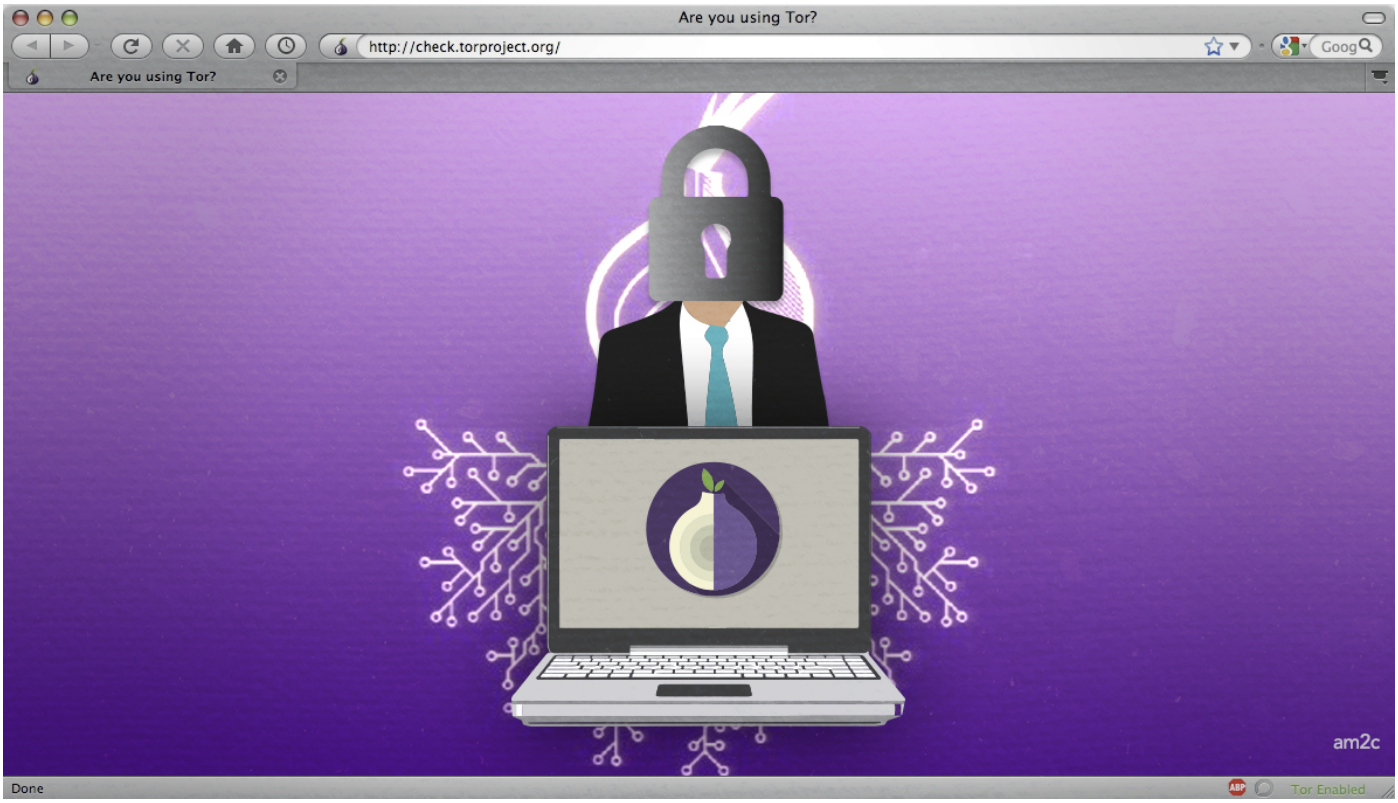
.Seguridad
Cultura de prevención para TI
Published on *Revista .Seguridad* (http://revista.seguridad.unam.mx)

LA RED TOR COMO ELEMENTO DE PRIVACIDAD EN NUESTRAS VIDAS

Marco Antonio Ruano Muñoz

numero-30



Con el incremento de servicios en la nube, el abaratamiento de dispositivos tecnológicos y la reducción de su tamaño, se ha elevado de forma abrumadora la facilidad para conectarse a Internet y realizar tareas cotidianas, permitiendo comunicarse con personas al otro lado del planeta en instantes, realizar

operaciones bancarias sin necesidad de hacer una fila, enviar importantes correos con información sensible o hacer las compras del supermercado desde el hogar. Sin embargo, cuando una persona aprende a utilizar una de estas plataformas no recibe un curso enfocado a la seguridad y protección de su información, por tanto, es de suma importancia considerar aspectos como la privacidad y el anonimato a la hora de sumergirnos en la red.

