“Análisis de los programas de vigilancia en Internet ”

“Internet Surveillance Programs”

Alfonso González Luis

Máster interuniversitario de seguridad de las tecnologías de la información y de las comunicaciones

Universitat Oberta de Catalunya, 13 de Junio de 2014

Directora: Cristina Pérez Solà

AUTORIZACIÓN DE DIFUSIÓN

El abajo firmante, matriculado en el máster interuniversitario de seguridad de las tecnologías de la información y de las comunicaciones, autoriza a la Universidad Oberta de Catalunya (UOC) a difundir y utilizar con fines académicos, no comerciales y mencionando expresamente a su autor el presente Trabajo Fin de Grado:

"**Análisis de los programas de vigilancia en Internet**", realizado durante el curso académico 2013-2014 bajo la dirección de Cristina Pérez Solà, y a la Biblioteca de la universidad a depositarlo en el Archivo Institucional con el objeto de incrementar la difusión, uso e impacto del trabajo en Internet y garantizar su preservación y acceso a largo plazo.

13 de Junio de 2014

Alfonso González Luis

RESUMEN

Durante el último año y con la publicación de documentos confidenciales por parte del ex analista de la NSA Edward Snowden, han salido a la luz diversos programas de vigilancia por parte de los gobiernos. Estos programas recogen información de los ciudadanos a través de las redes de telecomunicaciones y en un marco donde la legalidad de los mismos puede quedar en entredicho.

En esta memoria se puede encontrar una breve introducción al origen de dichas filtraciones así como una definición de las grandes agencias de inteligencia que operan dichos programas. El tema central de este proyecto trata de estudiar cuatro grandes proyectos de vigilancia de los que se tiene constancia. Se describirá en detalle cada uno de ellos, centrándose en el tipo de datos que recoge, como lo hace y cual es la finalidad de la información recogida.

Por último se presentará una serie de herramientas que los usuarios pueden utilizar con objetivos de protegerse o al menos dificultar la captación de datos por parte de los gobiernos. Estas medidas no son simplemente técnicas sino que incluyen acciones a llevar o evitar en el uso diario de las tecnologías y la redes.

Palabras clave:

- ***Programas de vigilancia***
- ***PRISM***
- ***MUSCULAR***
- ***XKEYSCORE***
- ***TEMPORA***
- ***NSA***
- ***GCHQ***

ABSTRACT

During last year and as a result of the release of confidential documents by former NSA analyst Edward Snowden, various surveillance programs run by governments have come out to the public knowledge. These programs collect information from citizens through telecommunications networks and its legality may be doubtful.

Herein you can find a brief introduction to the origin of the leaks and a definition of major intelligence agencies operating such programs. The focus of this project is to study the four major surveillance programs. We will describe in detail each of them, focusing on the type of data collected, how they collect it, and what is the purpose of the collected information.

Finally we will present various tools that users can use to protect themselves against this programs or at least hinder the uptake of data collected by governments. These measures are not simply technical but it will include actions to take or avoid in our daily use of technology and networks.

Keywords:

- ***Surveillance Programs***
- ***PRISM***
- ***MUSCULAR***
- ***XKEYSCORE***
- ***TEMPORA***
- ***NSA***
- ***GCHQ***

ÍNDICE

ÍNDICE DE ILUSTRACIONES

CAPÍTULO 1

1.1 INTRODUCCIÓN

Las recientes revelaciones del ex empleado de la CIA Edward Snowden, han mostrado al mundo que la cantidad de información que la NSA estaba recogiendo sobre los ciudadanos era mucho mayor que la que en un principio se pensaba. Programas de vigilancia como son PRISM, BULLRUN, Upstream o Xkeyscore fueron descubiertos recogiendo y analizando grandes cantidades de datos tanto de ciudadanos de los Estados Unidos como extranjeros. Por otra parte, la existencia de algunos de estos programas, estaba amparada por posibles interpretaciones de leyes Estados de Unidos. Este hecho hace que el problema se vuelva incluso peor ya que existe un conflicto de intereses, y derechos entre los ciudadanos y el gobierno.

El objetivo de este proyecto es por tanto crear un informe actualizado de los programas de vigilancia en internet actuales. Este informe contendrá una revisión de los programas de vigilancia en internet conocidos hasta el momento e investigará el trasfondo histórico y contextual que permitió tanto la aparición de estos programas como su revelación pública. Posterior a este análisis estaríamos en condiciones de estudiar las herramientas que tienen a disposición los ciudadanos para que puedan mantener su privacidad durante la transmisión digital de información.

1.2 OBJETIVOS

Los objetivos planteados para la realización de este trabajo son los que a continuación quedan mencionados:

1. Hacer un análisis general de los distintos programas de vigilancia que existen en Internet por parte de los gobiernos. Esto incluye a otros países con programas similares a Estados Unidos como puede ser el caso de Francia o Reino Unido.

