REDES DE ANONIMATO
Tor

Mauricio Pasquier Juan
11/02/2010

Índice de contenido

Introducción

> *"If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place."*
>
> *Eric Schmidt, CEO de Google*

> *"Too many wrongly characterize the debate as 'security versus privacy'. The real choice is liberty versus control."*
>
> *Bruce Schneier, experto en seguridad informática*

A lo largo de este trabajo se hablará sobre anonimato, lo que significa en internet y el peligro que sufre actualmente. El anonimato es deseable por varias razones, de las cuales serán analizadas las más importantes. Se analizará la importancia del efecto red en las redes de anonimato.

Existen varias iniciativas para proveer una comunicación anónima en internet, orientadas a distintos nichos, resistentes y vulnerables a diferentes ataques y con características y tecnologías muy variadas. Se verán las tecnologías más importantes: mixes, proxies, enrutamiento de cebollas, enrutamiento de ajos y circuitos telescópicos.

Se hará foco en **Tor**, una red superpuesta orientada a la conexión que usa circuitos telescópicos para proveer de anonimato a cualquier aplicación que utilice **flujos** TCP para la comunicación (e.g. navegación web, acceso ssh, chat). Tor se propone anonimizar el canal de comunicación, no los datos que lleva (normalmente es usado con otras aplicaciones para aumentar el anonimato). Logra esto creando circuitos que pasan a través de varios **nodos**, con la característica de que un `nodo n` conoce sólo la identidad del `nodo n-1` y del `nodo n+1`, o sea, el anterior y el posterior en el circuito. El tráfico fluye en forma de **celdas** de longitud fija, que viajan envueltas mediante encriptación simétrica y son "peladas", como las capas de una cebolla, de nodo a nodo (de ahí el nombre de este tipo de redes). Se verá en detalle cómo es la red, el proceso de conexión y las decisiones de diseño tomadas durante su desarrollo.

A lo largo del trabajo se tratará de vincular extensivamente a la documentación utilizada, y se recopilará la misma en un apéndice.

Todo el trabajo será realizado con tecnología libre y en formatos estándar y publicado en el blog: http://redescebolla.wordpress.com.

Anonimato

> *“This demonstrates the value of not being seen.”*
>
> *Monty Python, How not to be seen*

En contra de la creencia de la mayoría de los usuarios de internet, raramente somos anónimos al conectarnos. Esto es en parte debido a las características de los protocolos fundamentales de internet (**TCP/IP**) y en parte debido a la combinación de políticas de privacidad débiles de los proveedores de servicio (e.g. ISPs, buscadores, redes sociales) con leyes invasivas cada vez más cercanas al Gran Hermano de Orwell.

¿Qué quiere decir “anonimato” en internet?

La comunicación entre clientes y servidores en internet funciona principalmente mediante la pila de protocolos TCP/IP. En este modelo, cada **host** (cada equipo conectado a la red, funcione tanto de cliente como de servidor) necesita una dirección IP, prácticamente única. Esta dirección es un identificador global en internet, lo que significa que, mientras dure nuestra conexión, todas nuestras acciones están relacionadas por esa dirección IP. No es posible conectarse a internet sin una.

La asignación de direcciones se realiza a través de entes reguladores (e.g. LACNIC), que habilitan a distintas organizaciones o empresas, en especial a los **Proveedores de Servicio de Internet** (ISP), a administrar un **rango de IPs**. A su vez, los ISPs distribuyen estas direcciones entre sus clientes, ya sea asignando permanentemente una misma IP a un mismo cliente (**IP estática**) o asignando una IP tomada al azar entre las disponibles en el momento (**IP dinámica**). Es así como a través de una IP se puede obtener gran variedad de información sobre el host, como por ejemplo una localización geográfica bastante aproximada o el historial de navegación desde dicha dirección. Son datos como estos los que ponen de manifiesto que no somos anónimos al conectarnos a internet. Aunque es ampliamente utilizado el uso de pseudónimos (e.g. nicknames, cuentas de usuario), que permiten mantener una comunicación periódica con anonimato, para esto debe ser imposible vincular el pseudónimo con el usuario real.

Un atacante podría fácilmente averiguar información privada interceptando las conexiones TCP que se realizan desde nuestra máquina a internet, o desde internet hasta un servidor, y en ambos casos recorrer la ruta inversa de los paquetes de datos hasta llegar al otro extremo de la conexión, descubriendo así que Alice se conecta con Bob, o que Bob recibe conexiones de Alice. Por otro lado, puede no existir un atacante, sino que simplemente nosotros deseamos permanecer anónimos a un determinado servicio. En términos simples, ser anónimo en internet quiere decir que no se puede determinar que uno es el origen y/o el destino de cierta conexión que ha interceptado. Esto se logra ocultando la información que proveen los paquetes IP.

¿Por qué se necesita el anonimato?

Existen varias razones por las que alguien podría querer ser anónimo en la web, entre las que destacamos:

- es sabido que los ISPs y los buscadores en general venden la información registrada de la actividad de sus usuarios. Si bien es esperable que no provean identificación del usuario, se ha probado que se puede deducir la identidad de un usuario en base a dicha información supuestamente anónima. Un usuario puede querer evitar este uso de su actividad online.
- es común que los buscadores y otro tipo de servicios (e.g. YouTube) restrinjan el acceso a diversa información de acuerdo al país de origen de la solicitud (e.g Argentina), en base a leyes, regulaciones, o incluso amenazas de juicios. Para los proveedores de servicios es más simple censurar que hacer frente a una posible instancia judicial. Mediante el anonimato puede evitarse este tipo de censura arbitraria.
- el usuario puede querer investigar o aprender sobre temas delicados para la opinión pública (e.g. enfermedades, prácticas sexuales).
- a partir de una dirección IP, es posible recabar mucha información sobre el host realizando la solicitud. Un usuario puede querer evitar que esta información privada esté disponible para terceros.
- el cliente puede necesitar realizar una denuncia de manera anónima (e.g. para denunciar prácticas ilegales en su lugar de trabajo sin arriesgarse a ser despedido al ser descubierto).
- mediante el anonimato pueden recuperarse temporalmente las garantías básicas de libertad de expresión, de culto o de conciencia, por ejemplo, que no suelen mantenerse durante regímenes dictatoriales.
- el anonimato protege de abusos de los que tienen más poder. Si siguen las tendencias actuales respecto de la privacidad, será cada vez más importante para los usuarios disponer de una técnica confiable de ser anónimos durante su actividad online.
- simplemente hacer valer sus derechos fundamentales.

El efecto red

Al momento de elegir qué sistema usar para proveer anonimato, es importante considerar el efecto red además de las características intrínsecas de seguridad del sistema: ¿cómo afecta a la seguridad de cada usuario la cantidad de usuarios que usan el sistema?

Existen estudios que indican que la usabilidad de un sistema (que repercute directamente en la cantidad de usuarios que ingresan al mismo) tiene tanta o más relevancia al elegir qué sistema usar que lo seguro que sea el sistema técnicamente. Este tipo de estudios analizan el **conjunto de anonimato**, que es el conjunto total de personas que podrían llegar a ser los participantes reales en la comunicación de interés para un atacante. Mientras más grande es este conjunto, más improbable es que el atacante detecte al verdadero responsable. Entonces, se dice que "el anonimato ama la compañía". No se puede ser anónimo sin un conjunto de anonimato suficientemente variado. Por ejemplo, si una organización creara un sistema de anonimato para sus miebros, cualquier conexión procedente de dicho sistema sería fácilmente correlacionable con algún miembro de esa organización. En cambio, en un sistema de confianza distribuida, la variedad de usuarios, procedencias y tipos de conexión protege de esos ataques.

La cantidad y variedad de personas y organizaciones que usan Tor es la razón principal por la que este trabajo se enfoca dicho sistema.

