

Ich anonym im Internet?

Demonstration der Ausspähung von Daten

Hanno 'Rince' Wagner
rince@cccs.de

16. Februar 2008

Inhaltsverzeichnis

1	Über mich / Über den CCCS	2
2	Datenspuren im Netz	2
2.1	Klassisch: Logfiles	2
2.2	Weitergehend: Cookies	3
2.3	Heimlich: Webbugs	3
2.4	Weitergehend: Javascript	3
3	Was kann ich tun	4
3.1	Einleitung	4
3.2	Einen sicheren Client nutzen	4
3.3	Einen sicheren Mailclient nutzen	5
3.4	Im Netz: Anonymisierungsdienste nutzen	5
3.5	TOR: Das Prinzip	6

Randnotizen mit dem Symbol □→ dienen der Orientierung während der Präsentation; sie verweisen jeweils auf die Folie mit dem aufgeführten Titel.

Zusammenfassung

Je intensiver das Internet auch von den normalen Bürgern benutzt wird, umso mehr wird über den Benutzer auch gespeichert - einige Sachen offen und mit Wissen des Zusehers, einige Sachen aber verdeckt. Dieser Vortrag soll die Möglichkeiten der Überwachung aufzeigen und die Gelegenheit geben Webseiten zu überprüfen.

1 Über mich / Über den CCCS

Ich selbst arbeite in Stuttgart und bin dort einerseits Systemadministrator und seit letztem Jahr der betriebliche Datenschutzbeauftragter der Firma. Das Thema Datenschutz hat mich auch schon privat früher interessiert, daher bin ich Gründungsmitglied bei Fitug und CCCS, beim CCC seit Anfang der 90er-Jahre und bei EDRi seit vorletztem Jahr dabei.

☐→
Über mich / Über
den CCCS

Der CCCS wurde von aktiven Stuttgartern 2001 gegründet, als 14tägigen Stammtisch an unterschiedlichen Plätzen. Nachdem die Interessierten mehr oder minder zu einer festen Gruppe wurden fingen wir mit Vorträgen für die Allgemeinheit an - die Vorträge sind meistens technischer Natur, aber an die normale Bevölkerung gerichtet. Das heisst sie versuchen möglichst wenig in die Technik hineinzugehen.

2 Datenspuren im Netz

2.1 Klassisch: Logfiles

Bevor wir dazu kommen wie man sich halbwegs unerkannt im Netz bewegen kann, will ich erst einmal darstellen was bisher von den interessierten Parteien überhaupt an Daten gesammelt wird - legal oder mit fragwürdigen Hilfen. Den Anfang machen die sogenannten Logfiles - Dateien, die der Diensteanbieter hat und in denen mitgeschrieben wird, zu welcher Uhrzeit welche IP welchen Teil des Dienstes angefragt hat. Als Beispiel habe ich eine Zeile eines Webserver-Logfiles und ein Jabber-Server dazugebracht:

☐→
Logfiles

Example 1. 78.94.xx.yy -- [10/Feb/2008:01:15:55 +0100] „GET /archives/anstaendig.gif HTTP/1.1“ 200 37295 „http://blog.rince.de/archives/530-Hoerbuecher-mal-in-grauenhaft...-audible.de.html“ „Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.12) Gecko/20080201 Firefox/2.0.0.12“

Dieses Beispiel zeigt, dass die IP 78.94.xx.yy (IP anonymisiert) um 01:15 Uhr nachts am 10. Februar 2008 bei dem Webserver nach einem Bild gefragt hat. Dabei hat der Webbrowser freiwillig von sich preisgegeben dass er von einer Webseite von blog.rince.de hingeführt wurde, und dass als Browser ein Firefox Webbrowser genommen wurde.

Example 2. 20080209T23:46:10 rince@jabber.rince.de login ok 194.95.226.145 laptop
20080209T23:46:13 sessionstart ;rince@jabber.rince.de;
20080209T23:46:51 sessionend ;rince@jabber.rince.de;339

Bei diesem Beispiel sieht man das der Benutzer rince@jabber.rince.de sich von der IP 194.95.226.145 am 09. Februar 2008 um 23:46 Uhr sich eingeloggt hat - und sein Rechner scheint „laptop“ zu heissen. Er hat sich kurz danach wieder ausgeloggt.

2.2 Weitergehend: Cookies

Cookies sind primär dazu gedacht, Besucher einer Webseite wiederzuerkennen. Dafür bekommt jeder Besucher eine eindeutige ID zugesendet die der Webbrowser speichert. Zusätzlich wird dieser Information eine Lebenszeit zugeordnet - solange ist diese Information gültig. Man kann aber in Cookies auch sehr viel mehr speichern als „nur“ eine Identifikationsnummer - man kann einen Login-Status speichern, eine Art Spur die der Besucher hinterlegt hat. Und wenn die Lebenszeit sehr lange gewählt wird kann ein Cookie auch mehrere Jahre gültig sein.

