Análisis de Subgraph OS: un Sistema Operativo para Privacidad y Anonimato

Rafael Bonifaz

20 de noviembre de 2016

Universidad de Buenos Aires.
Posgrado de Seguridad Informática.
Sistemas Operativos

Contenido

Índice de ilustraciones

Sobre este documento

Escribí este documento para la clase de Seguridad en Sistemas Operativos que tomé como parte de la maestría de Seguridad Informática Seguridad Informática en la Universidad de Buenos Aires. Subgraph OS es una distribución GNU Linux pensada en dar privacidad y anonimato a las personas. Más allá de la distribución, gran parte de las herramientas que vienen en la misma pueden ser utilizadas en cualquier sistema GNU/ Linux y en algunos casos en otros sistemas operativos.

Considero que el conocimiento debe ser accesible para la mayor cantidad de personas, por lo que he decidido publicar en mi blog este documento. Este documento lo publico con licencia Creative Commons Compartir Igual.

1 Introducción

Internet ha cambiado la forma en que vive la sociedad moderna a tal punto que hoy en día es difícil imaginar un mundo sin estar conectados. Si bien este cambio tiene aspectos positivos, en los últimos años se empezó a publicar una serie de documentos secretos que revelan espionaje informático y vigilancia masiva hacia las personas que usan la red. De entre estas revelaciones destacan las realizadas por Edward Snowden gracias a las cuales se conoce el espionaje informático de alcance mundial realizado por la Agencia de Seguridad Nacional de Estados Unidos (*NSA*).

La criptografía y el software libre son herramientas que permiten a las personas proteger su privacidad en Internet. En video conferencia realizada para el evento Campus Party 2014 en Quito Jullian Assange dijo "*No hay elección, tenemos que pasarnos al software libre para nuestra mejor protección*"(Julian Assange: "No Hay Elección, Tenemos Que Pasarnos Al Software Libre Para Nuestra Mejor Protección" 2014).

Según Edward Snowden:

> La criptografía funciona. Sistema de criptografía fuertes bien implementados son una de las pocas cosas en las que se puede confiar. Lamentablemente, la seguridad en los equipos terminales de los usuarios es extremadamente débil por lo la NSA frecuentemente encuentra formas de evadirla(Edward Snowden: NSA Whistleblower Answers Reader Questions 2013).[1]

Subgraph OS es un sistema operativo de software libre basado en Debian. Esta pensado en proteger la seguridad del terminal del usuariopara de esta forma proteger sus comunicaciones. Por un lado provee herramientas para proteger la comunicación en la red como Tor, correo cifrado y chat cifrado. Por otro lado provee características para proteger la seguridad física de la terminal como cifrado de disco duro, parches al kernel para bloquear el acceso a USBs. Por último da nivel de seguridad a nivel de aplicación mediante el aislamiento de aplicaciones.

El presento trabajo se lo ha realizado con pruebas de laboratorio utilizando Subgraph OS en una máquina virtual Virtualbox. Además se ha realizado una investigación de las principales herramientas con las que trabaja y se realizó una entrevista a David Mirza que es uno de los desolladores del software.

La seguridad de los terminales de trabajo no es algo sencillo y requiere cierto nivel de complejidad que hace complicado el reto de llegar a ser utilizado por usuarios no técnicos. Incluso para personas con perfil técnico no es tan fácil entender toda la tecnología que esta detrás de una herramienta como Subgraph OS. En este trabajo se verán las principales características.

2 Motivación

Según las revelaciones hechas por Snowden(Global Surveillance Disclosures (2013–present) 2016), Internet es una gran herramienta de vigilancia masiva controlada por pocos gobiernos y algunas de las principales corporaciones de Internet como Apple, Google, Facbook, Microsoft, entre otros que participan en programas de espionaje como PRISM(U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program - The Washington Post 2013). Al utilizar un

1 Texto original: "Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on. Unfortunately, endpoint security is so terrifically weak that NSA can frequently find ways around it. "

servicio en línea para compartir información con otro individuo,, también se lo hace con el proveedor del servicio. Esto pone en riesgo la privacidad de las personas y la confidencialidad de la información de las organizaciones.

El contenido de las comunicaciones en Internet, no es lo único que puede ser accedida por empresas de terceros. Además, se debe prestar atención a los metadatos cuando se quiere proteger la privacidad en Internet. Estos son datos que describen a otros datos. En el caso de las comunicaciones por Internet, estos pueden ser la frecuencia con la que una persona se comunica con otra, si la comunicación es cifrada o no, la fecha, dirección IP, etcétera.

Una forma fácil de entender la implicaciones de los metadatos en la privacidad de las persona es verlo en una imagen. El proyecto Immersion[2] de la Instituto de Tecnología de Massachussets permite analizar los metadatos de cuentas de correo de servicios como Gmail, Yahoo o MS Exchange. Para este análisis toma en cuenta las cabeceras de un correo electrónico: “de”, “para”, “copia” y las marcas de tiempo. No considera el asunto del correo ni el contenido del mismo. Es decir solo con metadatos puede generar la red de contactos de una persona en un gráfico fácil de visualizar como se puede ver en la ilustración 1.

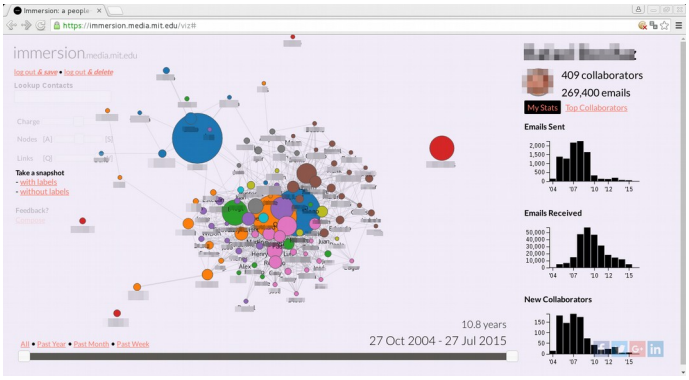

Ilustración 1: Imagen generada con Immersion: https://immersion.media.mit.edu/

Los círculos más grandes son las personas con las que más se comunica el individuo de esta gráfica. Sin leer el contenido, ni el asunto del mensaje el proveedor de un servicio podría conocer la red de contactos de sus usuarios.

Para evitar compartir metadatos con terceros existen varias opciones. Una de ellas es utilizar servicios propios en lugar de servicios centralizados. En el caso de una organización, por ejemplo, si el servidor de correo es gestionada por si misma entonces no compartirá metadatos con terceros al no ser que se comunique con ellos (ejemplo, un correo externo). En el caso de individuos que no tienen servidor propio, pueden utilizar servicios de anonimato como Tor para crear pseudónimos y de esta manera ocultar los metadatos.

