Vergleich der gängigen Anonymisierungsdienste im Internet

Kay Petzold
Hochschule für Technik Stuttgart

31. Dezember 2007

Inhaltsverzeichnis

1. Einleitung

Das Internet ist eines der verbreitetsten und wichtigsten Kommunikations- und Informationsmedien.
In den Bereichen Forschung, Wirtschaft und Privatleben werden immer mehr Informationen durch das Internet bereitgestellt und bezogen und es ist sehr wichtig, dass die kommunizierenden Parteien die Möglichkeit haben, anonym zu bleiben.
Diese Arbeit führt solche Szenarien anhand von Beispielen auf und ordnet sie unter dem jeweiligen Aspekt der Anonymität ein. Es gibt verschiedene Dienste, die es den Kommunikationspartnern ermöglichen, ihre Privatsphäre zu schützen.
Die Privatsphäre ist ein durch das Grundgesetz geschütztes Gut. Die Bedeutung der Anonymität ergibt sich direkt daraus, dass durch den Verlust der Anonymität die Privatsphäre verloren geht.
Anonymität ist auch mit wirtschaftlicher und politischer Sicherheit verbunden. Es kann für Unternehmen oder diplomatische Beziehungen von entscheidender Wichtigkeit sein, dass dritte Parteien keine Information darüber erhalten, wer die Kommunikationspartner sind.
Da das Internet eine sehr große Anzahl an Kommunikationsvarianten und deren verschiedene technische Protokolle vereint, muss der Blickpunkt eingegrenzt werden.
Es werden nur die Informationsbereitstellung und der Informationsbezug zwischen Webbrowsern und Webservern betrachtet. Anonymisierungsdienste für Mail- und Dateitransporte verwenden eigene Kommunikationsstrukturen.
Anhand von verschiedenen Anwendungsgebieten und Szenarien wird erörtert, welche Voraussetzungen und Anforderungen an eine anonyme Kommunikation gestellt werden.
Die beiden gängigsten Anonymisierungsdienste für das WWW werden beschrieben, verglichen und auf die Erfüllung ihrer Anforderungen beurteilt. Der Vergleich führt in die Thematik der Anonymität im Internet ein.

2. Exkurs: Grundlagen der anonymen Kommunikation

2.1 Definitionen von Privatsphäre und Anonymität

Für den Begriff der Privatsphäre gibt es keine einheitliche Definition. Folgende Definition eignet sich für dieses Thema:

Die Privatsphäre ist der Bereich, in dem eine Person selbst bestimmt, wem sie wann und welche Information über sich selbst zugänglich macht.

Der Begriff der Anonymität kommt aus dem griechischem anonym = namenlos. Dies bedeutet, dass die Identität einer Person nicht auszumachen ist. Der Grad der Anonymität wird daran gemessen, wie gleichverteilt die Wahrscheinlichkeit ist, Rückschlüsse zu einer einzelnen Identität aus einer Gruppe heraus ziehen zu können.

Die vier Stufen der Anonymität anhand von Beispielen

- Eindeutige Identifikation
Reelle Namen oder Kreditkartennummern
Bei einer Kommunikation oder Transaktion bei der eine eindeutige Identifikation verwendet wird, lässt sich der Kommunizierende immer eindeutig einer natürlichen Person zuordnen.

- Persistente Pseudonyme
E-Mail Adressen oder Nick-Namen in Foren
Wenn wiederholt unter demselben Pseudonym kommuniziert wird, bekommt dieses Pseudonym eine immer stärker ausgeprägte Reputation oder ein feineres Profil. Hierdurch lassen sich wiederum Rückschlüsse auf die natürliche Person hinter dem Pseudonym ziehen.

- Zuweisbare Anonymität
Ein anonym gekauftes Pre-Paid Handy
Hier lässt sich nicht herausfinden wer sich hinter der Sender- oder der Empfängerrolle verbirgt, jedoch lassen sich alle gesendeten und empfangenen Daten sowie die jeweiligen Kommunikationspartner diesem Gerät zuordnen.

- Nicht zuweisbare Anonymität
Barzahlungen auf dem Markt
Der Händler hat weder Information über die Identität des Käufers, noch lässt sich bestimmen welche Einkäufe dieser Kunde den Monat über getätigt hat.