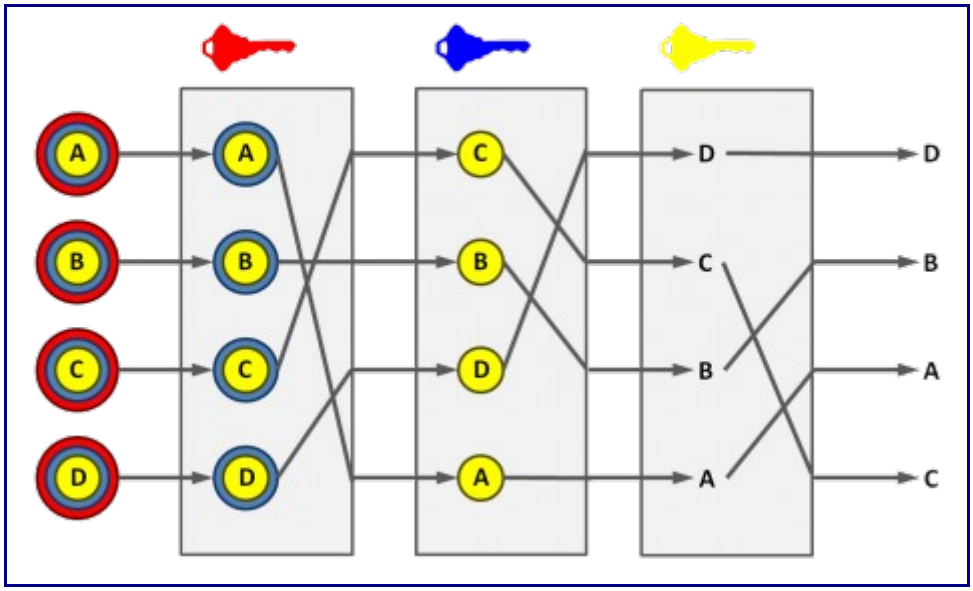
Tecnologías

> *"Capas. Las cebollas tienen capas. Los ogros tienen capas. ¿Entiendes? Ambos tenemos capas."*
>
> *Shrek*

Mixes o mix networks

Los **mixes** o **redes de mezcla** se retrotraen a los inicios de la década del '80. Inventados por David Chaum, usan una cadena de servidores proxy para crear una instancia de comunicación difícil de rastrear.

Básicamente, funcionan de la siguiente manera: el mensaje a enviar (A) es encriptado por el cliente con la clave pública de cada uno de los servidores proxy a recorrer. Luego es enviado al primer proxy de la cadena, el cual remueve su capa de encriptación, lo demora en espera de más mensajes (B, C y D), y los reenvía al siguiente proxy de la cadena en un orden distinto al de llegada, hasta que el último proxy obtiene el mensaje original y lo envía a destino.



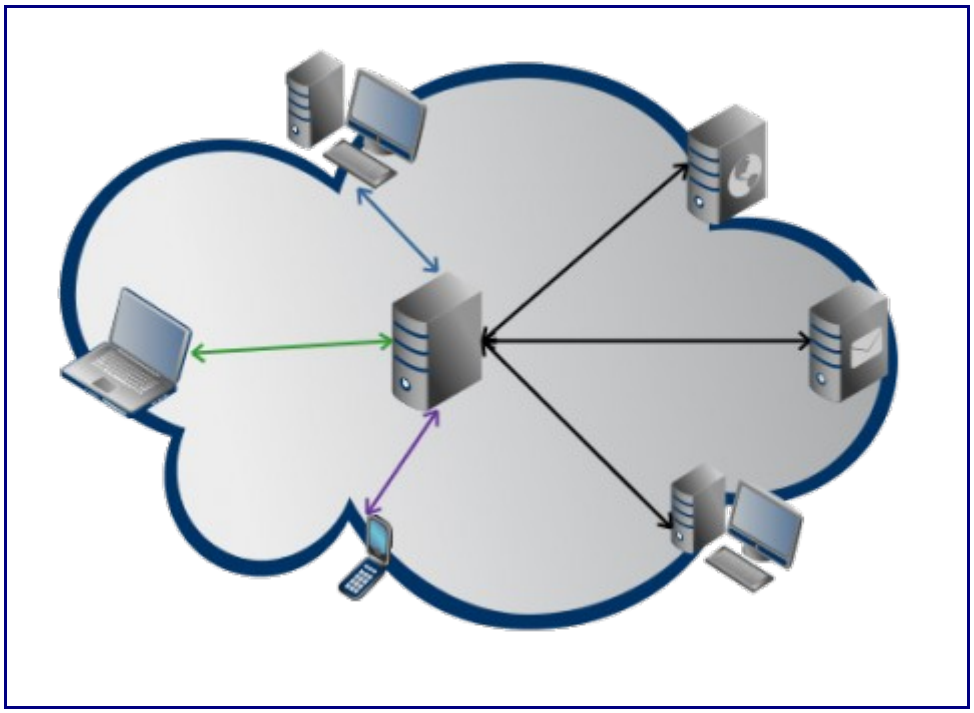
Gracias a la encriptación en capas entre proxies y a la demora y reordenamiento los ataques de confirmación de tráfico, un observador no puede determinar qué mensaje de salida corresponde a qué mensaje de entrada (específicamente, se evitan los ataques de análisis de tráfico y de confirmación de tráfico). Se utiliza una cadena de proxies para disminuir la probabilidad de que el servidor esté controlado por un atacante (si al menos uno de los servidores de la cadena es honesto, se preserva algo de anonimato).

El problema que acarrea este enfoque es la altísima latencia que tiene la red, dado que se utiliza encriptación de clave pública en cada salto, además de las demoras voluntarias. Es útil para aplicaciones como el email, que no requieren respuestas en tiempo real.

Las mejoras sobre el trabajo de Chaum se orientaron en dos direcciones: reducir la latencia para poder anonimizar tráfico interactivo, o aumentar y hacer variable la latencia para maximizar el anonimato contra atacantes globales. Mixminion es una de las últimas versiones de este segundo enfoque: un protocolo anónimo de reenvío basado en mensajes.

Proxies de un salto

Cuando el esfuerzo por anonimizar se concentró en flujos interactivos que requieren baja latencia, surgieron los **proxies de un salto**. Son servidores proxy que concentran una gran cantidad de flujo entrante, aumentando el **conjunto de anonimato** (la cantidad de personas entre las que un usuario determinado está escondiendo su identidad) al tiempo que remueven la información que indica el origen de los datos y retransmiten.



Son un punto único de falla, son vulnerables a un observador global que pueda correlacionar el tráfico entrante y el saliente, y además, es necesario confiar en que el servidor proxy es honesto.

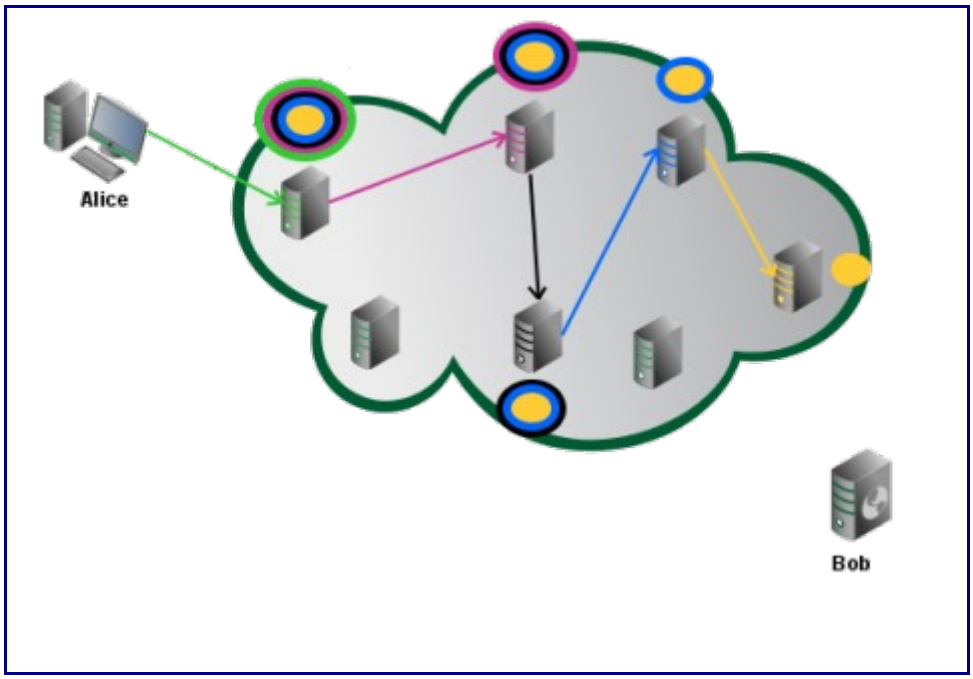
Enrutamiento de cebollas

Algo más complejos que los proxies de un salto son los sistemas de confianza distribuida orientados a la conexión. Con estos sistemas el usuario establece una conexión encriptada punto a punto bidireccional, y envía a través de la misma los datos en forma de celdas de tamaño fijo.

Establecer los circuitos es caro computacionalmente y suele requerir criptografía de clave pública, mientras que retransmitir las celdas es comparativamente gratis y normalmente sólo requiere encriptación simétrica. Dado que un circuito atraviesa varios servidores y cada servidor sólo conoce a los adyacentes en el circuito, ningún servidor puede vincular a las partes (Alice y Bob) de la comunicación.

