
Tails
theamnesicincognitolivesystem

A Cypherpunk's Manifesto

by Eric Hughes

Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world.

If two parties have some sort of dealings, then each has a memory of their interaction. Each party can speak about their own memory of this; how could anyone prevent it? One could pass laws against it, but the freedom of speech, even more than privacy, is fundamental to an open society; we seek not to restrict any speech at all. If many parties speak together in the same forum, each can speak to all the others and aggregate together knowledge about individuals and other parties. The power of electronic communications has enabled such group speech, and it will not go away merely because we might want it to.

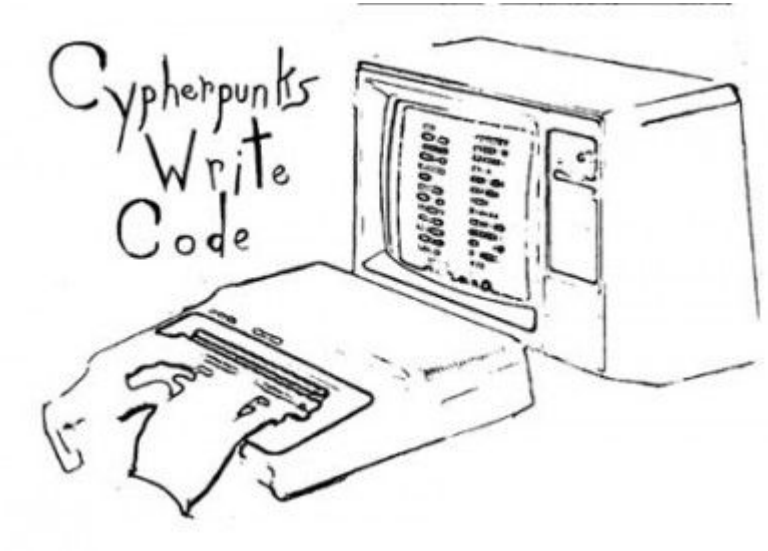
Since we desire privacy, we must ensure that each party to a transaction have knowledge only of that which is directly necessary for that transaction. Since any information can be spoken of, we must ensure that we reveal as little as possible. In most cases personal identity is not salient. When I purchase a magazine at a store and hand cash to the clerk, there is no need to know who I am. When I ask my electronic mail provider to send and receive messages, my

Puntos a tomar en cuenta del Manifesto:

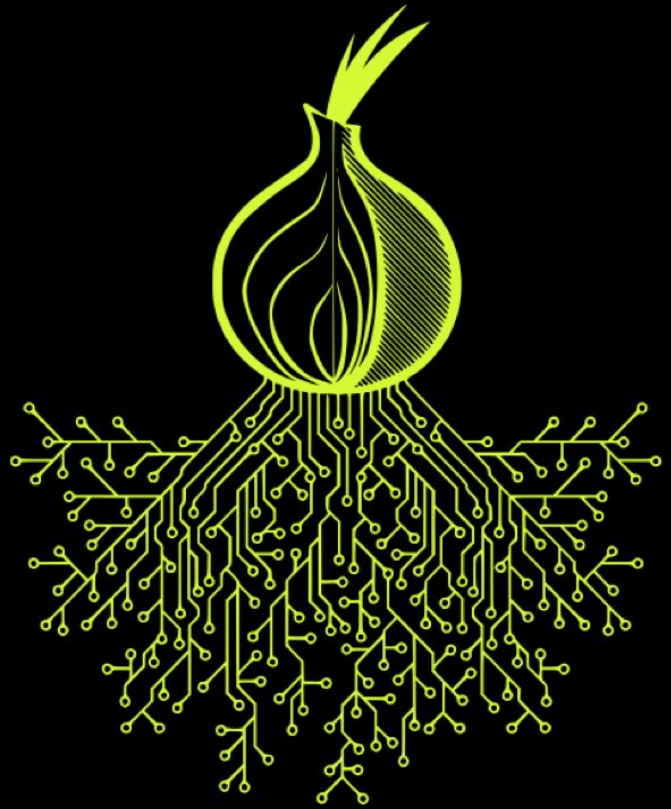
“La privacidad es necesaria para una sociedad abierta en la era electrónica. La privacidad no es secretismo. Una cuestión privada es algo que no queremos que todo el mundo sepa, pero una cuestión secreta es algo que no queremos que nadie sepa. La privacidad es la capacidad de revelarse selectivamente al mundo.”

“Un sistema anónimo ofrece la capacidad a los individuos para revelar su identidad sólo cuando lo deseen; esta es la esencia de la privacidad. Asimismo la privacidad en una sociedad abierta requiere de criptografía.”

-- Eric Hughes, A Cypherpunk Manifesto (1993)



¿Qué es Tails?



