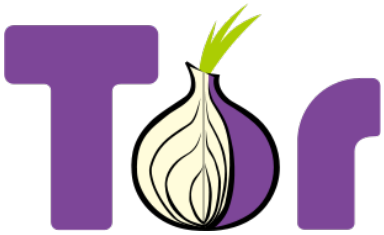
TOR
The Onion Router

Stefano Pezzino
spezzino.13@gmail.com

Universidad Católica "Nuestra Señora de la Asunción",
Facultad de Ciencias y Tecnología
Departamento de Electrónica e Informática
http://www.uca.edu.py



Resumen Tor es un software gratuito que posibilita la navegación anónima en internet. Funciona dirigiendo el tráfico de internet a una colección de nodos mundial mantenida por los propios usuarios de TOR que oculta la identidad, localización y uso de la conexión de cualquier auditoria de tráfico o monitoreo de red.

Key words: TOR, The Onion Router, Navegación anónima, Privacidad, Deep Web, Deepnet.

1. Introducción

Tor (abreviatura de The Onion Router en inglés) es una red de comunicación virtual que permite a los usuarios mejorar la privacidad y seguridad en internet.

Tor es un proyecto que desarrolla una red de comunicaciones distribuida de baja latencia, que funciona como una capa superior de internet, en la que el intercambio de mensajes entre los usuarios no revela su identidad ni dirección IP del dispositivo que están utilizando para realizar dicho intercambio. Además mantiene la integridad y confidencialidad de los mensajes que circulan a través de la red Tor ya que posee un mecanismo de encriptación muy sofisticado, impidiendo que un mensaje interceptado en el camino pueda ser entendido.

Un mensaje es encriptado múltiples veces antes de ser enviado a través de la red. Cada nodo intermedio puede desencriptar sólo una capa, revelando apenas

la dirección del siguiente nodo al cual debe ir el mensaje, de esta forma se logra la privacidad del mensaje. Cuando el mensaje llega al nodo de salida, se revela el contenido del mensaje y su destinatario final.

Entre los objetivos de diseño de la red Tor se encuentran el despliegue, la usabilidad, la flexibilidad y el diseño simple[1].

Otro concepto relacionado a Tor es *Deep Web*, o la internet oculta, que es el contenido web que no esta en la superficie. El contenido de la superficie corresponde a las páginas que pueden ser indexadas por los motores de búsqueda y contienen enlaces a otro sitios. En cambio, en la *Deep Web* se encuentran sitios que no contienen enlaces a otros sitios ni tienen enlaces provenientes de otros, además no pueden ser indexados por los motores de búsqueda. La única manera de acceder a la *Deep Web* es saber la url del sitio que se desea visitar[2].

Se calcula que la *Deep Web* es actualmente 400 a 500 veces mas grande que la *Surface Web*, contiene 7500 terabytes de información y 550 billones de documentos comparado con 19 terabytes y un billón de documentos que son propios de la *Surface Web*[3].

Despliegue: el diseño debe ser barato, fácil de implementar en el mundo real y requerir pocos recursos (por ejemplo ancho de banda). El propietario del nodo no debe ser totalmente responsable del contenido que circula por dicho nodo.

Usabilidad: la usabilidad es un requerimiento para garantizar la seguridad, porque un sistema difícil de usar va a tener pocos usuarios; y como un sistema anónimo oculta a los usuarios con otros usuarios, menos usuarios significa menos anonimidad. Además, no debe requerir la modificación de las aplicaciones, no introducir retrasos en la comunicación, presentar pocas opciones de configuración y soportar todos los sistemas operativos.

Flexibilidad: el protocolo debe ser especificado detalladamente, para permitir que sirva de base para investigaciones futuras, permitiendo la evolución del proyecto.

Diseño simple: el diseño del protocolo y los parámetros de seguridad deben ser fácilmente entendibles. Tor apunta a desplegar sistemas simples y estables que integren las mejores herramientas que protejan el anonimato.

1.1. Historia

Los orígenes de Tor se remontan a 1995 cuando se inician los trabajos de investigación sobre enrutamiento por capas (Onion Routing) en la Oficina de Investigación Naval de la Marina de los Estados Unidos. La motivación principal fue la de proteger las comunicaciones del gobierno. A esta versión se le conoce como generación cero de Onion Router y fue desarrollada por Michael Reed, Paul Syverson y David Goldschlag[4].

En 1996 se adopta el protocolo Diffie-Hellman para intercambiar claves de encriptación entre los nodos y lograr el secreto perfecto hacia adelante, es decir, que el descubrimiento de claves actuales no compromete la seguridad de las claves utilizadas con anterioridad[5]. También se presenta una prueba de concepto y

prototipo funcionando sobre Solaris y una red de cinco nodos con proxies para la navegación web.

En 1997, el proyecto consigue financiamiento de la Agencia de Investigación de Proyectos Avanzados de Defensa (DARPA) bajo el programa de Redes de Alta Confidencialidad. Se publica además, el diseño de Onion Routing para el uso de celulares desde localizaciones ocultas y para el control de la información de localización de otros dispositivos que realizan seguimiento. En el Simposio de Seguridad y Privacidad de la IEEE se publica el diseño de la primera generación de Onion Routing, que incluye mejoras como el número de rutas variable, la separación del proxy de navegación del router, introducción de políticas de seguridad para los nodos de salida, módulo de criptografía separado de la aplicación, permitiendo que el mismo se ejecute en hardware especializado, entre otras mejoras.

