Das AN.ON-System – Starke Anonymität und Unbeobachtbarkeit im Internet

Hannes Federrath
Freie Universität Berlin, Institut für Informatik

In: Bäumler, Mutius (Hg.): Das Recht auf Anonymität, 2003

1 Einführung

Als der Gesetzgeber im Jahr 1997 das Teledienstedatenschutzgesetz (TDDSG) verabschiedete, zeigte er durchaus Mut. Dort wurde im § 4 Abs. 1 festgelegt:

> 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 Möglichkeit zu informieren.

Nach der Novellierung des TDDSG im Rahmen des Gesetzes über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr (EGG) am 9.11.2001 wurde aus dem zitierten Absatz der § 4 Abs. 6 TDDSG (Pflichten des Diensteanbieters); inhaltlich wurden jedoch an diesem Abschnitt keine Veränderungen vorgenommen.

Mit den Terroranschlägen vom 11. September 2001 ist das Risiko und verständlicherweise auch die Angst der Menschen gewachsen, Opfer von Terrorakten zu werden. Natürlich sah und sieht sich der Staat in der Pflicht, seine Bürger bestmöglich vor Terror zu schützen.

Man kann und sollte den Verbleib des zitierten Absatzes auch nach den Terroranschlägen als Bestätigung sehen, dass selbst unter dieser schwierigen Ausgangslage dem Bürger die Möglichkeit gegeben werden sollte, sich und seine Kommunikation zu schützen. Insbesondere bieten die Vorschriften der Strafprozessordnung (StPO, § 100 a, g, h) weitreichende Möglichkeiten sowohl der Strafverfolgung als auch der Prävention (nach einem Verdacht auf eine bevorstehende Straftat). Zu den rechtlichen Grundlagen von Anonymität im Internet siehe auch [2] in diesem Buch.

2 Das Projekt AN.ON

Seit Januar 2000 fördert das Bundeswirtschaftsministerium das Forschungs- und Entwicklungsprojekt „AN.ON – Starke Anonymität im Internet“. Das Ziel dieses Projekts ist die Schaffung eines offenen Systems zur anonymen Internetkommunikation. Die Quellcodes der Software sind öffentlich bekannt. Jeder interessierte Programmierer kann sich an der (Weiter)-Entwicklung der Software beteiligen oder auch nur nachvollziehen, wie das System arbeitet und sich so vom tatsächlichen Schutzniveau des Verfahrens überzeugen.

Die Entwicklung und Förderung von Software mit offengelegtem Quellcode insbesondere im Sicherheitsbereich Tradition. Auch das Bundeswirtschaftsministerium hat mit seiner Förderung von AN.ON seine Unterstützung für des Open-Source-Projekte erneut bewiesen. Mit dem Gnu Privacy Guard (GPG) [3] entstand eine unabhängige Implementierung einer Verschlüsselungssoftware, die zu der sehr bekannten und weit verbreiteten Software Pretty Good Privacy (PGP) [7] kompatibel ist. Das bedeutet, PGP-Benutzer können auch mit GPG verschlüsselte Nachrichten entschlüsseln und umgekehrt.

3 Technische Grundlagen

Die technische Basis des im AN.ON-Projekt entwickelten Systems ist das Verfahren der umkodierenden Mixe, das im Jahre 1981 von dem amerikanischen Kryptographen David Chaum publiziert wurde [1] hier vereinfacht dargestellt wird. Eine

ausführliche Beschreibung des Mix-Netzes findet sich beispielsweise in [6].

Umkodierende Mixe realisieren die Unbeobachtbarkeit der Kommunikationsbeziehung zwischen einem Sender und einem Empfänger. Hierzu sendet der Sender seine Nachricht nicht direkt an den Empfänger, sondern über mehrere hintereinandergeschaltete Rechner, sog. Mixe, die jeweils von unabhängigen Betreibern betrieben werden. Um die Verkettung der ein- und ausgehenden Nachrichten eines Mixes durch einen Beobachter zu verhindern, haben alle eingehenden Nachrichten die gleiche Länge und wurden vom Sender mit dem öffentlichen Verschlüsselungsschlüssel des Mixes verschlüsselt. Der Mix sammelt Nachrichten mehrerer Sender, entschlüsselt sie und gibt sie in veränderter Reihenfolge (zufällig, d.h. gemixt, oder geordnet, auf alle Fälle aber unabhängig von der Eingangsfolge) wieder aus.

