

Anonimato En Internet

Integrantes:

Matias Lacasia

Stefano Valencia

Fecha: 06/09/13

Resumen

Hoy en día internet es el gran medio para transportar información, tanto personal, financiera, etc. Pero navegar en la red no es una actividad anónima y hay quienes buscan sacar provecho de ello capturando, bloqueando y/o falsificando la información. Existen métodos que permiten cierto grado de privacidad o anonimato en el uso del internet y algunos de los más conocidos serán abordados en este trabajo. En definitiva, si se quiere navegar de forma segura y sin que se rastreen los datos transmitidos al hacerlo, es necesaria una aplicación dedicada, pues por defecto, los protocolos usados comúnmente en internet no están preparados para hacerlo (hasta se puede decir que van contrarios a esto).

Introducción

Con el nacimiento de ARPANET a finales de los '60 y su posterior evolución a INTERNET ha hecho que la forma de comunicación cambiara y más aun con la creación de W.W.W. (World Wide Web). Hoy en día Internet está en cada aspecto la vida diaria, es más fácil acceder a la información de manera impersonal pero siempre queda registro de las conexiones en la red. Todo lo que se transmite en Internet puede archivarse o intervenir, es por ello que hoy se pueden escuchar palabras como "censura", "espionaje", "piratas informáticos" entre otros. Pero hay métodos para evitar lo anterior y en este trabajo se ha querido abordar los más conocidos, con el fin de poder navegar de forma "anónima".

Cada computador tiene un dirección MAC (dirección física asignada por el fabricante) y una dirección IP asignada por la red a la que está conectado, el enfoque de estos métodos de protección de identidad, está en ocultar la IP del computador del usuario (más bien, la IP del router del usuario, que es el que hace las conexiones al exterior), ya que gracias a NAT, la MAC del computador no se conoce fuera de la subred del router.

Los protocolos usados por estos programas en general son los mismos usados por conexiones no anónimas, es el uso creativo de estos protocolos, junto con técnicas de encriptación de datos y una distribución inteligente de redes, que se pueden llevar a cabo las diversas técnicas de anonimato usadas.

Soluciones Generalizadas

Servidores proxy

Una de las soluciones más generales encontrada para el problema del rastreo de la información (navegación anónima) es la de los servidores proxy, éstos consisten en servidores independientes a la red del usuario, que sirven como un intermediario entre un usuario y el servidor de destino al que éste desea ingresar (donde se puede encontrar una página web, base de datos, etc). El modo de funcionamiento es tal que el usuario envía al proxy la petición que va dirigida al servidor, y luego el proxy envía al servidor ésta petición en lugar del usuario, para recibir la respuesta y enviarla de vuelta al usuario. Lo importante de esto para el anonimato es que el servidor de destino considera al proxy como el origen de la petición (IP y MAC indicadas en paquetes), quedando así oculto el usuario. Existen servidores proxy de dos tipos, transparente y no transparente, el no transparente funciona de la manera anteriormente descrita, además de que no guarda registro del usuario que envió la petición, el proxy no transparente en cambio, no protege del anonimato completamente, pues puede requerir registrarse para usarlo, o enviar paquetes con headers indicando el usuario del que viene la petición. Es necesario mencionar que si bien el servidor de destino no sabe los datos del usuario, el proxy si los conoce, por lo que es necesario que éste proxy sea confiable, ya que no se posee anonimato hacia él. Algunas configuraciones encadenan servidores proxy de manera en que sólo el primer servidor conoce los datos del usuario.

Remailer

Un Remailer es un servidor que recibe un mensaje para un destinatario establecido, y lo redirige hacia éste, pero ocultando el remitente. Este sistema permite el envío de mails de manera anónima, y dependiendo del tipo de Remailer, es posible recibir respuesta por mail. Existen dos tipos de Remailer, está el Remailer anónimo, que envía mails sin remitente, conservando total anonimato pero sin permitir una respuesta del destinatario, y está el Remailer pseudónimo (o Nym), que una vez le llega el mensaje, le asigna un pseudónimo (una llave criptográfica) al remitente, y envía el mail con este pseudónimo como remitente, esto permite al destinatario responder el mail, indicando como destinatario al pseudónimo generado por el Nym, el cuál luego envía la respuesta a la dirección asociada al pseudónimo.