En 1999 el desarrollo de Onion Routing es suspendido debido a la falta de fondos y a que los desarrolladores abandonaron el Laboratorio de Investigación.

En 2001 se reactiva el desarrollo gracias a los fondos de DARPA, esta vez bajo el programa de Redes Tolerantes a Fallas, con el objetivo de completar el código de la primera generación lo suficiente como para levantar una red de prueba y además agregar tolerancia a fallos y manejo de recursos.

En 2002 se abandona el código de la primera generación por ser antiguo. Se inicia el desarrollo de la segunda generación bajo la dirección de Roger Dingledine, Nick Mathewson y Paul Syverson.

En 2003, se aportan fondos desde la Oficina de Investigación Naval para el desarrollo y la implementación de la segunda generación, desde DARPA para implementar manejo de recursos y tolerancia a fallos y desde el Laboratorio de Investigación Naval para la construcción de servidores ocultos. En octubre la red Tor es desplegada y el código fuente se libera bajo licencia MIT.

En 2004 se implementan los servicios ocultos. El proyecto pasa a ser financiado por la Electronic Frontier Foundation (EFF)

Actualmente, el proyecto es manejado por Tor Project, una organización sin fines de lucro y dirigido por Roger Dingledine[6].

2. Como funciona TOR

Tor distribuye la comunicación sobre varios lugares en internet, tal que en ningún punto pueda accederse a la ubicación real del usuario que utiliza la red. En lugar de elegir un camino directo desde el origen al destino, los paquetes que circulan dentro de la red Tor toman caminos aleatorios a través de varios relays que cubren el camino seguido de tal manera que ningún observador en ningún punto pueda determinar el origen o destino del paquete.

Primero se obtiene una lista de nodos activos desde un servidor de directorio (Fig. 1). Con esa información se prepara el camino.

Para crear un camino dentro de Tor, el cliente crea de forma incremental circuitos encriptados de conexión con varios relays en la red. El circuito es extendido un nodo a la vez, y cada nodo solo sabe cuál nodo le transmitió el

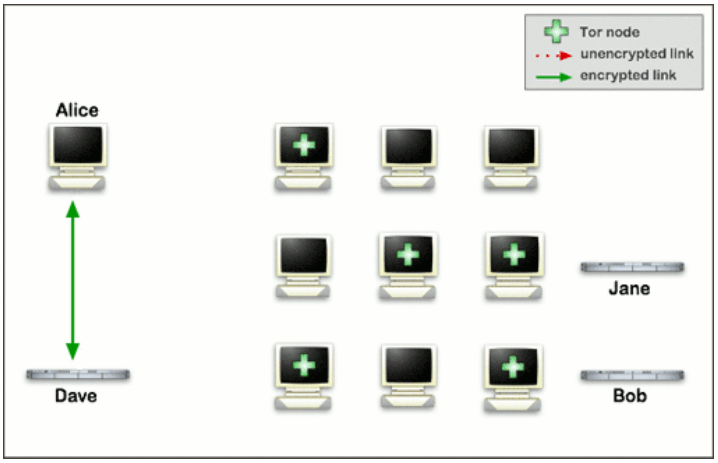


Figura 1. El cliente Tor de Alice obtiene una lista de nodos Tor de un servidor de directorio.

paquete y a cual debe transmitir (Fig. 2). Ningún nodo en particular sabe el recorrido completo que el paquete debe atravesar. El cliente produce un par de claves pública/privada para encriptar los datos con cada nodo que forma parte del camino, para que sea imposible a otro nodo rastrear la conexión mientras esta pasa por la red.

Cuando un circuito ha sido establecido, se pueden transferir distintos tipos de datos, y diferentes tipos de aplicaciones pueden utilizar la red Tor. Como cada relay no sabe más que la dirección del siguiente nodo, no existe forma que alguien o incluso un nodo comprometido pueda examinar el tráfico que esta pasando por ese punto, ni siquiera puede saber el origen o el destino de la conexión.

Cabe destacar que Tor solo funciona sobre TCP (Transmission Control Protocol), ésto es debido a como se construye el circuito, y como se maneja el mismo. Sería imposible determinar con anticipación por donde se dirigirán los paquetes para poder negociar las claves de encriptación con esos nodos, así mantener segura la comunicación.

Tor mantiene el circuito abierto durante los siguientes diez minutos luego de su creación, por motivos de eficiencia. Transcurrido ese tiempo, se crea un circuito nuevo (Fig. 3) para prevenir el rastreo de paquetes puedan determinar que los mismos vienen de una misma conexión[7].

2.1. Elementos de la red

Tal como se observa en la Fig. 4, los elementos que forman la red Tor son los siguientes:

Nodo de entrada: Es el primer nodo del circuito y sirve como entrada de los datos a la red Tor. El cliente Tor se comunica únicamente con este nodo para enviar contenido a través de la red.