El Enrutamiento de cebollas pertenece a este tipo de estos sistemas. La creación de un circuito en este diseño involucra la propagación de un mensaje inicial que tiene la forma de una estructura de

datos especial (patentada en Estados Unidos), la **cebolla**, que consiste en una capa de encriptación por cada nodo que vaya a formar parte del circuito (predeterminados por el creador del circuito). Una vez removida su capa correspondiente, el **Router de cebollas** descubre la dirección del siguiente nodo y una clave de sesión que será usada para la encriptación simétrica con el cliente. Entonces reenvía la estructura de datos al siguiente salto. Una vez formado el circuito, el cliente puede enviar celdas de datos mediante encriptación simétrica con las claves de sesión.



Enrutamiento de ajos

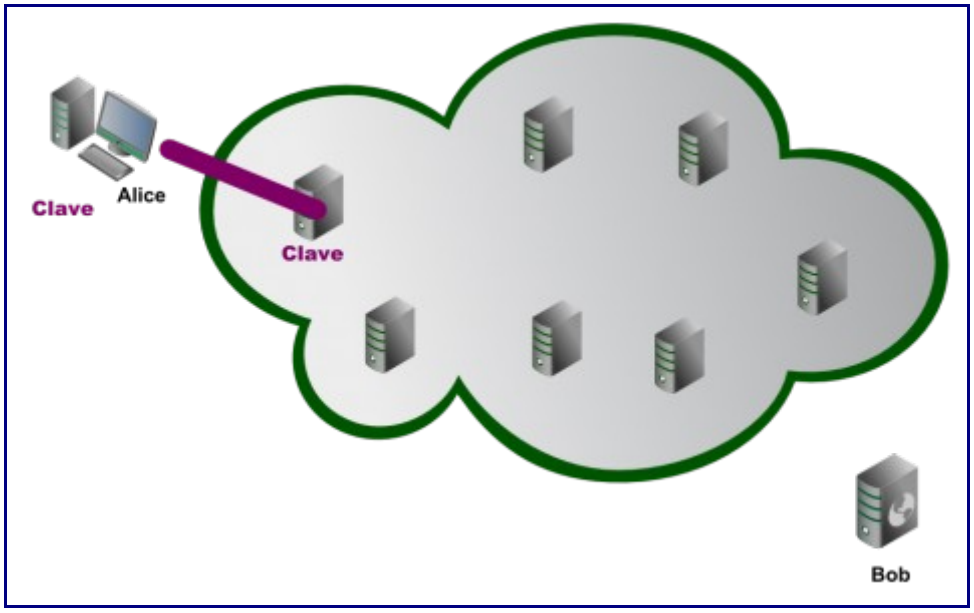
El Enrutamiento de ajos es una extensión del enrutamiento de cebollas, en la que la estructura de datos fundamental (el **ajo**) es similar a la de su antecesor, pero a su vez tiene la capacidad de contener un número de mensajes (**dientes**), también encriptados junto a información de enrutamiento, que se enrutan por separado una vez que el nodo ha eliminado la capa de encriptación que le corresponde. Estos mensajes se usan tanto para el tráfico de datos de usuario como para mensajes de control entre routers, entre otras cosas, lo que ayuda a hacer indistinguible un tipo de tráfico del otro, promoviendo el anonimato. Es usado principalmente en la red I2P.

Circuitos telescópicos

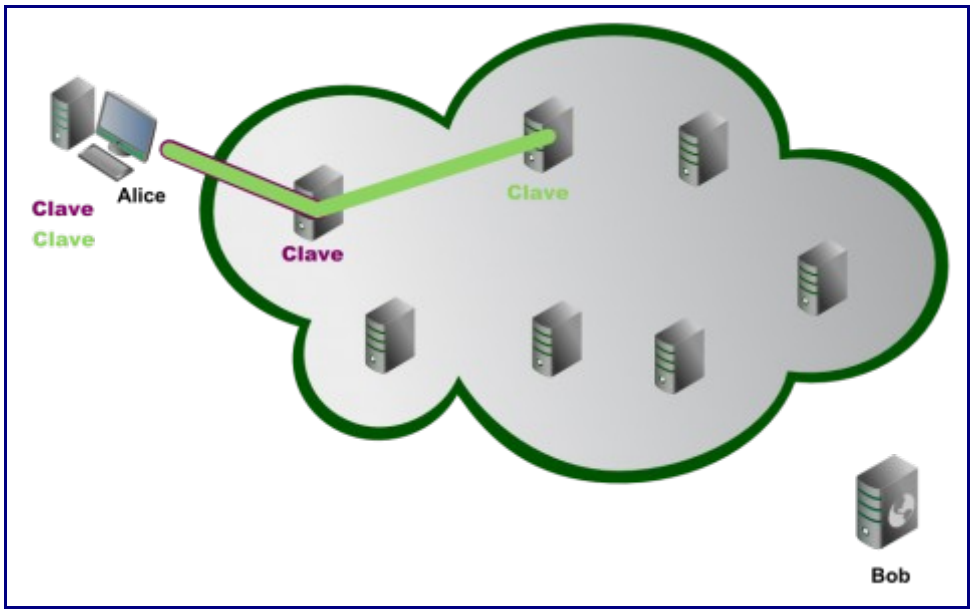
Los circuitos telescópicos son el nucleo de la segunda generación del Enrutamiento de cebollas: Tor reemplaza la creación de circuitos en un sólo paso de su antecesor por la creación en etapas, extendiendo el circuito un salto a la vez y negociando con cada uno una clave de sesión temporal, a través del túnel creado con su anterior. Este esquema supera varias desventajas del anterior, como la posibilidad de que el cliente sepa cuando un nodo que ha seleccionado no responde, o la vulnerabilidad a ataques de predecesor.

El proceso de creación de circuitos es el siguiente: Alice elige un nodo de entrada a la red (también llamados **entry guards**) y crea una conexión TLS a la misma. Una vez realizada la conexión, ambos determinan un **secreto compartido** usando el algoritmo Diffie-Hellman. Este secreto es la clave de sesión efímera usada por ambos para encriptar y desencriptar las celdas transmitidas de

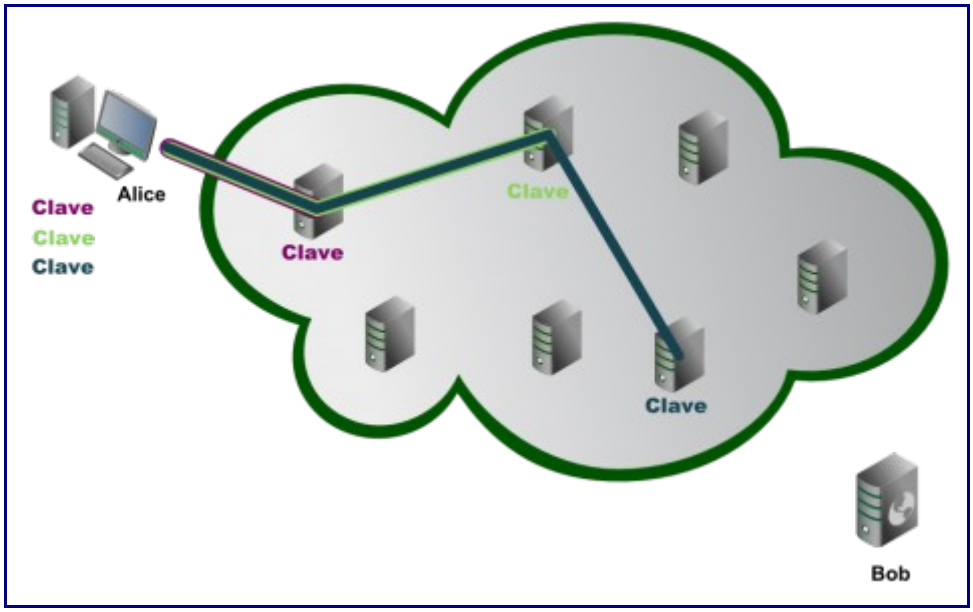
uno a otro, formando un túnel.