Ilustración 2: Países clientes de Hackingteam según las filtraciones de 2015. Fuente: https://hipertextual.com/2015/07/los-paises-iberoamericanos-que-usaron-a-hacking-team-para-espiar

Las grandes corporaciones de Internet y la NSA no son los únicos que espían a los usuarios de Internet. Existen técnicas de ataques podrían ser utilizados por criminales o

2 https://immersion.media.mit.edu/

incluso por gobiernos. A mediados de 2016 la empresa Hackingteam fue infiltrada y su información fue publicada en Internet. Gracias a esta filtración se pudo saber que esta empresa trabajó con gobiernos de hispanoamericana para espiar a sus ciudadanos(Los Países Iberoamericanos Que Usaron a Hacking Team 2015).

Si bien con las filtraciones de Snowden se generó conciencia a nivel global sobre los peligros de la vigilancia masiva. Ya existían proyectos de software libre pensados en la privacidad y el anonimato. La distribución GNU/Linux Tails[3] esta pensado en esto. Esta distribución funciona desde una memora USB o un Live DVD que enruta todo su tráfico a través de Tor.

Luego de las publicaciones de Snowden se empezaron a crear otras distribuciones orientadas a proteger a sus usuarios de posibles ataques a su terminal de trabajo. Una de ellas es Qube OS[4] y la otra es Subgraph OS[5].

El presente trabajo se concentra en analizar Subgraph OS. Para esto se ha realizado una investigación sobre las principales funcionalidades de esta distribución que incluye una entrevista a David Mirza que es uno de sus desarrolladores, misma que se puede leer íntegramente en el Anexo 1. Según Mirza la motivación para crear Subgraph OS es la de crear un sistema operativo FLOSS que se enfoque en la seguridad del *endpoint* (Mirza, David 2016).

3 Descripción general de Subgraph OS

Según su página web, Subgraph OS es un plataforma de computación resistente a los adversarios(Subgraph OS n.d.). Según Mirza una plataforma de computación resistente a adversarios tiene su principal foco en:

> "*...proteger contra ataques en los que un exploit es enviado al objetivo a través de Internet. Por ejemplo, a través de adjuntos a correos electrónicos o a través de una página web. Entonces vulnerabilidades en un navegador, vulnerabilidades de un visor de PDFs, vulnerabilidad en correo electrónico, etcétera. Vulnerabilidades en las aplicaciones que el usuario utiliza en su terminal.*(Mirza, David 2016)[6]"

SubgraphOS es una distribución GNU/Linux basada en Debian que puede funcionar en modo live o se puede instalar en el disco duro. Incluye algunas características como:

- Navegador de Internet Tor
- Correo electrónico funciona a través de Tor con soporte de PGP
- Chat cifrado fin a fin con el protocolo OTR y Ricochet
- PDF en modo fuera de línea para evitar ataques a través de PDFs con código malicioso
- Disco duro cifrado como única opción al instalar
- Aplicaciones funcionan en "Sandboxes" separadas entre sí, por cuál una falla de seguridad en una aplicación no afectará a otra.
- Kernel asegurado con GR security Kernel

3 Puede ser descargada desde: https://tails.boum.org/
4 Puede ser descargada desde: https://www.qubes-os.org/
5 Puede ser descarga desde: https://subgraph.com/sgos/
6 Texto original: "defending against attacks where an exploit is delivered to the target from the Internet, e.g. in an email attachment or a website. So browser vulnerabilities, PDF viewer vulnerabilities, mail client vulnerabilities, etc. Vulnerabilities in applications the user runs on their desktop"

- Firewall que solicita que avisa y permite filtrar o no tráfico hacia Internet

Para Mirza Subgraph OS se diferencia de Tails y Qube OS por tener mitigación de exploits para todas las aplicaciones, bajo consumo de recursos, mayor control sobre las aplicaciones y sus permisos así como una mejor interfase de usuario. A pesar de esto, estas tres distribuciones buscan colaborar entre sí a través de una lista de correo electrónico[7](Mirza, David 2016).

4 Tor

Una de las principales características de SubgraphOS es que todo el tráfico de Internet pasa a través de la red Tor. Esta red permite ocultar la dirección ip de origen al destino de una petición TCP y oculta el destino de las peticiones TCP al proveedor de Internet. Esto se hace para dar anonimato y privacidad al usuario.

4.1 Funcionamiento red Tor

Generalmente se accede a Tor utilizando el navegador de Internet "Tor Browser Boundle". Si bien este es un uso común no es el único. Esta red puede ser utilizada para cualquier protocolo tipo TCP como puede podría ser IMAP, SMTP, FTP, XMPP y cualquier otro. Es decir a través de la red Tor se puede ocultar la dirección de IP de cualquier protocolo TCP.

Para lograr esto se utiliza una forma de enrutamiento conocido como "Ruteo de Cebolla". En el cliente funciona un programa llamado *Onion Proxy (OP),* el mismo que no requiere ningún privilegio de administración y se encarga de enrutar los paquetes a través de la red Tor utilizando los *Onion Routers (OR)*. El OP normalmente viene embebido en el programa "Tor Browser Bundle" y de esa misma instancia se podrían conectar otros programas a través del puerto 9150 en *localhost*.

El tráfico se agrupa en paquetes de 512 bytes conocidos como células. La comunicación entre el cliente y el servidor se la hace a través de TLS utilizando claves de larga duración para mantener la identidad del OR.

Los OR pueden ser identificados en la red a través de los servidores de llaves públicas que se encuentran en la red. Los OP no utilizan llaves públicas ya que interesa que no sean identificados para garantizar el anonimato. La comunicación entre OP con OR y de OR con OR es protegida a través de cifrado simétrico con AES de 128 bits. Se utiliza Diffie Hellman para el intercambio de clave de sesión.

La comunicación funciona de la siguiente forma:

1. Se establece un canal cifrado utilizando TLS entre el OP y el primer OR1 del circuito.
2. Se establece un canal TLS entre el OP y el segundo OR2 ruteando el tráfico a través del primer OR1.
3. A través de OR1 y OR2 se establece conexión TLS entre el OP y el tercer OR3.
4. El circuito de Tor queda formado y se puede utilizar para navegar en Internet de forma anónima o para cualquier otro servicio TCP.

Es importante notar que OR1 conoce la dirección ip de OP y OR2. OR2 conoce los IPs de OR1 y OR3, pero no conoce la del OP, ni el destino de la comunicación. El OR3 conoce el ip del OR2 y

7https://secure-os.org

del destino de la comunicación, pero desconoce los IPs de OP y OR1 como se puede ver en la ilustración 3.

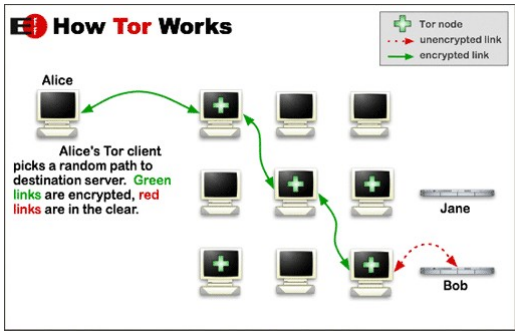

Ilustración 3: Explicación del funcionamiento del ruteo de Tor. Fuente del gráfico: https://www.torproject.org/about/overview.html.en

OR3 es un Tor relay por donde se sale al Internet de forma anónima. Hay que prestar atención a este ruteador, ya que si bien desconoce el origen de la comunicación, puede conocer los datos enviados al destino final si estos no están cifrados.