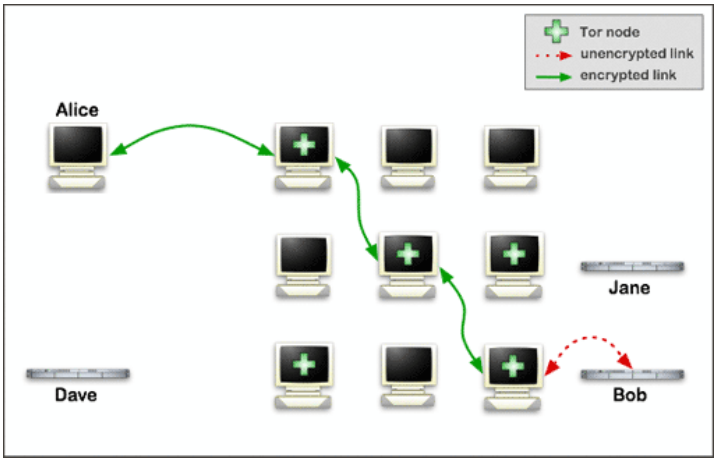


Figura 2. El cliente Tor de Alice elige un camino aleatorio hasta el servidor de destino.

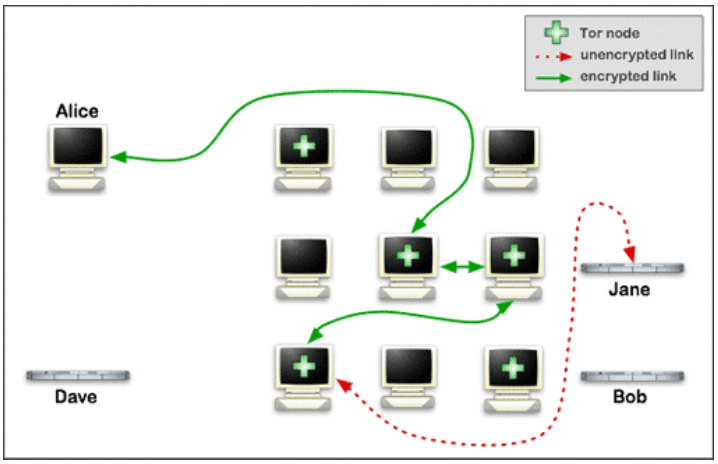


Figura 3. Cuando el usuario visita otro sitio, el cliente Tor de Alice elige un nuevo camino aleatorio.

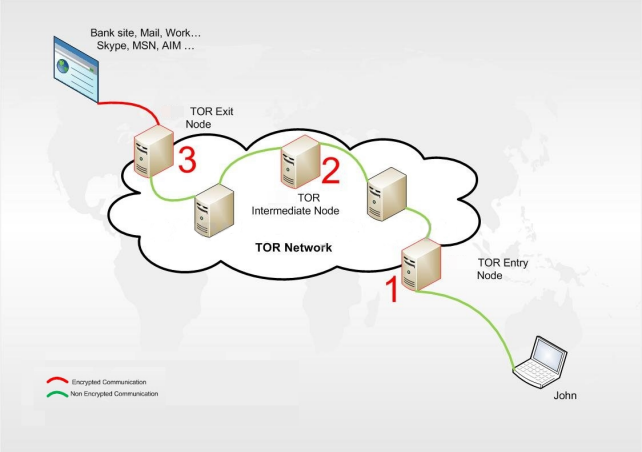


Figura 4. Vista de los elementos de la red Tor.

Nodos intermedios o relay: Es el subconjunto de nodos Tor por los cuales pasa el mensaje dentro de la red. El circuito corresponde al nodo de entrara, el nodo de salida y todos los nodos intermedios.

Nodo de salida: Corresponde al último nodo en el circuito y es el que finalmente desencripta el mensaje para revelar su contenido y el destinatario final. Para el servidor que recibe el mensaje, le parecerá que éste nodo es el que está comunicando realmente, protegiendo así la identidad del emisor original.

2.2. Enrutamiento por capas

La idea del enrutamiento por capas (Onion Routing) el proteger la privacidad del emisor del mensaje, a la vez que se protege el contenido del mismo mientras atraviesa la red (ver Fig. 5).

El concepto de Onion Routing o enrutamiento por capas viene dado por la representación de las capas de la cebolla (onion). Cada nodo o router se encarga de remover una capa de la cebolla, revelando así la dirección del siguiente nodo que debe recibir el mensaje. Cada nodo siguiente a su vez remueve una capa hasta que se obtiene el mensaje original.

Onion Routing utiliza el principio de Chaum: *mix cascades*. Según este principio, los mensajes que viajan desde el origen hasta el destino a través de una secuencia de nodos que reenvían el mensaje de forma impredecible[8].

