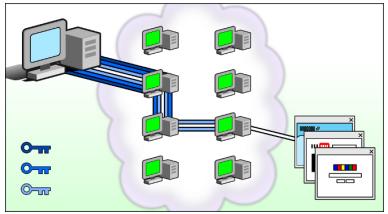
¿Qué es TOR?

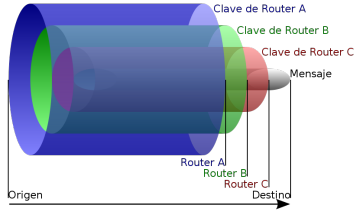
- TOR (**The Onion Routing**): Una red de anonimato
- No es una red P2P: aunque es una red entre particulares
- Es software: procede de investigación, pero no es una red dedicada
- Algo de historia: de proyecto militar a organización sin ánimo de lucro.

¿Qué es TOR?
- TOR (**The Onion Routing**): Una red de anonimato
- No es una red P2P: aunque es una red entre particulares
- Es software: procede de investigación, pero no es una red dedicada
- Algo de historia: de proyecto militar a organización sin ánimo de lucro.

- El Enrutamiento de cebolla es una red de túneles virtuales de comunicación superpuesta a Internet que garantiza el anonimato de sus usuarios y de los enrutadores que median en la comunicación y proporciona integridad y confidencialidad de los datos que se intercambian.
- Usuarios y encaminadores tienen distintos roles y existen servidores de directorio. Los enrutadores son individuales o empresas qu prestan su ancho de banda. También hay servicios (web, mensajería) llamados hidden services que se prestan anónimamente (no conoce su ubicación, ni quién los gestiona, desde donde, etc.)
- Anteriormente un complemento de Firefox (Tor Button) ahora es un navegador seguro (Tor Browser Bundle y Vidalia) en múltiples idiomas y varios proyectos de software más relacionados. Otros programas: Tails (SO seguro), Orbot (Tor para Android), Stem (biblioteca python para controlar Tor, muy fácil para jugar con Tor), TorBirdy (Tor para Thunderbird), etc.
- Tor se inició como un proyecto de investigación de la Marina de EE.UU. llamado Onion Routing, alla por 1996, para la construcción un protocolo que resista análisis, escuchas y ataques tanto de agentes externos como de enrutadores maliciosos. Pasó a ser dirigi por la EFF (Electronic Frontier Foundation) y actualmente es una Organización sin ánimo de lucro: The Tor Project.

¿Cómo funciona?





Anonimización y encriptación

Cabeceras anónimas y uso de autenticación y encriptación (TLS/SSLv3) entre los nodos de la red Tor (clientes/*relays* y entre *relays*).

Los datos pueden o no estar encriptados en origen, pero las cabeceras (con las direcciones IP) siempre van en claro. Lo que realmente se anonimiza es la dirección de origen (de la petición) y destino (de la respuesta), ya que son direcciones cambiantes a lo largo del camino virtual. Aunque se soliciten páginas en claro (canal en blanco en la imagen de la izquierda), los paquetes entre los *relays* sí se encriptan (canales en tonos de azul), pero sólo el usuario final comparte las claves con cada *relay* para desencriptar cada capa.

Algunos nombres comunes

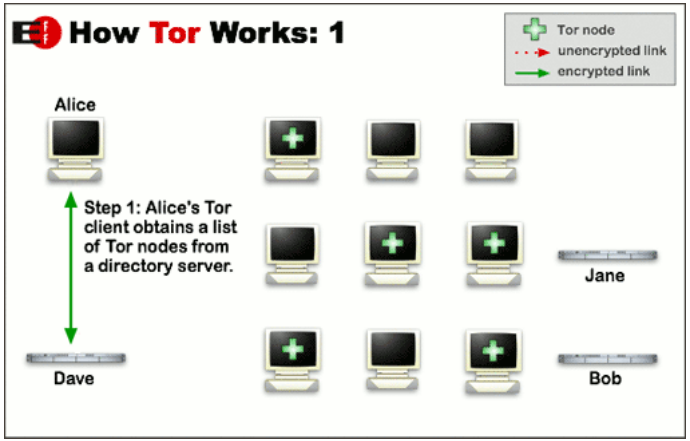
- **Relay**: nodo repetidor
- **Entry guard**: nodo de entrada elegido al azar
- **Exit relay**: nodo repetidor de salida (hacia Internet)
- **Hidden service**: servicio oculto (a Internet, sólo visible en Tor)
- **Bridge**: puente de entrada a la red Tor
- **Obfuscated bridge**: puente que ofusca la entrada a la red Tor

Algunos nombres comunes

- **Relay**: nodo repetidor
- **Entry guard**: nodo de entrada elegido al azar
- **Exit relay**: nodo repetidor de salida (hacia Internet)
- **Hidden service**: servicio oculto (a Internet, sólo visible en Tor)
- **Bridge**: puente de entrada a la red Tor
- **Obfuscated bridge**: puente que ofusca la entrada a la red Tor

- Nodo de Tor (ejecuta Tor) y permite enrutar peticiones de clientes de Tor hacia otros nodos de la red Tor, pero nunca fuera.
- Nodo de Tor elegido aleatoriamente para ser en punto de entrada a la red Tor. El cliente elige pocos nodos como punto de entrada para pasar inadvertido a los ataques de correlación, aunque hace más visible su tráfico si un nodo de entrada es comprometido.
- Nodo de Tor que permite enrutamiento de peticiones tanto hacia nodos de la red Tor como hacia servidores externos, ya sea en comunicación segura o no.
- Permite proveer servicios basado en comunicación TCP, p.e. un servidor web, a otros nodos de la red de forma anónima, sin revelar IP propia. Por supuesto, además de configurar el servicio hay que instalar el o los programas que los dan (p.e. el servidor web).
- Es un relay oculto (no está listado en el directorio) y, de este modo no es fácil de localizar. Sirve como nodo de entrada a la red Tor para aquellos clientes que tienen dificultades para conectarse a los repetidores porque el ISP puede estar bloqueando el tráfico hac los relays conocidos.
- Es un tipo de puente que utiliza algún software de ofuscación. Actualmente solo obfsproxy y flashproxy están desplegados y funcionando. Realiza una ofuscación del tráfico entre un cliente y el puente de modo que los censores no puedan distinguirlo del tráfico habitual y, por tanto, bloquearlo.

