HAGENER
UNIVERSITÄTSREDEN XX.X

Tage der Forschung 1999

Dipl.-Inform. Thomas Demuth

JANUS – Schutz der Privatsphäre im World Wide Web

Vortrag gehalten auf den
Tagen der Forschung 1999
am 4. Mai 1999

Impressum

Hagen, September 1999

Herausgeber:	Der Rektor
Redaktionsleitung:	Prof. Dr. Dr. Thomas Vormbaum
Redaktion und Satz:	Ass. Oliver Schwindt
Druck:	Zentrale Reproduktion der FernUniversität - GHS

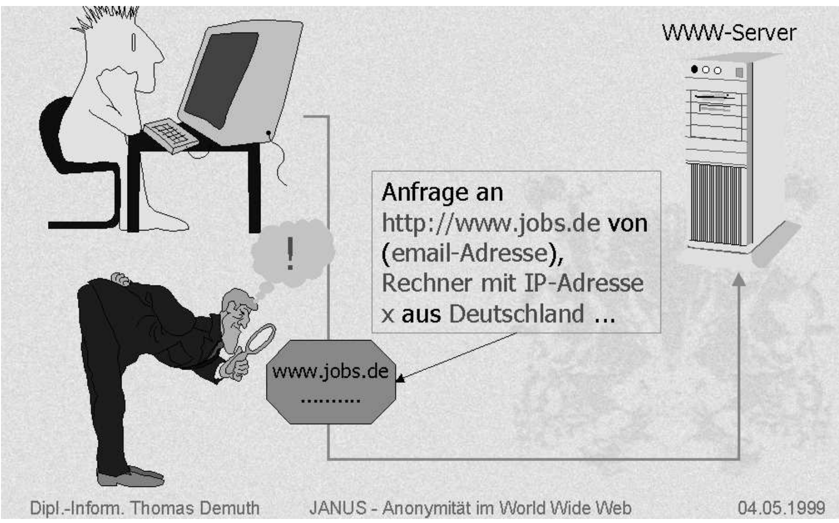
Gliederung

XXX Seite bleibt komplett leer XXX

Motivation

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 dieses verhindern wollen, können Dienste verwenden, die ihre Identität verbergen (anonymisieren).



Ungeschützte Navigation im WWW

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.

In dem hier analysierten Fall betrachten wir einen 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)*. Zur Identifikation einer Web-Seite dient dabei die sogenannte *URL (Uniform Ressource Locator)*, unter der jede Web-Seite weltweit eindeutig referenzierbar ist.

Eine HTTP-Anfrage 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.

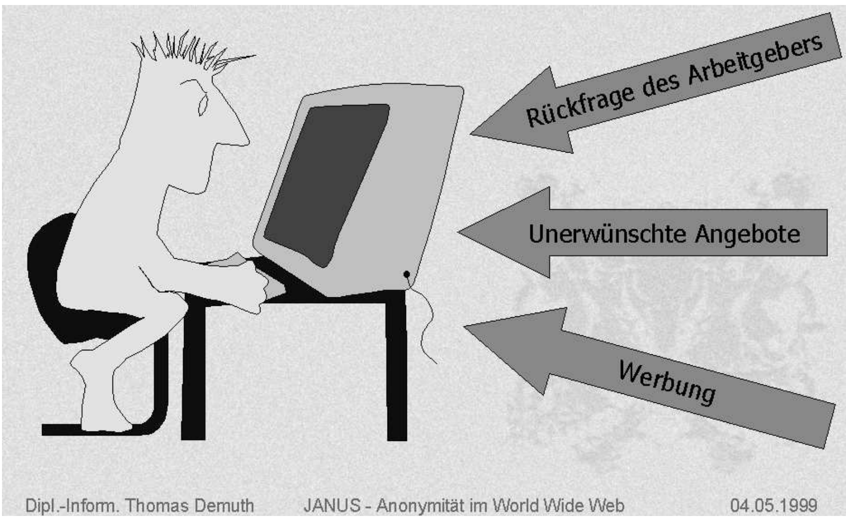
Client-Anonymität

Die erwähnten, mit der Anfrage an den Server übermittelten, Verwaltungsinformationen können dabei Daten über den Benutzer des Browsers (sog. *Client*) 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*) 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.

Resultate des ungeschützten Navigierens im WWW können neben der Erstellung von Benutzerprofilen peinliche Rückfragen oder auch unerwünschte Werbung sein.



Auswirkungen von Datenspionage

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

Server-Anonymität

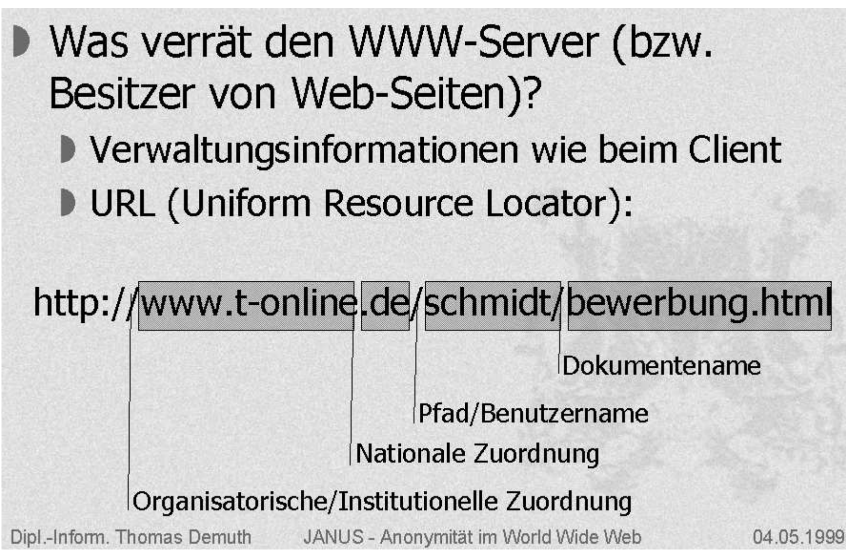
Bei bereits existierenden Verfahren wird die Anonymität für den Benutzer eines Dienstes gewährleistet.

