I2P. El Proyecto de Internet Invisible

Contents

Introducción: La Seguridad en la Red

La seguridad en la red. Como bien todos sabemos en la red se mueve un volumen de datos abrumador. Datos que, en malas manos, pueden suponer daños para tanto los dueños de esos datos como sus destinatarios. Desde "inocentes" "me gusta" en cualquier red social hasta una compra online con nuestra tarjeta de crédito.

A muy poca gente parece que le importe publicar que le guste un vídeo de gatitos, o que te gusten las camisetas que un amigo tuyo se ha comprado por internet. Pero seguro que existe alguna tienda de ropa que estará interesada en anunciarte camisetas con dibujos de gatitos.

Esto parece ser inofensivo. ¿En qué me puede perjudicar esto? Sólo me está facilitando las cosas y poniéndome anuncios que me interesan. No quiero que me salgan anuncios de robots de cocina o del último disco del artista de turno. Enhorabuena, creo que has llegado al final de las ventajas de que tus datos sean publicados abiertamente. Porque son ventajas… ¿no?

Dejándonos de reflexiones filosóficas sobre que nos controlan y manipulan y dicen qué tenemos que comprar y ser, que eso es ya un tema que viene al caso, pero no es el momento, analizaremos otros aspectos que pueden llegar a ser bastante perjudiciales.

Lo primero que se nos viene a la cabeza es que nos roben nuestra contraseña del banco, nos timen con una compra y se queden con los datos de nuestra tarjeta… pero todos estos fallos son fallos de seguridad que todo el mundo somos capaces de ver y sobre todo de percibir su peligro.

Entonces, ¿qué factores no percibimos?

Volvamos al caso anterior de los gatitos y las tiendas de camisetas. Cambiemos el "me gusta en fotos de gatitos" por una búsqueda en Google de "qué hacer si te duele el pecho al hacer ejercicio" y "una tienda de camisetas" por "la aseguradora que tendrás de aquí a 20 o 30 años". Ahora la cosa cambia bastante. Lo que antes implicaba un bonito anuncio ahora implica una indeseable subida en la cuota de la aseguradora de 300€ extra al mes. Puede que esos 3600€ al final del año puedan servirte para tener unas buenas vacaciones, o para pagar los estudios de tus hijos. En el peor de los casos, puede que no puedas permitirte esa cantidad de dinero y que nunca puedas recibir un tratamiento adecuado en igualdad de condiciones.

Igual este ejemplo es un poco dramático, y las cifras puedan ser exageradas. Pero… `¿alguien es capaz de compartir un ejemplo que refleje la importancia de la privacidad en la red?`

Entonces, una vez hemos pensado en esto igual nos empezamos a plantear la importancia de la privacidad en la red. Pero de nuevo… `¿qué opciones tenemos para evitar esto?`

Podemos empezar con pequeños cambios. Sustituir por ejemplo buscadores como Google por otros que no te rastreen y almacenen tus datos, como DuckDuckGo. Incluso hablando de rastrear, podemos sustituir Google Maps, que realiza una cronología de tu ubicación para situarte en cada momento desde el momento en el que conseguiste tu móvil por otros mapas como Open Street Map, que además por ser software libre puede contribuirse a que cada día esté mejor documentado. O Google Street View por Mapillary. Como podemos ver Google es un recopilador de datos por defecto, pero no es el único, también es una buena consideración sustituir Instagram y Facebook por otras redes sociales, como Mastodon.

Pero como es comprensible, es muy difícil desligarse de todas estas compañías y no quedarse "aislado" en el mundo. Por esto, hay que ir poquito a poco y con buena voluntad.

Otras opciones "más drásticas" o "menos usuales" consisten en hacer uso de herramientas de privacidad que implementan medidas extra de seguridad. Tal vez la más popular de ellas y la que sólo vamos a mencionar levemente sea TOR. Sin embargo, nos centraremos más en I2P, el Proyecto de Internet Invisible.

TOR

La red Tor, a grandes rasgos, es un grupo de servidores controlados por voluntarios del proyecto que permiten mejorar la privacidad y la seguridad de sus usuarios en Internet. Usan diversos "túneles virtuales" en lugar de conexiones directas y así pueden compartir información en redes públicas sin comprometer su privacidad.

Tanto Tor como I2P son redes de proxies anónimas, que permiten a los usuarios salir anónimamente a través de su red. Aun así guardan ciertas diferencias. El modelo de amenazas y el diseño de los outproxies son distintos. También Tor usa un enfoque basado en directorios mientras que I2P tiene una base de datos de la red distribuida de la cual se seleccionan los pares. Y sobre todo, para aquellos que estén más familiarizados con Tor, la terminología que tienen ambos para referirse a ambas cosas difiere (celda-mensaje, circuito-tunel, nodo de entrada/salida-inproxy/outproxy…)

El proxy de salida de I2P/Tor tienen a pesar de todo algunas vulnerabilidades frente a ataques de análisis una vez la comunicación deja la red Tor.

