DuD
Datenschutz und Datensicherheit

Anonym im World Wide Web?

JANUS – Schutz von Inhalteanbietern im WWW

Thomas Demuth, Andreas Rieke

Nicht nur für ein anonymes Navigieren, sondern auch für das anonyme Anbieten von Seiten im World Wide Web kann es gute Gründe geben. Die Autoren motivieren dies anschaulich und stellen ein System (JANUS) vor, das, angelehnt an das MIX-Konzept von David Chaum, die Anonymisierung von „Surfern“ und Inhaltsanbietern im WWW erlaubt[1].

[FOTO] Dipl.-Inform. Thomas Demuth

Wiss. Mitarbeiter am Lehrgebiet Kommunikationssysteme der FernUniversität Hagen; Forschung im Bereich Anonymität und Sicherheit in offenen Netzen.
E-Mail: thomas.demuth@fernuni-hagen.de

[FOTO] Dipl.-Ing. Andreas Rieke

Wiss. Mitarbeiter am Lehrgebiet Kommunikationssysteme der FernUniversität Hagen; Forschung im Bereich Verschlüsselung und Fehlerkontrolle in ATM-Netzen sowie im Bereich Anonymität.
E-Mail: andreas.rieke@fernuni-hagen.de

Einleitung

Das World Wide Web (kurz: WWW) hat sich in den letzten Jahren über den akademischen Bereich hinaus im Alltagsleben etabliert. Es dient zur Informationsbeschaffung und -verteilung, aber auch zur allgemeinen Kommunikation.

Viele der Nutzer des WWW sind sich durchaus bewußt, daß sie beim Navigieren durch das Netz Datenspuren hinterlassen. Bei jedem Zugriff auf eine WWW-Seite hinterläßt der Web-Browser bei dem Besitzer dieser Seite bzw. bei dem Betreiber des Web-Servers Informationen. Benutzer, die dies verhindern wollen, können Dienste verwenden, die ihre Identität verbergen (anonymisieren).

Doch wie sieht die Situation aus, wenn nicht der Nutzer, sondern der Anbieter einer Web-Seite anonym bleiben möchte? Für diese zunächst ungewöhnlich anmutende Annahme gibt es nicht nur durchaus plausible Gründe, sondern auch Ansätze zur Realisierung.

1 Motivation

In diesem Beitrag gehen wir von einer Client-Server-Kommunikationsbeziehung (speziell: im WWW) aus. Darunter wird ein Szenario verstanden, in dem ein Anwender bzw. ein Anwenderprozeß (Client) die Dienste eines Anbieters (Server) über ein Kommunikationsprotokoll nutzt.

In dem hier betrachteten Fall ist dies ein Anwender, der mittels eines Web-Browsers (Netscape Communicator, Internet Explorer, o. ä.) auf Web-Seiten zugreift.

Browser und Server kommunizieren miteinander in einer standardisierten Form, dem *Hypertext Transfer Protocol (HTTP)*, welches im Kapitel 2.2 kurz erläutert wird. Zur Identifikation einer Web-Seite dient dabei die sogenannte *URL (Universal Ressource Locator)*, unter der jede Web-Seite weltweit eindeutig referenzierbar ist.

Eine HTTP-Anfrage (GET) an den Web-Server, auf dem sich eine gewünschte Web-Seite befindet, erstellt der Browser dadurch, daß er die URL der Seite samt einiger Verwaltungsinformationen an den Web-Server sendet. Dieser antwortet mit dem Inhalt der Seite und ebenfalls zusätzlichen Verwaltungsinformationen.

1.1 Client-Anonymität

Die erwähnten, mit der Anfrage an den Server übermittelten Verwaltungsinformationen können dabei Daten über den Benutzer des Browsers sowie über die Konfiguration des von ihm verwendeten Rechners wie z. B.

