in: IT-Sicherheit ohne Grenzen? Tagungsband 6. Deutscher IT-Sicherheitskongreß
des BSI 1999, SecuMedia-Verlag, Ingelheim 1999, 59-70

Anonymer und unbeobachtbarer Webzugriff für die Praxis

Uwe Danz[1], Hannes Federrath[2], Marit Köhntopp[3], Huberta Kritzenberger, Uwe Ruhl[4]

Kurzfassung:
Bei jeder Nutzung des Internet hinterläßt der Teilnehmer Spuren. Solche Datenspuren können auf allen Stationen des Übertragungsweges gespeichert und ausgewertet werden. Es existieren jedoch technische Verfahren, die es dem Nutzer ermöglichen, anonym und unbeobachtbar zu kommunizieren. Das vorliegende Konzept beschreibt eine Variante des anonymen Internet-Zugriffs unter HTTP (Hypertext Transfer Protocol): Durch die Hintereinanderschaltung unabhängiger Stationen (Mixe), die die Nachrichten stets sammeln, umkodieren und in einer anderen Reihenfolge aussenden, kann der einzelne Internet-Zugriff unter der Vielzahl von zeitgleichen Nutzungen der anderen Teilnehmer verdeckt werden. Diese Technologie findet beispielsweise ihre Anwendung im Projekt „Neue Medien in der Kinder- und Jugendpsychiatrie“ der Medizinischen Universität zu Lübeck. Dort soll ein anonymer Internet-Zugriff geschaffen werden, damit sich Kinder und Jugendliche frei über die Gefahren des Drogenkonsums informieren und austauschen können.

Stichwörter: Anonymität, Internet, WWW, Mix, Unbeobachtbarkeit, Unverkettbarkeit, Datenschutz

Abstract:
Using the Internet there remain traces. Such data traces can be stored and analysed at all hops along the path of transmission. However, there are technical methods enabling the user to communicate anonymously and unobservably. The presented concept describes a version of anonymous Internet access using HTTP (hypertext transfer protocol): By sending the messages over a series of independent stations (mixes) which collect the messages, change their outlook, and output them in a different order, each Internet access can be covered by the amount of simultaneous accesses of other users.
This technology is e.g. applied in the project „New Media in Child and Youth Psychiatry“ of Medical University of Luebeck. There shall be created a possibility for anonymous Internet accesses, so that children and young people may gather information and talk freely about the dangers of drug consumption.

Key Words: Anonymity, Internet, WWW, Mix, Unobservability, Untraceability, Privacy

1 Einführung

Seit das Internet von immer mehr Personen genutzt wird, ist der Bedarf an der Auswertung der Nutzerdaten gestiegen. Bei jeder Nutzung hinterlassen die Teilnehmer an vielen Stellen Datenspuren, die von Diensteanbietern oder Access-Providern ausgewertet werden können. Die Teilnehmer haben jedoch das Bedürfnis und den Anspruch, daß ihre personenbezogenen Daten geschützt werden. Im deutschen Rechts-

1 Uwe Danz, Commerzbank AG Frankfurt
2 Hannes Federrath, Technische Universität Dresden, Fakultät Informatik
3 Marit Köhntopp, Der Landesbeauftragte für den Datenschutz Schleswig-Holstein, Kiel
4 Huberta Kritzenberger, Uwe Ruhl, Medizinische Universität zu Lübeck

raum ist der Schutz der personenbezogenen Daten, die bei der Internet-Nutzung anfallen, beispielsweise im *Teledienstedatenschutzgesetz* und im *Mediendienste-Staatsvertrag* geregelt. Dort werden explizit die Grundsätze der Datenvermeidung und Datensparsamkeit festgeschrieben. Außerdem soll nach diesen Regelungswerken ermöglicht werden, daß der Nutzer Tele- und Mediendienste anonym oder unter Pseudonym in Anspruch nehmen kann, soweit dies technisch möglich und zumutbar ist.

Die Erfahrung hat gezeigt, daß sich fast immer, wenn personenbezogene Daten zur Verfügung stehen, Begehrlichkeiten entwickeln, die Daten zu anderen Zwecken zu verwenden oder auch zunächst nur zu sammeln, um sie für spätere Gelegenheiten auswerten zu können. Ein Mißbrauch dieser Daten läßt sich dann oft nicht ausschließen (siehe auch [GoWB_97]). Rein rechtliche oder organisatorische Maßnahmen zum Schutz der anfallenden Daten sind weniger wirksam als eine technische Lösung, bei der gar nicht erst personenbezogene Daten entstehen oder bei der diese automatisch in ihrer Verwendungsmöglichkeit begrenzt werden. Sicherlich reichen in den meisten Fällen technische Lösungen allein nicht aus, da z.B. Regelungen für Kontrollen und Prüfungen vorgesehen werden müssen, sondern sie müssen durch rechtliche und organisatorische Maßnahmen ergänzt werden.

