



Universidad Nacional
ARTURO JAURETCHE

Seguridad de la Información

TP Final

Salvatori Emiliano

Julio del 2020

Índice

| | |
|--|-----------|
| 1. Objetivos | 3 |
| 2. Resumen | 3 |
| 3. Introducción | 3 |
| 4. Anonimato | 3 |
| 4.1. ¿Por qué el anonimato? | 4 |
| 4.2. La gran muralla de fuego China | 4 |
| 4.3. El país de la libertad | 5 |
| 4.4. La seguridad en casa | 5 |
| 5. El camino posible | 6 |
| 5.1. La redes de Baja Latencia | 6 |
| 5.2. Enrutamiento de tipo cebolla | 7 |
| 5.3. TOR | 8 |
| 6. Algunos problemas con el anonimato | 9 |
| 6.1. Ataques basados en complementos | 10 |
| 6.2. Ataque Torben | 11 |
| 6.3. Fuga de información 2P | 11 |
| 6.4. Ataques basados en tiempo | 11 |
| 6.5. Ataques mediante el predecesor | 12 |
| 6.6. Ataques mediante Servidores ocultos | 12 |
| 6.7. Ataques de reloj sesgado | 12 |
| 7. Siendo anónimo | 13 |
| 7.1. Descarga | 13 |
| 7.2. Configuración y arranque | 14 |
| 8. Conclusiones | 15 |
| Bibliografía | 16 |

1. Objetivos

En el siguiente Trabajo de Investigación para la materia **Seguridad de la información Comisión nº 1**, se abordará la seguridad en Internet provista por la red TOR (*The Onion Router*), cómo funciona, las características provistas por el servicio, y las posibles vulnerabilidades a tener en cuenta.

2. Resumen

Las libertades de expresión y albitrio generalmente se consideran pilares esenciales de la libertad civil. Internet planteó desde sus comienzos, una cuestión particularmente espinosa tanto para aquellos que desean expresarse libremente y hacer uso de su libre albedrío, como para aquellos que buscan suprimir tales actividades. Por un lado, Internet proporciona un medio de comunicación que conecta instantáneamente dos puntos cualesquiera en el globo; y, sin embargo, entre los puntos finales de esa comunicación existen muchas vulnerabilidades explotadas por quienes se interesan por acallar o amainar las voces disidentes, haciendo uso de varios métodos: ataques legales, ataques de denegación de servicio, ataques fuera de línea contra participantes, etc.

En un intento por proporcionar el anonimato necesario para garantizar estas libertades, se han realizado investigaciones en el área del enrutamiento anónimo bajo Internet. El objetivo de estos sistemas es ocultar los puntos finales de una comunicación en la red de un posible intruso. Este trabajo intenta realizar un resumen sobre las formas de ocultamiento que proporciona TOR, sus flaquezas y una mirada hacia el futuro de Internet

3. Introducción

La comunicación secreta ha existido durante casi toda la historia de la civilización humana: Julio César usó su cifrado homónimo para enviar mensajes a sus generales. El cifrado se ha vuelto útil para proteger el contenido de los mensajes secretos, pero no puede ocultar la identidad de las partes que se comunican. A menudo, el hecho de que determinados ciudadanos o entidades intercambien información (independientemente de su contenido) es una preocupación importante de seguridad, como por ejemplo, aquellos ciudadanos bajo gobiernos opresivos que navegan por sitios web sobre democracia [Véase la sección 4.2].

4. Anonimato

Se pueden identificar tres clases de anonimato:

1. El anonimato del remitente, el cual indica la incapacidad de cualquier parte que no sea el remitente para deducir la fuente de un mensaje.

2. El anonimato del receptor, que indica la incapacidad de cualquier parte que no sea el destinatario para deducir el destino de un mensaje.
3. El anonimato entre remitente y el receptor, que refiere a la idea que, si bien es posible deducir que dos partes están utilizando el mismo sistema, no es posible deducir que lo están utilizando para comunicarse entre sí.

El anonimato generalmente se aborda en relación con el tamaño de la red de quienes lo emplean: es decir, el conjunto de entidades que podrían haber enviado o recibido una comunicación particular. Un usuario tiene más anonimato si el grupo bajo el que se encuentra utilizando el mismo método de encriptación, es grande y menos si el grupo es pequeño. Por lo tanto, es tarea del atacante minimizar el tamaño del conjunto de anonimato; y es trabajo del diseñador del sistema y del usuario maximizarlo.

Algunos describen ¹ el anonimato como un proceso continuo que indica la probabilidad con la que un atacante puede hacer coincidir con precisión una comunicación particular con un remitente.

Las necesidades de anonimato de un usuario en particular podrán variar según la situación: a veces un usuario puede requerir su inocencia, y otras veces se hará necesario el anonimato fuera de toda sospecha delictiva.

4.1. ¿Por qué el anonimato?

Se podría argumentar que el cifrado de mensajes proporciona protección suficiente en Internet, y que ofuscar tanto la fuente como el destinatario del tráfico es excesivo. Sin embargo, esto no es así, dada la relativa facilidad con la que los usuarios generalmente pueden ser vinculados a las direcciones IP, y la naturaleza potencialmente sensible de algunos sitios web.

