Entre todos cuidamos mejor los secretos

¡Hagamos crecer las redes de anonimato en la región!

Gunnar Wolf

ECSL 2020

Contenidos

Nos gusta compartir y ser abiertos

- Tal vez les suene *raro* el dar lugar a los *secretos* en un foro dedicado a las tecnologías libres, la libre circulación de ideas, la interoperabilidad y la transparencia
- La tecnología, por abierta que sea, no implica que estemos dispuestos a *claudicar* en la defensa de los derechos humanos

Nos gusta compartir y ser abiertos

- Tal vez les suene *raro* el dar lugar a los *secretos* en un foro dedicado a las tecnologías libres, la libre circulación de ideas, la interoperabilidad y la transparencia
- La tecnología, por abierta que sea, no implica que estemos dispuestos a *claudicar* en la defensa de los derechos humanos

- *La privacidad* es un derecho humano

Nos gusta compartir y ser abiertos

- Tal vez les suene *raro* el dar lugar a los *secretos* en un foro dedicado a las tecnologías libres, la libre circulación de ideas, la interoperabilidad y la transparencia
- La tecnología, por abierta que sea, no implica que estemos dispuestos a *claudicar* en la defensa de los derechos humanos

- *La privacidad* es un derecho humano
- La privacidad *sólo puede ser garantizada* por el anonimato

¿No basta un buen cifrado para asegurar la privacidad?

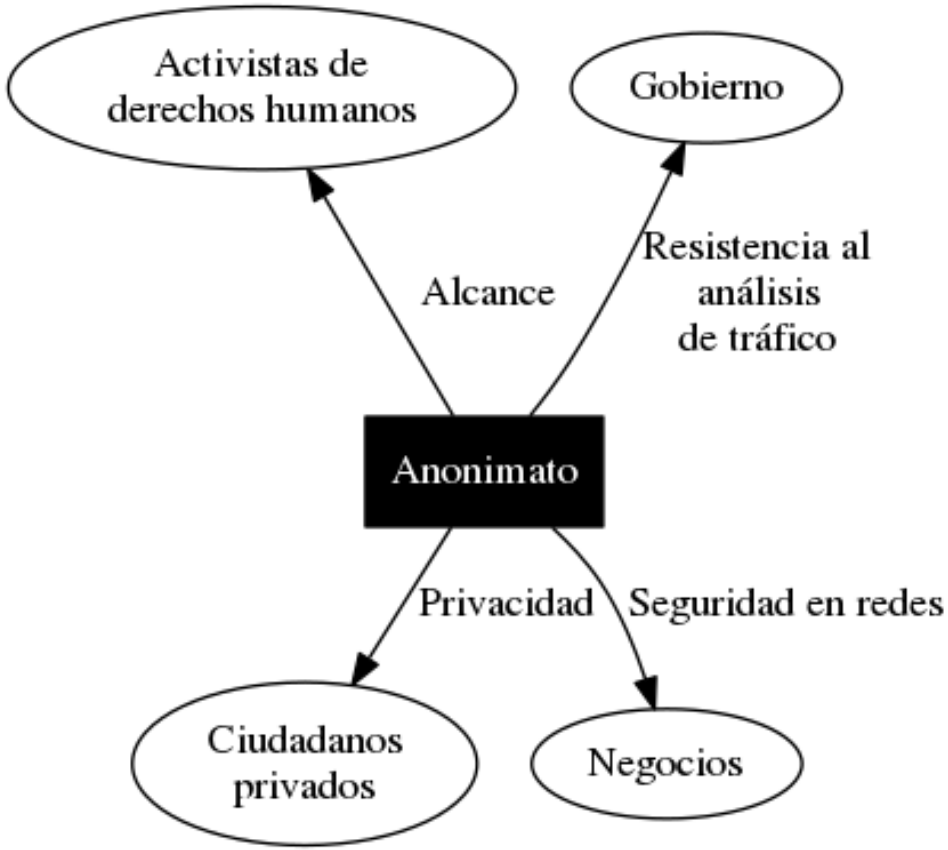
- Las buenas prácticas de cifrado nos *encaminan* hacia la privacidad
- Pero conocen ya de la profundidad del análisis de *metadatos*. . .