2.2 Anonyme Kommunikation

Nach der Betrachtung der Anonymität im Allgemeinen wird jetzt die Anonymität unter dem Kontext der Kommunikation erläutert. Zu einer Kommunikation gehören immer ein Sender einer Nachricht sowie ein Empfänger dieser Nachricht. Damit diese Kommunikation anonym verlaufen kann, müssen sowohl der Sender als auch der Empfänger einer Gruppe potentieller Kommunikationsbeteiligter angehören.

Anonyme Kommunikation lässt sich in drei Aspekte unterteilen.

- Die Identität des Verfassers einer Nachricht soll verborgen bleiben.

- Die Identität des Empfängers einer Nachricht soll verborgen bleiben.

- Es soll nicht möglich sein, dass Sender und Empfänger zueinander in Beziehung gesetzt werden.

Beziehung zwischen Kommunikationspartnern

- Anonymität gegenüber Dritten
Zwei oder mehr Parteien kennen sich oder wissen voneinander. Das Ziel der Anonymität besteht darin, dass kein Dritter erkennen kann wer die beteiligten Parteien sind und dass sie miteinander kommunizieren. Planen zum Beispiel zwei Firmen eine Fusion, könnten dritte Parteien Rückschlüsse aus einem erhöhten Nachrichtenaustausch zwischen den Fusionspartnern ziehen.

- Einseitige Anonymität in der Kommunikation
Ein Kommunikationspartner möchte gegenüber dem anderen anonym bleiben, wie bei einem anonymen Hinweis zur Verbrechensaufklärung.

Schutzebenen für Nachrichten

Ohne Schutzmaßnahmen werden die Daten unverschlüsselt und mit Sender- und Empfängeradresse übertragen.
Durch Verschlüsselung wird nur der Inhalt der Nachricht vor Auslesen durch Dritte geschützt. Die Adressdaten können jedoch von Dritten gelesen werden.
Werden die Nachrichten zusätzlich mit Hilfe geeigneter Verfahren anonymisiert, sind auch die Metadaten der Nachrichten vor dem Auslesen durch Dritte geschützt. Es können keine Rückschlüsse über den Inhalt der Nachricht oder die Identität der kommunizierenden Parteien gezogen werden.
Werden die anonymisierten Nachrichten zusätzlich durch steganographische Verfahren geschützt, kann die Existenz einer gesendeten Nachricht nicht nachgewiesen werden.

Level	Was ist zu schützen?	Angewendete Methode
3	Existenz einer Nachricht	Steganographie
2	Metadaten der Nachricht	Anonymisierungsdienste
1	Inhalt der Nachricht	Verschlüsselung
0	nichts	keine

Tabelle 1: Schutzebenen für Nachrichten

3. Anonymisierungsdienste im Internet

3.1 Anonyme Kommunikation im Internet

3.1.1 Kommunikation zwischen Webbrowser und Webserver

Das WWW besteht aus Inhalten, die durch Webbrowser erreichbar sind. Diese Inhalte werden von Webservern bereitgestellt. Webbrowser und Webserver kommunizieren miteinander über das http- Protokoll. Es werden nicht nur statische Inhalte übertragen, die Browser übernehmen mittlerweile auch die Aufgabe einer interaktiven grafischen Benutzeroberfläche für komplexe Webanwendungen. Das Protokoll ist nicht mehr auf das Übertragen von Seiteninhalten und Formulardaten beschränkt, sondern dient als Trägerprotokoll für viele Arten von Anwendungen.

3.1.2 Nachrichtentransport und Rückverfolgung im WWW

Das http-Protokoll [1] steuert die Übertragung von Daten zwischen Webserver und WebClient, es verwendet das TCP-IP Protokoll [2] als Transportprotokoll. TCP-IP ist ein verbindungsorientiertes Protokoll. In dieser Verbindungsorientiertheit liegt die Problematik einer Anonymisierung des Nachrichtenversandes im Internet. Damit eine Verbindung aufgebaut werden kann ist es zwingend notwendig, dass die TCP-IP Pakete eine gültige Sender- und Empfängeradresse besitzen. Anhand der Adressen der TCP-IP Pakete erfolgt die Zuordnung des Internetzuganges zum Anschluss des Hauses. Dies hat zu Folge, dass der Grad der Anonymität sich nur noch auf die Gruppe derjenigen bezieht, die diesen Internetzugang mitbenutzen.

