

Privacy Enhanced Technologies

Rainer Giedat Frank Markus Abbühl

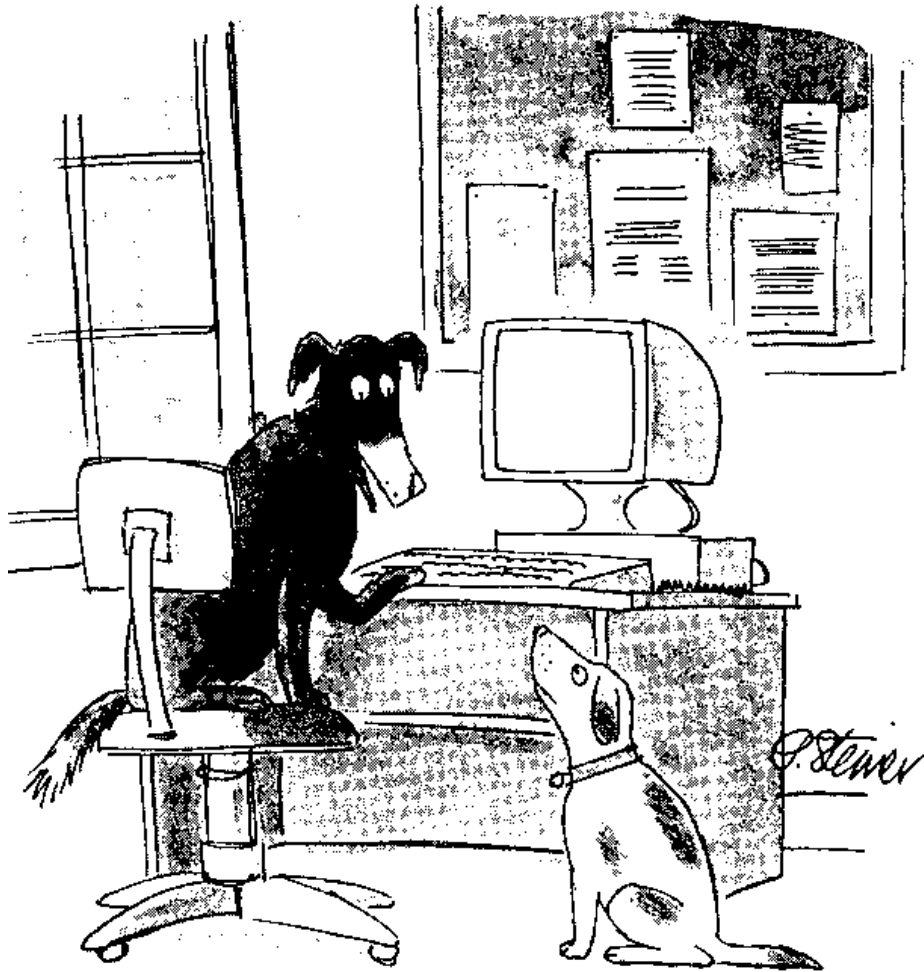
26. Juli 2002

Inhaltsverzeichnis

1	Einleitung	2
1.1	Überblick	3
1.2	Eingrenzung	3
1.3	Begriffe und Grundlagen	3
1.3.1	Datenschutz	3
1.3.2	Anonymität	4
1.3.3	Pseudonymität	4
1.4	Notwendigkeit von PETs	5
2	Technologien	5
2.1	Anon-Proxies	6
2.1.1	Angriffsmöglichkeiten	6
2.1.2	Der Anonymizer	7
2.1.3	Janus/Rewebber	7
2.2	Mixe	8
2.2.1	Das Mix-Konzept	8
2.2.2	Angriffe	10
2.3	Kombinierte Verfahren	10
2.3.1	Crowds	10
2.3.2	Peekabooby	11
3	Diskussion	12
3.1	Möglichkeiten des Mißbrauchs	12
3.2	Zukunftsmusik	13
3.2.1	Verbraucher	13
3.2.2	Gesetzgeber	13
3.2.3	Industrie und Dienstleister	13
3.3	Schlußwort	14

1 Einleitung

”Im Internet weiß keiner, daß du ein Hund bist”, so beschreibt ein Karikaturist der amerikanischen Zeitschrift ”The New Yorker” die vermeintliche Anonymität der Internetnutzer.



”On the Internet, nobody knows you’re a dog.”

Abbildung 1: Karikatur aus ”The New Yorker” vom 5. Juli 1993

Hätte er damals schon geahnt, welche Ausmaße das Sammeln von Daten der Portalschützer, Suchmaschinenbetreiber, Zugangsanbieter und der Werbetreibenden annimmt, wie der *Clickstream*¹ des Internetnutzers ausgewertet wird und wie mit Hilfe von Cookies und Sitzungsidentifikatoren detaillierte

¹Die Art und Weise, wie der Besucher durch eine Webseite navigiert

Persönlichkeitsprofile erstellt werden können, hätte er wohl geschrieben: "Im Internet weiß jeder, daß Du Schappi bevorzugst"

1.1 Überblick

Zu Beginn werden wir versuchen, wichtige Begriffe wie Datenschutz, Anonymität und Pseudonymität zu definieren und zu erklären sowie die relevanten datenschutzrechtlichen Grundlagen zu erläutern. Nach der Abgrenzung zu verwandten Themengebieten werden wir noch kurz auf die rechtliche Situation und die Notwendigkeit des Einsatzes datenschutzfreundlicher Technologien eingehen.