2. Una vez encontrados estos programas, analizar su funcionamiento origen y motivación. Tratar de encontrar que tipo de información explotan y con que objetivos específicos.

3. Contextualizar la aparición de dicho programas así como investigar el trasfondo histórico de los mismos.

4. Búsqueda y análisis de herramientas que los ciudadanos tienen a su disposición para poder realizar transmisión digital de información de manera segura.

1.3 ORGANIZACIÓN DEL TRABAJO

En esta sección del presente documento atenderemos a los aspectos metodológicos y de diseño de la investigación sobre los programas de vigilancia en internet. Intentaremos explicar la naturaleza de las técnicas elegidas, es decir, exponer el camino que hemos elegido para abordar el objeto de estudio, así como también aportar una justificación acerca de por qué hemos elegido realizar el estudio de esta manera.

Dado que nuestro TFM está fuertemente ligado a la metodologías de trabajo de la UOC, creemos que es conveniente trabajar de forma evolutiva e iterativa. Se plantean una serie de entregas definidas por el propio alumno con un plazo de tiempo prefijado.

Así mismo, y debido a que nuestro objeto de estudio es puramente investigativo, es de vital importancia la recogida de información. Afortunadamente existe en la red multitud de documentos y presentaciones internas de los organismos encargados de desarrollar y explotar dichos programas.

Una vez recogida esta información y como parte esencial de la metodología de trabajo es aplicar sobre los datos obtenidos síntesis de forma que nos quedemos únicamente con la información relevante y así poder realizar sobre ella inferencias que nos permitan las consecución de los objetivos planteados en el comienzo del presente documento.

CAPÍTULO 2

2.1 INTRODUCCIÓN

El presente capítulo servirá como introducción a los conceptos y terminología empleados durante el presente trabajo. Trataremos de explicar de la forma mas clara y concisa posible los diferentes términos empleados en el mundo de la vigilancia en las redes por parte de los gobiernos. Así mismo se introducirán brevemente las dos grandes agencias de espionaje que disponen de programas de vigilancia.

2.2 CONCEPTOS

- SIGINT: Se conoce por el nombre de SIGINT a la obtención de información a través de la interceptación de señales. Es importante destacar que estas señales no son exclusivamente electrónicas sino que puede ser considerado también como SIGINT la interceptación de la comunicación entre dos personas. La inteligencia de señales suele estar compuesta por tres grandes recursos bien diferenciados que son:

    - COMINT o inteligencia de las comunicaciones, que obtiene la información a través de las comunicaciones ya sean por radio, teléfono o internet.

    - ELINT o inteligencia electromagnética, que emplea dicho fenómeno físico para obtener información. Un ejemplo de este tipo de inteligencia serían los radares que permiten la localización de objetivos.

    - TELINT o inteligencia telemétrica cuya función es la captación de información mediante imágenes ópticas.

- SIGAD: Dentro de las agencias de los Estados Unidos se conoce como SIGAD (Signal Intelligence Activity Designator) a las colecciones de plataformas o medios que las agencias utilizan para obtener y procesar información. Generalmente se representa con una cadena alfanumérica compuesta por un prefijo de dos o tres letras y seguido de uno a tres caracteres numéricos.

- FISA: La Foreign Intelligence Surveillance Act de 1978 (FISA) o también conocida como Ley de Vigilancia de la Inteligencia Extranjera, se trata de una ley de los Estados Unidos que establece los procedimientos para la vigilancia física y electrónica y la recopilación de información de inteligencia extranjera. Una de las peculiaridades de esta ley es que permite incluir en las vigilancia a ciudadanos estadounidenses y residentes permanentes sospechosos de actividades de espionaje o terrorismo.

- FISC: Acrónimo de Foreign Intelligence Suerveillance Court, es el Tribunal de Vigilancia de Inteligencia Extranjera, creado y autorizado por la FISA que se encarga de supervisar y autorizar en caso de que sea necesario las solicitudes de vigilancia contra presuntos sospechosos de actividades de espionaje o terrorismo dentro de los Estados unidos.

- DATA FLOW: Cuando los programas de vigilancia realizan escuchas que obtienen los datos directamente de los cables de comunicaciones ya sean submarinos o terrestres se conoce como data flow.

- PROVEEDORES: Cuando los programas de vigilancia adquieren las comunicaciones de los proveedores de servicios como puede ser Google, Facebook, Yahoo!, etc podemos afirmar que esta recogida de información se hace a través de proveedores.

