ieee.es
Instituto Español de Estudios Estratégicos

Documento
Opinión

16/2012 21 febrero de 2012

*Luis de Salvador Carrasco**

REDES DE ANONIMIZACIÓN EN INTERNET: CÓMO FUNCIONAN Y CUÁLES SON SUS LÍMITES

REDES DE ANONIMIZACIÓN EN INTERNET: CÓMO FUNCIONAN Y CUÁLES SON SUS LÍMITES

Resumen:

Los servicios de publicación de filtraciones como Wikileaks, los ataques de Anonymous, las redes de financiación del crimen organizado, las botnets y las redes terroristas se comunican a través de Internet. Para poder operar con confidencialidad precisan de algo más que sistemas de cifrado, necesitan de medios que oculten el origen y el destino de sus comunicaciones y así evitar su localización, es decir, redes de anonimización. La más destacada de todas ellas es Tor. Aunque estas redes no son una garantía total de privacidad, pues tienen sus límites, sus riesgos y ofrecen un grado de anonimización que podría ser sorteado.

Abstract:

Whistleblower sites like Wikileaks, attacks from Anonymous, funding networks of the organized crime, botnets and terrorist organizations use Internet. They need confidentiality in their communications, and it means more than just cipher their messages. They need to hide the source or destination of their links and then to avoid localization. Therefore they will use of anonymity networks, like Tor. Although, those networks are not a full guarantee of privacy, thus they have limits, risks and a degree of privacy that could be dodged.

Palabras clave:

Sistemas de anonimización, Tor, conflicto asimétrico, Internet, ciberguerra.

Keywords:

Anonymity networks, Tor, asymmetric warfare, Internet, cyberwar.

INTRODUCCIÓN

El anonimato en Internet se podría definir como la capacidad de realizar cualquier acceso, comunicación o publicación en la red sin que terceros tengan la posibilidad de identificar o localizar al autor de dicha acción.

La privacidad en la navegación es un principio que tiene muchas aristas. Por un lado, preserva la libertad de los ciudadanos y permite el libre crecimiento personal, cultural y político, sobre todo en aquellos países en los que existen regímenes represivos.

Por otro lado, el anonimato supone una ventaja para la realización de actividades delictivas en Internet (violación de la propiedad intelectual, spam, ciberacoso, injurias, estafa, robo de identidad, pederastia, etc.), y sobre todo para el encubrimiento de actividades o agresiones en el caso de conflictos asimétricos o terrorismo. Esto último incluye desde los filtrados de información, actividades de inteligencia en fuentes abiertas, acciones de propaganda, mando y control, hacking y ciberguerra, etc. Es más, sin que fuese posible sortear la identificación, muchas de estas últimas acciones no serían viables.

Las variables que definen el anonimato son: "quién soy", "dónde estoy" y "qué hago". Estas tres variables son distintas pero íntimamente relacionadas entre sí, de forma que en muchos casos es posible deducir una de otra. Por ejemplo, si no se sabe quién soy o dónde estoy, mi comportamiento en la red no se me puede atribuir con facilidad, por el contrario, si se conoce dónde estoy y qué estoy haciendo, se puede inferir quién soy. En particular, "quién soy" es una variable mediatizada por la asimilación ordenador[1]-usuario ya que siempre se accede a través de un terminal. Esta identidad es cada día más estrecha, pues los dispositivos son cada vez más personales, aunque existen recursos para identificarnos por encima del sistema que estemos utilizando para acceder a la red.

Para proteger estas tres variables existen dos tipos de salvaguardas: las legales y las técnicas. Las legales se derivan de los derechos fundamentales definidos en la Constitución y desarrollados en las leyes: el derecho al honor, la intimidad, la privacidad y el secreto de las comunicaciones.

Entre las técnicas se encuentran los mecanismos para ocultar la identidad, la localización[2] y los servicios accedidos. Una de estas técnicas son las redes de anonimización.

[1] Más que ordenador, sistema final, pues quien dice ordenador, dice portátil, teléfono móvil, i-phone, i-pad o cualquier otro dispositivo que nos permita la comunicación.

[2] A través de la dirección IP se puede obtener información de geolocalización en algunas páginas web que dan una información muy genérica, p.e. http://ip-address-lookup-v4.com/ , pero a través de los ISP u operadores telefónicos es posible disponer de la localización e identificación del usuario con toda precisión.