3.1.3 Einsehbarkeit der Nachrichten

Das Internet besteht aus Rechnern die netzartig miteinander verbunden sind. Die Struktur dieses Netzes wird über das IP-Protokoll [3] definiert. Ein wesentliches Merkmal des IP-Protokolls ist, dass die Nachrichten von Knoten zu Knoten dieses Netzes, Router genannt, übertragen werden. Die Routenwahl der Datenpakete wird für jedes Paket von den einzelnen Routern bestimmt. Jeder Routerbetreiber kann den Inhalt und den Adresskopf dieser Pakete mitlesen. Aus diesem Grund ist auch der Inhalt der Datenpakete durch geeignete Verschlüsselungsverfahren zu schützen.

3.1.4 Risikobewertung

Das Internet ist nicht durch geografische Entfernungen oder durch eine Teilnehmeranzahl begrenzt. Geschätzte 1,2 Milliarden Menschen haben Zugang zum Internet [4]. Dadurch erhöht sich auch die Wahrscheinlichkeit, dass Kommunikationen die anonym sein sollten und potentielle Angriffe auf Kommunikationskanäle zusammentreffen. Das Risikobewusstsein muss hier angepasst werden.

Ein Anonymisierungsdienst hat die Aufgabe, den Benutzern die Entscheidung darüber zu überlassen, ob der Kommunikationspartner oder eine dritte Person seine IP-Adresse der natürlichen Identität oder den Aufenthaltsort dem Benutzer zuordnen kann.

3.2 Anonymisierungskonzepte für den Nachrichtentransport in Internet

Um Datenflüsse in Netzen anonymisieren zu können, kombiniert man folgende zwei Grundverfahren.

- Ein Beobachter überwacht einen Knoten

Das Konzept der Mixe gewährleistet, dass eingehende Nachrichten an einem Knoten nicht mit den ausgehenden Nachrichten dieses Knotens in Bezug gebracht werden können.

- Ein Beobachter untersucht die Nachricht

Das Konzept des Onion-Routing gewährleistet, dass die Route einer Nachricht, die sie durch das Netz wählt, nicht nachvollziehbar ist.

3.2.1 Mixe

Das Konzept der Mixe wurde 1981 von David Chaun entwickelt [5]. Ein Mix hat die Aufgabe, dass seine eingehenden Nachrichten nicht mit den ausgehenden in Beziehung gebracht werden können. Die dafür benötigten Funktionen sind:

- Sammeln von Nachrichten.
Nur innerhalb einer Gruppe ist Anonymität möglich. Dazu müssen mehrere Nachrichten von verschiedenen Nutzern gesammelt werden. Diese werden dann zusammen in einem Schub an den nächsten Mix weitergeleitet.

- Umcodieren der Nachrichten.
Die ausgehenden Nachrichten bedürfen einer anderen Form als die Eingegangenen, damit diese nicht miteinander in Beziehung gebracht werden können, dies wird durch Verschlüsselung der Nachrichten erreicht. Verschlüsselung kann mit Briefumschlägen verglichen werden. Alle ausgehenden Nachrichten werden in einen andersfarbigen Umschlag gepackt.

- Umsortieren der Nachrichten.
Damit die eingehenden Nachrichten nicht mit den ausgehenden Nachrichten in Beziehung gebracht werden können, müssen die Nachrichten den Mix in einer anderen Reihenfolge verlassen als sie eingegangen sind. Dies wird durch einfaches Umsortieren erreicht.

- Löschen von Duplikaten.
Ein möglicher Angreifer könnte eingehende Nachrichten speichern und die Kopien ein zweites Mal einspielen. Dadurch könnte er Rückschlüsse daraus ziehen wenn er die ausgehenden verschlüsselten Nachrichten nach Wiederholungen untersucht.
Durch diesen Angriff wäre der Mix überbrückt, da man jetzt die eingehende Nachricht mit der dazugehörigen ausgehenden Nachricht in Beziehung setzen kann.