4.2. La gran muralla de fuego China

Pongamos un ejemplo en concreto sobre la utilidad del anonimato en la red: La gran muralla de fuego de China.

La red de redes llegó a China en 1994 pero ya en 1997, antes de que se masificara, el Ministerio de Seguridad Pública (no el de Educación o el de Tecnología), responsable de regularla, comenzó a buscar la forma de reducir la cantidad de información filtrada. Para lograrlo limitó a solo tres la cantidad de conexiones con el exterior (o IXP), por donde podía fugarse datos sensibles del gigante asiático. Por eso los no menos de 500 millones de usuarios chinos de internet utilizan solo tres "ventanas" hacia el mundo, las cuales están permanentemente monitoreadas.

Así fue que se desarrolló la muralla de fuego que encierra todo el país, no tanto para protegerlo de ataques externos, como para encerrar a sus ciudadanos y que no accedan a la información políticamente sensible que existe en el mundo. Más que una muralla de protección, es una cárcel virtual que, además, permite rastrear permanentemente la actividad de los ciudadanos en la red, filtrándola o bloqueándola. La muralla de fuego

¹Para mayor información, consultar: Michael Reiter y Aviel Rubin. *Anonymity for web transactions. Transactions on Information and System Security*, Junio 1998

también permite saber realmente, con nombre y apellido quién navega por internet. Hasta los cybercafés de ese país deben registrar a sus usuarios, además de controlar qué sitios visitan[4].

4.3. El país de la libertad

Si bien China es uno de los casos más evidentes de sesgo de la libertad de expresión, como también lo puede ser Corea del Norte; no hay que olvidar el caso más emblemático: Estados Unidos.

Actualmente, buena parte de los cables de fibra óptica del mundo pasan por el gigante norteamericano, de la misma manera que antes los caminos conducían a Roma, la ciudad más poderosa de aquel imperio romano. En este país se encuentra la columna vertebral de la red de redes por cuestiones históricas y técnicas[4]. Esta particular distribución de las redes no es ingenua ni sus consecuencias solo económicas. Julian Assange, el fundador de Wikileaks lo explicaba de la siguiente manera: "El nuevo gran juego no es la guerra por los oleoductos. Es la guerra por los caños de internet: el control sobre los recorridos de los cables de fibra óptica que se distribuyen por el lecho marino y la tierra. El nuevo tesoro global es el control sobre el enorme flujo de datos que conectan continentes y civilizaciones linkeando la comunicación de miles de millones de personas y organizaciones"²

El anillo que se encuentra alrededor de nuestro continente nos conecta con el resto del mundo, y este anillo, a su vez, es gestionado desde Miami, en los Estados Unidos, por lo que prácticamente todas las comunicaciones que realizamos pasan por ese país. Es por ello que si queremos enviar un mail a nuestro vecino, utilizando por ejemplo algún servicio de mail gratuito, como puede ser Gmail, según lo dispuesto por la topología de la red, el mail viajará desde nuestra casa, saldrá por el anillo de latinoamérica, y caerá en algún servidor alojado en los Estados Unidos, para luego ser redireccionado nuevamente hacia Argentina, llegando a la casa de nuestro vecino. Esta topología, entre otras cosas permite espiar de manera sutil a todo nuestro continente, como sucedió con el famoso caso de la mandataria de nuestro país vecino, Dilma Rousseff.³

4.4. La seguridad en casa

También hay usos para utilizar el anonimato de redes en una escala mucho menor. Considere la situación en la que un usuario doméstico desea visitar un sitio web relacionado con temas delicados tales como enfermedades terminales, o preferencias sexuales. Es muy probable que dicho usuario prefiera que otros no sepan de estas visitas; pero aún así, la arquitectura de muchas redes residenciales es tal que todo el tráfico es visible para muchos otros clientes. Aunque el cifrado evitará que un vecino entrometido vea el contenido real transferido, una simple búsqueda de DNS a menudo

²Assange, Julian "How Cryptography is a Key Weapon in the Fight Against Empire States" The Guardian, 9/7/2013. <http://www.theguardian.com/commentisfree/2013/jul/09/cryptography-weapon-fight-empire-states-julian-assange> [consultado en julio de 2020]

³Nepomuceno, Eric "Espiar a Dilma no le salió gratis a Washington", Página 12, 22/12/2013. <https://www.pagina12.com.ar/diario/elmundo/4-236223-2013-12-22.html> [consultado en Julio 2020]

revelará el sitio web desde el que se originan las páginas. Quizás de forma más insidiosa (incluso con el cifrado), el operador del sitio web sabe qué direcciones IP están accediendo a su contenido y puede vincular a personas específicas con actividades específicas en el sitio. Tampoco hay que olvidar que todos los proveedores de internet tienen la posibilidad de vincular las direcciones IP de los usuarios con las páginas o sitios que visitan.

