Herramientas de privacidad en la red

Gunnar Wolf

Instituto de Investigaciones Económicas UNAM
Desarrollador del proyecto Debian

OS UPIITA, 17 de agosto, 2012

Índice

Más de lo que cabe en una presentación

A lo largo de esta presentación mencionaré varias herramientas, incluyendo desde dónde descargarlas.

Más información respecto a ellas, incluyendo tutoriales y explicaciones detalladas:

http://www.cuidatuinfo.org/

(Repito esta liga al final de la presentación)

Trabajo específico a un ámbito

- Esta presentación va orientada al uso de programas y tecnologías para proteger un poco nuestra información personal en el uso cotidiano de la red
  - Enfocado al uso que hacemos desde una computadora *tradicional*
- *No* vamos a abordar áreas muy amplias, como:

  Redes sociales Un medio, no una tecnología. Y un medio en el que estamos sujetos a lo que *cada empresa* indique.

  Telefonía celular La rastreabilidad es inherente al dispositivo. Son plataformas suficientemente complejas para merecer una presentación completa para sí.

¿Por qué nos preocupa la privacidad en la red?

Porque no existe

Porque *por diseño* no está ahí

Nota: Donde digo *privacidad* digo en general *seguridad de la información*

¿A qué me refiero con *herramientas de privacidad*?

A programas (y a formas de trabajo) orientadas a que:

- La comunicación provenga del remitente aparente
- Los datos (en tránsito o almacenados) no hayan sido alterados
- Los datos no se divulguen más allá de los destinatarios
- Terceros no se enteren de la naturaleza de mis comunicaciones
- Evitar que mi equipo corra programas no deseados
- Evitar dejar huella rastreable de mi actividad
- Ayudarme a mantener mecanismos seguros de *autenticación*

. . . Y aterrizando en el mundo real

Muchos de nosotros *queremos* o *preferimos* poder confiar en nuestras comunicaciones.
Algunos lo **requieren**.

El verdadero público que espero que pueda beneficiarse de esto:

- Organizaciones de derechos humanos
- Periodistas
- Migrantes

Gente para la cual la privacidad y la seguridad de la información no es meramente una postura ideológica

Índice

¿De qué me estoy cuidando?

Cuando protejo mis datos, los protejo *de alguna amenaza*. ¿En quién estoy *dispuesto a confiar*?

- Otros usuarios de la misma computadora
- Usuarios de la misma red en la que trabajo
- Que me construyan un perfil mercadológico
- Atacantes externos
  - ¿Cuál es la naturaleza del ataque? ¿Por qué les puede importar mi información? ¿Cuál es el nivel de riesgo que corro?
- Un gobierno nacional

Una vez definiendo los niveles adecuados...

El software libre y la confianza

- Si quieres confiar en tu computadora, ¡usa sólo software libre!
- Aunque tú no programes, hay gente que ha auditado los principales componentes del sistema *sin intereses ocultos*
- Muchos integrantes de la comunidad desarrolladora son fuertes activistas de la privacidad de la información

Confiar en la confianza misma

La confianza absoluta no existe. Ni con software libre.

- El que tengas acceso al código fuente no significa que estés ejecutando *ese* código fuente
- El que tú hayas compilado (incluso escrito) un programa no garantiza *que el compilador* no esté trucado (Ken Thompson, 1984)
- Sin embargo, tienes *mucha mayor probabilidad* de que así sea.

¿Es suficiente para tí?

Confiar en la confianza misma

La confianza absoluta no existe. Ni con software libre.

- El que tengas acceso al código fuente no significa que estés ejecutando *ese* código fuente
- El que tú hayas compilado (incluso escrito) un programa no garantiza *que el compilador* no esté trucado (Ken Thompson, 1984)
- Sin embargo, tienes *mucha mayor probabilidad* de que así sea.

¿Es suficiente para tí?

Índice

El esquema usuario/contraseña

¿Has analizado al esquema usuario/contraseña?