Ziele einer technischen Realisierung von Datenvermeidung in offenen Netzen sind Unbeobachtbarkeit, Unverkettbarkeit und Anonymität. Die Unbeobachtbarkeit ist gewährleistet, wenn sich nicht erkennen läßt, wer Daten sendet oder empfängt. Dabei ist in den bestehenden Netzen das Ereignis des Sendens bzw. des Empfangens eines Datenpaketes stets beobachtbar; allerdings kann durch das Generieren von Dummy Traffic kein Angreifer daraus einen Nutzen ziehen. Dummy Traffic bedeutet, daß ein Nutzer (verschlüsselte) Leernachrichten, die für einen Beobachter von außen nicht von echten Botschaften zu unterscheiden sind, sendet, solange er keine echten Nachrichten zu senden hat. Dennoch besteht die Gefahr, daß trotz eines unbeobachtbaren Zugriffs auf eine Webseite die Verkettung verschiedener Ereignisse, z.B. über Cookies oder Metainformation des Hypertext Transfer Protocols (HTTP), möglich ist. Anonymität ist nur gewährleistet, wenn trotz der Auswertung aller Ereignisse keine Aussage über die Identität des Nutzers getroffen werden kann.

Es gibt eine Menge Beispiele aus der Praxis, die die Wichtigkeit von Unbeobachtbarkeit, Unverkettbarkeit und Anonymität unterstreichen: So sollten Abrufe von Patentinformationen durch innovative Unternehmen über das Internet ebenso wie gemeinnützige oder öffentliche Beratungsangebote (Seelsorge, aber auch über Bürgerbüros) und Meinungsäußerungen (besonders auch anonyme Abstimmungen oder Wahlen) unbeobachtbar, unverkettbar bzw. anonym sein.

2 Die Mix-Idee

Das Mix-Konzept wurden von David Chaum in [Chau_81] beschrieben. Die Grundidee der Mixe läßt sich am Beispiel herkömmlicher Briefe wie folgt veranschaulichen:

> *Der Sender S verpackt eine Postkarte in einen Briefumschlag mit der Adresse des Empfängers E (Ende-zu-Ende-Verschlüsselung). Damit der Briefwechsel zwischen S und E nicht direkt nachvollziehbar ist, wird der gesamte Brief in einen weiteren Umschlag gesteckt und mit der Adresse eines Freundes F_1 versehen. Dieses Verfahren kann rekursiv von F_2 bis F_x wiederholt werden. Mit wachsenden x wird einerseits die Kommunikationsbeziehung zwischen S und E schwerer nachvollziehbar. Andererseits erhöhen sich die Beförderungsdauer sowie die Masse und die Maße der Nachricht stetig. Die so vorbereitete Nachricht wird an den Freund F_x gesendet. Dieser entfernt den äußersten Umschlag und sendet die Nachricht weiter an die nur für ihn sichtbare Adresse des Freundes F_{x-1}. Nach x Schritten ist die Nachricht beim Empfänger angekommen. Jede Person F_i (i = 1..x) erfüllt dabei die Aufgabe eines Mixes.*

Übertragen auf Rechnernetze, bei denen eine digitale Kommunikationsbeziehung geschützt werden soll, besteht die Nachricht aus einem beliebigen Datenblock. Die Mixe sind geeignete Rechner im Kommunikationsnetz, die von möglichst unabhängigen und vertrauenswürdigen Personen oder Gruppen betrieben werden. Weiterhin stehen die Briefumschläge für asymmetrische Kryptosysteme. Sie sind notwendig, damit jeder Sender verschlüsselte Nachrichten an die Mixe senden kann und nur für diese die Nachrichten zu entschlüsseln sind.

3 Übersicht über verschiedene Anonymitätstechniken

Das beschriebene Mix-Konzept wird bereits in einigen Systemen verwendet, beispielsweise den *ISDN-Mixen* [PfPW_89] für ISDN-Telefonie sowie in *Babel* [GüTs_96] und beim *Mixmaster* [Cott_95] für E-Mail-Nachrichten.