EL NAVEGADOR TOR

Tor es una herramienta utilizada en todo el mundo por características que la hacen particularmente atractiva para aquellas personas que deseen “enmascarar” su actividad en línea, así como acceder a ciertas áreas que no se encuentran indexadas por la mayoría de los motores de búsqueda.

Típicamente, la red en la que navega un usuario consiste en una arquitectura cliente-servidor, la cual permite que el cliente (el navegador utilizado por una persona) haga una petición a un servidor solicitando cierta información, como puede ser una página web, una imagen, video, etcétera, y el servidor devolverá una respuesta por medio del protocolo HTTP con el resultado, siendo este visualizado en el navegador.

La red Tor (The Onion Routing) funciona de forma análoga. Sin embargo, la gran diferencia radica en que esta es una red distribuida, es decir, está compuesta por varios nodos además del cliente y el servidor con el que desea comunicarse. Estos nodos conformados por voluntarios que aportan una porción de su ancho de banda para permitir el funcionamiento brindan la posibilidad de navegar por Internet de forma anónima, ya que cuando un usuario envía datos para establecer una comunicación, esta información es cifrada con 3 llaves distintas, de modo que el primer nodo únicamente es capaz de descifrar una de estas llaves para reenviar la información al segundo nodo, que a su vez removerá una “capa” más del cifrado y de nuevo trasladará el contenido al último nodo (nodo de salida), el cual descifra la última llave y redirige la petición hacia el servidor objetivo.

Cada uno de estos nodos cuenta con la localización de los puntos más cercanos, es decir, de donde viene la información y a donde se dirige, y este camino que se recorre se configura de forma aleatoria constantemente, lo cual dificulta el análisis de tráfico proveniente hacia algún usuario.

Este proyecto de software libre, entre algunas otras funcionalidades desarrolladas, cuenta con un navegador listo para trabajar con esta red, el cual trabaja con el protocolo HTTPS que asegura la comunicación de principio a fin. Sin embargo, vale la pena mencionar que Tor no cuenta con cifrado de extremo a extremo, por lo que, si no se usa HTTPS, el nodo de salida es un punto vulnerable en el cual se puede perder el anonimato deseado.

En la figura 1 podemos observar el funcionamiento de la red Tor y el uso de HTTPS, en donde un usuario intenta acceder a un sitio, ingresando sus credenciales para autenticarse, y enviando cierta información, así como su localización gracias a la dirección IP. Suponiendo que alguna persona o incluso el proveedor de servicios de Internet (ISP en el recuadro rojo, que se encarga de proveer a personas y compañías la posibilidad de conectarse a Internet) monitorea el tráfico proveniente de la red

del usuario, únicamente podrán revelar su localización. Para hacerlo requieren de ciertos permisos y procesos legales interpretados por abogados (icono rosa en la figura 1) y autoridades (icono azul). El primer nodo de Tor solo sabe de dónde proviene la información, pero no tiene acceso a esta, ni sabe cuál es el destino; el segundo nodo no cuenta con información alguna de la petición, y solo el nodo de salida conocerá el sitio al que se intenta acceder. Mientras que, del lado del servidor (interpretado en el recuadro negro), al recibir los datos no tendrá conocimiento de dónde proviene la petición gracias al funcionamiento de la red.

