Paakat: Revista de Tecnología y Sociedad
ISSN: 2007-3607
Universidad de Guadalajara
Sistema de Universidad Virtual
México
suv.paakat@redudg.udg.mx

Año 5, número 9, septiembre 2015-febrero 2016

El proyecto Tor

José Antonio Amaro López[1]
Centro Universitario de Ciencias Sociales y Humanidades
de la Universidad de Guadalajara, México.

[Recibido: 12/06/2015. Aceptado para su publicación: 6/08/2015]

Resumen
La privacidad es importante al momento de conectarse a Internet, el usuario debe tener la seguridad de que no existe una tercera persona escuchando u observando la red para recopilar sus datos. Por lo anterior, se describe el proyecto Tor y cómo logra asegurar la privacidad y el anonimato de los navegantes en Internet, con base en el modelo de cebolla (*onion routing*).

Palabras clave
Privacidad, anonimato, proyecto Tor.

Tor Project

Abstract
Privacy is important when a user is connected to Internet, the user must have the assurance that there is no third person listening in the network to get their data. Therefore the Tor project is described and how is it assure the privacy and anonymity of the Internet navigators, supported by the onion routing.

Key words
Privacy, anonymity, Tor Project.

Desde tiempos remotos, la comunicación tuvo un papel importante en la sociedad para transmitir conocimientos, ideas, organizar, influir en la toma de decisiones y compartir, con el fin de sobrevivir en el entorno hostil en el que se desenvolvían los seres humanos.

En la actualidad, la comunicación sigue teniendo un papel primordial en nuestras vidas, debido a la cantidad de información que se produce, se transmite y se intenta administrar para la toma de decisiones, para proveer educación, para el ocio, para vender productos o servicios, etc.

Pero en la comunicación, el medio para transmitir la información también es relevante, ya que éste debe asegurar que los datos enviados lleguen a su destinatario, completos, de manera eficiente, confiable y sin ser interceptados y decodificados por un sujeto no autorizado. Es decir, el medio por el cual se transmite la información debe proveer de métodos para que los datos lleguen al destino, sin contratiempo, y de manera segura.

Por lo anterior, y con el auge de Internet a partir de los años noventa, el medio por el cual se establecen la mayoría de las comunicaciones entre dos o más personas, es a través de diversos equipos interconectados que dan vida a esta red de redes y que permiten el envío de una gran cantidad de mensajes, lo cual reduce la confiabilidad y aumenta la facilidad para interceptar las comunicaciones, debido a la gran cantidad de información que viaja a través de Internet, además, de la gran cantidad de personas conectadas.

De acuerdo con el documento "ICT Facts & Figures-The world in 2015", elaborado por la Unión Internacional de comunicaciones (ITU), para finales del año 2015 habrá 3.2 billones de personas conectadas a Internet, lo cual generaría la transmisión de una cantidad inmensa de información y de comunicaciones. En la actualidad no existe un número exacto de la cantidad de bytes transmitidos por los usuarios de la Internet[2], pero Hilbert y López (2011) establecieron que en 2007 las personas lograron comunicar casi 2×10^{21} bytes de información, y, de acuerdo con un estudio presentado en el año 2010, por la empresa EMC[2], durante ese año la cantidad creada de información fue de 1.2 zetabytes[3] (Gantz, y Reinsel, 2010, p. 1).

Precisamente, debido a la cantidad de información que se genera y a los usuarios que se conectan a la Internet, se presenta un problema de seguridad, donde la información pueda ser interceptada y decodificada por un tercero, el cual puede obtener acceso a cuentas de bancos, contraseñas de correos electrónicos, copiar archivos del disco duro, mensajes de WhatsApp, documentos personales, fotografías, controlar la computadora infiltrada de manera remota, etcétera; con la finalidad de vender la información o hacerse de recursos mediante el saqueo de las cuentas bancarias de la víctima.