- die im E-Mail-Programm des Browsers eingestellte E-Mail-Adresse,
- die Betriebssystemversion,
- den Typ des Web-Browsers,
- die symbolische Adresse des Rechners,
- den Ort des Internet-Zugangs (Land),
- die Tatsache, ob ein Web-Server bereits einmal kontaktiert worden ist (mittels sog. *Cookies*[2]) und/oder
- die Adresse (URL) der zuvor besuchten Seite

beinhalten. Somit wird dem Betreiber des kontaktierten Web-Servers in der Regel (und meist ohne Wissen des Benutzers) eine Fülle von Informationen übermittelt, die auf unterschiedliche Weise mißbraucht werden kann. Beispielsweise kann der Betreiber des Servers ein Nutzungs- und, sofern der Nutzer z. B. über die E-Mail-Adresse identifiziert werden kann, auch ein Nutzerprofil erstellen, insbesondere dann, wenn sich Betreiber von Web-Servern zusammenschließen und gesammelte Informationen austauschen oder abgleichen.

Eine unmittelbare und noch als harmlos, aber dennoch lästig einzustufende Folge

[1] Dieses Projekt wurde am Fachgebiet Kommunikationssysteme der FernUniversität Hagen unter Aufsicht von Prof. Dr.-Ing. F. Kaderali durchgeführt. Wir bedanken uns bei Prof. Kaderali, Prof. Pfitzmann und seinen Mitarbeitern und unseren Kollegen für interessante Diskussionen und wertvolle Hinweise.

[2] Zu Cookies siehe Bizer und Wichert, DuD 5/1998, S. 273 und 277.

sind gezielte Werbeaktionen per E-Mail. Es ist jedoch auch denkbar, daß Regierungen Web-Seiten mit kontroversen Inhalten publizieren, um durch Auswertung der Zugriffe auf diese Seiten Informationen über daran interessierte Gruppierungen und Personen zu erhalten.

Man erkennt an diesen Beispielen, daß der Wunsch nach Anonymität nicht notwendig auf das Verbergen illegalen Verhaltens zielt. Das gerne gewählte Argument, „wer nichts zu verbergen hat, benötigt keine Anonymität", ist im Kontext des WWW also nicht überzeugend.

Will ein Nutzer eines Dienstes in einer solchen Client-Server-Kommunikationsbeziehung seine Identität nicht preisgeben, spricht man von *Client-Anonymität*.

1.2 Existierende Anonymitätskonzepte

Im folgenden werden verschiedene Ansätze vorgestellt, deren Ziel es ist, Client- und damit Benutzeranonymität bei der Benutzung des Internet im allgemeinen und des Dienstes WWW im besonderen zu gewährleisten.

■ The Anonymizer

„The Anonymizer" (zu erreichen unter http://www.anonymizer.com/) ist einer der ältesten Dienste zur Bereitstellung von Benutzeranonymität und wirkt wie ein Mittelsmann. Diese Funktion wird auch als *Proxy* bezeichnet: Jede Anfrage eines Clients an einen Server läuft über diesen Proxy, der oben erwähnte Verwaltungsinformationen inspiziert. „The Anonymizer" entfernt dabei sensible Daten oder modifiziert diese. So werden beispielsweise die Absenderangaben von E-Mail-Nachrichten unterdrückt.

■ Crowds

Bei diesem Ansatz [RR97] versteckt sich der Benutzer in einer Gruppe von anderen Benutzern bzw. deren Rechnern. Auf jedem Rechner existiert zu diesem Zwecke ein Hilfsprogramm. Eine Anfrage des Web-Browsers wird hierbei von diesem Programm entgegengenommen und mit einer bestimmten Wahrscheinlichkeit, der als Parameter in das Programm einfließt, entweder zu einem anderen Rechner der Gruppe weitergeleitet oder an den ursprünglich adressierten Web-Server gesendet. Letzterer kann somit nicht sicher sein, daß die Anfrage tatsächlich von dem Client stammt, der die Verbindung zu ihm aufgebaut hat. Innerhalb der Gruppe verläuft die Kommunikation verschlüsselt, um Angriffe von außen zu erschweren.