Der zweite Abschnitt befaßt sich mit den technischen Aspekten, wir werden anhand einiger Beispiele zeigen, wie Anon-Proxies, Mixe und einige weitere auf diesen Grundlagen aufbauende Technologien wie Crowds und dem neuen Peekabooby funktionieren.

Zum Schluß hin wollen wir kurz einige Möglichkeiten des Mißbrauch diskutieren und einen Ausblick auf zukünftige Entwicklungsmöglichkeiten bieten.

1.2 Eingrenzung

Datenschutzfreundliche Technologien werden in vielen Bereichen benötigt und eingesetzt, wie zum Beispiel Medizin, Medien, Verkehr und bargeldlosen Zahlungsverfahren. Im Anhang zu [2] werden diese detailliert beschrieben. Im Rahmen dieser Arbeit werden wir uns jedoch auf die Beschreibung datenschutzfreundlicher Technologien im Internet beschränken, einige der Schlußfolgerungen sind jedoch durchaus auf andere Bereiche übertragbar.

Zur Umsetzung datenschutzfreundlicher Technologien werden meist kryptographische Methoden wie Hashfunktionen, Digitale Signaturen, Zertifikate und verschiedene Verschlüsselungsverfahren eingesetzt. Eine genaue Beschreibung würde den Rahmen dieser Arbeit bei weitem sprengen, wir werden jedoch, soweit uns bekannt, die eingesetzten Verfahren zumindest nennen.

1.3 Begriffe und Grundlagen

1.3.1 Datenschutz

In der Deutschen Übersetzung des Titels *Privacy Enhanced Technologies* als *Datenschutzfreundliche Technologien* schwingt leider nicht mehr die gesamte Bedeutungsbandbreite des englischen Wortes "privacy" mit. Neben den gängigen Übersetzungen als Privatsphäre, Alleinsein oder Ungestörtheit faßt man "privacy" auch auf als "das Recht, in Ruhe gelassen zu werden" [4]. Das deutsche Recht spricht in diesem Zusammenhang auch von *Informationsselbstbestimmung*, was bedeutet, daß jeder Einzelne festlegen darf, welche Daten über ihn abgespeichert werden.

Um diesem Ziel gerecht zu werden, sollte man möglichst das Prinzip der *Datenvermeidung* verfolgen, also möglichst dafür sorgen, das problematische Daten gar nicht erst anfallen. Wenn dies nicht möglich ist, greift man auf das Prinzip der *Datensparsamkeit* zurück, man versucht einfach, so wenige personenbezogene Daten wie möglich zu erheben.

1.3.2 Anonymität

Anonymität ist ein Zustand, der durch den Prozeß der Anonymisierung erreicht wird. In [2] wird dieser wie folgt definiert: "Anonymisierung ist eine Veränderung personenbezogener Daten derart, daß die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr einer bestimmten oder bestimmbar natürlichen Person zugeordnet werden können." Diese absolute Forderung kann aber je nach Gesetzeslage auch etwas aufgeweicht werden. Im Falle des §3 BDSG bedeutet *nicht*: "nur mit einem unverhältnismäßig hohen Aufwand an Zeit, Kosten und Arbeitskraft". Weitere Ausweitungen von *nicht* sind vorstellbar, zum Beispiel "nur von autorisierten Dritten". Es gibt jedoch noch weitere Aspekte zu beachten: Üblicherweise geht man davon aus, daß derjenige anonym bleiben möchte, der die Informationen abruft, zum Beispiel aus dem World Wide Web. In diesem Fall spricht man von *Clientanonymität*. In bestimmten Fällen möchte jedoch auch der Anbieter von Informationen anonym bleiben [7], in diesem Fall spricht man von *Serveranonymität*.

Ebenso kann es wünschenswert sein, daß der Urheber und/oder der Adressat einer Nachricht anonym bleiben möchte, hier spricht man von *Sender-* bzw. von *Empfängeranonymität*. In verschiedenen Kontexten können diese Begriffe durchaus vermischt werden, zum Beispiel kann bei einer HTTP-Anforderung der Client sowohl Sender als auch Empfänger sein.

1.3.3 Pseudonymität

Eine spezielle Möglichkeit, die Anonymität von Personen zu wahren, ohne auf das Speichern der Daten selbst zu verzichten, ist die *Pseudonymisierung*. Gemäß [2] ist "Pseudonymisierung [...] das Verändern personenbezogener Daten durch eine Zuordnungsvorschrift derart, daß die Einzelangaben über persönliche oder sachliche Verhältnisse ohne Kenntnis oder Nutzung der Zuordnungsvorschrift nicht mehr einer natürlichen Person zugeordnet werden können." Selbstverständlich sind hierbei für das Wort *nicht* die gleichen Erweiterungen denkbar, wie im Falle der Anonymisierung.

