Funcionamiento de una Red Anonimizadora: La red Tor

Publicado en: SG #56 (/REVISTA/56)

PROGRAMAR ES UN ESTILO DE VIDA (/SECCI%C3%B3N-REVISTA/PROGRAMAR-ES-UN-ESTILO-VIDA)

Autor: Gunnar Wolf (/buzz/autores/gunnar-wolf)

(http (http (http (http
/inte /sha /sha /sub

Ha pasado medio año desde que nos encontramos en la última columna, en el número 55 de Software Gurú. En dicha columna abordé algunos argumentos importantes relativos al tipo de vigilancia al cual estamos sometidos, tanto por gobiernos como por empresas particulares. Dejé varias ideas inconclusas, apuntando a que retomaría el tema.

Y, en efecto, hay mucho que retomar. Muchas cosas han ocurrido en los últimos meses, y hasta parecería que algunas de ellas se apresuraron a ocurrir en los días previos a la escritura de esta columna, para asegurarse que no se me olviden.

La columna anterior llevó como pieza central una cita del pensamiento de John Perry Barlow, uno de los soñadores que en primer término imaginó, y poco a poco ayudó a conformar y, como fundador de la Electronic Frontier Foundation, defender un conjunto de reglas de la interacción en línea cementadas en el respeto a las libertades individuales. Hay que subrayarlo — La fundación misma de la EFF, en 1990, resulta por sí misma tremendamente visionaria. El pasado 7 de febrero, después de una larga y muy interesante vida, Barlow falleció. Nos toca continuar imaginando y luchando por un ciberespacio libre, un espacio para la invención y el desarrollo de la humanidad.

Cerramos la columna anterior mencionando el arresto de Dmitry Bogatov, joven profesor de matemáticas y desarrollador de software libre en Rusia, por causas relacionadas con la operación

de un nodo de salida de la red Tor, actividad que, de propio, no es ilegal en Rusia. Bogatov pasó arrestado diez meses. El 31 de enero fue puesto nuevamente en libertad parcial (con restricciones de movilidad fuera de su región). Desafortunadamente, esto no significa que el sistema judicial ruso comprendió la naturaleza de la red Tor. Menos de dos semanas más tarde, otro operador de un nodo de salida Tor, Dmitry Klepikov, fue arrestado. La movilización en medios y la presión internacional logradas tras el caso de Bogatov afortunadamente lograron que Klepikov fuera liberado 48 horas más tarde.

El tercer punto a recapitular es probablemente de mucho menor importancia en el gran esquema de las cosas, pero no puedo pasarlo por alto: Mencioné que estaba comenzando con los preparativos de un proyecto que me llevaría a profundizar más acerca de la privacidad y el anonimato. Me da mucho gusto reportarles que, en efecto, DGAPA-UNAM aceptó mi proyecto PE102718, con lo cual me comprometo a desarrollar por dos años los temas que en esta columna comienzo a arañar.

¿Cómo funciona la anonimización?

El principio básico bajo el cual opera Tor, la principal red de anonimización en Internet, es sencillo; fue presentado ya en 1981 por David Chaum, y si bien Tor es la más importante, hay varias otras redes construidas sobre este mismo fundamento.

Un conjunto de usuarios normales de Internet configuran sus computadoras como nodos de una red superpuesta. El anonimato que esta red pueda brindar depende, necesariamente, de que la cantidad de nodos sea suficiente para esconder al tráfico de un individuo entre la multitud de usuarios de esta red.

Cuando un usuario de Tor desea conectarse a la red, contacta como primer paso a los servidores de directorio, que le proveen un listado de nodos activos. De éstos nodos, el cliente de Tor elige a tres para el establecimiento de un circuito: Un nodo «guardia» (de entrada), un nodo intermedio, y un nodo de salida.

El cliente Tor tiene varios mecanismos locales para recibir la comunicación de programas variados — Puede ser un navegador cualquiera (si bien recomiendan fuertemente el uso de Tor Browser [1], pero también puede ser casi cualquier programa que se comunique sobre TCP/IP. Lo más frecuente es crear un túnel para la comunicación sobre Tor empleándolo como un Proxy SOCKS.