- ¿Quién usa contraseñas de forma segura?
  - Una diferente para cada sitio
  - Cambiándolas frecuentemente
  - Nunca escribirlas
- ¿Quién usa contraseñas seguras?
  - Buena longitud (más de 10-15 caracteres)
  - No pronunciables
  - No sólo alfanuméricas

Si sí. . . No eres humano.

El esquema usuario/contraseña

¿Has analizado al esquema usuario/contraseña?

- ¿Quién usa contraseñas de forma segura?
  - Una diferente para cada sitio
  - Cambiándolas frecuentemente
  - Nunca escribirlas
- ¿Quién usa contraseñas seguras?
  - Buena longitud (más de 10-15 caracteres)
  - No pronunciables
  - No sólo alfanuméricas

Si sí... No eres humano.

Que la computadora haga lo que sabe hacer

KeePassX

http://www.keepassx.org

- Base de datos de contraseñas
- Con generador con diferentes características de aleatoreidad
- La base misma puede (**debe**) guardarse cifrada por una contraseña maestra
  - O mejor aún, un *archivo llave*

Viviendo con KeePassX

KeePassX

http://www.keepassx.org

- Centraliza el manejo de las contraseñas ✔
- Facilita mantener una contraseña por sitio ✔
- Fácil de usar para usuarios no-técnicos ✔
- Base de datos cifrada con AES o Twofish ✔
- ¡Hay que considerar el riesgo de que un archivo único resulte comprometido! ✗
- Sin embargo... **¡Mucho** mejor que pedir al navegador que recuerde contraseñas!

Índice

¡Mi correo! ¡Mi mensajería!

- Lo primero en lo que pensamos al hablar de este tema es en cifrar nuestra comunicación interpersonal directa: El correo
  - Pero la comunicación asíncrona ha crecido a otras tecnologías también: Hablemos de la mensajería instantánea.
  - Además, ¿qué hay de *todos nuestros documentos*? ¿Qué acaso no son información personal?
- Hoy en día hay cifrado seguro al alcance de todos ✔
  - . . . Pero requerimos que *todos los involucrados* estén de acuerdo en usarlo, lo conozcan, y usen tecnología compatible ✗
  - Y la mayor parte de las implementaciones son muy poco amigables a usuarios no-expertos

La otra cara de la moneda: *Firmar* nuestras palabras

¿Firmar? ¿Por qué lo menciono aquí? ¿No hablábamos justo de lo *contrario*, de *ocultar* mi información?

- La *criptografía de llave pública* nos permite ambas cosas
- Resulta tanto o más importante que nadie vea una conversación privada en tránsito como tener la certeza de que hablamos con quien creemos hablar
  - O que un documento estático viene de quien dice venir

Algunas características de PGP/GnuPG

`http://www.gnupg.org`

- Funciona en base a criptografía de llave pública, en base a identidades, *no a un secreto compartido*
- Maneja un *llavero* de *identidades conocidas*
  - *Servidores de llaves* funcionan como directorio global ✔
  - Permite confiar en la identidad de alguien *sin siquiera conocerlo* si se confía en quien lo certifica ✔
- Se cifra un documento *para un conjunto de identidades*
  - No se usa *contraseña por documento* ✔
- Se *firma* un documento para certificar su origen ✔
- . . . Pero es **muy poco** amigable al usuario novato ✗

Poniéndole cara humana

Thunderbird+Enigmail

`http://www.enigmail.net`

- *Enigmail* es una extensión para el cliente de correo *Thunderbird* de Mozilla
- Brinda acceso simple a toda la funcionalidad de GnuPG ✔
- Requiere aún algo de tutoría para comprender los conceptos, pero el manejo se vuelve natural, bien integrado, y al alcance de todos ✔

¿Y la mensajería instantánea?