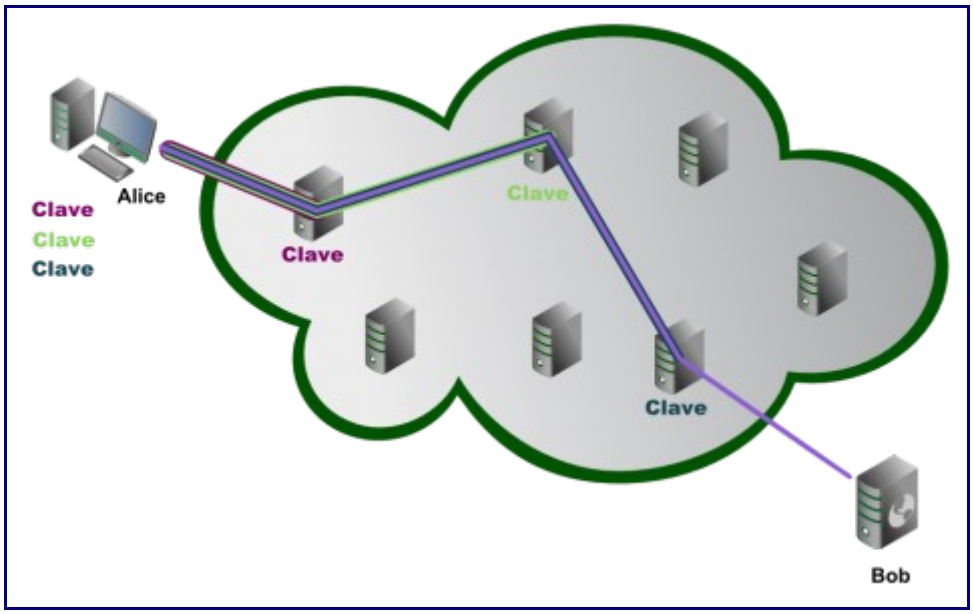
Ahora Alice tiene un túnel que llega al nodo de entrada. A través del mismo, realiza una conexión TLS con el siguiente nodo del circuito, y nuevamente negocia un secreto compartido que servirá de clave de sesión mientras dure el circuito. Ahora Alice tiene un túnel al segundo nodo que atraviesa el túnel ya creado al primer nodo (se empieza a ver por qué el diseño se llama de **circuitos telescópicos**).



La sucesiva extensión del circuito y creación de túneles continúa mientras el cliente lo desee. En la actual implementación de Tor, la extensión de los circuitos está fijada en 3 saltos.



Una vez creados todos los túneles, Alice envía un mensaje al último nodo del circuito (**nodo de salida** o **exit node**) pidiéndole que acceda al servicio de Bob. Como cada nodo sólo sabe de su antecesor y su posterior, este nodo no conoce la identidad de quien solicita la conexión, o sea, no sabe para quién está creándola.



Ahora Alice puede empezar a enviar datos, cifrados con cada clave de sesión en el orden inverso al que van a ser recorridos los nodos, a través de estos mismos. Al llegar a cada nodo, la capa de encriptación correspondiente es removida, tal como ocurría con las cebollas, hasta el nodo de salida, que envía el flujo hacia Bob. Hay que aclarar que los datos entre el nodo de salida y Bob no están cifrados por Tor. Si dicha propiedad es importante (y debería serlo para alguien que está usando Tor para obtener anonimato) es necesario usar otras herramientas como Privoxy junto con Tor.

Enfoque en Tor

> *"La Libertad significa libertad para decir que dos más dos son cuatro. Si eso se admite, todo lo demás se da por añadidura."*
>
> *Winston, 1984*

Propiedades

Esta es una lista parcial de las propiedades más importantes de Tor:

- Es una red superpuesta sobre Internet
- Protege contra ataques de análisis de tráfico
- Promueve activamente la facilidad de uso
- Tiene alta visibilidad
- Vive en el espacio del usuario
- Es multiplataforma
- Está ampliamente documentado
- Es software libre
- Tiene una gran base de usuarios

Es una red superpuesta sobre Internet

La topología de Tor consiste en una cantidad de **Retransmisores Tor** (también llamados Enrutadores de cebollas, nodos u OR), administrados por voluntarios, que mantienen conexiones TSL (sobre TCP/IP) permanentemente entre sí, para formar esta red. Los **Clientes Tor** (proxies de cebollas u OP) los ubican mediante una base de datos semidistribuida, para solicitarles que retransmitan sus flujos TCP y así lograr anonimato.

Los Retransmisores se dividen en varios tipos, relativos al uso circunstancial que le de un cliente (i.e. de entrada, medios, de salida). Primeros en orden de importancia están los **nodos de salida** (exit nodes), que son los que comunican la red Tor con el exterior. Dado que son la cara visible de todos los usuarios de la red, es frecuente que sean bloqueados por abuso en diferentes sitios. Para reducir el riesgo, Tor permite fijar políticas de salida (e.g. bloquear el puerto 25 para anular el spam, limitar el ancho de banda cedido).

Protege contra ataques de análisis de tráfico

El objetivo de Tor, determinado por su Modelo de amenazas, es proteger contra el análisis de tráfico. Básicamente, Tor dificulta que un atacante actuando como cliente descubra el destino de una conexión, que un atacante actuando como servidor descubra el orígen de una conexión, y que un grupo de Retransmisores vinculen al cliente con los destinatarios de sus conexiones.

Promueve activamente la facilidad de uso

Los desarrolladores de Tor enfatizan la facilidad de uso del sistema como medida de aumentar el conjunto de anonimato, es decir, la base de usuario. Con este fin han creado el controlador visual

Vidalia, y los paquetes de aplicaciones preconfiguradas que incluyen en un mismo instalador Tor, Vidalia, Torbutton, Polipo, Firefox, y Pidgin.

Tiene alta visibilidad

Tor tiene un gran apoyo de las comunidades de académicos (que repercute, por ejemplo, en papers y estudios formales sobre su funcionamiento) y hackers (que colaboran, entre otras cosas, en correcciones de bugs, aplicaciones relacionadas, usabilidad). Periódicamente obtiene fondos de organizaciones no gubernamentales (e.g. la EFF), del gobierno, de universidades y de individuos, lo que le permite tener desarrolladores pagos tiempo completo. Esta visibilidad ayuda a aumentar la cantidad de usuarios.

Vive en el espacio del usuario

El software de Tor puede instalarse sin privilegios de administrador, no requiere cambios al kernel (en contraposición a otros enfoques) e incluso existen versiones portables para ser ejecutadas sin instalación.

Es multiplataforma

Existen versiones tanto para los sistemas operativos GNU/Linux, los derivados de BSD, Mac OS X, y Windows (2000, XP, Vista, 7 y las Server Editions). Esta variedad de plataformas soportadas ayuda a que crezca la base de usuarios.

Está ampliamente documentado

Tiene muy buena documentación, actualizada y variada y en diversos idiomas. Los protocoles intervinientes están completamente detallados, y los encargados del proyecto Tor mantienen una biblioteca actualizada de papers sobre anonimato y seguridad.

Es software libre

Tor, y todo el software relacionado con el proyecto, está distribuido bajo licencias libres. Además de la importancia general que tiene el desarrollo de software libre, es específicamente importante en el caso de las redes de anonimato. Que sea libre permite la auditoría por parte del cliente y de los interesados en general, así como la subsistencia al actual grupo de desarrolladores. El hecho de que el funcionamiento interno del programa sea conocido por todos, incluso por los atacantes, no le quita seguridad al mismo, de acuerdo al principio de Kerckhoff (“Un sistema criptográfico debe ser seguro incluso si todo, excepto la clave, es conocido públicamente”) y a la máxima de Shannon (“El enemigo conoce el sistema”).

Tiene una gran base de usuarios

Esto se debe a que los desarrolladores han entendido que el número de usuarios participantes en un sistema de anonimato es tanto o más importante que las características técnicas que protegen la privacidad. Activamente buscan facilitar el ingreso, bajando barreras técnicas, promoviendo a Tor, investigando, haciéndolo portable a distintas plataformas, mejorando su interfaz, etc.

El ecosistema de Tor

Hay una variedad de aplicaciones que trabajan en conjunto para que la red Tor sea funcional, segura y usable. Estas son algunas de ellas:

- Tor
- Vidalia
- Polipo
- Torbutton
- TorDNS

Tor

Tor, el llamado Proxy de cebollas (OP) es la puerta de entrada a la red. Maneja conexiones entrantes y salientes a través de esta aplicación, y recibe las solicitudes de otras aplicaciones (mediante SOCKS). Cada OP puede ser configurado como Retransmisor (OR), lo que lo convierte en parte de la columna vertebral de red Tor, donde usa parte de su ancho de banda disponible para retransmitir datos de los demás.

Vidalia

Vidalia es una GUI para controlar el servicio Tor, escrita con el framework Qt y multiplataforma (GNU/Linux, Unix, Mac, Windows).

Polipo

Polipo es un proxy HTTP de caché, que maneja SOCKS4a, lo que evita que Firefox envíe las solicitudes de DNS por fuera de la red Tor, poniendo en peligro el anonimato.

Torbutton

Torbutton es una extensión de Firefox que permite habilitar el uso de Tor en el navegador con un simple click. Además, mientras está activado realiza cambios en la configuración para mejorar la seguridad (e.g. desactiva Flash y javascript).

TorDNS

TorDNS es un servidor DNS local, lo que permite que las aplicaciones realicen solicitudes de IPs a través de un nombre de host usando la red Tor.

Modelo de despliegue

Se ha mostrado la tecnología de Tor para la creación de circuitos, las propiedades principales de la red y las diferentes aplicaciones que le dan forman. ¿Pero cómo funciona todo en conjunto?