Daneben gibt es andere Anonymitätstechniken[5]:

Das *Onion-Routing* [ReSG_98] für interaktive Verbindungen auf Socket-Ebene baut ähnlich wie die ISDN-Mixe einen Kanal auf, der allerdings je nach Nachrichtenaufkommen unterschiedlich lange genutzt wird. Dies kann für Angriffe ausgenutzt werden: Zwei kooperierende Onion-Router können demzufolge alle dazwischenliegenden Stationen überbrücken, da sie erkennen, wie lange der jeweilige Kanal genutzt wird. Die Umsetzung des *PipeNet* [GoWa_97, McCo_97] wurde zugunsten der Entwicklung des Onion-Routing aufgegeben. Mit *Crowds* [ReRu_97] wird bei der WWW-Nutzung erreicht, daß jeder Teilnehmer nur mit einer geringen Wahrscheinlichkeit echter Adressat ist. Allerdings ist die globale Systemsicht eines Angreifers verboten. Ähnliches gilt für den *Anonymizer* [Boya_97], der als eine Art Stellvertreter (Proxy) die Anfragen für die Nutzer stellt. Hierbei muß zusätzlich dem Anonymizer bzw. seinem Betreiber vertraut werden. Der *Lucent Personalized Web Assistant* [LPWA_97] verlangt eine Benutzerauthentisierung und kennt somit die Identität des Teilnehmers. Er fungiert ebenfalls nur als Proxy. Der Ansatz von *Mixed Mobile IP*

[5] Ein Überblick über verschiedene Anonymitätstechniken findet sich unter [FePf_98, Möll_98, Roes_98].

[LoEB_96] versucht, den aktuellen Aufenthaltsort vor dem Netzbetreiber zu verbergen. Dazu werden Mixe benutzt. Allerdings verwenden die mobilen Geräte keine Kryptographie; somit muß jeder Teilnehmer der ersten bzw. letzten Station seines Übertragungsweges vertrauen, da sie den Nachrichteninhalt und den Kommunikationspartner kennt.

4 Der WWW-Mix

Ein normaler Webzugriff verläuft nach dem folgenden Prinzip: Der Nutzer gibt die Adresse der gewünschten WWW-Seite an bzw. folgt einem Link auf der angezeigten Seite. Daraufhin generiert der Browser einen Request, der direkt in das Internet gesendet werden kann (siehe Abb. 1).

Dabei können Metainformationen - wie beispielsweise die E-Mail-Adresse des Nutzers - übermittelt werden. In jedem Fall weisen die übertragenen IP-Pakete eine Quell- und Zieladresse auf, die in der Regel die Rechner des Absenders und des Empfänger eindeutig kennzeichnen. Durch eine Auswertung dieser Informationen ist jeder Angreifer auf dem Übertragungsweg zwischen Browser und WWW-Server in der Lage, die einzelnen Anfragen den jeweiligen Nutzern zuzuordnen.

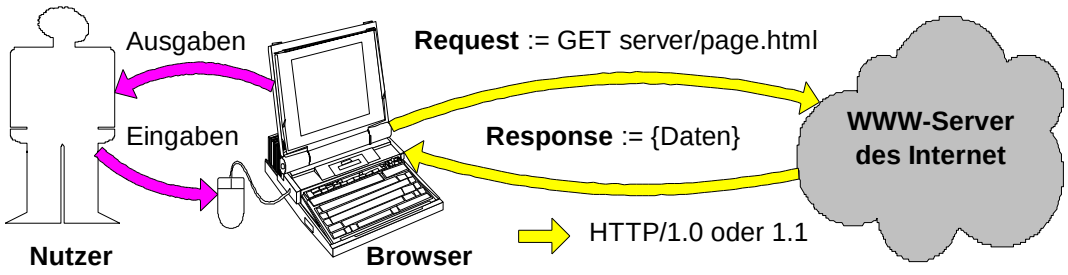

Abb. 1: Webzugriff unter HTTP

Ein Schutz gegen Angriffe dieser Art besteht in der Zwischenschaltung eines **Proxy**, d.h. eines Rechners, der als Stellvertreter für die Anfragen und Antworten der Nutzergruppe fungiert (siehe Abb. 2). Auf diesem Wege bleiben einem Angreifer die Netzstruktur und die Quellen der Anfragen bzw. die Senken der Antworten unbekannt. Die Verwendung eines Proxy bietet sich insbesondere dann an, wenn bereits eine Firewall zum Schutz des internen Netzes installiert ist, die diese Stellvertreterfunktion wahrnehmen kann.

