Desmitificando la Deep Web

Introducción a ToR

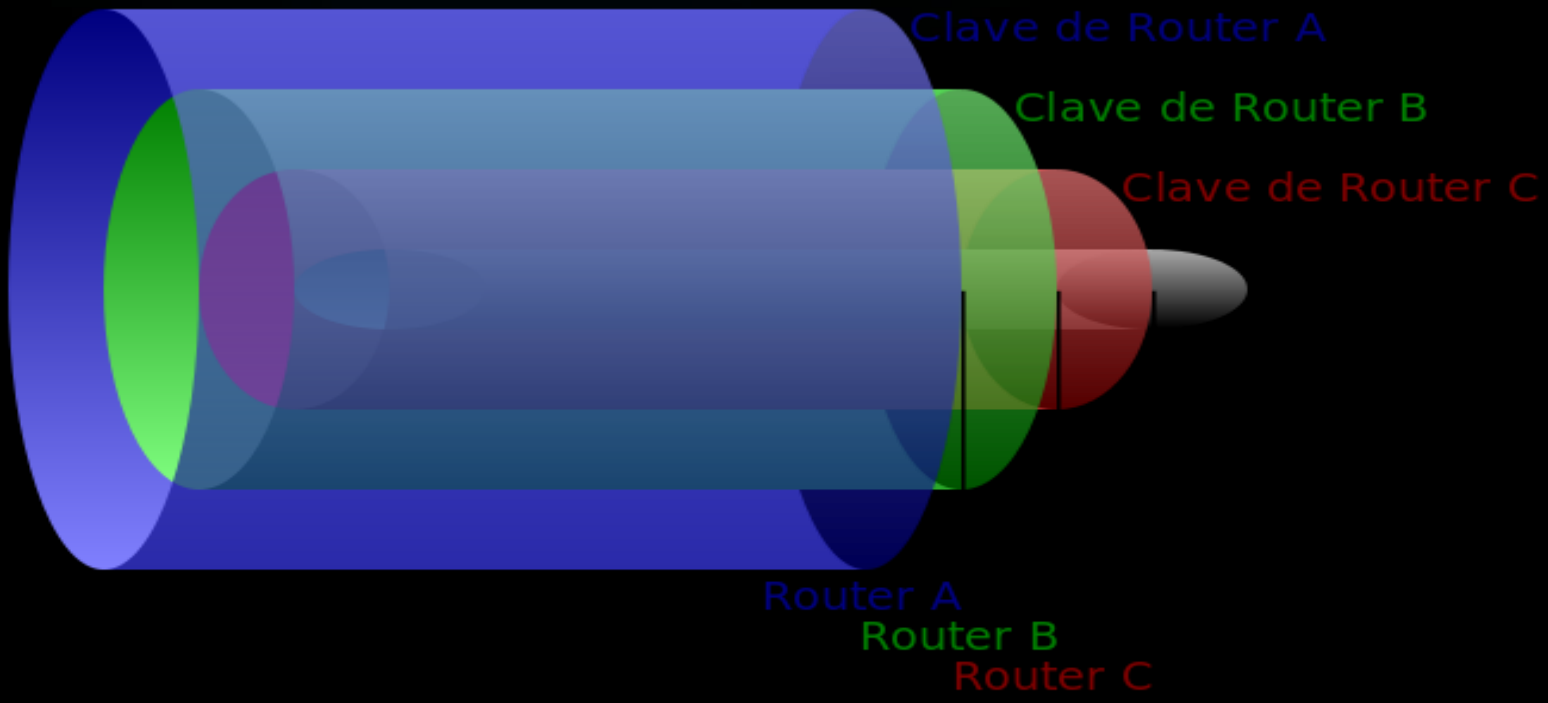
Ing. Fernando Villares – ITFLOSS 2017

Deep Web y Dark Net

- La internet profunda recibe numerosos nombres… Deep web, dark web o dark net, internet invisible o internet oculta.
- Así se le denomina al contenido de internet que no es indexado por los motores de búsqueda convencionales, debido a diversos factores.
- Se accede a ella a través de accesos cifrados anónimos como ToR, i2p, FreeNet, Riffle, etc.
- La deep web no es sinónimo de delitos, pedofilia ni contratación de delincuentes informáticos, sinó que es una herramienta clave para la defense de los derechos humanos y la privacidad en el siglo XXI.