Es el caso del empleado de la CIA, Edward Snowden, quien mediante herramientas y procesos tecnológicos logró hacerse de una cantidad considerable de documentos privados del gobierno de Estados Unidos, lo que desenmascaro una red de vigilancia e intercepción de comunicaciones secreta que tiene este país, y evidenció a otros países que contaban con agencias para vigilar a sus ciudadanos, incluso a otros fuera de su territorio, violando los derechos a la privacidad con que cuenta todo ser humano.

Debido a lo anterior, se desarrollan herramientas para mejorar la privacidad en las comunicaciones que se establecen entre los usuarios, tal como la red TOR[4] (*The Onion Routing*), una red abierta que le permite a los usuarios defenderse contra el análisis de tráfico que realizan algunas instancias gubernamentales sobre Internet, y que es una forma de vigilancia que amenaza la libertad personal, la privacidad, la confidencialidad en los negocios, así como las relaciones y la seguridad del Estado (TOR, 2014).

La red TOR se basa en el modelo de enrutamiento tipo cebolla, de ahí su nombre, donde el mensaje que se envía es introducido a la red mediante un equipo llamado "embudo de entrada", el cual se encarga de construir una estructura de datos especial y de establecer la ruta que deberán seguir los datos a través de la red *onion*. Este equipo de entrada o cualquier equipo enrutador que pertenezca a la red *onion*, descifrará el mensaje y en él encontrará el siguiente equipo al cual deberá ser enviado, no sin antes volver a encriptar el mismo. Se envía el mensaje al siguiente equipo el cual realiza el proceso de descifrar, encriptar y enviar el mensaje hasta alcanzar un "embudo de salida", el cual entrega el mensaje al destinatario.

Como se puede ver, esta red consta de una serie de múltiples capas de encriptación, y mantiene la información sobre la ruta que se propagará el mensaje, hasta encontrar el equipo "embudo de salida" que entregará la información al usuario final. El receptor sólo conoce el equipo que le envío el mensaje ("embudo de salida") y es, a este equipo, al cual se enviará la respuesta, lo que permite a los usuarios mantenerse anónimos y, por lo tanto, lograr su privacidad.

Para enlazarse a esta red, la organización Tor Project (quien la mantiene), desarrolló un navegador llamado Tor Browser —tomando como base el código fuente del navegador Firefox—, el cual le permite a una persona conectarse de manera automática a la red Tor o configurar la conexión según las necesidades del usuario.

El navegador Tor Browser no es diferente de los más utilizados como Internet Explorer, Firefox o Safari. Tiene un menú, barra de direcciones, un área para mostrar el contenido de la página visitada, etc., lo interesante es la configuración del mismo porque, de manera estándar, tiene activado el uso de JavaScript, CSS, Flash entre otros *plugins*[5] para que el usuario pueda ver sus páginas como en cualquier otro navegador. Aunque para mantenerse anónimo en esta red, Tor Project sugiere desactivar todos los *plugins* que comúnmente se utilizan en otros navegadores, ya que mediante estos agregados las empresas o el gobierno pueden realizar un seguimiento de los usuarios, de donde es posible obtener datos sobre las páginas que visitan, las cosas que compran, las personas con quienes mantienen contacto, etc. El seguimiento a los usuarios puede ser utilizado en alguna demanda legal para comprobar que actividad se realizó desde cierto equipo, porque se puede obtener la fecha, hora y el lugar de acceso.

Empresas como Google, Yahoo! y Facebook, por mencionar algunas, logran revisar, recopilar, organizar y analizar información de sus visitantes, y, con base en ello, enviarles propaganda comercial, política e informativa adecuada a sus intereses de los usuarios según los clics que dieron o las páginas que visitaron en el día, las semanas, los meses o años. Todos estos datos convierten a las personas en posibles clientes o victimas de quienes utilizan su información con la finalidad de lograr acceder a su computadora y recabar información privada.

