinlichkeit nicht genügend Zeit, die Zuordnung zwischen Ein- und Ausgang der Nachricht festzustellen.

Für das Surfen im World Wide Web ist das einzige derzeit benutzbare System, das auch praktisch schon recht gut gegen große Brüder schützt, die Software Freedom (http://www.freedom.net) der kanadischen Firma Zero-Knowledge.

Freedom basiert auf der Idee, jene Funktionen eines Mixes zu implementieren, die der Verzögerung von Nachrichten nur wenig schaden, aber alle anderen Funktionen wegzulassen. Leider sind das genau die Funktionen, die nötig wären, um einen Big Brother abzuwehren. Bei der Konzeption des Systems wurde also bewusst auf Sicherheit gegenüber sehr starken Angreifern verzichtet. Immerhin, und das ist ein wichtiges Eingeständnis, wird in den entsprechenden Freedom-Whitepapers (http://www.freedom.net/info/freedompapers/) darauf hingewiesen, welche Angriffe durch das System nicht abgewehrt werden. Für einen normalen User klingen die dort beschriebenen Angriffe wie die Phantasien eines Paranoikers, für Sicherheitsexperten belegen die Ausführungen, dass die Entwickler von Freedom recht genau nachgedacht haben. Letztendlich wurde bei Freedom der Performance der Vorzug gegeben, was sich der Benutzer mit einer hohen, aber nicht perfekten Sicherheit erkauft. So werden Replay-Angriffe nur erschwert, ohne sie wirklich zu verhindern. Es findet bisher kein Dummy-Traffic statt, so dass Angriffe über die zeitliche Verkettung möglich sind. Auch »*n*-1«-Angriffe könnten auf dieses System erfolgreich durchgeführt werden.

Einen ähnlichen Ansatz wie Freedom verfolgte das Projekt Onion Routing (http://www.onion-router.net/), indem auf die Funktionen eines Mix verzichtet wurde, die die Verzögerungszeit von Datenpaketen unvorhersagbar machen. Leider stellt Onion Routing keine Software zur Verfügung, die sich ein Benutzer installieren könnte. Stattdessen gibt es einen vereinfachten Proxy-Modus, der allerdings nicht sicherer als die Verwendung von Anonymizer oder Rewebber ist. Damit können die Betreiber von Onion Routing, das Naval Research Laboratory, ein Forschungslabor des amerikanischen Verteidigungsministeriums DoD (Department of Defense), natürlich wieder mitlesen, wofür sich die Benutzer interessieren — Big Brother als Betreiber eines Anonymitätsdienstes.

Eine originelle und von allen anderen Konzepten abweichende Idee zur Anonymisierung von Webzugriffen verfolgt das Projekt Crowds (http://www.research.att.com/projects/crowds/) das in den Forschungslabors des amerikanischen Telefonkonzerns AT&T entstand. Die Benutzer des Systems schließen sich in einer Crowd (dt.: Menschenmenge, Gedränge) zusammen. Jeder Benutzer installiert auf seinem PC ein Programm, den Jondo (von John Doe, dem »Mann ohne Gesicht«). Der Jondo nimmt die URLs entgegen, die der Benutzer aufrufen will, sendet

sie aber nicht direkt an den Server, sondern verschlüsselt sie und schickt sie an den Jondo eines zufällig ausgewählten Mitglieds der Crowd. Der Jondo entschlüsselt die URL und wirft eine (virtuelle) Münze. Bei »Kopf« wird die URL an den Server geschickt, bei »Zahl« wird sie erneut verschlüsselt und wieder an ein anderes Mitglied der Crowd geschickt. Dessen Jondo verfährt ebenso. Die Sicherheit des Verfahrens kommt dadurch zustande, dass der Benutzer, der die URL an den Server schickt, stets behaupten wird, er habe die URL nur zur Weiterleitung erhalten. Dummerweise erfährt ein Jondo, der eine URL zur Weiterleitung erhalten hat, alle übermittelten Daten, da die URLs und die Antworten vom Webserver unverschlüsselt im Jondo vorliegen. Es empfiehlt sich daher, Crowds nicht für Webseiten einzusetzen, bei denen vertrauliche Informationen zwischen dem Browser und dem Server ausgetauscht werden. Da Crowds den amerikanischen Exportbeschränkungen unterliegt, darf die Software zurzeit nicht aus den USA ausgeführt werden.