PRINCIPIOS DE LAS REDES DE ANONIMIZACIÓN

Cuando un terminal se conecta a Internet es necesario que disponga de un número que lo identifique de forma unívoca, que lo diferencie de cualquier otro ordenador en la red y permita localizarlo, de igual forma que las direcciones postales distinguen cada calle y cada casa de cualquier otra en el mundo. Cuando un usuario solicita o envía una información, se genera una carta o paquete en el que se escribe tanto la dirección destino como el remitente. Se puede enviar información sin remitente[3], pero entonces nunca se podrá enviar una respuesta al origen. Y, aunque no nos demos cuenta, para acceder a una página de Internet, mandar un correo o escribir en un blog, es necesario intercambiar una gran cantidad de paquetes, intercambio que no podría ocurrir si no se tiene conocimiento de la dirección origen. Detrás de un simple "clic", hay un denso dialogo entre el ordenador origen y el destino que permite que se ejecute la acción que deseamos, y ese dialogo permite registrar quién se encuentra tras cada acceso a un servicio.

El envío de paquetes en Internet es muy similar al envío de paquetes en el correo ordinario. Aunque tenemos la sensación de que el paquete lo enviamos directamente al destinatario, realmente lo enviamos a una oficina postal, que a su vez lo reenviará a sucesivas oficinas postales (normalmente recorriendo una jerarquía) hasta llegar a la oficina del distrito postal del destino. Cada oficina recoge los paquetes postales, los registra y luego redirige los paquetes a otra oficina o a su destinario. Esa redirección se denomina enrutar el paquete. La oficina se comporta como un enrutador (router) y cada vez que se enruta un paquete se lee en el mismo de dónde viene y a dónde va.

La escritura de la dirección origen en el paquete nos delata ante cualquiera que intercepte dicho mensaje en cualquier punto del reenvío de paquetes, aparte de poder acceder al contenido del mismo. Una forma para garantizar la confidencialidad es cifrar el contenido del paquete, que es como cerrar su contenido con una llave. Pero claro, esto no evita que las direcciones origen y destino aparezcan claras a cualquier observador o intruso.

Un modo de evitarlo es, previamente al envío del paquete, negociar una ruta entre oficinas postales para alcanzar el destino desde el origen. Cuando se envía un paquete a la oficina más próxima, en este sí aparece la escrita dirección del remitente. Pero cuando ese paquete se reenvía a la siguiente oficina, se borra dicha dirección y se rescribe como remitente la de la anterior oficina postal, de forma que se elimine el rastro del origen. Así sucesivamente hasta que se sirve el paquete al destino final. La dirección origen que lee el destinatario es el

[3] Se puede falsificar el origen y utilizar técnicas de spoofing, pero el propósito no será entonces un acceso anónimo.

de la oficina postal más próxima a él. La información de quiénes somos realmente está protegida por la confidencialidad de las oficinas postales intermedias. Estas guardan el registro de la ruta negociada mientras dure el intercambio de información para permitir la comunicación bidireccional. La oficina postal ya no sólo es un enrutador, sino un agente de reenvío (proxy).

APLICACIONES DE LAS REDES DE ANONIMIZACIÓN

Los servicios de anonimización son una herramienta que permite sortear la censura gubernamental que limita el libre acceso a contenidos en Internet. Estos servicios consiguieron que los opositores a Mubarak sorteasen el bloqueo[4] impuesto en la red, encubren a los ciudadanos sirios que difunden noticias a través de sus blogs, permiten al pueblo chino el acceso a las webs occidentales[5] y protegen la libertad de información y de prensa en general.

En los países donde las libertades están garantizadas, las redes de anonimización preservan la privacidad y la identidad de los ciudadanos de los usos abusivos que de los datos de navegación puedan realizar terceros[6] y de la negligencia al tratar esos datos. Además, permiten sortear controles o limitaciones impuestos por empresas al acceso a contenidos de Internet, para el caso de usuarios que navegan desde su puesto de trabajo, o los establecidos a nivel más general, como los que bloquean el acceso a páginas que ofrecen contenidos ilegales[7].

Estas redes también son una ventaja para aquellas organizaciones que se enfrentan al control y supervisión de los gobiernos, especialmente en el caso de conflictos asimétricos[8]. Sin ellas, serían difíciles de entender muchas actividades de hackers, como ataques basados

[4] No todos los países utilizan las mismas técnicas de bloqueo, mientras que en China existe un bloqueo centralizado a nivel de backbone basado en direcciones IP y palabras clave (relacionadas con derechos humanos, Taiwán, Tíbet, etc.), en Irán las estrategias están descentralizadas al ser los ISP responsables de implementar las políticas de censura.

[5] Existen otros recursos no relacionados con mecanismos de anonimización que permiten evitar las limitaciones al acceso a determinadas webs, como acceso a las cachés en Internet, servicios de traducción, RSS, nombres de dominios alternativos, etc.

[6] Podrían ser empresas en el caso de marketing, o pedófilos en el caso de que accedan a la red menores de edad.

[7] En USA hay filtrados automáticos de contenidos pedófilos en ciertas redes. En España se intenta limitar el acceso a aquellas páginas en las que se vende mercancía pirata o de imitación. En ese caso, las autoridades se ponen en contacto con los Servidores de Nombres para eliminar las referencias a dichas páginas. Este sistema es válido siempre y cuando no se utilicen los sistemas de anonimización.