Con el fin de evitar que terceros pueden interceptar nuestras comunicaciones y para mantener la privacidad, Perry; Clark: y Murdoch, 2015, describen cómo el navegador Tor Browser logra mantener el anonimato de un internauta en la red:

1. Le proporciona al usuario la seguridad de que terceros no puedan acceder a su historial de navegación, con la intención de conocer si la persona ha visitado sitios ilícitos o ha realizado búsquedas prohibidas. Esto se logra porque Tor Browser no guarda registro del historial en el disco duro de la computadora, aunque si es necesario se puede habilitar lo anterior.
2. Se modifica el código fuente del navegador Tor Browser. Así, se evita que un usuario mal intencionado fuerce el sistema operativo de la computadora donde se encuentra

instalado, realice instrucciones arbitrarias que provoquen abandonar la red Tor, y, por lo tanto, se pierdan el anonimato y la privacidad. Se deshabilitan de manera estándar los *plugins*[6] y los complementos[7] del navegador para evitar que se pueda realizar un seguimiento e identificación del usuario mediante el análisis de los paquetes que envía cuando se encuentra navegando en Internet.

3. Se informa al usuario, mediante páginas emergentes, qué aplicaciones externas o de terceros (*plugins*, complementos, ventanas generadas por JavaScript, entre otros), tratan de realizar alguna actividad mientras se navega. Algunos de estos pequeños programas suelen activarse sin la autorización del usuario y pueden recabar datos que serán enviados a desconocidos o, en su caso, perder la conexión con la red Tor.
4. Se genera un directorio privado o aislado donde se descargan los archivos, datos sobre el uso de la red Tor, documentos abiertos recientemente, etc., con el propósito de asegurar que el usuario sea capaz de eliminar, de manera segura y completa, dicho directorio de su computadora y no dejar rastro de que ha utilizado o se ha conectado a la red Tor.
5. Se mantiene el anonimato de los usuario impidiendo que Tor Browser ejecute scripts[8] de java[9], CSS o HMTL5[10], debido a que JavaScript[11] y CSS pueden crear una lista de fuentes que el usuario utiliza en su navegador, obtener la resolución del monitor, el tamaño del mismo, el tamaño de la barra de herramientas, el tamaño de la barra de título tanto del sistema operativo como del navegador. Con JavaScript también es posible obtener información del rendimiento que tienen el navegador y el microprocesador. El HTML5 se desactiva porque al reproducir un video, este lenguaje puede identificar las características de la tarjeta de video instalada.

En ese sentido, el historial de navegación, la información que se recaba mediante los scripts, complementos, CSS o el HTML5 generan una huella digital única (*Fingerprint*) de una persona, con el cual se puede conocer su identidad y ubicar la computadora que utiliza, conocer los sitios que navega, sus preferencias en compras, las redes sociales que visita, etc.

La información recabada, en el mejor de los casos, permite que las empresas reconozcan a los internautas para enviarles propaganda comercial, pero en el peor de los casos, el perfil personal puede ser utilizado por un *hacker* para acceder a la computadora o a los servidores de la empresa donde labora la víctima.

No sólo Tor Project ofrece privacidad para los usuarios de computadoras personales, el programa Orbot, para celulares y *tablets*, también está disponible, aunque sólo para dispositivos con el sistema operativo Android.

Al igual que el Tor Browser, esta aplicación encripta el tráfico de Internet y conecta al usuario a la red Tor siguiendo el mismo esquema anteriormente descrito. Ofrece navegación privada en la red, envío de mensajes privados mediante mensajería instantánea y en Twitter.

Además, Tor Project cuenta con la opción de un sistema operativo portátil (Tails, 2015), el cual es almacenado en una USB, DVD o SD card para ser utilizado en cualquier computadora, lo que permite incrementar la privacidad y el anonimato del usuario al simular que se conecta a la red desde una computadora que no existe físicamente. De esta manera, obliga a que todas las conexiones que se realicen a Internet lo hagan mediante la red Tor, lo que asegura que todas las conexiones y los programas protejan la privacidad del usuario.