■ LPWA

Der „Lucent Personalized Web Assistant" [BGG+97, BGG+98, GGM+97] bietet dem Benutzer als Einstiegspunkt eine Web-Seite, bei der dieser sich authentifizieren muß. Er ist damit dem System bekannt. Jeder weitere Zugriff auf das WWW läuft über den LPWA ab. Für jede angeforderte Web-Seite wählt der LPWA nun ein Pseudonym, unter dem die Seite abgerufen wird. Das Erstellen eines Benutzerprofiles ist somit nicht sinnvoll möglich. Auch das anonyme Versenden von E-Mail wird von LPWA unterstützt.

■ Onion Routing

Onion Routing [GRS96, SRG97] arbeitet auf einer netzwerknahen Ebene (es setzt z. B. direkt auf TCP/IP-Schnittstellen auf) und bietet einen Grad an Unbeobachtbarkeit für verschiedene Dienste (WWW, FTP, E-Mail, etc.). Ziel des Verfahrens ist, die Kommunikationsbeziehung für einen Außenstehenden zu verschleiern. Auch hier sendet jeder Web-Client seine Anfragen an einen Proxy. Dieser wählt aus einer Menge von anderen Proxies eine Route zum Ziel-Server aus. Alle Proxies besitzen ein eigenes Schlüsselpaar eines Public-Key-Verfahrens. Von dem Start-Proxy wird eine Datenstruktur gebildet, die „schichtenweise" aus den Adreßinformationen der auf der Route liegenden Proxies und zusätzlichen Daten besteht, verschlüsselt mit den öffentlichen Schlüsseln der einzelnen Proxies. Die entstandene Struktur durchläuft dann sämtliche Proxies, die mittels ihrer geheimen Schlüssel die für sie aufgebrachte Schicht „abschälen"; es entsteht eine Route durch das Proxy-Netz, auf der die weitere Kommunikation verschlüsselt abläuft.

1.3 Server-Anonymität

Bei allen vorgestellten Verfahren wird die Anonymität für den Benutzer eines Dienstes gewährleistet. In Übereinstimmung mit der Erweiterung der Definition des Begriffes der „Sicherheit in der Kommunikationstechnik" um den Aspekt der Mehrseitigkeit [MP97] wird nun die Anonymität des Diensteanbieters (die Server-Anonymität) betrachtet.

Die folgenden Beispiele zeigen, daß es gute Gründe für den Wunsch nach Server-Anonymität gibt:

- Ein Wissenschaftler möchte seine Forschungsergebnisse bei einer Konferenz präsentieren und wird gebeten, seinen Artikel zum Zwecke der Begutachtung in anonymer Form einzureichen. Er kann Namen und Adresse aus dem Text entfernen, doch wie kann er in anonymer Form Referenzen auf bereits veröffentlichte, eigene Papiere einfügen?
- Ein Arbeitnehmer befindet sich in ungekündigtem Arbeitsverhältnis und sucht eine neue Anstellung. Er möchte auf einem Web-Server, auf dem ihm privater Platz zur Verfügung steht, mittels seines Erfahrungsprofils für sich werben, ohne über die URL Rückschlüsse auf seine Identität zu geben.
- In einem totalitären Staat möchte eine Bürgerrechtsgruppe über das WWW Schriften publizieren, ohne Repressalien fürchten zu müssen.

Die oben geschilderte Problematik der aufschlußreichen Verwaltungsinformationen trifft auch auf Server-Anonymität zu. Zur Lösung dieses Problems lassen sich zunächst dieselben Mechanismen einsetzen, mittels derer auch die bereits vorgestellten Verfahren zur Sicherstellung von Client-Anonymität arbeiten.

Ein elementares Hindernis ist jedoch, daß die Adresse (URL) der gewünschten Seite einem Benutzer bekannt sein *muß*. Inwieweit diese URL Aufschluß über den entsprechenden Server gibt, zeigt das folgende Kapitel.