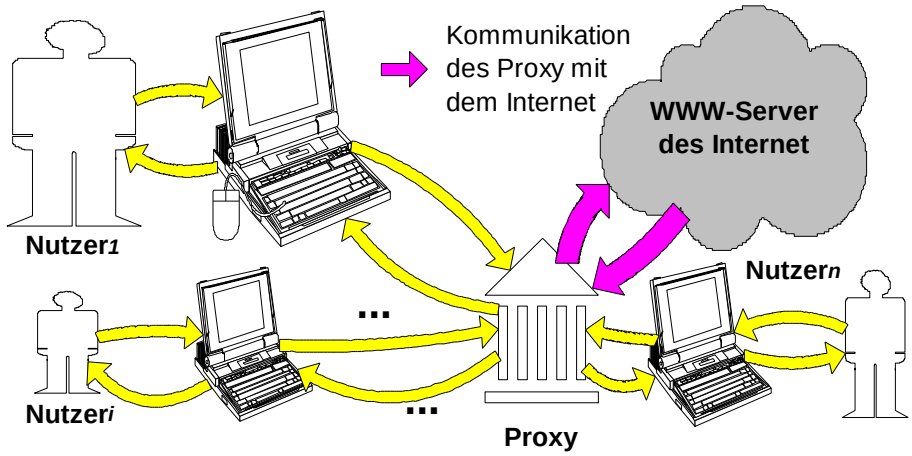

Abb. 2: Stellvertreterfunktion des HTTP-Proxy beim Webzugriff

Mit der beschriebenen Netztopologie ist allerdings eine Verbindung verschiedener Organisationsstrukturen (Firmen, Behörden) oder die effiziente verteilte Nutzung kaum möglich. Außerdem gibt es keinerlei Schutz gegen neugierige Systemadministratoren, die den einzelnen Proxy warten, oder gegen Angriffe, die ihn kompromittieren.

Darüber hinaus ist ein Insider, d.h. ein Angreifer, der den internen Datenverkehr überwacht, in der Lage, Nutzerprofile über deren Kommunikationsverhalten oder sogar über deren mutmaßliche Interessen zu erstellen. Erst wenn die Verbindung zwischen den Nutzern und dem Proxy verschlüsselt wird, sind die Nutzer vor einem Insiderangriff dieser Art geschützt, solange der Proxy nicht selbst der Angreifer ist. Jedoch kann trotz einer Verschlüsselung die Kooperation von Angreifern, die sich vor und nach dem Proxy befinden, jegliche Kommunikationsbeziehungen aufdecken, da die im Proxy eintreffenden Datenströme zumindest zeitlich und in ihrer Reihenfolge nicht verändert werden und daher eine Zuordnung der eingehenden und ausgehenden Datenpakete möglich ist.

Eine technische Problemlösung läßt sich mit Mixen realisieren. Dabei ist die Anonymität der Clients nur gesichert, wenn sich alle Benutzer des Systems an Regeln halten, die sicherstellen, daß die Nachrichten weder über ihr Aussehen noch über ihr zeitliches Verhalten im System von anderen unterschieden werden können und die Mehrzahl der Nutzer nicht mit den Angreifern kooperiert.

Dies wird erreicht, indem sämtliche Requests der Nutzer durch jeweils einen Nutzer-Proxy (siehe Abb. 3) auf eine pro Nachrichtenschub konstante Länge gebracht und mehrfach verschlüsselt werden. Die so vorbereiteten Pakete werden im ersten Mix gesammelt, bis eine möglichst große Anzahl von Anfragen verschiedener Nutzer (z.B. Anonymitätsgruppe von 1 bis *n*) vorliegt. Die Weiterleitung der kodierten Anfragen bis zum Cache-Proxy erfolgt über mehrere Mixe. Dabei werden die einzelnen Pakete umkodiert, auf Wiederholungen getestet (und ggf. wiederholt gesendete Pakete

entfernt), umsortiert und jeweils ein Schlüssel für den Rückweg (die Antwort) hinterlegt. Der Cache-Proxy transformiert die erhaltenen Pakete in die ursprüngliche Form, wie sie vom Browser des Nutzers generiert wurden, und stellt die Anfrage an das Internet. Die Antworten werden im Cache-Proxy gepuffert, und je nach dem Nachrichtenaufkommen der anderen Teilnehmer erfolgt die Rücksendung der Response in einer geeigneten Blockgröße.