Ein solches Verfahren realisiert die Anonymität des Senders bezüglich seiner gesendeten Nachricht (sog. Senderanonymität), d.h. der erste Mix sowie alle anderen potentiellen Beobachter kennen zwar den Sender einer (verschlüsselten) Nachricht, erfahren jedoch weder etwas über den Empfänger, noch über den Inhalt der Nachricht. Der letzte Mix kennt den Empfänger einer Nachricht, kann jedoch nicht den Sender zuordnen. Mittlere Mixe kennen jeweils nur den vorhergehenden und den nachfolgenden Mix, über den die Nachrichten gesendet wurden.

Die Kommunikationsbeziehung zwischen Sender und Empfänger bleibt selbst dann unbeobachtbar für alle Außenstehenden, Mixbetreiber und Netzbetreiber, wenn sie alle Verbindungen des Kommunikationsnetzes abhören und aufzeichnen können. Erst wenn alle an einer Kommunikationsbeziehung beteiligten Mixe zusammenarbeiten, können die Mixe eine Verbindung enttarnen.

Da ein Mix verschlüsselte Nachrichten konstanter Länge empfängt, muss der Sender die Nachrichten für die Mixe vorbereiten. Er muss zu kurze Nachrichten um Füllzeichen erweitern und zu lange Nachrichten entsprechend aufteilen. Eine Nachricht wird ggf. zunächst mit dem Verschlüsselungsschlüssel des Empfängers verschlüsselt und dann mit der Empfängeradresse versehen. Anschließend wird die Nachricht mit dem öffentlichen Verschlüsselungsschlüssel des letzten Mixes verschlüsselt, das Ergebnis mit dem öffentlichen Verschlüsselungsschlüssel des vorletzten Mixes noch einmal verschlüsselt u.s.w. Schließlich entsteht eine mehrfach verschlüsselte Nachricht, die an den ersten Mix gesendet wird und von ihm (und nur von ihm) entschlüsselt werden kann. Das Ergebnis dieser Entschlüsse-

lung kann nur vom zweiten Mix entschlüsselt werden u.s.w. Jeder Mix entfernt gewissermaßen eine Verschlüsselungsschale.

Um einen Angriff durch Nachrichtenwiederholung zu verhindern, testet ein Mix, ob er eine eingehende Nachricht (bzw. einen sog. Fingerabdruck von ihr) bereits verarbeitet hat und verwirft sie gegebenenfalls. Um einen Angriff durch probeweise Verschlüsselung einer ausgegebenen Nachricht mit dem öffentlichen Verschlüsselungsschlüssel des Mixes zu verhindern, fügt der Sender vor jeder Verschlüsselung Zufallsbits zur Nachricht hinzu, die der Mix nicht mit ausgibt.

Zwischen dem Sender und dem ersten Mix werden nur verschlüsselte Nachrichten ausgetauscht. Gleiches gilt für die zwischen den Mixen ausgetauschten Nachrichten. Sofern die Nachricht für den Empfänger verschlüsselt wurde, erfährt auch der letzte Mix nichts über den Inhalt der Nachricht.

Damit die Zuordnung von Sender und Empfänger einer konkreten Nachricht tatsächlich nicht möglich ist, müssen alle Sender zu jedem Zeitpunkt genau eine Nachricht senden und möglichst sogar alle Empfänger genau eine Nachricht empfangen. Andernfalls beschränken sich die möglichen Kommunikationsbeziehungen auf die aktiven Sender und Empfänger. Da ein Beobachter typischerweise alle Sende- und Empfangsereignisse über einen längeren Zeitraum aufzeichnen wird, und viele Kommunikationsbeziehungen auch über einen längeren Zeitraum aufrechterhalten werden, kann durch Schnittmengenbildung die Unbeobachtbarkeit des Einzelnen weiter sinken.