2.3 NSA

La National Security Agency (NSA) fue creada por el presidente Harry Truman en 1952, sobre el precedente de la Agencia de Seguridad de las Fuerzas Armadas, que surgió al acabar la Segunda Guerra Mundial. Es una de las columnas fundamentales de la inteligencia de Estados Unidos. A diferencia de otras otras agencias más conocidas como la CIA, consagrada al espionaje o acciones encubiertas en el exterior, la NSA se dedica básicamente a la interceptación de comunicaciones y a la generación de inteligencia. Está dividida en dos partes: el Directorio de Señales de Inteligencia, que recoge información transmitida por actores externos, tanto en el extranjero como en EE.UU., y el Directorio de Garantía de Información, que protege los sistemas de información nacionales. En ambas

funciones tienen un papel relevante la criptografía. Su servicio de captación y descifrado de mensajes beneficia al resto de agencias de inteligencia. Casa día intercepta y almacena millones de correos electrónicos, llamadas telefónicas y otros elementos de comunicación.

2.4 GCHQ

GCHQ o Government Communications Headquarters (Cuartel General de Comunicaciones del Gobierno) es uno de los tres servicios de inteligencia de los que dispone el Reino Unido junto al MI5 y MI6. Al igual que su equivalente estadounidense su función no se centra en el espionaje sino que adquiere notoriedad en dos campos que son:

- La inteligencia de señales (SIGINT), que supone la monitorización, intercepción y descifrado de datos, sobre todo en la lucha contra el terrorismo y el crimen organizado;

- La *information assurance* (IA), una especialización de la seguridad de la información, para proteger los sistemas de comunicaciones informáticas del gobierno británico.

Los orígenes de la agencia se remontan a la primera guerra mundial. Hasta dicho momento el gobierno británico disponía de dos agencias independientes de inteligencia conocidas como MI1b y NID25 respectivamente. Tras la finalización de la guerra se decidió crear una única agencia bajo el nombre de Government Code and Cypher School. Aunque en un principio los trabajos de la agencia fueron el análisis del tráfico diplomático con el estallido de la Segunda Guerra Mundial, la GC&CS adquirió mayor importancia siendo uno de sus mayores logros el descifrado del código enigma Alemán, en el que participó Alan Turing.

Tras la finalización de la guerra, la agencia adquiere su nombre actual y entre sus logros se encuentra la invención del algoritmo RSA años antes de que fuera publicado por Rivest, Shamir, y Adleman en el MIT[1]

CAPÍTULO 3

3.1 INTRODUCCIÓN

A lo largo de este capítulo trataremos de aportar la mayor información posible sobre cuatro grandes programas de vigilancia conocidos que son:

- PRISM
- XKEYSCORE
- MUSCULAR
- TEMPORA

Para cada uno de ellos analizaremos su origen, forma de funcionamiento, datos que captura y la finalidad para la que fueron creados. Así mismo, aportaremos un análisis sobre el impacto social que ha conllevado su filtración y las reacciones sociales que ha sido observada tras las mismas. El carácter secreto de estos programas hace que la información que se dispone de ellos sea muy limitada y que el conocimiento sobre características como su forma de funcionamiento se deba en muchos casos a un proceso de ingeniería inversa o a la simple especulación.

3.2 PRISM

3.2.1 INTRODUCCIÓN

El primer programa que analizaremos será PRISM. Hemos creído necesario comenzar por este pues aun no siendo el que más datos recaba fue el primer programa que ponía de manifiesto lo que desde hacía tiempo se creía. Los gobiernos estaban interceptando de alguna forma las comunicaciones a través de las redes para protegerse ante ataques de posibles enemigos o como un método de espionaje e inteligencia.

Puesto en marcha en 2007 por la Agencia Nacional de Seguridad, en adelante NSA, PRISM es un programa clandestino de vigilancia que tiene como objetivo recoger las comunicaciones de internet en base a peticiones hechas a las compañías de internet para su posterior análisis. Su filtración se produjo el 6 de Junio de 2013 cuando los periódicos The Guardian[1] y The Washington Post[2] publicaron parte de la información extraída por

Snowden de la NSA en la que se podía visualizar una serie de diapositivas que hablaban sobre PRISM así como la copia de una orden judicial que obligaba a Verizon a darle a dicha agencia datos sobre las comunicaciones de sus clientes.

La posibilidad de la existencia de PRISM reside en la existencia de la denominada Ley "Protect America Act" aprobada durante la administración Bush. Con dicha Ley se eliminaba el requisito de autorización para la vigilancia de los objetivos de inteligencia extranjeros, que obligaba a que los mismos debieran estar estar presumiblemente fuera de los Estados Unidos. PRISM es operado bajo la supervisión de la U.S. Foreign Intelligence Surveillance Court (FISA Court, o simplemente FISC[3]) de conformidad con el Ley de Vigilancia de Inteligencia Extranjera (FISA[4])

3.2.2 DATOS RECOGIDOS

A través de las revelaciones de Snowden se conoce que PRISM es un tipo de programa de vigilancia que obtiene la información a través de nueve proveedores que son[5]:

- Microsoft: Es el primer proveedor de datos del programa PRISM y comenzó a proporcionar datos el 11/09/07
- Yahoo: comenzó a proporcionar datos a las colecciones de la NSA el 12/3/08
- Google: el 14/01/09 comienzan a incorporarse datos de Google a PRISM
- Facebook: 03/06/09 se incorporan datos de Facebbok
- Paltalk: 07/12/09 se incorporan datos de Paltak
- Youtube: 24/09/10 se incorporan datos de Youtube
- Skype: 06/02/11 se incorporan datos de Skype
- AOL: 31/03/11 se incorporan datos de AOL
- Apple: 1/10/12 se incorporan datos de Apple

Los programas de la NSA recogen principalmente dos tipos de datos: los metadatos y el contenido. Los metadatos son el subproducto de las comunicaciones sensibles, tales como los registros telefónicos que revelan a los participantes, horas y duración de las llamadas. Sin embargo, PRISM es un tipo de programa que almacena contenido. Según las propias diapositivas filtradas el contenido almacenado incluye:

- Email

- Chat – Vídeo
- Voz
- Fotos
- Datos guardados
- VoIP
- Trasferencias de archivos
- Videoconferencias
- Notificaciones de actividad del objetivo (logins, etc)
- Detalles sobre las redes sociales.

3.2.3 FUNCIONAMIENTO

Una vez entendido el origen de PRISM, el tipo de datos que recoge y las motivaciones de su existencia es importante señalar como funciona. En este apartado incluiremos las bases tanto legales como técnicas que posibilitan su funcionamiento.

Por una parte, si observamos el aspecto legal su existencia se basa en dos leyes fundamentales y que podemos considerar comunes a todos los programas de vigilancia existentes en territorio estadounidense y que son:

- La Sección 702 de la Ley de Enmiendas de la FISA (FAA)
- La Sección 215 de la Ley Patriota.

La primera autoriza a la colección de contenido las comunicaciones previstas en PRISM mientras que la segunda, autoriza la recolección de metadatos de las compañías telefónicas como Verizon. Sin embargo, varios informes y documentos filtrados indican que los estatutos han sido interpretadas por los tribunales de inteligencia de la FISA para otorgar una autoridad mucho más amplia para la que fueron originalmente concebidos. También indican que los tribunales de FISA sólo aprueban los procedimientos de recolección de la NSA, y no se requieren garantías individuales para objetivos específicos.

Por otra parte, para conocer las características técnicas que posibilitan su existencia encontramos que el método más fiable para interpretar su funcionamiento son las propias diapositivas filtradas. En ellas se describe a PRISM como el SIGAD[6] más utilizado para la generación de reportes dentro de la NSA. En las mismas diapositivas se explica que una

gran cantidad de comunicaciones digitales se producen a través del territorio de los Estados Unidos. Esta afirmación cobra sentido cuando pensamos en que las mayores empresas tecnológicas residen en dicho país (Microsoft, Facebook, Google, Apple). Por lo tanto y como los procesos de enrutado de la información a través de internet siguen el camino más barato y no el más directo, es bastante probable que la información sobre un objetivo de la NSA pase por los Estados Unidos en algún momento tal y como se explica en el mismo documento.

Desde el punto de vista del analista su trabajo comienza por introducir "selectores" (términos de búsqueda) en un sistema de búsqueda, a continuación se lanzan tareas para obtener la información de otros sitios de recolección, conocidos como SIGADs. Los SIGADs son conocidos por un nombre en clave clasificado y otro no clasificado. Cada tipo de SIGAD se encarga de tratar diferentes tipos de datos. Un SIGAD conocido como NUCLEON se encarga de recoger el contenido de las conversaciones telefónicas, mientras que otros como MARINA actúan de almacén de metadatos internet. Como indicábamos al comienzo de esta sección, el propio PRISM es un SIGAD que se lanzará para recabar la información de sus propias fuentes, que son los proveedores de servicios mencionados anteriormente.

3.2.4 FINALIDAD

De forma genérica podríamos decir que PRISM surge con el objetivo de proveer al gobierno estadounidense y sus aliados de información que le ayude a protegerse ante amenazas que puedan dañar su territorio o a sus ciudadanos. No obstante, esta es una definición bastante genérica que podría ser utilizada para cualquier otro programa de vigilancia del que se disponga.