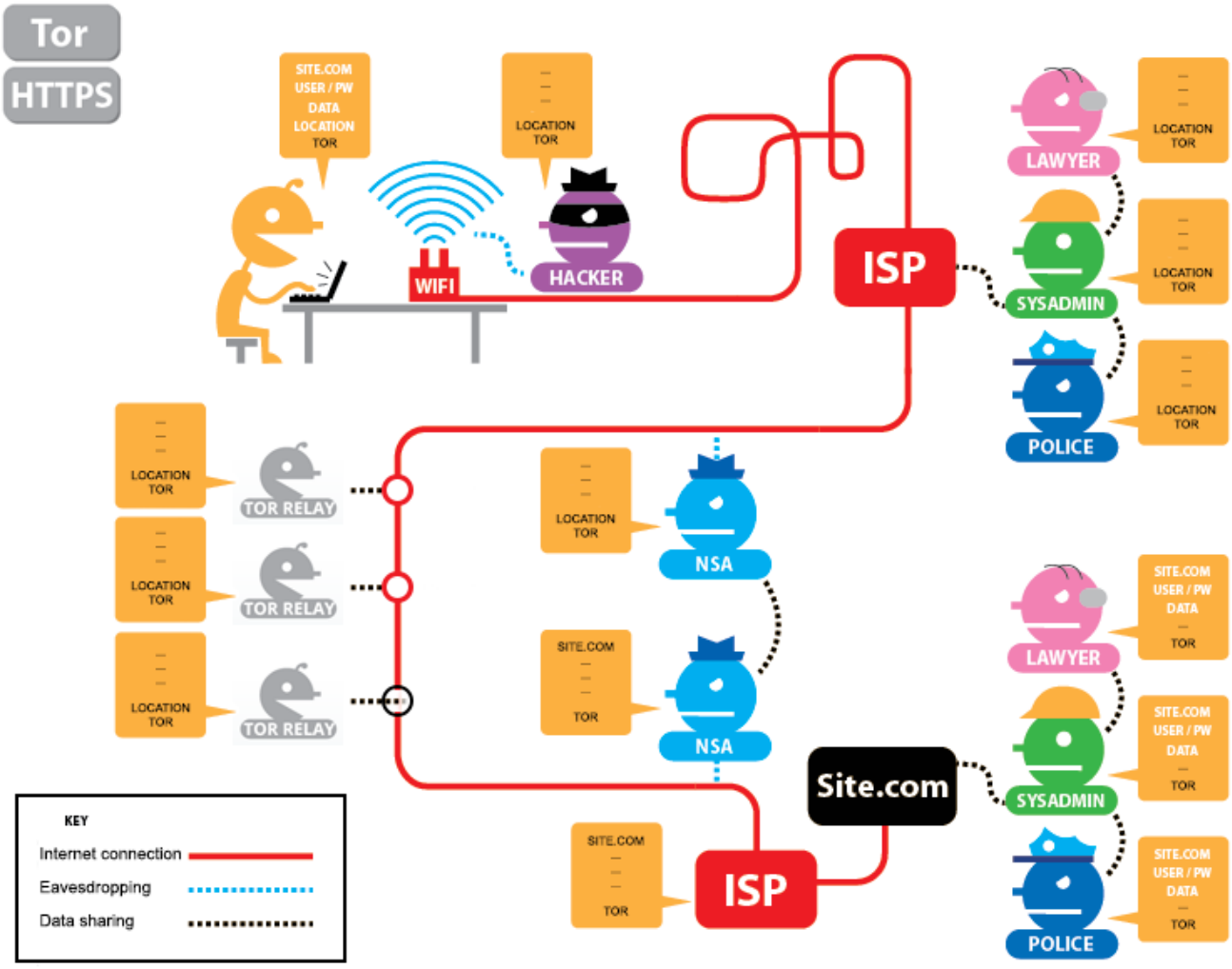


Figura 1. Cómo funciona la red Tor

Por otro lado, resulta contraproducente acceder a sitios que solicitan al usuario ingresar cierta información para identificarse, como su nombre, correo electrónico, números de tarjetas bancarias, etcétera, y se perderá la dosis de anonimidad buscada.

Podemos también observar las figuras en azul que representan a organizaciones de seguridad nacional, típicamente agencias del gobierno, las cuales monitorean este tipo de infraestructura de forma periódica, debido al gran número de actividades criminales que se llevan a cabo a costa del

anonimato que da la red.

Este esquema realizado por la Electronic Frontier Foundation, organización sin fines de lucro y cuyo objetivo es defender la libertad de expresión en el mundo digital, pretende mostrar que Tor por su cuenta no es perfecto, y solo garantiza anonimidad cuando se utiliza HTTPS.

A diferencia de otros navegadores que cuentan con una configuración predeterminada que permite la recolección y envío de cierta información sobre el usuario y su actividad (a menos que sean desactivadas dichas características manualmente cuando es posible), el navegador Tor promueve su uso advirtiendo sobre ciertos hábitos que se suelen arraigar, los cuales pueden ser inconvenientes para el objetivo esperado de la red, por ejemplo: compartir archivos mediante Torrent, instalar o activar *plugins* en el navegador, no usar el protocolo HTTPS en sitios web, o abrir documentos descargados por medio de la red Tor mientras se encuentre en línea, por mencionar algunos.