Zensur im Internet verhindern

Eine wesentliche Voraussetzung, um der Zensur von Inhalten zu begegnen, ist sicher die Möglichkeit, diese Inhalte anonym abzurufen bzw. zu verbreiten. Auf der anderen Seite, ist es aber auch wichtig, daß der Zugriff auf unbeliebte Inhalte nicht unterbunden werden kann. Diesen Ansatz verfolgt das Projekt Freenet (http://freenet.sourceforge.net). Es besteht aus einem Netz von Rechnern, in dem zu veröffentlichende Informationen verteilt gespeichert (repliziert) werden. Jede Information ist dabei über einen (textuellen) Schlüssel abrufbar. Richtet sich die Anfrage an einen Server, der die gewünschten Daten nicht lokal gespeichert hat, wird die Anfrage an benachbarte Rechner des Netzes weitergeleitet. Dieser Vorgang setzt sich fort, bis die Daten auf einem Server gefunden werden. Auf dem Weg, den die Anfrage durch das Netz genommen hat, wird die Antwort dann zu dem entsprechenden Nutzer zurück übertragen. Dabei wird die Nachricht auf den durchlaufenen Servern eine Zeit lang gespeichert. Somit liegen die häufig abgefragten Informationen meist in einem der Knoten der näheren Umgebung vor, was die Netzbelastung verringern soll. Die beste Route, auf der eine Anfrage weitergesendet werden soll, wird dadurch ermittelt, dass der Schlüssel analysiert und an denjenigen Server geschickt wird, der schon einmal eine Anwort mit einem ähnlichen Schlüssel zurückgesendet hat. Damit dieses Vorgehen einen Sinn ergibt, sind die Schlüssel hierarchisch strukturiert (ähnlich den Verzeichnissen in einem Dateisystem), und ein Freenet-Server speichert vorwiegend Schlüssel eines Teils der Baumstruktur.

Entwickelt wurde Freenet vor allem, um eine Zensur des Internets unmöglich zu machen: Da weder der Autor noch der Betreiber eines Servers noch sonst irgendein Nutzer wissen, in welchem Rechner welche Informationen gespeichert sind (der Betreiber weiß dies höchstens für seinen eigenen Rechner), kann auch keine Information zensiert werden. Auch ist der Urheber einer Information nur sehr schwer ermittelbar: Im Prinzip kennt nur der Server, auf dem ein Nutzer neue Informationen direkt geladen hat, den Urheber. Aber selbst dieser Server kann im Prinzip nicht ermittelt werden, da auch er die entsprechende Informationen von einem anderen erhalten haben kann. Ebenso ist die Abfrage einer Information nur schwer verfolgbar, da viele Stellen existieren, an denen sie gespeichert ist. Dieses Modell geht aber von einem räumlich sehr beschränkten Beobachter aus. Um zu ermitteln, wer eine bestimmte Information gesendet hat oder wer sie abruft, muß der Beobachter alle Freenet-Server kontrollieren oder das gesamte Netz abhören. Umgekehrt ist die Überwachung einzelner Teilnehmer jedoch problemlos durch Abhören ihrer Internetverbindung (z.B. durch den ISP) bzw. des jeweils ersten Freenet-Servers möglich.

Am Massachusetts Institute of Technology (MIT) arbeitet man derzeit an einem System namens Free Haven (http://freehaven.net/), dessen Ziel es ist, den globalen Massenspeicher Internet sicher zu machen gegen die »Zerstörung« gespeicherter Daten. Free Haven möchte mit Hilfe der Mixe die anonyme und verteilte Speicherung von Daten erreichen, ohne dass Benutzer, die illegal handeln, sich ihrer Verantwortung entziehen können. Ob dieser hohe Anspruch von dem System wirklich erfüllt werden kann, muss die Zukunft zeigen.