Para cerrar el círculo sobre la privacidad de un usuario, Tor Project también encubre las conexiones que se realizan desde una computadora a un *onion router*[12] mediante un

programa llamado *Plugabble Transport* que busca evitar que un tercero pueda identificar las conexiones a la red Tor mediante al análisis de los paquetes[13] enviados en Internet entre dos computadoras. Incluso, en la página de Tor Project se puede descargar un conjunto de librerías para que el usuario interesado pueda desarrollar programas que interactúen con esta red, crear fragmentos de código que permitan optimizar o incrementar la privacidad de la misma. También mantienen un observatorio que se encarga de analizar Internet con el fin de detectar la censura, la vigilancia y la manipulación de la red.

Conclusiones

Como se puede ver, el trabajo que se ha realizado para asegurar la privacidad y el anonimato en la Internet ha requerido de mucho esfuerzo y tiempo para el desarrollo de nuevas aplicaciones que abonen a incrementarla. Se ha expuesto lo sencillo que es realizar un seguimiento de las actividades realizadas por un usuario en la Internet, si éste no toma previsiones para que sus conexiones sean seguras.

Se han invertido muchas horas para descubrir las preferencias de los usuarios en la Internet con la finalidad de ofrecerles servicios adecuados a sus necesidades. ¿Qué tan conscientes estamos de la cantidad de información que proporcionamos al dar un clic? No siempre existe un consentimiento explícito, salvo por los contratos que se firman para el uso de una red social o programa, o al aceptar los términos y las condiciones (muy pocas veces revisados). Se debe tomar en cuenta que en estos contratos se especifica el tratamiento que las empresas darán a nuestra información, correos, nombre, las páginas que visitemos o los clics navegar en Internet.

A la par, también se trabaja para identificar a aquellas personas que hacen uso de la red Tor con fines ilícitos: tráfico de personas, armas, drogas, pornografía infantil, entre otras, incluso, las autoridades que persiguen estos delitos la utilizan para encubrir sus investigaciones y poder identificar a los delincuentes.

Para ello, las policías cibernéticas de los países aprovechan la información que el delincuente va dejando mientras navega en Internet, como los perfiles en las redes sociales, los lugares en donde trabaja, las conexiones al GPS que realiza en su teléfono celular, las páginas que visita, el historial de navegación que se obtiene mediante troyanos que se envían al delincuente y que permiten a la policía tener acceso y control de la computadora personal del mismo, así como activar el micrófono o la cámara del equipo. Existe un portafolio[14] que simula una antena de conexión de celulares la cual capta los datos contenidos en éste y puede ser una herramienta más para identificar a delincuentes.

Los delincuentes crean sus propios sitios de internet dentro de la Red Tor y hacen uso de las bondades del proyecto para evitar que la policía pueda identificarlos, por lo que la policía cibernética muchas veces debe trabajar como incógnito, simulando ser un cliente que busca material pornográfico, armas, contratar mercenarios, etcétera.

La tecnología procura mejorar los procesos o la calidad de vida de las personas, sus conexiones a Internet, el *software* o *hardware* con la finalidad de obtener el mayor provecho para mantener contacto, facilitar las relaciones comerciales, los procesos de comunicación o de producción en una empresa y, en caso de cometer actos ilícitos tanto fuera como dentro de la red; estas herramientas facilitan la ubicación de los delincuentes, los usuarios son los principales responsables del uso que le den.