Para entender la problemática latente, en un país con una tradición bastante irregular en materia de respeto por los derechos humanos como el nuestro, ¿qué podrían hacer las fuerzas represivas con ese tipo de información durante la dictadura?[4]; o quizás aún mucho más cercano a nuestro tiempo: ¿Acaso en los últimos gobiernos no han habido decenas de denuncias sobre escuchas a determinados personajes claves en lo que respecta a las áreas económico y político del país? ⁴ ¿Acaso la ley no establece ninguna sanción para aquellos que detentan el poder de turno? ⁵

Ante este vacío (¿o también "vicio"?) por parte de los gobiernos, es que se precisan herramientas que permitan reivindicar las libertades y es aquí donde entra en juego Tor.

5. El camino posible

Como hemos visto, ya no sólo es de total trascendencia encriptar el mensaje entre el emisor y el destinatario, sino que también es de suma importancia borrar las huellas por donde el mensajero ha transitado, como también el camino a proseguir hasta concluir su tarea de emisario.

A continuación veremos de manera concisa, las formas en que se pueden abordar esta problemática.

5.1. La redes de Baja Latencia

En general, las redes de comunicación anónimas se pueden dividir en dos categorías principales; **Redes de Comunicación Anónimas de Alta Latencia** en las que el mensaje tarda un tiempo relativamente más largo en viajar a través de la red y llegar a su destino, (cuyo tiempo suele oscilar entre unas pocas horas y varios días). Este retraso es tolerable cuando se utiliza para aplicaciones no interactivas como el correo electrónico por ejemplo, sin embargo, hoy en día la mayoría de las aplicaciones en Internet son aplicaciones interactivas en tiempo real que requieren de una baja latencia, como por ejemplo la navegación web, acceso a shell de forma remota o comunicaciones basadas en IRC.

Por otro lado, los sistemas diseñados para proporcionar anonimato y bajas latencias cuando se usan aplicaciones interactivas en tiempo real se denominan **Redes de Comunicación Anónimas de Baja Latencia**.

⁴<https://www.pagina12.com.ar/276241-el-juez-federico-villena-fue-apartado-de-la-causa-por-el-esp>
[Consultado en Julio 2020]

⁵<https://www.pagina12.com.ar/201902-escuchas-un-anuncio-sin-grandes-consecuencias> [Consultado en Julio 2020]

En este trabajo, abordaremos éstas últimas mediante la red TOR, sin dejar de mencionar que existen otros proyectos similares, como por ejemplo *Invisible Internet Project* (I2P) ⁶, o el teorizado Tarzan ⁷, siendo la primera, una de las que actualmente se encuentran entre las comunicaciones anónimas de baja latencia más utilizadas.

5.2. Enrutamiento de tipo cebolla

Un enfoque para lograr bajas latencias y, al mismo tiempo, protegernos contra ataques foráneos, es el enrutamiento bajo el diseño en capas (cuya semejanza es la de las capas de una cebolla, de ahí proviene el epíteto de *cebolla*), el cual es posiblemente el más predominante hoy en día en Internet. La misma, es una red de superposición distribuida y diseñada para volver anónimas las aplicaciones basadas en TCP. Según expertos, "el doble objetivo del enrutamiento en capas es, por un lado, dificultar el análisis del tráfico para cualquier intruso, protegiendo la comunicación (y desvinculándola de los que participan en ella) de terceros, ajenos a la comunicación; y en segundo lugar, proteger las identidades tanto del receptor como del emisor".[2]

La forma en que funciona el *enrutamiento cebolla*, es mediante un conjunto de servidores llamados Onion Routers (de aquí en más OR), los cuales se utilizan para retransmitir mensajes. Cada OR mantiene un par de claves, tanto privada como pública, siendo la parte pública la que debe ser conocida por todos los clientes que deseen participar en la red.

Los clientes eligen una secuencia ordenada de OR que utilizarán para transmitir sus datos y establecer un circuito, es decir, un túnel bidireccional. Este método se denomina *cifrado de tipo cebolla*. Cada capa contiene una clave simétrica, una etiqueta e información de direccionamiento sobre el siguiente OR. Los mensajes enviados a través del circuito también están encriptados mediante éste método cebolla, pero esta vez usando la clave simétrica de cada OR. Cada uno de estos solo puede eliminar la capa de cifrado correspondiente y reenvía el mensaje al siguiente OR. Sólo el último OR en el todo el camino, puede reenviar el mensaje a su destino.

La respuesta potencial del receptor se envía al último OR en el circuito y se retransmite al remitente a través del mismo camino que se utilizó por vez primera. En esta ocasión, cada OR agrega una capa de cifrado al mensaje. Por lo tanto, se construye otro mensaje cifrado de tipo cebolla que solo el remitente puede descifrar, recuperando así el mensaje.

Un hecho importante con respecto al anonimato y la seguridad es que solo el primer OR de un circuito conoce la dirección IP del cliente, y solo el último OR conoce al receptor de un mensaje. Todos los OR intermedios solo conocen a su predecesor y su sucesor, sin siquiera saber qué otros OR están participando en el circuito. Se puede usar un recorrido para retransmitir múltiples mensajes desde una sola aplicación, pero cada flujo TCP necesita su propio itinerario.