2 Grundlagen

Die folgenden Abschnitte beschreiben die wissenschaftlichen und technischen Grundlagen, auf denen das in diesem Beitrag vorgestellte System zur Sicherstellung von Server-Anonymität im WWW aufbaut.

2.1 Mixe

David Chaum beschreibt in seinem Grundlagenaufsatz [Cha81] das Konzept der „*Mixe*" und entwickelt mit diesen unter anderem ein System zum Versenden von Nachrichten (E-Mails), das folgende Eigenschaften besitzt:

Die Kommunikationsbeziehung zwischen einem Sender und einem Empfänger wird vor äußeren Beobachtern verborgen.

Dazu wird eine Nachricht über mehrere Zwischenstationen, die Mixe, transportiert. Jeder Mix ist in der Lage, den Weitertransport zu verzögern, Reihenfolge und Länge der Nachrichten zu verändern und auch Nachrichtenattrappen zu erzeugen. Um den Inhalt der Nachrichten zu schützen, wird er verschlüsselt. Ein Beobachter einer solchen Konstellation kann aus dem Beobachten von ein- und ausgehenden Nachrichten nicht auf eine Kommunikationsbeziehung zwischen einem bestimmten Sender und einem Empfänger schließen, sofern genügend Nutzer zugleich auf einen Mix zugreifen.

> Es kann eine (anonyme) Rückadresse gebildet werden, die von einem Sender an einen Empfänger übermittelt wird. Durch diese Rückadresse kann der Empfänger antworten, ohne die reale Adresse des Senders und damit dessen Identität zu kennen.

Der Transport der Nachricht erfolgt ebenfalls über eine Reihe von Mixen. Diese nutzen zur Verschlüsselung ein asymmetrisches Verfahren. Die tatsächliche Adresse des ursprünglichen Senders wird dabei jeweils mit den öffentlichen Schlüsseln der Mixe chiffriert. Die durch diese Prozedur verschleierte Adresse nutzt der Empfänger als Rückadresse: Auf dem „Rückweg“ kann ein Mix die Adresse des jeweils nächsten Empfängers wieder entschlüsseln.

2.2 HTTP

Das *HyperText Transfer Protocol* [BLFF96] definiert den Mechanismus der Kommunikation sowie die Struktur der Nachrichten, die zwischen einem Web-Server und einem Web-Client ausgetauscht werden.

Die URL, mit deren Hilfe eine Web-Seite weltweit eindeutig identifiziert werden kann, ist gemäß einer feststehenden Syntax konstruiert und enthüllt daher verschiedene Informationen:

- den Namen des Web-Servers und damit die Zugehörigkeit zu einer Organisation oder den Standort sowie das Land, dem der Server zugeordnet werden kann,
- den Verzeichnispfad, über den unter Umständen auf den Besitzer des Dokumentes geschlossen werden kann und
- den Dokumentennamen selbst.

Auch wenn durch den Namen des Web-Servers nicht immer offensichtlich auf die geographische oder institutionelle Zugehörigkeit geschlossen werden kann, so existieren doch Mechanismen und Verzeichnisse, mit deren Hilfe dieses möglich ist.

Jede HTTP-Antwortnachricht eines Servers gliedert sich in zwei Bestandteile:

- Im Nachrichtenkopf finden sich die bereits erwähnten Verwaltungsinformationen sowie weitergehende „Meta-Informationen“.
- Der Nachrichtenkörper enthält die eigentliche Nachricht, z. B. eine Web-Seite. Die meisten dieser Dokumente bestehen aus Text, Grafik und Verweisen und werden mittels der Seitenbeschreibungssprache *HTML (Hypertext Markup Language)* [HTML] beschrieben.

Auch die HTML-Seite selbst kann auswertbare „unsichtbare“ Informationen enthalten (wie z. B. über den zur Erstellung der Seite verwendeten Web-Editor, den Autor der Seite und die letzte Änderung).