Man unterscheidet *selbstgenerierte Pseudonyme*, *Referenz-Pseudonyme* und *Einweg-Pseudonyme*. Im ersten Fall nimmt der Betroffene selbst die Pseudonymisierung vor, im zweiten Fall ist eine Wiederherstellung des Bezuges zur Person möglich, allerdings nur durch Konsultation einer Referenzliste. Einweg-Pseudonymen werden, wie der Name schon sagt, mit Hilfe von

Einweg-Funktionen² erstellt. Der Bezug zur Person kann nur durch Kenntnis der Funktionsparameter wiederhergestellt werden.

1.4 Notwendigkeit von PETs

Eigentlich werden den datenschutzrechtlichen Interessen der Bürger durch die deutsche und europäische Gesetzgebung sehr gut geschützt. In [2] werden zahlreiche Beispiele genannt: Bereits im Volkszählungsurteil von 1983 wird der Anspruch auf Anonymisierung anerkannt, "Informationelle Selbstbestimmung" und "möglichst frühzeitige faktische Anonymisierung" sind gemäß (BVerfGE 65, 1-49) unverzichtbar. Neben dem Bundesdatenschutzgesetz (BDSG) kennen auch das Informations- und Kommunikationsdienstesgesetz (IuKDG) mit dem Teledienstedatenschutzgesetz (TDDSG) und im Mediendienste Staatsvertrag (MDStV) den Grundsatz der Datenvermeidung.

Wenn doch alles so gut geregelt ist, warum sollte sich der einzelne dann noch selbst um den Schutz seiner Daten kümmern?

Der offensichtlichste Grund ist die Tatsache, daß es sich beim Internet um ein weltumspannendes Netzwerk handelt, die genannten Gesetze jedoch nur bundesweit oder teilweise europaweit gelten. Niemand (außer der amerikanischen Gesetzgebung) kann einem amerikanischen Dienstleister verbieten, Daten über seine europäischen Kunden zu sammeln.

Darüberhinaus bieten, wie wir später noch zeigen werden, datenschutzfreundliche Technologien auch die Möglichkeit, die in einigen Staaten leider immer noch herrschende Zensur zu umgehen. Dies kann aber nur mit Hilfe der sogenannten "freien Welt" funktionieren.

Und nicht zuletzt hat der Einsatz dieser Technologien einen vorbeugenden Effekt: Wenn sich die Menschen jetzt an deren Einsatz gewöhnen, wird es in der Zukunft, wenn jeder den Schutz seiner Privatsphäre als Selbstverständlichkeit betrachtet, sehr viel schwieriger sein, diesen zum Beispiel nach einem Regimewechsel gesetzlich zu verbieten, ohne Proteste in der Bevölkerung zu provozieren.

Datenschutzfreundliche Technologien geben dem Verbraucher die Möglichkeit, den Schutz seiner eigenen Daten auch selbst in die Hand zu nehmen und sich durch aktive Datenvermeidung gegen Datensammler und Zensur zu wehren.

2 Technologien

In diesem Kapitel werden wir die technische Umsetzung von einigen bekannten Programmen besprechen. Dazu werden wir zuerst allgemein auf

²auch Hash-Funktionen genannt

die zugrundeliegende Theorie eingehen, uns dann mit den Vor- und Nachteilen beschäftigen, Angriffsmöglichkeiten und Schwächen besprechen und zum Schluß jeweils ein oder zwei Programme vorstellen, die das Besprochene leisten. Dabei gilt es, sehr unterschiedliche Ansprüche zu erfüllen:

Das Lesen von Dokumenten im World Wide Web oder im Usenet, das Herunterladen von Daten per File Transfer Protocol (FTP) kann problemlos vollkommen anonym erfolgen. Die einfachste Möglichkeit, Client- und/oder Serveranonymität zu gewährleisten, bieten sogenannte *Anon-Proxies*.

Wer hingegen Emails versendet, möchte seine Identität im Normalfall³ nicht vor dem Empfänger verbergen. Allerdings gibt es gute Gründe, Nachrichten unbeobachtet auszutauschen. Das Wie und Warum wird im Abschnitt über die Mail-Mixe besprochen.

Die genannten Technologien decken die wesentlichen Internetprotokolle ab, weisen jedoch zum Teil inherente Schwächen auf, die nur durch eine Kombination der Verfahren gemindert oder gar aufgehoben werden können. Um solche Programme geht es im letzten Abschnitt.

2.1 Anon-Proxies

Ein gewöhnlicher Proxy-Server fungiert als Stellvertreter zwischen Sender und Empfänger. Der Webbrowser des Betrachters schickt die Anfrage für eine Webseite an den Proxy-Server, dieser leitet die Anfrage *stellvertretend* an den Webserver weiter, welcher seinerseits die Anfrage bearbeitet und die Antwort an den Proxy-Server zurücksendet, welcher sie wiederum an den Rechner des Betrachters weiterleitet.