- The Amnesic Incognito Live System (in short: Tails).
- Privacy Enhancing Live Distribution (PELD).
- Basado en Debian y Open Source.

Tails aspira a preservar tu **privacidad** y **anonimato** y te ayuda a:

- **usar Internet anónimamente** y **burlar la censura**; todas las conexiones a Internet son forzadas a ir a través de la red de Tor.
- **no deja traza** en el ordenador que estás usando a menos que lo pidas explícitamente.
- **usa las más modernas herramientas de cifrado** para cifrar tus archivos, e-mails y mensajería instantánea.

Características principales:

- **Bloqueo de conexiones automáticas por aplicaciones**. Si una aplicación intenta conectarse de forma automática, esa conexión será bloqueada por seguridad.
- **Incorpora herramientas criptográficas,** como por ejemplo cifrado de dispositivos USB con **LUKS** (el estándar de Linux para llevar a cabo dicha tarea) o de correos y documentos utilizando **OpenPGP.**
- **Es capaz de correr en una Máquina Virtual.**

- **Utiliza únicamente la memoria RAM de la computadora anfitriona**. De esta forma, hace imposible que mediante un análisis forense del disco rígido de la computadora se pueda llegar a los datos manipulados. De aquí la palabra **amnesia**.
- **Soporta Cold boot attack.**
- **Permite eliminar archivos de forma segura**. Utilizando Nautilus Wipe, verifica que los datos eliminados sean quitados de memoria.
- **Prioriza la comunicación HTTPS**. Para lograrlo utiliza HTTPS Everywhere, un plugin para el navegador **Firefox**.

Cold boot attack:

Un **ataque de arranque en frío** consiste en que un atacante con acceso físico a una computadora realiza un volcado de memoria de la memoria de acceso aleatorio de una computadora al realizar un restablecimiento completo de la máquina de destino. Por lo general, los ataques de arranque en frío se utilizan para recuperar claves de cifrado de un sistema operativo en ejecución por motivos de investigación maliciosos o criminales. El ataque se basa en la propiedad de remanencia de datos de DRAM y SRAM para recuperar contenidos de memoria que permanecen legibles en los segundos a minutos posteriores a la desconexión de la alimentación.

Máquina Virtual

Una máquina virtual es un software instalado al interior de un sistema operativo que simula en todo y para todo el funcionamiento de una computadora permitiendo la instalación de un segundo sistema operativo perfectamente funcionando.

¿Cómo funciona una maquina virtual?

Un programa de máquina virtual es un programa informático que crea un sistema de ordenador virtual, con dispositivos de hardware virtual. Este equipo “**máquina virtual**” se ejecuta como un proceso en una ventana de su sistema operativo actual. Puede arrancar un disco de instalación de sistema operativo (o CD en vivo) dentro de la máquina virtual y el sistema operativo será “engañado” creyendo que se está ejecutando en un ordenador real.

El sistema operativo de la máquina virtual se almacena en un **disco duro virtual**, generalmente un archivo grande, de varios gigabytes, almacenado en su disco duro. Ese archivo es para el sistema operativo como un disco duro real. Esto significa que no tendremos que perder tiempo con la partición.

Las máquinas virtuales añaden algo de sobrecarga, por lo que no será tan rápido como si se hubiera instalado el sistema operativo en hardware real.

Usos de las máquinas virtuales.

Las máquinas virtuales **nos permiten experimentar** con otro sistema operativo sin salir de su sistema operativo actual.

Las máquinas virtuales también están aisladas del resto de su sistema, lo que significa que el software en una máquina virtual no puede escapar de la máquina virtual y alterar el resto de su sistema

Por ejemplo si queremos verificar que un programa o una serie de archivos contienen uno o más virus, se pueden probar directamente en la máquina virtual sin que nuestra computadora tenga un problema mínimamente.

Programas para hacer máquinas virtuales

VirtualBox (Windows/Linux/Mac, gratis)

Parallels (Mac)

Vmware VMware (Windows/Linux/Mac)

QEMU (Linux)

Windows Virtual PC (Windows)

¿De que se compone?

Generalmente, las máquina y recursos virtuales y hardware que administra de la misma forma que administraría un equipo físicos virtuales tienen un sistema operativo

Debe tener un CD/DVD-ROM o imagen ISO que contenga los archivos de instalación de un proveedor de sistemas operativos.

Bibliografía:

•https://es.gizmodo.com/los-cinco-mejores-programas-para-crear-maquinas-virtual-1789667830

•https://azure.microsoft.com/it-it/overview/what-is-a-virtual-machine/

•https://www.fastweb.it/web-e-digital/macchine-virtuali-cosa-sono-e-come-funzionano/

•https://www.eldiario.es/cv/amigoinformatico/Maquinas-virtuales_6_685641440.html

•https://tails.boum.org/contribute/design/

- https://www.activism.net/cypherpunk/manifesto.html