¿Cómo funciona?: Paso 1

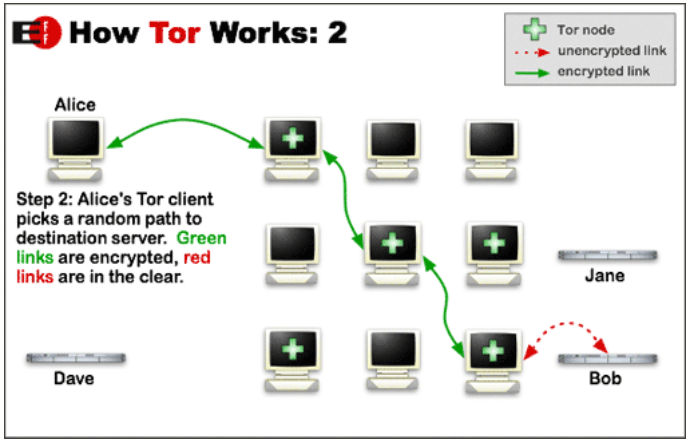


- Obtención de la lista de enrutadores desde un servidor de directorio.

¿Cómo funciona?: Paso 1
Obtención de la lista de enrutadores desde un servidor de directorio.

- El usuario Alice solicita por un canal seguro la lista de nodos Tor a un servidor de directorio.

¿Cómo funciona?: Paso 2

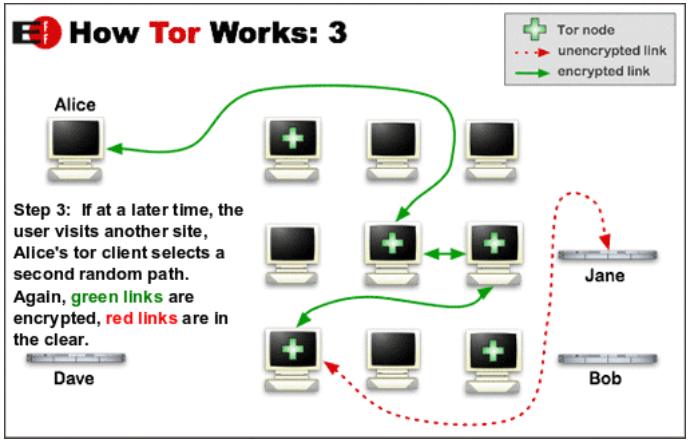


- Creación del camino virtual

¿Cómo funciona?: Paso 2
Creación del camino virtual

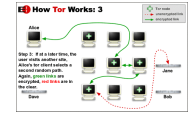
- El cliente Tor construye un circuito de conexiones a través de los nodos de forma incremental. Ningún nodo conoce el camino completo, sólo conoce a su antecesor y a su descendiente y sólo el cliente conoce las claves en cada salto a lo largo del camino.

¿Cómo funciona?: Paso 3



- Comunicación por rutas aleatorias

¿Cómo funciona?: Paso 3



Comunicación por rutas aleatorias

- Una vez establecido, el camino se mantiene sólo durante un máximo de diez minutos, tras lo cual se selecciona un nuevo camino virtual de forma aleatoria.

Log de Tor: el bootstrap

```
5%: Connecting to directory server.
10%: Finishing handshake with directory server.
15%: Establishing an encrypted directory connection.
20%: Asking for networkstatus consensus.
25%: Loading networkstatus consensus.
I learned some more directory information, but not enough to build a circuit:
We have no usable consensus.
40%: Loading authority key certs.
45%: Asking for relay descriptors.
I learned some more directory information, but not enough to build a circuit:
We have only 0/4824 usable microdescriptors.
We'd like to launch a circuit to handle a connection, but we already have 32
general-purpose client circuits pending. Waiting until some finish.
We now have enough directory information to build circuits.
80%: Connecting to the Tor network.
85%: Finishing handshake with first hop.
90%: Establishing a Tor circuit.
Tor has successfully opened a circuit. Looks like client functionality is working.
100%: Done.
```


La traza de ejecución de Tor describe muy bien los pasos anteriormentes mencionados. Además, demuestra como en ocasiones hay problemas para encontrar y dar un nuevo circuito al cliente. Los *microdescriptors* son una versión reducida de los descriptores de nodos, bastante estables (duran una semana) y tienen la información mínima útil para los clientes. El *networkstatus consensus* es la información de estado sobre los nodos Tor que las autoridades de directorio (de 5 a 10) generan cooperativamente para determinar cuando un nodo está o no activo. Son los propios *relays* los que suben esta información a las autoridades de directorio con sus capacidades y estado, aunque también existen cachés para en *relays* para agilizar este tráfico.

¿Quién lo financia? Sponsors

- Más de 1M de dólares: ONG anónima, BBG, SRI International y el Buró de democracia, derechos humanos y trabajo de EE.UU
- Hasta 1M de dólares: Sida, NSF y RFA
- Hasta 500K dólares: Internews Europa, NSF y The Knight Foundation
- Menos de 500K de dólares: NLNet, NRL, un ISP y otros

¿Quién lo financia? Sponsors
- Más de 1M de dólares: ONG anónima, BBG, SRI International y el Buró de democracia, derechos humanos y trabajo de EE.UU
- Hasta 1M de dólares: Sida, NSF y RFA
- Hasta 500K dólares: Internews Europa, NSF y The Knight Foundation
- Menos de 500K de dólares: NLNet, NRL, un ISP y otros

- Una ONG anónima norteamericana; el Broadcasting Board of Governors, una agencia federal que supervisa los medios de comunicación internacionales civiles americanos, formada por, entre otros, John Kerry); el Stanford Research Institute, dedicada a l investigación e innovación, p.e. inventores de Siri, el asistente personal comprado por Apple; y el Buró de democracia, derechos humanos y trabajo de EE. UU.

- La Agencia de Cooperación y Desarrollo Internacional de Suecia, una organización del ministerio de exteriores para administrar la mitad del presupuesto sueco en ayuda al desarrollo; la National Science Foundation, agencia federal para el progreso de la ciencia, salud y bienestar con un presupuesto de 7000M); y Radio Free Asia, la Radio Free Asia, una corporación privada sin ánimo de lucr para la difusión de noticias que, a su vez, es liderada y financiada por la BBG.

- Organización internacional para el desarrollo y ayuda de medios independientes, libertad de información y de expresión); la NSF ot vez, pero a través de la Universidad de Drexel; y la The Knight Foundation, una fundación privada sin ánimo de lucro dedicada a promover el periodismo de calidad, innovación en los medios y promover las artes, cuyo CEO fue también el director del Miami Herald, que ganó tres premios Pulizer y el Ortega y Gasset español de excelencia en periodismo.

- Fundación NLnet (ISP danesa cofundadora de la EUnet, primera red europea), el NRL (Naval Research Laboratory), un ISP anónim de USA, Google, Human Rights Watch, Access Now (organización pro derechos humanos centrada en Internet), la Fundación Cristiana Nacional, Torfox (un navegador Firefox con Tor más sencillo, sin Vidalia) y 4300 donaciones individuales.

¿Quién lo gestiona?

La junta directiva está formada por:

- **Roger Dingledine**: presidente y director
- **Ian Goldberg**: presidente de la junta
- **Nick Mathewson**: vicepresidente y director
- **Fran Rieger**: director
- **Caspar Bowden**: director
- **Meredith Hoban-Dunn**
- **Andrew Lewman**: director ejecutivo
- **Rob Thomas**: director y CEO de Team Cymru
- **Wendy Seltzer**: director y fundador de *Chilling Effects*

¿Quién lo gestiona?