Diese Methodik wird im Prinzip auch von Anon-Proxies verwendet. Um die Anonymität des Betrachters zuverlässig zu schützen, muß der Anon-Proxy aktiv eingreifen und zum Beispiel Metainformationen, die automatisch vom Webbrowser übermittelt werden zu entfernen und die zurückgesendete Antwort von "gefährlichen Inhalten" wie Cookies, JavaScript und ActiveX zu befreien. Auch Verweise auf andere Seiten (sogenannte Hyperlinks) werden derart verändert, daß sie dem Browser wieder den Weg über den Anon-Proxy weisen. Auf diese Weise wird eine mehr oder weniger lückenlose Clientanonymität gewährleistet, auf ähnliche Art und Weise sorgt Janus/Rewebber auch für Serveranonymität.

2.1.1 Angriffsmöglichkeiten

Der c't Artikel [3] nennt drei strukturelle Nachteile:

Anon-Proxies bieten keinen Schutz vor dem Betreiber selbst, da dieser sowohl den Sender als auch den Empfänger kennt und diese Informationen problemlos verwerten könnte.

³außer es handelt sich um einen Werbe-Spammer

Zweitens kann das Parsen der HTTP- und FTP-Übertragungen oder von HTML-Seiten nicht immer lückenlos funktionieren: Es gibt immer einen Weg, zum Beispiel mit Hilfe von Code-Obfuskation oder durch Ausnutzen von Eigenheiten des Webbrowsers den Parser außer Kraft zu setzen. Reduziert man Webseiten auf den reinen Textinhalt, geht zu viel Information verloren und die Benutzer werden diese Technologie nicht akzeptieren.

Ein weiteres unlösbares Problem stellt ein "Großer Bruder"⁴ dar: Wer über die technischen Mittel verfügt, die ein- und ausgehende Kommunikation eines Anon-Proxy zu beobachten, kann diese leicht in Korrelation bringen, da die Anfragen zeitlich dicht zusammenliegen.

Eine im Artikel nicht genannte aber sehr einfache Möglichkeit besteht darin, einfach die Benutzung des Anonymisierungsdienstes bzw. aller Anonymisierungsdienste zu verbieten oder schlicht durch eine Firewall zu unterbinden.

2.1.2 Der Anonymizer

Eine der ersten Firmen, die kommerzielle Lösungen für datenschutzfreundliche Technologien im Internet anbietet, ist die 1996 gegründete Firma *Anonymizer.com*. Neben der klassischen Anonymisierung von Webzugriffen bietet die Software gesicherte Cookies, URL-Verschlüsselung, Werbefilter und anonymes versenden von Email.

Beim "Anonymizer surfing" mit "Secure Tunneling" wird mit Hilfe der port-forwarding Funktion der Secure Shell ein verschlüsselter Tunnel zum Anonymizer Server aufgebaut, so daß auch die Kommunikation zwischen Anwender und Anon-Proxy nicht von Dritten⁵ belauscht werden kann.

Hier noch ein exemplarische Zugriff aus der Logdatei des Webservers beim Zugriff auf meine Homepage...

```
access.log.1:168.143.113.120 - - [22/Jul/2002:16:46:12 +0200] \
"GET / HTTP/1.0" 200 604 "-" "Mozilla/4.78 (TuringOS; Turing Machine; 0.0)"
```

...und ein veränderter Hyperlink aus der zurückgelieferten Seite:

```
<a href="http://anon.free.anonymizer.com/http://marax.dyndns.org/~phrank">
```

2.1.3 Janus/Rewebber

Das Projekt *Janus*⁶ wurde an der Fernuniversität Hagen entwickelt und wird nun unter dem Namen *Rewebber* kommerziell vermarktet.

Im Unterschied zu einem einfachen Anonymisierungsdienst, wie er oben beschrieben wurde, bietet Janus/Rewebber die Möglichkeit, die Anonymität in beiden Richtungen zu gewährleisten, also zusätzlich auch Server-Anonymität

⁴Angelehnt an den "Big Brother" aus George Orwells Roman "1984"

⁵Arbeitgeber, Internet Service Provider, Netz-Infrastrukturbetreiber

⁶Vorlage war der Zweigesichtige Gott aus der griechisch-römischen Mythologie

zu bietet. Der Betreiber einer Webseite kann die URL mit dem öffentlichen Schlüssel des Rewebbers verschlüsseln und nur dieser kann mit seinem privaten Schlüssel wieder die ursprüngliche Adresse wiederherstellen. Die unverschlüsselte URL der Zeitschrift Datenschutz und Datensicherheit...