3 JANUS

Das System JANUS, das im weiteren vorgestellt wird, bietet neben der Client-Anonymität als Novum die gewünschte Server-Anonymität. Der Name des Systems soll diese Dualität ausdrücken: Wie der gleichnamige römische Gott der Durchgänge und Torbögen erlaubt das System JANUS die Anonymisierung beider Richtungen einer Kommunikationsbeziehung im WWW.

3.1 Einsatzumgebung

Für den allgemeinen Fall gehen wir davon aus, daß viele Web-Clients über ein JANUS-Netz auf Web-Server zugreifen. Die Kommunikation ist dabei nicht auf eine JANUS-Instanz beschränkt, sondern es können zwischen Client und Server viele Instanzen durchlaufen werden. Eine derartige Kaskadierung erhöht die Sicherheit gegenüber Angriffen von außen (Beobachtung von ein- und ausgehenden Nachrichten oder Abhören von Kommunikationsverbindungen).

Die Verzögerung, die aus einer solchen Kaskadierung resultiert, kann vernachlässigt werden, da der JANUS-Prototyp auf der Strecke zum Web-Server noch keine Nachrichteninhalte verschlüsselt. Auch der Zeitaufwand für die Behandlung der URLs ist minimal.

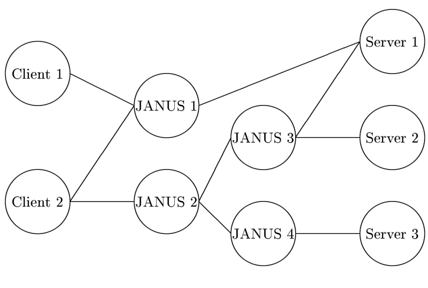

Abb. 1: Zugriff über JANUS

3.2 Der Prototyp

Am Forschungsinstitut für Telekommunikation (FTK) – einem An-Institut der FernUniversität Hagen – wurde ein JANUS-Prototyp entwickelt, der auf einem Rechner der FernUniversität Hagen zu erreichen ist. Die Verschleierung der URLs wird im Prototyp mittels asymmetrischer Verschlüsselung (Public-Key-Verfahren) erreicht. Jede JANUS-Instanz besitzt dabei einen öffentlichen und einen geheimen Schlüssel.

Will ein Anbieter eine Web-Seite publizieren, so verschlüsselt er die URL dieser Seite mit dem öffentlichen Schlüssel einer JANUS-Instanz. Dieser Vorgang läßt sich vereinfacht durch Zugriff auf entsprechende Web-Seiten bewerkstelligen, die auf den JANUS-Web-Servern zur Verfügung stehen. Optional kann der Anbieter auch sukzessive mit den Schlüsseln mehrerer JANUS-Systeme chiffrieren. Die resultierende „URL“ entspricht einer anonymen Rückadresse nach dem Mix-Konzept von Chaum und gibt keinen Aufschluß über die ursprüngliche URL. Sie besteht aus der Adresse des JANUS-Servers, der zur Verschlüsselung verwendet worden ist, einem Präfix und der chiffrierten URL.

Durch diesen Vorgang entsteht beispielsweise aus der WWW-Adresse „http://www.dud.de/“ die folgende anonymisierte Adreßangabe:

> „http://janus.fernuni-hagen.de/janus_encrypted/MTCJP0kAFqxDL90HDhMsvd7RHTitnujYJNi18tOif0mHEx+Jgx41kMOr4D+N$E320GHFJwqbKe39Y6lHlPYufLvS$biQOpH9Oc0F5qOWB6h4p7dLXROS945ryA6g1l4zWVg=“.

Diese URL kann der Anbieter der Web-Seite nun auf beliebige Weise öffentlich bekannt machen. Aufgrund der Länge und des Aufbaues bietet sich eine Verbreitung per E-Mail an. Auch ist der Verweis auf diese URL von einer WWW-Seite möglich, allerdings darf deren Adresse die erzielte Anonymität nicht kompromittieren.