[8] En relación a cómo se emplean por y contra los actores asimétricos es muy interesante el documento: Torres Soriano, Manuel, *El papel de internet en los procesos de abandono y debilitamiento de la violencia terrorista,* Documento de Opinión IEEE 75/2011.

en URL y el control de botnets, las filtraciones de Wikileaks o Cryptome, la actividad de grupos de desestabilización como Anonymous y el mantenimiento de las infraestructuras terroristas[9], tanto para dar soporte a sus redes de mando control, realizar actividades de propaganda en la red, proselitismo, financiación, la cibermilitancia,[10] etc.

Las redes de anonimización permiten encubrir las actividades de inteligencia sin el riesgo de ser localizados e identificados. Gracias a ellas, las organizaciones de inteligencia, estatales o no, pueden acceder de forma discreta y sistemática a fuentes abiertas y llevar a cabo operaciones cibernéticas, bien proactivas o iniciadas en respuesta de una acción hostil.

SOLUCIONES DE ANONIMIZACIÓN

Existen dos tipos de soluciones para navegar anónimamente. La primera consiste en hacer uso de páginas web que, sin tener que instalar o usar ninguna aplicación, permiten acceder vía web a determinados servicios[11] de forma anónima: son los llamados proxies o agentes de reenvío, que también se conocen como anonimizadores single-point. Aparte de su menor eficacia para preservar el anonimato (están más orientados a sortear controles como los filtrados de contenidos corporativos o estatales), suelen tener la limitación que no permiten usar cualquier cliente TCP, como servicios de correo no web-mail, IRC, P2P, etc. Es decir, sólo sirven para navegar, no para realizar otras actividades en Internet. Para tener un mejor servicio, más completo y seguro, es necesario utilizar técnicas más elaboradas que encadenan redes de routers, es decir, redes de anonimización, como Tor.

TOR

La red Tor es la red de anonimización más popular y, además, completamente gratuita. Ve la luz en el año 2002 como un proyecto patrocinado por el Naval Research Laboratory[12], fue financiado por la Electronic Frontier Foundation y actualmente por Tor Project, una organización no gubernamental basada en USA[13]. El antecedente de Tor fue la red Zero Knowledge Systems, proyecto que fracasó en 2001 por falta de fondos.

---

[9] Desaparecería el concepto de Internet como "Santuario", como señala Juan Hernández Gutiérrez, J. *Insurgencia y contrainsurgencia, Actores armados no estatales: Retos a la seguridad global*, IEEE Cuadernos de Estrategia, junio 2011.

[10] Jordán, J. *El terrorismo global una década después del 11-S, Actores armados no estatales: Retos a la seguridad global*, IEEE Cuadernos de Estrategia, junio 2011.

[11] Como http://anonymouse.org, aunque en http://proxy.org/ se puede conseguir una lista de más de 2000 de estos servicios.

[12] El NRL es un laboratorio conjunto de la Armada y del Cuerpo de Marines de los EE.UU.: http://www.nrl.navy.mil/.

[13] Fraser, Nicholas A. et al. *Tor: An Anonymous Routing Network for Covert On-line Operations* Center for Information Security Education and Research, Air Force Institute of Technology, IOSphere, Fall 2005.

Actualmente, Tor es un conjunto de cientos de servidores a lo largo de más de 20 países operados por voluntarios. Estos servidores se denominan “routers cebolla” (onion routers u OR), de donde se origina el nombre Tor como acrónimo de “The Onion Routing Project”.