La elección de los OR por donde pasa la comunicación la decide el cliente de un listado de servidores publicado en los "Directory Servers" de la red(Dingledine, Mathewson, and Syverson 2004).

En teoría, cualquier aplicación que trabaje bajo un protocolo TCP podría funcionar a través de Tor sin necesidad de ser modificada. El único requisito es que pueda funcionar a través del proxy TCP SOCKS.

Tor y la NSA

El 4 de octubre de 2013 el periódico Inglés "The Guardian" publicó un reportaje donde se analizan documentos filtrados por Snowden sobre los intentos de la NSA de atacar a la red Tor(Ball, Schneier, and Greenwald 2013). De los documentos filtrados existe la presentación titulada "Tor Stinks", que data de junio de 2012, de la que se extrae la diapositiva de la lustración 4.

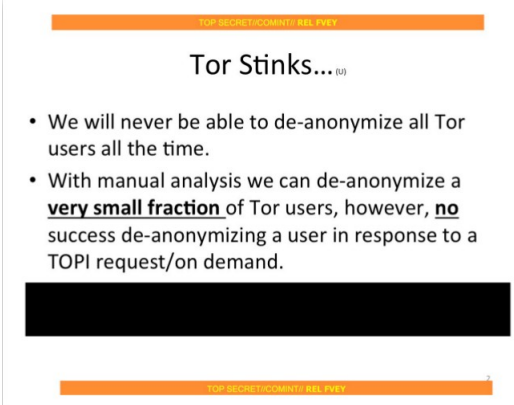

Ilustración 4: Diapositiva tomada de la presentación Tor Stinks de la NSA: https://edwardsnowden.com/2013/10/04/tor-stinks-presentation/

Según esta presentación de diciembre de 2012 la NSA no tenía una forma de acceder a todos los usuarios de la red Tor y tenía grandes problemas para espiar a quiénes lo usan. El uso de la red Tor en SubgraphOS da un nivel de protección que hace difícil el trabajo de las agencias de seguridad más importantes del mundo. Ese mismo poder viene integrado por completo en Subgraph OS para que lo use cualquiera de sus usuarios.

4.2 Navegador Web

El navegador de Internet es probablemente la aplicación más utilizada para acceder a servicios en Internet. Cada vez que se accede a un sitio web el proveedor de Internet puede saber que se esta accediendo a ese sitio. El servidor donde funciona la página web registra información de los usuarios a través de datos como la dirección *IP* y *cookies*. Muchas veces existen páginas de terceros que acceden a esta información a través de servicios como Google Analytics.

El navegador Tor es una versión modificada de Firefox que funciona con Tor de forma integrada y además trabaja con plugins como No-Script y HTTPS-Everywhere. Con No-Script se limita el

funcionamiento de las aplicaciones de Javascript para que no filtren información de la máquina a un sitio malicioso. Con HTTPS-Everywhere intenta siempre conectarse a sitios web que funcionan con HTTPS y de esta manera disminuir el riesgo de enviar tráfico plano.

Problemática con Navegador Tor

Si bien el Navegador Tor es muy seguro, tiene sus problemas de usabilidad. Existen sitios para los cuáles se requiere resolver *captchas* para acceder desde el Navegador Tor. Esto hace que el uso de Tor sea incomodo en páginas populares, en especial las s que usan el servicio de Claudfare. Este servicio es cada vez más popular porque permite a sitios web protegerse de ataques de DoS.

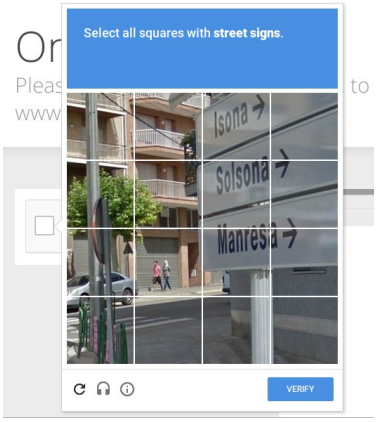

Ilustración 5: Ejemplo de captcha que se debe resolver al acceder a una página web que usa los servicios de Claudfare

Si bien Claudfare es un problema para los usuarios de Tor, no es el único. Una búsqueda en Google suele requerir resolver un captcha y sitios que requieren mucho Javascript o Flash no suelen funcionar de la manera esperada. Por otro lado herramientas como Flash o Javascript pueden ser utilizados para extraer información local de la máquina y de esta manera comprometer el anonimato.

4.3 Onionshare

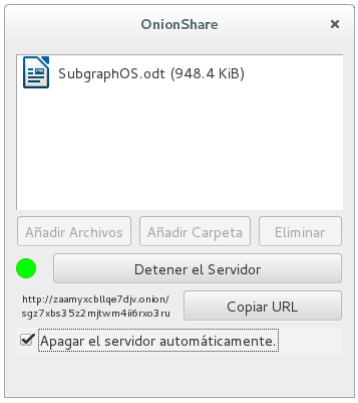

Ilustración 6: Herramienta Onionshare para compartir archivos

Onionshare es una aplicación sencilla que permite compartir archivos o carpetas a través de la red Tor sin depender de los servicios de un tercero como podría ser Google Drive o Dropbox. Para esto se crea un servicio oculto de Tor temporal que corre un servidor web por donde se puede compartir el archivo o carpeta. Cualquier persona que tenga acceso a un navegador Tor y tenga el enlace del archivo lo podrá descargar. Lo que hace que compartir archivos sea fácil. Adicionalmente Onionshare permite que el servicio oculto se elimine automáticamente después de de la primera descarga. Así el archivo solo llega a una personales

Un problema que se puede tener con Onionshare es compartir el enlace del archivo de forma segura. Para solucionar este problema se puede utilizar alguna de las aplicaciones de chat o correo electrónico cifrado que trae SubgraphOS.

4.4 Metaproxy

Las principales aplicaciones de Subgraph OS vienen configuradas para funcionar a través de Tor. Sin embargo el sistema no permite que salga tráfico de la máquina sino se lo hace a través de esta red. Para esto Subgraph esta desarrollando el servicio Metaproxy que permite enrutar el tráfico TCP a un servidor SOCKS, en el caso de Subgraph OS Tor.

Para su funcionamiento debe trabajar con reglas de *iptables* que fuercen el tráfico hacia Metaproxy. Esto ya viene configurado en la distribución.