Aplicaciones disponibles

Freenet

Freenet es una aplicación P2P que permite compartir archivos de manera anónima, funciona como una red distribuida en el espacio, con los usuarios de la aplicación como nodos (identificados en la red por pseudónimos, que son creados aleatoriamente como llaves de encriptación) que tienen a disposición copias del archivo que se quiere descargar. Existen dos modos de uso, freenet permite conexiones con nodos adyacentes aleatorios, mientras que darknet implementa un sistema de amigos (nodos con los que previamente se intercambiaron claves encriptadas) en el que sólo se pueden conectar nodos confiables. Su funcionamiento consiste en que el usuario que busca un archivo, consulta a un nodo adyacente por éste, si no lo encuentra, éste procede a consultar a sus nodos adyacentes, hasta llegar al final de una línea de nodos, que como no encuentran el archivo responden negativamente, luego, el nodo en el que comenzó la línea, suponiendo que tiene más nodos adyacentes, busca en el siguiente, y así sucesivamente hasta encontrar el archivo, una vez se encuentra el archivo, éste se copia en el nodo anterior del camino de búsqueda y así hasta llegar al nodo que pidió el archivo. La ventaja de éste método de búsqueda y descarga es que cada nodo cree que el nodo que pidió el archivo es el nodo anterior, por lo que se desconoce que nodo pidió el archivo originalmente, siendo así la búsqueda anónima. El problema que tiene es que un nodo debe dar a conocer su información (IP, MAC, para generar el enlace) a los nodos adyacentes, por lo cual se debe tener confianza en la seguridad de éstos, también tiene problemas de velocidad en la descarga, ya que se debe copiar el archivo en cada nodo de la ruta de búsqueda.

I2P

I2P es un servicio de red anónimo, que consiste en una red superpuesta, con cada nodo siendo representado por un pseudónimo (llave criptográfica) y comunicándose con otro nodo por medio de túneles (creados por un método llamado “garlic routing”, en que se le solicita a un nodo adyacente que participe del túnel, y luego le pida a su nodo adyacente lo mismo, hasta 3 saltos) encriptados en entrada y salida, y que son del tipo outbound (túnel de salida) o inbound (túnel de entrada), conectándose un tipo outbound del nodo origen a un tipo inbound del nodo destino. Paquetes enviados tienen indicado el pseudónimo del nodo de origen (transmisión está basada en mensajes como IP) por lo que es posible rastrear el tráfico de un nodo, esto podría presentar un riesgo si nodos no fueran identificados por llaves de encriptación, pero éste sistema de pseudónimos permite comunicarse sin revelar la dirección IP del usuario. Al ser una red superpuesta con su propio protocolo de red y transporte (similar a TCP) y diseñada para que otro software pueda usarlo, existen diversas aplicaciones compatibles con I2P, incluyendo clientes de BitTorrent, IRC y Email.