El cliente cifra a cada uno de los paquetes para su comunicación tres veces, con las llaves públicas de los tres nodos elegidos: Al nivel más interno, con la del nodo de salida; el resultante de esa operación, con la del nodo intermedio, y por último, lo hace con la del nodo guardia.

Cada uno de los paquetes que conforma determinada comunicación es entregado al nodo guardia. Éste sabe su ubicación en el circuito, por lo que podría revelar la identidad del usuario, pero desconoce el tráfico que está reenviando, sólo sabe que debe entregarlo a determinado nodo intermedio. El nodo intermedio no sabe nada respecto a la comunicación, únicamente la

dirección de sus dos compañeros. Por último, el nodo de salida sabe a qué IP destino se dirige la conexión, y en caso de no estar ésta cifrada (por ejemplo, empleando HTTPS en vez de HTTP — ies importante preferir HTTPS incluso sobre redes anonimizadoras! [2]), puede conocer el contenido de la comunicación, pero no la dirección de donde ésta se originó.

A modo de ejemplo, la figura 1 presenta una captura de pantalla de mi visita a la página de Software Gurú: el servidor registró una visita proveniente de la IP alemana 94.130.183.184; dicha IP, del nodo fallbacksen, provino de nullstreet en Canadá, y ésta de Fission3 en Francia. Claro, esta conexión se originó en mi computadora de escritorio, en la ciudad de México. Naturalmente, esto tiene como efecto un fuerte aumento en la latencia. Si bien una medición seria tendría que hacerse entre cada uno de dichos puntos, estimando la latencia desde mi computadora en México suma unos 450 milisegundos a cada conexión.