4.5 Firewall

El sistema operativo viene con un firewall a nivel de usuario que avisa cada vez que una aplicación genera tráfico de red y permite al usuario aceptar este tráfico y recordar esa decisión. Si bien al principio esto puede ser molesto, con el tiempo el sistema creará solo las excepciones necesarias dando al usuario mayor control del uso de Internet de su equipo. Así mismo si alguna aplicación con malware quiere acceder a Internet y el firewall bloqueará este acceso y avisará al usuario.

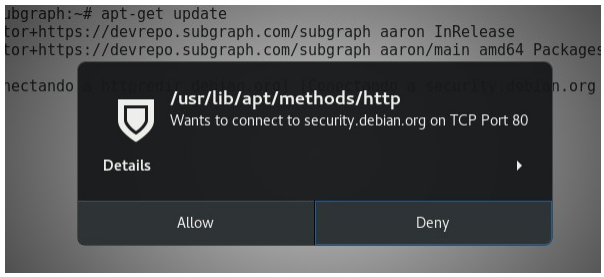

Ilustración 7: Activación del firewall al momento de actualizar repositorios

Aplicaciones como el navegador de Internet, correo electrónico y chat acceden a Internet sin ninguna alerta. Sin embargo en el caso de otras aplicaciones como el gestor de paquetes *apt* genera alertas. En las pruebas realizadas hubo un problema ya que *apt* solicita los paquetes de forma aleatoria a los servidores de Debian y esto hace que cada vez que se actualice los repositorios se deba añadir excepciones ya que se quiere descargar desde una dirección IP diferente. Considerando que Subgraph OS esta en versión alfa, se espera que este problema sea resuelto en futuras versiones.

5 Correo Electrónico

El correo electrónico es una de las herramientas de comunicación más utilizada en Internet. Sin embargo tiene problemas serios de seguridad ya que los mensajes viajan en texto plano. Si bien los protocolos de correo electrónico se pueden proteger utilizando SSL/TLS y STARTLS para asegurar para que la comunicación viaje cifrada entre cliente - servidor y también entre servidores, esto no siempre sucede. Además es común el uso de servicios de correo a través de *webmail* lo que hace que los correos sean guardados en el servidor.

Si el correo esta guardado en el servidor en texto plano, estos podrían ser leídos por el administrador del servidor de correo. Si el servidor de correo llegará a ser comprometido y los correos están almacenados en texto plano, estos podrían ser extraídos de forma masiva hacia un tercero. Un caso reciente de que esto sucediera es la filtración de correos electrónicos de Hillary Clinton hacia Wikileaks(WikiLeaks - Hillary Clinton Email Archive n.d.) que probablemente tuvo una repercusión importante en las últimas elecciones a presidente de los Estados Unidos del 2016.

Una forma de proteger el correo electrónico es cifrarlo de forma local antes de enviarlo. Para esto existe el protocolo PGP que a través de criptografía de llave pública permite cifrar el contenido de los correos.

La implementación libre de PGP más utilizada se conoce como GPG. Esta es una utilidad de línea de comando sobre la cuál se puede cifrar y firmar información además de gestionar llaves públicas y privadas. Al ser una utilidad de línea de comando, tiene interfaces gráficas que permiten gestionar de una forma amigable. Es muy común utilizar la combinación de Thunderbird con el complemento Enigmail.

5.1 PGP en Subgraph OS

Subgraph OS trabaja con el cliente de correo electrónico Icedove que es una versión de Thunderbird a la que se cambió el nombre y el logotipo(Icedove - Debian Wiki n.d.). La principal funcionalidad de Icedove es la de cliente de correo electrónico y por defecto no tiene la capacidad de cifrar los mensajes.

Para cifrar los mensajes Icedove utiliza el complemento Enignmail que permite gestionar llaves públicas y privadas así como cifrar y firmar mensajes. En el caso de Subgraph OS ya vienen las 2 aplicaciones instaladas y listas para funcionar desde la primera vez que se ejecuta.

Si bien GPG es bastante seguro para cifrar el contenido de los mensajes, tiene otros problemas. El principal tiene que ver con usabilidad ya que no es tan fácil entender el concepto de llave pública y privada para alguien que no conoce el tema.

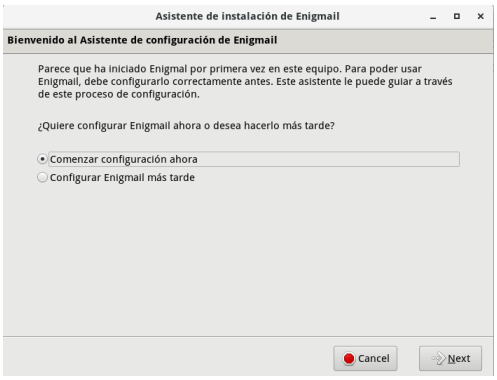

Ilustración 8: Asistente de configuración de Enigmail en Subgraph OS

PGP permite firmar los mensajes y de esta manera garantizar la autenticidad de los mismos. Sin embargo, no existe un esquema de autoridad certificadora centralizada. Para autenticar un usuario se lo suele hacer de manera manual verificando un *hash* de la llave pública conocido como "*fingerprint*". Una vez verificada la llave pública la comunicación se mantiene autenticada.

PGP también permite que cualquier pueda firmar la llave pública de otra persona y subirla a un servidor público de llaves. De esta manera, por ejemplo, si Alice verificó la identidad de Bob y quiere comunicarse con Carlos. Bob verificó la identidad de Carlos, firmó su llave pública y la subió al repositorio público de llaves. Cuando Alice quiere cifrar un correo a Carlos, ve que su llave pública tiene una firma válida de Bob, por lo cuál confía en esta clave.

La combinación de las personas que han firmado las llaves públicas entre sí se conoce como red de confianza y es una forma descentralizada de verificar la identidad de las personas en PGP.

5.2 Correo Electrónico y Metadatos

PGP solamente cifra el contenido de un mensaje, no cifra los metadatos asociados al mismo. De esta manera metadatos como destinatario, remitente asunto y fecha de envío pueden ser interceptados. Si bien el contenido de un mensaje no puede ser leído por un tercero, los metadatos sí. No se puede saber el contenido del mensaje, pero sí se puede saber quién se comunica con quién como ya se habló en el caso de Immersion.

Una forma de ocultar los metadatos es utilizar pseudónimos. Para crear uno pseudónimo que no se asocie con la identidad real de una persona se debe crear la cuenta a través de algún software de anonimato como Tor. De esta manera con Subgraph OS se podría crear una cuenta de correo electrónica anónima a través del navegador Tor y luego utilizarlo en Icedove para cifrar el contenido del mensaje.

En el caso de SubgraphOS, Icedove es una de las aplicaciones a las que se le da más importancia. Por este motivo viene con un complemento de Thunderbird conocido como Torbirdy. Torbirdy se encarga de enrutar el tráfico de Icedove por Tor. Además toma otras medidas de seguridad como cambiar el uso horario en la configuración de Icedove y no permitir el envío de correos en formato HTML.