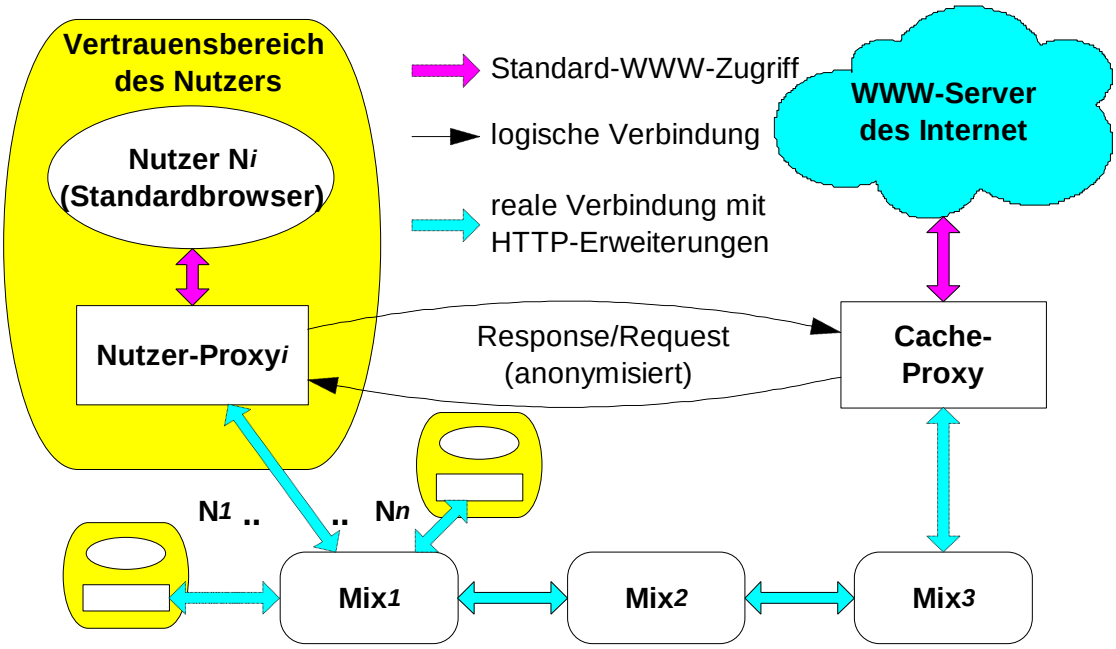

Abb. 3: WWW-Mix-Konzept

Die Fragmentierung in Blöcke von jeweils konstanter Länge erfordert in der Regel ein Auffüllen von kurzen Nachrichten mit zufälligen Bits (Padding) bzw. ein Zerteilen von langen Nachrichten. Dabei können die gepufferten Nachrichtenteile eventuell im nächsten Schub übertragen werden. Diese Aufgaben des Cache-Proxy sind deterministisch und somit stets kontrollierbar. Angriffe auf ihn können die Verfügbarkeit beeinträchtigen, nicht aber die Anonymität [Danz_98].

Unter der Annahme, daß die verwendeten Kryptosysteme nicht gebrochen sind und mindestens ein Mix vertrauenswürdig ist, gewährleistet das Mix-System innerhalb der Gruppe von Teilnehmern, die nicht mit den Angreifern kooperieren, die Anonymität [Chau_81]. Das zugrundeliegende Angreifermodell wird in Abschnitt 6 erläutert.

5 Skalierung und zeitliches Verhalten der Mix-Nutzung

Innerhalb der Anonymitätsgruppe kann die Festlegung auf Anfragen gleicher Längen, z.B. auf 1 KByte, getroffen werden. Damit sind in der Regel die Übertragungen von

GET-Anfragen, Anfragen an Suchmaschinen (GET/POST), Chat-Reaktionen (POST) und kurze E-Mail-Nachrichten ohne Aufteilung in mehrere Blöcke möglich.

Weiterhin sollten die Blöcke der HTTP-Response pro Schub (d.h. pro Nutzung des aufgebauten Kanals) eine jeweils konstante Länge besitzen. Dies läßt sich im allgemeinen nicht ohne tiefgreifende Veränderungen der Blockgrößen erreichen, da das Datenaufkommen auf dem Rückweg zum Nutzer sehr unterschiedlich sein kann. So kann eine Response nur einige Byte wie z.B. die Information „Seite nicht modifiziert“ enthalten, während andere Nutzer ein Video von mehreren MByte empfangen wollen.

Die Bestimmung der optimalen Länge der Response-Blöcke erfolgt durch den Cache-Proxy und ist abhängig von der Bandbreite, dem akzeptablen Verhältnis zwischen Nutzdaten und Dummy Traffic, den maximalen Verzögerungszeiten und der Qualität der Internet-Anbindung zu den angefragten Servern. Sobald sich alle Nutzer auf Parameter für den Cache-Proxy geeinigt haben, kann dieser pro Schub die jeweilige Blocklänge bestimmen und demzufolge kurze Nachrichten auffüllen bzw. lange in mehrere Blöcke aufspalten. Mit der nächsten Anfrage können dann weitere Teile nachgefordert werden. Eventuell generiert der gleiche Nutzer auch eine Anfrage mit höherer Priorität, die dann bevorzugt bearbeitet wird.

Interessant ist weiterhin die Bestimmung des Antwortzeitpunktes. Auch dieser ist von den Benutzerinteressen abhängig. Falls es zu möglichst geringen Verzögerungszeiten kommen soll und das Netz bzw. die Mixe sehr performant sind, kann der Cache-Proxy, sobald eine Antwort zumindest teilweise vorliegt, alle bis zu diesem Zeitpunkt gesammelten Informationen vollständig an die Nutzer senden. Andernfalls sind Entscheidungen wie „mindestens 50% der Anfragen sind zu 90% beantwortbar“ möglich. Allerdings müssen zusätzliche Regeln für stromorientierte Verfahren und ebenso für eventuelle Offline-Situationen berücksichtigt werden.