Bei der Gestaltung der so anonym publizierten Web-Seite muß aufmerksam vorgegangen werden. Über den Inhalt darf nicht auf den Autor oder den Web-Server, auf dem die Seite liegt, geschlossen werden können. Explizite Adreßangaben (im Klartext) sind also nicht erlaubt. Auch müssen Referenzen auf der Seite HTML-konform sein, da JANUS das Auftreten von Verweisen erkennen muß, um diese ebenfalls verschlüsseln zu können.

Ein Internet-Nutzer kann diese URL wie eine reguläre Adresse behandeln. Da die Serveradresse der URL aus der WWW-Adresse einer JANUS-Instanz (im obigen Beispiel an der FernUniversität Hagen) besteht, wird dieser kontaktiert und erhält die restliche Zeichenkette als Parameter. Er dechiffriert diese mit seinem geheimen Schlüssel und erhält seinerseits eine URL, die er an eine andere JANUS-Instanz oder, falls sie nun vollständig entschlüsselt worden ist, direkt als Anfrage an einen Web-Server weiterreicht.

Um auch Client-Anonymität zu erzielen, filtert bzw. modifiziert JANUS die Felder im Kopf der Nachricht. So ersetzt er z. B. die ursprüngliche E-Mail-Adresse des Benutzers durch seine eigene, ersetzt die Typenangabe des Web-Browsers oder entfernt die Adresse der Web-Seite, die übermittelt wird, falls die abgerufene URL auf einer anderen Seite referenziert wurde („Referer"-Feld). Die ursprünglich durch den Web-Browser initiierte Anfrage wird derart modifiziert, daß der Web-Server nicht auf den ursprünglich Abrufenden einer Web-Seite schließen kann.

Der von einer JANUS-Instanz kontaktierte Web-Server übermittelt als Antwort den Inhalt der referenzierten Web-Seite. Es ist sehr wahrscheinlich, daß diese Seite Referenzen auf andere Seiten enthält; diese Referenzen stellen somit kompromittierende Informationen dar.

Daher wird die Seite mittels eines Parsers auf Verweise untersucht, die gefundenen Referenzen werden sukzessive auf die bereits geschilderte Art und Weise verschlüsselt (siehe Abb. 2).

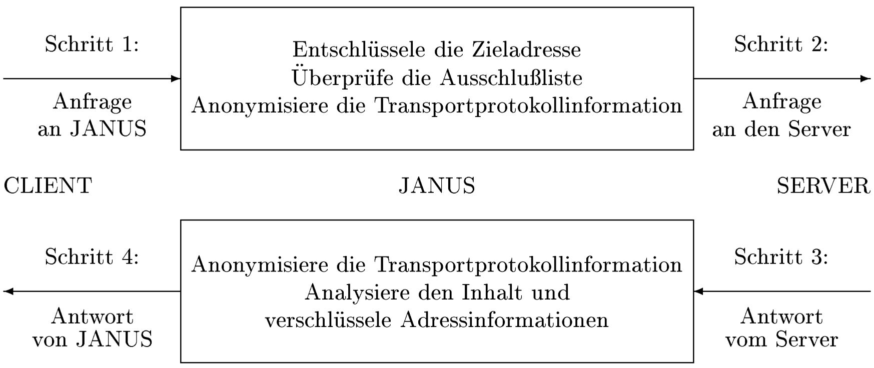

Abb. 2: Arbeitsweise eines JANUS

Da JANUS modular aufgebaut ist, läßt sich für jedes denkbare Format einer Web-Seite bzw. eines Web-Objektes eine Analyseeinheit entwickeln, die Verweise entsprechend anonymisiert.

Auch auf dem Rückweg der Antwort vom Server zum Client werden die Felder mit Verwaltungsinformationen im Nachrichtenkopf entsprechend verändert, um Server-Anonymität zu erreichen.

3.3 Realisierung

JANUS verwendet zur Chiffrierung RSA [RSA78], ein asymmetrisches Verschlüsselungsverfahren. Es besitzt einen öffentlichen und geheimen Schlüssel mit einem Modulus von 768 bit.