La junta directiva está formada por:
- **Roger Dingledine**: presidente y director
- **Ian Goldberg**: presidente de la junta
- **Nick Mathewson**: vicepresidente y director
- **Fran Rieger**: director
- **Caspar Bowden**: director
- **Meredith Hoban-Dunn**
- **Andrew Lewman**: director ejecutivo
- **Rob Thomas**: director y CEO de Team Cymru
- **Wendy Seltzer**: director y fundador de *Chilling Effects*

- Desarrollador original de Tor junto con Nick Mathewson y Paul Syverson, lidera además la investigación en el comunicaciones anónimas.
- Criptógrafo, experto en privacidad, profesor y diseñador del protocolo de IMS seguro Off-the-Record Messaging (p.e. Gwibber).
- Programador original y arquitecto jefe de Tor y Libevent.
- Además lidera la empresa alemana GSMK Cryptophone dedicada al desarrollo y producción de teléfonos de comunicación encripta integral con código fuente publicado para su revisión.
- Un especialista en políticas de protección de datos en la UE y EE.UU, leyes de vigilancia, gestión de identidad, ética de la informaci y defensor de los derechos de autodeterminación y de la comprensión pública de la investigación de la privacidad en informática. Antes consejero jefe de privacidad en Microsoft del 2002 al 2011, dijo que no tenía "ni idea"sobre PRISM durante su estancia.
- Responsable del comité de auditoría, contable, asesora
- Y además secretario y tesorero
- Organización SAL para una Internet más segura. Tiene una empresa asociada que comercializa servicios de inteligencia empresar análisis de amenazas, seguridad, etc.
- Un proyecto de la EFF (Electronic Frontier Foundation) y las universidades de Harvard, Stanford, San Francisco, Maine, etc. especializado en la defensa contra órdenes de suspensión y desistimiento del gobierno.

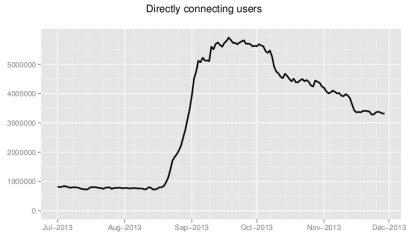
¿Quién lo usa?

- Organismos gubernamentales
- Periodistas, blogueros y activistas
- Agentes de las fuerzas del orden
- Multinacionales
- Personas normales

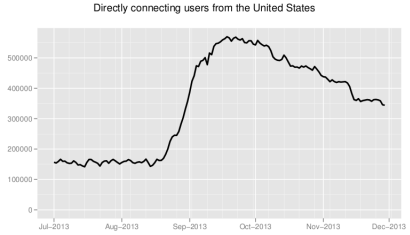
¿Quién lo usa?
- Organismos gubernamentales
- Periodistas, blogueros y activistas
- Agentes de las fuerzas del orden
- Multinacionales
- Personas normales

- De hecho, como ya hemos explicado, nació como un proyecto militar para la protección de las comunicaciones gubernamentales de gobierno de los EEUU, y hasta la NSA lo usa. También sabemos que gobiernos como China, Iran, India, Mongolia (entre otro mucho lo usan.
- Algunas organizaciones y agencias de comunicación apoyan el proyecto. Otras, como Reporteros sin Fronteras, asesoran a periodistas, blogueros y disidentes en el uso de Tor de modo que puedan garantizar su privacidad y seguridad. Periodistas y activist de todo el mundo, censurados por sus gobiernos, como Periodistas Ciudadanos de China, usan Tor para escribir sobre lo que pasa su entorno mas cercano para intentar promover un cambio en sus países o simplemente denunciarlo para que sea de dominio públi
- Las fuerzas del orden la usan para proporcionarse el anonimato necesario para infiltrarse en ciertas redes: trata de personas, blanqueo de dinero, redes de pornografía infantil, etc.
- Les proporciona la facilidad de intercambio de información altamente sensible: secretos comerciales; transmisión datos como financieros, estratégicos, patentes; entre otros.
- Cada vez más ciudadanos los usan, a medida que se publican más sobre el control de las agencias gubernamentales (de todos los países) quieren ejercer sobre las comunicaciones de todo el mundo.

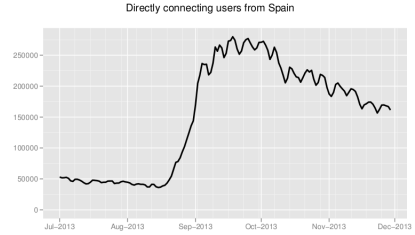
¿Quién lo usa?



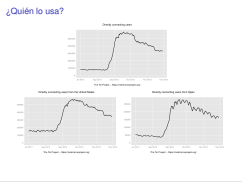
The Tor Project – https://metrics.torproject.org/



The Tor Project – https://metrics.torproject.org/



The Tor Project – https://metrics.torproject.org/



Las gráficas que se muestran se han obtenido a partir del portal de métricas que ofrece el proyecto Tor.
Como se puede observar en las gráficas, se muestra un gran aumento en el número de usuarios que usan la red Tor. Este incremento se debe a las publicaciones realizadas por el periódico The Guardian sobre los documentos filtrados por Snowden sobre el espionaje realizado por la NSA.
Las filtraciones comenzaron en Junio de 2013 y a partir de esa fecha la red no se detecta un incremento del número de usuarios que la usan. Es a principios de octubre, cuando The guardian publica los famosos documentos donde se hace patente los propósitos de la NSA respecto a la vigilancia de todo el tráfico de Internet, y los problemas que detecta cuando los usuarios usan la red Tor. En sea fecha, la red experimenta un aumento considerable de usuarios que la usan.
La gráfica de arriba muestra el incremento global de usuarios, y las dos de abajo el incremento en Estados Unidos y España. En USA se pasa de tener conectados una media de usuarios por debajo de los 200K usuarios a sobrepasar los 500K. En España el número de usuarios es significativamente inferior al de los USA, pero de 50K usuarios se pasa a sobre pasar los 250K.
También es significativo que el número de usuarios ha descendido globalmente, pero está muy lejos de alcanzar el número de usuarios que tenía antes de las filtraciones.

En la página que aparece en las gráficas, explica detalladamente como se obtienen y calculan estas métricas. Para estimar el

número de usuarios que usan la red Tor, contabilizan el número de peticiones realizadas a los directorios para obtener la lista de

nodos.

¿Cómo lo usan? (1)

Aplicaciones de usuario

Facilitan el anonimato en la navegación por Internet.