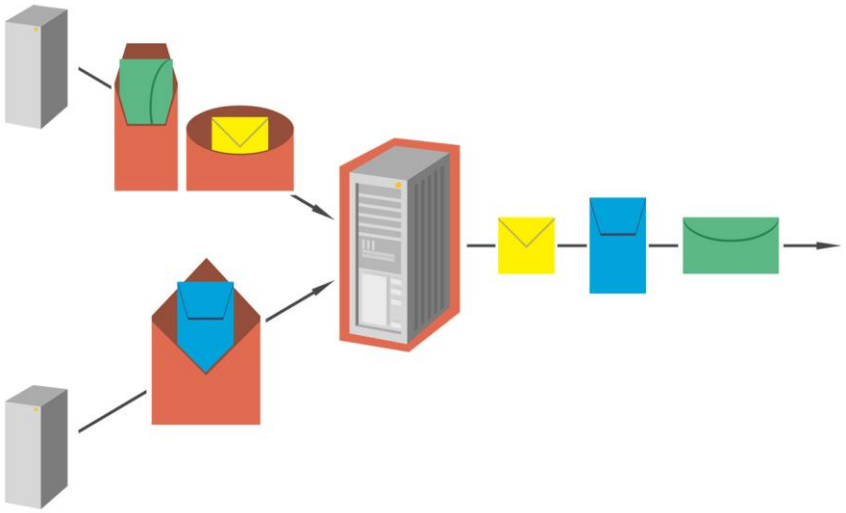

Abbildung 1: Nachrichtenumsortierung durch einen Mixserver

3.2.2 Onion-Routing

Dieses Verfahren hat seinen Namen durch sein Schalenprinzip. Es wurde zusammen von David Goldschlag, Michael Reed und Paul Syverson entwickelt [6]. Das Grundkonzept stammt von David Chaum. Es vervollständigt Chaums Konzept der Mix-Kaskaden, indem es die Routenwahl einer Nachricht im Netz verdeckt. Der Sender wählt vor dem Versenden einer Nachricht die Knotenpunkte und deren Reihenfolge, die die Nachricht durchlaufen wird, aus. Anschließend schreibt der Sender die Adressen der Knotenpunkte schichtweise auf die Nachricht. Als Verschlüsselung wird ein asymmetrisches Verschlüsselungsverfahren [7] verwendet. Die Schichten sind jeweils mit dem öffentlichen Schlüssel des Knotenpunktes verschlüsselt. Wenn eine Nachricht einen Knotenpunkt erreicht, wird die oberste Schicht entschlüsselt und somit abgeschält und an den dadurch ermittelten nächsten Knoten geschickt. Durch dieses Verfahren wird sichergestellt, dass eine Nachricht nur dann entschlüsselt werden kann, wenn diese alle Knotenpunkte in der vorgesehenen Reihenfolge passiert hat. Das entspricht einem Brief, der in vielen ineinandergesteckten Umschlägen gepackt wurde. Es muss zusätzlich davon ausgegangen werden, dass jeder Umschlag nur vom Adressaten geöffnet werden kann. Der Brief wird immer an den nächsten ersichtlichen Adressaten weitergesendet.