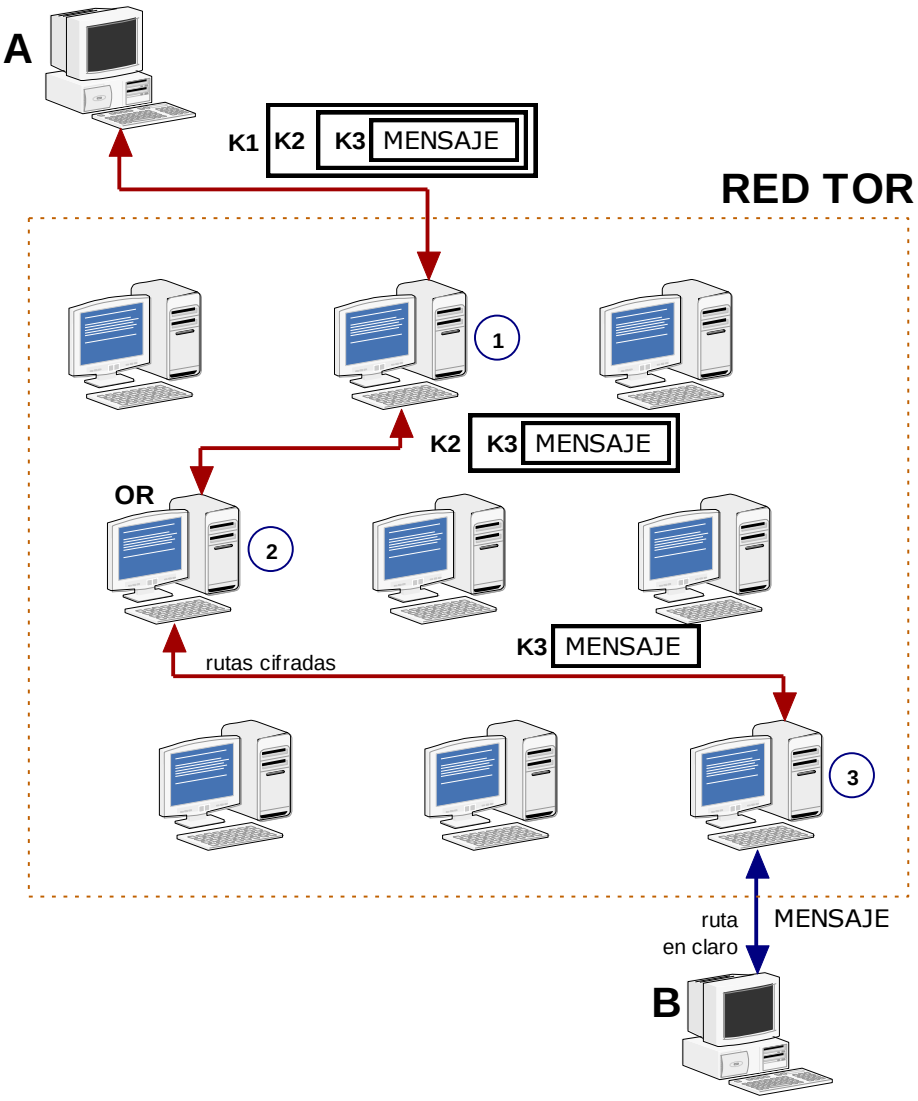

Imagen 1 La red Tor selecciona una ruta aleatoria a través de sus routers, y cifra sucesivamente el mensaje con claves de cada router. El mensaje sólo está en claro en el enlace que une el nodo de salida al destinatario final

Se puede acceder a Tor a través de un cliente Tor instalado en el ordenador que se puede descargar desde la propia página del proyecto[14] y, actualmente, existen aplicaciones para móviles Android, una de ellas Orbot, y también en la tienda de Apple ha aparecido recientemente Covert Browser para navegar con Tor desde iPad. Tor se basa en el concepto de enrutado por capas, donde los mensajes se empaquetan en varios niveles de cifrado antes de ser enviados. Cuando un usuario A quiere comunicarse con un usuario B a través de

[14] www.torproject.org.

Tor ha de ponerse en contacto con un OP (onion proxy). La red Tor establecerá entre ambos un circuito a través de tres OR. Cuando un mensaje llega al primer OR de un circuito, se elimina el primer nivel de cifrado y se reenvía al siguiente OR. Este proceso se repite hasta que alcanza el OR del final del circuito. En ese momento, el mensaje es descifrado (por lo tanto ya en texto plano) y reenviado al destino.

JAP

Tor no es la única opción para acceder a este tipo de redes. JAP (también conocido como JonDonym[15] o Java Anon Proxy) es un servicio de anonimización patrocinado por la Universidad de Regensburg y la de Dresde[16]. Proporciona una cadena de servicios de proxy o reenvío, de al menos tres etapas, en el servicio de pago, y de solo dos etapas en el servicio gratuito. La mayoría de los nodos están basados en Alemania. La fiabilidad de esta red no se basa en el gran número de nodos o su aleatoriedad, como en el caso de Tor, sino en la auditoría y certificación que se realiza de forma regular a los operadores que proporcionan los nodos a la red.

El acceso a la red JonDonym se realiza instalando un cliente, llamado Jondo sobre Java, y soporta tráfico HTTP y HTTPS, con un tiempo de respuesta que se estima mejor que Tor.

I2P

Como aparece en la propia web de I2P[17], ésta es una red anónima creada en 2003, gratuita, de código abierto, que ofrece a las aplicaciones que requieren de protección de identidad una simple capa para la comunicación segura.

Los principios son los mismos que en la red Tor, con cifrado por capas entre routers. Aunque hay algunas diferencias: por ejemplo, no hay cifrado en la comunicación entre el origen y el primer nodo I2P, ni entre el último nodo I2P y el destino. Además, las rutas establecidas o túneles no son bidireccionales ni hay un servicio centralizado que almacene el conjunto de routers, como en Tor, sino que éste es distribuido. Soporta varios tipos de protocolos, como protocolos de correo, P2P, mensajería instantánea, creación de sitios web anónimos en I2P, IRC y otros.