El componente principal del modelo es Tor en sí. Como ya se ha visto, cada instalación de Tor puede funcionar tanto en forma de cliente (OP) como de retransmisor (OR). Es sólo cuestión de una pequeña configuración. Nada impide a un usuario que quiera acceder a la red Tor como cliente administrar su propio Retransmisor, y de hecho, puede beneficiar su anonimato. El perjuicio es que se comparte el ancho de banda con los demás usuarios de la red, pero como ya se ha probado, un mejor servicio aumenta la seguridad para todos, al aumentar el conjunto de anonimato.

Otra parte fundamental del modelo es algo que anonimizar. Cualquier aplicación que use flujos TCP es plausible de conectarse a Tor, mediante SOCKS. Si una aplicación no utiliza SOCKS o no lo utiliza correctamente, puede interponerse un proxy entre Tor y la aplicación que traduzca dicho protocolo.

Cuando una aplicación necesita a conectarse a la red Tor, primero busca un retransmisor de salida con las políticas adecuadas a la conexión que desea realizar. Esto lo hace mediante las **Autoridades de Directorio**, que guardan dicha y otra información referida a los Retransmisores. No cualquiera puede convertirse en Autoridad de Directorio; se determina si es posible, para cada administrador de Retransmisor, en base al mérito obtenido en el sistema. Actualmente hay seis de estas Autoridades, que replican la información que manejan en los demás Retransmisores para evitar cuellos de botella en el sistema. Si hay diferencias entre las decisiones de las Autoridades, el cliente decide por la opinión mayoritaria.

El siguiente paso es crear el circuito. Una vez hecho esto, se transmiten los datos encriptados simétricamente, y el nodo de salida puede empezar a transmitir el flujo TCP al destinatario. Esta misma conexión sirve para las respuestas del mismo. Tor permite multiplexar varios flujos TCP por un mismo circuito, para minimizar el impacto del tiempo de creación en el retardo de la conexión.

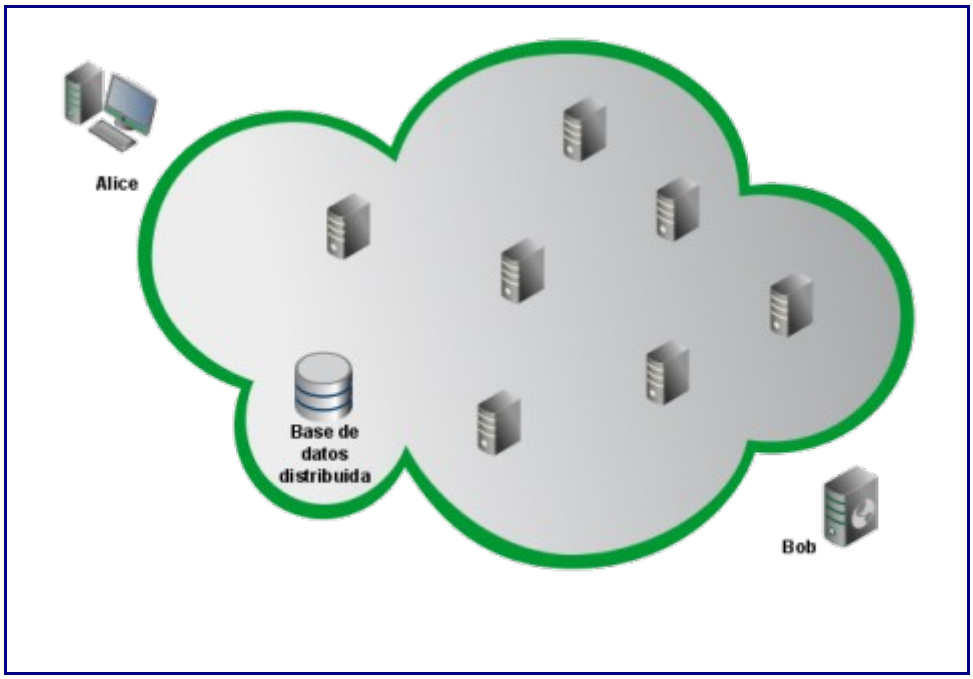
Servicios ocultos o de ubicación oculta

Ya vimos cómo logra un usuario conectado a Tor ser anónimo para el servicio (Bob) al que accede. Pero, ¿qué pasa si es Bob el que desea permanecer anónimo? Para esto existen los **servicios ocultos**

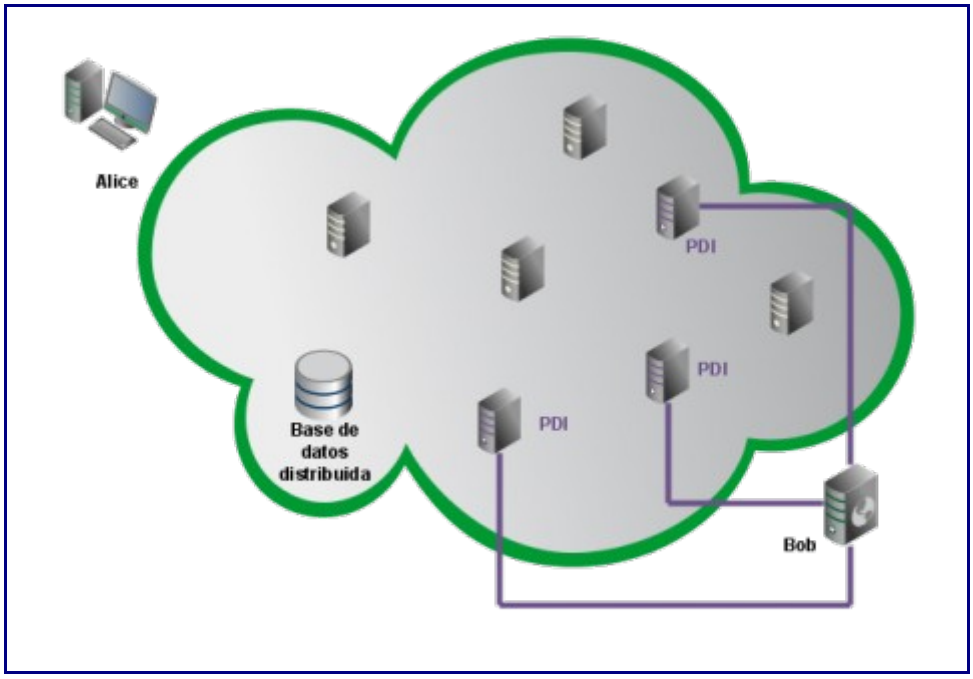
o de ubicación oculta (location-hidden services). Mediante un servicio oculto, es posible ofrecer un servidor en la red Tor sin una IP que lo identifique, con la desventaja de que es necesario accederlo a través de Tor.

Cómo funcionan, paso a paso

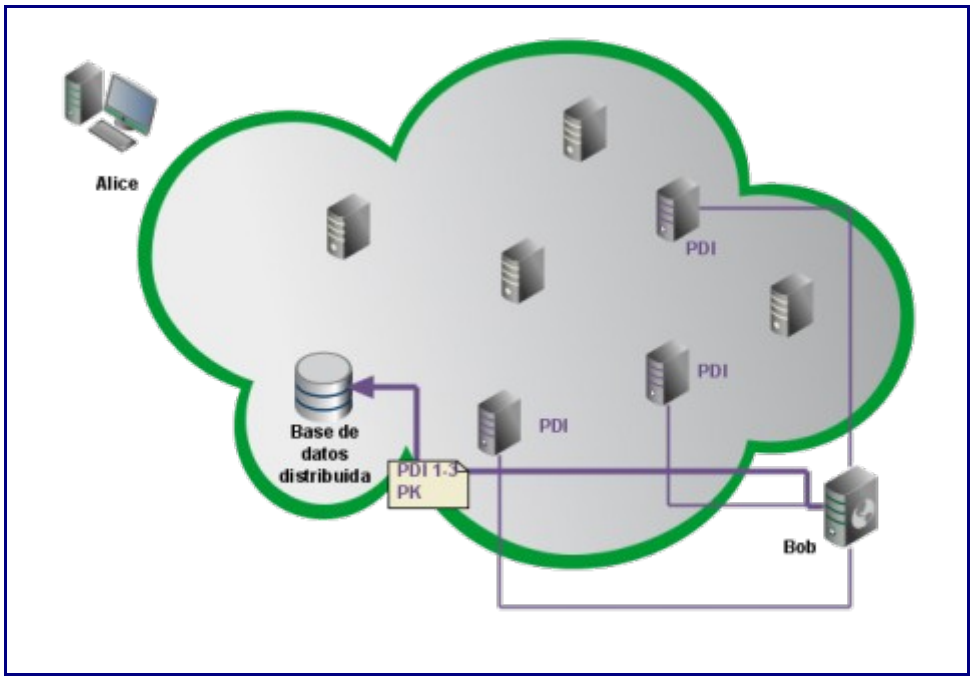
Supongamos que Bob quiere ofrecer un servidor web anónimo. Después de la configuración, Tor genera una par de claves pública/privada que identifican al servicio. Con la clave pública, genera un **digest**, que forma parte de la dirección del servicio (e.g. `l73fuoioj5hzznxc`), junto con el pseudo dominio de nivel superior (**pseudo TDL**) `.onion`, dando como resultado la dirección por la que se accede al servicio: `http://l73fuoioj5hzznxc.onion`.