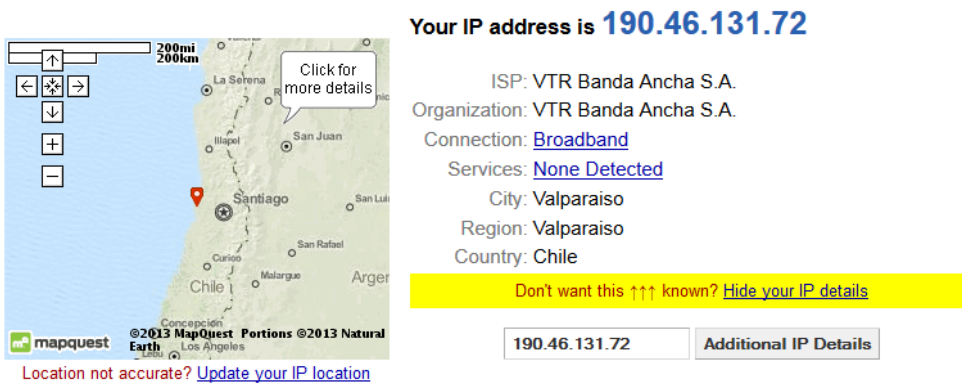
TOR

TOR consiste en una aplicación de la técnica llamada “Onion Routing” para anonimizar el tráfico web de los usuarios conectados a la “red TOR”, esto por medio de un browser que envía sus request a través de esta red hacia los servidores de la página web requerida, que pueden estar fuera o dentro de la red TOR (TOR hidden services). El funcionamiento de TOR consiste en tres etapas. Primero, para conectarse a la red TOR, el usuario debe obtener las direcciones IP (Y llaves públicas de encriptación) de los nodos de la red, esto lo hace conectándose a un servidor y descargando un directorio de nodos (siendo estos nodos escogidos aleatoriamente). En segundo lugar, el cliente de TOR escoge un camino aleatorio de nodos (deben ser 3: nodo de entrada, nodo de relay y nodo de salida) y comienza el método de Onion Routing, éste consiste en que el nodo origen se conecta al nodo de entrada enviándole un mensaje encriptado con su llave pública (disponible del directorio), que contiene una ID de circuito, una petición de establecer un circuito y su mitad de un intercambio de llaves, luego, el nodo de entrada responde en un mensaje desencriptado con su propia mitad del intercambio de llaves y con un hash de la nueva llave para que nodo de origen compruebe que comparten la misma llave, al recibir este mensaje, el nodo de origen y el nodo de entrada comienzan a encriptar todos sus mensajes con ésta llave privada, bajo esta conexión, el nodo origen le pide a nodo de entrada que extienda el circuito al nodo indicado (nodo relay), esto lo hace mandándole al nodo relay un mensaje (encriptado con la llave pública del nodo relay), que nuevamente incluye una ID de circuito, una petición del nodo de entrada para establecer un circuito, y la mitad de un intercambio de llaves del nodo de origen, nuevamente el nodo relay responde en un mensaje desencriptado con su propia mitad del intercambio de llaves y con un hash para comprobar la coherencia de éstas, estableciendo así un circuito entre el nodo de entrada y el nodo relay, luego, el nodo de entrada le envía al nodo de origen un mensaje de la extensión exitosa del circuito, junto con la llave que comparten ahora el nodo de origen y el nodo relay, luego, el nodo relay extiende el circuito de la misma forma hacia un nodo de salida (usando un mensaje de extensión de circuito enviado desde el nodo de entrada pero encriptado con la llave compartida entre nodo de relay y nodo de origen), y devuelve al nodo de origen la llave que ahora comparte con el nodo de salida (TOR usa 3 saltos, Onion Routing sirve para cuantos se desee), así queda armado el circuito, con los 3 nodos de la red teniendo una llave privada compartida con el nodo de origen, pero cada uno “pensando” que el nodo anterior es el nodo de origen (logrando así seguridad, ya que no se puede analizar donde comienza del circuito), además de cada nodo pasando mensajes desde un circuito al siguiente (usando las ID de circuito). La última etapa del funcionamiento es cuando el nodo de origen requiere un archivo HTML de un servidor, para esto, el nodo de origen envía un mensaje encriptado con su llave compartida al nodo de entrada, que indica pasar el contenido del mensaje al nodo siguiente (nodo relay), el