¿No basta un buen cifrado para asegurar la privacidad?

- Las buenas prácticas de cifrado nos *encaminan* hacia la privacidad
- Pero conocen ya de la profundidad del análisis de *metadatos*. . .

Privacidad implica anonimato

El cifrado no es suficiente para proteger nuestra privacidad.
¿Qué brinda el *anonimato* a diferentes sectores?



Contenidos

¿Cómo *preservar el anonimato* en Internet?

Internet ofrece múltiples puntos desde donde espiar comunicaciones

- Red basada en paquetes
- Papel de los *ruteadores*
- No hay garantía de rutas
- Los protocolos de red no implementan cifrado

La privacidad *nunca fue* criterio de diseño (aunque tampoco la *espiabilidad*)

Redes de mezclado

En 1981, David Chaum publicó *Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms* →

`https://www.freehaven.net/anonbib/cache/chaum-mix.pdf`

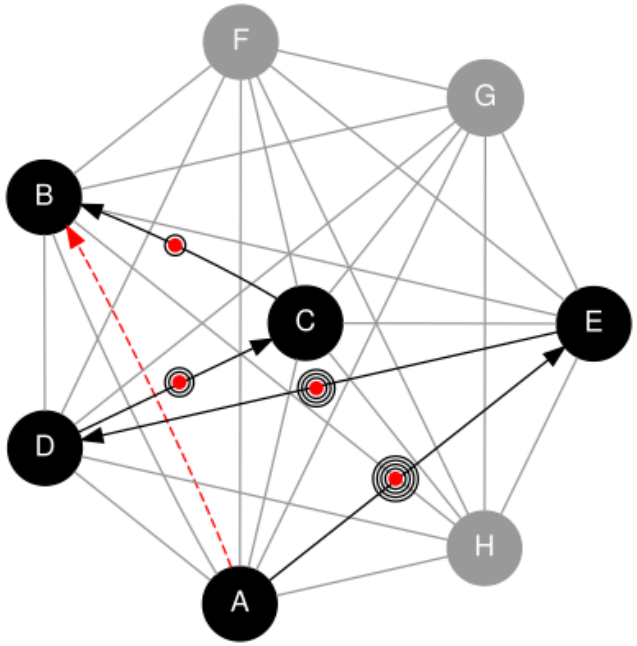
- Basado en criptografía de llave pública
- Un mensaje es enviado mediante una *red de mezclado* del remitente al destinatario, sin que sea posible a ningún nodo (o externo) saber de quién a quién va
- Cifra el contenido con la llave pública *consecutiva* de 3 participantes de una *red de mezclado* e_1, e_2, e_3, y lo entrega por correo electrónico al primero de éstos

$$c = (((m^{e_3} \mod n_3)^{e_2} \mod n_2)^{e_1} \mod n_1)$$

- Los servidores s_3, s_2, s_1 van *retirando capas* hasta obtener el mensaje a ser entregado

Ruteo cebolla

- Hacia 1996, se aplica esta idea a comunicación en tiempo real sobre Internet, con protocolos arbitrarios → *Hiding Routing information* (David M. Goldschlag, Michael G. Reed, Paul F. Syverson; International Workshop on Information Hiding)
- Término *Ruteo cebolla* (por eso de ir pelando la información capa por capa