Para prevenir que el contenido del mensaje sea leído por un atacante que está interviniendo la conexión, los mensajes son encriptados entre los routers. La principal ventaja del enrutamiento por capas, es que no es necesario confiar en cada router. Si algún router está comprometido, la comunicación anónima aún es posible debido a que cada router dentro de la red Tor acepta un mensaje, vuelve a encriptar y transmite al siguiente router. Si el atacante controla todos

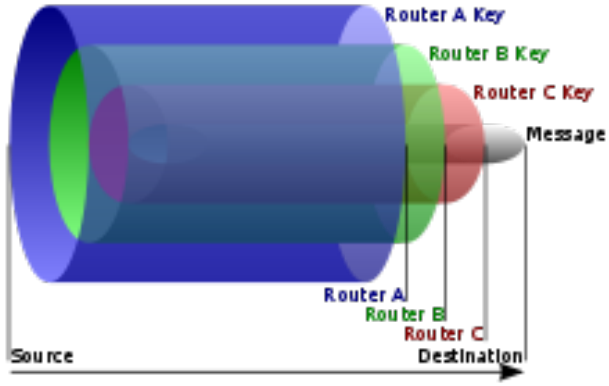


Figura 5. Capas de encriptación.

los routers puede rastrear el camino de un mensaje dentro de la red, pero no puede determinar si solo controla un router dentro de la red[4].

2.3. Servicios ocultos

Tor posee un mecanismo que permite a sus usuarios publicar servicios dentro de la red TOR, protegiendo sus identidades. Los servidores que son configurados para recibir conexiones entrantes solo desde la red Tor son llamados servicios ocultos. En lugar de revelar la dirección IP, un servicio oculto es accedido a través de su dirección onion. Tor entiende estas direcciones y puede encaminar los datos desde y hacia servicios ocultos, siempre protegiendo la anonimidad de ambas partes (el servidor y el cliente).

Algunos servicios ocultos relevantes que posee Tor:

TorMail: un servicio de correo electrónico anónimo.
Wikileaks: una copia del sitio WikiLeaks.
Deepsearch: un buscador de sitios .onion.
Fenergy: un servidor de archivos anónimo.
Silk Road, Atlantis, Black Market Reloaded sitios donde se puede comprar drogas y material ilegal de todo tipo.

2.4. .onion

.onion es un pseudo dominio de primer nivel, solo alcanzable desde la red Tor. Se utiliza para dotar de puntos de entrada a servicios ocultos anónimos. Estas direcciones no son nombres reales de DNS y el dominio .onion no existe en el servidor DNS raíz de internet, pueden ser accedidos mediante proxies apropiados o utilizando Tor Browser Bundle.

El propósito de este sistema es hacer que tanto el proveedor de la información como el cliente que accede a ella sean difíciles de rastrear, ya sea por una red intermediaria o desde afuera de Tor.

Las direcciones .onion contienen 16 caracteres alfanuméricos (Fig. 6) que corresponde al resultado de la aplicación de una función de hash a la clave pública del nodo Tor en el momento que se configura el servicio oculto[9].

`http://lotjbov3gzzf23hc.onion/`

Figura 6. Dominio .onion para el sitio de estado de la red Tor.

2.5. Tor Browser Bundle

Tor Porject ofrece un navegador que integra el software necesario para conectarse a la red Tor. El usuario simplemente descarga la herramienta y se conecta a la red sin necesidad de configurar algún parámetro.

El navegador (Fig. 7) está basado en la versión de soporte extendido (ESR) de Firefox y contiene un botón para cambiar la identidad (crear un nuevo circuito).

También se incluye el panel de control Vidalia (Fig. 8), que sirve para configurar Tor en los siguientes modos:

Cliente: funciona solo para navegar, simplemente envía paquetes a la red y recibe la respuesta.

Relay: permite que el nodo sea incluido en un circuito Tor, posibilitando el paso de mensajes encriptados dentro de la red.

Nodo de salida: el tráfico que llegue a este punto será redirigido a servidores que están fuera de la red, actúa como punto de escape de la red.

Puente: los clientes que estén configurados de esta manera, no serán incluidos en la lista de nodos del servidor de directorio Tor. Esto imposibilita a los proveedores de internet bloquear el acceso a la red Tor. Ya que no se publican estos nodos, son más difíciles de encontrar y para conectarse es necesario saber la dirección.

El software está disponible para Windows, Mac OS X y Linux, además puede ejecutarse desde una memoria USB sin necesidad de instalar localmente[10].

3. Ventajas

Algunas de las ventajas que presenta Tor:

Sistema distribuido: como se observa en la Figura 9, existen más de 4.000 nodos relay y cerca de 2.000 nodos puente activos en la red, esto hace casi imposible que un ataque tenga efecto sobre la red. Además, están distribuidos en todo el mundo, lo que dificulta que un gobierno apague la red como mecanismo de censura.