- Tor Browser Bundle
- Orbot
- TorBirdy

¿Cómo lo usan? (1)
Aplicaciones de usuario
Facilitan el anonimato en la navegación por Internet.
Tor Browser Bundle
Orbot
TorBirdy

- Proporciona todo lo necesario para navegar de forma segura por Internet. Está compuesto por: software de Tor; Vidalia, una herramienta que permite controlar Tor. Inicia, para y visualiza el estado de Tor, monitorizar el ancho de banda consumido, y configu algunos aspectos de Tor; una versión modificada de Firefox ESR pre-configurada para proteger la privacidad del usuario; y Torbutto encargado de la seguridad a nivel de aplicación y la privacidad en Firefox desactivando todos los tipos de contenidos activos.
- Se trata de un cliente de código abierto, para la red Tor para dispositivos Android. Una vez activado, permite una interacción anónim sobre Internet.
- Es un componente para Thunderbird, y otras aplicaciones no-web de Mozilla, encargada de la seguridad y privacidad a nivel de aplicación. Actualmente puede descargarse una versión experimental (beta).

¿Cómo lo usan? (2)

Aplicaciones y APIs para desarrollo

Permiten integrar la anonimización mediante la red Tor.

- Tor Cloud
- Obfsproxy
- Stem
- Tails

¿Cómo lo usan? (2)
Aplicaciones y APIs para desarrollo
Permiten integrar la anonimización mediante la red Tor.
Tor Cloud
Obfsproxy
Stem
Tails

- Permite desplegar, de forma sencilla, bridges en la infraestructura de cloud computing Amazon EC2, que ayudan a los usuarios a acceder a un Internet sin cesuras. Con estos puentes, se dona ancho de banda y puntos de acceso que permiten mejorar la seguridad y valocidad de acceso a la red Tor.
- Es una herramienta especialmente diseñada para evitar la censura en la red. ¿Cómo lo hace? Ofuscando el tráfico Tor para que parezca un trafico normal, impidiendo a las herramientas DPI identificar las lista de cifrado TLS.
- Es una librería Python para las aplicaciones interaccionen con Tor.
- Un SO que puede ser almacenado en un DVD, USB o SD card, cuyo objetivo es preservar el anonimato y privacidad. Todas la conexiones usan Tor, no deja rastro en el computador que usamos a menos que se pida expresamente. Utiliza herramientas criptográficas para cifrar archivos, correos y mensajería instantánea.

Argumentos a favor (técnicos)

- Navegación anónima
- Privacidad en las comunicaciones
- Donaciones de ancho de banda a la red

Argumentos a favor (técnicos)
- Navegación anónima
- Privacidad en las comunicaciones
- Donaciones de ancho de banda a la red

- Como ya hemos visto en la presentación de Tor, proporciona una navegación anónima, que oculta las direcciones IP del origen y destino de la comunicación. Esto permite la protección de la navegación a la vigilancia sobre el tráfico de red. Recordemos que cad relay solo conoce la IP de su antecesor y sucesor.
- La privacidad se consigue construyendo un circuito de conexiones encriptadas a través de la red.
- El proyecto también provee de herramientas que permiten a las organizaciones e individuales contribuir a la mejora de la red, incluyendo nuestros propios equipos dentro de la red.

Argumentos a favor (sociales)

- Libertad de expresión
- Evitar la censura
- Dificultar el robo de identidad y la comercialización de los registros de navegación

Argumentos a favor (sociales)
- Libertad de expresión
- Evitar la censura
- Dificultar el robo de identidad y la comercialización de los registros de navegación

- Estos son dos de los derechos fundamentales que todo el mundo reconoce que proporciona la anonimización que ofrece Tor. Mediante la utilización de los servicios ocultos, los usuarios puede configurar sitios Web que otros pueden utilizar para publicar información que pueda ser censurada.

- Al no conocerse el origen de las comunicaciones es muy difícil el robo de nuestra identidad, si se hace un uso correcto de la herramienta y siguiendo las recomendaciones del proyecto nuestra información viajará segura.
- Debido al cambio de IP durante nuestra navegación, a los sitios les resulta muy difícil registrar nuestra historia de navegación. Esto dificulta el tratamiento de la información obtenido para su uso con fines comerciales o económicos.

Argumentos en contra (1)

- Impunidad ante delitos graves:
  - Terrorismo
  - Blanqueo de dinero
  - Trata de personas
  - Pederastia
- No proporciona seguridad
- No es 100 % anónimo

Argumentos en contra (1)
- Impunidad ante delitos graves:
  - Terrorismo
  - Blanqueo de dinero
  - Trata de personas
  - Pederastia
- No proporciona seguridad
- No es 100 % anónimo

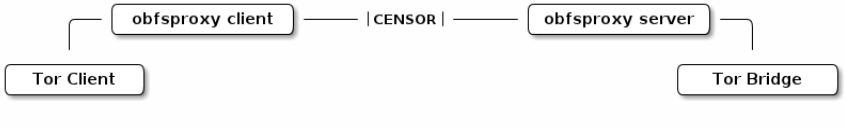
- Ante esto no hay mucho que añadir a los comentarios expuestos por los desarrolladores del propio proyecto. Aseguran que por supuesto el uso que puede hacerse de Tor es tan accesible para usuarios comunes como para criminales, pero la motivación es distinta. Los criminales actual al margen de la ley y pueden conseguir el anonimato mediante el robo de identidades o bien utilizar s tiempo y dinero en el desarrollo o compra de mejores herramientas que les garantice su anonimato.

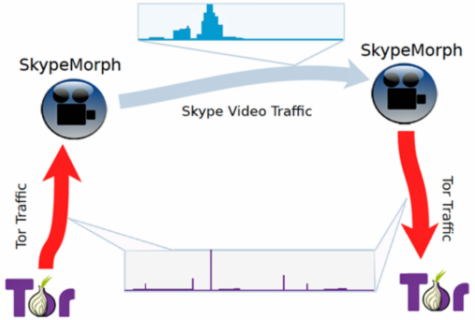
- Tor cifra la información a su entrada y la descifra a su salida, asegurando el anonimato. Pero si el usuario no utiliza protocolos segur para sus comunicaciones, como https, el propietario de un nodo de entrada o salida puede fisgar en el contenido de la comunicació En 2007 un investigador en seguridad informática sueco, Dan Egerstad, desvelo una lista de cuentas de correo y contraseña de organismos de países como Irán o China controlando el tráfico saliente de los servidores Tor que el donó. Esta vulneración no se debió a una debilidad de la red, sino a un mal uso del servicio por no usar protocolos seguros de comunicación.