Referencias

Gantz, J. y Reinsel, D. (2010). *The Digital Universe Decade-Are You Ready?* Recuperado el 1 de junio de 2015 de http://www.emc.com/collateral/analyst-reports/idc-digital-universe-are-you-ready.pdf

Hilbert, M. y López, P. (2011). The World's Technological Capacity to Store, Communicate, and Compute Information. *Science Magazine,* núm. 332, pp. 60-65. Recuperado el 20 de mayo de 2105 de http://www.sciencemag.org/content/332/6025/60.full.pdf DOI:10.1126/science.1200970

International Telecommunication Union. (2015). *ICT Facts & Figure. The world in 2015*. Recuperado el 18 de mayo de 2015 de http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf

O'Morain, M., Titov, V. y Wendy Verbuggen, W. (2005). Onion Routing for Anonymous Communications. Recuperado el 19 de mayo de 2015 de http://ntrg.cs.tcd.ie/undergrad/4ba2.05/index.html

Perry, M., Clark, E. y Murdoch, S. (2015). The Design and Implementation of the Tor Browser [DRAFT]. Recuperado el 15 de mayo de 2015 de https://www.torproject.org/projects/torbrowser/design/

Tails. The amnesic incognito live system. (2015). Recuperado el 17 de mayo de 2015 de: https://tails.boum.org/index.en.html

The guardian Project. (s.f.). Recuperado el 17 de mayo de 2015 de https://guardianproject.info/apps/orbot/

Tor: Home. (s.f.). Recuperado el 25 de Julio de 2014, de TOR project: Anonymity Online: https://www.torproject.org/

Tor: Overview. (s.f.). Recuperado de TOR Project: Anonymity Online: https://www.torproject.org/about/overview.html.en

Tor: Pluggable Transports. (s.f). Recuperado el 15 de mayo de 2015, de https://www.torproject.org/docs/pluggable-transports.html.en

[1] José Antonio Amaro López. Licenciado en informática con orientación en sistemas computacionales; maestro en Tecnologías para el Aprendizaje, ambos por la Universidad de Guadalajara. Profesor docente del Departamento de Geografía y Ordenación Territorial del Centro Universitario de Ciencias Sociales y Humanidades de la Universidad de Guadalajara

[2] En la página http://pennystocks.la/internet-in-real-time/ se puede observar la cantidad aproximada de gigabytes que generan los usuarios de la Internet en tiempo real por segundo.

[3] Un zetabyte equivale a un trillón de gigabytes.

[4] Es una organización compuesta por un grupo de voluntarios sin fines de lucro, creada en 1996 por el Laboratorio de Investigación Naval de los Estados Unidos de Norte América, que continúo con su desarrollo dentro de la Electronic Frontier Foundation (EFF), y, a partir de 2004, como Tor Project, cuyo fin es la defensa de la privacidad de los internautas.

[5] Es un programa o conjunto de programas que se agregan al navegador con al finalidad de interactuar con el *software* de una empresa. Funcionan en cualquier navegador.

[6] Solo se permite el uso restringido de *plugins* de Flash y de Gnash. Gnash es un reproductor libre (Open GNU), de archivos de flash (.swf) para navegadores.

[7] Es un programa o conjunto de programas diseñados para un navegador en particular y que permiten mejorar la experiencia del usuario al conectarse a la Internet.

[8] El usuario puede configurar si desea que se ejecuten los *script* o complementos que requiera.

[9] En la dirección http://w2spconf.com/2011/papers/jspriv.pdf se puede encontrar un ejemplo de como se utiliza JavaScript para identificar a un usuario mediante la huella digital (*fingerprint*) que va dejando en la red.

[10] Nuevo estándar para la creación de páginas web.

[11] Lenguaje de programación para la creación de páginas web.

[12] Equipo que revisa, encripta y envía los mensajes a través de la red Tor.
[13] Un paquete es la cantidad mínima de información que se envía a través de Internet y que identifica a la persona que lo envió, al destinatario y el contenido.
[14] Un ejemplo, a grandes rasgos, de la vigilancia de celulares: prodigy.msn.com/es-mx/noticias/video/cómo-funciona-la-vigilancia-de-celulares/vi-AAcLkiH?refvid=CCSXK