Ruteo Cebolla

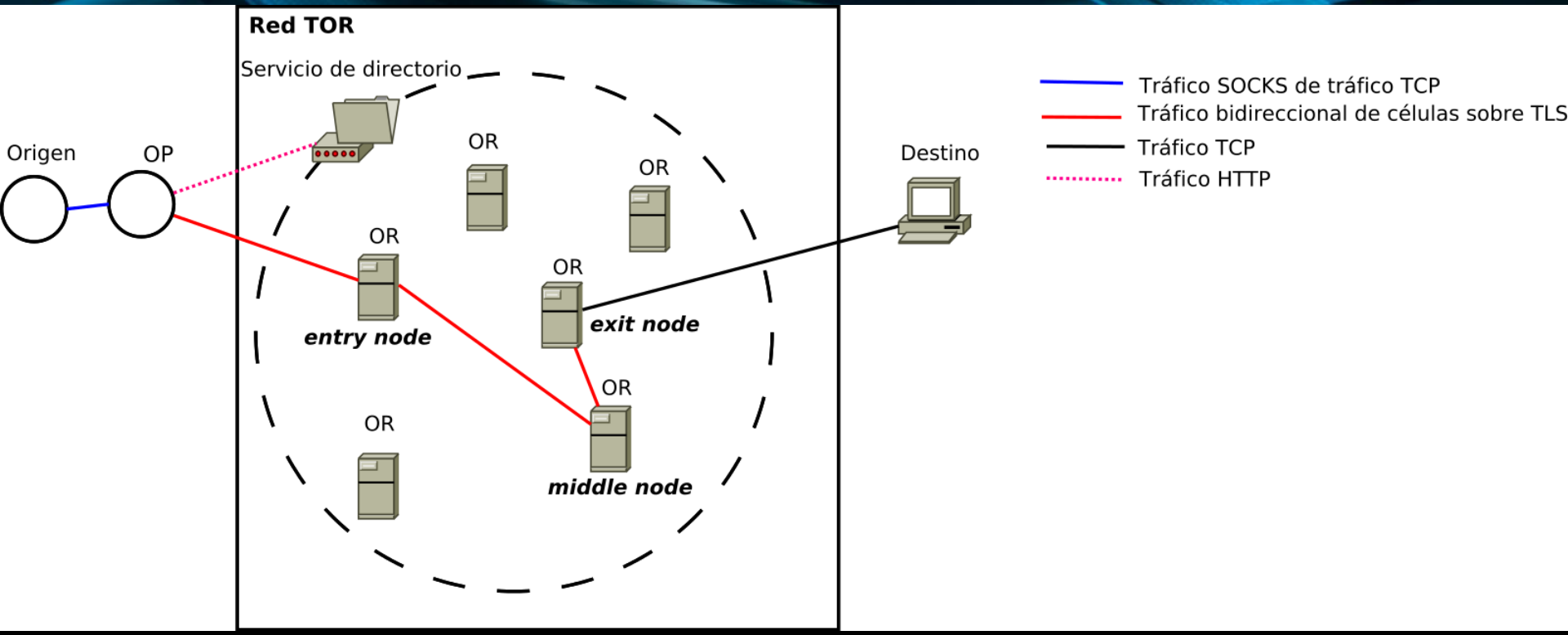
El ruteo cebolla aprovecha la idea de David Chaum de esconder la relación entre el origen y el destino de una información encapsulando los mensajes en capas de criptografía de clave pública



ToR – The Onion Router

- Proyecto cuyo objetivo principal es el desarrollo de una red de comunicaciones distribuida de baja latencia y superpuesta sobre internet, en la que el ruteo de los mensajes intercambiados entre los usuarios no revela su identidad, es decir, su dirección IP (anonimato a nivel de red) y que, además, mantiene la integridad y el secreto de la información que viaja por ella.
- Origen Armada de EEUU, autores originales en 2002, Roger Dingledine, Nick Mathewson y Paul Syverson, actualmente en manos de la fundación THE TOR PROJECT.

¿Cómo funciona el ruteo Cebolla?



Formada por serie de nodos que se comunican mediante el protocolo TLS sobre TCP/IP manteniendo así secreta e íntegra, sin modificaciones externas, la información desde un nodo a otro.

2 tipos de entidades:

•Nodos OR (*Onion Router*): Routers y en algunos casos servidores de directorio (DNS) de una especie de servicio de mantenimiento. Mantienen una conexión TLS con cada uno de los otros OR. Las conexiones OR-OR no son nunca cerradas deliberadamente salvo cuando pasa cierto tiempo de inactividad. Cuando un OR comienza o recibe nueva información de directorio intenta abrir nuevas conexiones a cualquier OR que no esté conectado.

•Nodos OP (*Onion Proxy*): Los usuarios finales ejecutan un software que hace la función de nodo OP, cuya función es obtener información del servicio de directorio, establecer circuitos aleatorios a través de la red y manejar conexiones de aplicaciones del usuario. Los OP aceptan flujos TCP de aplicaciones de usuarios y las multiplexa a través de la red OR's. Las conexiones OR-OP no son permanentes. Un OP debería cerrar una conexión a un OR si no hay circuitos ejecutándose sobre la conexión y ha vencido cierto temporizador