☐→
Cookies

2.3 Heimlich: Webbugs

Bei Webbugs wird eine kleine Grafik mit in die Seite eingebettet. Diese Grafik ist quasi unsichtbar - aber der Aufruf selbst ist das wichtige. Die Grafik liegt üblicherweise nicht auf dem Webserver den man gerade besucht sondern auf den Servern eines „Datensammlers“, der das Besuchverhalten ausforschen will. eTracker ist eine Firma die diese Methode zur Analyse nutzt. Allerdings anonymisiert sie ihre Ergebnisse für die Auftraggeber - diese können mit den Ergebnissen zwar einen Trend herauslesen, aber keinen einzelnen Besucher ermitteln.

☐→
Webbugs

Im Unterschied zu „normalen“ Logfiles gehen diese Daten an einen Dritten - jemanden, der im Auftrag des Webserverbetreibers diese Daten sammelt und analysiert.

2.4 Weitergehend: Javascript

das Prinzip Javascript

- Javascript wird vom Browser sofort nachgeladen, sobald die Webseite es benötigt, ohne Interaktion des Nutzers.
- Javascript kann dabei die lokalen Dateien auslesen und an den Webserverbetreiber weiterleiten
- Oder auch das Aussehen der Webseite verändern

Potentielle Missbrauchsmöglichkeiten sind:

- Umlenken von URLs, wo die nächsten Daten von geladen werden
- Öffnen von Popups
- Datenauslesen via Cross-Site Scripting
- <http://www.zendas.de/service/browserdaten.html> (Zendas Browsercheck)

Durch Javascript wird der Webbrowser, der bisher nur passiv arbeitet (er lädt nur die Webseiten die der Benutzer laden will) selbst aktiv und macht Verbindungen zu anderen Seiten auf um dort Informationen nachzuladen. Dadurch lassen sich auch sichtbare Informationen verändern oder Informationen austauschen. Bei ebay wurde solch eine Methode vom Heinz Heise Verlag benutzt um einen eBay-Verkäufer sehr vertrauenswürdig aussehen zu lassen.

☐→
Javascript

3 Was kann ich tun

3.1 Einleitung

Wie kann ich mich schützen?

kabelschneider.png ¹

Man könnte einfach beschliessen, ohne Internet auskommen zu wollen. Dies ist in der heutigen Zeit aber eher kontraproduktiv. Ausserdem gibt es ein Recht auf Anonymität im Internet. Die Frage ist nur, wie man dieses Recht am besten ausüben kann.

☐→
Was kann ich tun?

3.2 Einen sicheren Client nutzen

Viele Leute nutzen den vom Betriebssystemhersteller empfohlenen Webbrowser. Meistens ist dies der Internet Explorer. Auch wenn Microsoft Sicherheitslücken inzwischen relativ schnell schliesst ist dies beim Internet Explorer meistens nicht ausreichend; die implementierten Sicherheitsfunktionen lassen sich entweder austricksen oder leicht aushebeln. Alternative Web-Browser haben mehrere Vorteile - einerseits sind sie meistens flexibler, andererseits bedeutet auch diese Nicht-Monopolstellung, dass sie für Schädlinge nicht attraktiv sind.

☐→
Einen sicheren Webbrowser nutzen

- Microsoft Internet Explorer ist der Standard-Browser auf Windows-Betriebssystemen. Leider hat er auch viele Sicherheitsprobleme, welche gerne auch von Crackern ausgenutzt wird.
- Firefox ist ein alternativer Webbrowser mit einer breiten Nutzerbasis. Dieser ist aus dem Mozilla, früher Netscape (AOL) entstanden.
- Opera stammt aus der Feder einer norwegischen Firma und hat eine eigene Anzeige-Maschine geschrieben die teilweise deutlich schneller als andere Browser ist.
- Camino und Safari sind zwei Browser die auf MacOS X hauptsächlich benutzt werden.
- lynx/w3m/curl sind textbasierte Browser, die keine Grafiken anzeigen.

¹Foto von Germanium, <http://flickr.com/photos/germanium/1580297705/>)

3.3 Einen sicheren Mailclient nutzen

Für Mailclients gelten fast dieselben Regeln wie für Web-Browser, insbesondere weil die komplexeren Systeme auch intern Web-Browser nutzen um HTML-Mails darzustellen.

□→
*Einen sicheren
Mailclient nutzen*

- Thunderbird stammt aus derselben Quelle wie Firefox - es entstammt der Mozilla-Suite von AOL/Netscape.
- The Bat! ist ein relativ alter, aber immer noch guter Mailclient für Windows
- Pegasus Mail ist ein Mailclient der ursprünglich aus der Novell-Ecke kommt, aber inzwischen an heutige Verhältnisse angepasst wurde.
- mutt/pine/elm sind textbasierte Mailclients. Da sie kein HTML anzeigen können sind sie deutlich sicherer als graphische Mailclients.