Um die Sender- und Empfängergruppe nicht zu verkleinern, existieren folgende Möglichkeiten: Wer nichts zu senden hat, sendet Leernachrichten (Dummy Traffic), um die Gruppe der Sender zu einem Zeitpunkt nicht unnötig zu verkleinern. Der letzte Mix erkennt Leernachrichten und wirft sie weg. Die einzige theoretische Möglichkeit zum Erreichen einer konstanten Empfängergruppe besteht in der Verteilung aller Nachrichten an alle Empfänger. Dies ist jedoch in den meisten Anwendungsfällen nicht praktikabel. Deshalb begnügt man sich praktisch damit, dass zwar bekannt ist, welche Empfänger Nachrichten empfangen, allerdings mittels Senden von Leernachrichten vollständig verborgen bleibt, welche Sender etwas zu senden haben.

4 Praktische Umsetzung

Im Rahmen des Projektes AN.ON wird ein Mix-basiertes System zum anonymen Websurfen entwickelt und testweise verfügbar gemacht. In der Terminologie des vorangegangenen Abschnitts sind die Sender von Nachrichten die Web-Surfer und die Empfänger die Web-Server. Das bedeutet, die „Nachricht“, die der Web-Surfer anonym an den Web-Server senden möchte, ist die URL (Uniform Resource Locator) der anzuzeigenden Webseite. Es wird die Kommunikationsbeziehung zwischen Web-Surfer und Web-Server verborgen, d.h. der Server, alle Außenstehenden sowie die beteiligten Mixe erfahren somit nicht, welcher Surfer welchen Server kontaktiert und welche Seiten er abruft.

Die Adaption und technische Umsetzung des Verfahrens der umkodierenden Mixe für das Websurfen im Internet wird durch die im AN.ON-Projekt entwickelte Software JAP [5] realisiert. JAP wird auf dem Rechner des Web-Surfers installiert und zwischen den Browser und das Internet geschaltet. Jede aufzurufende URL wird im JAP anonymisiert, indem sie für die zu durchlaufende Mix-Kette vorbereitet wird, d.h. mehrfach verschlüsselt wird.

Während die (mehrfach verschlüsselte) URL durch die Mixe *entschlüsselt* und zum Server geleitet wird, werden die Daten zur Anzeige der Webseite im Browser auf dem Rückweg vom Server zum Browser in jedem Mix zur Vermeidung der Zuordnung auf den Ein- und Ausgängen *verschlüsselt*. Hierzu werden im JAP für jede aufzurufende URL für jeden Mix Sitzungsschlüssel erzeugt und für die Dauer der Verbindung (maximal wenige Sekunden) im Hauptspeicher des Mixes hinterlegt. Das bedeutet, auch die aufzurufenden Inhalte werden durch die Mixe geleitet und somit anonymisiert.

JAP erhält schließlich die (mehrfach verschlüsselten) Inhalte, die dort mit den zuvor erzeugten Sitzungsschlüsseln wieder entschlüsselt und dem Web-Browser zuleitet werden.

5 Erreichte Sicherheit

Die Benutzer von JAP sind geschützt vor der Beobachtung ihres Surf-Verhaltens. Auf der Kommunikationsverbindung zwischen dem PC und dem Internet Service Provider (ISP) ist erkennbar, dass der Benutzer mit dem ersten Mix der Mix-Kette kommuniziert. Da alle Inhalte verschlüsselt sind, erfährt ein Beobachter nichts darüber, welche URLs aufgerufen werden. Somit ist auch der eigene ISP nicht mehr in der Lage, Surfprofile zu erstellen. Er kann jedoch aufzeichnen, wann und wie lange welcher Benutzer mit einem ersten Mix kommuniziert hat und welche Datenmenge er ausgetauscht hat.