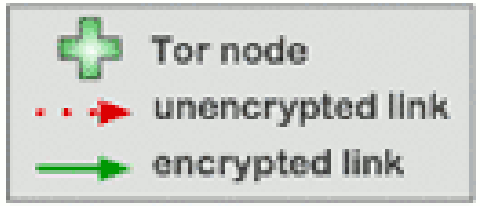
Esquema Básico

- A partir de la información obtenida de su configuración y del servicio de directorio el OP decide un circuito por el que van a circular los paquetes. Por defecto el circuito tienen 3 nodos OR.
- El OP negocia, usando un enfoque telescópico, las claves de cifrado necesarias con cada OR del circuito para proteger sus datos en todo el camino antes de realizar transmisión alguna. La obtención de las claves simétricas (AES-128), una para cada sentido de comunicación (Kf<-forward key, Kb<-backward key), se realiza a partir del protocolo de establecimiento de claves Diffie-Hellman para obtener una clave compartida y a partir de ella derivar las dos claves simétricas. El circuito es construido desde el punto de entrada (usuario) de la siguiente forma: Los mensajes para negociar las claves de la comunicación entre ORn y ORn+1 se realizan a petición del OP y retransmitiendo paquetes a través de los nodos OR1,... ORn. En cada paso los mensajes son cifrados con las claves de sesión negociadas, o cuando no lo están, con la clave de onion del host que recibe el dato
- A continuación cifra el paquete que contiene la clave para el último OR del circuito,
- A continuación hace lo propio del penúltimo
- Hace lo mismo con todos los nodos hasta hacer lo propio con el paquete para el primer nodo.

Esquema básico (continuación)

- Envía el paquete resultante al primer nodo del circuito. Observar que el paquete construido con este proceso se puede considerar como un paquete envuelto en varias capas de cifrado. Por eso se usa la metáfora de la cebolla para describir este tipo de método de ruteo
- El primer OR quita 'su' capa de la cebolla y envía el paquete al siguiente nodo
- Según va llegando el paquete a cada OR éste pela la capa externa. De esta forma ningún OR puede hacerse con la imagen completa del circuito ya que sólo conoce los OR/OP anterior y posterior.
- Como terminología se llama 'exit server' o 'exit node' al último servidor del circuito (y por tanto el único que se comunica con el destino), el primer OR se le llama 'entry node' (único que se comunica con el origen de la comunicación) y al resto de nodos se les llama middle-node.
- Podemos observar que la forma en la que se establecen las claves y todas estas capas de cebolla que se construyen con ellas permiten que la información permanezca secreta mientras va circulando por el circuito de nodos OR. Además, al estar el cifrado de las capas basado en claves de sesión, aunque un atacante recopilara todos los mensajes no podría descifrarlos una vez que estas claves de sesión son descartadas por el OR (perfect forward secrecy).

How Tor Works: 1



Alice

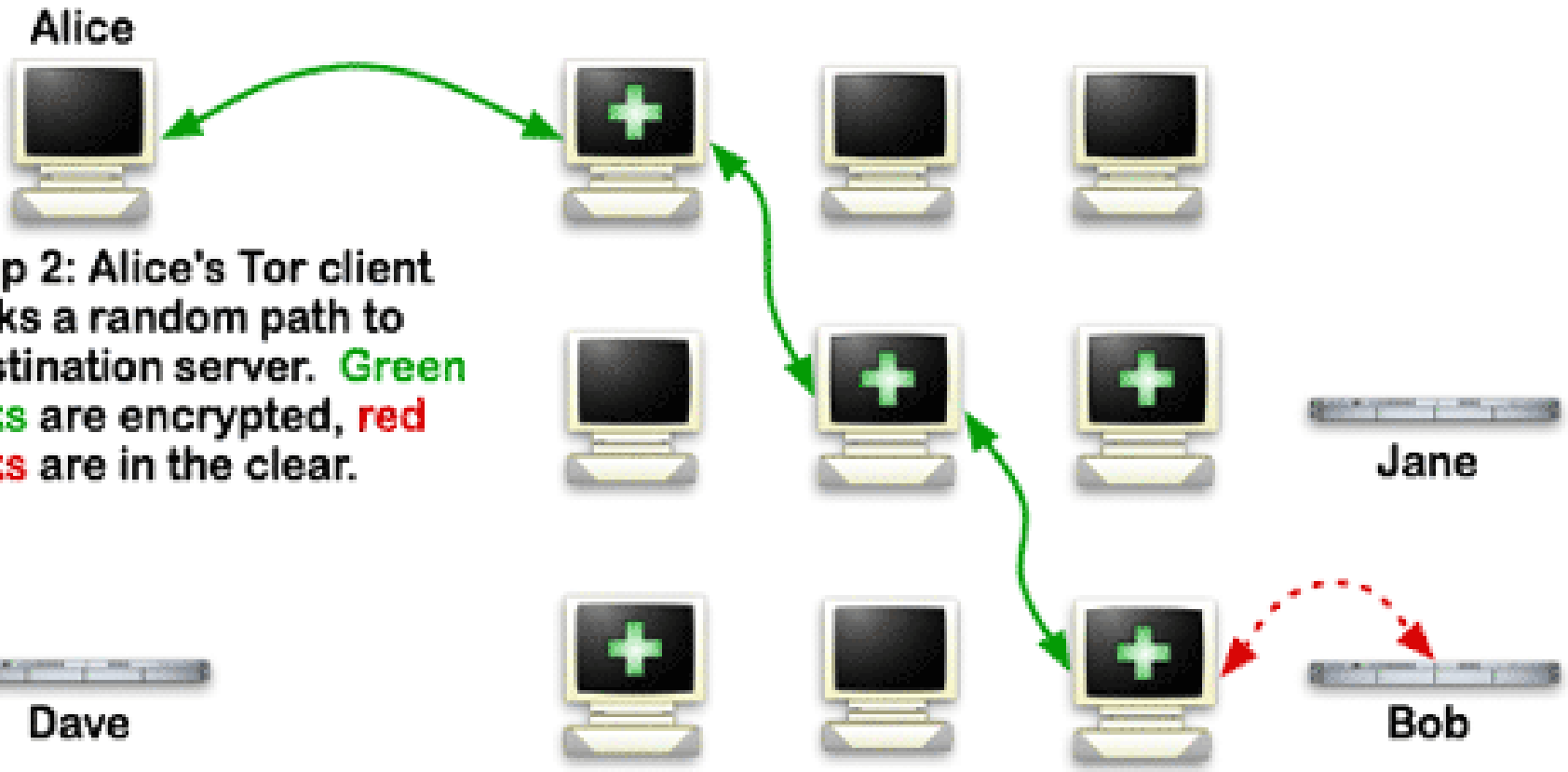
Step 1: Alice's Tor client obtains a list of Tor nodes from a directory server.