Sobald die Nutzer-Proxys eine Antwort des Cache-Proxy durch die symmetrischen Rückkanäle des Mix-Netzes erhalten haben, generieren sie sofort eine neue Anfrage. Dieser Request kann durch den Nutzer initiiert sein, aus einer Nachforderung eines fehlenden Nachrichtenblockes bestehen oder eine Dummy-Anfrage sein. Letztere sind notwendig, um in verkehrsschwachen Zeiten andere Teilnehmer zu schützen. Dieses „solidarische Handeln“ fällt den Teilnehmern um so leichter, je kostengünstiger ihr Online-Zugang ist.

Eine detaillierte Beschreibung erfolgte in [Danz_98]. Für einen praktischen Einsatz wäre eine Skalierung des Systems durch Analyse des Verhaltens von repräsentativen Nutzergruppen sinnvoll. Eine dynamische Anpassung an sich verändernde Rahmenbedingungen ist mit geeigneten Systemen ebenso denkbar.

Abschließend kann festgestellt werden, daß die Verzögerungszeiten durch die Kryptographie und das schubweise Passieren aller Nachrichten durch die Mixe notwendig für starke Anonymität sind. Die größten Einschränkungen in der Performance sind allerdings bei der Blockung der Nachrichten zu erwarten, da bedingt durch die „Gleichmacherei“ stark differenziertes Nutzerverhalten zu hohen Verzögerungszeiten oder einen großen Anteil an Dummy Traffic bzw. Padding führt.

6 Angreifermodelle

Das Angreifermodell läßt sich allgemein in die Rechenkapazität der Angreifer, die Angriffsstrategie, die technischen Möglichkeiten und die räumliche Verbreitung unterteilen. Für Mix-Systeme ergeben sich folgende Aussagen bezüglich des zu betrachtenden Angreifermodells:

- Zur Umsetzung von Mixen werden asymmetrische Kryptosysteme benötigt; diese kann jeder Angreifer mit unbeschränkter Rechenleistung brechen. Aus diesem Grund wird ein komplextheoretisch beschränkter Angreifer vorausgesetzt.
- Ein globaler Angreifer kann nur mit einem immensen Aufwand das gesamte Internet abhören. Aus diesem Grund gehen viele alternative Lösungskonzepte (siehe Abschnitt 2) nur von einem lokalen Angreifer aus, der nicht alle Leitungen zwischen den zu schützenden Kommunikationspartnern beobachten kann. Falls allerdings eine Kommunikation in einem regional begrenzten Gebiet erfolgt, ist das Beobachten aller Leitungen (z.B. durch die Administratoren oder den Provider) leicht möglich. Alle Ansätze sollten demzufolge von einem Angreifer ausgehen, der sämtliche Leitungen belauschen und eventuell sogar Daten auf ihnen manipulieren kann.
- Da eine einzelne technische oder organisatorische Einheit zur Wahrung der Vertraulichkeit stets ein absolutes Vertrauen in sie selbst voraussetzt, sollte durch die Kaskadierung von Systemen verschiedenartiger Produkte und mit differierenden Betreibern eine höhere Sicherheit gewährleistet werden. Auf die Mixe bezogen bedeutet dies, daß alle außer einem Mix korrupt sein können.
- Der Blick über die Schulter des Teilnehmers deckt immer seine Identität bzw. die Anonymität seines Schaffens auf. Technisch könnte ein solcher Angriff durch das unbemerkte Kontrollieren seines Kommunikationsgerätes, z.B. mit Hilfe von Trojanischen Pferden, durchgeführt werden. Um anonym zu kommunizieren, muß der Teilnehmer demzufolge seiner lokalen Hard- und Software vertrauen können.
- Da der Einzelne nur innerhalb einer Menge anonym sein kann, muß vorausgesetzt werden, daß die Anzahl der Angreifer innerhalb der Anonymitätsgruppe gering im Vergleich zu der Gesamtzahl der Nutzer ist. Ein *n*-1-Angriff, bei dem sich alle anderen Teilnehmer gegen einen Nutzer verschworen haben, wird demzufolge nicht betrachtet.

Anhand dieses Angreifermodells können die verschiedenen Systeme verglichen und bewertet werden. Der Nutzer kann weiterhin abschätzen, unter welchen Voraussetzungen er anonym kommuniziert.

7 Praktische Anwendung

Die Umsetzung des Mix-Konzepts ist ansatzweise in einigen Anonymisierungsdiensten im Internet zu finden (z.B. bei den Mixmastern für den E-Mail-Dienst, siehe Abschnitt 2); die Systeme sind jedoch bislang noch nicht weit verbreitet. Um die Vor- und Nachteile von Mix-Systemen besser erforschen zu können, ist eine Erprobung in der

Praxis im Rahmen von realen Anwendungen nötig. Dies soll in dem Projekt „Neue Medien in der Kinder- und Jugendpsychiatrie" an der Medizinischen Universität zu Lübeck geleistet werden, das ein breitgefächertes Angebot an Internet-Diensten einschließlich anonymer Online-Beratung zur Prävention von Ecstasy-Konsum realisiert.