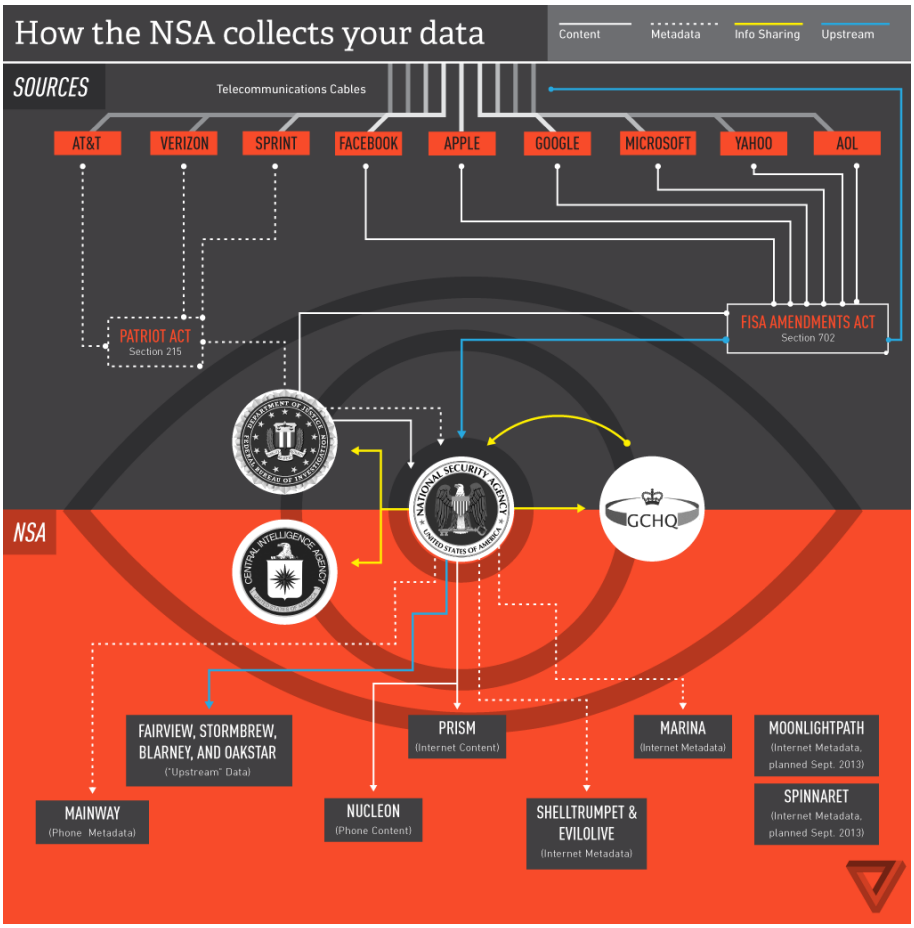
La particularidad que tiene PRISM y que va unido intrínsecamente a su finalidad es la capacidad para captar información desde los grandes proveedores de servicios en internet. A través de dicho programa la NSA puede obtener información muy valiosa sobre su objetivos. Si comparamos PRISM con otro SIGAD que base su funcionamiento en una conexión a un flujo de datos (ej: Upstream), queda evidenciado que la ventaja del primero frente al segundo es la capacidad de realizar búsquedas ya que podemos acceder a la información almacenada y no únicamente a colecciones en tiempo real.

Por lo tanto, podemos concluir que la finalidad de PRISM es la de un SIGAD que permita realizar búsquedas y vigilancia sobre los datos obtenidos de sus diversos proveedores de contenidos.

3.2.5 REPERCUSIONES

Aunque como indicábamos al comienzo del capítulo PRISM no es el programa que más datos recopila, si que fue el primero en hacerse público, por lo que su repercusión mediática fue la más extendida y su conocimiento por parte de la población es más amplio. Todas las compañías que aparecieron como “proveedores” de datos en los documentos filtrados por Snowden hicieron declaraciones públicas a través de sus representantes en los días posteriores al 6 de Junio de 2013.

Las declaraciones siguieron todas una línea similar argumentando que o bien no proveían al gobierno de los Estados Unidos de *acceso directo* a sus sistemas de información y que solo se respondía ante peticiones formales a través de una orden judicial, o bien desconocían totalmente la existencia de dicho programa de vigilancia.



Illustración 1: Esquema del funcionamiento de PRISM

3.3 XKEYSCORE

3.3.1 INTRODUCCIÓN

El segundo programa de vigilancia del que hablaremos es XkeyScore, es quizás un programa menos conocido que PRISM pero que sin embargo aporta mucha mas información a la NSA y sus aliados. Según palabras del propio Snowden y tal como descubriremos a continuación podemos considerar XkeyScore más como un motor de búsqueda dentro de la NSA que un programa de vigilancia ya que su principal utilidad es la de devolver información filtrada según las consultas que haga el analista al sistema. Para obtener los datos y metadatos de sus búsquedas se apoya en otros SIGAD's.

La existencia del programa se reveló públicamente en julio de 2013[7] por Edward Snowden en los periódicos Sydney Morning Herald y O Globo. Es de nuevo operado por la NSA y

ha sido compartido con otras agencias de espionajes de países como Alemania, Australia o Nueva Zelanda.

XKeyscore es un sistema complicado y varios autores tienen diferentes interpretaciones acerca de sus capacidades reales. Edward Snowden y Glenn Greenwald explicaron XKeyscore como un sistema que permite una vigilancia casi ilimitada de cualquier persona en cualquier parte del mundo, mientras que la NSA dijo que el uso del sistema es limitado y restringido. De acuerdo al periódico The Washington Post y al reportero de seguridad nacional Marc Ambinder, XKeyscore es un sistema de recuperación de datos de la NSA, que consiste en una serie de interfaces de usuario, bases de datos back-end, servidores y software que selecciona ciertos tipos de datos y los metadatos que la NSA ya ha recopilado mediante otros métodos.