[15] http://www.jondos.org/en/index.html.
[16] http://anon.inf.tu-dresden.de/index_en.html.
[17] http://www.i2p2.de.

OTROS SERVICIOS

Existen otros servicios como Anonymizer[18], servicio de pago que ofrece una red privada de anonimización, Freenet[19], en este caso para chatear y publicar de forma anónima, los servicios de re-mail[20], que permiten enviar correos de forma anónima, etc.

CARACTERÍSTICAS Y DEBILIDADES DE LAS REDES DE ANONIMIZACIÓN

Las características que definen una red de anonimización son: el grado de anonimización que proporcionan (definido como su resistencia a ataques de re-identificación), su fiabilidad, su ancho de banda y su latencia[21]. Por supuesto, a mayor anonimización y fiabilidad, menor ancho de banda y mayor latencia.

Un factor crítico para determinar la fortaleza de una red de anonimización es el número de nodos que la componen y el volumen de tráfico que la atraviesa. Un sistema con pocos nodos o que tiene muy poco tráfico es muy vulnerable al ataque por análisis de tráfico. Los nodos de entrada y salida a una red de anonimización son, necesariamente, públicos y, observando el tráfico entre ellos y correlando los accesos, es fácil determinar quién accede a qué[22]. Este es un factor crítico en el caso de los servicios de pago, como JAP u otras redes de anonimización privada, en el que el número de usuarios en un momento dado puede no superar la centena. Por ello, una iniciativa lanzada por los desarrolladores de Tor ha sido la de animar a suscribirse a los servicios de Cloud Computing de Amazon (el líder en el mercado de servicios en la nube) para emplear sus servicios de computación virtual para implementar puentes a Tor[23], y de esta forma aumentar enormemente el número de nodos.

De todos los nodos de la red, el de salida es el punto clave en la comunicación entre el usuario y el servicio remoto, donde los datos normalmente están sin cifrar, se puede realizar un historial de navegación de un usuario en una sesión determinada, obtener información de cuentas y claves de acceso o acceder a las cookies de sesión. Toda esta información, puede unirse como piezas de un puzle para re-identificar al usuario de la red[24].

---

[18] http://www.anonymizer.com.
[19] http://freenetproject.org/.
[20] Una lista de remailers está disponible en http://www.spywarewarrior.com/uiuc/info20b.htm.
[21] El ancho de banda implica la velocidad de descarga, la latencia el tiempo que pasa desde que se solicita la descarga de un contenido hasta que empieza a servirse.
[22] Murdoch, S. et al. *Low-Cost Traffic Analysis of Tor* University of Cambridge, Computer Laboratory 2005 IEEE Symposium on Security and Privacy.
[23] https://blog.torproject.org/blog/run-tor-bridge-amazon-cloud.
[24] Los ataques a las redes de anonimización no sólo parten de los estados. Anonymous también lo hizo

Las redes pueden utilizar técnicas como mixing para dificultar el análisis de tráfico. Un servidor se dice que es un Mix si toma un conjunto de mensajes, un pool, los transforma (empleando cifrado o descifrado), los reordena en el pool y retarda su salida. El inconveniente del mezclado es que incrementa la latencia y no permite su uso con servicios interactivos, por lo que no se suele aplicar. Es adecuado para comunicaciones sin requisitos de tiempo real, como correo electrónico. Otra debilidad es que, como es natural, las propias redes de anonimización contienen la información de quién accede a qué. Por supuesto, el primer nodo de la red conoce la IP del usuario y el último el destinatario y el tráfico no cifrado[25]. Hay que confiar en que la red de anonimización no guarde registros de quién accedió a qué utilizando sus servicios. Por supuesto, todas ellas proclaman que tal registro no se produce, aunque algunas con matices[26].

Cualquier red de anonimización es vulnerable a ataques por denegación de servicio, abriendo de forma masiva sesiones contra sus nodos. Hay estrategias para minimizar esta vulnerabilidad, pero también tienen impacto tanto en la latencia del sistema como en la privacidad de los usuarios. Para prevenirlos, la red Tor incorpora protocolos de "proof-of-work"[27] y así evitar a los OR tener que completar un gran número de operaciones de cifrado en caso de agresión.

Un ataque adicional sobre redes no privadas, como Tor, es poblar la red con nodos controlados por algún sujeto, que se pueden emplear para monitorizar las comunicaciones. Claro está, es una estrategia sólo al alcance de organizaciones con suficientes recursos, ya sea estatal o no estatal. Esta estrategia no permitiría re-identificar todo el tráfico de la red o de un usuario a su elección, pues focalizar el análisis sobre una comunicación específica en un momento dado sería muy difícil ya que los nodos se eligen de forma aleatoria, pero para los casos en los que los nodos elegidos sean precisamente los de entrada o de salida, la información que proporciona sobre el tráfico es muy alta. Más interesante es que, controlando parte de la red, se puede atacar la disponibilidad de la misma en un momento o situación crítica, eliminando todo el tráfico que se realice a través de los nodos controlados por dicha organización.