⁶"The invisible Internet Project", <https://geti2p.net/en/> [consultado en Julio de 2020]

⁷"Tarzan: A Peer-to-Peer Anonymizing Network Layer", <https://www.cs.princeton.edu/~mfreed/docs/tarzan-ccs02-slides.pdf> [consultado en Julio de 2020]

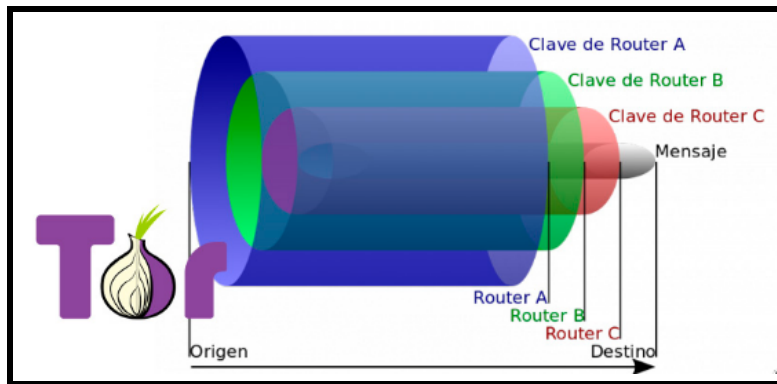


Figura 1: Metodo de cifrado de un mensaje bajo TOR

5.3. TOR

Tor es una red de comunicación anónima de baja latencia basada en circuitos de confianza distribuida. Su diseño se funda en el enrutamiento de tipo cebolla, pero realiza varias modificaciones y mejoras con respecto a la seguridad, la eficiencia y la capacidad de implementación.

La red Tor es una red superpuesta que utiliza un conjunto de servidores voluntarios, llamados, como se especificó anteriormente, Onion Routers (OR), que utiliza para construir los circuitos y mediante estos, transmitir los mensajes. Cada usuario ejecuta un software denominado *Onion Proxy* (OP) que gestiona todos los procesos relacionados con Tor, por ejemplo, estableciendo circuitos o manejando conexiones desde aplicaciones de usuario. Para construir un camino, el OP selecciona un conjunto ordenado de usualmente tres OR del conjunto de todos los OR conocidos.

El primer OR del conjunto se llama Guardia de Entrada, el último se llama Enrutador de Salida y todos los demás se llaman Enrutadores Intermedios. El proceso de selección de cada OR para un determinado recorrido se llama Selección de Nodo. Para obtener una lista de todos los OR conocidos, se utiliza un conjunto de servidores de tipo *directory authority*.

Después de seleccionar un conjunto de OR, el OP contacta al Guardia de Entrada y construye un circuito con este (Figura n° 2). El circuito recién creado se usa para contactar al siguiente OR para diagramar el camino que recorrerá el mensaje.

Este procedimiento se repite iterativamente hasta que todos los OR del conjunto formen parte del circuito, y una vez confeccionado el camino, se puede utilizar para transmitir los mensajes de forma anónima (Figura n° 3). Los mensajes están encriptados mediante el método cebolla y solo el enrutador de salida puede acceder y reenviar un mensaje a su destino.

Se puede objetar que el mensaje enviado por el Enrutador de Salida a Bob, no está encriptado (Figura n° 3). Esto en verdad se encripta con de la misma forma que se explicó en la sección 5.2, sólo que para que se realice de manera exitosa, requiere una explicación más detallada de la *Encriptación de tipo cebolla* que aquí por razones de

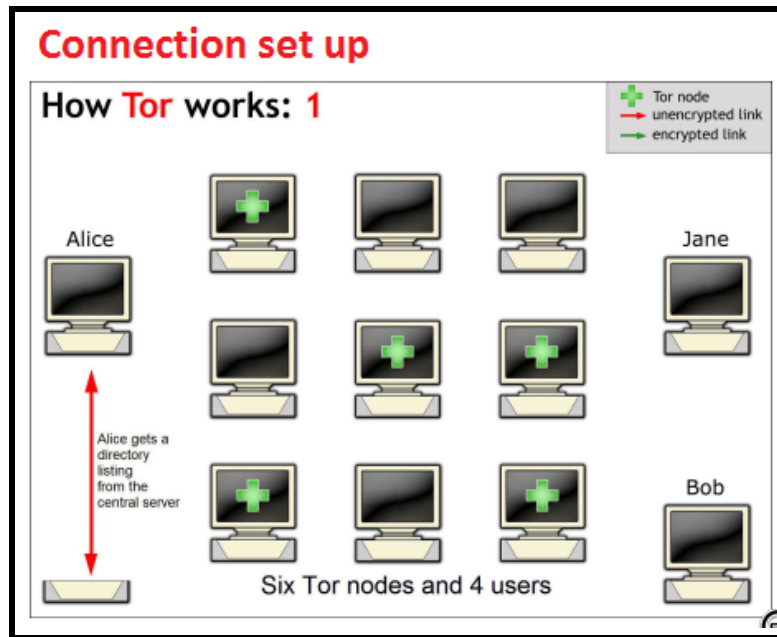


Figura 2: Configurando la conexión mediante un cliente y el servidor central

espacio de deberá de obviar.⁸

Procederemos a evidenciar algunas de las vulnerabilidades que deben enfrentar tanto los desarrolladores, como los usuarios de la red cebolla ante la navegación anónima.