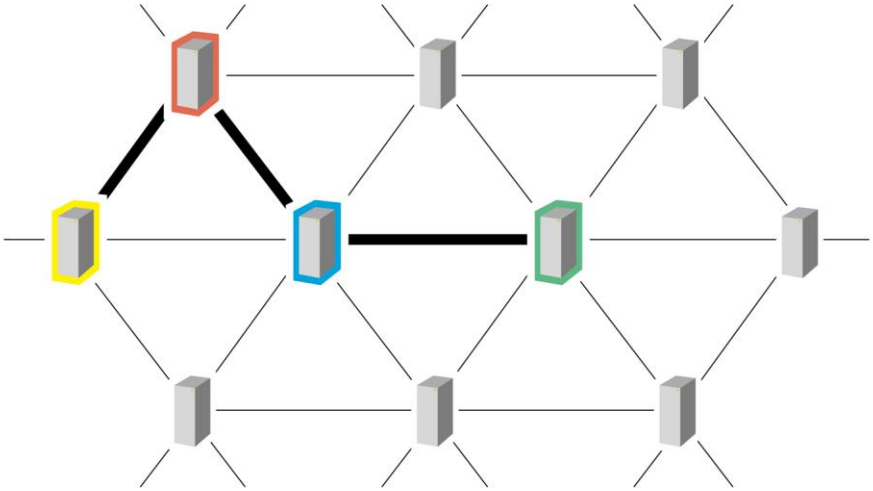

Abbildung 2: Ausgewählte Knoten im Netz

Abbildung 3: Schichtenmodell des Onion Routing

3.3 TOR

3.3.1 Anonymisierungsprinzip

TOR anonymisiert die Ziel und Quell IP-Adressen sowie die Transportroute von TCP-Verbindungen. Es ist ein Netz aus über tausend Mix-Servern, die über das Onion-Routingverfahren verbunden sind [8]. Diese Mixe können als Eingangs-, Durchgangs- und auch als Ausgangs- Server betrieben werden. TOR ist mit einem Maulwurfstunnelsystem zu vergleichen. Es kann nicht vorhergesagt werden, wohin sich ein Maulwurf bewegt wenn er in einem Tunnel verschwindet. Ebenso kann nicht ermittelt werden woher ein Maulwurf ursprünglich herkam wenn er den Tunnel wieder verlässt. Der Routenverlauf innerhalb des Tunnelsystems bleibt verborgen.

3.3.2 Kommunikationsablauf

Der Webbrowser verbindet sich mit dem TOR-Client durch einen Proxy. Dieser zusätzliche Proxy anonymisiert die http-Anfrage, in dem webbrowserspezifische Daten herausgefiltert werden.
Der TOR- Client lädt über eine unverschlüsselte Verbindung von einem Verzeichnisserver eine Adressliste verfügbarer TOR-Server herunter. Im zweiten Schritt wählt der Client

diejenigen TOR-Eingangs- und Durchgangsserver aus, die an dem Tunnel-Verbindungsaufbau beteiligt sein sollen. Im dritten Schritt errichtet der Client einen durch Onion Routing teleskopartig verschlüsselten Tunnel zu dem TOR-Server, der die Rolle des Ausgangserver übernimmt. Dieser Ausgangserver stellt als letzen Schritt die Verbindung zum Zielrechner her.

3.3.3 Strukturentscheidungen

Das TOR-Projekt ist unter die GNU-Lizenz [9] gestellt, um die Software kostenfrei weiterzuverbreiten. Jeder hat die Möglichkeit, den Anonymisierungsdienst zu verwenden oder einen eigenen TOR-Server zu betreiben um das Projekt zu unterstützen.

3.4 Jap

3.4.1 Anonymisierungsprinzip

JAP anonymisiert den http Nachrichtenversand zwischen Webbrowser und Webserver. JAP übernimmt die Funktion eines Proxy-Servers. Die Anfragen des Clients werden vom Proxy-Eingangsserver entgegengenommen. Der Nachrichtentransport vom Eingangs- zum Ausgangsserver verläuft über Durchgangsserver durch Onion Routing. Der Proxy-Ausgangsserver tritt jetzt gegenüber dem Webserver als Client auf und sendet die Nachricht mit der eigenen IP-Adresse als Absenderadresse versehen an den Webserver weiter.

3.4.2 Kommunikationsablauf

Der Benutzer sucht sich in den Clienteinstellungen aus der Liste der JAP-Server die teilnehmenden Mixe aus. Der JAP-Client tritt gegenüber dem Webbrowser direkt als Proxy auf. Der Webbrowser sendet die http- Anfrage an den JAP-Client. Anschließend baut der Client durch Onion-Routing einen teleskopartig verschlüsselten Tunnel zu den Exit-Proxys. Dieser Exit-Proxy sendet als letzen Schritt die http-Anfrage zum Zielrechner. Die Antwort des Webservers gelangt auf demselben Weg zurück zum Anwenderbrowser.

3.4.3 Strukturentscheidungen

Das JAP- Netz besteht derzeitig aus acht Mix-Servern. Die Betreiber dieser Mix-Server sind handverlesene Hochschulen und Vereine[10]. Eine Selbstverpflichtungserklärung zur Einhaltung strenger Datenschutzbestimmungen und Sicherheitsrichtlinien erhöht die Vertrauenswürdigkeit des Dienstes [11].

4. Prüfung und Vergleich der Dienste

4.1 Anforderungen

4.1.1 Funktionale Anforderungen

Aus der allgemeinen Betrachtung der anonymen Kommunikation in Kapitel 2 ergeben sich folgende Anforderungen an die Anonymisierungsdienste.

- Ausreichender Anonymitätsgrad
Der Anonymitätsgrad der Kommunikationsteilnehmer muss der vierten Stufe entsprechen.

- Webserveranonymisierung gegenüber Dritten
Ein externer Beobachter darf nicht herausfinden können, welche Webseiten ein Benutzer besucht.