Gerade im Bereich der neuen Designerdrogen lassen sich Kinder und Jugendliche weniger über herkömmliche Beratungsangebote ansprechen. Da diese Gruppe in starkem Maße die neuen Medien nutzt, können über zielgruppenspezifische Internet-Angebote neue Wege der Suchtprävention beschritten werden. Durch ein im Hinblick auf Inhalt und Gestaltung niedrigschwelliges Angebot sollen für Jugendliche wichtige, mit Drogenkonsum und Abhängigkeit zusammenhängende Fragen beantwortet und auch Wege zur Unterstützung im Notfall, beispielsweise bei einer akuten Vergiftung, aufgezeigt werden. Die wahrheitsgemäße Beantwortung von online verfügbaren Checklisten und Fragebögen ermöglicht hilfesuchenden Jugendlichen eine subjektive Einordnung ihrer eigenen Gefährdung im Bereich Drogenkonsum. Die beantworteten Fragen können an ratgebende Therapeuten übermittelt werden. Weiter wird verschiedenen direkten Kommunikationsmöglichkeiten ein breiter Raum gegeben. Seine wesentlichen Bausteine sind ein Dienst für E-Mail an die Beratungsstelle und ein moderiertes Chatcafé. Letzteres soll zu bestimmten Zeiten geöffnet sein und von einem Therapeuten betreut werden, der Fragen zum Thema Ecstasy oder auch zu sehr persönlichen Problemen der Ratsuchenden online beantwortet. In diesem Zusammenhang werden auch Fragen zu kritischen Bereichen wie beispielsweise zu Beschaffungskriminalität erwartet, mit denen Jugendlichen im Normalfall weitgehend alleingelassen sind und ohne ein Vorwissen über tatsächliche Bestrafungsmöglichkeiten den Schritt zur hilfreichen Erstberatung nur selten finden.

Ein vertrauenswürdiges Umfeld, das wesentlich für jegliche Beratung ist, läßt sich technisch durch Mixe aufbauen. Um aussagekräftige Ergebnisse über den praktischen Einsatz von Mix-Technologien zu erhalten, wird im Projekt ein interdisziplinärer Ansatz verfolgt, bei dem Vertreter aus den Fachgebieten Informatik, Medizin, Psychologie und Rechtswissenschaften das Projekt begleiten. Von großer Bedeutung ist auch die Akzeptanz der Nutzer und die Schaffung von Vertrauen, was ebenfalls detailliert zu untersuchen ist.

Der Mix-Prototyp muß auf verschiedene Internet-Dienste erweitert werden, wie sie das Projekt der Online-Drogenberatung erfordert, das neben einer Webnutzung mit Sachinformationen, Checklisten und Online-Fragebögen auch Filetransfer, E-Mail-Versand und Teilnahme an moderierten Chatcafés anbietet. Dabei entstehen Probleme durch den unterschiedlich großen Bandbreitenbedarf verschiedener Dienste sowie in bezug auf die Akzeptanz von unvermeidbaren Verzögerungszeiten. Weiterhin läßt sich Dummy Traffic vom eigentlichen Nutzer zum Mix-System nur mit hohem Aufwand realisieren, da ihm nur beschränkte Übertragungskapazität zur Verfügung steht. Darüber hinaus muß der Nutzer dahingehend aufgeklärt sein, daß er nicht unbewußt seine Identität aufdeckt, beispielsweise durch gedankenloses Ausfüllen von Eingabe-

masken mit Namen und Geburtsdatum oder durch Verwendung von Browsern, die die E-Mail-Adresse an den anfragenden Server übermitteln.

Weitere praktische Anwendungsmöglichkeiten, in denen der Bedarf nach Anonymität der Nutzer evident ist, sind beispielsweise das Abgeben von Lotto-Tips, Diskussionen über umstrittene Themen, Abrufe von Informationen aus dem Sozialhilfe- oder medizinischen Bereich, Wahlen und Abstimmungen oder auch das Bewerten von eingereichten Artikeln bei Konferenzen [GoWB_97].

8 Zusammenfassung und Ausblick

Das beschriebene Konzept erweitert die bisherigen Ansätze der Mixe auf die Nutzbarmachung von HTTP. Ein Prototyp wurde bereits zur CeBIT ‘98 in Hannover vorgestellt [FeMa_98]. Derzeit wird beim Landesbeauftragten für den Datenschutz Schleswig-Holstein an einer vollständigen Implementierung gearbeitet, bei der nicht nur Webangebote, sondern auch weitere Internet-Dienste anonym genutzt werden können sollen.