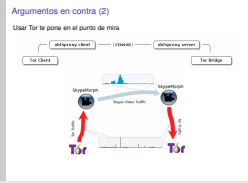
- La propia NSA reconoce que el número de usuarios que podría des-anonimizar es muy bajo. Y las técnicas que proponen están má encaminadas al seguimiento del comportamiento de los usuarios objetivos cuando no usan la red Tor, ya que un ataque a la red no resulta efectivo. Un ejemplo de ello, es utilizar los mismos alias tanto en la navegación abierta como con Tor o bien capturando la cookies generadas en la navegación abierta para identificarlos cuando se usa Tor. Aunque al mismo tiempo, estudian otras técnicas para degradar, denegar y romper los accesos a Tor. Una de estas técnicas se basan en la utilización de alguno de sus servidores QUANTUM, servidores estratégicamente colocados en Internet, con la autorización de los operadores más importantes, que permit identificar el tráfico Tor, aunque no identificar al usuario. Esta identificación se realiza de forma manual, pero una vez identificado, la NSA redirige el tráfico de este usuario a otro servidores llamados Foxacid, que dependiendo de la clasificación dada al usuario, realiza una serie de ataques al equipo para infectarlo y conseguir el control del mismo. Toda esta estrategia se centra en el ataque a las vulnerabilidades de Firefox como ejecución scripts o flash, si esto características se desactiva la identificación es muy difícil, o vulnerabilidades nativas como en la implementación de la librería E4X cuya deficiente gestión de títulos largos y un error en el interprete de XML permitían la inyección de código en el fichero RDF de inicio de Firefox. Todos estos problemas se han solventado en Firefox y en la versión que proporciona Tor Browser.

Argumentos en contra (2)

Usar Tor te pone en el punto de mira







- El objetivo de todos los gobiernos es identificar, filtrar y bloquear el tráfico de Tor. En los documentos filtrados de la NSA, se muestr algunas características que permitirían identificar el tráfico Tor. Entre ellas, y la que explotó Irán para bloquear el tráfico, fue la fecha de caducidad de los certificados usados por los *relays* (2 horas), que no es una fecha muy real para este tipo de certificados. Sin embargo, China ha conseguido bloquear el tráfico dinámicamente, mediante técnicas de inspección profunda de paquetes (DPI). Pe este bloqueo tiene una debilidad, la forma de saber si se trata de una conexión Tor es interceptar la conexión y establecer una nuev conexión Tor, si tiene éxito la IP es bloqueada. Una vez bloqueada, los escaners chinos continúan enviado conexiones y si en algún momento no se establece, el bloqueo es liberado (artículo *How China Is Blocking Tor*). La solución a estos bloqueos es el uso de la herramienta de ofuscación del tráfico, como obfsproxy que permite ofuscar el tráfico para confundirlo con peticiones normales, o SkypeMorph desarrollada por investigadores de la Universidad servidores de Waterloo (Canada) que permite ofuscar el tráfico Tor como si se tratara de tráfico de Skype (este software está en el punto de mira de la NSA). Otras investigaciones proponen como solución la fragmentación de paquetes, ya que los sistemas censores no están preparados para el reensamblaje de paquetes, el problema de usar esta técnica es que todos los usuarios que usen la red deben tener la capacidad de fragmentación y reensambla y además provoca una sobrecarga y por tanto un bajo rendimiento.
- *obsfproxy* se trata de una herramienta desarrollada en python que no forma parte de los clientes Tor Browser y Orbot pero que permite realizar la ofuscación del tráfico evitando la censura mostrándolo como si fuera tráfico normal o inofensivo de navegación. Está dirigida a usuarios que tienen una fuerte censura en su entorno y las comunicaciones son realizadas mediante los nodos *bridges*. Para ello, estos nodos deben tener instalada la herramienta que les permite realizar el reensamblado del tráfico.
- *SkypeMorph* recoge el tráfico saliente de Tor transformándolo en tráfico de una video llamada de Skype. A su llegada al *bridge*, el tráfico es reensamblado para transformarlo en tráfico Tor. Para una información más detallada, en el documento de enlaces se encuentra la referencia al artículo que los describe.

Argumentos en contra (3)

Controlar el circuito controlando varios nodos

Si se controlan C de N nodos totales, la probabilidad de evitar la vigilancia está en el orden de (N-C)/N

Argumentos en contra (3)
Controlar el circuito controlando varios nodos
Si se controlan C de N nodos totales, la probabilidad de evitar la vigilancia está en el orden de (N-C)/N

La mayoría de las agencias están intentando controlar el mayor número de nodos de la red Tor con el objetivo de realizar una reconstrucción del circuito. El estudio realizado por la NSA (*Tor Stinks*) muestra que el circuito podría ser reconstruido si se controlan 3 nodos: un nodo de entrada, un nodo interno y un nodo de salida, pero la tasa de éxito es muy pequeña debido a que la elección de los nodos es completamente aleatoria.
Cada cliente Tor selecciona de forma aleatoria un *exit relay* de un conjunto de nodos pequeño, normalmente 3 con una caducidad de 30 días.

Supongamos que un atacante controla C *relays* de un total de N. Si cada vez que se quiere usar la red se selecciona un nuevo *relay* de entrada y de salida, el atacante tendrá una probabilidad de (C/N)^2 de correlacionar nuestro tráfico, debido a que en un periodo de tiempo existen muchos cambios en el tráfico de forma que puede permitir al atacante identificarnos, porque en un tráfico normal no existen tantos cambios. Sin embargo, si el cliente Tor realiza la selección sobre un conjunto pequeño de *relays* como punto de entrada y solo para su primer salto, la correlación del tráfico es más difícil, debido a que los cambios en el primer salto son muy pocos comparados con los cambios en los *relays* de salida. La probabilidad en este caso de evitar la vigilancia está en el orden de (N-C)/N.

Argumentos en contra (4)

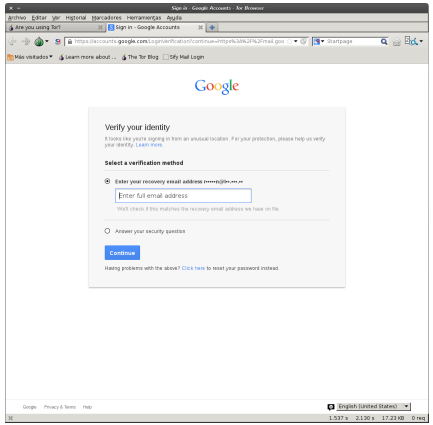
Tráfico lento

El número de usuarios que usa la red supera ampliamente al número de *relays* que comparten su ancho de banda.

Argumentos en contra (4)
Tráfico lento
El número de usuarios que usa la red supera ampliamente al número de relays que comparten su ancho de banda.

Este problema es reconocido por los propios autores de Tor, ver la página FAQ. La razón principal se debe al propio diseño de Tor, el tráfico salta de nodo en nodo y las demoras y cuellos de botella están siempre presentes. La red está formada por voluntarios que ceden ancho de banda, configuran sus máquinas para que actúen con *relays* o *bridges* o creando *hidden services*. Actualmente existe una gran diferencia entre el número de usuarios que usan la red y el número de usuarios que ceden recursos a la red. En el documento de enlaces, se encuentra el enlace a un artículo con una clasificación de los problemas que hacen que Tor no tenga un rendimiento óptimo y los pasos a seguir para tratar de resolverlos.