6 Chat

Una de las herramientas más comunes de comunicación es el chat. Al igual que el correo electrónico, el chat suele depender del servidor de terceros. Si bien es común que la comunicación entre el servidor y el cliente es cifrada, el contenido de los mensajes no siempre lo es. Una herramienta tan popular como WhatsApp, recién en abril del 2016 empezó a cifrar los mensajes fin a fin(Business n.d.). Incluso si los mensajes son cifrados fin a fin, los metadatos no.

Subgraph OS tiene 2 opciones para resolver este problema. La primera es utilizar el cliente XMPP CoyIM que soporta OTR y la otra opción es Ricochet que es un servicio que funciona a través de la red Tor sin la necesidad de un servidor intermedio.

6.1 XMPP con OTR

XMPP es un protocolo que se usa principalmente para chat, aunque también tiene otros usos como Voz/IP y esta definido en los RFCs 6120, 6121 y 6122(XMPP | An Overview of XMPP n.d.). Es un protocolo federado que funciona de forma similar al correo electrónico. Es decir que usuarios de distintos servidores se pueden comunicar entre sí como se puede ver en la ilustración 9.

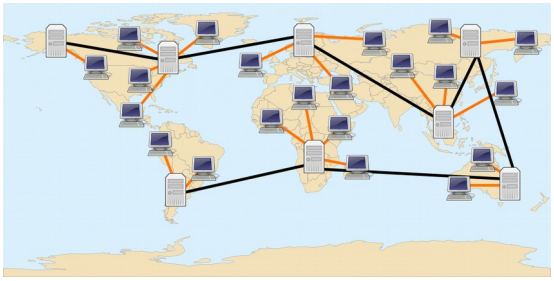

Ilustración 9: Esquema federado de XMPP. Fuente: Savant-fou/Tango Desktop Project/STyx - Travail dérivé de http://commons.wikimedia.org/wiki/File:Network-server.svg + http://commons.wikimedia.org/wiki/File:World_map_with_nations.svg, Public Domain, https://commons.wikimedia.org/w/index.php?curid=10590628

Una ventaja de utilizar XMPP vs las actuales tecnologías de chat es que se tiene la posibilidad de implementar un servidor propio. También existen varios servidores públicos en Internet donde se pueden registrar cuentas de manera anónima a través de Tor[8]. Por último la comunicación entre cliente y servidor se la realiza a través de TLS.

Con cuentas anónimas de XMPP creadas con Tor se puede proteger los metadatos. Para proteger el contenido es necesario cifrar la comunicación. Para esto se utiliza el protocolo OTR que cifra los mensajes antes de ser enviados. Este protocolo se puede combinar con varios protocolos de chat[9]. Uno de ellos es XMPP, el único requisito es que el protocolo de chat funcione con algún cliente compatible con OTR.

8 Un listado extenso de servidores se puede ver en el siguiente enlace: https://xmpp.net/directory.php

9 XMPP es solo uno de los protocolos sobre los cuáles se puede utilizar OTR: El programa pidgin (https://pidgin.im) soporta varios protocolos como los Google Talk o Facebook.

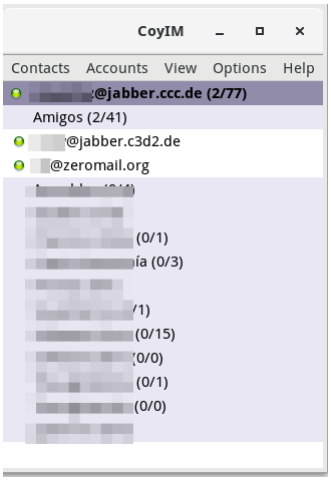

Ilustración 10: Captura de pantalla de CoyIM

El protocolo OTR funciona creando un canal de chat cifrado a través de Diffie Hellman con AES sin autenticar. La clave de cifrado se cambia en cada mensaje por lo que tiene la característica de *perfect secret forward*. Una vez que el canal esta cifrado las partes se autentican utilizando el algoritmo DSA(Off-the-Record Messaging Protocol Version 3 - DRAFT n.d.). La autenticación puede ser manual utilizando los huellas de las llaves públicas o se lo puede hacer a través de pregunta y respuestas entre las partes que realizan el chat y de esta manera abstraer el concepto de llaves a los usuarios.

En el caso de Subgraph OS viene con el cliente CoyIM que soporta el protocolo XMPP que tiene como objetivo principal la seguridad y facilidad de uso. Entre sus características se destaca que busca de forma automática conectarse a través de Tor, soporte para OTR, importar cuentas de chat y llaves OTR de otros programas como Pidgin. Este cliente todavía se encuentra en versión beta.

A través de CoyIM se puede crear cuentas anónimas de chat y ocultar gran cantidad de metadatos como la ubicación geográfica del usuario. Sin embargo, hay cierta metadata que se sigue compartiendo con el servidor de chat como las cuentas de chat que se comunican entre sí (aunque estas sean anónimas) así como la lista de contactos que se guarda en el servidor.

6.2 Ricochet

Ricochet es un protocolo nuevo que permite comunicarse sin un intermediario y de esta manera no confiar en un tercero para proteger la privacidad del usuario. Para conseguir esto en lugar de crear un usuario en un servidor, lo que hace Ricochet es crear un servicio oculto para cada usuario. En lugar de un cuenta de usuario lo que se tiene es un identificador del tipo: "**ricochet:6irmh7gsvrb55ejj**". Con este identificador otros usuarios pueden hacer solicitud de contacto y de esta manera se pueden añadir a la lista de contactos. A diferencia de XMPP la lista de usuarios se guardan localmente. Toda la comunicación cifrada fin a fin siempre(Ricochet n.d.).

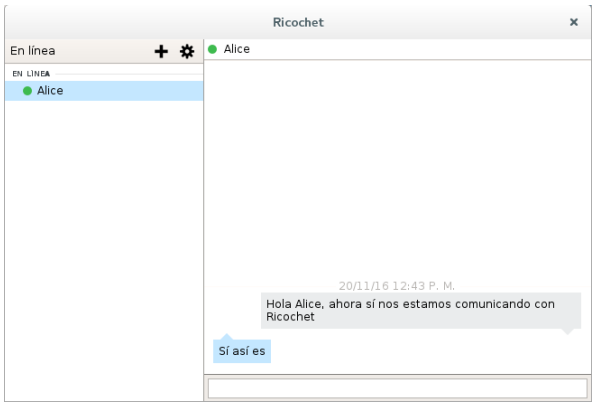

Ilustración 11: Ejemplo de conversación de chat utilizando Ricochet

Si bien SubgraphOS viene con Ricochet instalado por defecto y documentado en su guía de usuario. En las pruebas realizadas no funcionó. Considerando que Subgraph OS se encuentra en una versión alfa se espera que este problema se solucione en futuras versiones. Sin embargo se realizaron pruebas de Ricochet utilizando máquinas virtuales y el uso fue bastante sencillo. El mayor problema es compartir el identificador del chat de forma segura.