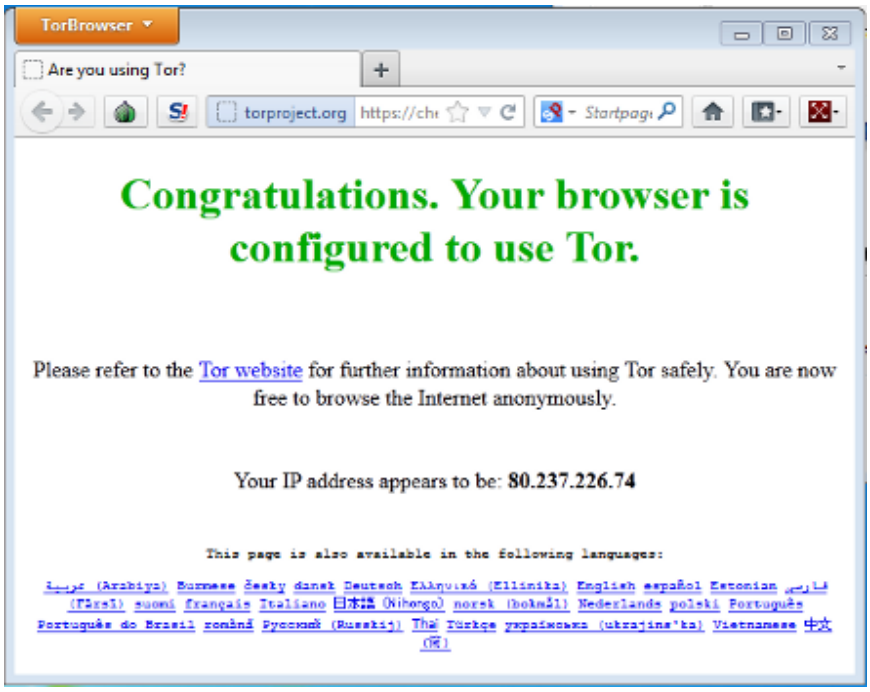


Figura 7. Tor Browser.

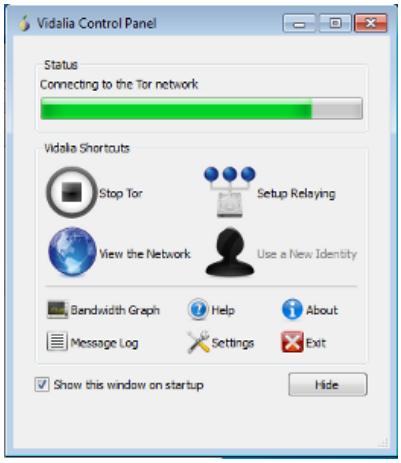


Figura 8. Vidalia Control Panel.

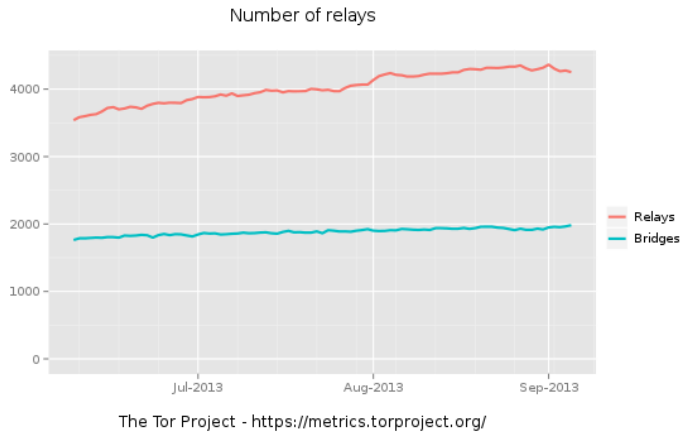


Figura 9. Cantidad de nodos Tor activos[11].

Privacidad: Tor fue creado con la privacidad y anonimidad en mente. Todo está diseñado para proteger la identidad de los usuarios que utilizan la red.

4. Desventajas

Algunas desventajas que presenta Tor (y el enrutamiento por capas en general) con respecto a la seguridad y privacidad:

Análisis de tiempo: un atacante puede determinar cuando un nodo se esta comunicando con un sitio web, mediante el establecimiento de una correlación entre el momento que el servidor envía un mensaje y el tiempo en el que el nodo lo recibe.

Ataques de intersección: los nodos se desconectan de la red o fallan periódicamente, cualquier circuito que quede funcionando no puede ser enrutado a través del nodo que falló o cualquier nodo nuevo que se agregó a la red, lo que aumenta las posibilidades de realizar un análisis de tráfico exitoso.

Ataques de nodo predecesor: un nodo comprometido puede mantener un historial de la sesión a medida que ocurren cambios en el circuito. Si la misma sesión es observada luego de varios cambios, el nodo comprometido tiende a conectarse frecuentemente con el nodo origen que con cualquier otro nodo, lo que incrementa las posibilidades de un análisis de tráfico.

Observación del tráfico en el nodo de salida: el último nodo en el circuito, el nodo de salida, tiene acceso completo al contenido transmitido desde el emisor al receptor. Esto se previene utilizando SSL en la comunicación, de forma que el nodo de salida solo vea una conexión encriptada.

Otras desventajas:

Sistema lento: debido a que el tráfico es redirigido varias veces entre los nodos, se vuelve algo lento. El tiempo de creación del circuito también es notable, debido a que se debe negociar con cada nodo la clave de encriptación.

Bloqueo desde el proveedor de internet: los ISP frecuentemente buscan y bloquean los nodos que están dentro de su red, lo que hace difícil poder conectarse.

