

# La Red de Anonimato Tor

## Enrutamiento de tipo cebolla

E.Salvatori

Departamento de Ingeniería  
Universidad Arturo Jauretche

**Seguridad de la Información**



Universidad Nacional  
ARTURO JAURETCHE

# Indice

- 1 ¿Por qué el anonimato?
  - Las libertades individuales
  - Ocultando al Emisario
- 2 El camino posible: Tor
  - Redes de baja latencia
  - Enrutamiento Tor
- 3 Vulnerabilidades
  - Problemas con el anonimato
  - Descripción de los Ataques
- 4 Laboratorio
  - Objetivos
  - Descargando el contenido



# Resumen

- 1 ¿Por qué el anonimato?
  - Las libertades individuales
  - Ocultando al Emisario
- 2 El camino posible: Tor
  - Redes de baja latencia
  - Enrutamiento Tor
- 3 Vulnerabilidades
  - Problemas con el anonimato
  - Descripción de los Ataques
- 4 Laboratorio
  - Objetivos
  - Descargando el contenido



# Internet

## Arma de doble filo

Internet presenta un arma de doble filo: es útil para expresar libremente cualquier reflexión sobre cualquier tema para cualquier persona en el globo, pero por otro lado, dadas las características de la topología de internet, es útil para espiar a quien se expresa de esta manera.



# Cifrando el mensaje

La criptografía no basta

A lo largo de toda la historia, la humanidad han empleado distintos métodos para cifrar mensajes y de esta forma proteger el contenido de cualquier intruso o fisgón que dé con el. Si bien la criptografía ha evolucionado a pasos enormes, deja de lado un gran inconveniente: Se pone el énfasis en el mensaje pero **se olvida del emisor**.



Universidad Nacional  
ARTURO JAURETCHÉ

# Resumen

- 1 ¿Por qué el anonimato?
  - Las libertades individuales
  - **Ocultando al Emisario**
- 2 El camino posible: Tor
  - Redes de baja latencia
  - Enrutamiento Tor
- 3 Vulnerabilidades
  - Problemas con el anonimato
  - Descripción de los Ataques
- 4 Laboratorio
  - Objetivos
  - Descargando el contenido



# Ocultando al emisorio

Para asegurar una completa privacidad entre las comunicaciones, será necesario no sólo ocultar los mensajes entre emisor y receptor, sino que también será necesario **ocultar el emisorio**. Dada la relativa facilidad con la que los usuarios pueden ser vinculados a direcciones IP o engañados mediante sitios webs, será de sumo interés el garantizar el anonimato tanto del mensaje como de las partes que se comunican.



# Resumen

- 1 ¿Por qué el anonimato?
  - Las libertades individuales
  - Ocultando al Emisario
- 2 El camino posible: Tor
  - Redes de baja latencia
  - Enrutamiento Tor
- 3 Vulnerabilidades
  - Problemas con el anonimato
  - Descripción de los Ataques
- 4 Laboratorio
  - Objetivos
  - Descargando el contenido



# Redes de Comunicación Anónimas de Baja Latencia

A diferencia de las Redes de Comunicación de Alta Latencia, donde los mensajes son entregados con mucho tiempo de retraso, (provocando de esta manera un ofuscamiento de los participantes de la comunicación), las **Redes de Comunicación Anónimas de Alta Latencia**, permiten un uso de Internet al cual estamos más acostumbrados: navegación web, interacción multimedia, etc.

# Resumen

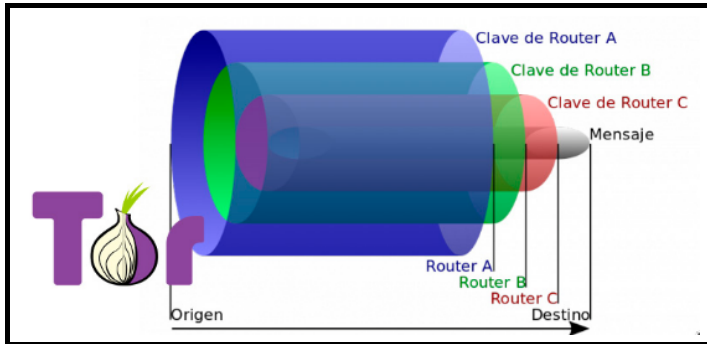
- 1 ¿Por qué el anonimato?
  - Las libertades individuales
  - Ocultando al Emisario
- 2 **El camino posible: Tor**
  - Redes de baja latencia
  - **Enrutamiento Tor**
- 3 Vulnerabilidades
  - Problemas con el anonimato
  - Descripción de los Ataques
- 4 Laboratorio
  - Objetivos
  - Descargando el contenido