6. Algunos problemas con el anonimato

Los routers de tipo cebolla, implementan una estrategia de mezcla muy cercana al método FIFO (Primero en Entrar-Primero en Salir), para proporcionar baja latencia. Esto hace que este enrutamiento sea susceptible a una serie de ataques, ya que la falta de tráfico de cobertura, permite que algún posible atacante pueda usar técnicas de análisis de tráfico y de tiempo real para monitorear determinados patrones en el tránsito de información, seguir el flujo de mensajes e identificar las partes que se comunican. Esencialmente hay dos clases principales de ataques que apuntan a la red Tor: ataques de análisis de tráfico, y ataques DoS. Siendo el objetivo principal de todos ellos, visibilizar el recorrido trazado por cada nodo y de esta manera, poner de manifiesto cada las partes que participan de la comunicación.

No obstante, el enrutamiento de cebolla es un diseño prometedor para proporcionar una red de comunicación anónima de baja latencia y muchos sistemas utilizados

⁸Sin embargo, se puede remitir a R.Dingledine, N. Mathewson, and P. Syverson, "Tor: The second-generation onion router", DTIC Document, Tech. Rep., 2014

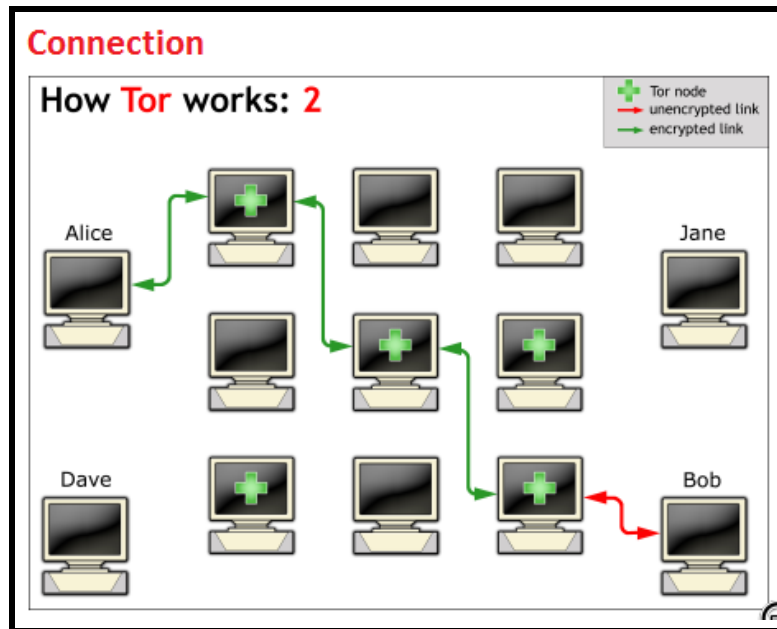


Figura 3: Diagramando el circuito entre los distintos nodos

actualmente se basan en este diseño. A continuación se resume de forma muy concisa los tipos de ataques perpetrados contra la red Tor.

6.1. Ataques basados en complementos

Estos ataques son dirigidos al usuario a través del navegador de Internet que adopta para navegar en la red. Estas aplicaciones hacen uso de software externo que se encuentra conectado al navegador (llamados comúnmente *complementos*), como puede ser por ejemplo: Flash, Java y controles ActiveX.

Estas aplicaciones se ejecutan como software separado del navegador, siendo ejecutados con permisos de usuarios en el sistema operativo. Algunas de estas tecnologías, como Java o Adobe Flash, por ejemplo, se ejecutan en máquinas o marcos virtuales apropiados sin pasar por los ajustes de configuración de proxy adoptados por el navegador Tor, por lo que se comunican directamente en la red de Internet, sin utilizar el ecosistema Tor. Los ataques al navegador pueden implementarse abordando diferentes enfoques. A continuación listamos dos de ellos:

- Operando en un servidor público de Internet contactado por el cliente, a través de un servidor malicioso que introduce, por ejemplo, el contenido adulterado de Adobe Flash en la página web.
- Adoptando un nodo de salida maligno, interceptando las comunicaciones de los usuarios en canales no encriptados (por ejemplo, conexiones HTTP no seguras) e introduciendo el contenido relacionado con complementos maliciosos.

Debido a la posible exposición de la identidad de los clientes derivada del uso de complementos del navegador, como lo sugieren los navegadores anónimos, dichas tecnologías, a menudo deshabilitadas por defecto, deben evitarse para comunicarse en la red de cebolla de forma anónima y segura.

6.2. Ataque Torben

El ataque Torben tiene como finalidad el identificar un cliente Tor, manipulando páginas web para obligar al usuario a acceder a contenido de fuentes no confiables y explotando las características de baja latencia de las redes de anonimización para inferir indicadores de las páginas web que se transmiten, por lo tanto recuperar información en las páginas web que el cliente visita a través de Tor.