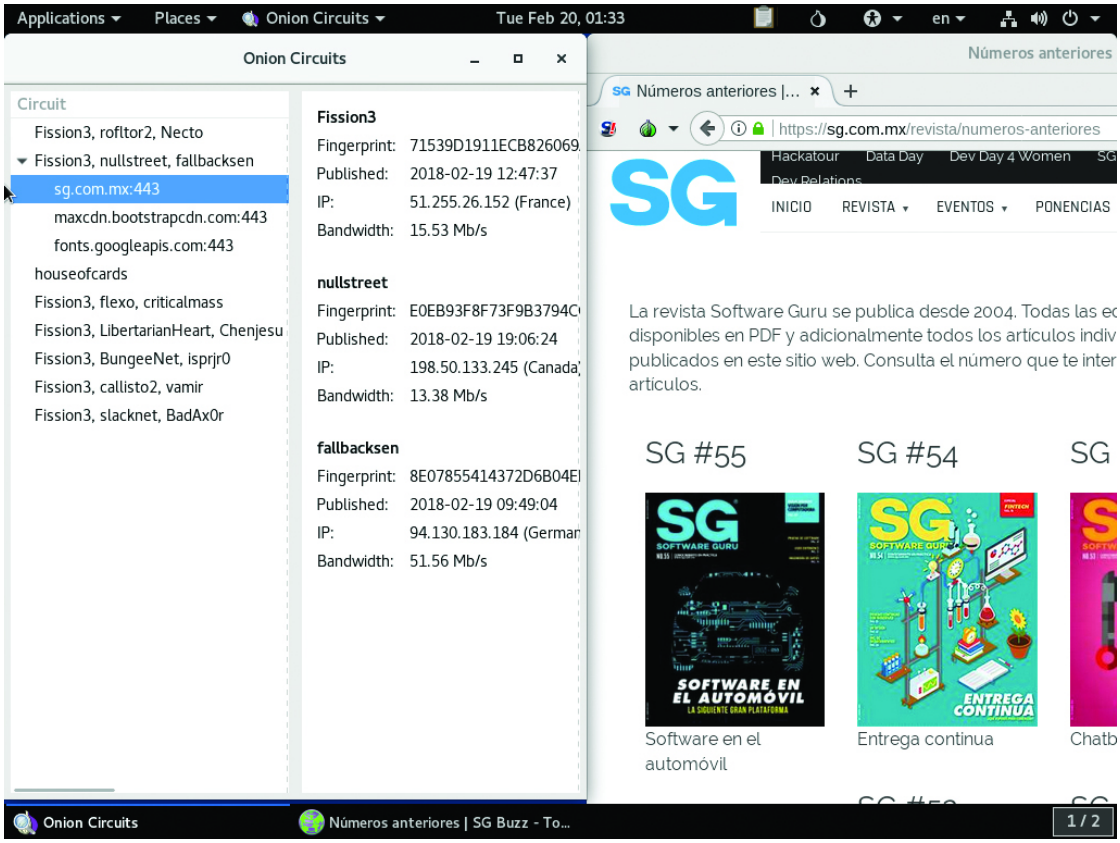

Figura 1. Navegación anonimizada con Tor

A quienes acostumbran trabajar con redes de cómputo, puede resultarles chocante mi reiterado uso del término “circuitos”. ¿Qué no acaso las redes de cómputo nos liberaron de los circuitos, que se establecían en las viejas redes telefónicas punto a punto, resultando en una arquitectura más frágil y de menor rendimiento que nuestras actuales redes basadas en paquetes?

La red Tor hace esto para reducir la varianza en las comunicaciones y lograr una red de relativamente baja latencia, comparada con las verdaderas redes anonimizadoras basadas en

paquetes. Al establecer cada circuito una sola vez, éste se mantiene estable a lo largo de una serie de conexiones IP relacionadas, evitando el costo de establecimiento de canal seguro paquete por paquete. Además, permiten que, a lo largo de una misma sesión, todas las conexiones de determinado usuario que llegan a cierto servidor parezcan originarse en el mismo punto — De no ser así, muchos sistemas rechazarían a dicha sesión.

La forma en que se eligen los nodos que atravesamos no es aleatoria; los circuitos construidos buscan evitar tocar puntos que compartan estructura general de ruteo (sistemas autónomos).

¿Qué sigue? El componente social

En la columna anterior presenté una argumentación general y, hasta cierto punto, anclada en mis vivencias personales respecto al avance del anonimato en línea a lo largo de los últimos 20 años. Esta columna presenta, muy a grandes rasgos, el funcionamiento de Tor, la principal red de anonimato. Pero queda pendiente un importante punto — El social. ¿Por qué fomentar redes de anonimato? ¿Qué casos de uso se encuentran en ellas que puedan ameritar dedicarle recursos y tiempo? Y, es más, ya que mencionamos los recursos: ¿Como puedo invitarlos a participar en ellas?

Abordaré dichos puntos en la próxima entrega de esta misma columna. ¡Hasta entonces!

Anotaciones

[1] El navegador Tor está basado en Firefox. Puedes leer más respecto a los fundamentos de diseño y los puntos particulares en que se diferencia en https://www.torproject.org/projects/torbrowser/design/ (https://www.torproject.org/projects/torbrowser/design/)

[2] En https://www.eff.org/pages/tor-and-https (https://www.eff.org/pages/tor-and-https) encontrarás un simple y claro diagrama interactivo que explica qué porción de nuestra información es protegida por HTTPS, qué porción es protegida por Tor, y por qué hay que usarlos a ambos cuando estos temas nos importan.

Log in (/user/login)

OPORTUNIDADES DE EMPLEO

- ARQUITECTO JAVA (https://sgtalento.com/content/arquitecto-java-0)
- Digital Designer (with Web Design) (https://sgtalento.com/content/digital-designer-web-design)
- Consultor BI-HANA (https://sgtalento.com/content/consultor-bi-hana)
- Consultor SAP PP (https://sgtalento.com/content/consultor-sap-pp)
- Consultor SAP MM (https://sgtalento.com/content/consultor-sap-mm)
- Administrador General (https://sgtalento.com/content/administrador-general)
- iOS Developer (https://sgtalento.com/content/ios-developer-5)
- Copywriter (https://sgtalento.com/content/copywriter)
- Practicante de CX (https://sgtalento.com/content/practicante-de-cx)
- Security Engineer (https://sgtalento.com/content/security-engineer-2)

RECOMENDAMOS

Software Guru es el medio preferido por las personas de habla hispana interesadas en construir software de alto desempeño.

> *Conocimiento para construir software grandioso.*

Más servicios de SG

Hackatour (https://sg.com.mx/hackatour)
Data Day (https://sg.com.mx/dataday)
Dev Day 4 Women (https://devday4w.com)
SG Virtual (https://sg.com.mx/sgvirtual)
SG Talento (https://sgtalento.com)
SG Campus (https://sgcampus.com.mx)
Dev Relations (https://devrel.sg.com.mx)

(http (http (http (http (http (mail