3.3.2 DATOS RECOGIDOS

Tal y como apuntábamos en el apartado anterior, XkeyScore no se encarga de la captura de los datos, así que en este apartado carece de sentido tratar de dilucidar como se obtienen los mismos sino que es mejor tratar de analizar las diferentes fuentes que que sirven datos a XkeyScore, y que aparecieron públicos en una diapositiva[8] publicada en Diciembre de 2013.

1. F6 (Servicio de Recolección Especial) - operación conjunta de la CIA y la NSA que lleva a cabo operaciones clandestinas, incluyendo el espionaje de diplomáticos y líderes extranjeros
2. FORNSAT - que significa colección de satélites extranjeros (Foreign Satellite Collection), y se refiere a las intersecciones de los satélites.
3. SSO (Special Source Operations) - una división de la NSA que colabora con los proveedores de telecomunicaciones.
4. Overhead - inteligencia derivada de aviones espías estadounidenses, aviones no tripulados y satélites.
5. Tailored Access Operations - una división de la NSA que se ocupa de la piratería y la guerra cibernética.

6. FISA - todos los tipos de vigilancia aprobados por el Tribunal de Vigilancia de Inteligencia Extranjera.
7. Terceras partes - los socios extranjeros de la NSA como las agencias de inteligencia de Bélgica, Dinamarca, Francia, Alemania, Italia, Japón, Países Bajos, Noruega, Suecia, etc.

3.3.3 FUNCIONAMIENTO

El funcionamiento de XkeyScore es bastante complejo, por una lado a diferencia de PRISM no podemos decir que se apoye en una base legal sólida que le aporte validez legal. Sin embargo, el aspecto que nos interesa aquí es el tecnológico.

Desde el punto de vista de la infraestructura, XkeyScore es un sistema distribuido formado por más de 500 servidores Linux distribuidos a lo largo del globo sobre los que se realizan consultas federadas. Esto significa que una única consulta es capaz de buscar sobre distintos recursos. Además se trata de un sistema escalable linealmente ya que solo hace falta añadir un nuevo nodo al cluster para aumentar las capacidades del mismo.

Como ya indicábamos, que se trate de un sistema de búsquedas federadas implica que una simple consulta provoque que se obtengan datos de todas las fuentes de información conectadas al sistema y que serán las mencionadas en el punto anterior. Como se puede observar, la cantidad de de información que se procesa es ingente y es por esto que XkeyStore puede operar de dos modos:

- Superficial: En el modo superficial, XkeyScore invierte poco tiempo en el procesamiento de los datos. Esto puede ser importante cuando queremos analizar datos con mayor rapidez o porque el flujo de datos de entrada que tenemos es demasiado grande.

- Profundo: Una de las desventajas del modo superficial es que utiliza selectores fuertes, esto es, ciertos valores clasificados como meta datos como pueden ser la dirección de correo electrónico o un número de teléfono. Sin embargo, la mayoría de acciones que se realizan en internet son anónimas por lo que se estaría desperdiciando gran cantidad de información. Haciendo un análisis profundo, se

pueden detectar anomalías que sean per se fuentes de inteligencia o lleven al hallazgo de algún tipo de selector fuerte que hubiese pasado desapercibido.

Además XkeyScore incorpora el concepto de plugins con lo que es posible indexar de manera sencilla cierta información. Los plugins existentes y su cometido quedan definidos en la siguiente tabla.

PLUGIN	**DESCRIPCIÓN**
Email	Indexa todos los emails encontrados en una sesión por nombre de usuario y dominio
Ficheros Extraídos	Indexa todos los ficheros encontrados en una sesión por el nombre del archivo y la extensión
Full Log	Indexa todos los DNI (Digital Network Intelligence) encontrados en la sesión.
HTTP Parser	Indexa el tráfico HTTP encontrado en la sesión (cliente)
Número de teléfono	Indexa todos los números de teléfono encontrados en la sesión
Actividad del usuario	Indexa el Webmail y la actividad del chat así como las cookies encontrada en una sesión

La capacidades que ofrece XkeyScore para los analistas son innumerables, no obstante en los documentos filtrados se exponen una serie de casos donde el uso de dicho programa muestra su potencial y que son:

- Búsquedas del uso de Google Maps y de los términos introducidos en el motor de búsqueda por parte del objetivo para detectar búsquedas o lugares sospechosos.
- Búsquedas de “anomalías” sin ninguna persona específica adjunta, como la detección de la nacionalidad de los extranjeros mediante el análisis del lenguaje utilizado en correos electrónicos interceptados. Un ejemplo sería detectar un alemán en Pakistán. El diario brasileño O Globo afirma que esto se ha aplicado a América Latina y específicamente en Colombia, Ecuador, México y Venezuela.