Jane

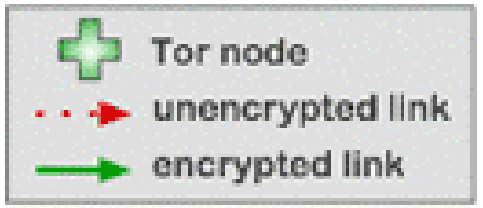
Dave

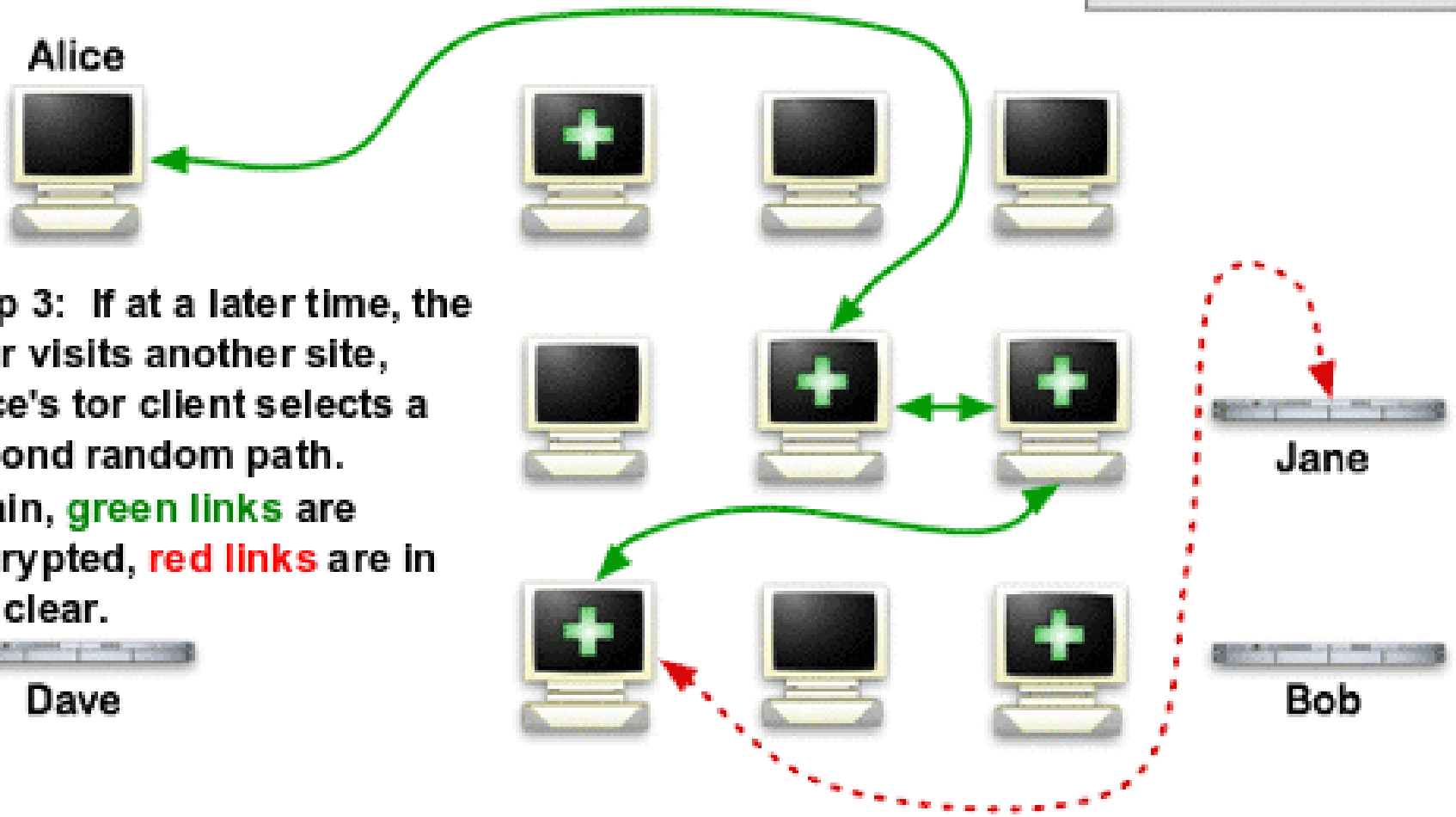
Bob

How Tor Works: 2



How Tor Works: 3





Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path. Again, green links are encrypted, red links are in the clear.

Puntos de Encuentro

Denominados por las siglas RP (*Rendezvous Points*), es, en lugar de explícitamente enviar un paquete a un destino, establecer un punto de encuentro que actúe como nivel de indirección. De esta forma desacoplamos el acto de enviar del acto de recibir. Cada extremo de la comunicación envía sus mensajes a ese punto de encuentro y desde ahí son enviados a donde corresponda usando circuitos que esconden la localización del destino.

Por ejemplo podríamos usar este sistema para conectarnos a un servidor de chat IRC.

Servicios Ocultos

- Servicios que ocultan la localización (por ejemplo, la dirección IP) de quien provee el servicio (Ej. un servicio web accesible sólo desde la deepweb) se les suele llamar **servicios de localización oculta** (*location-hidden services*) o simplemente **servicios ocultos** (*hidden services*).
- Para soportar esta funcionalidad los proveedores de servicios generan una clave pública y privada para identificar su servicio. Anuncian su servicio a distintos routers, haciendo peticiones firmadas con su clave pública, para que sirvan como punto de contacto. A los routers con esta función se les llama **puntos de introducción**, *introduction point*. El proveedor de servicio asocia a su servicio una FQDN del pseudo-TLD .onion y la publica en un servidor de directorio.