# Onion Routing

## El mensaje

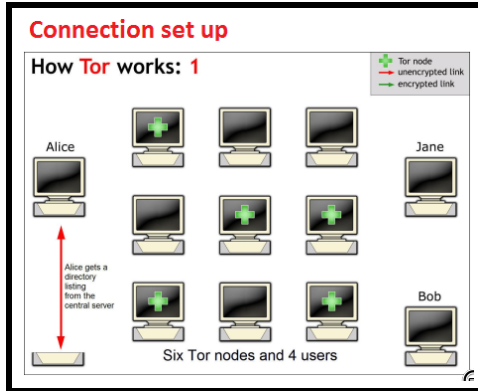
La forma que tiene Tor de encriptar el mensaje:



# Onion Routing

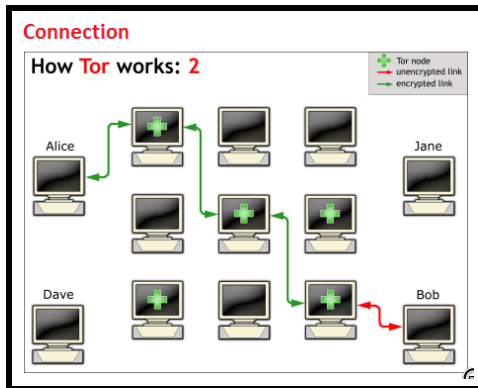
## Configuración del Circuito

El Enrutamiento de tipo cebolla (Onion Routing) funciona de la siguiente manera:



# Onion Routing

Circuito establecido



# Resumen

- 1 ¿Por qué el anonimato?
  - Las libertades individuales
  - Ocultando al Emisario
- 2 El camino posible: Tor
  - Redes de baja latencia
  - Enrutamiento Tor
- 3 **Vulnerabilidades**
  - **Problemas con el anonimato**
  - Descripción de los Ataques
- 4 Laboratorio
  - Objetivos
  - Descargando el contenido



# Tipos de Ataques

Se pueden establecer dos tipos de ataques perpetrados a la red Tor:

- 1 Ataques de análisis de tráfico.
- 2 Ataques DoS.

# Resumen

- 1 ¿Por qué el anonimato?
  - Las libertades individuales
  - Ocultando al Emisario
- 2 El camino posible: Tor
  - Redes de baja latencia
  - Enrutamiento Tor
- 3 **Vulnerabilidades**
  - Problemas con el anonimato
  - **Descripción de los Ataques**
- 4 Laboratorio
  - Objetivos
  - Descargando el contenido



# Ataques basados en complementos

- Dirigidos a los usuarios a través del navegador de Tor, haciendo uso de los software externos como Flash, Java o ActiveX.
- Estas aplicaciones se ejecutan por fuera del navegador, por lo que son el blanco perfecto para poder ejecutar código malicioso de forma intrusiva.
- Se puede perpetrar mediante un servidor malicioso, introduciendo contenido adulterado.
- O se puede interceptar comunicaciones no seguras (como HTTP) infectando un nodo de salida.

# Ataque Torben

Se manipula al econtenido de las páginas webs que visita el usuario para obligarlo a acceder a contenido no confiable.

# Fuga de Información 2P

El atacante, mediante la técnica **Hombre en el medio** intercepta el contenido de una lista devuelta por un rastreador torrent, evidenciando así el circuito establecido por la red Tor.