- Parte importante de nuestras comunicaciones hoy en día son mensajería instantánea
  - Manejamos datos *más sensibles* que por e-mail
- Típicamente viaja *en claro* (sin cifrado)
  - Es muy fácil espiar (o meterse en) conversaciones de gente en nuestra propia red
- En algunos casos, la empresa proveedora *guarda copia de todas las conversaciones*
  - Para perfiles mercadológicos
  - Para cumplir con requisitos legales de *monitoreo de la información* $\rightarrow$ ¿Reportar nuestra actividad a algún gobierno?
  - Muchos programas mensajeros incluyen anuncios dentro de su operación

Pidgin

Pidgin

http://pidgin.im

- Cliente multiprotocolo de mensajería instantánea
  - AIM, Gadu Gadu, IRC, ICQ, Jabber (GMail, Facebook, muchos otros), MSN, MxKit, MySpace, Napster, Sametime, Yahoo, Zephyr
- Integra todas las cuentas en una sóla interfaz ✔
- No presenta mensajes ✔
  - Aunque los protocolos que exigen pasar por su servidor pueden seguir creando nuestros perfiles o buscando patrones ✗

Off The Record (OTR)

Pidgin + OTR

`http://www.cypherpunks.ca/otr/index.php`

- Plugin para programas de mensajería en general para implementar cifrado *acorde al medio*
  - Cifrado ✔
  - Autenticación ✔
  - *Negabilidad* ✔
  - Secrecía a futuro perfecta ✔
- A prueba incluso de los sistemas que exigen pasar por un servidor central ✔

Off The Record (OTR)

Off The Record

http://www.cypherpunks.ca/otr/index.php

- Implementado por Pidgin, ampliamente utilizado
- Disponible para otros gestores de mensajería
  - Adium (MacOS)
  - Gibberbot (Android)
  - Kopete (KDE)
  - Jitsi (OTR para conexiones con audio/video)
  - Otros — http://www.cypherpunks.ca/otr/software.php

Índice

Caminito de migajas

Siempre que uso un navegador voy dejando pistas, y todo lo que hago permite analizar y profundizar mi perfil

- Sitios que incluyen scripts externos para *medición* — p.ej. *google-analytics.com*
  - Google ofrece análisis gratuito del tráfico de mi sitio, pero... ¿Es verdaderamente gratuito? ✗
- Es cómodo no tener que repetir nuestros datos de registro una y otra vez al usar sitios frecuentes, p.ej. *Facebook*
  - Muchísimos sitios Web incluyen llamadas a dichos sitios para incluir desde simples iconitos hasta aplicaciones completas ✗

Todo navegador moderno incluye un motor de ejecución externa irrestricta de Javascript. *¿Qué no podría hacer?*

Limitando la ejecución de scripts

NoScript

`http://noscript.net/`

- Extensión para los navegadores Mozilla (Firefox, Seamonkey, etc.) que limita la ejecución de código remoto ✔
  - Java, Javascript, Flash, Silverlight, etc.
- Por medio de *lista negra* y *lista blanca* se configura para adecuarse a nuestro patrón de uso frecuente ✔
  - . . . Aunque requiere de un periodo de entrenamiento, y el usuario siempre se ve tentado a *permitir todo* ✗
  - ¡Requiere *mantenerse consciente*!

Protección adicional de NoScript

NoScript

http://noscript.net/

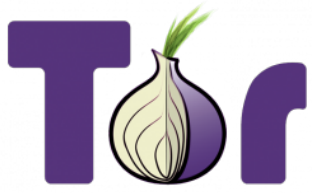
- Interfaz usuario sencilla, mostrando el estado general de la página de forma icónica () Presenta claramente el estado de la página ✔
- Algunas protecciones adicionales importantes: *Clickjacking*, *Cross-site scripting* ✔
  - Conceptos difíciles de explicar a usuarios novatos
  - . . . Pero por lo mismo, frecuentemente aparece como una molestia más que como una ayuda ✗