  - La FQDN tiene la forma <valorhash>.onion donde el valor hash es de 16 caracteres en Base32 y está generado usando una función hash sobre la clave pública del servicio.
  - Cuando un cliente se quiere conectar a cierta FQDN (por ejemplo ha encontrado la dirección a través de un sitio web) consulta un servicio de búsqueda (*lookup service*) y este le indica un punto de introducción (*introduction point*) y la clave pública del servicio.
  - Queda claro que estas búsquedas solo se pueden hacer a través de la red ToR para preservar el anonimato.
  - La comunicación siempre se realiza a través de un rendezvous point.

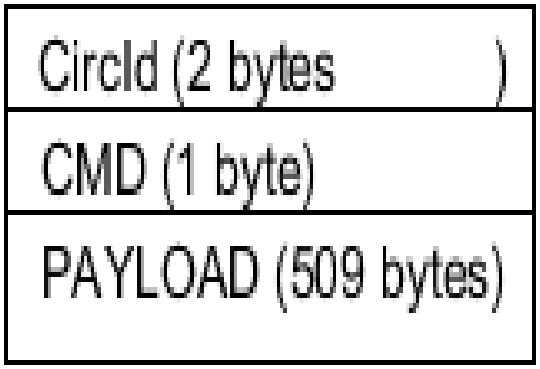
Detalles Técnicos - Células

- Una vez que se establece la conexión TLS, ya sea OP-OR o OR-OR, las entidades se envían paquetes de información estructurada llamadas células.
- Estas células tienen tamaño fijo de 512 bytes y pueden ser enviadas en registros TLS de cualquier tamaño o dividido en varios registros. Los registros de TLS no tienen que revelar ninguna información sobre el tipo o el contenido de las células que contiene.
- Varios circuitos pueden ser multiplexado sobre una misma conexión TLS. Las células están formadas por una cabecera y una carga útil.

