Propuesta de Proyecto Final de Carrera

Estudio del anonimato de una red de comunicaciones tipo TOR

Tutor: Francisco de Borja Rodríguez Ortiz

Autor: Luis Miguel Gómez Aparicio

1. Motivación

La Red informática mundial se ha convertido en una interfaz para la distribución de información; desde el correo electrónico, gestión de identidades, transacciones bancarias, páginas Web hasta las redes sociales, se intercambian paquetes con datos confidenciales. La evolución de la Web produce una transformación continua de las tecnologías que la rodean haciéndose más complejas. Estos cambios, afectan de forma notable a la interacción del usuario con la Web. Esta constante evolución de la Web repercute directamente en la seguridad del tratamiento de estos recursos. Desde los principios de internet, uno de los pilares principales para la comunicación, es la confidencialidad de la información que navega por la red. Para conseguir esta protección es necesario crear recursos que consigan convertir nuestras comunicaciones en anónimas.

El estudio de las diferentes alternativas para preservar el anonimato de las comunicaciones en plataformas interactivas es muy importante. Una posibilidad es realizarlo mediante la incorporación de un sistema de anonimato de tipo TOR [1] que preserva la identidad de los usuarios durante comunicaciones críticas. Con TOR, se impide enlazar al remitente con el destinatario observando el flujo de paquetes de uno a otro, protegiendo de esta forma su privacidad. Para tal fin, TOR combina varias capas de cifrado entre los distintos routers por los que pasa un paquete, para dificultar dicha observación. Por otra parte, también se da la necesidad de proteger la privacidad de la información en sí misma, aspecto que TOR no ataja, ya que, trabajando en el nivel de transporte, no se preocupa por los datos y metadatos que envían los protocolos de niveles superiores. En este punto, existen proxies que trabajan en las capas más altas, como el proxy web Privoxy [3].

Tor es una red superpuesta sobre internet que está distribuida para desarrollo, formación y proporcionar un despliegue de una red anónima para las comunicaciones en baja latencia. Está diseñada para conseguir que el encaminamiento de los mensajes entre los host mantenga su privacidad y no se releve la información de los usuarios. Tor se basa en el establecimiento de un sistema virtual utilizando un circuito por capas, un circuito de enrutamiento de cebolla (Goldschlag et al, 1996;. Reed et al, 1998.; Syverson et al., 2001). De

hecho, es conocido como la segunda generación de enrutamiento de cebolla. Antes de describir más profundamente el sistema TOR, enunciaremos los principios fundamentales del enrutamiento de cebolla para tener una comprensión de las bases de TOR.

El enrutamiento de cebolla busca el desarrollo de infraestructuras para comunicaciones privadas sobre una red pública. Tiene como objetivo separar la identificación del enrutado de los mensajes con la finalidad de conseguir la privacidad mediante un enrutado anónimo (*anonymous routing*). Es una red superpuesta basada en TCP como la navegación web, la mensajería instantánea... Los flujos de tráfico en el circuito se dividen en un tamaño fijo de celdas, que serán envueltas por una clave simétrica en cada nodo, como las capas de una cebolla. Está basado en el proyecto de Chaum de guardar la relación entre origen y destino encapsulando los mensajes en capas, encriptando cada una de ellas mediante clave pública. El enrutado esta compuesto por los nodos anteriormente estudiados, los nodos de mezclado MIXes convertidos en los router de cebolla. Estos router transmiten y ordenan los mensajes que dirigen en la red, para conocer los siguientes saltos en la misma tienen que descifrar la capa más superficial del mensaje, por lo que da apariencia de cebolla, ya que se encuentra el mensaje con diferentes capas para su descifrado. Cuando un router descodifica su capa superficial obtiene la cabecera que debe interpretar y el fragmento cifrado de las siguientes capas del mensaje. De manera que este mensaje es enviado al siguiente router de cebolla donde se repetirá la operación, conociendo este último solamente el contenido de la cabecera del router anterior. Un enrutador de cebolla sólo puede identificar el salto anterior y al siguiente a lo largo de una ruta. Datos que se pasan a lo largo de la conexión anónima. La red de enrutamiento de cebolla se accede a través de proxies. Esto se produce mediante la conexión de socket a un proxy específico en los router de cebolla. En cada capa de la cebolla está cifrado el siguiente salto en una ruta. El último router envía datos a otro tipo de proxy en la misma máquina, llamada a responder al proxy, cuyo trabajo consiste en pasar los datos entre la red de cebolla y el que responde.