<http://www.dud.de/>

...sieht verschlüsselt wie folgt aus:

[http://janus.fernuni-hagen.de/janus_encrypted/MTCJP0kAFqxDL90HDhMsvd7RHTitnujYJNit0if0mHEx+Jgx41kM0r4D+N\\$E320GHFJwqbKe39Y61H1PYufLvS\\$biQ0pH90c0F6q0WB6h4p7dLXR0S945ryA6g114zWVg=](http://janus.fernuni-hagen.de/janus_encrypted/MTCJP0kAFqxDL90HDhMsvd7RHTitnujYJNit0if0mHEx+Jgx41kM0r4D+N$E320GHFJwqbKe39Y61H1PYufLvS$biQ0pH90c0F6q0WB6h4p7dLXR0S945ryA6g114zWVg=)

Auf diese Weise können beide Seiten die Zensur umgehen: Zum einen kann sich der Betreiber einer Webseite dazu entschließen, nur die verschlüsselte URL zu veröffentlichen und so selbst anonym zu bleiben, er muß allerdings selbst darauf achten, keine aufschlußreichen Inhalte auf seinen Seiten unterzubringen. Zum anderen kann der Besucher den Rewebber wie einen gewöhnlichen Anon-Proxy benutzen und selbst die Ziel-URLs verschlüsseln, so daß auch hier Negativlisten nicht greifen. Die Verwendung einer komplett verschlüsselten Verbindung zum Anon-Proxy wäre hier jedoch sinnvoller, da sonst zumindest Inhaltsfilter auf Stichwörter anspringen könnten.

2.2 Mixe

2.2.1 Das Mix-Konzept

Bei der Kommunikation über E-Mail ist der Inhalt der Nachrichten nicht das einzigste schützenswerte Gut hinsichtlich der Privatsphäre. Oft wird als Argument gegen Verschlüsselung hervorgebracht, daß so kommunizierende Partner den Eindruck hinterlassen etwas zu Verbergen zu haben und somit erst recht das Interesse eines mutmaßlichen Beobachters auf sich ziehen würden. Deshalb ist es erstrebenswert neben dem Inhalt auch die Identität der Kommunikationspartner geheim zu halten. Dabei muß der Empfänger aber trotzdem wissen von wem er eine Nachricht erhalten hat und muß in der Lage sein dessen Identität zu überprüfen. Ein erster Ansatz wäre die Verschlüsselung der Adressen. Da die an der Übertragung beteiligten Mail-Server die Adressen zur korrekten Weiterleitung benötigen, wäre eine solche Mail nicht mehr auslieferbar oder der bearbeitende Server (möglicherweise nicht vertrauenswürdig) müsste diese entschlüsseln und alles wäre umsonst. Als Lösung wird die Nachricht über eine Reihe von Servern versendet. Dafür präpariert der Absender E-Mail indem er für jede beteiligte Station einen Header mit der Adresse der nächsten Anhängt und alles mit dessen public Key verschlüsselt. Aus diesem Grund kennt jeder Server nur die Adresse der letzten und nächsten Station. Solange nur einer von ihnen