Índice

Ocultando el contenido, gritando la naturaleza

- Siempre hay datos que se *cuelan* cuando establezco una conexión de red, aunque ésta sea cifrada
- Al conectar una computadora con un servidor, hay *muy grandes probabilidades* de que si alguien está monitoreando pueda averiguar la naturaleza base de la comunicación
  - Aunque se oculte el contenido, no se oculta la intención
- Puede realizarse bloqueo o degradación de servicio selectivo basado en la dirección destino
  - Suena a censura (ver el Gran Firewall de China)
  - Neutralidad de la red

Tor: The Onion Router

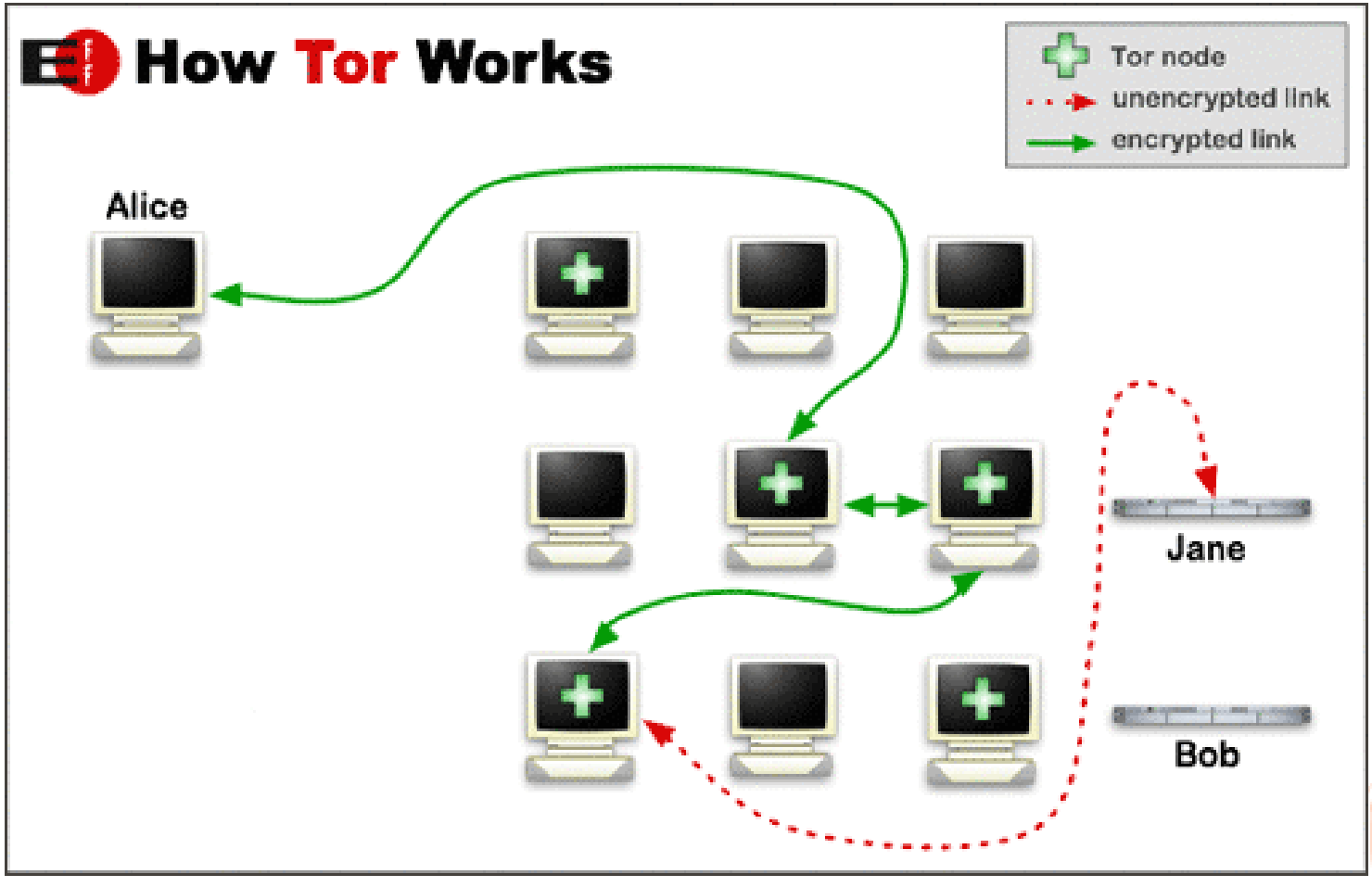


The Onion Router

`http://www.torproject.org/`

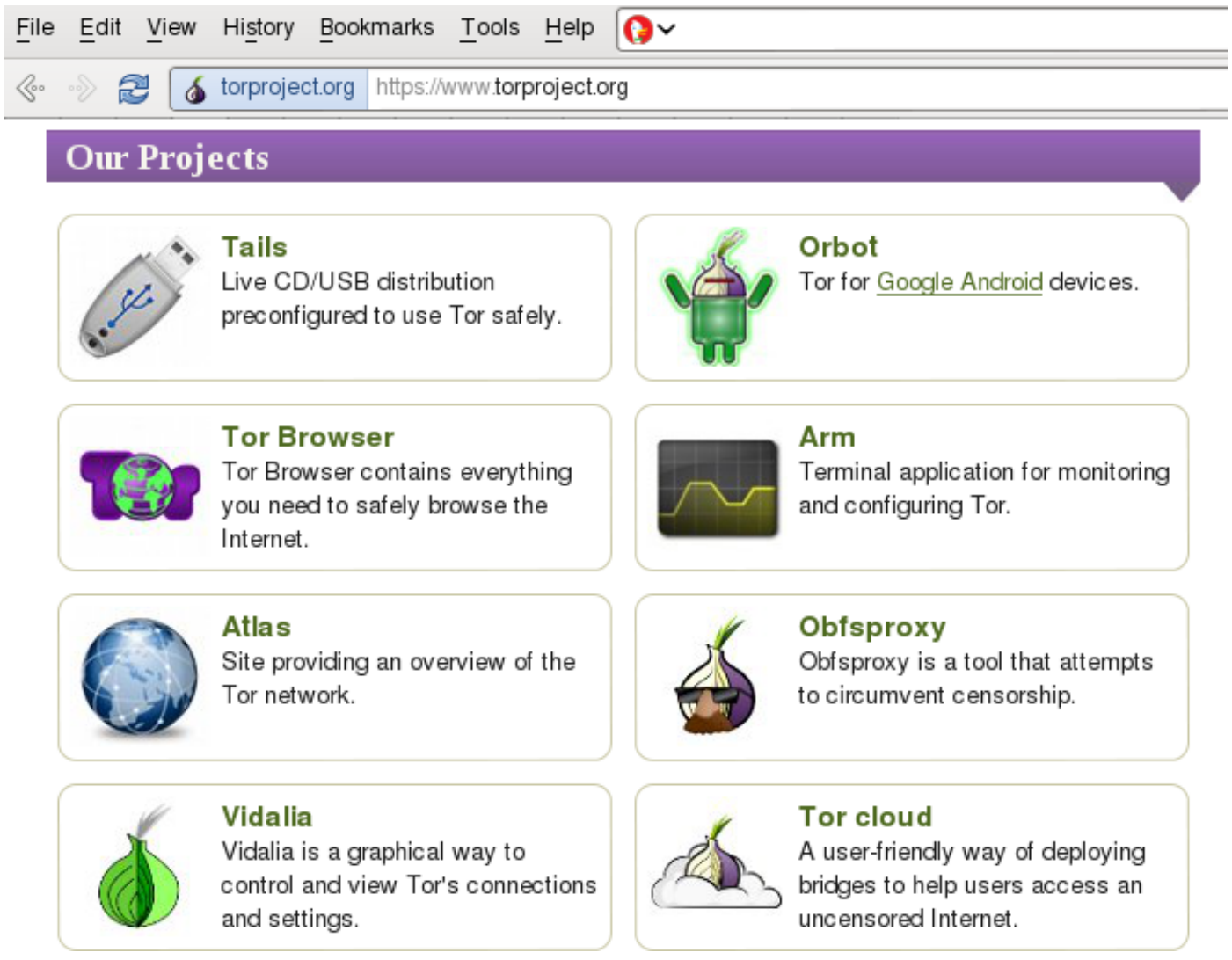
- Tor implementa una infraestructura de red destinada a imposibilitar el rastreo de *conexiones individuales*, cifrando los encabezados y aleatorizando sus rutas
- Cada *salto* de la conexión sólo conoce al antecesor y sucesor inmediatos
- La ruta que sigue una conexión se recalcula/aleatoriza periódicamente
- Esto imposibilita tanto el rastreo de las conexiones como el bloqueo efectivo basado en origen/destino