Cada uno de los routers de cebolla es sensible al descifrado que tiene una estructura de datos en capas, con una capa por cada uno de los routers de cebolla en la vía. Cada capa de la cebolla comprende un cifrado de la identidad del router de cebolla siguiente y material de cifrado. De manera más específica, el iniciador realiza una solicitud a un servidor proxy para establecer el circuito virtual a través de los routers de cebolla. En primer lugar, el proxy se conecta a un segundo proxy que define entonces la vía, seguidamente, el primer proxy define el camino por el que va a producirse las trayectorias individuales entre enrutadores cebolla adyacentes.

La topología de Tor consiste en una cantidad de Retransmisores Tor (también llamados Enrutadores de cebollas, nodos u OR), administrados por voluntarios, que mantienen conexiones TSL (sobre TCP/IP) permanentemente

entre sí, para formar esta red. Los Clientes Tor (proxies de cebollas u OP) los ubican mediante una base de datos semidistribuida, para solicitarles que retransmitan sus flujos TCP y así lograr anonimato. Los Retransmisores se dividen en varios tipos, relativos al uso circunstancial que le de un cliente (i.e. de entrada, medios, de salida). Primeros en orden de importancia están los nodos de salida (exit nodes), que son los que comunican la red Tor con el exterior. Dado que son la cara visible de todos los usuarios de la red, es frecuente que sean bloqueados por abuso en diferentes sitios. Para reducir el riesgo, Tor permite fijar políticas de salida (e.g. bloquear el puerto 25 para anular el spam, limitar el ancho de banda cedido).

Protege contra ataques de análisis de tráfico

El objetivo de Tor, determinado por su Modelo de amenazas, es proteger contra el análisis de tráfico. Básicamente, Tor dificulta que un atacante actuando como cliente descubra el destino de una conexión, que un atacante actuando como servidor descubra el orígen de una conexión, y que un grupo de Retransmisores vinculen al cliente con los destinatarios de sus conexiones.

Promueve activamente la facilidad de uso

Los desarrolladores de Tor enfatizan la facilidad de uso del sistema como medida de aumentar el conjunto de anonimato, es decir, la base de usuario. Con este fin han creado el controlador visual Vidalia, y los paquetes de aplicaciones preconfiguradas que incluyen en un mismo instalador Tor, Vidalia, Torbutton, Polipo, Firefox, y Pidgin.

Tiene alta visibilidad

Tor tiene un gran apoyo de las comunidades de académicos (que repercute, por ejemplo, en papers y estudios formales sobre su funcionamiento) y hackers (que colaboran, entre otras cosas, en correcciones de bugs, aplicaciones relacionadas, usabilidad). Periódicamente obtiene fondos de organizaciones no gubernamentales (e.g. la EFF), del gobierno, de universidades y de individuos, lo que le permite tener desarrolladores pagos tiempo completo. Esta visibilidad ayuda a aumentar la cantidad de usuarios.

Vive en el espacio del usuario

El software de Tor puede instalarse sin privilegios de administrador, no requiere cambios al kernel (en contraposición a otros enfoques) e incluso existen versiones portables para ser ejecutadas sin instalación.

Es multiplataforma

Existen versiones tanto para los sistemas operativos GNU/Linux, los derivados de BSD, Mac OS X, y Windows (2000, XP, Vista, 7 y las Server Editions). Esta variedad de plataformas soportadas ayuda a que crezca la base de usuarios.

Está ampliamente documentado

Tiene muy buena documentación, actualizada y variada y en diversos idiomas. Los protocoles intervinientes están completamente detallados, y los encargados del proyecto Tor mantienen una biblioteca actualizada de papers sobre anonimato y seguridad.

Es software libre

Tor, y todo el software relacionado con el proyecto, está distribuido bajo licencias libres. Además de la importancia general que tiene el desarrollo de software libre, es específicamente importante en el caso de las redes de anonimato. Que sea libre permite la auditoría por parte del cliente y de los interesados en general, así como la subsistencia al actual grupo de desarrolladores. El hecho de que el funcionamiento interno del programa sea conocido por todos, incluso por los atacantes, no le quita seguridad al mismo, de acuerdo al principio de Kerckhoff (“Un sistema criptográfico debe ser seguro incluso si todo, excepto la clave, es conocido públicamente”) y a la máxima de Shannon (“El enemigo conoce el sistema”).