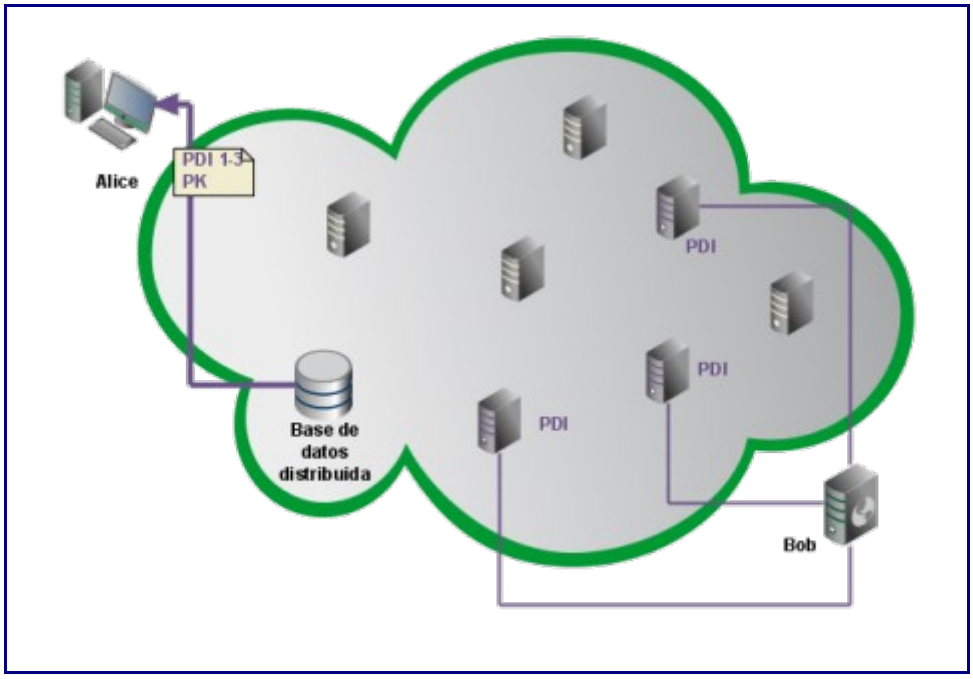
Para lograr la alcanzabilidad del servicio en la red Tor, el **primer paso** es elegir, aleatoriamente, un grupo de **Routers de Cebollas** (Onion Routers) para que sirvan de **Puntos de Introducción** (Introduction Points) y generar circuitos Tor (o sea, de 3 saltos, encriptados) a cada uno de ellos.



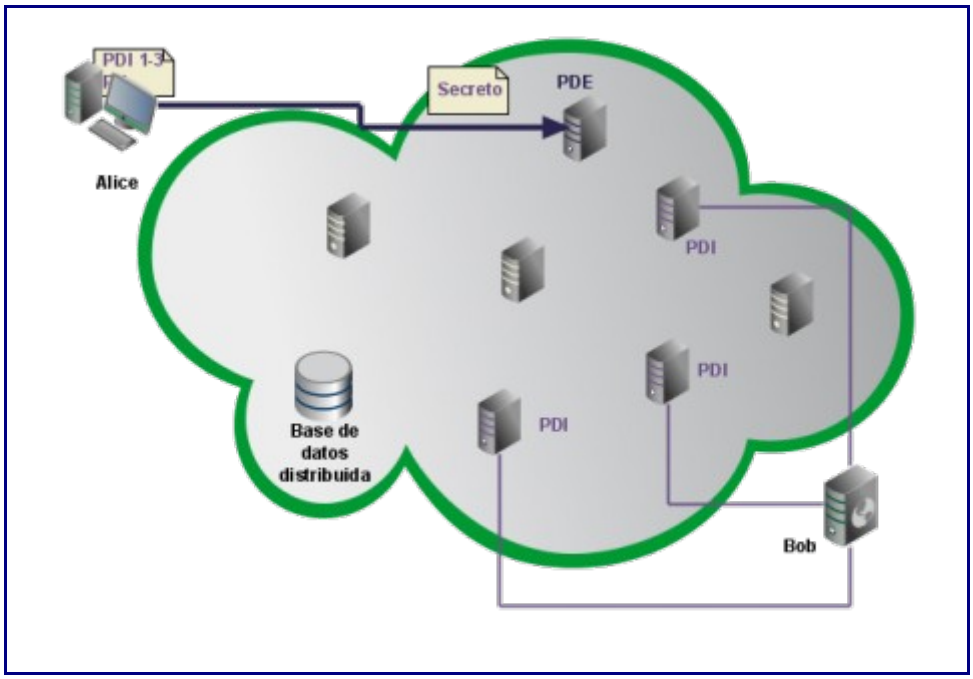
El **segundo paso** es crear un **Descriptor del servicio**, que incluye: la dirección *.onion*, el/los puertos por los que se accede al servicio, una descripción textual opcional y la dirección de los Puntos de Introducción, y firmado con la clave privada. Después es enviado a una tabla hash distribuida, una base de datos de donde cualquier nodo o cliente puede obtener el Descriptor.



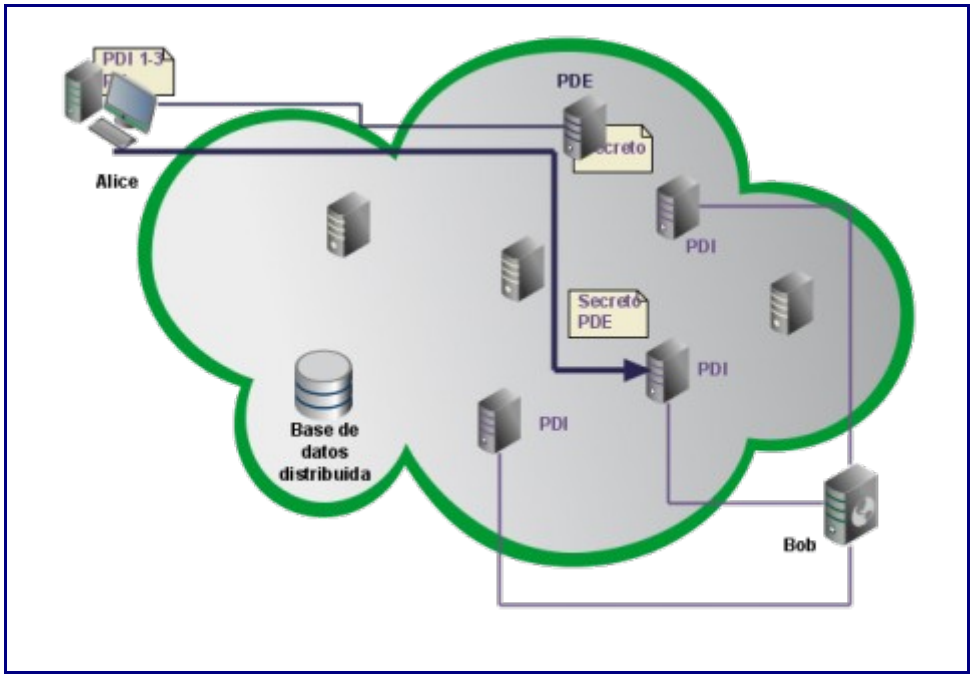
Ahora un cliente (Alice) desea conectarse al servicio. Asumimos que ya conoce la dirección, tal vez porque la vió en un índice de servicios ocultos o Bob se la dijo. Como **tercer paso**, Alice descarga el Descriptor del servicio de la base de datos distribuida y obtiene la dirección de los Puntos de Introducción.