- Detectar posibles documentos valiosos. El uso de selectores débiles permite hacer búsquedas como “Documentos Excel que tengan una dirección MAC de origen en Irak”
- Detectar las personas que usan cifrado a través de búsquedas como "todo el uso de PGP en Irán". La advertencia que se da en las diapositivas filtradas es que amplias consultas pueden dar lugar a demasiados datos para transmitir de nuevo al analista.
- Mostrar el uso de redes privadas virtuales (VPN) y máquinas que pueden ser potencialmente hackeadas mediante TAO (Tailored Access Operations).
- Seguimiento de la fuente y la autoría de un documento que ha pasado por muchas manos.

La mayoría de estos comportamientos no pueden ser detectados por otras herramientas de la NSA ya que operan con selectores fuertes (como el correo electrónico y las direcciones IP y los números de teléfono) y que los volúmenes de datos en bruto son demasiado altos para transmitirlas a otras bases de datos de la NSA.

En 2008, se planeó para añadir una serie de nuevas capacidades tales como:

- VoIP
- Más protocolos de red
- Exif tags, que a menudo incluyen los datos de geolocalización (GPS).

3.3.4 FINALIDAD

De nuevo, si tratamos de discernir el propósito de Xkeyscore, podemos indicar que surge con la motivación de permitir a los analistas a buscar en los metadatos, así como el contenido de los correos electrónicos y otras actividades de Internet, tales como el historial del navegador, incluso cuando no hay ninguna cuenta de correo electrónico conocida (un "selector" en la jerga de la NSA) asociado con el individuo como objetivo.

En este punto estamos ya en disposición de observar las primeras diferencias que existen entre PRISM y XkeyScore. Más allá de que uno sea un programa de recolección y otro de

búsqueda, en PRISM se utilizan selectores fuertes que asocian la información a una entidad. Por contra, con XkeyScore se puede llegar a lograr a la identificación de un individuo sin la existencia de ningunos de estos selectores fuertes analizando lo que se conoce como huella digital y que es el rastro único, que dejan los individuos a su paso por la red.

3.3.5 REPERCUSIONES

Una de las repercusiones del uso de XkeyScore que quedan reflejadas en los documentos filtrados, fue el éxito en la captura de más de 300 terroristas en 2008[9] que indudablemente ha llevado a salvar vidas. En el plano social, su repercusión mediática fue inferior a la producida con la filtración de PRISM producida quizás por el mayor grado de desconocimiento de los objetivos y funcionamiento del programa.

3.4 MUSCULAR

3.4.1 INTRODUCCIÓN

No es de extrañar por qué la NSA se ha centrado en Google y Yahoo. En términos de tráfico de datos, son dos de las mayores empresas de Internet. El Big Data que usan y generan estas dos grandes compañías es un gran negocio y a medida que se crean más datos, se necesitan más lugares para almacenar y analizarlos. Dado su tamaño, Google y Yahoo tienen centros de datos repartidos por todo el mundo. Ambas compañías utilizan enlaces de comunicación propios para conectar sus centros de datos por medio de un proceso que se denomina georedundancia. Con ello se aseguran que sus clientes tengan acceso a sus datos en todo momento. Para ello, se requiere que una enorme cantidad de datos de los clientes serán enviados desde y hacia los diferentes centros de datos continuamente.

Desde Julio de 2009[10] la NSA ha logrado poner un topo en esa red conocido por el nombre DS-200B o MUSCULAR. Es un punto de acceso localizado fuera de Estados Unidos y que funciona gracias a un acceso secreto a un conmutador de red por el que pasa el tráfico de Google y Yahoo. El acceso lo da un proveedor de telecomunicaciones, de nombre desconocido.

Una vez que esos datos se capturan, se envían a un servidor buffer, con capacidad para almacenar de tres a cinco días de tráfico. Teniendo en cuenta que la red privada de Google

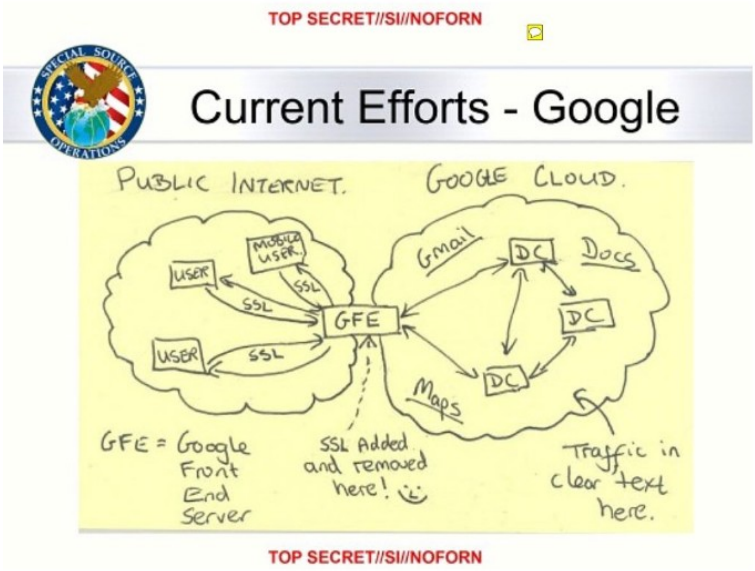
podría transmitir datos a una velocidad de incluso terabytes por segundo, estaríamos hablando de servidores de muy alta capacidad. Desde ese servidor buffer las herramientas de la NSA desempaquetarían y decodificarían los datos recogidos y después aplicarían filtros para quedarse sólo con la información interesante.