---

recientemente para sabotear el uso que de Tor realizaban redes de pederastas: http://arstechnica.com/business/news/2011/10/anonymous-takes-down-darknet-child-porn-site-on-tor-network.ars.

[25] Para mejorar la privacidad y otros ataques, antes de los nodos iniciales y finales se puede levantar una VPN, es decir, mantener una sesión cifrada, pero esto no será posible si el servicio al que se quiere acceder no lo soporta.

[26] La red Anonymizer, declara que sí guarda un registro de las direcciones accedidas, aunque no una correspondencia entre sitios accedidos y usuarios.

[27] En concreto el CCP, el protocolo de puzle en el lado del cliente, en el que el servidor pide al cliente que realice determinadas operaciones y así asegurarse que detrás de ese cliente no hay una máquina abriendo cientos o miles de sesiones.

OTRAS AMENAZAS A LA NAVEGACIÓN ANÓNIMA

La privacidad en Internet está amenazada de varias formas y las redes de anonimización no protegen de forma completa la intimidad de un acceso a través de la red. Cada vez que se accede a un servicio en Internet se transmite mucha información que identifica nuestro sistema[28], o al usuario como persona física, más allá de la dirección IP que se está empleando.

El acceso a una página web implica, no sólo descargar información de un único servidor, sino también contenido de terceros[29] que almacenan información en nuestro sistema en forma de cookies que nos identifican. Esto es muy común en las cookies insertadas por empresas de marketing en relación a los medidores de audiencia o a la publicidad conductual[30], que permiten rastrear nuestra identidad y nuestras preferencias.

De igual forma, los plugins insertados en las páginas (p.e. Flash) podrían establecer conexiones directas no anonimizadas con otros servicios y así identificar la identidad del usuario, así como también aplicaciones Java, Javascript o ActiveX que precisen de autentificación o accedan a los recursos de nuestro sistema.

El sector del comercio electrónico también es un enemigo de la navegación anónima. En dicho sector es muy importante el poder detectar cuándo una misma fuente está intentado acceder a servicios con personalidades diferentes (posiblemente falsas o robadas). Para ello se han desarrollado soluciones, que se emplean a nivel global, que identifican la firma de un ordenador[31] y siguen su comportamiento a través de cualquier portal de venta electrónica[32] o de cualquiera que tuviera dicho servicio contratado.

Asimismo, cualquier intercambio de contenidos que incluya, no sólo texto, sino información en algún formato conocido, incluirá metadatos, es decir, información complementaria sobre quién, cuándo, cómo y dónde se generó el fichero. Esto ocurrirá con documentos en Word,

[28] Podemos ver la información que proporcionamos de nuestro sistema en, por ejemplo, http://network-tools.com/analyze/.

[29] Dentro del código de una página web, por ejemplo, hay referencias a imágenes, publicidad, programas, etc., que están almacenados en servidores distintos al que explícitamente estamos accediendo, que registrarán nuestro acceso y descargaran, o accederán, a información adicional.

[30] Consultar las páginas http://www.privacychoice.org/ y para comprobar las conexiones que están realizando en la sesión actual del navegador es muy interesante la demo http://collusion.toolness.org.

[31] Cada vez que se realiza un acceso a través de Internet, se identifica el navegador, el lenguaje, las versiones de plug-ins instaladas y todo un conjunto de parámetros que dibujan de forma precisa (tal vez no unívoca) nuestro sistema.

[32] Consultar las soluciones que ofrece ThreatMetrix para comercio electrónico en http://threatmetrix.com/.

PDF e incluso fotografías, que vía formato EXIF incluye información de fecha, geolocalización de la imagen tomada o incluso los fragmentos eliminados de la imagen transmitida[33]. Es más, incluimos metadatos incluso en los tweets de tweeter[34].

La geolocalización de nuestros dispositivos no sólo depende de la dirección IP, que es ocultada por la red de anonimización. Protocolos superiores al del nivel de red sortean la ocultación de la IP proporcionando información geográfica y, en muchos casos, muestra la localización tanto en dispositivos móviles como en ordenadores personales o routers[35] de forma transparente al usuario, sin precisar una activación expresa de dicho servicio[36].