- Benutzeranonymisierung gegenüber Dritten
Ein externer Beobachter darf nicht herausfinden können, von welchen Benutzern eine Webseite besucht wird.

- Benutzeranonymisierung gegenüber dem Anbieter
Der Betreiber des Webservers darf nicht herausfinden können, wer der Besucher der Webseite ist.

- Webserveranonymisierung gegenüber dem Benutzer
Der Besucher einer Webseite darf nicht herausfinden können, wer der Betreiber des Webservers ist.

4.1.2 Strukturelle Anforderungen

Neben den rein funktionalen Anforderungen gibt es zusätzlich folgende strukturelle Anforderungen an einen Anonymisierungsdienst.

- Der Dienst darf nicht kompromittierbar sein.
Durch staatliche Einflussnahme mit dem Ziel einer Strafverfolgung oder politischer Verfolgung, können die Betreiber gezwungen werden, die Verbindungsprotokolle der Mix-Server herauszugeben.
Einzelne Betreiber der Mix-Server können den Dienst missbrauchen. Der Dienst muss stabil gegenüber diesen Einflüssen sein.

- Der Dienst soll verfügbar sein.
Benutzergruppen darf der Zugang zu diesem Dienst nicht verwehrt werden können. Der Dienst sollte staatlicher Einflussnahme sowie technischen Angriffen standhalten.

4.2 Prüfung der Anforderungen

4.2.1 Prüfung der funktionalen Anforderungen

- Ausreichender Anonymisierungsgrad
- Benutzeranonymisierung gegenüber Dritten
- Benutzeranonymisierung gegenüber dem Anbieter
- Webserveranonymisierung gegenüber Dritten

Beide Anonymisierungsdienste erfüllen die ersten vier Anforderungen durch die kombinierte Verwendung von Mix-Servern und Onion Routing.

- Webserveranonymisierung gegenüber dem Benutzer

TOR unterstützt durch ‚Versteckte Dienste' diese Anforderung. Versteckte Dienste anonymisieren die IP-Adressen von Webservern. Diese Webinhalte sind nur durch das TOR-Netz erreichbar [12].

JAP wurde als reiner Client- Proxy entworfen. Die Erfüllung dieser Anforderung wurde nicht zum Ziel gesetzt.

4.2.2 Prüfung der strukturellen Anforderungen

-Kompromittierbarkeit

Die TOR-Struktur als weltumspannendes Netz vieler autonomer Mixe, erschwert staatliche Einflussnahme auf den Dienst, da die Mixe auf mehrere Rechtsterritorien verteilt sind.
Durch die Autonomie der Mix-Betreiber lässt sich nicht verhindern, dass TOR-Ausgangserver dahingehend modifiziert werden, den Datenstrom mitzulesen oder zu manipulieren. Der TOR-Client bietet die Möglichkeit, eine Auswahl der Ausgangsserver zu treffen. In der Standardkonfiguration des TOR-Clients ist diese Auswahl nicht vorgesehen. Anwender, die nicht beurteilen können, welche Ausgangsserver-Betreiber vertrauenswürdig sind, begeben sich in größere Gefahr, Opfer eines Angriffes zu werden, als wenn sie den Dienst überhaupt nicht verwenden.

Die JAP- Mixe werden überwiegend in Deutschland betrieben. Dies führt zu einer stärkeren Gefährdung durch staatlichen Einfluss[13].
Die strengen Vorgaben an die ausgewählten Mix-Betreiber minimieren die Gefahr eines Missbrauches des JAP-Dienstes.

-Verfügbarkeit

Aufgrund der Möglichkeit für jeden, einen eigenen TOR-Server zu betreiben, ist das TOR-Netz sehr dynamisch und unterliegt einer ständigen Veränderung. Um jemanden vom TOR-Netz abzuschneiden, muss der Zugang zu allen TOR-Eingangsservern blockiert werden. Diese Gefahr ist sehr gering.
Durch den Charakter eines selbstgetragenen Gemeingutes, ist es nicht möglich, das TOR-Netz durch äußere Einflussnahme zu deaktivieren.

Durch die sehr begrenzte Anzahl von JAP-Mixen, ist es für Netzbetreiber sehr leicht, die IP-Adressen der JAP-Mixe zu blockieren. Der Benutzer wird vom JAP-Dienst abgeschnitten.