# Ataques basados en tiempo

Se mide el rendimiento de la red de circuitos creados a través de cada nodo y por lo tanto, cuando un cliente se conecta, el servidor web puede medir nuevamente la latencia de cada nodo Tor y observar cuáles ha aumentado su rendimiento, poniendo de evidencia el circuito.



# Ataques mediante predecesor

Los nodos maliciosos se dispersan en la red y como serán elegidos al azar entonces es posible rastrear al emisor, ya que cada nodo (que NO fuese el del comienzo) conoce sólo su predecesor. Por lo tanto se hace un análisis retrospectivo hasta dar con el emisor.

# Ataques mediante Servidores Ocultos

El atacante puede estudiar y relacionar patrones de tráfico tanto como circuito y como atacante, e identificar si su instancia de nodo de enrutamiento se encuentra en el circuito entre el servidor oculto y el punto de encuentro.



# Ataques de Reloj sesgado

Se describe un ataque mediante esta técnica en el que un usuario externo malintencionado genera exceso de procesamiento en un Servidor Tor con la intención de elevar la temperatura del procesador, alterando así las características operativas de su reloj de manera que se pueda detectar esta injerencia en los paquetes de red que emite la máquina.



# Resumen

- 1 ¿Por qué el anonimato?
  - Las libertades individuales
  - Ocultando al Emisario
- 2 El camino posible: Tor
  - Redes de baja latencia
  - Enrutamiento Tor
- 3 Vulnerabilidades
  - Problemas con el anonimato
  - Descripción de los Ataques
- 4 Laboratorio
  - Objetivos
  - Descargando el contenido



# Objetivos del Laboratorio

- 1 Mostrar de forma fácil y sencilla el uso de Tor.
- 2 Probar los conocimientos aprendidos con la línea de comando en sistemas GNU/Linux.
- 3 Evidenciar que lo expuesto anteriormente, se puede llevar a cabo de manera fácil y hogareña.



# Resumen

- 1 ¿Por qué el anonimato?
  - Las libertades individuales
  - Ocultando al Emisario
- 2 El camino posible: Tor
  - Redes de baja latencia
  - Enrutamiento Tor
- 3 Vulnerabilidades
  - Problemas con el anonimato
  - Descripción de los Ataques
- 4 Laboratorio
  - Objetivos
  - Descargando el contenido

# Descargando Tor


## Página de descarga



# En la línea de comando

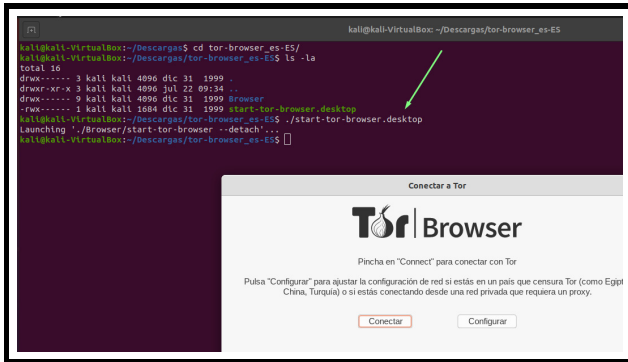
## Desempaquetando la descarga

```
kali@kali-VirtualBox:~/Descargas$ ls -la
total 77588
drwxr-xr-x  2 kali kali   4096 jul 22 09:32 .
drwxr-xr-x 16 kali kali   4096 jul  9 17:49 ..
-rw-rw-r--  1 kali kali    680 jul  9 17:01 acl.zip
-rwxrwxrwx  1 kali kali    242 jul  3 22:30 borrarUsuario.sh
-rwxrwxrwx  1 kali kali    518 jul  9 17:11 crearUser.sh
-r-----  1 kali kali 79422768 jul 22 09:30 tor-browser-linux64-9.5.1_es-ES.tar.xz
kali@kali-VirtualBox:~/Descargas$ tar -xf tor-browser-linux64-9.5.1_es-ES.tar.xz
kali@kali-VirtualBox:~/Descargas$ ls -la
total 77592
drwxr-xr-x  3 kali kali   4096 jul 22 09:34 .
drwxr-xr-x 16 kali kali   4096 jul  9 17:49 ..
-rw-rw-r--  1 kali kali    680 jul  9 17:01 acl.zip
-rwxrwxrwx  1 kali kali    242 jul  3 22:30 borrarUsuario.sh
-rwxrwxrwx  1 kali kali    518 jul  9 17:11 crearUser.sh
drwx-----  3 kali kali   4096 dic 31 1999 tor-browser-es-ES
-r-----  1 kali kali 79422768 jul 22 09:30 tor-browser-linux64-9.5.1_es-ES.tar.xz
kali@kali-VirtualBox:~/Descargas$
```