3.4 Im Netz: Anonymisierungsdienste nutzen

Anonymisierungsdienste sind dazu da, dem Webserver-Betreiber (oder, je nach Anonymisierungstyp) auch den Zwischenstellen die Herkunft einer Anfrage zu verschleiern. Dies kann entweder durch einen einfachen Mittler geschehen (wie ein Notar im wirklichen Leben) oder durch verschlüsseln von Daten und auch Traffic, so dass auch durch eine Trafficanalyse nicht erkennbar ist wer für wen welche Daten verschickt und bekommen hat.

□→
Anonymisierungsdienst

3.5 TOR: Das Prinzip



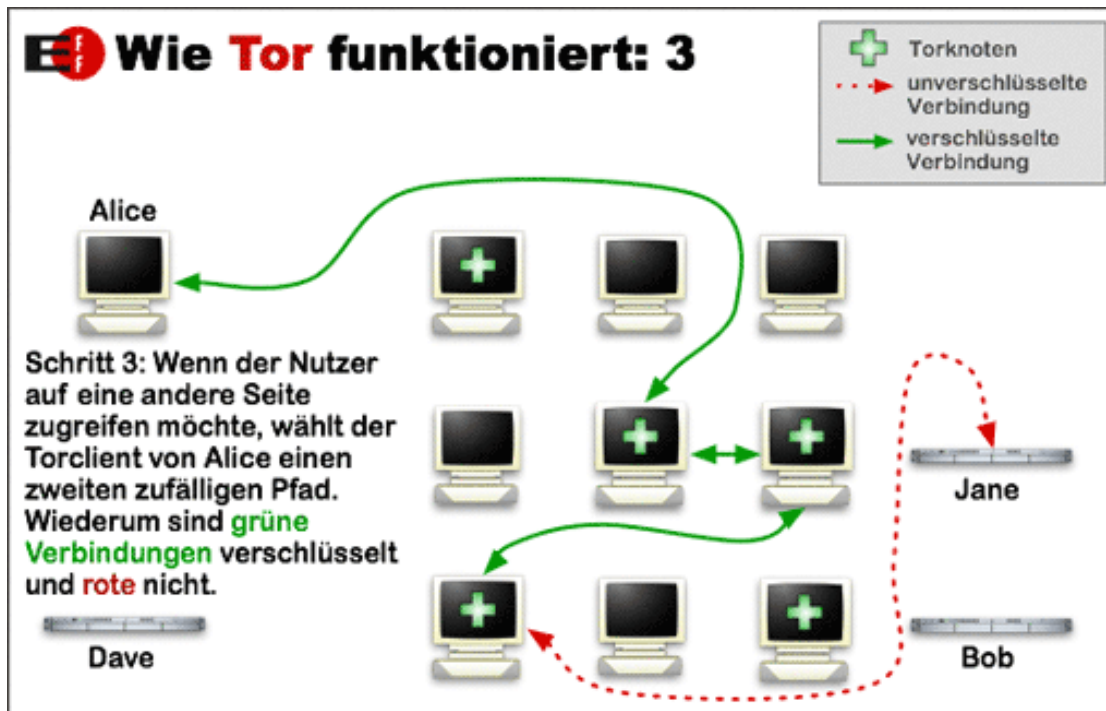
□→
TOR

² TOR funktioniert wie folgt: Auf dem eigenen Rechner hat man ein Programm laufen welches alle Web-Anfragen „bündelt“ und an eine Begin-Node des TOR-Netzwerkes schickt. Hierbei werden die Daten bereits verschlüsselt.

²Bilder entnommen von <http://www.torproject.org/overview.html.de>, MIT-Lizenz



Das TOR-Programm entscheidet wieviele Knoten im TOR-Netzwerk das Datenpaket durchlaufen muss bis es bei einer Exit-Node das TOR-Netzwerk verlassen darf. Die dabei benutzten TOR-Knoten kennen dabei weder den Inhalt des Datenpakets noch Anfragenden noch Zieladresse, sie kennen nur den Rechner von dem sie dieses Datenpaket bekommen haben und den an den sie schicken sollen.



Erst die Exit-Node kann die Anfrage entschlüsseln, das Ziel abfragen und so die Anfrage stellen. Der Rückweg geht dann über dasselbe Prinzip - dann fungiert die Exit-Node als Start-Node und nur das letzte Glied in der TOR-Kette weiss wer der Empfänger der Antwort ist. Es wird dabei auch ein anderer Weg als bei der Anfrage gewählt.

Um zu verhindern dass über Verkehrsverhalten ein Rückschluss gezogen werden kann generiert das TOR-Netzwerk auch notfalls Dummy-Pakete die hin und hergeschickt werden.

□→
 Fazit
 □→
 Lizenz



Lizenz: Creative Common License, Namensnennung, nicht-kommerziell, Weitergabe unter derselben Lizenz erlaubt.