Solange wenigstens ein Mix die Zuordnung seiner Ein- und Ausgabenachrichten für sich behält, können auch die Mixe nicht beobachten. Insofern ist es sehr wichtig, dass die beteiligten Mixe unabhängig sind und keinerlei Daten über die gemixten Verbindungen speichern.

Beim Aufruf von URLs, die mit https beginnen (sog. SSL- bzw. TLS-Verschlüsselung, Secure Sockets Layer, Transport Layer Security), erfährt der letzte Mix nur, zu welchem Webserver er sich verbinden soll. Beim Aufruf von „normalen“ URLs (http://...) erfährt der letzte Mix zusätzlich, welche Seiten auf dem Server abgerufen werden.

Der Web-Server erfährt, dass die aufzurufende Webseite über den AN.ON-Dienst abgerufen wurde.

Die Identität des Urhebers des Requests, d.h. des JAP-Benutzers, erfahren weder der letzte Mix, noch der Webserver. Es gibt eine Ausnahme: Beim Abruf von personalisierten Webseiten, die nur unter Angabe eines Benutzernamens abrufbar sind (z.B. E-Mail-Dienste mit Web-Interface), erfährt bei https der Web-Server (bei http auch der letzte Mix) den Benutzernamen. In diesem Fall realisiert das AN.ON-System die Unverkettbarkeit von Identität und Benutzername, d.h. sog. *Pseudonymität*. Beim Aufruf von personalisierten Web-Diensten mittels https, die die Identität des Benutzers kennen (z.B. Internet-Banking), realisiert das AN.ON-System immer noch die Unbeobachtbarkeit der Web-Dienst-Benutzung vor allen Außenstehenden, dem eigenen ISP und den Betreibern der Mixe. Das bedeutet, der Web-Dienst und der Benutzer kennen sich, kommunizieren jedoch vor allen Außenstehenden unbeobachtbar miteinander.

6 Praktische Erfahrungen

Die öffentliche Testphase des AN.ON-Dienstes begann im September 2000. Seitdem steht JAP im Internet für alle gängigen Betriebssysteme (Windows, Macintosh, Linux etc.) zum Download bereit [5]. Mit einer Meldung auf dem Heise-News-Ticker [4] vom Januar 2001 weckte der Dienst erstes öffentliches Interesse. In den folgenden Wochen stieg die Nutzerzahl auf durchschnittlich 200–300 gleichzeitige Nutzer. Im September 2001 benutzten durchschnittlich 500–600 Nutzer gleichzeitig den Anonymisierungsdienst. Die Leistungsfähigkeit des Systems konnte durch eine Speicheraufrüstung erhöht werden, so dass ab Januar 2002 durchschnittlich 800–1000 Nutzer gleichzeitig über das System surfen konnten. Während die Hard- und Software noch deutlich mehr Nutzer bedienen kann, ist die momentane Internet-Anbindung der Mixe mit etwa 1200–1400 Benutzern pro Mix-Kette an der Kapazitätsgrenze angelangt. Momentan werden über den Dienst ca. 4000 Web-Requests pro Minute abgewickelt. Dabei wird täglich ein Datenvolumen von ca. 90–100 GByte verarbeitet.

Der AN.ON-Dienst stellt einen Dienst zum anonymen Abrufen von Informationen (Webseiten) im Internet zur Verfügung und ist nicht gedacht zum anonymen Verbreiten von Informationen. Bei interaktiven Web-Angeboten müssen jedoch auch Daten zum Web-Server übermittelt werden, beispielsweise der Suchbegriff an eine Suchmaschine. Dies hat zur Folge, dass der Benutzer des AN.ON-Dienstes falsche Angaben (z.B. falsche Kreditkartennummer in einem E-Shop) machen kann, ohne rückverfolgbar zu sein. Während des Testbetriebs kam es im Zeitraum Januar 2001 bis August 2002 zu insgesamt 17 Anfragen von Strafverfolgungsbehörden. In der Mehrzahl handelte es sich um Verdachtsfälle von Kreditkartenbetrug, weiterhin Verdacht von Computerbetrug, Datenveränderung, Computersabotage, Beleidigung, Verleumdung und Morddrohung. In zwei Fällen bestand der Verdacht auf Abruf kinderpornographischer Inhalte über den AN.ON-Dienst.