7 Aislamiento de Aplicaciones

Subgraph OS ejecuta las aplicaciones gráficas de forma aislada a través de contenedores conocidos como "*sandboxes*". De esta manera permite que las aplicaciones solamente puedan escribir en un espacio del disco duro, no puedan interactuar con otras a través del servidor X, se restringe el acceso a la red y llamadas al sistema operativo. De esta manera una aplicación comprometida no podría afectar el funcionamiento de otras(Subgraph OS Handbook n.d.).

Para esto Subgraph creo la herramienta OZ que permite configurar el aislamiento de aplicaciones.

7.1 PDF sin Internet

Un caso de uso de los *sandbox* de *OZ* es el lector de PDFs. Un atacante podría utilizar un PDF con código malicioso para insertar malware en el equipo y enviar información a través de la red. Evince, el lector de PDFs, viene configurado en un Sandbox por lo que si se abre un PDF con código malicioso este no tendrá acceso a Internet. De la misma manera si Evince tuviera una falla de seguridad y esta fuera explotada la vulnerabilidad no podría salir del contenedor de OZ.

8 Otras características de seguridad

8.1 Grsecurity

Grsecurity son un conjunto de parches que se aplican al *kernel* de Linux para mejorar su seguridad que se empezaron a desarrollar en febrero del 2001. Un componente importante de Grsecurity es Pax que permite mapear la memoria en modo de que ciertas partes de la misma sea solo para datos o sea del tipo no ejecutable. De esta manera intenta evitar ataques del tipo *buffer overflow*. Otra característica de Grsecurity es la posibilidad de un control de acceso de usuarios más restrictivo que el permitido en los sistemas Linux. Adicionalmente tiene características que dan mayor seguridad a los sistemas *chroot(Grsecurity/Overview - Wikibooks, Open Books for an Open World n.d.)*.

En el caso de Subgraph OS viene con un kernel compilado con soporte de Gresecurity. En el caso de las pruebas realizadas en laboratorio se pudo verificar que venía con el kernel **4.5.7-grsec-amd64**.

8.2 Protección USB para equipo bloqueado

Un posible ataque podría suceder es que el usuario de la máquina deje la computadora con la sesión bloqueada. Un atacante podría intentar inyectar código malicioso en el equipo a través de una memoria USB. Subgraph OS viene con la funcionalidad de *USB Lockout* que bloquea el acceso a los puertos USBs cuando el equipo esta bloqueado.

El soporte para el bloqueo de USB se lo hace a través del parche Pax de Grsecurity(Subgraph OS Handbook n.d.).

9 Disco duro cifrado

Cuando se tiene acceso físico a la computadora, no importa que tan segura sean las contraseñas de los usuarios del equipo. Un adversario podría encender el equipo con un sistema operativo desde una memoria USB o en un dispositivo óptico. Al hacer esto fácilmente pueden acceder al disco duro con privilegios de *root*. Si fuera el caso, también se podría sacar el disco duro y abrirlo desde otra computadora.

Si se piensa en computadoras personales donde se puede grabar información sensible. ¿Qué pasaría si estos equipos son robados? La persona que robó el equipo fácilmente podría tener acceso a toda la información guardada en el mismo. Este riesgo es todavía mayor si se piensa en equipos portátiles que se los lleva por la calle.

Una forma de evitar este peligro es cifrar el sistema de archivos del equipo. De esta manera no hay forma acceder a la información sino se conoce la contraseña que protege la clave de cifrado. Al momento de instalar Subgraph OS, se lo hace cifrando el disco duro. Para esto se crea un sistema lvm cifrado que incluye la partición de swap y todos los directorios del sistema operativo a excepción de */boot*.

9.1 Dm-crypt y Luks

DM-crypt

Desde la versión 2.6 del kernel de Linux viene con soporte de D*evice Mapper* que permite crear dispositivos de bloques virtuales. Crypt es parte de Device Mapper y permite tener cifrado transparente a nivel de de dispositivos de bloque utilizando el api de criptografía del *kernel* Linux. El usuario puede especificar los parámetros de cifrado simétrico como el algoritmo, la clave y el método, y de este modo crear un dispositivo de bloque en /dev. El dispositivo podría ser utilizado para un sistema de archivos, para sistemas RAID de software o LVM(Dmcrypt · Wiki · Cryptsetup / Cryptsetup n.d.).

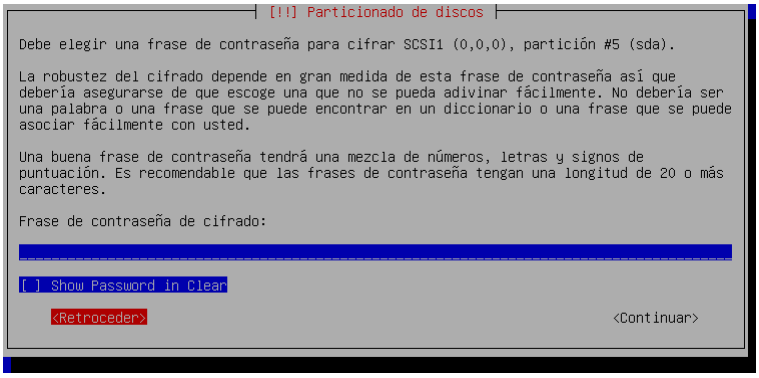

Ilustración 12: Configuración de contraseña para cifrado de disco duro al momento de instalar

En el caso Subgraph OS, se utiliza dm-crypt para crear los volúmenes lógicos de *LVM* sobre lo cuál se instalará el sistema operativo. Al momento de instalar el trabajo se hace forma automática y lo único que se solicita al usuario es la contraseña de cifrado como se puede ver en la ilustración 12.

```
Volumen cifrado (sda5_crypt) - 21.2 GB Linux device-mapper (crypt)
     #1             21.2 GB    K  lvm
LVM VG subgraph-vg, LV root - 19.1 GB Linux device-mapper (linear)
     #1             19.1 GB    f  ext4          /
LVM VG subgraph-vg, LV swap_1 - 2.1 GB Linux device-mapper (linear)
     #1              2.1 GB    f  intercambio    intercambio
SCSI1 (0,0,0) (sda) - 21.5 GB ATA VBOX HARDDISK
     #1  primaria  254.8 MB    F  ext2          /boot
     #5  lógica     21.2 GB    K  cifrado       (sda5_crypt)
```

Ilustración 13: Esquema de particionamiento creado para un disco duro de 20G

En las pruebas de laboratorio se creó una máquina virtual con Virtualbox a la que se le asignó un disco duro virtual de 20G y 2 G de memoria ram.