Das System ist in der Lage, die Protokolle HTTP, FTP (File Transfer Protocol) und GOPHER zu behandeln. Nicht unterstützt werden vom Prototyp:

- Java[3]: Java-Programme („Applets") werden aus dem Datenstrom herausgefiltert.
- JavaScript: Auch diese Sprache, die in HTML-Text eingebettet werden kann, wird entfernt.
- Cookies: Mit diesen „Datenportionen", die ein Web-Server auf dem Rechner eines Benutzer einer Web-Seite ablegen kann, können die Mechanismen der Anonymisierung unterlaufen werden; sie werden daher von JANUS nicht übermittelt.

3.4 Implementierung

JANUS wurde in seiner jetzigen Form (Version 1.0) in der Programmiersprache Perl und unter Verwendung geeigneter Perl-Bibliotheken für WWW-Client und -Server-Funktionen sowie zur RSA-Verschlüsselung implementiert. Das System wird derzeit auf einer SUN-Workstation (Sparc Ultra) betrieben und ist im WWW unter der URL

http://janus.fernuni-hagen.de/

erreichbar. Ein zweiter Server, der mit SSL[4] arbeitet und somit dem Client verbindungsorientierte Sicherheit (Verbindungsverschlüsselung) bietet, kann unter der Adresse

https://janus.fernuni-hagen.de/

kontaktiert werden. Dort stehen ebenfalls weitere Informationen zur Verfügung.

4 Vorkehrungen gegen Mißbrauch

Ein Anonymisierungs-Dienst, der in dieser Form für jedermann verfügbar ist, reizt leider dazu, ihn zu mißbrauchen. Dieser Mißbrauch kann legale und moralische Grenzen verletzen.

WWW-Seiten, deren Inhalt gegen nationales oder internationales Recht verstößt oder die Grenzen des guten Geschmackes überschreitet, sind daher über JANUS nicht verfügbar.

Zu diesem Zweck führt jede JANUS-Instanz eine Ausschlußliste, in der Adressen von Seiten oder auch kompletten Web-Servern aufgeführt sind, auf die kein anonymer Zugriff unterstützt wird. Versucht ein Benutzer auf eine solche gesperrte Seite zuzugreifen, erhält er von JANUS anstelle der angeforderten Seite einen entsprechenden Hinweis. Die Betreiber des Prototypen nehmen auf eine begründete Meldung Adressen in diese Liste auf.

Sofern ein Mißbrauch festgestellt wird, kann die entsprechende URL jederzeit entschlüsselt werden, um beispielsweise Strafverfolgungsbehörden die Originaladresse auszuhändigen.

5 Sicherheit

Auf ein JANUS-System sind, ähnlich MIX-Netzen, die folgenden Angriffe auf die Anonymität denkbar:

- Aus Praktikabilitätsgründen können bei dem JANUS-Prototypen anonymisierte Adressen mehrfach verwendet werden. Dieses ermöglicht sog. „Replay"-Attacken, bei denen durch wiederholtes Übermitteln einer URL durch den Client und die Bildung von Durchschnitts-, bzw. Differenzmengen zwischen den jeweiligen Nachrichten, die bei dem JA-

[3] Zu Java-Applets siehe Mack, DuD 9/1998, S. 509 ff.

[4] Secure Sockets Layer. Siehe Esslinger/Müller, DuD 12/1997, S. 691 ff.

NUS ein- und ausgehen, Verknüpfungen gefunden werden können und der JANUS überbrückt werden kann.
- Bei unverschlüsselter Übertragung der WWW-Seiten ist es für einen externen Angreifer prinzipiell möglich, durch Vergleich der Nachrichten, die in eine JANUS-Instanz hinein und wieder aus ihr herausgehen, zwischen diesen einen Bezug herzustellen. Somit kann die anonyme Web-Adresse aufgedeckt werden.
- Die Länge von ein- und ausgehenden Nachrichten kann diese oft mit Eindeutigkeit unterscheidbar machen.
- Auch anhand der Reihenfolge von ein- und ausgehenden Nachrichten kann eine Zuordnung möglich sein.
- Eine weitere Verkehrsanalyse ist möglich, wenn zu wenige oder, als Grenzfall, eine einzelne Nachricht (Anfrage) weitergeleitet wird; hier ist der Zusammenhang von ein- und ausgehenden Nachrichten offensichtlich.