Experiencia con Tor



Bloqueo por IP (I)

La elección aleatoria de la identidad de navegación elegida por Tor, nos lleva a un bloqueo de las cuentas de los sitios más populares de Internet.

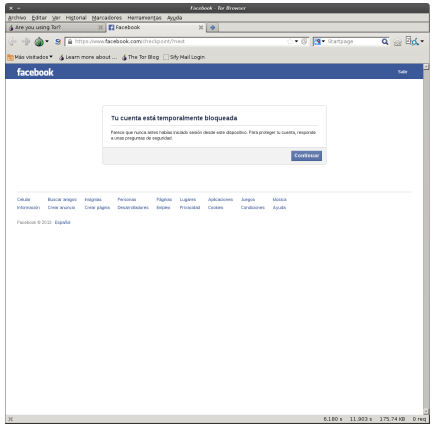
Experiencia con Tor
Bloqueo por IP (I)
La elección aleatoria de la identidad de navegación elegida por Tor, nos lleva a un bloqueo de las cuentas de los sitios más populares de Internet.

Tor anonimiza mediante la elección aleatoria de una de las IP's de los nodos que están en la red Tor, por tanto, algunos sitios muy utilizados bloquean el acceso a las cuentas de sus usuarios cuando detectan que se realizan conexiones desde ubicaciones no habituales. En esta y las siguientes diapositivas mostraremos los problemas que hemos tenido al realizar la navegación usando Tor Browser.

En este caso, intentamos acceder a nuestra cuenta de GMail y al detectar el acceso desde una ubicación poco frecuente nos

solicita que verifiquemos nuestra identidad.

Experiencia con Tor



Bloqueo por IP (II)

Facebook también controla el país de procedencia de las peticiones por IP, lo que supone un bloqueo de la cuenta.

Experiencia con Tor
Bloqueo por IP (II)
Facebook también controla el país de procedencia de las peticiones por IP, lo que supone un bloqueo de la cuenta.

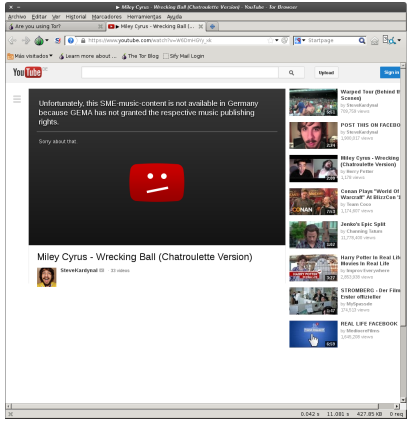
Otro ejemplo lo encontramos cuando queremos acceder a nuestra cuenta en Facebook. Nos bloquea la cuenta, y al igual que en el caso anterior, trata de verificar nuestra identidad. Pero además, realiza una paso adicional, nos envía un correo informándote del acceso desde una ubicación no habitual y las instrucciones para desbloquear tu cuenta.

No hemos probado el hecho de seguir navegando por el perfil de Facebook, pero nos ha surgido esta pregunta: ¿qué pasaría si

no nos desconectamos y nos cambia la IP mientras estamos conectados? Creemos que esto sería un completo desastre ya que

en cualquier momento podemos volver a cambiar la ubicación y nos volvería a bloquear.

Experiencia con Tor



Bloqueo por IP (III)

Es conocido que Youtube bloquea el acceso a ciertos contenidos dependiendo del país del que proceda la petición.

Experiencia con Tor
Bloqueo por IP (III)
Es conocido que Youtube bloquea el acceso a ciertos contenidos dependiendo del país del que proceda la petición.

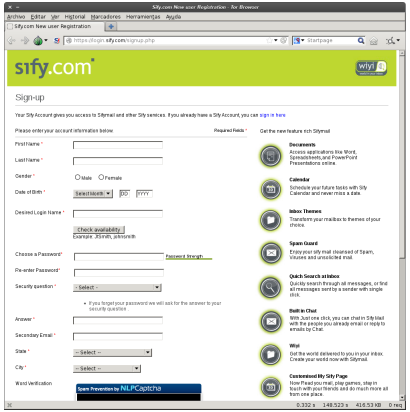
Es conocido que Youtube bloquea el acceso a ciertos videos dependiendo del país del que proceda la petición. Pues en este caso, nos hemos encontrado con este tipo de bloqueo. Al iniciar la navegación, Tor nos ha proporcionado una identidad cuya IP está ubicada en Alemania. Al detectar la procedencia por IP nos ha bloqueado el acceso.

Para evitar esto, puedes volver a solicitar una nueva identidad y volver a intentar acceder al contenido, Pero debemos ser

consciente que lo mismo que puede acceder a los contenidos, estos te puede ser bloqueados ya que la asignación de identidad

es completamente aleatoria.

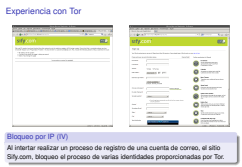
Experiencia con Tor



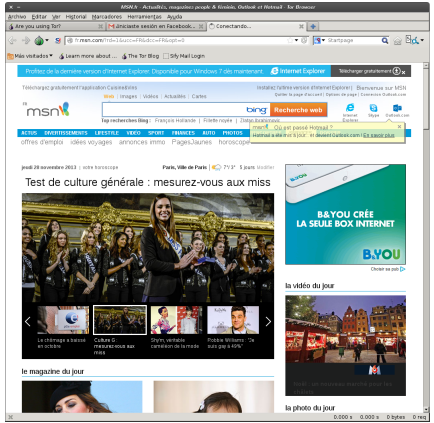
Bloqueo por IP (IV)

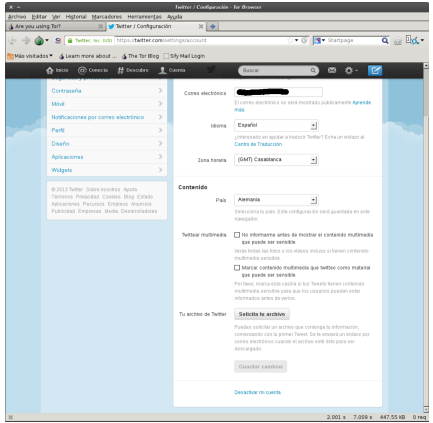
Al intertar realizar un proceso de registro de una cuenta de correo, el sitio Sify.com, bloqueo el proceso de varias identidades proporcionadas por Tor.

2013-12-04
Proyecto TOR
Cuestiones éticas
Experiencia con Tor También tratamos de realizar un proceso de registro para obtener una cuenta de correo electrónico. El sitio elegido fue Sify.com. Cuando intentamos solicitar el registro de una cuenta de correo no encontramos que esta página bloquea a varias IP's de *exit nodes*, supuestamente porque se realizan registros de patrones maliciosos de identificadores desde estos nodos. Después de varios cambios de identidad conseguimos acceder a la página de registro de cuenta y completamos el proceso. Una vez que has creado la cuenta, yo no tuvimos problemas de acceso independientemente de la IP asignada.