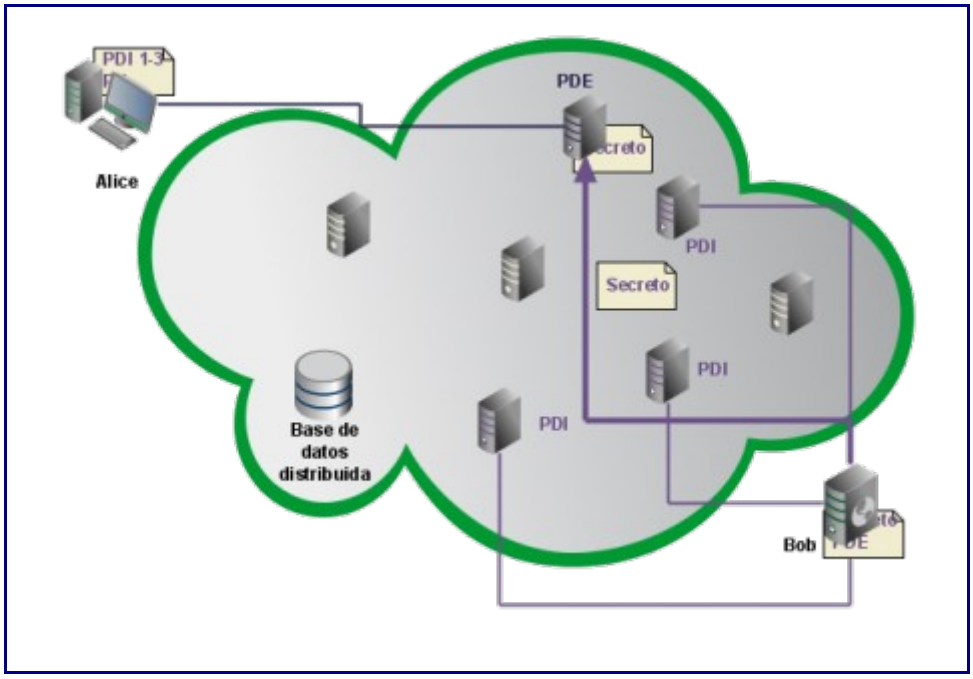
Para el **cuarto paso** Alice ha creado un circuito Tor hasta un nodo cualquiera, pidiendole que actúe como **Punto de Encuentro**. Para esto, le comunica un secreto de un sólo uso, generado para este encuentro.



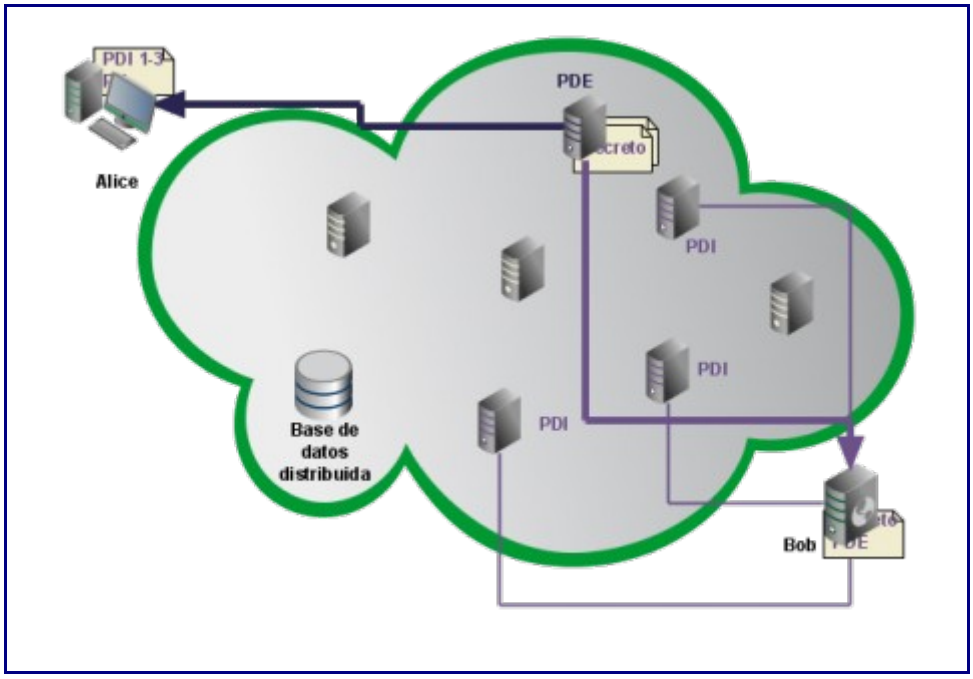
Quinto paso: ahora Alice crea un mensaje de Introducción, encriptado con la clave pública del servicio oculto, que incluye la dirección del Punto de Encuentro y el secreto de un sólo uso, y le pide a alguno de los Puntos de Introducción que se lo envíe al servicio oculto.



En el **sexto paso** el servicio oculto desencripta el mensaje y obtiene la dirección del Punto de Encuentro y el secreto. Crea un circuito Tor hacia dicho Punto de Encuentro y le envía el secreto.



En el **séptimo y último paso**, el Punto de Encuentro notifica a Alice de la conexión establecida, y ambos pueden empezar a comunicarse a través de sus circuitos Tor de manera normal. El Punto de Encuentro simplemente reenvía los paquetes que le llegan, que están encriptados de punta a punta.



Es importante aclarar que los Puntos de Introducción no son usados en la comunicación final para evitar que un sólo retransmisor sea completamente responsable del servicio oculto.

Problemas conocidos

Como todo software, Tor no está libre de problemas. Algunos ataques caen fuera de su modelo de amenaza, por lo que no protege bien contra ellos. Otros son iniciativas de censores para limitar el uso de Tor. Algunos son problemas inherentes de escalabilidad del diseño actual (aunque no afectarían al sistema en mucho tiempo, y ya se está trabajando para solucionarlos) o por el tipo de uso que se le está dando. Y los más frecuentes, son malas configuraciones o aplicaciones defectuosas en el lado del cliente.

Vulnerabilidad a diversos ataques

Tor es vulnerable si el atacante puede ver los dos extremos de la comunicación. Es posible que un observador que pueda analizar el tráfico de entrada de un usuario y observe algunos (a menos que sea un observador global) destinatarios que estime probables, correlacione el tiempo de entrada y de salida si acertó en el destinatario. De esta manera confirma una sospecha previa.

Bloqueo de las Autoridades de Directorio

En algunos países, se intenta disuadir el uso de Tor, mediante bloqueos a gran escala. Estos ataques son posibles porque las IP de los Retransmisores son conocidas, así como también las Autoridades de Directorio. Para evitar la imposibilidad de conectarse a la red sin acceso a las Autoridades, los desarrolladores de Tor crearon los Retransmisores de Puente, que simplemente son Retransmisores no listados en los Directorios. La manera de descubrir la dirección de un Retransmisor de Puente es visitar la página `https://bridges.torproject.org/` o enviar un mail a `bridges@torproject.org` con la línea “get bridges” en el cuerpo. Vale la pena aclarar que no es posible bloquear estos Retransmisores como los publicados, porque estos servicios sólo

devuelven un muy reducido número de Retransmisores, normalmente los más cercanos al cliente que los solicita.

Problemas de escalabilidad

Actualmente, Tor requiere que cada nodo Retransmisor esté conectado con todos los demás. Es evidente que este diseño no es escalable. Se está trabajando para que Tor soporte topologías restringidas, en las que cada nodo se conecta sólo a unos pocos.

Aumento de la relación clientes/retransmisores

Si bien la cantidad de usuarios aumenta permanentemente, la mayor parte de los usuarios elige no ser un Retransmisor. A medida que, comparativamente, más usuarios acceden a la red sólo para usar ancho de banda, y menos ofrecen su ancho de banda, el rendimiento de la red para todos decae. Actualmente se están investigando formas de incorporar incentivos no monetarios en Tor, para que aumente la cantidad de Retransmisores.

Mala configuración local

Se han comprobado ataques basados en abusos de funcionalidades del navegador (e.g. javascript) o plugins externos (e.g. Flash) en donde se ha violado el anonimato del cliente aún cuando usa Tor. Esto es porque los elementos activos insertados en una página web por un servidor malicioso (o comprometido) no son controlados por el usuario. Este tipo de ataques es la razón de ser de Torbutton.

Solicitudes DNS por fuera de Tor

Algunas aplicaciones, como Firefox, realizan conexiones DNS para averiguar la IP del destino y recién entonces se conectan a SOCKS (por lo tanto a Tor). Estas solicitudes, ajenas a Tor, muestran la verdadera identidad del cliente a los adversarios. Se puede usar un servidor DNS local que resuelva las solicitudes por la red Tor (como TorDNS), o, para HTTP, se puede configurar el navegador para que use un proxy que soporte SOCKS4a (usa hostnames en vez de IPs) o para que resuelva búsquedas de DNS remotamente.

Conclusiones

“Sí, la tierra señala a sus elegidos.
Y al llegar el final, tendrán su premio, nadie los nombrará.
Serán lo “anónimo”.
Pero ninguna tumba guardará su canto…“

Atahualpa Yupanqui, Destino del canto

A lo largo de este trabajo se ha visto cómo el anonimato en internet es un derecho pocas veces respetado en las políticas de los proveedores, de los gobiernos y de las corporaciones; es necesario imponerlo en la técnica. La mejor forma de hacer esto es lograr un sistema de anonimato que, además de tratar de proteger contra los ataques más preocupantes, haga un balance entre seguridad y usabilidad. Tor es uno de estos sistemas. No es perfecto, claro, pero es una base, un faro, con las características innatas necesarias para contrarrestar la invasión a la privacidad llevada adelante por los que tienen el poder, fortalecido por una comunidad de anónimos detrás suyo, que, ayudándose mutuamente, hablarán cada vez más fuerte y no podrán ser silenciados nunca más.