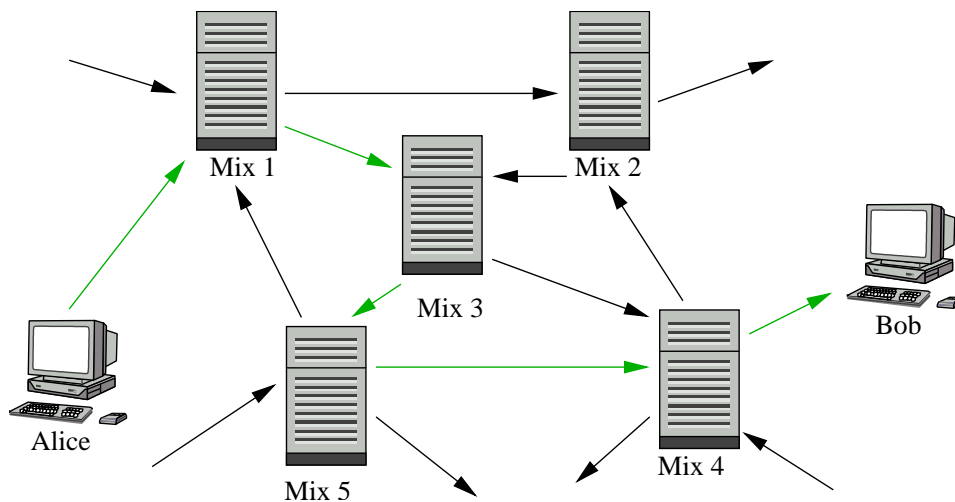


Abbildung 2: Vorbestimmter Weg einer Email durch das Mix-Netz

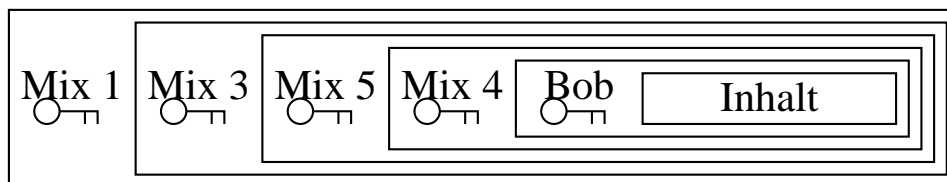


Abbildung 3: Verschachtelte Verschlüsselung dieser Email

vertrauenswürdig ist erfolgt die Übermittlung anonym, weil jeder höchstens den Sender oder den Empfänger, aber nie beide kennen kann. Ihre Namen haben die Mixe aber wegen einer anderen, entscheidenden Eigenschaft. Angenommen eine Art *Big Brother* wäre in der Lage das gesamte Netz zu beobachten. Er könnte aufgrund der Zeit und der Reihenfolge der ein- und ausgehenden Nachrichten - die zweite die reinkommt geht als zweites wieder raus - die E-Mail vom Sender zum Empfänger verfolgen. Deshalb 'mixt' der Mix die Nachrichten durcheinander um keinen Rückschluss aufgrund der Reihenfolge zuzulassen. Um den Beobachter noch mehr durcheinander zu bringen werden eingehende Botschaften eine Zeit lang gesammelt und dann Schubweise ausgesendet und gelegentlich mit Dummy-Traffic vermischt. Letzteres wird sich aber wohl schwer durchsetzen, weil sich zusätzlicher Verkehr negativ auf die Performance des Netzes auswirken kann und auf nach Datenvolumen abgerechneten Verbindungen zusätzlich Geld kostet. Bei Mixen wird eine bestimmte Länge der Nachrichten gefordert um einem Angreifer die Möglichkeit zu nehmen sie aufgrund ihres Aussehens zu verfolgen.

2.2.2 Angriffe

Ein Spion könnte aber auch eine eingehende E-Mail abfangen und zweimal kurz hintereinander durch den Mix schicken. Diejenige (nun, weil entschlüsselt, anders aussehende), die zwei mal herauskommt ist dann die, die der Angreifer vorher geklont hat - er kann ihren Weg verfolgen. Um dies zu verhindern berechnet ein Mix eine Checksumme über eingehende E-Mails und speichert diese in einer Datenbank vorübergehend ab. Alle innerhalb einer gewissen Zeit eingehenden Nachrichten, mit gleicher Checksumme (mit sehr, sehr hoher Wahrscheinlichkeit gleiche E-Mails) werden dann nicht weiterverarbeitet.

Die einzige Möglichkeit, die ein Angreifer nun noch hat, wäre so viele E-Mails über einen Mix zu verschicken, daß alle bis auf eine von ihm selbst sind. Dadurch weiß er, daß die Nachricht die er nicht kennt die ist, die er verfolgen möchte. Auf so eine Art Attacke kennt ein Mix leider keine passende Antwort.

2.3 Kombinierte Verfahren

2.3.1 Crowds

In Crowds verbinden sich möglichst viele Web-Benutzer um durch ihre große Anzahl ihre Spuren zu verwischen. Dazu werden die Anfragen an einen Web-Server nicht direkt an diesen gestellt, sondern an ein beliebiges Mitglied der "Menschenmenge". Selbst dieser ist nun schon nichtmehr in der Lage zu entscheiden, ob der Absender des empfangenen Packets der ursprüngliche Absender ist oder auch nur ein Crowd-Mitglied, das selbst nur eine empfangene Anfrage weitergeleitet hat. Jetzt wird das Packet entweder an das Ziel oder wieder an ein weiteres, zufällig ausgewähltes, Mitglied geschickt. Jede beteiligte Station⁷ merkt sich seine Entscheidung, damit sie die Antwort den selben Weg wieder zurück übertragen kann. Das ist dringend nötig, denn ein Jondo darf und kann nicht wissen wer die Anfrage ursprünglich gestellt hat. Jede weitere Anfrage wird von nun an über den selben Weg gehen. Die Übertragung zwischen jeweils zwei Jondos werden symmetrisch (aus Performancegründen) verschlüsselt.

Crowds bieten keinen Schutz gegen allsehende Big Brother. Dieser sieht, wenn von einem Jondo eine Verbindung ausgeht ohne daß vorher eine eingegangen ist (Client) und kann den Datenfluß zwischen jeweils zwei Jondos bis zum Server verfolgen. Hat der Beobachter keine Einsicht in das Netz in dem die Crowd-Mitglieder oder der Server stehen ist Server- bzw. Clientanonymität gewährleistet.

⁷Der Crowd-Client, eine Art Proxy-Server, heißt *jondo*, was sich wiederum von "John Doe" ableitet. Dieser Name wird in Amerika Koma-Patienten mit unbekannter Identität gegeben