Experiencia con Tor





Idioma

Algunas páginas seleccionan erróneamente el idioma del país, su elección la basan en la IP y no en el idioma del navegador o en el configurado en el perfil.

Experiencia con Tor
Idioma
Algunas páginas seleccionan erróneamente el idioma del país, su elección la basan en la IP y no en el idioma del navegador o en el configurado en el perfil.

Al entrar en algunas páginas, se selecciona erróneamente el idioma del país al que pertenece la IP en lugar del idioma elegido en el navegador. Es un claro ejemplo de que están tratando un dato privado, la ubicación. El sitio MSN que nos muestra la página en francés y el idioma configurado en el navegados es ingles.

El otro ejemplo es Twitter, que no bloquea ni cambia el idioma, pero si guarda tu ubicación. Por tanto, una forma de saber si usas

o no Tor puede ser comprobando cuantas veces cambias de ubicación en una sesión de Twitter.

Demo de Tor Browser

- Instalación
- Ejecución
- Configuración de modo de ejecución con Vidalia
- Uso complementos de seguridad (HTTPEverywhere, ScriptBlocker)
- Demostración de tiempo de carga de páginas (Tor Browser/Firefox)

Demo de Tor Browser
- Instalación
- Ejecución
- Configuración de modo de ejecución con Vidalia
- Uso complementos de seguridad (HTTPEverywhere, ScriptBlocker)
- Demostración de tiempo de carga de páginas (Tor Browser/Firefox)

- ¡Leer "Want Tor to really work?.ªntes! O no servirá para nada usarlo. Windows: Seleccionar idioma y preconfiguración (bridge, relay exit node) y ejecutar. Apple OS X: Descomprimir aplicación (arrastras y soltar en Aplicaciones) GNU/Linux: Descomprimir Tor (arrastrar y soltar) y ejecutar, aunque tor (solo el proxy SOCKS) también está en varias distribuciones comunes (Fedora, Ubuntu, et Android: Usar repositorio F-Droid o Guardian Project (apps seguras)

- Vidalia es la interfaz gráfica que controla la configuración y arranque del demonio tor. Permite arrancar, parar y configurar el modo d ejecución. ¿Quiénes somos? La pantalla principal de Tor Browser nos lleva a la utilidad de verificación de Tor, pero podemos conoc la identidad que tenemos (cuál es nuestro exit node utilizando el Atlas). También es posible elegir un exit node nuevo pulsando en Üsar una nueva identidad".

- El botón Çonfiguración de retransmisión"permite convertirnos en un non-exit relay (.ºexcepto los repetidores de salida"), un exit relay (repetidores de salida") o bridge (.Ayude a usuarios censurados"). Usando el botó de preferencias es posible (pestaña Red") conectarnos usando un proxy HTTP (Üso un proxy para...") o utilizando un bridge (puente) añadiéndolo manualmente.

- No se recomienda instalar ningún complemento, pero Tor Browser viene con dos complementos imprescindibles para mejorar la seguidad. HTTPEverywhere proporciona reglas para navegar preferiblemente por las alternativas seguras de los servidores web. E algunos casos es trivial (https por http), pero en otras (p.e. Google) no lo es. ScriptBlocker sirve para (des)habitar de forma selectiva (o global) la ejecución de código JavaScript. Además utiliza lista blanca de sitios y protege contra XSS y distribución desencriptada cookies de sitios seguros, entre otros.

- Por ejemplo http://elpais.es, al no cargar complementos, tiene un peso muy inferior en la versión recuperada por Tor Browser y, sin embargo es cuatro veces más lento tanto en alcanzar el primero como el último byte. La página del proyecto Tor (https://torproject.o se carga completamente, pero los tiempos son similares, una caída de rendimiento de 4X. Para más detalles, leer el artículo "Performance Improvements on Tor.en la página de bibliografía.

Referencias

Documento `enlaces-tor.pdf`:

- Imprescindibles: la página de Tor
- Recursos importantes: divulgación, investigación y desarrollo
- Tutoriales: instalación, uso, integración, etc.
- Vídeos: con tiempo y subtítulos (algunos)
- Prensa: lo que se dice de Tor
- Presentaciones: formato rápido de leer
- Bibliografía científico-técnica: más seria

Referencias

Documento `enlaces-tor.pdf`:
- Imprescindibles: la página de Tor
- Recursos importantes: divulgación, investigación y desarrollo
- Tutoriales: instalación, uso, integración, etc.
- Vídeos: con tiempo y subtítulos (algunos)
- Prensa: lo que se dice de Tor
- Presentaciones: formato rápido de leer
- Bibliografía científico-técnica: más seria

- La página del proyecto Tor y todos los enlaces que contiene son valiosísimos, la referencia primera y última por completa y detallad aunque un bastante prolija y técnica en ocasiones. Las preguntas más frecuentes (varias categorías, son muy útiles y las 10 recomendaciones, necesaria.
- Si se va a hacer divulgación de Tor, investigar o desarrollar, estos recursos son muy valiosos. En el repositorio GIT, además, hay también documentación muy técnica.
- Aunque son casi todos en inglés, son muy útiles en configuraciones especiales y para usar Tor de forma avanzada o integrarlo con alguna herramienta.
- Hay tutoriales en vídeo, vídeos de divulgación, temas avanzados, etc. Para los que prefieren escuchar y ver antes que leer.
- La primera es la página de prensa del proyecto, que sea actualiza constantemente, pero las referencias en prensa se han disparad con el caso Snowden, así que esta relación es por fuerza obsoleta.
- Para los que gustan de este formato. Aquí se incluye la presentación del congreso de 2011 que también está en vídeo y que es mu importante.
- La documentación más seria y estable, en artículos que, como en el caso de "Tor: The Second-Generation Onion Router", tiene un alto número de citas. Está ordenada por fecha, con los últimos artículos al final.

Conclusiones y cuestiones abiertas

- ¿Utilizaría Tor? ¿Por qué?
- ¿Convencen las explicaciones de los gestores de Tor respecto a las garantías de anonimato? ¿Concuerda con la percepción de la NSA?
- Retos sociales
- Cuestiones técnicas

Conclusiones y cuestiones abiertas
- ¿Utilizaría Tor? ¿Por qué?
- ¿Convencen las explicaciones de los gestores de Tor respecto a las garantías de anonimato? ¿Concuerda con la percepción de la NSA?
- Retos sociales
- Cuestiones técnicas

- Sí, porque al menos proporciona la opción de poder ser anónimo si lo deseas. Ser anónimo permite ser libre en Internet, no ser clasificado ni discriminado, y poder ver lo que quiera bajo mi responsabilidad sin tutelas no elegidas. Y si deseo facilitar mis datos, l hago voluntaria y conscientemente, no bajo falsos beneficios (facilitarme la navegación, orientarme mejor) que solo ocultan un mod de negocio basado en la venta de datos privados.