# En la línea de comando

## Accediendo al ejecutable



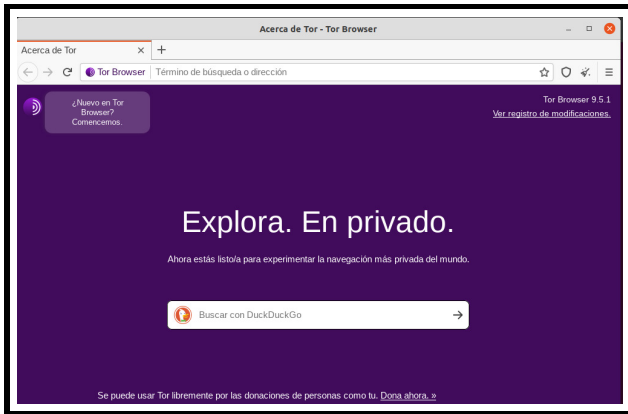
The screenshot shows a Kali Linux terminal window with the following commands and output:

```
kali@kali-VirtualBox: ~/Descargas/tor-browser_es-E5
kali@kali-VirtualBox:~/Descargas$ cd tor-browser_es-E5/
kali@kali-VirtualBox:~/Descargas/tor-browser_es-E5$ ls -la
total 16
drwx----- 3 kali kali 4096 dic 31 1999 .
drwxr-xr-x 3 kali kali 4096 jul 22 09:34 ..
drwx----- 9 kali kali 4096 dic 31 1999 Browser
-rwx----- 1 kali kali 1684 dic 31 1999 start-tor-browser.desktop
kali@kali-VirtualBox:~/Descargas/tor-browser_es-E5$ ./start-tor-browser.desktop
Launching './Browser/start-tor-browser --detach'...
```

A green arrow points from the `start-tor-browser.desktop` file in the terminal output to the Tor Browser window. The Tor Browser window has a title bar that says "Conectar a Tor". It features the Tor logo and the text "Browser". Below the logo, it says "Pincha en 'Connect' para conectar con Tor". At the bottom, there are two buttons: "Conectar" and "Configurar".

# Listo para comenzar

## Navegador Tor



# Comparativa entre ser conocido y anónimo

## Navegador Firefox y Tor

The image shows a side-by-side comparison of IP address information. On the left, a standard browser shows an IP address of 186.13.16.1, which is associated with Claro Argentina, Buenos Aires, and Berazategui. On the right, the Tor network shows an IP address of 216.239.90.19, which is associated with VIF Internet. A red arrow points from the 'City: Berazategui' on the left to the 'Surf Privately' button on the right, indicating the transition to anonymity.

My IP Address Is:	My IP Information:
IPv4: <b>186.13.16.1</b> IPv6: Not detected	ISP: Claro Argentina <b>City: Berazategui</b> Region: Buenos Aires Country: Argentina <a href="#">Make My IP Address Private</a>
IPv4: <b>216.239.90.19</b> IPv6: Not detected	ISP: VIF Internet Services: <a href="#">Tor Exit Node</a> <a href="#">Surf Privately</a> <a href="#">Click Here</a>



# Bibliografía I



J. Kurose, K. Ross

*Computer Networking: A Top-Down Approach.*  
Pearson, 2016.



A. Tanenbaum

*Computer Networks.*  
Pearson, 2010.



H. Schulzrinne & others

RFC nº 3550.  
*IEFT.ORG*, 2(1):50–100, 2003.



Universidad Nacional  
ARTURO JAURETCHÉ