Damit wird ebenfalls gezeigt, wie sich eine starke Anonymität realisieren läßt. Zwar ist in den Multimediagesetzen (Teledienstedatenschutzgesetz, Mediendienste-Staatsvertrag) vorgeschrieben, daß eine Inanspruchnahme von Diensten und ihre Bezahlung anonym oder unter Pseudonym ermöglicht werden muß, sofern dies technisch möglich und zumutbar ist. Doch zur Zeit läuft diese Forderung weitgehend leer, so daß hier erheblicher Umsetzungsbedarf besteht. Da gesetzlich der Grundsatz zur Datenvermeidung und Datensparsamkeit festgeschrieben ist, sind Verfahren, die eine starke Anonymität anbieten, anderen mit weniger starker Anonymität oder Pseudonymität vorzuziehen. Auf keinen Fall dürfen sich zweitklassige Verfahren mit „Pseudo-Anonymität“ durchsetzen, die einen umfassenden Schutz lediglich vorgaukeln.

Das Spektrum der potentiellen Anwendungsbereiche ist riesig, und das Bewußtsein der Nutzer über den Wert von Anonymität in der Informationsgesellschaft, in der anders als im herkömmlichen Bereich meist überall Spuren hinterlassen werden, wächst. Daher setzen sich die Datenschutzbeauftragten dafür ein, daß dem Recht der Nutzer auf informationelle Selbstbestimmung gerade in Kommunikationsnetzen Rechnung getragen wird.

Literatur

Boya_97 J. A. Boyan: The Anonymizer: Protecting User Privacy on the Web; Computer-Mediated Communication Magazine, 4 (9), September 1997, http://www.anonymizer.com.

Chau_81 David Chaum: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms; Communications of the ACM 24/2 (1981), 84-88.

Cott_95 Lance Cottrell: Mixmaster & Remailer Attacks; 1995, http://www.obscura.com/~loki/remailer/remailer-essay.html.

Danz_98 Uwe Danz: Schutz der Kommunikationsbeziehung im World Wide Web; Diplomarbeit, TU Dresden, Institut für Theoretische Informatik, 1998.

FePf_98 Hannes Federrath, Andreas Pfitzmann: „Neue“ Anonymitätstechniken – Eine vergleichende Übersicht; Datenschutz und Datensicherheit, 22 (1998) 11, 628-632.

FeMa_98 Hannes Federrath, Kai Martius: Anonymität und Authentizität im World Wide Web; 2. ITG Anwenderfachtagung „Internet – frischer Wind in der Telekommunikation“, 21.-22.10.1998, Stuttgart.

GoWB_97 Ian Goldberg, David Wagner, Eric Brewer: Privacy-enhancing Technologies for the Internet; IEEE COMPCON 97, IEEE Computer Society Press, 1997, 103-109, http://www.cs.berkeley.edu/~daw/privacy-compcon97-www/privacy-html.html.

GoWa_97 Ian Goldberg, David Wagner: TAZ Servers and the Rewebber Network – Enabling Anonymous Publishing on the World Wide Web; CS 268 Final Project, University of California, http://http.cs.berkeley.edu/~daw/cs268/taz.ps.

GüTs_96 Ceki Gülcü, Gene Tsudik: Mixing Email with Babel; 1996 Symposium on Network and Distributed System Security, IEEE Computer Society Press, 1996, 2-16, http://www.zurich.ibm.com/~cgu/Report/report.ps.gz.

LoEB_96 T. Lopatik, C. Eckert, U. Baumgarten: Mixed Mobile Internet Protocol; TU München, Institut für Informatik, 1996.

LPWA_97 Lucent Personalized Web Assistant 1997, http://www.bell-labs.com/project/lpwa/overview.html.

McCo_97 J. McCoy: Anonymous Networking and Virtual Intranets: Tools for Anonymous Corporations; Financial Cryptography FC 97, Springer, 1997, 33-37.

Möll_98 Ulf Möller: Anonymisierung von Internet-Diensten; Studienarbeit, Uni Hamburg, Fachbereich Informatik, 1998, http://agn-www.informatik.uni-hamburg.de/people/3umoelle/st.ps.

PfPW_89 Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: Telefon-MIXe: Schutz der Vermittlungsdaten für zwei 64-kbit/s-Duplexkanäle über den (2*64+16)-kbit/s-Teilnehmeranschluß; Datenschutz und Datensicherung, 13 (1989) 12, 605-622.

ReSG_98 Michael G. Reed, Paul F. Syverson, David M. Goldschlag: Anonymous Connections and Onion Routing; IEEE Journal on Selected Areas in Communication, Special Issue on Copyright and Privacy Protection, 1998, http://www.onion-router.net/Publications/JSAC-1998.ps.

ReRu_97 M. Reiter, A. Rubin: Crowds: Anonymity for Web Transactions; DIMACS Technical Report 97-15, 1997.

Roes_98 Thomas Roessler: Anonymität im Internet; Datenschutz und Datensicherheit, 22 (1998) 11, 619-622.