El proyecto *Tor*

Tor — The Onion Router

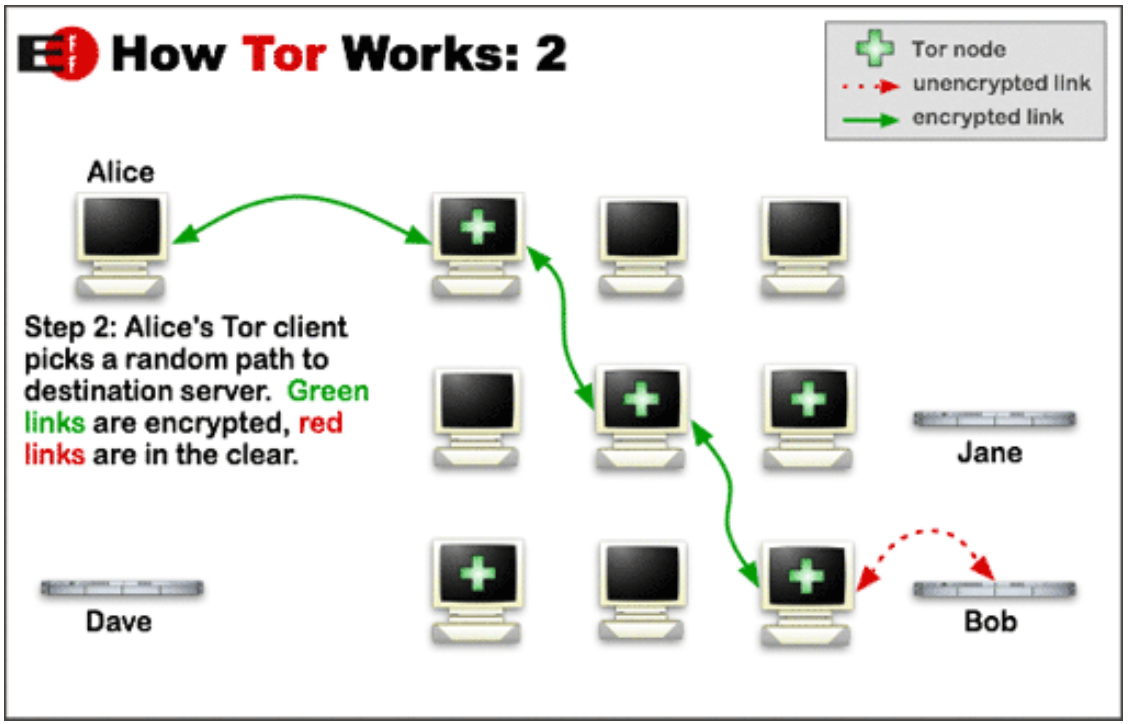
La red anonimizadora más extendida

- Más de 6000 nodos en el mundo operados por voluntarios
- Respaldado por numerosas organizaciones de promoción de seguridad y privacidad en línea
  - EFF
  - RiseUp
  - Internet Defense League
  - Muchas ONGs, ...
- *Proxys cliente* y navegadores dedicados disponibles para sistemas operativos de escritorio, móbiles, distribuciones *amnésicas*, etc.

El proyecto *Tor*: ¿Cómo funciona?