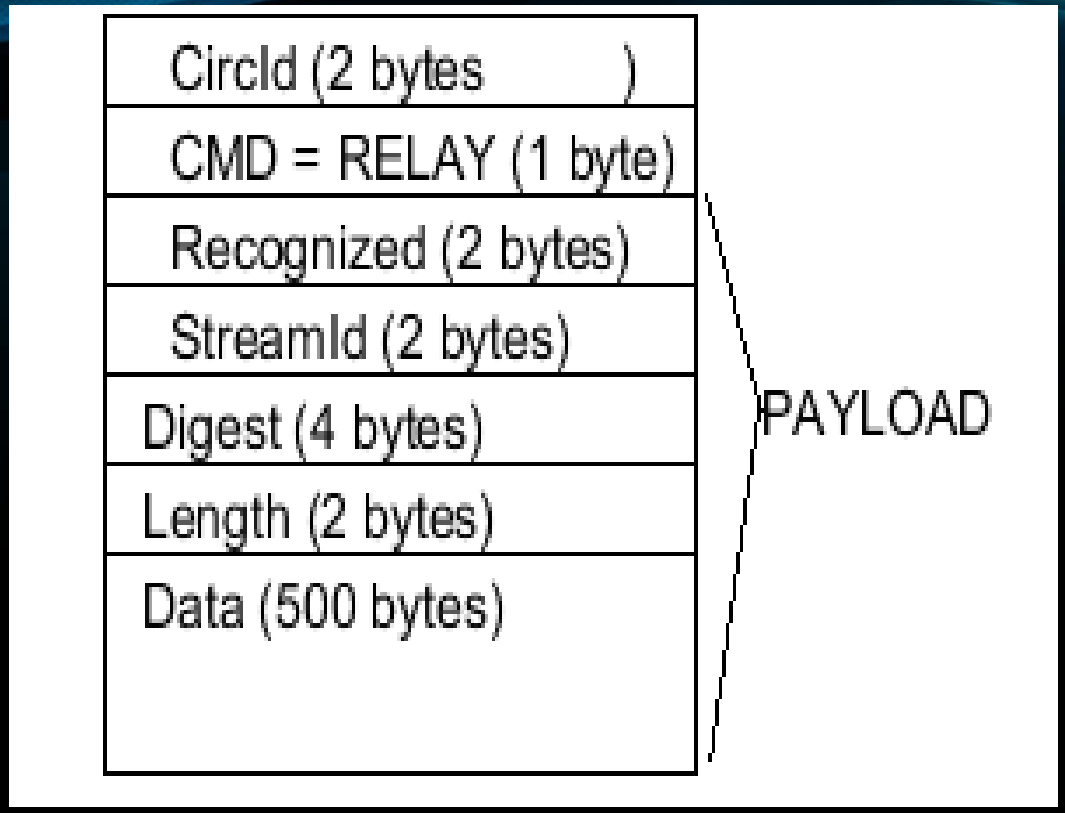
Formato:

- circID.- Es el identificador de circuito y especifica el circuito a el que se refiere la célula
- CMD.- Indica el comando que especifica el significado de la célula. Atendiendo al tipo de comando (valor de CMD)

Tipos de Células



Célula de Control



Célula de Transmisión

Claves en cada OR

- ***Clave larga de identidad o identity Key*** que sirve sólo para firmar información (Ej: descriptor de las capacidades del OR o info de directorio cuando actúa como servidor de directorio) y certificados, y es usado para permitir identificación. Para denotar la clave de identidad de el nodo OR n usamos **PKORn_ID**
- ***Clave mediana de ruteo u Onion Key*** que sirve para cifrar las peticiones de establecimiento de circuito (CREATE) para negociar las claves efímeras. Las claves viejas deben ser aceptadas durante al menos una semana después de que haya sido cambiada para dar tiempo a que todo haya sido actualizado. Para denotar la onion key de el nodo OR n usamos **PKORn_OK**
- ***Clave pequeña de conexión o Connection Key*** usada en el handshake TLS. Esta clave se mete en un certificado que se firma con la clave de identificación. Ambos certificados (certificado de la clave de conexión y certificado de la clave de identificación) se envían en el handshake del TLS.. El certificado de la clave de identificación está autofirmado. Esta clave debería cambiarse frecuentemente, al menos una vez al día.

FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E08 8A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B 302B0A