- Los gestores del proyecto no garantizan un anonimato total ya que únicamente se centra en proteger el transporte y no el contenid Por tanto, insisten en la responsabilidad que el usuario tiene en el uso de protocolos seguros (https) que garanticen la confidencialid del contenido e intentar no proporcionar datos relevantes que puedan identificarle. Las explicaciones y recomendaciones, coinciden con la información extraída de los documentos filtrados de la NSA. La agencia reconoce que han tenido muy poco éxito atacando directamente el protocolo Tor. Reconociendo que nunca serán capaces de des-anonimizar a todos los usuarios de Tor todo el tiemp Por tanto, se han centrado en un análisis manual. Han tenido éxito: (1) Explotando las posibles vulnerabilidades de la versión de Firefox,(2) en la identificación de cookies usadas por los usuarios cuando no usan la red Tor o (3) con el seguimiento de la navegaci en abierto de los usuarios, correlacionando la información obtenida en foros, redes sociales, etc.. con la obtenida del tráfico Tor.

- Un modelo débil contra amenazas: mantenerse útil y práctico a gran número de usuarios antes que ser perfecto y no llegar a usuar con pocos recursos. Retos sociales: una mayor usabilidad contribuye a la imagen seguridad, los actos de los usuarios dan la reputación a Tor (la publicidad suele ser masiva la negativa, minoritaria la positiva), la sostenibilidad depende del voluntariado, percepción de lentitud (ancho de banda) porque Tor se usa para intercambio de archivos, bloqueo de IPs de Tor por listas negras (u de políticas en exit nodes), listas por clase C, SMTP, etc.

- Tor no anonimiza en la capa de aplicación (las aplicaciones pueden revelar la IP) ni en la de física (los paquetes revelan características del SO) y algunos protocolos (p.e. DNS) deben entenderse para anonimizarlos. La anonimización de TCP (no UDP) usando SOCKS se queda pequeña. La anonimización al nivel de red sería difícil aunque muy interesante. Más en Challenges....

Enlaces sobre el Proyecto Tor

Imprescindibles

- Proyecto Tor
- La wiki de Tor
- Preguntas más frecuentes: 76 preguntas y sus respuestas sobre Tor
- Blog de Tor: Un compendio de noticias e ideas en marcha sobre Tor
- Página de herramientas: todas las herramientas para navegar y desarrollar con Tor
- 10 recomendaciones a la hora de elegir una herramienta de anonimización
- Tor Metrics Portal: Este sitio proporciona fácil acceso a los datos y documentación sobre todo tipo de datos interesantes de la red Tor, visualizandolos en gráficos e informes.

Recursos importantes

- Página de Roger Dingledine de bibliografía sobre anonimidad
- Canal de Youtube del proyecto tor (The TorProject's channel)
- Repositorio GIT de proyectos Tor
- Programas de ayuda para usar con Tor (Support programs)

Tutoriales (escritos)

- How To Access Darknet Using TOR Easy Tutorial
- On Secure Anonymity With Tor: SSH and SOCKS: Tutorial par usuarios de Windows de uso de Tor como anonimizador de conexiones SSH.
- Running Tor on Mac OS X: para ejecutar Tor sin interfaz gráfica
- Running a Tor relay, bridge, exit or hidden service: Tor en BSD
- Tutorial: SSH over Tor
- Tutorial: How to make a Hidden Tor Website or Service

Vídeos

- Instalación y uso Tor (5:32) subtítulos automáticos en inglés.
- Instalación y uso Orbot (6:34) subtitulado en inglés.
- Instalación y configuración de puentes (7:17)
- Navegación anónima con Tor (5:23) subtitulado en español.
- Tor and China (1:27:46): Roger Dingledine en el 23rd Chaos Communication Congress de 2006.
- How governments have tried to block Tor (1:25:40) en el 28th Chaos Communication Congress de 2011. Roger Dingledine y Jacob Applebaum hablando de los bloqueos en Iran, Siria y de nuevo China. Subtitulado automático en inglés.
- Colección de vídeos de Tor: Tor media

Prensa

- Página de prensa de Tor, actualizada: Tor Press and Media Information
- Tor: The king of high-secure, low-latency anonymity: Documento filtrado por Snowder sobre la investigación de la NSA a la red Tor
- Tor Stinks: Documento Powerpoint de la NSA acerca de Tor
- Glenn Greenwald: columnista elegido por Snowder para filtrar sus documentos.
- Attacking Tor: how the NSA targets users' online anonymity: Identificación de usuarios Tor mediante la explotación de vulnerabilidades del navegador Firefox
- La anonimicidad y la red Tor: Es una traducción del artículo Anonymity and the Tor Network publicado por Bruce Schneier en su blog. Habla del funcionamiento de Tor, resaltando que Tor solo anonimiza sin proporcionar privacidad.
- NSA report on the Tor encrypted network: Es un documento, publicado por The Washington Post, encargado por la NSA. Describe la características técnicas de Tor y propone una serie de posibles ataques teóricos y prácticos con la red, algunos de los cuales los ha llevado a cabo según revelaciones de los documentos filtrados por Snowden. Además propone una adatación del protocolo, inditiguible de la original, para permitir a la NSA reunir información dentro de la red Tor.

Presentaciones

- Design of a blocking-resistant anonymity system (pdf)
- How governments have tried to block Tor (pdf)

Bibliografía científico-técnica

- Please slow down!: the impact on tor performance from mobility, caso de estudio que le permite comprobar el rendimiento de Tor en dispositivos móviles con Orbot.
- How China Is Blocking Tor: este trabajo investiga como China implementa los posibles mecanismos de bloqueo de la red Tor y contramedidas propuestas.
- Información para reproducir el experimento anterior
- Design of a blocking-resistant anonymity system
- Hiding Routing Information (1996)

- Tor: The Second-Generation Onion Router (2004): citado por 2027 artículos
- Anonymity Loves Company: Usability and the Network Effect (2006): antiguo pero importante reflexión de usabilidad (de los otros) frente a seguridad (la tuya).
- Compromising Tor Anonymity Exploiting P2P Information Leakage (2010): Un ataque sencillo contra Tor por el uso de Bittorrent sobre Tor
- StegoTorus: a camouflage proxy for the Tor anonimity system (2012)
- SkypeMorph: protocol obfuscation for Tor bridges (2012)
- Challenges in deploying low-latency anonymity (draft): detalles de las experiencias más recientes y del futuro de Tor
- Performance Improvements on Tor or Why Tor is slow and what we're going to do about it: Describe los problemas que causan la lentitud de Tor y los pasos para solucionarlo.