Tor — The Onion Router

La red anonimizadora más extendida



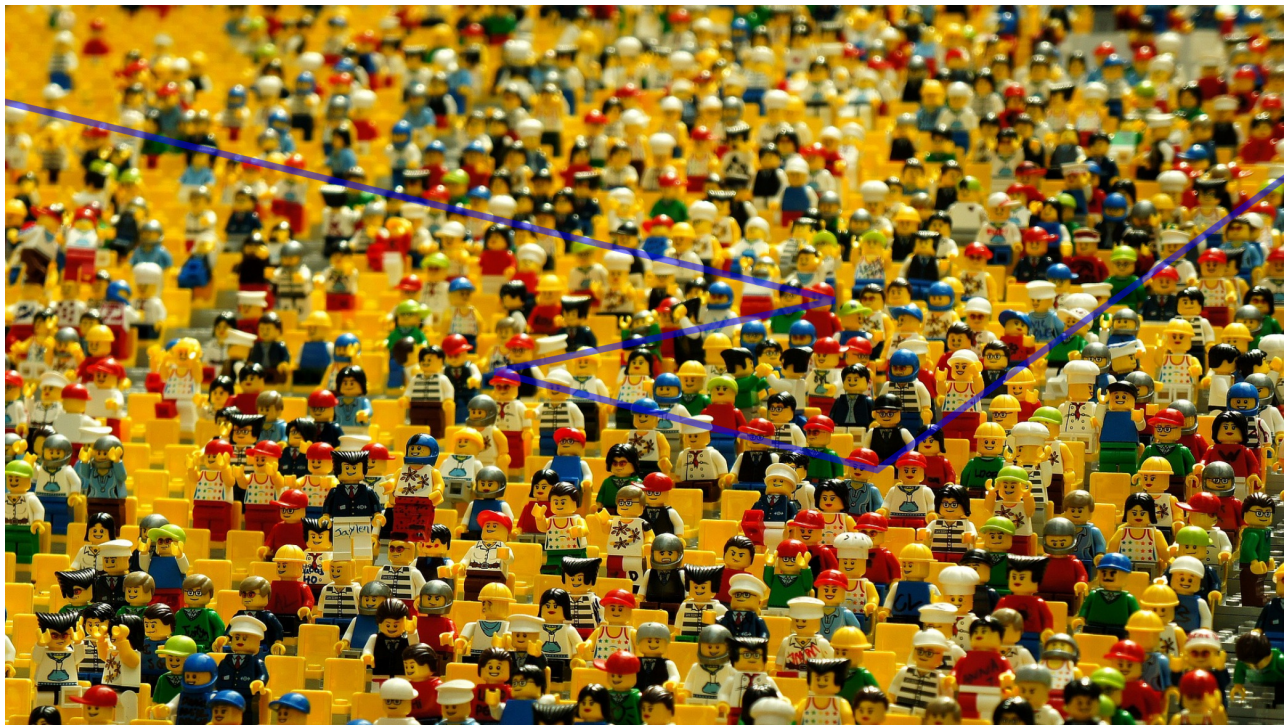
Contenidos

El anonimato requiere de buena compañía

- Para que una red anonimizadora *tenga sentido*, requiere que haya *suficiente diversidad* entre sus integrantes
- De no ser así, se vuelve relativamente sencillo para un atacante *observar suficientes nodos* y correlacionar los paquetes que llegan y salen
- Entre más puntos de entrada, mezcla y salida tenga nuestra red, mejor será su anonimato
  - No sólo más en cantidad: más ISPs, más jurisdicciones legales...