Bei MP3-Fans sind die Programme Napster (http://www.napster.com/) und Gnutella (http://www.gnutella.de/) sehr beliebt, die ähnlich dem Internet Relay Chat (IRC) funktionieren. Statt zu chatten, geht es um den Austausch von Dateien. Während das Verzeichnis mit den Speicherorten bei Napster zentral liegt und nur der Datenaustausch direkt zwischen den Teilnehmern geschieht, läuft bei Gnutella alles verteilt ab. Die Benutzer hatten zeitweise die Illusion, dass diese Kommunikation unbeobachtet ablaufen würde. Doch die Rockband Metallica hatte mit Hilfe der Firma NetPD (Net Police Department) eine Liste von 335 435 Napster-Nicknames inclusive der IP-Adressen zusammengestellt, die Metallica-Songs raub-

kopiert haben sollen, woraufhin Napster diese Benutzer-Nicknames sperren musste. Eine andere Methode zur Identifikation unliebsamer Teilnehmer ist die Wall of Shame (http://www.zeropaid.com/busted/), die sich gegen Tauschhändler von Kinderpornographie richtet. Dafür wurde ein geheimer Gnutella-Server eingerichtet, der mit expliziten Dateinamen wirbt. Beim Download dort werden u.a. die IP-Adresse und Download-Zeit des Interessenten mitgeloggt. Diese Methode ist natürlich nicht nur beim Laden strafrechtlich relevanter Daten möglich. Erst die Kombination mit Techniken wie Mixen könnte Anonymität und Unbeobachtbarkeit gewährleisten.

Anon-Debatte?

Wieviel Anonymität und Unbeobachtbarkeit wollen wir: im Internet, in unserer Gesellschaft? Ähnlich der polarisierenden Kryptodebatte, die vor einigen Jahren sehr hitzig geführt wurde und auch jetzt immer wieder aufflackert, geht es um eine Abwägung zwischen verschiedenen Werten. Hat jeder Teilnehmer ein Recht auf Anonymität, wie dies in der Declaration of Human Rights in Cyberspace [10] von der Internet-Community formuliert oder aus dem Datenschutzrecht (z.B. auf europäischer Ebene siehe [11]) abgeleitet wird? Aktuell wird eher das Gegenteil diskutiert: Zum Zwecke der Strafverfolgung sollen die Provider Verbindungsdaten zur Identifikation von Benutzern speichern und bereit halten, z.B. für E-Mail [12].

Außerdem ist eine absolute Anonymität gegenüber allen Dritten nicht in jedem Fall zweckmäßig: Im jeweiligen Kontext muss der Teilnehmer entscheiden können, ob er seinen Namen gegenüber einem Kommunikationspartner angeben möchte oder sich lieber unter einem Pseudonym zu erkennen gibt. Verschiedene Grade zwischen Anonymität und Identität können jeweils unbedingt nötig oder von den Beteiligten nur gewünscht sein. Auf diesem Gebiet gibt es zwar bereits wissenschaftliche Untersuchungen [13], jedoch müssen die dort gewonnen Erkenntnisse erst noch in der Praxis umgesetzt werden. Ohne diese Erfahrungen kann die uns bevorstehende Anon-Debatte nicht fundiert geführt werden.

Eine Verpflichtung für alle Nutzer, bei jeder Bewegung ihrer Bewegungen in der Online-Welt authentische Datenspuren zu hinterlassen, würde massiv gegen ihren Datenschutz verstoßen und kann daher nicht die Lösung sein. Stattdessen sollte man überlegen, wie auf der Grundlage eines möglichst unbeobachtbaren Netzes die Strafverfolger mit richterlicher Anordnung im Einzelfall ermitteln können. Wenn jedoch die Provider und irgendwelche Big Brother im In- und Ausland standardmäßig alle Daten speichern, könnte sich eine Subkultur bilden, die ihre eigenen Lösungen des Problems sucht — mit der Folge, daß Strafverfolgung »im Netz« vielleicht völlig unmöglich wird. Die schnelle Verbreitung und der eindrucksvolle Erfolg von Napster und Gnutella beim Endbenutzer sind gute Beispiele dafür, wie schnell solch eine Entwicklung gehen kann.