System Details:
Platform: Windows 7
Win16: False
WinInstallerMinVer: 0

Browser Type and Version:
Browser: Firefox
Fullversion: 8.0.1
Gecko: True
GeckoBuildDate: 20100101
Crawler: False
Authenticode Update: 0

Cookie Test:
Session cookies: Enabled
Permanent cookies: Enabled

Browser Security:
JavaScriptEnabled: True
VBScriptEnabled: False
JavaEnabled: True
ActiveXEnabled: False
SSL: True
Port Check for Ports 80,139,554,16771:
Open Ports: 80,16771
PopupsBlocked: True
ImagesEnabled: True
HighSecurity: False

Connection Details:
ConnectionType:
Proxy: False
CompressGZip: True
AOL: False
MSN: False

Display and Layout:
Width: 1600
WidthAvail: 1600
Height: 900
StyleSheets: True
PNG: True
FontSmoothing: False
FontColor: True
FontSize: True
Tables: True
TableBGColor: True
TableBGImage: True
ColorDepth: 24
Frames: True
IFrames: True
Background Sounds: False

Scripting Capabilities:
ActiveXControls: False
ActiveXEnabled: False
JavaScript: True
JavaScriptEnabled: True
JavaScriptVer: 1.8
JavaScriptBuild:
VBScript: False
VBScriptEnabled: False
VBScriptBuild:
XML: True
XMLHttpRequest: True
DHTML : True
FileUpload: Yes
Channel Definition Format: False
MouseOver: True

Plugin Information:
Acrobat Version: 9.1.0.163.
Authorware Plugin Not Installed.
Citrix Plugin Not Installed.
Crystal Reports Plugin Not Installed.
Director (Shockwave) Plugin Not Installed.
Macromedia Flash Version: 11.1 r102.
Flip4Mac Plugin Not Installed.
iPixViewer Plugin Not Installed.
MapGuide Plugin Not Installed.
QuickTime Plugin Not Installed.
RealPlayer Plugin Not Installed.
Microsoft Silverlight Plugin Version: 4.0.
SVGViewer Plugin Not Installed.
Viewpoint Plugin Not Installed.

Java Information:
JavaApplets: True
JavaEnabled: True
MSJVM DLL Build:

Wireless Device Information:
PDA: False
WAP: False
HDML: False

Locale Information:
Language: Spanish
User Language: es-es
System Language:
Time Zone Difference: 6
Browser Date and Time :
mi?rcoles, 14 de diciembre de 2011 23:00:11
Browser Date and Time ms: 1323900011139

Imagen 2 Ejemplo de parámetros de nuestro sistema capturados normalmente en un acceso a Internet[37].

Los canales ocultos en nuestros sistemas son otro riesgo al anonimato. Un ejemplo muy gráfico de canal oculto es el reciente escándalo Carrier IQ[38]: instalado en el móvil, con total desconocimiento del usuario, se encuentra un software que envía información de toda su

[33] Se conocen como thumbnails y reflejan, a menor resolución, la imagen original antes de ser recortada o parcialmente borrada. Algunos ejemplos se pueden encontrar en: http://no.spam.ee/~tonu/exif/?offset=1920.

[34] Es interesante consultar el mapa de metadatos de un tweet en: http://www.slaw.ca/wp-content/uploads/2011/11/map-of-a-tweet-copy.pdf, o buscando directamente por "map of a twitter status object".

[35] No sólo Google utiliza la información de los routers Wifi, existen otras compañías, como: http://www.skyhookwireless.com/.

[36] Un ejemplo de geolocalización es el servicio que se encuentra activado por defecto en Firefox, aunque se supone que cada vez que se geolocaliza se advierte al usuario (salvo errores): http://www.mozilla.org/es-ES/firefox/geolocation/.

[37] De http://network-tools.com/analyze.

[38] http://androidsecuritytest.com/features/logs-and-services/loggers/carrieriq/.

actividad, puede que incluso aquello que se escribe, a un tercero o terceros. La comunicación de todos esos datos se lleva a cabo empleando conexiones alternativas a las seguras, cifradas o anónimas que se hayan podido establecer.

Por otro lado, una razón que hace más interesante el uso de redes de anonimización es la previsión para el año próximo de que los ISP proporcionen acceso a nodos IPv6 directamente a los usuarios domésticos finales y, en general, a los usuarios de las redes[39]. Una de las particularidades del direccionamiento IPv6 es que la dirección MAC del dispositivo, numeración que identifica de forma unívoca una máquina (ordenador, tablet, móvil o electrodoméstico en la Web 3.0), forma parte de esa dirección. Por lo tanto, la identificación del ordenador ya no se enmascarará en los routers, sino que se almacenará en los registros de acceso de los servidores (y los nodos de entrada a las redes de anonimización). Esto implica que, independientemente de la red a la que se conecte un sistema, se identificará éste de forma unívoca, lo que, por ejemplo, permitirá identificar un ordenador que se comunique a través de una WIFI abierta.