9.2 LUKS

DM-crypt funciona de modo *plain* y de modo *LUKS (Linux Unified Key Setup)*. El modo *plain* todas las tareas de cifrado se hacen de forma manual, mientras que *LUKS* permite hacerlo de forma más amigable.

```
root@subgraph:~# cryptsetup luksDump  /dev/sda5
LUKS header information for /dev/sda5

Version:        1
Cipher name:    aes
Cipher mode:    xts-plain64
Hash spec:      sha256
Payload offset: 4096
MK bits:        512
MK digest:      a3 04 75 b5 34 35 a0 ca 38 f2 0d ea 24 a6 8c ff c5 1b ba 80
MK salt:        67 87 65 56 fd 78 8e f1 fc ad 8a d6 ec 02 8a 28
                e7 89 ab d1 3a a7 c7 87 4e 19 ea b8 b3 c7 24 99
MK iterations:  90750
UUID:           8d0f3de3-8df0-4f4f-b26f-12731ec36819

Key Slot 0: ENABLED
        Iterations:             757394
        Salt:                   29 5a bb 6e f3 c8 6a c1 c2 aa 1f 11 fa 20 de 65
                                3d d7 05 15 75 34 a1 51 1f 49 0c 7f c8 67 91 b7
        Key material offset:    8
        AF stripes:             4000
Key Slot 1: DISABLED
Key Slot 2: DISABLED
Key Slot 3: DISABLED
Key Slot 4: DISABLED
Key Slot 5: DISABLED
Key Slot 6: DISABLED
Key Slot 7: DISABLED
root@subgraph:~#
```

Ilustración 14: Información sobre LUKS sobre la particionamiento creado

Cuando se crea un dispositivo con *LUKS* este crea de forma aleatoria la clave de cifrado. Esta clave de cifrado no es la misma que la contraseña que se utiliza en el teclado. La clave de cifrado puede ser protegida hasta con 8 contraseñas diferentes. Esto sirve para casos particulares donde más de una persona debe acceder a una unidad cifrada y cada uno puede tener contraseñas distintas. LUKS también permite definir el algoritmo de cifrado(Cifrando Discos, Particiones O Ficheros Con LUKS | Un Pingüino En Mi Servidor n.d.).

Subgraph OS realiza todo el trabajo de cifrado de disco de forma automática. Se puede ver los metadatos de la partición cifrada del laboratorio en la ilustración 14.

10 Conclusión

Considerando los riesgos a la privacidad y el anonimato en Internet Subgraph OS provee soluciones interesantes. A nivel físico permite cifrar el disco duro y bloquear el acceso a memorias USB cuando el sistema se encuentre bloqueado. A nivel de red protege el anonimato y la privacidad el usuario a través de enviar el tráfico por la red de Tor y su sistema de firewall. Protege las comunicaciones a través de cifrado fin a fin. Por último da protección a las aplicaciones al aislarlas las unas de las otras.

El cifrado de disco duro es una herramienta muy poderosa que permite a un usuario proteger su información. Si un equipo es robado, la información del mismo no va a poder ser accedida sin conocer la contraseña que protege esa información. De esta forma se puede garantizar la confidencialidad de la información. Sin embargo, si la computadora esta prendida y se tiene acceso físico, esta podría ser infectada a través de una memoria flash. Subgraph OS pensó en esta posibilidad y bloquea el acceso a memorias USB si la computadora se encuentra bloqueada.

A nivel de red envía todo el tráfico por Tor. Si bien esto da muchas ventajas en lo que se refiere a la privacidad y el anonimato de un usuario ya que no es fácil conocer su ubicación geográfica. Trae otros problemas como los de usabilidad. Si bien Mirza sostiene que Subgraph OS esta pensado para ser utilizado por todas las personas(Mirza, David 2016). ¿Estarán todos los usuarios dispuestos a aceptar las incomodidades con las que viene asociado Tor como son navegación lenta, captchas y mal funcionamiento de ciertas páginas web? Tal vez las personas que sean objetivos de algún programa de vigilancia no tendrán problema para aceptar esta incomodidad. Por otro lado Subgraph OS no funciona con UDP, aunque Mirza dice que se tiene planes para soportarlo en el futuro(Mirza, David 2016).

El sistema de Firewall es muy interesante porque se puede saber exactamente que aplicación accede a Internet y cuál no. Saber que una calculadora quiere acceder a Internet, por lo menos daría en que pensar, aunque podría tener usos legítimos[10]. Por otro lado tener que aceptar excepciones de manera constante puede ser muy incómodo. De las pruebas hechas en laboratorio aplicación *apt* de momento tiene problemas de usabilidad. Sin embargo estos no son tan difíciles de hacer y se puede contribuir a la solución del problema reportando el error. Se entiende que luego de un tiempo de uso ya no será necesario aceptar más conexiones y el equipo hará lo que tiene que hacer.

El cifrado fin a fin es muy útil aunque no siempre es tan fácil de utilizar. De las aplicaciones que vienen en Subgraph OS tal vez la menos segura y más difícil de usar es PGP. Herramientas como Ricochet llaman la atención ya que son fáciles de usar, la comunicación va cifrada siempre y la protección de metadatos es muy alta. El chat con XMPP es un punto intermedio en el cuál se comparten pocos metadatos y se puede cifrar la comunicación fin a fin.

El aislamiento de aplicaciones un esquema de seguridad muy interesante. Si bien las pruebas de laboratorio no se pudo evidenciar problemas de usabilidad. Esto no se puede conocer hasta no usar la aplicación de forma permanente. Solo ahí se encontrarán los posibles problemas.

Otro dato a destacar de Subgraph OS es que su desarrollo se lo hace a través de pequeños componentes que luego podrían ser incorporados por terceros. De hecho el software *paxrat* ya esta en proceso de ser incorporado en Debian(Mirza, David 2016).

Si bien Subgraph OS se encuentra en una versión alfa, trae ideas interesantes para la protección de los equipos de escritorio. Es importante destacar que los problemas de usabilidad no se los puede conocer en detalle hasta no utilizar la herramienta de manera permanente. Será interesante ver como este tipo de distribución evoluciona en el futuro y si la computación en el futuro estará enfocada a la privacidad.

10 De hecho la calculadora del entorno GNOME se conecta a Internet para consultar información financiera.

11 Bibliografía

Ball, James, Bruce Schneier, and Glenn Greenwald
2013 NSA and GCHQ Target Tor Network That Protects Anonymity of Web Users. The Guardian, October 4. https://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption , accessed November 15, 2016.

Business, Author: Cade Metz Cade Metz
N.d. Forget Apple vs. the FBI: WhatsApp Just Switched on Encryption for a Billion People. WIRED. https://www.wired.com/2016/04/forget-apple-vs-fbi-whatsapp-just-switched-encryption-billion-people/, accessed November 19, 2016.

Cifrando Discos, Particiones O Ficheros Con LUKS | Un Pingüino En Mi Servidor
N.d. http://blog.inittab.org/administracion-sistemas/cifrando-discos-particiones-o-ficheros-con-luks/, accessed November 15, 2016.

