Fundamentos de Redes (2017-2018)
Doble Grado en Ingeniería Informática y Matemáticas
Universidad de Granada

Invisible Internet Project (I2P)

Antonio Coín Castro
Alberto Jesús Durán López

6 de noviembre de 2017

Índice

1. Motivación

El incremento en el uso cotidiano de las nuevas tecnologías conlleva una serie de riesgos ocultos a la mayoría de los usuarios, que normalmente no son conscientes de los mismos, sino que se centran en su uso sin preocuparse de otros factores.

Es por esto que vemos de vital importancia poner de manifiesto los puntos negativos que afectan a los usuarios de internet, sobre todo en cuanto a privacidad se refiere. Este problema en particular es preocupante, pues cada vez que nos conectamos a la red cedemos una gran cantidad de datos que en manos equivocadas puede suponer un grave peligro para nosotros.

Afortunadamente, existen diversos métodos que, en mayor o menor medida nos ayudan a prevenir esta cesión indiscriminada de datos, sin privarnos de la facilidad y comodidad del uso corriente de Internet. En este trabajo nos centraremos en un software en particular, llamado **Invisible Internet Project (I2P)**. Sin embargo, antes explicaremos con un poco más de detalle los riesgos concretos en un acceso corriente a Internet, así como otros métodos menos sofisticados para protegernos.

2. Anonimato en el acceso corriente a Internet

¿Alguna vez te has planteado qué ocurre cuando abres el navegador y te conectas a una web de Internet? En teoría es un proceso sencillo de cara al usuario, algo que hacemos de forma casi automática. Sin embargo, lo que en realidad ocurre en las capas interiores es un proceso complejo si no se tienen conocimientos suficientes.

¿Qué ocurre cuando cuando nos conectamos a una red? Para ilustrar el proceso de conexión, podemos pensar en una plaza o un parque de una ciudad, y personas entrando y saliendo del mismo. Podemos pensar que al conectarnos a Internet realizamos un proceso análogo a entrar en la plaza, pues podemos ver que hay otros usuarios conectados, y relacionarnos con ellos si así lo queremos. Pero no es exactamente lo mismo, pues en el primer caso somos conscientes de los riesgos que conlleva entrar al parque, y solo compartimos la información que nosotros queremos en cada momento. En Internet, automáticamente estamos cediendo una gran cantidad de información, como si fueramos al parque con el DNI en alto, y cualquier persona podría, desde la distancia, saber a qué se dedica una persona, por qué ha venido al parque, su dirección, etc.

Uno de los mayores problemas es la huella digital que dejamos inconscientemente al realizar cualquier conexión. Se trata de nuestra *dirección IP*, la cual es fácilmente detectable y nos identifica de forma unívoca en Internet. Además, es posible **geolocalizar** el dispositivo desde el cual se está accediendo, simplemente con saber la dirección IP (por ejemplo, en `https://whatismyipaddress.com/`).

Existen otros problemas derivados, como el envío del historial de búsqueda, cookies de rastreo, y otra información almacenada en nuestro navegador que nos puede identificar de forma única.
Es por esto que surge la necesidad de ocultar nuestra dirección IP en Internet, y nuestro rastro en general. Para ello, existen diferentes alternativas:

- **Proxy:** Se trata de un servidor intermediario entre las conexiones de un cliente y un servidor, centrado en la navegación. De esta manera, al visitar una página web se puede enviar y recibir información a través de un proxy, y así ocultar nuestra dirección IP a la página de destino, que verá la IP del proxy. Puede utilizarse para acceder a contenido bloqueado en algunos países, como medio de evitar la censura.
- **VPN:** Es un acrónimo para *Virtual Private Network*, red privada virtual. Se trata de un medio de extender una red privada a través de una red pública, de forma que simula que un usuario conectado a través de VPN forme parte físicamente de la red privada. Esto proporciona diversas ventajas:
  - Se puede acceder remotamente a los recursos de la red privada como si se formase parte de ella.
  - Se camufla la dirección IP, pues la dirección que se ve es aquella que proporciona la red virtual.
  - Se garantiza la confidencialidad, de forma que los paquetes intercambiados en la red están encriptados.
  - Existe un sistema de autentificación para conectarse a la red e impedir accesos no deseados.
  - También se proporcionan mecanismos para mantener la integridad de los mensajes y detectar mensajes fraudulentos.
- **Redes de anonimato.** Son el objetivo central de este trabajo, y las discutiremos posteriormente.
- **Otros.** Existen otros mecanismos, menos sofisticados pero muchas veces muy efectivos, como utilizar buscadores que respetan la privacidad (`https://duckduckgo.com/`).