JAP wird nicht von Privatpersonen selbst getragen, sondern ist ein Gemeinschaftsprojekt der TU-Dresden, der Universität Regensburg und dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein. Durch die Trennung von Dienstbetreibern und Dienstbenutzern ist die Gefahr größer, dass der Dienst aufgrund veränderter Gesetzesgrundlagen eingestellt wird.

4.3 Vergleich

Anforderung	TOR	JAP
Ausreichender Anonymisierungsgrad	Ja	Ja
Benutzeranonymisierung gegenüber Dritten	Ja	Ja
Benutzeranonymisierung gegenüber dem Anbieter	Ja	Ja
Anbieteranonymisierung gegenüber Dritten	Ja	Ja
Anbieteranonymisierung gegenüber dem Benutzer	Ja	Nein

Tabelle 2 : Vergleich der funktionalen Anforderungen

Anforderung	TOR	JAP
Kompromittierungsstabilität	fallabhängig	fallabhängig
Verfügbarkeit	gut	eingeschränkt

Tabelle 3 : Vergleich der strukturellen Anforderungen

5. Fazit

Verlässliche Anonymität im Internet erfordert von den Anwendern ein sehr gutes Verständnis der Kommunikationsprozesse für jeden einzelnen Anwendungsfall. Die Recherche zu diesen beiden Diensten hat gezeigt, dass selbst Fachartikel inhaltlich nicht korrekt waren und falsche Aussagen von anderen Redaktionen übernommen wurden. Die JAP-Gruppe hat in einer Stellungnahme zu einem Artikel des Heise-Magazins [14] über abgehörte TOR-Ausgangsserver darauf hingewiesen, dass im Gegensatz zum JAP-Dienst, die TOR-Benutzer keine Auswahlmöglichkeiten der Ausgangsknoten haben [15]. Nach einer Untersuchung der TOR-Spezifikation hat sich jedoch herausgestellt, dass der TOR-Client diese Auswahl unterstützt. Wenn selbst der Alternativdienst falsch informiert ist, ist es erst recht für den Standardanwender unmöglich sich zu orientieren. Die Kernproblematik in diesem Missbrauch besteht darin, dass die Anwender sich in falscher Sicherheit wiegen und nicht wissen, dass sie zusätzlich die Verbindung verschlüsseln müssen. Die Vielfalt der Anwendungen bei denen das Internet als Kommunikationsmedium verwendet wird, macht es für den Anwender sehr schwer, die jeweiligen Prozesse auf die Anforderungen einer anonymen Kommunikation hin zu untersuchen. Verlässliche Anonymität im Internet ist für Standardanwender nicht möglich.

Literatur

[1] RFC 2616 - Hypertext Transfer Protocol -- HTTP/1.1
http://www.faqs.org/rfcs/rfc2616.html
[2] RFC 793 - Transmission Control Protocol
http://www.faqs.org/rfcs/rfc793.html
[3] RFC 791 - Internet Protocol
http://www.faqs.org/rfcs/rfc791.html
[4] Internet World Stats http://www.internetworldstats.com/stats.htm
[5] Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms
http://world.std.com/~franl/crypto/chaum-acm-1981.html
[6] Onion Routing http://www.onion-router.net
http://portal.acm.org/citation.cfm?id=293443
[7]Asymmetrische Verschlüsselung http://www.bsi-fuer-buerger.de/schuetzen/07_0301.htm#asym
[8]Number of Running Tor routers http://www.noreply.org/tor-running-routers/
[9]The GNU General Public License http://www.gnu.org/licenses/gpl-3.0.html
[10] Status der Anonymisierungs-Server http://anon.inf.tu-dresden.de/status.php
[11] Selbstverpflichtung der Mixbetreiberhttp://anon.inf.tu-dresden.de/operators/help/operatorCommitment20030924_de.html
[12] Versteckte Dienste http://www.torproject.org/overview.html.de
[13]Presserklärungen http://anon.inf.tu-dresden.de/presse/index.html
[14]Neue Angriffe auf Tor - JAP ist davon nicht betroffen http://anon.inf.tu-dresden.de/TorAttacks.html
[15] Anonymisierungsnetz Tor "abgephisht" http://www.heise.de/newsticker/meldung/95770

Alle Quellen zuletzt abgerufen am 30. Dezember 2007