6.3. Fuga de información 2P

Este tipo de ataque se lleva a cabo con el fin de evidenciar a los clientes de Tor mediante la explotación de sus conexiones de tipo punto a punto. De hecho, considerando, por ejemplo, el protocolo BitTorrent, es posible que un usuario malintencionado recupere la dirección IP de un cliente que se conecta a través de Tor para comunicarse con el rastreador de torrent.⁹

El atacante utiliza en este caso, el hecho que aunque la lista de rastreadores se puede recuperar de forma anónima a través de Tor, las conexiones P2P a menudo se logran de manera insegura, comunicándose directamente con el par. Por lo tanto, es posible que el atacante explote, mediante la técnica *Hombre en el Medio*, de la red Tor para alterar el contenido de la lista devuelta por el rastreador de torrent, al incluir en la lista la dirección IP de un par de torrent malicioso. Dado que la comunicación con dicho par no se establecería a través de Tor, es posible que el atacante recupere la dirección IP del cliente que origina la solicitud al rastreador.

6.4. Ataques basados en tiempo

Poco tiempo después del despliegue masivo de Tor, algunos especialistas sobre seguridad, hicieron público un método por el cual los usuarios de la red podrían sufrir degradaciones en el anonimato. En este tipo de ataques, un atacante pasivo¹⁰ (que sólo monitorea la red) podría intentar establecer una relación entre el tráfico que ingresa y el que sale de una red anónima para vincular un emisor y un receptor. Como se explicó anteriormente, cuanto más sean los participantes de la red, esto genera alguna latencia en las demás conexiones anónimas.

Un servidor web malicioso, podría por ejemplo, interferir el mapa completo de un cliente al obtener una lista de todos los nodos Tor y caracterizar su rendimiento midiendo los efectos de los circuitos creados a través de cada nodo (recordar que Tor

⁹Un rastreador de torrents es un servicio de red en el que el cliente debe comunicarse para recuperar información sobre la lista de pares capaces de compartir el recurso solicitado. La información de pares se proporciona como pares de dirección IP y puerto de escucha.

¹⁰Si este adversario particular es o no una preocupación práctica es un tema de debate; Tor asume que no y sistemas como Tarzán aplicaban una política de creación de circuitos que intencionalmente difundía un camino entre distintos dominios, disminuyendo de esta manera, la posibilidad de tal ataque.

es una red de ruta libre en que el iniciador define toda la ruta). Por lo tanto, cuando un cliente se conecta, el servidor web puede medir nuevamente la latencia a través de cada nodo Tor y observar cuáles han aumentado, lo que indicaría un circuito adicional.

6.5. Ataques mediante el predecesor

Algunos autores suponen que el iniciador de una conexión anónima mantendrá esa conexión aún cuando se presenten modificaciones en la topología de red. Son estas modificaciones las que son clave para el atacante. Los nodos maliciosos se dispersan en la red y como serán elegidos al azar por el protocolo que establece la topología, entonces es posible rastrear el emisor. Recordemos que naturaleza de IP es tal que un nodo conoce a su predecesor en el circuito. Estadísticamente, el iniciador del circuito será el predecesor de todo el circuito a lo largo del tiempo; dadas suficientes reformas en el circuito, el atacante podría adivinar con certeza razonable qué nodo es el iniciador.

6.6. Ataques mediante Servidores ocultos

Similar al ataque anterior, es un método utilizado para exponer Servidores Ocultos en la red Tor. Su ataque es capaz de identificar una máquina que ejecuta un servicio oculto en cuestión de minutos, utilizando solo un nodo malicioso. Este tipo de vulnerabilidades hizo que algunos especialistas propongan algunas modificaciones a la red Tor para mitigar esta vulnerabilidad.

Un usuario que desee localizar un servidor oculto primero debe convertirse en miembro de la red de enrutamiento Tor. Una vez en su lugar, este nodo malicioso realiza conexiones continuas a la red Tor, cada uno en un intento de convertirse en el nodo más cercano al servidor, entre este y el punto de encuentro. El atacante puede estudiar y relacionar patrones de tráfico tanto como circuito y como atacante, e identificar si su instancia de nodo de enrutamiento se encuentra en el circuito entre el servidor oculto y el punto de encuentro.

Para neutralizar este tipo de ataques, los especialistas han presentado un sistema de nodos de guardia, en el que el servidor oculto utiliza varios puntos de entrada diferentes pero fijos a la red de anonimato. Pero aún así, esto suma complicaciones al entramado de nodos, por lo que no parece ser una solución definitiva, quedando abierta la problemática a distintos abordajes.

6.7. Ataques de reloj sesgado

Se describe un ataque mediante esta técnica en el que un usuario externo malintencionado genera exceso de procesamiento en un Servidor Tor con la intención de elevar la temperatura del procesador, alterando así las características operativas de su reloj de manera que se pueda detectar esta injerencia en los paquetes de red que emite la máquina. Es un enfoque muy interesante similar a un canal secreto, aunque requiere que el atacante detecte el tráfico saliente en todos los servidores Tor potenciales, lo que puede ser un requisito poco realista.

7. Siendo anónimo

Como se explicó en la sección 4.4 es necesario que se disponga de medios por los cuales cualquier ciudadano (sin importar sus conocimientos técnicos) haga valer sus derechos civiles como la libertad de expresión, es necesario que se garanticen determinadas protecciones como el rastreo, la vigilancia y la censura. Para ello la red Tor dispone de una configuración sencilla para comenzar a navegar por internet de forma anónima. A continuación se indican los pasos a seguir para hacer uso de la red Tor.