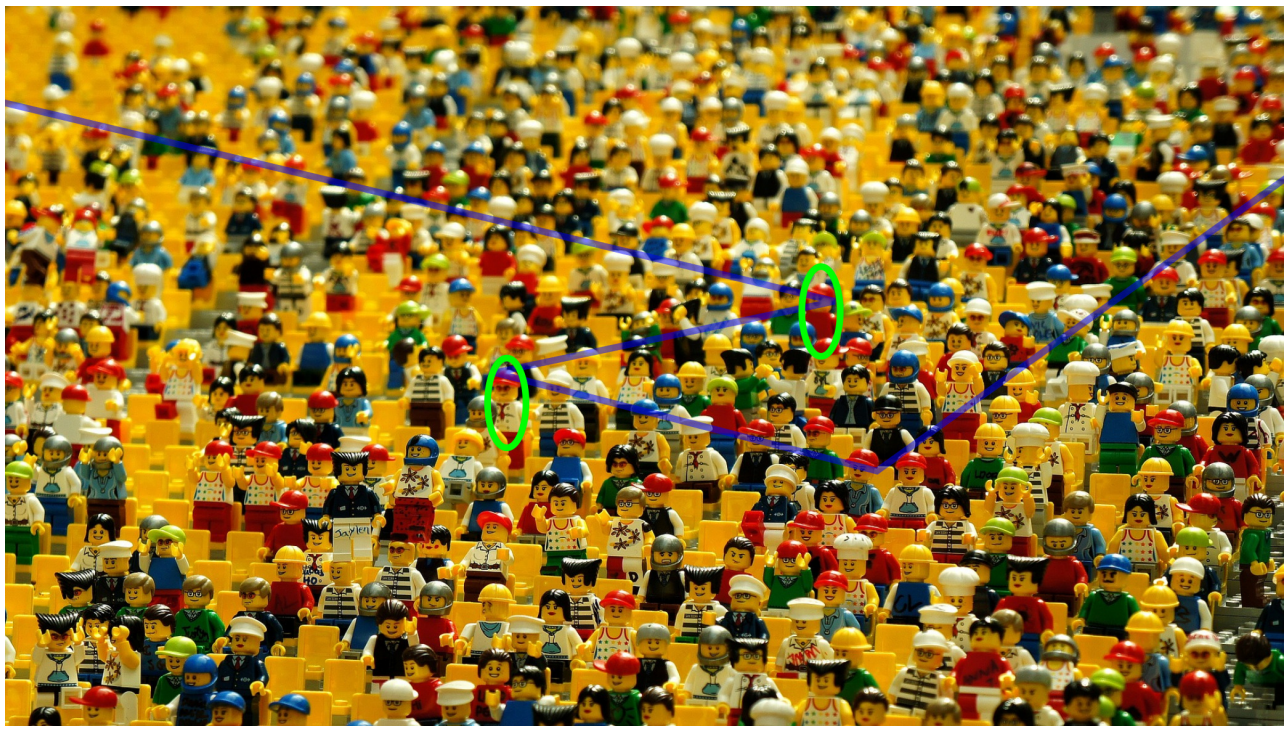
Operando un *relay*

Es importante *ayudar a las redes de anonimato* contribuyendo con nodos de mezcla.



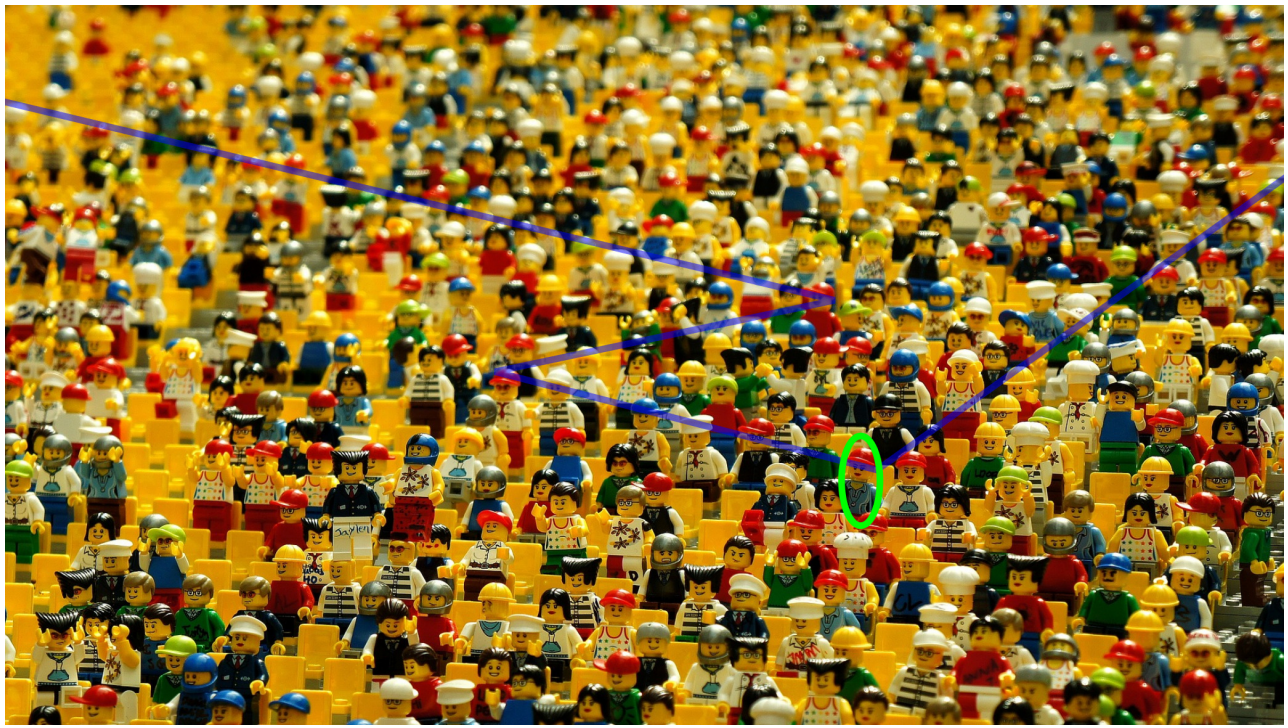
Operando un *relay* de entrada o intermedio

- Reciben o reenvían las conexiones
- *Sin ningún riesgo legal*
- Muy bajo impacto en nuestro nivel de tráfico
- Podemos operarlos desde casa o nuestras organizaciones



Operando un *relay* de salida

- Interfaz entre la red Tor y la red abierta
- *Puede haber riesgos legales*
- Afecta la operación habitual de la red (conviene que sea una red dedicada).