contenido del mensaje (ahora sin la encriptación origen-entrada) está encriptado con la llave origen-relay, y le indica al nodo relay pasar el contenido del mensaje al nodo siguiente (nodo de salida), el nodo de salida revisa el contenido, el que está encriptado con su llave compartida con el nodo de origen, y que indica que debe pasarle un request HTTP al servidor en cierta dirección. Una vez le llega el request al servidor, éste le envía el archivo al nodo de salida, que lo encripta con su llave compartida y envía al nodo relay, el cuál encripta el mensaje (ya encriptado con la llave origen-salida) con su propia llave compartida y lo envía hacia el nodo de entrada, que vuelve a encriptarlo con su llave y envía al nodo de origen, el cuál debe ahora desencriptar el mensaje usando las 3 llaves compartidas, por capas (de ahí el nombre Onion Routing). Este método de transmisión de datos asegura que la única IP abierta al público (en caso de que servidor no esté dentro de la red TOR) sea la del nodo de salida, mientras que hacia atrás los otros nodos (que pueden ser de una cantidad variable cuando es Onion Routing normal) están ocultos.

Resultados Prácticos

What Is My IP Address? (Now detects many [proxy servers](#))



Your IP address is 190.46.131.72

ISP: VTR Banda Ancha S.A.
Organization: VTR Banda Ancha S.A.
Connection: [Broadband](#)
Services: [None Detected](#)
City: Valparaiso
Region: Valparaiso
Country: Chile

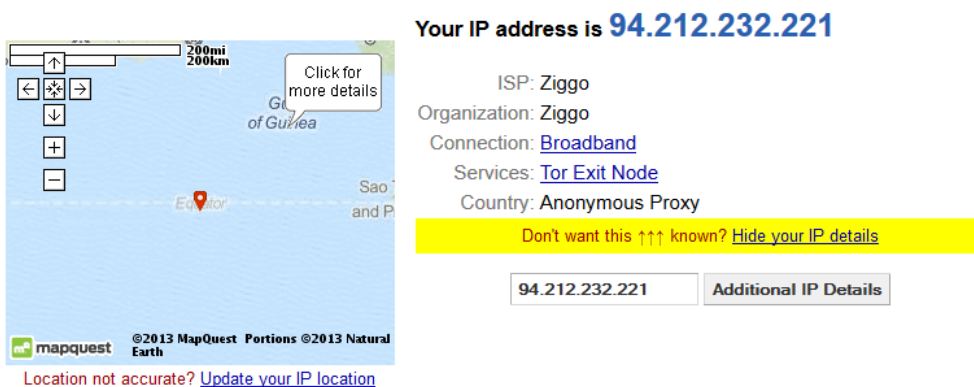
Don't want this ↑↑↑ known? [Hide your IP details](#)

190.46.131.72 [Additional IP Details](#)

Location not accurate? [Update your IP location](#)

Imagen 1: IP desde browser Mozilla Firefox

What Is My IP Address? (Now detects many [proxy servers](#))



Your IP address is 94.212.232.221

ISP: Ziggo
Organization: Ziggo
Connection: [Broadband](#)
Services: [Tor Exit Node](#)
Country: Anonymous Proxy

Don't want this ↑↑↑ known? [Hide your IP details](#)

94.212.232.221 [Additional IP Details](#)

Location not accurate? [Update your IP location](#)

Imagen 2: IP desde TOR browser.

Conclusiones

El anonimato para diversos usos de internet es posible mediante un diverso número de aplicaciones y técnicas, siendo el más complejo de los presentados Onion Routing. Si bien no existe un método de alcanzar anonimato absoluto (incluso TOR tiene vulnerabilidades en la estabilidad y cantidad de nodos, así como en los scripts que se puedan usar en el browser), se puede obtener buenos resultados para otorgar seguridad a la navegación, escogiendo la herramienta adecuada para lo que se quiera realizar.

Referencias

<http://www.elimparcial.es/tecnologia/el-problema-de-la-privacidad-en-internet-50150.html>

<http://www.wikipedia.org/>

<http://www.i2p2.de/>

<https://freenetproject.org/>

<https://www.torproject.org/>