Apéndice: Ataques comunes

Ataque de análisis de tráfico

El análisis de tráfico consiste en observar el comportamiento y las características del tráfico, en vez del contenido del mismo. La encriptación no ayuda, ya que los métodos comunmente usados no tratan de ofuscar la cantidad de datos transmitidos, por lo que el atacante puede determinar, además de quiénes son el remitente y destinatario, cuál es el tamaño de los mensajes intercambiados.

Ataque de confirmación de tráfico

Es un ataque pasivo en el que el adversario confirma que los dos extremos de una comunicación (i.e. Alice y Bob) al observarlos y correlacionar las características (e.g. tamaño, frecuencia) del tráfico saliente de Alice con las del tráfico entrante de Bob.

Ataque de intersección

Este ataque es realizado a largo plazo, y consiste en la determinación, con una buena probabilidad, del comportamiento o perfil de los distintos usuarios y las relaciones entre ellos, mediante el estudio de los patrones de uso a lo largo del tiempo. Por ejemplo, el hecho de que no todo el mundo está mandando mensajes todo el tiempo es una fuga de información para un atacante dispuesto a esperar.

Ataque de predecesor

Este ataque permite descubrir quién es el cliente en base al proceso de creación de circuitos. El atacante contabiliza las veces en que cada nodo aparece en un circuito, con la consecuencia de que el nodo que más veces aparezca es probablemente un cliente de la red.

Ataque de maleabilidad

Cuando la integridad del flujo de datos no es confirmada debidamente, surge la posibilidad de este ataque. Consiste en que, aunque el atacante no puede descifrar las celdas, cualquier cambio a los datos encriptados crea cambios correspondientes en los datos que dejan la red. Esto permite, por ejemplo, que el atacante cambie la dirección de destino de una celda, o cambie un comando FTP de `dir` a `rm *`.

Ataque de Sybil

Este ataque, llamado así por el sujeto de estudio del libro Sybil (una mujer con desórden de personalidades múltiples), consiste en corromper un sistema distribuido o de reputación creando una gran cantidad de usuarios falsos, todos controlados por el mismo atacante, con el fin de corromper el sistema e influir en las decisiones tomadas en forma distribuida.

Apéndice: Configuración de servicios ocultos en Tor

Configuración paso a paso de un servicio oculto de ejemplo. Es prerequisito tener Tor funcionando. En este ejemplo vamos a proveer un servicio web con el servidor web thttpd, en **linux**. Se sugiere este servidor web por ser bastante localizado y pequeño, deja poca huella y es liviano. Además, es recomendable usar un servidor web dedicado para el servicio oculto, por razones de seguridad.

Pasos

1. Instalar e iniciar el servidor web
    1. Descargar la última versión (al momento de escribir esto es la 2.25b.)
    2. Descomprimir el archivo
       `tar -xzvf thttpd-2.25b.tar.gz`
    3. Ir al directorio creado (`thttpd-2.25b`) y compilar
       `./configure && make`
    4. Crear el **document-root** del servicio
       `mkdir` *servicio*`; cd` *servicio*
    5. En este directorio ponemos los archivos a servir
    6. Arrancar el servidor web escuchando un puerto cualquiera
       `../thttpd -p` *puerto* `-h localhost`
2. Configurar el servicio oculto
    1. Abrir el archivo `torrc y buscar la parte de los servicios ocultos`
    2. Agregar las siguientes líneas (siendo *usuario* el que ejecutará Tor y *puerto* el que se eligió anteriormente)
       `HiddenServiceDir /home/`*usuario*`/`*servicio*`/`
       `HiddenServicePort 80 127.0.0.1:`*puerto*`/code>`
    3. Guardar el archivo de configuración y reiniciar Tor

En este momento Tor crea, en el `HiddenServiceDir` elegido el par de claves pública/privada y el archivo `hostname`, que es donde se ubica la dirección `.onion` del servicio.

Es posible configurar muchos servicios ocultos en una misma máquina, y para cada servicio oculto es posible configurar varios puertos virtuales (como el puerto `80` en el ejemplo) donde Tor interceptará las llamadas y redigirá al puerto real configurado.

Apéndice: Nombres convencionales en criptografía

Es común en la literatura criptográfica usar nombres propios comunes para referirse a las partes involucradas, en lugar de identificadores más "académicos" como *persona A* o *participante B*. Estos nombres se eligen de tal manera que se corresponden con las letras del abecedario, o que den algún indicio de la función que cumplen en la comunicación.

Nombres usados en este documento:

- **Alice:** normalmente, Alice es la persona o el participante que inicia la comunicación.
- **Bob:** es quien recibe los mensajes de Alice, o quien provee el servicio a donde Alice se conecta.

Apéndice: Bibliografía

Bibliografía técnica

- Biblioteca de Free Haven
- Onion Routing

Proyectos de software

- Tor
- Mixminion
- I2P

Activismo por la libertad de expresión

- Electronic Frontier Foundation
- Irrepressible Info
- Chilling Effects

Otros

- Declaración universal de los derechos humanos
- Schenier on Security
- Wikipedia
- Búsqueda de Creative Commons

Apéndice: GNU Free Documentation License

Version 1.3, 3 November 2008

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The “Invariant Sections” are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The “Cover Texts” are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A “Transparent” copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not “Transparent” is called “Opaque”.

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The “Title Page” means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, “Title Page” means the text near the most prominent appearance of the work’s title, preceding the beginning of the body of the text.

The “publisher” means any person or entity that distributes copies of the Document to the public.

A section “Entitled XYZ” means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as “Acknowledgements”, “Dedications”, “Endorsements”, or “History”.) To “Preserve the Title” of such a section when you modify the Document means that it remains a section “Entitled XYZ” according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or

control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

1. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
2. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.
3. State on the Title page the name of the publisher of the Modified Version, as the publisher.

4. Preserve all the copyright notices of the Document.
5. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
6. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.
7. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.
8. Include an unaltered copy of this License.
9. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.
10. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.
11. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.
12. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.
13. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.
14. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.
15. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties—for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled “History” in the various original documents, forming one section Entitled “History”; likewise combine any sections Entitled “Acknowledgements”, and any sections Entitled “Dedications”. You must delete all sections Entitled “Endorsements”.

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an “aggregate” if the copyright resulting from the compilation is not used to limit the legal rights of the compilation’s users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document’s Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special

permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled “Acknowledgements”, “Dedications”, or “History”, the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, or distribute it is void, and will automatically terminate your rights under this License.

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, receipt of a copy of some or all of the same material does not give you any rights to use it.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License “or any later version” applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation. If the Document specifies that a proxy can decide which future versions of this License can be used, that proxy’s public statement of acceptance of a version permanently authorizes you to choose that version for the Document.

11. RELICENSING

“Massive Multiauthor Collaboration Site” (or “MMC Site”) means any World Wide Web server that

publishes copyrightable works and also provides prominent facilities for anybody to edit those works. A public wiki that anybody can edit is an example of such a server. A “Massive Multiauthor Collaboration” (or “MMC”) contained in the site means any set of copyrightable works thus published on the MMC site.

“CC-BY-SA” means the Creative Commons Attribution-Share Alike 3.0 license published by Creative Commons Corporation, a not-for-profit corporation with a principal place of business in San Francisco, California, as well as future copyleft versions of that license published by that same organization.

“Incorporate” means to publish or republish a Document, in whole or in part, as part of another Document.

An MMC is “eligible for relicensing” if it is licensed under this License, and if all works that were first published under this License somewhere other than this MMC, and subsequently incorporated in whole or in part into the MMC, (1) had no cover texts or invariant sections, and (2) were thus incorporated prior to November 1, 2008.

The operator of an MMC Site may republish an MMC contained in the site under CC-BY-SA on the same site at any time before August 1, 2009, provided the MMC is eligible for relicensing.

ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

```
Copyright (C) YEAR YOUR NAME. Permission is granted to copy,
distribute and/or modify this document under the terms of the GNU
Free Documentation License, Version 1.3 or any later version
published by the Free Software Foundation; with no Invariant
Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of
the license is included in the section entitled "GNU Free
Documentation License".
```

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the “with … Texts.” line with this:

```
with the Invariant Sections being LIST THEIR TITLES, with the
Front-Cover Texts being LIST, and with the Back-Cover Texts being
LIST.
```

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.