CIFRADO USADO EN ToR

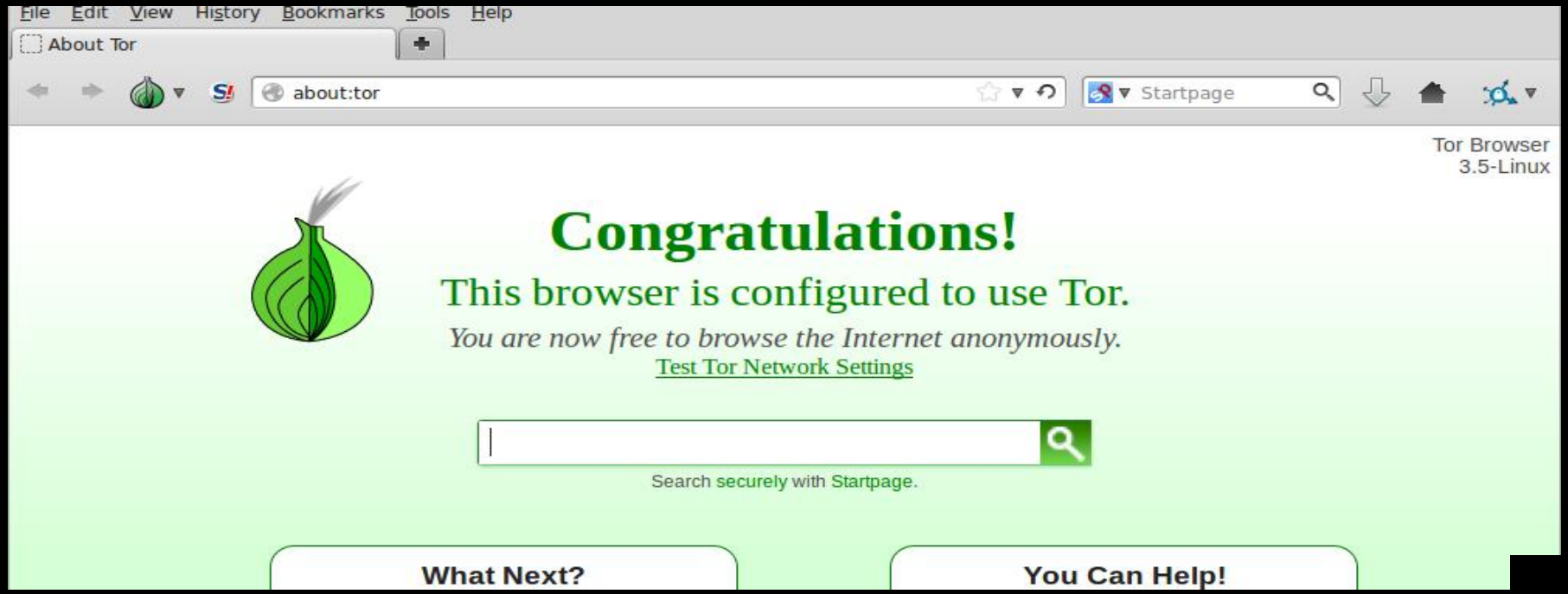
- Para establecer las conexiones se usa estándar TLS. Todos los OR y OP tienen que soportar TLS_DHE_RSA_WITH_AES_128_CBC_SHA. Los OP para comunicarse con los OR pueden usar:
  TLS_DHE_RSA_WITH_AES_256_CBC_SHA,
  TLS_DHE_RSA_WITH_AES_128_CBC_SHA,
- Como algoritmo simétrico de cifrado se usa AES en counter mode (AES-CTR) con claves de 128 bits, con vector de inicialización con todos los bytes a 0
- Como algoritmo de clave pública usa RSA con claves de 1024 bytes y exponente fijo 65537. Usa como esquema de relleno OAEP-MGF1 con SHA-1 usado como hash.
- Como función hash usa SHA-1
- Para establecimiento de claves usa Diffie-Hellman con g=2 y para p usamos el primo seguro de 1024 bits obtenido de RFC 2409 con valor hexadecimal:
  - FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E0 88A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A 431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F4 4C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F2411 7C4B1FE649286651ECE65381FFFFFFFFFFFFFFFF

Detalles para usar ToR de forma segura.

- ToR por si solo no garantiza anonimato, se debe cambiar la forma de pensar y muchas costumbres.
- Usar servicios de VPN y ToR en conjunto como inicio.
- Nunca maximizar el navegador (image canvas).
- Desactivar todo tipo de scripting y extras en los navegadores, java script, extensiones etc.
- No navegar desde tu casa o conexiones sensibles.
- Cambiar periódicamente de circuitos ToR.
- Mantener todo el sistema permanentemente actualizado.
- Preferentemente usar distros GNU/LINUX a tal fin.
- En celulares usar ORBOT + ORFOX + VPN.

ToR Browser

El navegador ToR basado en Código Fuente de Mozilla utiliza la red ToR distribuida y administrada por voluntarios alrededor del mundo: Está diseñado para minimizar el riesgo de espionaje en tus conexiones de internet así como prevenir el aprendizaje de patrones en sitios que visitás, anular la geolocación asi como permitir la navegación en sitios bloqueados.