CONCLUSIONES

Las redes de anonimización, una muestra más de la iniciativa del DoD en el desarrollo de Internet, son un recurso imprescindible para preservar la privacidad en la red y la libertad de los ciudadanos, sobre todo en estados represivos, pero también da soporte a actividades delictivas, a la delincuencia organizada, a operaciones asimétricas y actividades de inteligencia.

Las redes de anonimización no garantizan completamente la privacidad, sino que la hacen más difícil de romper. El grado de interconectividad alcanzado en la red, que permite cruzar datos de muchas fuentes, la complejidad de las TIC, que hacen difícil conocer en profundidad todas sus implicaciones técnicas, y el uso de sistemas que son cajas negras[40] incluso para usuarios avanzados, hacen que el anonimato de los usuarios quede fácilmente comprometido. Para tener una mayor seguridad en la ocultación de la identidad es necesario tomar precauciones adicionales y tener definidos claramente unos procedimientos de actuación, de acceso y utilización de la red, que incluirán el empleo de soluciones técnicas como pueden ser: entornos virtuales exclusivos para accesos anónimos, cuentas de correo

[39] Mediante el modo dual-stack, que permitirá simultanear éste con el anterior IPv4.
[40] Hay dispositivos que pueden resultar muy atractivos, que todo el mundo quiere tener, pero de los que se desconocen sus debilidades. Pueden resultar caramelos envenados. Un ejemplo histórico es el siguiente, cuando finalizó la Segunda Guerra Mundial, las máquinas Enigma que recogieron los británicos fueron distribuidas entre sus aliados como un sistema seguro de comunicación, aunque aquellos conservaban su capacidad de romper el cifrado de todas ellas.

de uso único, sesiones no simultáneas con distintos propósitos, disciplina de utilización de Internet[41], limitación de su uso, etc. Pero sobre todo es fundamental conocer qué tecnología se está empleando, sus limitaciones y sus puntos oscuros, tanto de los sistemas que están sobre la mesa, como los que se portan en los bolsillos.

Por otra parte, una gestión responsable de los sistemas de información, sobre todo en las Administraciones Públicas y en el sector Defensa, ha de prevenir el acceso hacia y desde redes de anonimización y otros agentes de reenvío[42]. Esto supone implantar mecanismos para rechazar el tráfico que pueda proceder de un nodo de anonimización[43] como potenciales agresores[44]. Por otro lado, es necesario monitorizar todo el tráfico de salida hacia dichos nodos para detectar el uso fraudulento de nuestros propios servicios. En uno u otro caso, hay que ser conscientes que el uso de recursos de anonimización evidencia y delata conductas que han/pueden levantar sospechas y señalar posibles objetivos de vigilancia. Se ciernen amenazas sobre el uso anónimo de Internet. Entre ellas, existen voces en el mundo de Internet que claman por el fin de una navegación que preserve la privacidad de los usuarios, bien a nivel global o bien a nivel de determinados servicios. Facebook[45] y Google+ protagonizan iniciativas para evitar la creación de falsos perfiles e intentan liderar un movimiento contra el anonimato en Internet, al que se suman servicios como Spotify, Amazon y otros. Cabe preguntarse si el final de la navegación anónima afectará únicamente al usuario común, no especializado, que será el que se verá afectado por su pérdida de privacidad, o delatado por emplear técnicas que no proporcionan las necesarias garantías.

Luis de Salvador Carrasco
Doctor en Informática[46]

41 En el caso de utilizar simultáneamente aplicaciones seguras como otras no seguras en la misma sesión de Tor, estaremos proporcionando información adicional para nuestra reidentificación. Para ello, ver el estudio: Le Blond, S. et al. One Bad Apple Spoils the Bunch Exploiting P2P Applications to Trace and Profile Tor Users I.N.R.I.A, France abril 2011.

42 Como se señala en el *Nuevo Concepto Estratégico de la OTAN*: http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf: "... se debe … desarrollar nuestra capacidad de prevenir, detectar, defenderse y recuperarse de ciberataques…". Actualmente, se puede acceder a las webs del IEEE, de Defensa, de empresas del sector o de las FyCSE desde proxies o desde Tor.

43 Se pueden encontrar en Internet listas de los nodos Tor http://proxy.org/tor.shtml y de otros servicios de anonimización.

44 Los últimos casos de ataque a las AA.PP. han procedido de nodos de anonimización.

45 Facebook ha iniciado una guerra contra los pseudónimos, una de sus víctimas fue el escritor Salman Rushdie, quien tuvo problemas para tener una cuenta en Facebook con su propio nombre, ya que su nombre es Ahmed Salman Rushdie y la dirección de la red social sólo le permitía una cuenta con el nombre Ahmed Rushdie.

46 Las ideas contenidas en los ***Documentos de Opinión*** son de responsabilidad de sus autores, sin que reflejen, necesariamente, el pensamiento del IEEE o del Ministerio de Defensa.