Tiene una gran base de usuarios

Esto se debe a que los desarrolladores han entendido que el número de usuarios participantes en un sistema de anonimato es tanto o más importante que las características técnicas que protegen la privacidad. Activamente buscan facilitar el ingreso, bajando barreras técnicas, promoviendo a Tor, investigando, haciéndolo portable a distintas plataformas, mejorando su interfaz, etc.

2. Objetivos

Los objetivos que persigue este proyecto final de carrera son :

- Estudio de las diferentes posibilidades para generar una red TOR “virtualizada”.
- Estudio de las alternativas para incorporar proxies que actúen en niveles superiores al de transporte para anonimizar la información transportada en TOR.
- Formación en sistemas de seguridad en plataformas interactivas.
- Estudio de conceptos básicos y avanzados para la protección de la información y su anonimato en dichas plataformas.
- Formación en redes de comunicaciones basadas en estructuras TOR.
- Creación de grupo en esquemas de firmas grupales.
- Estudio de la negociación básica de información prefijada firmada anónimamente.
- Estudio de los diferentes patrones de tráfico en una red TOR que pueden violar el anonimato de las comunicaciones en la misma.
- Detección automática, mediante diferentes tipos de métricas, de los patrones de tráfico en una red TOR que pueden violar el anonimato de las comunicaciones.

3. Planificación

A continuación se definen de manera general el tiempo necesario para cumplir los objetivos definidos anteriormente. La duración puede variar dependiendo de los problemas que puedan surgir a lo largo del proyecto:

- Revisión del estado del arte de redes anónimas (4 semanas) Durante este tiempo se evaluará las soluciones de seguridad para redes anónimas.
    - Se recomienda ir recopilando en un documento la información de una forma más extensa y así integrarla en la memoria final del proyecto.
- Validación de las redes anonimato más extendidas y utilizadas en la actualidad así como sus limitaciones y sus brechas de seguridad. (3 semanas) Durante este periodo se buscará información sobre las redes y se comprobará cuál es la idónea para la el proyecto y que funcionalidades tienen.
    - Tras este período se debería tener documento donde se expliquen las soluciones existentes y las funcionalidades de las mismas. Al final de

este documento se debe argumentar cuál/es es/son la/las red/es idónea/s para continuar el proyecto final de carrera.

- Construcción y compilación de los módulos necesarios para operar con el tipo de redes tipo TOR. Se recomienda seguir estos pasos:
    - Instalación del Visual Studio.
    - Realización de un tutorial para conocer el funcionamiento básico del mismo.
    - Realización de scripts para demostrar el funcionamiento básico de la red. Al final de esta fase se debe recoger en un documento, esta fase de validación del simulador para que quede constancia de su correcto funcionamiento. Para ello se comparará su funcionamiento con el teórico.
- Comprobar el rendimiento de la red en la de red tipo TOR. (4 semanas) En esta tarea se realizarán experimentos.
    - Informe con los experimentos realizados.

- Escritura del proyecto para su entrega en la escuela (6 semanas) Utilizando el trabajo realizado durante el proyecto se escribirá el documento para la defensa.

4. Medios a utilizar

Los instrumentos que vamos a utilizar para la realización de este proyecto final de carrera se enumeran a continuación:

- Máquina compatible PC.
- Sistema operativo Ubuntu
- Visual Studio
- Acceso a internet.

REFERENCIAS

[1] http://www.torproject.org/

[2] J. Diaz, D. Arroyo, F. B. Rodriguez. “Fair anonymity for the Tor network”

[3] J. Diaz, D. Arroyo, F. B. Rodriguez. “Anonymity revocation through standard infrastructures”

[4] J. Diaz, D. Arroyo, F. B. Rodriguez. “Complete fairness for Anonymizing infrastructures”

[5] http://vndh.net/article:anonymized-virtualization18

[6] http://privoxy.org

[7] «Tor Project: Core People (https:/ / www. torproject. org/ about/ corepeople)». The Tor Project. Consultado el 12 de agosto de 2008.

[8] Dingledine, Roger (20-09-2002), « pre-alpha: run an onion proxy now!

[9] https://gitweb.torproject.org/tor. git/ commit/ bec76476efb715498b86282d4969c096df336140

[10] https://gitweb.torproject.org/tor.git/commit/213ba1a70b41ea975f2e0119a746aa1bad6f1e22

[11] Cyrus Farivar."The Internet of Elsewhere: The Emergent Effects of a Wired World".Rutgers University Press 2011

[12] Paul Syverson, "A peel of Onion", ACSAC'11. Orlando, Florida USA. Diciembre de 2011

[13] Roger Dingledine et al. "Tor: The Second-Generation Onion Router"