Der Rewebber – Anonymität im World Wide Web

Dipl.-Inform. Thomas Demuth, Universität Hagen
Dr.-Ing. Andreas Rieke, ISL Internet Sicherheitslösungen GmbH

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 Webbrowser bei dem Besitzer dieser Seite bzw. bei dem Betreiber des Webservers Informationen. Benutzer, die dieses verhindern wollen, können Dienste verwenden, die ihre Identität verbergen (anonymisieren).
Doch wie sieht die Situation aus, wenn nicht der Nutzer, sondern der Anbieter einer Webseite 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 Webbrowsers (Netscape Communicator, Internet Explorer, o. ä.) auf Webseiten zugreift.
Browser und Server kommunizieren miteinander in einer standardisierten Form, dem *Hypertext Transfer Protocol (HTTP)*. Zur Identifikation einer Webseite dient dabei die sogenannte *URL (Uniform Ressource Locator)*, unter der jede Webseite weltweit eindeutig referenzierbar ist.
Eine HTTP-Anfrage (GET) an den Webserver, auf dem sich eine gewünschte Webseite befindet, erstellt der Browser dadurch, daß er die URL der Seite samt einiger Verwaltungsinformationen an den Webserver 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 sowie über die Konfiguration des von ihm verwendeten Rechners wie z. B.

- die im Browser eingestellte Email-Adresse,
- die Betriebssystemversion,
- den Typ des Webbrowsers,
- die symbolische Adresse des Rechners,
- den Ort des Internet-Zugangs (Land),
- die Tatsache, ob ein Webserver bereits einmal kontaktiert worden ist (mittels sog. *Cookies*) und/oder
- die Adresse (URL) der zuvor besuchten Seite

beinhalten. Somit wird dem Betreiber des kontaktierten Webservers 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 Email-Adresse identifiziert werden kann, auch ein Nutzerprofil erstellen, insbesondere dann, wenn sich Betreiber von Webservern zusammenschließen und gesammelte Informationen austauschen oder abgleichen.
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*, diese allerdings durch ihre Struktur Aufschluß über Besitzer, Ort, etc. des zugehörigen Dokumentes geben kann.
Das System Rewebber bietet neben der Client-Anonymität als Novum die gewünschte Server-Anonymität.

Einsatzumgebung
Für den allgemeinen Fall gehen wir davon aus, daß viele Webclients über ein Rewebber-Netz auf Webserver zugreifen. Die Kommunikation ist dabei nicht auf eine Rewebber-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 Rewebber auf der Strecke zum Webserver noch keine Nachrichteninhalte verschlüsselt. Auch der Zeitaufwand für die Behandlung der URLs ist minimal.

Die Verschleierung der URLs wird mittels asymmetrischer Verschlüsselung (Public-Key-Verfahren) erreicht. Jede Rewebber-Instanz besitzt dabei einen öffentlichen und einen geheimen Schlüssel.
Will ein Anbieter eine Webseite publizieren, so verschlüsselt er die URL dieser Seite mit dem öffentlichen Schlüssel einer Rewebber-Instanz. Dieser Vorgang läßt sich vereinfacht durch Zugriff auf entsprechende Webseiten bewerkstelligen, die auf den Rewebber-Webservern zur Verfügung stehen. 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 Rewebber-Servers, der zur Verschlüsselung verwendet worden ist, einem Präfix und der chiffrierten URL.

Durch diesen Vorgang entsteht beispielsweise aus der WWW-Adresse „http://www.isl-online.de/“ die folgende anonymisierte Adreßangabe:
„http://www.rewebber.de/surf_encrypted/
MTCTFC3oiNMnYRkhgibK1h7A5vctIKCWPEukC8TYkKJ2YWweLThuxaRZGuKHB
mu0RW0OFaYVrekrFw1c3Jcie9QMgA44Coo$q9PmM77IyFxc3d6k0jekV5zt7WMrh
NnOTqQ=“.
Diese URL kann der Anbieter der Webseite 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 Rewebber-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 Rewebber-Instanz oder, falls sie nun vollständig entschlüsselt worden ist, direkt als Anfrage an einen Webserver weiterreicht.
Um auch Client-Anonymität zu erzielen, filtert bzw. modifiziert der Rewebber die Felder im Kopf der Nachricht. So ersetzt er z. B. die ursprüngliche Email-Adresse des Benutzers durch seine eigene, ersetzt die Typenangabe des Webbrowsers oder entfernt die Adresse der Webseite, die übermittelt wird, falls die abgerufene URL auf einer anderen Seite referenziert wurde („Referer“-Feld). Die ursprünglich durch den Webbrowser initiierte Anfrage wird derart modifiziert, daß der Webserver nicht auf den ursprünglich Abrufenden einer Webseite schließen kann.
Der von einer Rewebber-Instanz kontaktierte Webserver übermittelt als Antwort den Inhalt der referenzierten Webseite. 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.
Da der Rewebber modular aufgebaut ist, läßt sich für jedes denkbare Format einer Webseite bzw. eines Webobjektes 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.

Realisierung
Der Rewebber 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
Das System ist im WWW unter der URL

http://www.rewebber.de/

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

https://www.rewebber.de/

kontaktiert werden. Dort stehen ebenfalls weitere Informationen zur Verfügung.

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.
Das Rewebber-System, das im Internet frei verfügbar ist, belegt, daß Client- und Server-Anonymität im World Wide Web technisch gewährleistet werden kann.