7.1. Descarga



Figura 4: Seleccionando las plataforma GNU/Linux para la descarga

Como primer paso, será necesario dirigirse a la página oficial de descarga del proyecto Tor ¹¹ y una vez en ella, elegir la plataforma bajo la que se ejecutará el navegador. Se disponen hasta el momento de este escrito, cuatro plataformas posibles estables, como también la posibilidad de descargar el código fuente y de probar otras plataformas experimentales, donde ejecutar Tor:

1. Windows
2. OS X
3. GNU/Linux
4. Sistemas Android
5. Código Fuente

¹¹<https://www.torproject.org/es/download/>

6. Plataformas experimentales

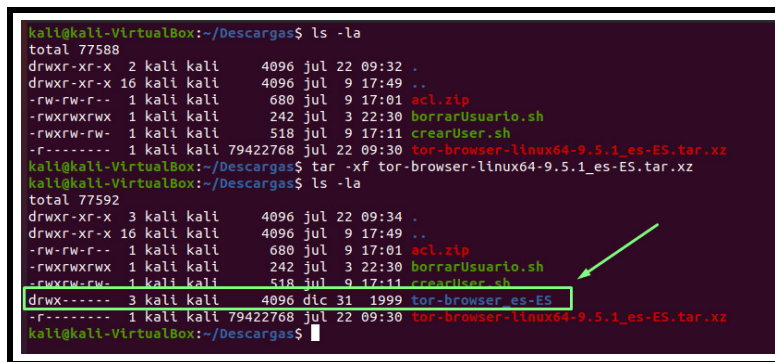
En este trabajo se abordará la plataforma GNU/Linux. Se procede a seleccionar la plataforma como muestra la Figura 4. Una vez que seleccionamos esto, nos descargará un archivo de tipo *tar.xz*.

7.2. Configuración y arranque

Una vez obtenido el paquete de extensión *tar.xz* será necesario desempaquetarlo mediante la aplicación de línea de comando *tar* junto con la opción '-xf'¹²

Una vez desempaquetado el archivo descargado, se puede observar que contiene un directorio y un ejecutable de extensión *.desktop*.

Para ejecutar este último será necesario ingresar el comando tal y como se puede visualizar en la Figura 5



```
kali@kali-VirtualBox:~/Descargas$ ls -la
total 77588
drwxr-xr-x 2 kali kali 4096 jul 22 09:32 .
drwxr-xr-x 16 kali kali 4096 jul 9 17:49 ..
-rw-rw-r-- 1 kali kali 680 jul 9 17:01 acl.zip
-rwxrwxrwx 1 kali kali 242 jul 3 22:30 borrarUsuario.sh
-rwxrwxrwx 1 kali kali 518 jul 9 17:11 crearUser.sh
-r----- 1 kali kali 79422768 jul 22 09:30 tor-browser-linux64-9.5.1-es-ES.tar.xz
kali@kali-VirtualBox:~/Descargas$ tar -xf tor-browser-linux64-9.5.1-es-ES.tar.xz
kali@kali-VirtualBox:~/Descargas$ ls -la
total 77592
drwxr-xr-x 3 kali kali 4096 jul 22 09:34 .
drwxr-xr-x 16 kali kali 4096 jul 9 17:49 ..
-rw-rw-r-- 1 kali kali 680 jul 9 17:01 acl.zip
-rwxrwxrwx 1 kali kali 242 jul 3 22:30 borrarUsuario.sh
-rwxrwxrwx 1 kali kali 518 jul 9 17:11 crearUser.sh
drwx----- 3 kali kali 4096 dic 31 1999 tor-browser-es-ES
-r----- 1 kali kali 79422768 jul 22 09:30 tor-browser-linux64-9.5.1-es-ES.tar.xz
kali@kali-VirtualBox:~/Descargas$
```

Figura 5: Se desempaqueta el archivo, creando el directorio principal

Una vez logrado esto, es posible navegar de forma anónima, teniendo en cuenta algunas peculiaridades de la red y las posibles vulnerabilidades que se trataron en la sección 6.

Como se puede observar en la Figura nº 6 es necesario ejecutar el programa mediante línea de comando. Una vez realizado esto, se puede optar entre configurar la conexión de una forma más avanzada o simplemente establecer la conexión con los nodos. Como se explicó en la sección 5.2, una vez que se solicita conectar con la red que nos proporcionará el anonimato, es necesario que la misma genere un circuito con los nodos disponibles. Establecida una vez la topología, se nos proporciona el navegador de tipo Firefox, el cual se encuentra preparado exclusivamente para resguardar cualquier invitación a revelar nuestra identidad en Internet. Esto se puede visualizar en la Figura nº 7

¹²Para mayor información, dirigirse a la página del manual: <https://linux.die.net/man/1/tar>