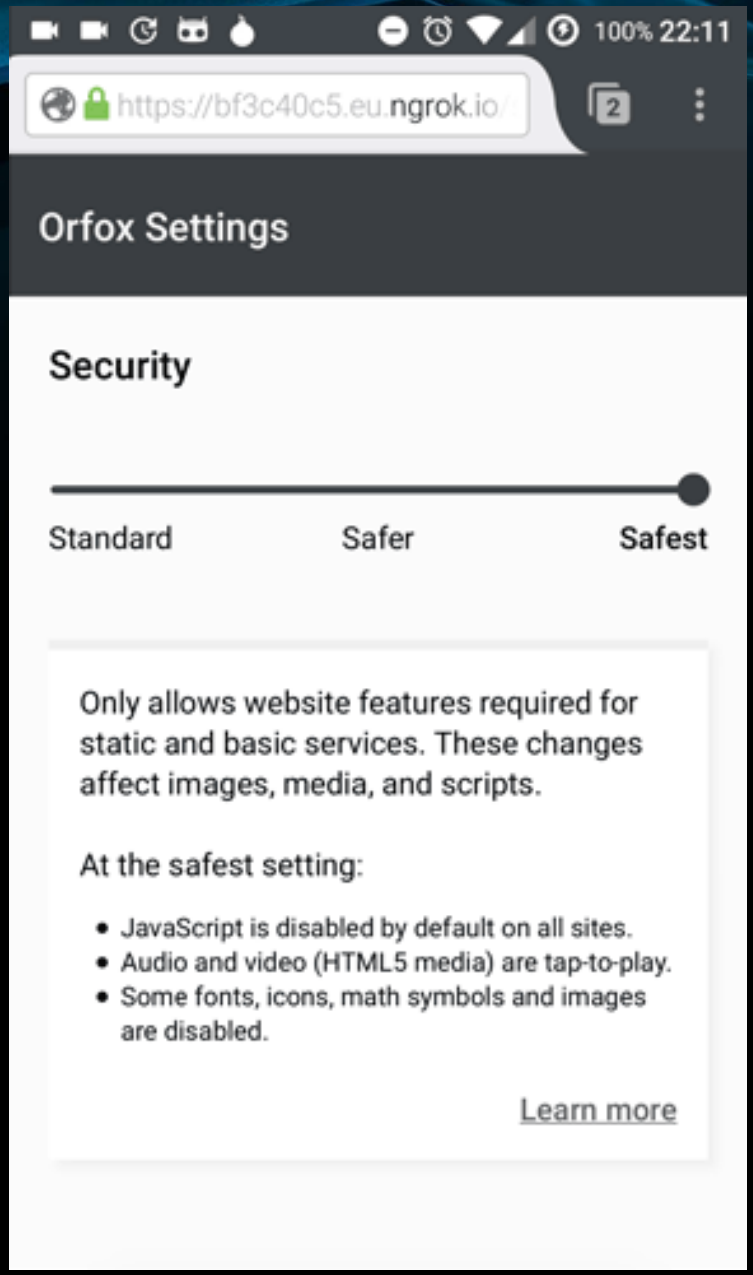
ToR Messenger

- Tor Messenger es un programa de chat multi-plataforma que apunta a ser seguro por defecto y envia todo su tráfico a través de la red ToR. Soporta una amplia variedad de redes de transporte como ser Jabber (XMPP), IRC, Google Talk, Facebook Chat, Twitter, Yahoo, y otros y permite usar mensajería Off-the-Record (OTR) automáticamente.
- Permite además su uso en múltiples idiomas y a través de una interfaz sencilla.

T.A.I.L.S.

- Tails es una distro LINUX live que podés arrancar en cualquier PC desde USB o CD.
- Apunta a preservar anonimidad y privacidad, ayudando a:
  - **Usar Internet anónimamente y saltar enlaces censurados ya que todas las conexiones son forzadas a circular por la red ToR.**
  - **No dejar trazas en la máquina que usás a menos que explicitamente quieras hacerlo.**
  - **Usar herramientas criptograficas de última generación** para cifrar archivos, correos y mensajeria.

Orbot y Orfox en Android



Algunas páginas para comenzar…

- DuckDuck Go el buscador version onion
  - https://3g2upl4pq6kufc4m.onion/
- The hidden WIKI
  - http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page
- NotEvil, el buscador que no quiere ser Google
  - http://hss3uro2hsxfogfq.onion/
- Mail2Tor, servicio de correo Seguro
  - http://mail2tor2zyjdctd.onion/
- Facebook en formato onion
  - http://facebookcorewwwi.onion
- 8Chan la versión ONION de lo que sería 4Chan
  - http://oxwugzccvk3dk6tj.onion/index.html

Problemas legales de los Exit NODES

- La libertad de expresión está protegida por el art. 14 de la CN y el 13 de la CADH.
- Una dirección IP no es necesariamente una persona.
- Las investigaciones por delitos sobre nodos de salida de ToR deben realizarse con la colaboración de fuerzas necesarias entre países y sin pérdida de tiempo.
- El anonimato y la privacidad de las personas no es un delito sino UN DERECHO HUMANO básico.
- A primera instancia no existe delito alguno en brindar tráfico de salida a la red ToR, de la misma forma que brindarle wifi a un amigo tampoco lo es.

Problemas legales de los Exit NODES

¡GRACIAS POR TODO!

- **Ing. Fernando Villares – 10/2017**
- **https://www.intelix.com.ar**
- **@fmvillares en twitter**
- **Bajo licencia Creative Commons Atribución-CompartirIgual 4.0 Internacional (CC BY-SA 4.0)**