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?
- 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 die folgende Abbildung.



Struktur einer URL (Uniform Ressource Locator)

JANUS

Das Projekt JANUS, das im Fachbereich Kommunikationssysteme initiiert wurde, bietet neben der Client-Anonymität als Novum die gewünschte Server-Anonymität.

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 beliebig 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.

Der Prototyp

Der JANUS-Prototyp ist auf einem Rechner der FernUniversität Hagen zu erreichen. 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. Die resultierende „URL“ entspricht einer anonymen Rückadresse und gibt keinen Aufschluß über die ursprüngliche URL. Sie besteht aus der

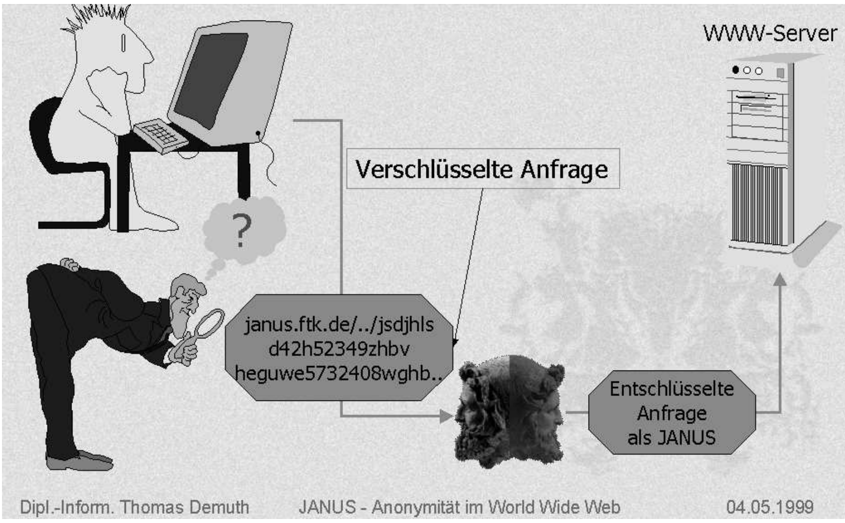
Adresse des JANUS-Servers, der zur Verschlüsselung verwendet worden ist, einem Präfix und der chiffrierten URL.

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

„http://janus.fernuni-hagen.de/janus_encrypted/
MTAv1bxExPNZEQQGzD245BRFpfxqp85jiIFL0EvUYezIvyPiLVL
dAhH7FXBf0tUUcyRzuS4hLOkqOQgJ2DbrxJDapOsdjNvkHKnjj
1kr0j9HUSN1Ref4jYlJPd0o+t7ZmpKo=“.

Diese URL kann der Anbieter der Web-Seite nun auf beliebige Weise öffentlich bekannt machen.

Ein Internet-Nutzer kann diese URL wie eine reguläre Adresse behandeln. Da die Serveradresse der URL aus der WWW-Adresse einer JANUS-Instanz 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.

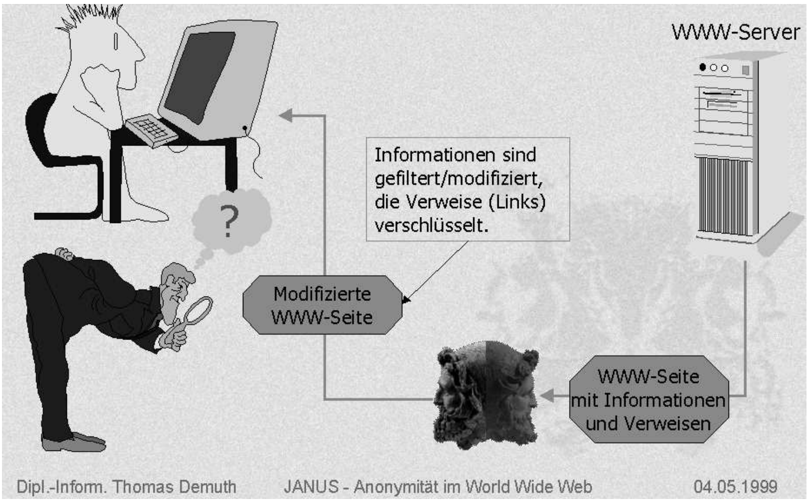


Transport einer Anfrage

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.



Rücktransport der angeforderten WWW-Seite

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.

Schritt 1: → Anfrage an JANUS	Entschlüssele die Zieladresse Überprüfe die Ausschlußliste Anonymisiere die Transportprotokollinformation	Schritt 2: → Anfrage an den Server
CLIENT	JANUS	SERVER
Schritt 4: ← Antwort von JANUS	Anonymisiere die Transportprotokollinformation Analysiere den Inhalt und verschlüssele Adressinformationen	Schritt 3: ← Antwort vom Server

Arbeitsweise von JANUS

Realisierung

JANUS verwendet zur Chiffrierung RSA, 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, HTTPS, FTP (File Transfer Protocol) und GOPHER zu behandeln.

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 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.

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.

Ausblick

Das als Prototyp implementierte JANUS-System ist seit November 1997 im Internet zu erreichen. Pro Tag verarbeitet der Prototyp durchschnittlich 300.000 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.

Dieser Begriff darf nicht nur einseitig (Client gegenüber Server) gesehen werden. 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.