Incluso, ya hay disponible una versión para móviles con sistema operativo Android, y no es para menos, ya que “los dispositivos móviles se utilizan más que las computadoras tradicionales para búsquedas en la Web” (Gibbs, 2016). Esta herramienta llamada Orbot, permite utilizar un proxy local inmerso en la red Tor, y también brinda la habilidad de cifrar la información saliente del *smartphone* o *tablet* e incluso de otras aplicaciones instaladas compatibles.

Por supuesto al pasar la información por una serie de nodos en una red distribuida, es claro que la velocidad no será la misma que al navegar por Internet de forma tradicional, ya que en vez de seguir una ruta directa el tráfico se tiene que desviar hacia los nodos intermediarios, por lo que no es recomendable para algunas tareas cuya eficiencia dependa de la velocidad, como el *streaming*.

Otra desventaja es que algunos proveedores de Internet bloquean nodos de la red Tor, debido a la presión que ejercen los gobiernos de algunos países, por ejemplo, China y Rusia, quienes no están de acuerdo con su uso, debido a la complejidad que implica para sus organizaciones de inteligencia al monitorear a usuarios que pueden hacer uso de la red para actividades delictivas. Este hecho puede dificultar conectarse a ciertos sitios al estar conectado a la red.

Afortunadamente, hay nodos distribuidos por muchos países que no cuentan con este tipo de políticas, ya que su uso no representa ningún tipo de problema, siempre y cuando no se realicen actividades ilegales.

CONCLUSIÓN

Claramente, si una herramienta resulta benéfica para incrementar el nivel de privacidad en línea, la combinación con otras más, como el sistema operativo Tails, servicios de mensajería como Tor Messenger, el uso de redes virtuales privadas (VPN), entre otras, puede ofrecer una solución que, sumada con un uso correcto, responsable y seguro, significará un buen escudo para proteger la información de cada persona.

Sin embargo, la red Tor no solo consiste únicamente en un medio para mantener las comunicaciones privadas, sino también funge como un acto de colaboración entre personas en muchos países que están dispuestos a ceder una porción de su ancho de banda para mantener esta red activa y que todos puedan ser partícipes de ella.

¿Cómo se puede colaborar? Una forma de fortalecer la red es aumentar el número de nodos, es decir ser partícipe de la misma, ya que, a mayor número de nodos, incrementará la disponibilidad de conexiones posible y la secuencia de los tres posibles nodos a seleccionar para una conexión resultará más cambiante, añadiendo complejidad a un posible análisis estadístico que permita conocer información sobre un usuario.

REFERENCIAS

- Caddy, B. (2017). Google tracks everything you do: here's how to delete it. Recuperado el 28 de julio de 2017, de http://www.wired.co.uk/article/google-history-search-tracking-data-how-to-delete
- Electronic Frontier Foundation. (s/f). How HTTPS and Tor Work Together to Protect Your Anonymity and Privacy. Recuperado el 28 de julio de 2017, de https://www.eff.org/pages/tor-and-https
- Gibbs, S. (2016). Mobile web browsing overtakes desktop for the first time. Recuperado el 28 de julio de 2017, de https://www.theguardian.com/technology/2016/nov/02/mobile-web-browsing-desktop-smartphones-tablets
- How HTTPS and Tor Work together to Protect Your Anonymity and Privacy. (2017). Recuperado el 28 de julio de 2017, de https://www.eff.org/es/pages/tor-and-https
- Orbot: Tor for Andorid. (2017). Recuperado el 28 de julio de 2017, de https://www.torproject.org/docs/android.html.en
- TOR Download. (2017). Want Tor to really work? Recuperado el 28 de julio de 2017, de https://www.torproject.org/download/download-easy.html.en#warning

Este artículo se desarrolla vinculado con el proyecto PE102718 PAPIME/DGAPA/UNAM.

SI QUIERES SABER MÁS, CONSULTA:

- Mitos y realidades de la Internet profunda.
- El cifrado web (SSL/TLS)
- Ningún navegador es seguro