Anwendung: Internet-Wahlen

Seit einiger Zeit heiß diskutiert: Wahlen im Internet (z.B. http://www.internetwahlen.de/). Dabei geht es nicht nur um Bundestags- oder Europawahlen, sondern auch um alle möglichen Formen der Abstimmung sowohl im großen Maßstab als auch ein paar Nummern kleiner in Firmen oder Vereinen. Daneben können solche Verfahren ebenfalls für viele Arten der Bürgerbeteiligung an Verfahren des E-Government zum Einsatz kommen. Selbstverständlich darf bei der geheimen Wahl keiner herausfinden können, wer was gewählt hat. Außerdem dürfen nur die berechtigten Wähler ihre Stimme — meist maximal eine — abgeben. Zur Zeit werden vor allem Verfahren zur Verschlüsselung und (blinden) digitalen Signatur diskutiert, die vor Verfälschungen schützen und die unmittelbare Identifikation des Wählers erschweren. Dabei bleibt die nötige Anonymität und Unbeobachtbarkeit gegenüber den Betreibern im Internet oft vergessen: Allein die Tatsache, dass sich jemand virtuell in ein Internet-Wahllokal begibt, geht keinen Betreiber etwas an. Dieser kann vielleicht sogar beobachten, dass der Wähler dann noch zur Homepage seines Lieblingskandidaten surft. Für die Aufrechterhaltung des Wahlgeheimnisses, das ebenso die Umstände der Wahl wie die Entscheidung, nicht zu wählen, umfasst, sind wirkungsvolle Anonymitätsdienste als Basis unverzichtbar.
Verfahren wie Mixe sind zwar grundsätzlich dazu geeignet, diese Anonymität zu ermöglichen. Wenigstens für größere Internetwahlen mit hoher politischer Bedeutung müßte man dann aber die Benutzung von Anonymitätstechniken auch von seiten des Staates fördern und einen entsprechenden Grundschutz bereitstellen.

Literatur

[1] Lauren Weinstein: Massive Tracking of Web Users Planned -- Via ISPs. http://www.vortex.com/privacy/priv.09.13

[2] Thomas Demuth, Unerkannt surfen, Privatsphäre im World Wide Web, c't 06/00, 196

[3] Hannes Federrath: Unsicherheit formular-basierter Anonymitätsproxies. http://www.inf.tu-dresden.de/~hf2/anon/aproxies/

[4] Heise-Newsticker: Doch nicht anonym im Web. http://www.heise.de/newsticker/data/pab-23.02.00-000/
[5] David Chaum: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Communications of the ACM 24/2 (1981) 84-88. http://world.std.com/~franl/crypto/chaum-acm-1981.html
[6] David Chaum: The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability. Journal of Cryptology 1/1 (1988) 65-75.
[7] David A. Cooper, Kenneth P. Birman: Preserving Privacy in a Network of Mobile Computers. 1995 IEEE Symposium on Research in Security and Privacy, IEEE Computer Society Press, Los Alamitos 1995, 26-38. http://cs-tr.cs.cornell.edu:80/Dienst/UI/1.0/Display/ncstrl.cornell/TR95-1490
[8] Dogan Kesdogan, Roland Büschkes, Otto Spaniol: Stop-And-Go-MIXes Providing Probabilistic Anonymity in an Open System. in: Multilateral Security in Communications, Addison-Wesley 1999, 365-380.
[9] Interception capabilities 2000. http://www.spiegel.de/statichtml/stoa/ic2kreport.htm
[10] Declaration of Human Rights in Cyberspace, Draft Proposal, November 1997. http://www.be-in.com/9/ten/rightsdec.html
[11] Arbeitsgruppe für den Schutz der Rechte von Personen bei der Verarbeitung personenbezogener Daten (Art. 29-Gruppe nach der EG-Datenschutzrichtlinie): Anonymität im Internet, Empfehlung 3/97. http://www.datenschutz-berlin.de/doc/eu/gruppe29/anony_de.htm
[12] Jelle van Buuren: Das Europäische Parlament verlangt ein Ende der Anonymität im Internet, Telepolis 2000-04-05. http://www.heise.de/tp/deutsch/inhalt/te/5975/1.html
[13] 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.