Dingledine, Roger, Nick Mathewson, and Paul Syverson
2004 Tor: The Second-Generation Onion Router. DTIC Document. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA465464, accessed November 9, 2016.

Dmcrypt · Wiki · Cryptsetup / Cryptsetup
N.d. GitLab. https://gitlab.com/cryptsetup/cryptsetup/wikis/DMCrypt, accessed November 11, 2016.

Edward Snowden: NSA Whistleblower Answers Reader Questions
2013 The Guardian, June 17. https://www.theguardian.com/world/2013/jun/17/edward-snowden-nsa-files-whistleblower, accessed November 20, 2016.

Global Surveillance Disclosures (2013–present)
2016 Wikipedia. https://en.wikipedia.org/w/index.php?title=Global_surveillance_disclosures_(2013%E2%80%93present)&oldid=747847767, accessed November 10, 2016.

Grsecurity/Overview - Wikibooks, Open Books for an Open World
N.d. https://en.wikibooks.org/wiki/Grsecurity/Overview, accessed November 20, 2016.

Icedove - Debian Wiki
N.d. https://wiki.debian.org/Icedove, accessed November 19, 2016.

Julian Assange: “No Hay Elección, Tenemos Que Pasarnos Al Software Libre Para Nuestra Mejor Protección”
2014 Agencia de Noticias. http://www.telam.com.ar/notas/201409/79058-julian-assan-software-libre-ciberseguridad-espionaje.html, accessed November 20, 2016.

Los Países Iberoamericanos Que Usaron a Hacking Team
2015. https://hipertextual.com/2015/07/los-paises-iberoamericanos-que-usaron-a-hacking-team-para-espiar, accessed November 20, 2016.

Mirza, David
2016 Entrevista David Mirza. Correo electrónico. November 19.

Off-the-Record Messaging Protocol Version 3 - DRAFT
N.d. https://otr.cypherpunks.ca/Protocol-v3-4.0.0.html, accessed November 20, 2016.

Ricochet
N.d. Ricochet. https://ricochet.im/, accessed November 20, 2016.

Subgraph OS
N.d. https://subgraph.com/sgos/, accessed November 9, 2016.

Subgraph OS Handbook
N.d. https://subgraph.com/sgos-handbook/sgos_handbook.shtml, accessed November 20, 2016.

U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program - The Washington Post
2013. https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html, accessed October 16, 2016.

WikiLeaks - Hillary Clinton Email Archive
N.d. https://wikileaks.org/clinton-emails/, accessed November 16, 2016.

XMPP | An Overview of XMPP
N.d. https://xmpp.org/about/technology-overview.html, accessed November 19, 2016.

12 Anexo 1: Entrevista a David Mirza

En el año 2013 conocí a David Mirza en un evento del que fui organizador en Quito. El mismo trataba la temática sobre vigilancia masiva en Internet y lo llamamos Minga por la Libertad[11]. Durante el evento se hizo la publicación de Orchid que es un cliente y una librería de Tor desarrollada en Java por Subgraph. Recientemente Subgraph empezó a desarrollar Subgraph OS. Así que decidí contactarlo y realizar la siguiente entrevista para este trabajo.

David Mirza es socio fundador de la empresa SubgraphOS que mantiene el desarrollo de los proyectos de software libre Vega que es una aplicación análisis de seguridad a aplicaciones web, Orchid que es una implementación del protocolo Tor hecha en Java y recientemente Subgraph Os. Antes de esto, fue miembro fundador de Security Focus, donde moderó la lista de correo Bugtraq, foro histórico de seguridad informática, que en su apogeo contó con 50.000 miembros. David ha hablado en numerosas conferencias de seguridad y software libre, ha contribuido a libros, revistas y otro tipo de publicaciones. David también participó en un grupo de trabajo CANI en nombre de Symantec para desarrollar la primera versión del CVSS (Common Modelo de Scoring System) Vulnerabilidad y fue editor para la sección ”Tendencias” de “IEEE Security & Privacy” durante más de tres años.

A continuación la entrevista.

Who are the people behind Subgraph and what have you done in terms related to computer security?

We are a team of 4. Three of us have worked together for over 10 years in various companies in the past. Before this ,we were friends as teenagers in Calgary (Canada) originating the local hacking scene.

When we were in our 20s we all worked at SecurityFocus. I was moderating the Bugtraq mailing list from 2001-2005, and after that it was David McKinney.

Our background is in offensive security (vulnerability research, exploit development), with some additional experience working with privacy and censorship circumvention.

Why did you decided to create Subgraph OS? Did it had anything to do with Subgraph OS

Because there is no free software OS that prioritizes endpoint security., even though the best security mitigations (e.g. grsecurity) were pioneered as FLOSS projects and all the proprietary vendors copied it.

We wanted a FLOSS OS that's hard to hack. This didn't exist, therefore, Subgraph OS.

What do you mean by an "Adversary resistant computing platform"?
A platform for communication that is resistant to attack by network borne adversaries - an OS that uses the most cutting edge exploit mitigation & secure OS design ideas. We are primarily defending

11 https://web.archive.org/web/20131204163717/https://minga.asle.ec/

against attacks where an exploit is delivered to the target from the Internet, e.g. in an email attachment or a website. So browser vulnerabilities, PDF viewer vulnerabilities, mail client vulnerabilities, etc. Vulnerabilities in applications the user runs on their desktop.

What does make Subgraph OS better than distributions like Tails or QubeOS?

I would say:

a) Exploit mitigations for *all* applications
b) Lighter resource requirement
c) Finer grained controls over application behavior / permissions
d) Better UX

Is there collaboration between this projects?

We are discussing it, and hope that it happens. We created a forum for discussing these initiatives - the secure desktops mailing list (https://secure-os.org).

Is Subgraph OS for everyone or just for people who actually are targets?

We believe it should be for anyone, and are striving towards this goal (Though we are still in alpha).

Subgraph is base in Debian. Is it possibel to install any Debian application in Subgraph OS?

Yes! You can apt-get install anything in Debian. Most should work.

Tor works with TCP, how do you handle protocols that use UDP?

We don't yet. Coming in the future.

Can you do VoIP with Subgraph OS?

I've never tried. If it use TCP, should be possible.

From the Subgraph OS I see you can work with kvm virtual machines. Does the virtual machine would route all the traffic through Tor.

It should if it's NAT. If it's a bridge interface, then no.

Is Subgraph OS founded in any way so that it could be sustainable in time?

Yes - we are often doing security consulting work to support Subgraph OS development. The Subgraph organization is almost 7 years old. We are able to sustain ourselves, and we are not going anywhere. We expect to grow.

Are projects like Metaproxy, OZ and others created by Subgraph being submitted to Debian?

Yes, certain parts of Subgraph OS are of interest to and being considered by Debian. On example is the paxrat utility, which one Debian dev has recently packages. Metaproxy isn't one of those currently but certainly could be in the future.

How many people are working in the development of Subgraph OS?

Four full time Subgraph staff, plus a few volunteers /community members.