El *ruteo cebolla* en acción



https://www.torproject.org/about/overview.html.en

La versatilidad de Tor



Mantener la paranoia

- Tor no ofrece un *anonimato absoluto*, aunque sí una *anonimización*
- No hay cifrado *extremo a extremo* — El último salto irá *en claro*
- Algunos ataques/análisis son aún posibles
  - Se enfoca en proteger el *transporte de* los datos
  - No protege p.ej. contra ataques de cronometraje extremo a extremo
- Hay información delatora en todo navegador
  - Galletas, JavaScript, ¡hasta las entradas que da el usuario mismo!
- Usar Tor no te exime de ser inteligente y paranóico

Índice

Por más que cuide mis comunicaciones. . .

- ¿Qué pasa si alguien tiene *acceso físico* a mi equipo?
  - Robo de equipo ✗
  - Revisión en la aduana ✗
  - *Uso casual* en la oficina ✗
- Varias aplicaciones ofrecen cifrado de sus datos
  - Típicamente con algoritmos vulnerables ✗
- Puedo cifrar mis archivos uno a uno (p.ej. con GnuPG)
  - Pero típicamente los tendré que descifrar para trabajar con ellos, y la copia *en claro* queda en algún lugar del disco ✗
  - Requerir un proceso manual. . . es la mejor manera de olvidarlo ✗

Cifrando discos o particiones: LUKS

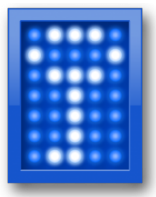
LUKS
Linux Unified Key Setup

LUKS+cryptsetup

`https://code.google.com/p/cryptsetup/`

- Cifrado genérico de *dispositivos de bloques* nativo a Linux
  - Aplicable transparentemente: A disco entero, a partición de datos, a partición swap, a un archivo-imagen ✔
- Soporte para múltiples llaves, revocaciones, etc. ✔
- Soportado desde sistemas Windows (con FreeOTFE) ✔
- . . . Pero muy complicado de comprender, configurar, manejar correctamente para usuarios finales ✗

Cifrando discos o particiones: Truecrypt



Truecrypt

`https://www.truecrypt.org/`

- Juego de características casi tan completo como LUKS ⇝
- Multiplataforma (principalmente orientado a Windows, pero plenamente operativo en Linux y MacOS) ✔
- Configurable/administrable a través de una intefaz gráfica (GUI) ✔

Índice

Hay más, mucho más

- En esta presentación muestro algunas herramientas base, sólo a modo de ejemplo
- Cada uno de nosotros debe analizar su situación de vida, sus factores de riesgo aceptable, y entonces puede decidir qué aspectos de seguridad informática fortalecer
- . . . Pero hoy en día prácticamente nadie puede escaparse *por completo* de estar sobre-exponiendo su vida en línea
- Lo más importante de todo: Estar conscientes y atentos.

Agradecimiento

Un gran agradecimiento a los compañeros de *Fundación Acceso*, y muy en particular al proyecto *Cuida tu info*, por la motivación, información y confianza.

¿Dudas?

¡Gracias por su atención!

Gunnar Wolf — gwolf@gwolf.org
Instituto de Investigaciones Económicas UNAM
Desarrollador del Proyecto Debian

http://www.cuidatuinfo.org
http://gwolf.org/seguridad/herramientas