6 Ausblick

Das als Prototyp implementierte JANUS-System ist seit November 1997 im Internet zu erreichen. Pro Tag verarbeitet der Prototyp durchschnittlich 2.500 Zugriffe; dabei wurde Kritik nur in der Anfangsphase wegen technischer Probleme laut.

In zukünftigen Versionen wird das JANUS-System über zusätzliche Funktionen verfügen, die Angriffe erschweren sollen:
- Die Seiteninhalte werden verschlüsselt übertragen.
- Die Länge der Nachrichten wird variiert.
- Der Nachrichtenausgabe wird eine willkürliche, z. B. eine lexikographische Reihenfolge aufgezwungen.
- Von JANUS werden Schein-Nachrichten und Schein-Anfragen erzeugt und weitergeleitet.
- Java-Applets und JavaScript-Programme können wiederum Referenzen enthalten; diese müssen ebenfalls verschlüsselt werden. Zur Erkennung solcher Referenzen ist die Erweiterung der Parsing-Fähigkeiten notwendig.

Durch diese Verbesserungen des Systems wird JANUS in seiner Funktionalität und Sicherheit stärker an das wissenschaftlich anerkannte Mix-Konzept von David Chaum angenähert.

Fazit

Anonymität ist im World Wide Web nicht nur in vielen Fällen notwendig, sondern auch realisierbar.

Wir haben gezeigt, daß dieser Begriff nicht nur einseitig (Client gegenüber Server) gesehen werden darf. Anonymität in offenen Netzen, hier im WWW, muß nicht auf die Anonymität des Benutzers eines solchen Netzes beschränkt sein.

Der entwickelte Prototyp eines JANUS-Systems, der im Internet frei verfügbar ist, belegt, daß Client- und Server-Anonymität im World Wide Web technisch gewährleistet werden kann.

Literatur

[BGG+97] D. Bleichenbacher, E. Gabber, P. Gibbons, On Personalized yet Anonymous Interaction, Bell Labs Technical Memorandum, Mai 1997

[BGG+98] D. Bleichenbacher, E. Gabber, P. Gibbons, Y. Matias, A. Mayer. On Secure and Pseudonymous Client Relationships with Multiple Servers, Technical report, Bell Labs, Lucent Technologies, Murray Hill, NJ, Mai 1998.

[BLFF96] T. Berners-Lee, R. Fielding, H. Frystyk, Hypertext Transfer Protocol – HTTP/1.0. RFC 1945, Mai 1996

[Cha81] David Chaum, Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms, Comm. of the ACM, Februar 1981

[GGM+97] E. Gabber, P. Gibbons, Y. Matias, How to make Personalized Web Browsing Simple, Secure, and Anonymous, Bell Labs Technical Memorandum, Mai 1997

[GRS96] D. Goldschlag, M. Reed, P. Syverson, Hiding Routing Information, Information Hiding, LNCS 1174, 1996

[HTML] „Introducing HTML 3.2“, W3C-Recommendation, http://www.w3.org/MarkUp/Wilbur/

[MP97] G. Müller, A. Pfitzmann, Mehrseitige Sicherheit in der Kommunikationstechnik, Addison-Wesley, 1997

[RR97] M. Reiter, A. Rubin, Crowds: Anonymity for Web Transactions, DIMACS Technical Report 97-15, AT&T, August 1997

[RSA78] R. Rivest, A. Shamir, L. Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communication of the ACM, Februar 1978

[SRG97] P. Syverson, M. Reed, D. Goldschlag, Private Web Browsing. Journal of Computer Security Special Issue on Web Security, 5(3):237-248, 1997.