Si tienen posibilidad, *es muy importante* apoyar a Tor con nodos de salida.

¿Cómo activar un *relay*?

La gente de bien usa Debian, ¿cierto? ;-)

```
# apt install tor
# editor /etc/tor/torrc
(...)
# El nombre que damos al relay
Nickname mirelay
# Ancho de banda m ximo a dedicar
RelayBandwidthRate 50000 KB
# Ancho de banda l mite
RelayBandwidthBurst 50000 KB
# Correo de contacto
ContactInfo gunnarcito@gwolf.org
# Permitimos salida? Si indicamos ‘‘allow’’ con alguna
# lista de puertos, ser  un relay de salida
ExitPolicy reject *:*
```

De los 6000 nodos...

¡Queremos tu participación! Ayuda a aumentar la cantidad de nodos en nuestra región del mundo...

País	Código	Relays	Salidas	Ancho de banda
Belice	bz	18	18	499.5 MB/s
Costa Rica	cr	16	4	24.43 MB/s
El Salvador	sv	0	0	0
Guatemala	gt	0	0	0
Honduras	hn	0	0	0
Nicaragua	ni	0	0	0
Panamá	pa	2	1	633.2 KB/s

Fuente: Tor Metrics, `https://metrics.torproject.org/rs.html#search/country:XX%20running:true`

Contenidos

Imágenes utilizadas en esta presentación

- *La Sapa*, logotipo del ECSL2020: https://softwarelibre.ca/images/ECSLogo2020.png
- Vigilancia (multicámaras), StockSnap (Pixabay) https://pixabay.com/es/photos/vigilancia-ladrillos-c%C3%A1maras-ni%C3%B1as-2616771/
- videoconferencia con Edward Snowden, por Gage Skidmore (CC-BY-SA), https://flic.kr/p/rbjtmZ
- Graffiti de Chelsea Manning, Wikimedia Commons (Smuconlaw), CC-BY-SA, https://commons.wikimedia.org/wiki/File:Graffito_of_Bradley_or_Chelsea_Manning,_Vienna,_Austria_-_20140721.jpg
- Logotipo de PRISM: NSA, US federal Government; original (C) Adam Hart-Davis © 1998-04-08, Public domain, via Wikimedia Commons, https://commons.wikimedia.org/wiki/File:PRISM_logo.jpg
- Amuletos / Un mundo nos vigila: Wikimedia Commons (Guruharsha) CC-BY-SA, GFDL, https://commons.wikimedia.org/wiki/File:Nazars_Greek_evil_eye_charms.jpg
- ¿Qué es el anonimato? (elaboración propia)
- Torre de vigilancia, Pixource (Pixabay), https://pixabay.com/es/photos/cctv-vigilancia-de-seguridad-c%C3%A1mara-2579551/
- Ruteo cebolla A-B-C-D-E (elaboración propia)
- Logotipo del proyecto Tor: Wikimedia Commons: Tor Project (CC-BY-SA) https://commons.wikimedia.org/wiki/File:Torproject.png
- EFF: How Tor Works (CC-BY) https://www.torproject.org/images/htw2.png
- Multitud: Pixabay (Thomas Buchenberger), https://pixabay.com/es/photos/humanos-personales-an%C3%B3nimo-masa-4906908/
- Muñecas: Pixabay (Thomas Buchenberger), https://pixabay.com/es/photos/mu%C3%B1ecas-mu%C3%B1ecas-de-trapo-juguetes-5359827/
- Legos: Pixabay (Eak K.) https://pixabay.com/es/photos/lego-figuritas-juguetes-multitud-1044891/
- Palomas: Pixabay (Stafford Green), https://pixabay.com/es/photos/c%C3%A1mara-esp%C3%ADa-paloma-vigilancia-712122/
- Vigilando al personaje: Pixabay ($\text{db}_{\textbf{oblikovanje}}$), https://pixabay.com/es/photos/c%C3%A1mara-video-pel%C3%ADcula-4973325/

Fin del rollo

¡Gracias por aguantarme!

¿Hay tiempo para preguntas y eso?