3. Invisible Internet Project. Estructura, funcionamiento y seguridad

I2P es una herramienta de **software libre** que ofrece una capa de red de abstracción para comunicaciones entre ordenadores, la cual permite a las aplicaciones que la utilizan transmitir mensajes de forma anónima y segura. Recordemos que una capa de red proporciona conectividad y selección de ruta entre dos sistemas de hosts que pueden estar ubicados en redes geográficamente distintas. Su misión es conseguir que los datos lleguen

desde el origen al destino aunque no tengan conexión directa.

En este caso, la selección de ruta o *routing* que ofrece I2P se basa en una serie de nodos conectados a la misma red, que crean caminos temporales y unidireccionales (túneles), siguiendo la técnica de enrutamiento *garlic*, que veremos a continuación.

Además, todas las comunicaciones están encriptadas *punto a punto*, lo que añade una capa extra de seguridad a nuestras aplicaciones.

3.1. Nodos y túneles. Algoritmo Kademlia

3.2. Enrutamiento tipo *garlic*

En la tecnología I2P, es necesario comprender que significa el término Garlic. Este término se puede aplicar a 3 conceptos diferentes:

- **Cifrado por capas:** Permite que los datos enviados a un receptor no sean descifrados en cada enrutamiento que se lleva a cabo en los diferentes túneles. En esta técnica se construyen caminos, o túneles, a través de una serie de pares (controles de entradas). Podemos distinguir dos fases:
  - Fase de construcción: cuando un mensaje se está transmitiendo en cada router (nodo), solamente se descifra la información correspondiente al siguiente router al que se le debe enviar el paquete.
  - Fase operación: Los mensajes pasan a través del túnel y el mensaje y sus instrucciones son mostradas en el punto final de este.
- **Agregación de múltiples mensajes juntos:** En *Onion Routing* los mensajes se encapsulan en capas de cifrado, a diferencia de *Garlic Routing* que encripta varios mensajes juntos para que el análisis de tráfico realizado por los atacantes resulte más difícil, así como para aumentar la velocidad de transferencia de datos.
- **Cifrado utilizando ElGamal/AES. :** Herramienta para cifrar la información que comentaremos más adelante.

3.3. Enmascaramiento de IP

3.4. Encriptación de la información

Se trata del mecanismo empleado por cada uno de los routers en cada canal de comunicación para cifrar los paquetes que viajan entre cada uno de ellos, todos los mensajes son cifrados utilizando el algoritmo de cifrado *ElGamal* y posteriormente se utiliza *AES+SessionTag*.

- **ElGamal:** Algoritmo de criptografía asimétrica. Su funcionamiento se basa en cálculos sobre logaritmos discretos usando un número primo y dos enteros.

- **AES. :** Es lo que se conoce como un cifrado simétrico por bloques, es decir, cifra y descifra los datos en bloques de 128 bits cada uno. Para ello utiliza una clave criptográfica específica que puede ser de 128,192 o 256 bits de tamaño. Dicha clave se especifica al nombrar el cifrado usado (AES-128, AES256...). Además, a cada bloque de texto se le aplica una operación XOR con el previo bloque ya cifrado, haciendo cada mensaje único con el uso de un vector de inicialización en el primer bloque. Esto es lo que se conoce como *Cipher Block Chaining - CBC*

- **Algoritmo:** La primera vez que un router quiere cifrar un mensaje para otro otro router, ambos cifran las claves para una clave de sesión AES256 con *ElGamal* y se adjuntan los bloques cifrados AES-256-CBC. Además del bloque cifrado, se crean un número de *SessionTag* (etiquetas de sesión) que pueden usarse si el remitente desea cifrar un *mensaje Garlic* para otro router, es decir, se cifra con AES los bloques pero usando la clave de sesión usada con la etiqueta de sesión anterior. Cabe destacar que cada etiqueta de sesión puede ser usada únicamente una vez para evitar vulnerabilidades y que tienen un ciclo de vida bastante corto.