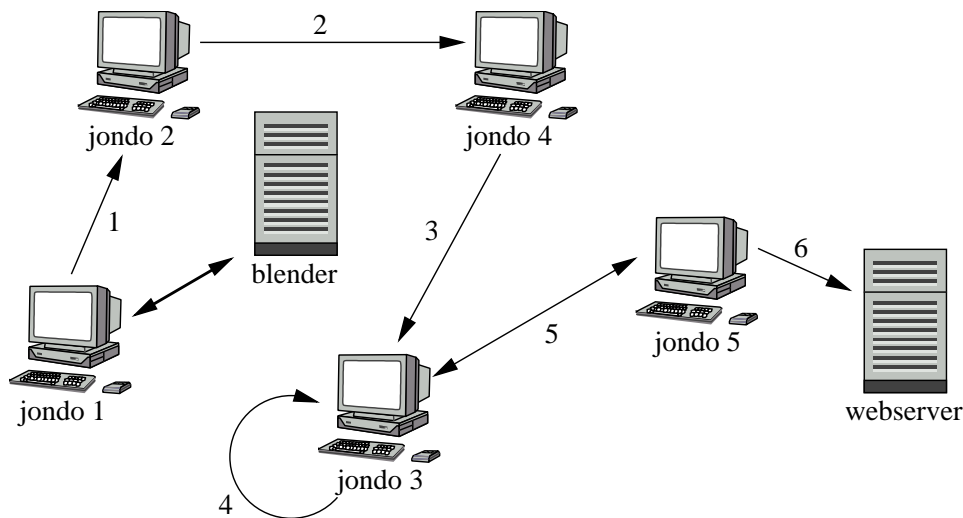


Abbildung 4: Zufälliger Weg einer HTTP-Anfrage durch die Crowd

Arbeitet eines der Mitglieder als Schnüffler, kann er natürlich die in der Anfrage enthaltene Server-Adresse lesen, da er sie entschlüsseln kann. Das ist für ihn nur von Nutzen, wenn er herausfinden kann, wer die Anfrage gestellt hat. Dazu benötigt er aber die Hilfe eines externen Beobachters oder er nimmt an, daß sein direkter Vorgänger die Anfrage gestellt hat. Die Wahrscheinlichkeit für letzteres ist aber $\frac{1}{2}^n$ (mit $n = \text{Anzahl der Crowd-Mitglieder}$).

Ein Server kann bei der Benutzung von Crowds nicht wissen, wer die ursprüngliche Anfrage gestellt hat. Weiß der Server allerdings nicht daß er es mit einer Crowd zu tun hat, hält er immer den letzten Jondo der Kette für den Betrachter der Web-Seite. Das könnte der Akzeptanz von Crowds schaden, denn dadurch würde jedes Mitglied Gefahr laufen für die Benutzung verbotener Dienste durch andere Mitglieder belangt zu werden.

Um eine Crowd zu verwalten muß eine zentraler Server (blender) existieren bei dem sich ein Jondo anmelden muß um einer Crowd beizutreten. Der Blender hält eine Liste mit allen angemeldeten Jondos bereit damit jeder weiß, wer zur Verfügung steht.

2.3.2 Peekabooty

Peekabooty wurde entworfen um Zensur im Internet zu erschweren. Mit dieser Software sollen die Benutzer in der Lage sein Zensur (z.B. durch Firewalls) mit der Hilfe Anderer außerhalb der indizierten Zone zu umgehen, möglichst ohne dabei erwischt zu werden.

Da nur Inhalte, die im Klartext vorliegen gefiltert werden können, sendet ein Knoten die Anfrage verschlüsselt an einen Partner im unzensierten Teil

im Netz und erhält von diesem die Inhalte dann verschlüsselt wieder zurück. In dieser Hinsicht arbeitet Peekabooty wie eine Crowd mit SSL-Verschlüsselung. Wie bei Crowds lebt Peekabooty von der Tatsache, daß eine große sich ständig ändernde Gemeinschaft aus Hosts schwer zu überwachen und zu blocken ist.

Der Knackpunkt dieses Verfahrens ist aber die *Initial Discovery*: Wie erfährt ein Knoten die Adressen der zur Verfügung, stehenden heimlichen Helfer ohne dabei beobachtet zu werden? Riecht nämlich eine zensierende Institution den Braten, kann sie die IP-Adressen der beteiligten Computer sperren (oder schlimmeres). Um das zu verhindern verfolgt Peekabooty zwei Ansätze:

1. Es werden Ressourcen benutzt, die eine zensierende Institution nicht einfach sperren kann, ohne sich damit selbst zu schaden. Peekabooty benutzt deshalb die Standard-Ports für SMTP, FTP und HTTPS.
2. Zur Übermittlung der benötigten Daten (IP-Adressen der Genossen) wird Steganographie verwendet.

3 Diskussion

Wir haben eben gesehen, wie man sowohl als Konsument als auch als Anbieter von Informationen das Prinzip der Datenvermeidung selbst aktiv umsetzen kann, indem man mit Hilfe datenschutzfreundlicher Technologien anonym und unbeobachtet über das Internet kommunizieren kann. Nun werden wir versuchen, die Möglichkeiten und Konsequenzen zu besprechen und die Vor- und Nachteile die sich daraus ergeben gegeneinander abzuwiegen.

3.1 Möglichkeiten des Mißbrauchs

Wie leider jede Form von Technologie bieten auch die datenschutzfreundlichen Technologien immer die Möglichkeit zum Mißbrauch. Wie kann man verhindern, daß jemand die eigentlich zum Schutz der Privatsphäre gedachten Vorkehrungen ausnutzt, um beispielsweise Nazipropaganda oder die allerorts gefürchtete Kinderpornographie zu verbreiten? Und wer soll darüber entscheiden, welche Inhalte "unerwünscht" sind?

Hier gibt es zwei Mögliche Antworten: Entweder man verbietet die Technologie an sich oder man verbietet zwar den Mißbrauch, nimmt aber erschwerte Bedingungen in Kauf.

Das Problem mit der ersten Lösung ist altbekannt: Ein Verbrecher wird sich sicher nicht durch ein Verbot davon abhalten lassen, diese Technologien einzusetzen, um weitere (und meist weitaus schlimmere) Verbrechen zu begehen. Ein reines Verbot hätte also nur zur Folge, das rechtschaffene Bürger, die um ihre Privatsphäre besorgt sind, kriminalisiert werden.

