Arquitectura de las Redes *Tor*

Marta Gómez Macías y Braulio Vargas López

8 de diciembre de 2015

1. ¿Qué es *Tor*?

Según [1], "la red Tor es un grupo de servidores operativos voluntarios que permiten a las personas mejorar su privacidad y seguridad en Internet". Esto quiere decir que una conexión a través de Tor nunca será directa, sino que pasará por estos servidores voluntarios para que no se pueda saber quién manda el paquete ni a dónde va dirigido. Además, Tor también se define como "una efectiva herramienta para la elusión de la censura, permitiendo a sus usuarios acceder a contenido que de otra forma se encontraría bloqueado."

1.1. ¿Por qué es *Tor* más seguro que otras herramientas?

Tal y como se explica en [1], usando Tor nos protegemos contra el "análisis de tráfico". Aunque el *payload* de los paquetes que enviamos a través de la red se encuentre encriptado, la cabecera normalmente no suele estarlo ya que se necesita para dirigir el paquete. Ésta cabecera facilita a los "sniffers" muchísima información sobre lo que estamos haciendo ya que incluye información como el "host" emisor, el "host" destino, el tamaño, el puerto al que va dirigido, etc.

¿La solución? Usar una red distribuida y anónima.

2. ¿Cómo mantiene *Tor* el anonimato?

3. Arquitectura

4. Protocolo

5. Ejemplo con Wireshark

Referencias

[1] T. Project, *Overview*. URL: https://www.torproject.org/about/overview.html.en. Consultado el 8/12/2015.