5. Usos

Prensa: periodistas pueden utilizar Tor para comunicarse con disidentes y denunciantes de forma segura. También se utiliza para filtrar información, como el caso PRISM que fue filtrado por Edward Snowden al periódico británico The Guardian[12].

Grupos activistas: grupos como Electronic Frontier Foundation (EFF) recomienda el uso de Tor para proteger la identidad de sus miembros y mantener libertades civiles en línea.

Corporaciones: las corporaciones utilizan Tor para proteger sus comunicaciones de personas que estén espiando el medio. También se utiliza como reemplazo de las redes privadas virtuales (VPN).

Otros usos incluyen simplemente navegación a sitios bloqueados por el ISP o por el país o para buscar información sensitiva.

En la actualidad, Tor se utiliza para navegar anónimamente, mas aún luego de las diferentes filtraciones sobre el programa de espionaje de Estados Unidos. Los periodistas utilizan para investigar e intercambiar información que puede ser considerada secreta o de importancia para algunos gobiernos, que harán lo imposible por evitar que salga a la luz. Tor sigue siendo el mayor proveedor de pornografía infantil, lastimosamente un porcentaje de los usuario lo utilizan con este fin. También se usa para acceder a sitios bloqueados o que solo están disponibles desde dentro del país (haciendo la función de un proxy).

6. Tecnologías similares

6.1. Java Anon Proxy

También conocido como JAP o JonDonym, Java Anon Proxy es un sistema proxy diseñado para navegar en internet con pseudo-anonimidad. La principal diferencia con Tor, es que permite al usuario elegir a quien confiarle su tráfico. El cliente JonDonym permite que el usuario elija los nodos entre varios nodos ofrecidos por distintas organizaciones. Como estos nodos son conocidos, son identificables y blancos fáciles para hackers y agencias de gobierno[13].

6.2. Invisible Internet Project

Más conocido como I2P, es una red de computadoras que permite a las aplicaciones enviar mensajes a otras de forma pseudo-anónima y segura. Toda la comunicación es encriptada *end-to-end*. Incluso los destinatarios son identificadores criptográficos, de modo que su dirección IP no pueda ser revelada. Se utiliza para el tráfico de aplicaciones como clientes de email, chat, archivos compartidos y túneles entre computadoras[14]. Una ventaja de este sistema es que todos los usuarios participan del ruteo, no solo los clientes que están configurados como relay, aumentando la capacidad total del sistema. I2P también posee transporte sobre UDP, haciendo que más aplicaciones puedan funcionar sin realizar cambios en la forma de conexión[15].

6.3. Privoxy

Es un servidor proxy sin cache con capacidades de filtrado para mayor privacidad. Funciona modificando los datos de la página web y las cabeceras HTTP antes que sea mostrada en el navegador, eliminando publicidad y javascript que pueda rastrear al usuario.

6.4. Garlic Routing

Es una variante de Onion Routing, con la principal diferencia que encripta múltiples mensajes combinados para hacer más difícil el ataque por análisis de tráfico[16]. Además, el camino es unidireccional, cuando el receptor quiere devolver una respuesta, debe crear un nuevo camino para llegar al emisor[17].

6.5. Freenet

Freenet es una plataforma peer-to-peer para la comunicación resistente a la censura. Utiliza un sistema distribuido de almacenamiento de datos para guardar información.

Freenet funciona guardando pequeños archivos encriptados en las computadoras de los usuarios y se conecta usando intermediarios que pasan el pedido y devuelven el contenido solicitado sin conocer el contenido del archivo por completo[18].

7. Silk Road

Lanzado en febrero de 2011, Silk Road es un mercado negro virtual operado como un servicio oculto de Tor. El rubro principal de este mercado son las drogas.

Los usuarios deben registrarse en el sitio para poder comprar, no así para vender, ya que las cuentas para vendedores son subastadas para prevenir estafas.

Entre los productos que se pueden encontrar en el sitio están las drogas: heroína, cocaína, LSD, marihuana; aunque también se puede encontrar arte, ropa, libros, joyas y otros objetos legales.

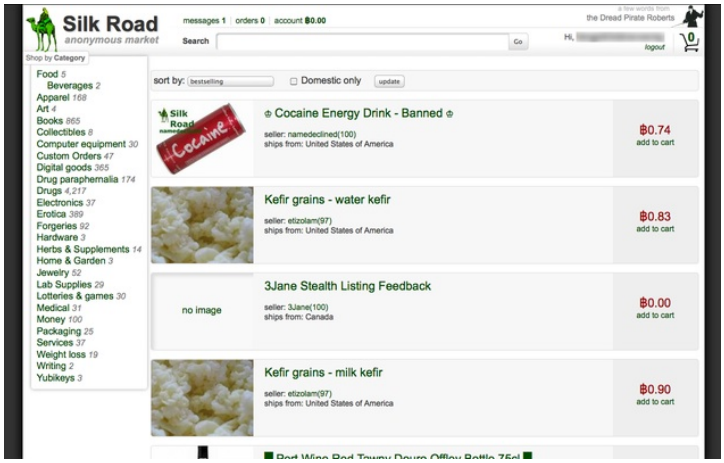


Figura 10. Página principal del sitio Silk Road.