Ventajas de Tor sobre I2P

Tor está mucho más extendido, tiene una comunidad mayor, con todo lo que ello implica a nivel de documentación, traducción, etc. y han sido capaces de dar soporte a problemas de escalado que I2P todavía no. Bloquea ataques DOS, los nodos cliente consumen muy poco ancho de banda, tiene un contro centralizado que permite reducir la complejidad de cada nodo. Tiene mejor uso de la memoria y está programado en C (no en java).

Ventajas de I2P sobre Tor

Está diseñado para garantizar los servicios ocultos mucho más rápido que Tor. Está totalmente distribuido. Los pares son continuamente elegidos en función de su rendimiento y categoría, en lugar de confiar en su capacidad indicada. Es tan pequeña que no ha intentado ser atacada con DOS. Los túneles I2P tienen una vida tan corta, lo cual dificulta las muestras que un atacante puede tomar. Permite tanto UDP como TCP. Además se están trabajando en otras medidas de seguridad contra ataques de análisis, tales como envolver múltiples mensajes para evitar el conteo, o introduciendo demoras en saltos donde las demoras no son perceptibles o incluso estableciendo túneles de tamaño fijo que completarían con relleno si no se alcanzase dicho tamaño.

Otra alternativa. Freenet

Freenet es una red completamente distribuida y anónima de publicación par a par. Esta ofrece una forma segura de almacenar datos y está enfocada a solucionar problemas de carga y desbordamientos. Pero mientras que Freenet está diseñada como un almacén distribuido de datos, sus usuarios han construido aplicaciones sobre el sistema para tener comunicaciones anónimas genéricas.

Este diseño de almacén hace que se pueda usar para acceder al contenido publicado por otros incluso sin que estos otros estén online. Esta funcionalidad I2P nunca la tendrá. Por esto a día de hoy no se puede usar I2P como sistema de almacenamiento distrubuido.

Freenet presenta algunos problemas de implementación, escalabilidad e incluso hay problemas con el anonimato de algunos algoritmos dada la heurística de ruteo de Freenet. Sin embargo sus propiedades desalentan a cualquier atacante que no tenga recursos suficientes para realizar análisis completos.

Invisible Internet Project. I2P

Ahora que tenemos un ligero conocimiento sobre cómo funcionan algunas de las otras redes anónimas más usadas, vamos a realizar un análisis algo más profundo de I2P.

En pocas palabras, I2P es un proyecto para construir, desplegar y mantener una red que soporte comunicación segura y anónima. Es administrable en cuanto a anonimato, fiabilidad, uso de banda ancha y latencia. Ninguno de estos puntos es presionable para comprometer la seguridad del sistema. De hecho es configurable dinámicamente en función de los ataques que pueda recibir.

La mayoría de las redes anónimas pretenden ocultar al autor original de una comunicación, pero no al destinatario. I2P, por el contrario, está diseñado para permitir la comunicación anónima entre dos pares que no son identificables entre ellos y entre terceras partes. Ahora mismo hay tanto sitios web internos que permiten publicación y hospedaje anónimo como proxies HTTP hacia la web normal que permiten la navegación anónima.

La red está orientada a mensajes, y es, en esencia, una capa IP segura y anónima donde los mensajes son direccionados hacia claves criptográficas y estos pueden ser más largos que los paquetes IP.

El diseño de I2P busca hacer más costosa la identificación de un individuo en un ambiente hostil, cubriendo su tráfico con el de otras personas que no requieran tal anonimato.

¿Cómo lo hace?

La red se compone de una instalación de nodos, llamados routers, con un número de rutas virtuales unidireccionales entrantes y salientes, llamados túneles. Cada router tiene una identidad cifrada que suele ser permanente. Estos routers se comunican entre ellos con UDP o TCP. La diferencia radica en que un cliente puede conectarse a cualquier router y autorizar la creación temporal de túneles para la comunicación a través de la red.

I2P tiene su propia base de datos de red para distribuir la información de rutas y contactos, igual que hacía Kademlia. De hecho implementa una modificación de su algoritmo.