Selbst in Ländern wie Amerika, Kanada oder Frankreich, die vor wenigen Jahren noch den Einsatz von Kryptographie verboten oder zumindest eingeschränkt haben, wurden die Gesetze sehr zugunsten der zweiten – und in unseren Augen auch vernünftigeren – Lösung angepaßt.

3.2 Zukunftsmusik

In [2] ergeht der Appell an Verbraucher, Gesetzgeber sowie Industrie und Dienstleistungsanbieter, datenschutzfreundliche Technologie zur fordern, zu fördern und bereitzustellen. Doch diese Dreiecksbeziehung kann nur funktionieren, wenn sich für alle beteiligten daraus ein Vorteil ergibt.

3.2.1 Verbraucher

Wie die eingangs erwähnte Karikatur "On the Internet, nobody knows you're a dog" illustriert, glaubt ein großer Teil der Internetteilnehmer immer noch, sich tatsächlich vollkommen anonym in den weltweiten Netzen zu bewegen. Ein noch größerer Teil ist sich zwar durchaus der Tatsache bewußt, daß er Spuren hinterläßt, ist aber nicht bereit, zusätzliche Programme zu installieren und zu konfigurieren, längere Übertragungszeiten in Kauf zu nehmen, kurz, einen nicht zu vernachlässigenden Zusatzaufwand zu betreiben.

Um die erste Gruppe zu alarmieren, wird sehr viel Aufklärungsarbeit nötig sein, doch das wesentlich größere Problem stellt die zweite Gruppe dar: Diesen Anwenderkreis kann man nur gewinnen, man man ihm den Einsatz von datenschutzfreundlicher Technologie so einfach wie möglich macht. Erst wenn alle Emailprogramme richtig und automatisch – am besten proaktiv – Nachrichten ver- und entschlüsseln und nur noch das Umlegen eines Schalters notwendig ist, um beim Verschicken eine Mixkette zu definieren, erst wenn jeder Webbrowser einen Knopf besitzt, der anonymes Surfen ein- und ausschaltet, wird die Breite Masse von solchen Technologien gebrauch machen.

3.2.2 Gesetzgeber

Trotz immer wieder aufflackernder Forderungen nach noch mehr Überwachung ist die gesetzliche Lage in Deutschland und sogar in der ganzen Europäischen Union sehr datenschutzfreundlich. Selbst Frankreich, wo noch bis vor kurzem der Einsatz Kryptographie verboten war und unter das Waffenrecht fiel, hat geradezu eine 180 Wende unternommen [4].

3.2.3 Industrie und Dienstleister

Der Appell an Industrie und Dienstleistungsanbieter "für den Verbraucher transparentere Systeme zu schaffen und datenschutzfreundliche Technologien verstärkt in ihre Systeme einzubauen" [2] wird jedoch nur umgesetzt

werden, wenn sich die Unternehmen durch deren Einsatz einen Wettbewerbsvorteil versprechen.

Zur Zeit sieht die Lage jedoch ganz anders aus: Die Unternehmen erhalten ihren Wettbewerbsvorteil gerade durch das Gegenteil: Das Sammeln und Auswerten von Kundendaten und dem Kundenverhalten. Man wird also alles erdenkliche tun, weiterhin intransparente Systeme zu schaffen und den Kunden dazu verleiten, möglichst viele persönliche Informationen preizzugeben. Daran wird sich auch nichts ändern, ehe sich ein stärkerer Druck vom Verbraucher ausgeht. Ein Teufelskreis.

3.3 Schlußwort

Wir wollen mit den Worten des Autors von Peekabooby schließen: "The goal is not a 100% censor-free network. The goal is to raise awareness of the issue worldwide. The goal is to open up people's eyes so that this software is not needed anymore."

Literatur

- [1] Bundesdatenschutzgesetz (BDSG), Stand Januar 2002
- [2] Arbeitspapier "Datenschutzfreundliche Technologien", Stand 11/1997, <http://www.datenschutz-berlin.de/to/datenfr.htm>
- [3] Hannes Federrath et al: "Tarnkappen fürs Internet", c't Magazin für Computertechnik, 16/2000
- [4] Éloïse Gratton: "The legality of online Privacy-Enhancing Technologies", ©2002 Lex Electronica, <http://www.lex-electronica.org>
- [5] Thomas Demuth, Matthias Sonntag: "Anonymität im World Wide Web", Telepolis 18.07.2001, Verlag Heinz Heise
- [6] Thomas Demuth: "Der Rewebber, Anonymität im World Wide Web",
- [7] Thomas Demuth, Andreas Rieke: "Janus - Schutz von Inhaltenanbietern im WWW", Datenschutz und Datensicherheit 22, 1998
- [8] Michael Reiter, Aviel Rubin: "Crowds: Anonymity für Web Transactions", AT&T Labs Research
- [9] Paul Baranowski: "Peekabooby: Distributed Anti-Censorship Software", Peekabooby Documentation Whitepaper