Las transacciones se realizan mediante bitcoins, la moneda anónima virtual, y el pedido es enviado por correo al destinatario. Se estima que en el sitio se hicieron transacciones por valor de 15 millones de USD en 2012[19].

Un experimento realizado por Forbes[20] comprobó que es posible rastrear los bitcoins y poder saber quien fue el que los gastó. Las propiedades de privacidad del bitcoin son paradójicas, cada transacción que se realiza es guardada en *blockchains*, el mecanismo descentralizado para rastrear quien posee cuales monedas y cuando, además de prevenir fraudes. La transacción se guarda como direcciones, que no están identificadas con ninguna persona.

Meiklejohn y sus colegas encontraron que mirando el blockchain se puede deducir quien es el dueño de esas direcciones de Bitcoin. Demostraron que utilizando métodos de clustering y con solo 344 transacciones propias se puede identificar a los dueños de más de un millón de direcciones Bitcoin[21].

Meiklejohn rastreó las transacciones realizadas por Forbes, y pudo determinar que las direcciones de Bitcoin estaban asociadas al servicio de billeteras Coinbase. Suponiendo que el gobierno puede obtener una orden para saber el nombre del propietario de la billetera, puede automáticamente determinar donde fueron gastados los bitcoins asociados a dicha billetera.

7.1. La clausura de Silk Road

Ross Ulbricht empezó promocionando su sitio en foros sobre drogas y sobre bitcoins bajo el seudónimo de “altoid”. Tiempo después publicó en “Bitcoin Forum” un mensaje solicitando personal para el puesto de IT en una compañia de bitcoins. Esta vez, “altoid” dejo su correo personal de gmail para ser contactado.

El FBI solicitó datos sobre esa cuenta a Google para continuar con la investigación. Los registros incluian cada dirección IP utilizada para acceder al correo. La dirección IP apuntaba a un departamento en San Francisco.

Ulbricht también publicó en StackOverflow solicitando ayuda, mostrando una porción del código de Silk Road, bajo su propio nombre. Tiempo despues cambió su nombre de usuario a “frosty”.

Un agente encubierto del FBI se contacto directamente con el administrador de Silk Road, sindicado como “Dread Pirate Roberts”, haciéndose pasar por un distribuidor de drogas queriendo hacer negocios en Silk Road. En el email, escribió que estaba buscando un comprador para un kilo de cocaína. Ulbricht dió instrucciones a un empleado para que compre la droga, depositando $7,000 en Bitcoins en una cuenta de Silk Road y estableciendo una dirección de entrega. El FBI procedió al arresto del empleado de Ulbricht.

El 26 de enero, Ulbricht se contactó con el agente encubierto explicándole que su empleado fue arrestado y además robó fondos de otros usuarios de Silk Road. También pidió al agente para que golpee al empleado y le obligue a devolver el dinero. Al día siguiente, Ulbricht solicitó al agente que mate al empleado porque temía que hable sobre el tema luego de su arresto. Para tal fin, ofreció al agente $80,000.

El 23 de julio, los investigadores lograron localizar un servidor de Silk Road en un país no identificado (según consta en el documento presentado a la corte). Solicitaron a los administradores del servidor una copia del mismo. Recibieron registros que contenían 1.2 millones de transacciones y todo el registro del correo.

Si bien no se sabe como el FBI logró capturar a Ulbricht, varias hipótesis son manejadas. En el documento presentado a la corte[22], se puede leer que el FBI utilizó varias técnicas de investigación tradicional como tambien de alta tecnología para desmantelar Silk Road.

Los expertos no saben si el FBI identificó una vulnerabilidad en Tor, o se utilizó un ataque directo al servidor a través de una puerta trasera del software que se estaba ejecutando para ganar acceso al mismo y poder controlarlo en forma remota.

El 1 de octubre de 2013 el FBI procede a la captura de Ross Ulbricht, quien fuera el creador y operador de Silk Road, bajo los cargos de distribución de drogas, conspiración e intento de homicidio[23][24][25][26].

8. El ataque a Freedom Hosting

Freedom Hosting era la mayor compañía de hosting para sitios onion. Antes del ataque perpetrado por el FBI, Freedom Hosting contenía el 50 % de los sitios onion dentro de Tor.

El ataque fue llevado a cabo mediante un exploit diseñado específicamente para la versión del navegador Firefox que viene incluido en Tor Browser Bundle. Este exploit permitía la carga de un archivo javascript que revelaba la dirección IP y dirección MAC de la computadora conectada al sitio con el script.

El objetivo del ataque fue capturar al propietario de la compañía Eric Eoin Marques, y acusarlo de ser facilitador de pornografía infantil, ya que la mayoría de los sitios hospedados en Freedom Hosting se dedicaban a distribuir y comercializar pornografía infantil.

Este ataque puso en duda la seguridad y privacidad de Tor, aunque realmente Tor no falló, simplemente fue un problema del navegador y no de la red en sí.

9. Controversias

Debido al carácter inherentemente anónimo de Tor, se ha utilizado la red para actividades ilegales como venta de drogas, tráfico de armas, pornografía infantil y distribución de contenido protegido por derechos de autor.