Da vom AN.ON-Dienst keinerlei Verbindungsdaten gespeichert werden, ist es rückwirkend nicht möglich, die IP-Adresse eines JAP-Benutzers zu einem konkreten Web-Request zuzuordnen. Die Speicherung von Verbindungsdaten eines Mixes würde der Idee eines Anonymisierungsdienstes zuwiderlaufen und wäre darüber hinaus nur dann sinnvoll, wenn *alle* beteiligen Mixe einer Mix-Kette solche Daten speicherten. Da eine solche präventive Datenspeicherung für die technische Aufrechterhaltung des Betriebs nicht erforderlich ist, wäre sie zudem ver-

mutlich nicht erlaubt.

Anbieter von Web-Angeboten, die den anonymen Zugriff (über den AN.ON-Dienst) auf ihre Inhalte verhindern wollen, können sich beim AN.ON-Dienst registrieren lassen. Dies verhindert jedoch nicht vollkommen die anonyme Nutzung solcher Angebote, da natürlich noch weitere Anonymisierer im Internet existieren.

Im Verlauf des Testbetriebs wurde der AN.ON-Dienst selbst Opfer von Angriffen. Dabei handelte es sich größtenteils um Denial-of-Service-Attacken, die zur zeitweiligen Unverfügbarkeit des Dienstes führten.

7 Schlussbemerkungen

Die rege Nutzung eines solchen (kostenlosen) Anonymisierungsdienstes führt dazu, dass die Kosten der Dienstnutzung auf Dauer nicht von einem Forschungs- und Entwicklungsprojekt wie es AN.ON ist, getragen werden können. Da das Forschungsprojekt Ende 2003 ausläuft, ist das Weiterbestehen des kostenlosen Dienstangebots vom Finden eines Trägers abhängig. Bereits zum jetzigen Zeitpunkt wäre der Ausbau des Dienstangebots (beispielsweise zusammen mit Internet Service Providern) sinnvoll und notwendig, da der kostenlose Testbetrieb offenbar von vielen (einigen zehntausend) JAP-Benutzern sehr positiv angenommen wurde und der AN.ON-Dienst derzeit an der oberen Lastgrenze betrieben wird.

Alternativ kommt auch die kostenpflichtige Nutzung des Dienstes in Frage. Das Finden von Partnern für die Verwertungsphase des im AN.ON-Projekt entwickelten Systems ist deshalb eine wichtige Aufgabe. Wir sind hier sehr zuversichtlich. Schließlich werden Datenschutz und IT-Sicherheit mehr und mehr zu Marketing-Argumenten von Informationstechnologie-Anbietern.

Literatur

[1] David Chaum: Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms. Communications of the ACM 24/2 (1981) 84–88.

[2] Claudia Golembiewski: Medienrecht – Anonymität im Recht der Multimediadienste. In: Helmut Bäumler, Albert von Mutius (Hg.): Das Recht auf Anonymität. 2003.

[3] The Gnu Privacy Guard Homepage. http://www.gnupg.org/.

[4] Heise-News: TU-Software schützt vor Datenschnüfflern, 10. Jan. 2001. http://www.heise.de/newsticker/data/wst-10.01.01-000/.

[5] The JAP Anonymity & Privacy Homepage. http://www.anon-online.de.

[6] Andreas Pfitzmann: Sicherheit in Rechnernetzen: Mehrseitige Sicherheit in verteilten und durch verteilte Systeme. Vorlesungsskript, TU Dresden, Fakultät Informatik, 1999. http://dud.inf.tu-dresden.de/~pfitza/.

[7] The International PGP Homepage. http://www.pgpi.org/.