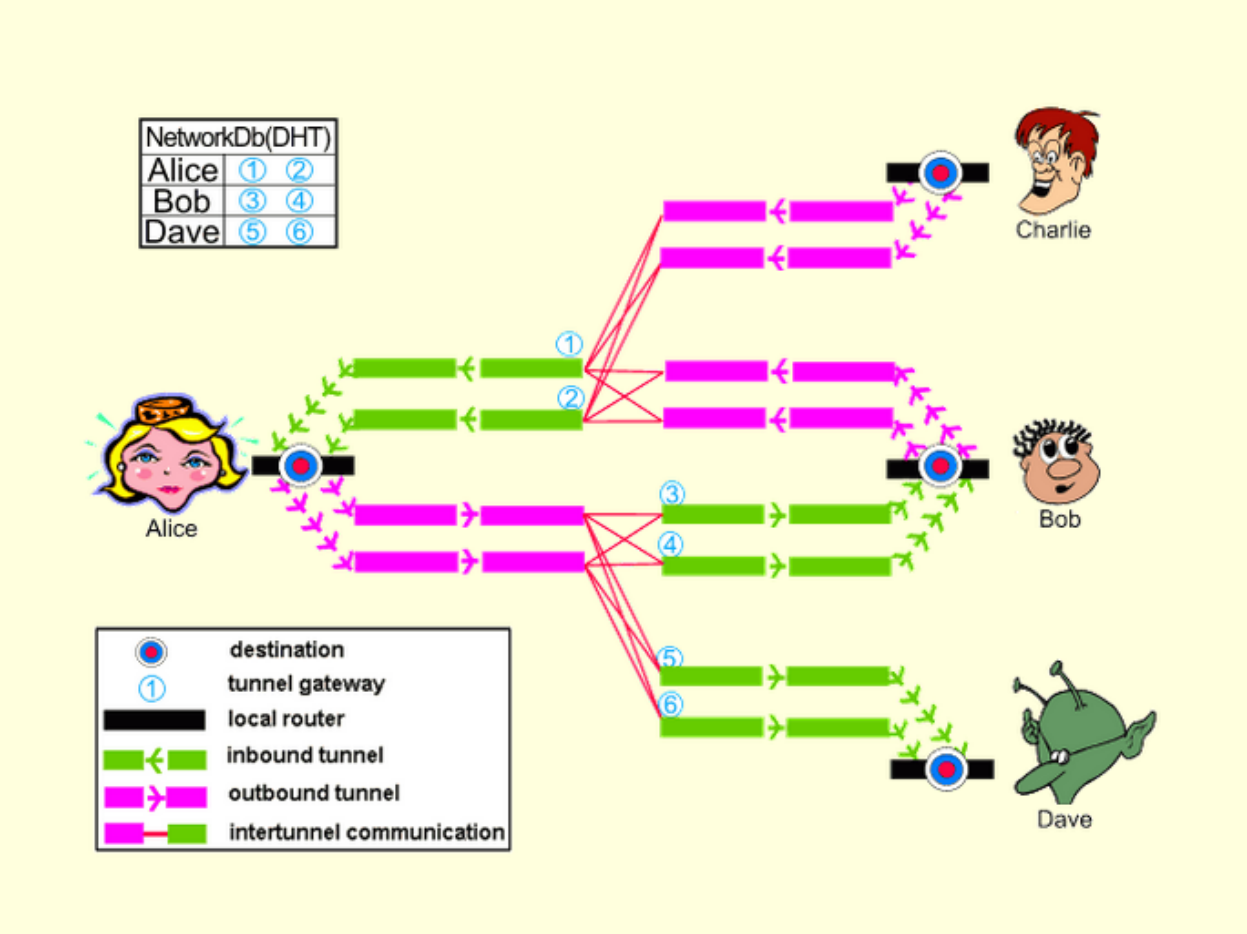

Figure 1: Ejemplo Comunicación

En esta foto observamos el esquema de una posible comunicación en I2P. Si Alice quiere hablar con Bob, envía un mensaje por su tunel de salida a algún tunel de entrada de Bob, sabe cómo enviarlos consultando la base de datos de la red, que es continuamente actualizada.

Bob, para responderle simplemente tiene que repetir el mismo proceso. Envía un mensaje al tunel de entrada de Alice. Para hacer las cosas más sencillas, se usa la envoltura garlic, una encriptación por capas, incluyendo la información necesaria para que Alice pueda responder sin tener que consultar la base de datos.

Respecto a las medidas de seguridad de I2P, como mencionábamos antes, es completamente distribuida, sin servidores que tengan estadísticas de uso ni control centralizado. Además, hace uso de un gram número de técnicas criptográficas, algoritmos de encriptación tales como cifrado Gamal de 2048 bits, AES de 256 bits, hashes SHA256…

Fuentes

- ¿Qué es TOR?
- Comparación TOR-I2P
- Comparación Freenet-I2P