

Anonymous Connections and Onion Routing

Seguridad Informática

Facultad de Ciencias Exactas, Ingeniería y Agrimensura
Universidad Nacional de Rosario

Agosto 2025

Cuando uno utiliza una red pública para comunicarse expone:

- Quienes hablan.
- Desde donde.
- Cuan frecuentemente.
- De que.

Esto se debe a muchos de los protocolos subyacentes.

Cuando uno utiliza una red pública para comunicarse expone:

- Quienes hablan.
- Desde donde.
- Cuan frecuentemente.
- De que.

Esto se debe a muchos de los protocolos subyacentes.

Por distintos motivos podemos querer evitar esta exposición, en particular al análisis del tráfico y a las posibles escuchas.

Permite la conexiones privadas entre dos puntos¹. La red permite evitar saber quien se comunica con quien.

Los datos cambian su forma a lo largo de la red lo cual contribuye al anonimato en tiempo real en ambas direcciones.

Tiene un funcionamiento similar al *firewall*. Para las comunicaciones actúa como un paso intermedio en la comunicación pero es una aplicación en si.

¹entre *initiator* y *responder*.

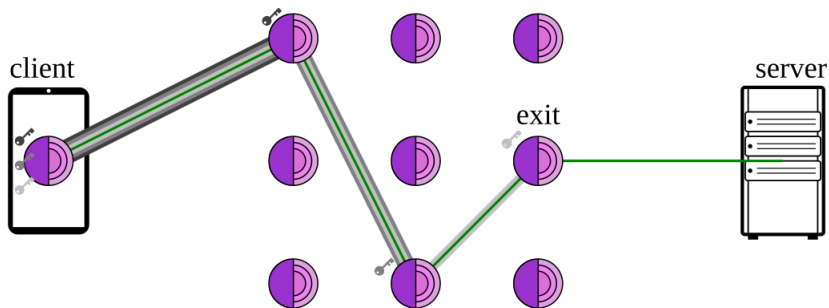


Figure: En este ejemplo se utilizan 3 saltos en lugar de 5

Proxys: Adaptación que permite reutilizar aplicaciones existen

- **Aplicación:** Interfaz entre la aplicación y el siguiente *proxy*. Encargado de aceptar o denegar las conexiones. Estandariza la comunicación, conoce el destino de la comunicación y el protocolo.
- **Onion:** Define la ruta de la conexión anónima. El encargado de construir las cebollas para la comunicación.

Routers: Nodos intermedios que se encargan de mover la información encriptada. El paso por uno implica quitar una capa de encriptación.

Puntos de salida: Encargado de establecer la conexión con el destinatario fuera de la red.

Onions:

```

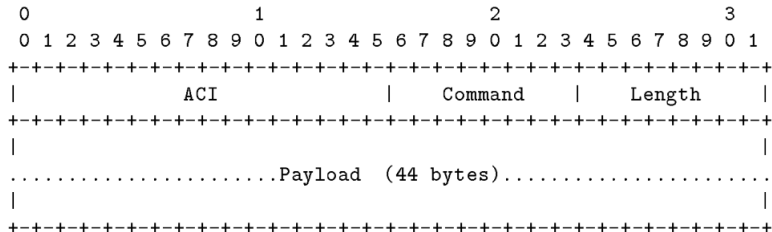
0           1           2           3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|0| Version   |Back F|Forw F|   Destination Port   |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|               Destination Address                 |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|               Expiration Time (GMT)                |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                                                     |
+               +
|               +
+               +
|               +
+               +
|               +
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

Es una estructura multi nivel.
Cada nivel tiene una forma de
encriptar propia. Se utiliza
tanto RSA como DES.

Comunicación entre *onion* routers

La conexión bidireccional y permanente. Ella multiplexa varias conexiones enviando células de tamaño fijo.



Dentro de una misma computadora se configuró una red.

- Contaba con 5 nodos.
- La sobrecarga viene de la criptografía.
- No se puede medir nociones de latencia.

Red de Prueba

Se montó una red de prueba con 13 nodos abierta al público

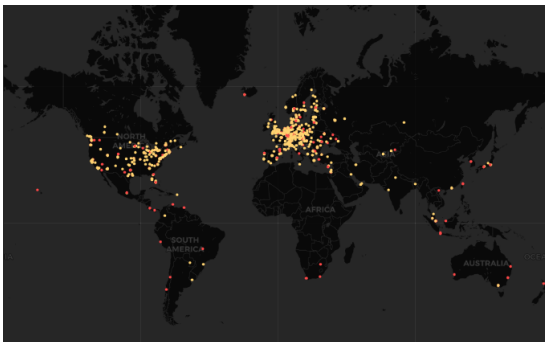


Figure: La red TOR hoy cuenta con más de 7 mil routers.²

²<https://metrics.torproject.org/networksize.html>

El principal objetivo de un atacante es identificar quienes se están comunicando y desde donde lo hacen.

La red es puede sufrir dos tipos de ataques:

- Pasivos: no hay modificaciones
- Activos: se manipulan paquetes o la red misma.

Ataque de marcado³: Interceptando distintas marcas distintivas propias de los mensajes, se buscaría descubrir (o deducir) cuál es el próximo paso al que va el mensaje.

Ataque por tiempo⁴: Utilizando el tiempo de los mensajes.

Los dos ataques requieren tener al menos 2 routers comprometidos. Su mitigación es mantener la red uniformemente ocupada.

³Marker attack

⁴Timing attack

Ataque compartiendo cantidad de paquetes vistos: Nodos comprometidos podrían compartir entre ellos la cantidad de paquetes de una sesión.

Ataque por modificación del tráfico: Generar perturbaciones en una sesión para que las cambios de frecuencia de las células.

Vulnerabilidades de la implementación

- Manejo de colas. (Causando demoras).
- Problemas con la generación de números aleatorios (para el padding).
- Caídas de nodos en la red.
- Errores en la implementación de los métodos criptográficos.

- Redes virtuales privadas.
- Chats anónimos.
- Acceso remoto.
- Búsqueda web.
- Servicio de email.

- Se puede separar el anonimato de la conexión de la comunicación.
- Se puede aplicar a muchos de los protocolos existentes.
- El protocolo actúa como una aplicación propia interponiéndose en las comunicaciones.