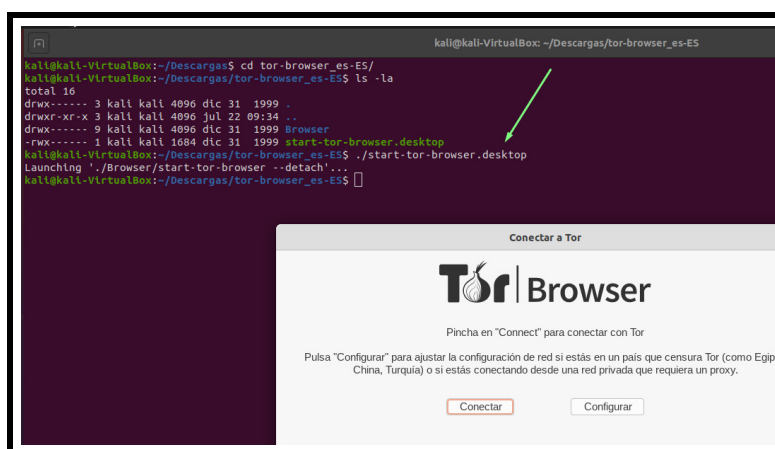


Figura 6: Se ejecuta el programa mediante la línea de comando

8. Conclusiones

En este informe, se proporcionó un acercamiento superficial al método de enrutamiento de tipo cebolla, sistema de comunicación anónima y de baja latencia, como así también se pasaron lista de las vulnerabilidades existentes y documentadas por especialistas, finalizando con un pequeño paso a paso para comenzar a navegar de forma anónima en Internet.

Si bien Tor es el sistema más popular y utilizado en este momento, existen otras arquitecturas de red, que proveen el mismo servicio de anonimato, como puede llegar a ser I2P, el cual es un competidor de rápido crecimiento. Ambos sistemas se actualizan constantemente para mejorar el rendimiento y proporcionar un mejor anonimato a la vez que protegen contra posibles atacantes. Tor, debido a su mayor conciencia en la comunidad académica, ya fue capaz de resolver problemas que otras arquitecturas tarde o temprano tendrán que enfrentar. Tor también se beneficia de una gran cantidad de estudios formales sobre su anonimato, resistencia a los ataques y rendimiento. Como se señaló anteriormente, la diferencia clave entre Tor y otros servicios del mismo estilo, es la forma en que se configura y se usan las conexiones virtuales, en términos de selección de nodos y su participación con el cliente.

En general, esta comparación entre mismos servicios de anonimato (pero con distintos abordajes técnicos) muestra que depende en gran medida del campo de aplicación para determinar qué sistema ofrece mejores resultados en términos de rendimiento y anonimato. Al navegar por la web pública, Tor sin duda ofrece un mejor rendimiento, mientras que I2P por ejemplo es casi inutilizable.

Aunque por otro lado, otros servicios proporcionan un anonimato más fuerte y un mejor rendimiento en comparación con Tor cuando se interactúa con servicios o usuarios dentro de la red. Al final, siempre es una compensación entre rendimiento y anonimato, sin importar qué sistema se use, aunque siempre se debe tener como meta final, la libertad individual de cada internauta dentro de un sistema de comu-

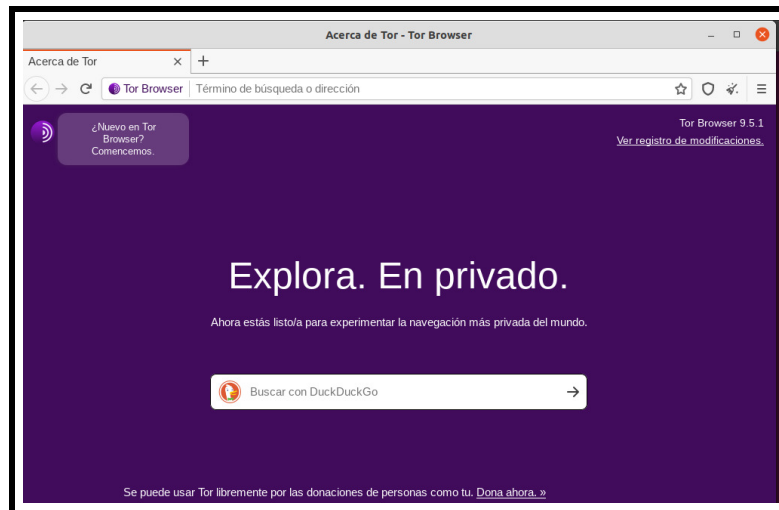


Figura 7: Navegador de tipo Firefox que permite la navegación anónima

nicación que resulta ser bastante desequilibrado e inequitativo, y aún mucho más en latinoamérica [4].

Bibliografía

- [1] Enrico Cambiaso y col. *Darknet Security: A Categorization of Attacks to the Tor Network*. Working Paper 2315. Genova, Italy: Consiglio Nazionale delle Ricerche (CNR-IEIT), 2017.
- [2] Bernd Conrad y Fatemeh Shirazi. *A Survey on Tor and I2P*. Working Paper 5694. Darmstadt, Germany: Department fo Computer Science, 2014.
- [3] Peter Johnson y Apu Kapadia. *From Chaum to Tor and Beyond: a Survey of Anonymous Routing System*. Working Paper 03755. Hanover: Department fo Computer Science, Dartmouth College, 2007.
- [4] Esteban Magnani. *Tension en la red*. Adruki, 2014.