Tor se puede utilizar para acceder a contenido censurado o prohibido por las leyes de un país, lo que podría tener consecuencias legales para el usuario que esté accediendo a dicho contenido.

También se ha detectado operaciones de lavado de dinero a través de bitcoins dentro de la red Tor.

Otros casos incluyen robo de identidad, fraude con tarjetas de crédito y divulgación de información clasificada.

10. Exponiendo el tráfico de Tor

Varios informes indican que la Agencia Nacional de Seguridad (NSA) de los Estados Unidos puede romper la encriptación de los mensajes que circulan dentro de la red Tor. Además como Tor utiliza tres nodos para cada conexión, existe una posibilidad mayor que éstos sean controlados por la NSA, lo que les facilita el trabajo de desencriptación. También se especula que la NSA controla nodos suficientes como para que una parte del tráfico pueda ser capturado y analizado.

En las versiones antiguas de Tor, se usaba el algoritmo de encriptación RSA/DH de 1024bits, que se sabe puede ser fácilmente desencriptado por hardware poderoso. La NSA también puede dirigir tráfico a los nodos que no controlan para que el algoritmo de balanceo de carga de Tor haga que el tráfico pase por los nodos que si controlan[27].

11. Conclusión

Tor es una tecnología que tiene el potencial de cambiar las comunicaciones por internet. Con las evidencias recientes de vigilancia por parte de los gobiernos, es necesario un método de comunicación segura, privada y anónima. Es aquí donde Tor Project cobra relevancia dado que provee todas las herramientas y software necesario para poder establecer una comunicación segura.

Los usos de tor son variados, desde permitir a los usuarios saltar la censura impuesta por países hasta actividades ilícitas y prohibidas.

El futuro de Tor recae en manos de los usuarios, los que ponen a disposición equipos para crear la red de nodos, ancho de banda para posibilitar el intercambio de información y tiempo y esfuerzo para mantener los nodos operativos.

Referencias

1. Dingledine, R., Mathewson, N., Syverson, P.: Tor: The second-generation onion router. (2004)
2. http://en.wikipedia.org/wiki/Deep_Web: Deep web (2013)
3. Bergman, M.K.: The deep web: Surfacing hidden value. The Journal of Electronic Publishing **7**(1) (2001)
4. http://en.wikipedia.org/wiki/Onion_routing: Onion routing (2013)
5. http://es.wikipedia.org/wiki/Perfect_forward_secrecy: Perfect forward secrecy (2013)
6. http://www.onion-router.net/History.html: Onion routing history (2013)
7. https://www.torproject.org/about/overview.html.en: About tor (2013)
8. Chaum, D.L.: Untraceable electronic mail, return addresses, and digital pseudonyms. Commun. ACM **24**(2) (1981) 84–90
9. http://en.wikipedia.org/wiki/.onion: .onion (2013)
10. https://www.torproject.org/projects/torbrowser-details.html.en: Tor browser bundle: Details (2013)
11. https://metrics.torproject.org/network.html: Tor project network metrics (2013)
12. http://www.theatlanticwire.com/technology/2013/07/privacy-methods-edward-snowden-uses/67118/: The privacy methods edward snowden uses (2013)
13. http://en.wikipedia.org/wiki/Java_Anon_Proxy: Java anon proxy (2013)
14. http://en.wikipedia.org/wiki/I2P: Invisible internet project (2013)
15. http://www.i2p2.de/how_networkcomparisons: Benefits of i2p over tor (2013)
16. http://en.wikipedia.org/wiki/Garlic_routing: Garlicrouting (2013)
17. http://www.i2p2.de/how_garlicrouting: Bundling multiple messages (2013)
18. http://en.wikipedia.org/wiki/Freenet: Freenet (2013)
19. Christin, N.: Traveling the silk road: A measurement analysis of a large anonymous online marketplace. (2013)
20. http://www.forbes.com/sites/andygreenberg/2013/09/05/follow-the-bitcoins-how-we-got-busted-buying-drugs-on-silk-roads-black-market/: Follow the bitcoins: How we got busted buying drugs on silk road's black market (2013)
21. Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoyy, D., Voelker, G.M., Savage, S.: A fistful of bitcoins: Characterizing payments among men with no names. (2013)
22. Tarbell, C.: Ulbricht criminal complaint (2013)
23. http://www.theguardian.com/technology/2013/oct/15/silk-road-ross-ulbricht-alleged-mastermind: Silk road's alleged mastermind 'not excessively concerned' about future (2013)
24. http://edition.cnn.com/2013/10/04/world/americas/silk-road-ross-ulbricht/: How fbi caught ross ulbricht, alleged creator of criminal marketplace silk road (2013)
25. http://www.usatoday.com/story/news/nation/2013/10/21/fbi-cracks-silk-road/2984921/: How fbi brought down cyber-underworld site silk road (2013)
26. https://medium.com/p/d48995e8eb5a: How dread pirate roberts (silk road) got caught. (2013)
27. http://blog.erratasec.com/2013/08/anonymity-smackdown-nsa-vs-tor.html: Anonymity smackdown: Nsa vs. tor (2013)