3.4.2 DATOS RECOGIDOS

Dado la particularidad del caso en el que estamos, podemos inferir aunque no queda explícito en los documentos filtrados, que la NSA es capaz de obtener toda la información que circula dentro de los servidores de la nube privada tanto de Yahoo como de Google. Esto incluye los datos de todos los usuarios que generen a través de sus servicios (email, chats, videos, archivos...)

3.4.3 FUNCIONAMIENTO

Tal y como muestra la figura 2, una vez la comunicación llega al GFE (Google Front End Server) el SSL es retirado y la información viaja en claro por la nube privada de Google.



Illustración 2: Muscular en los servidores de Google

De acuerdo con el documento filtrado la NSA envía millones de registros cada día desde las redes internas de Yahoo! y Google a los almacenes de datos de la agencia. El programa opera a través de un punto de acceso conocido como DS- 200B, que está fuera de los

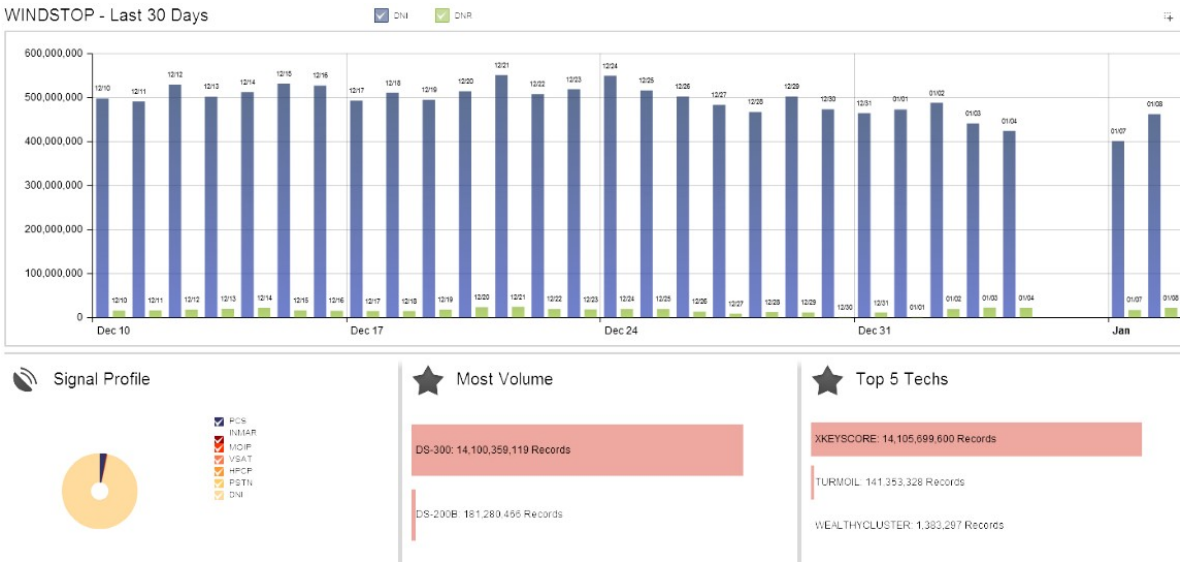
Estados Unidos, y que se basa en un operador de telecomunicaciones sin nombre para proporcionar un acceso secreto a la NSA y el GCHQ.

El programa MUSCULAR recupera más del doble de selectores en comparación con el más conocido PRISM. A diferencia de PRISM, el programa MUSCULAR no requiere de los mismos procesos de autorización como puede ser FISA.

Debido a la enorme cantidad de datos involucrados, MUSCULAR ha presentado un desafío especial para la Special Source Operations de la NSA. Por ejemplo, cuando Yahoo! decidió migrar una gran cantidad de buzones entre sus centros de datos, la base de datos de PINWALE de la NSA (su base de datos analítica principal para datos de Internet) fue rápidamente colapsada con los datos procedentes de MUSCULAR.

3.4.4 FINALIDAD

Muscular cobra sentido dentro de WINDSTOP, el programa de la NSA que engloba al menos cuatro sistemas de recogida de información y que dependen de países considerados aliados como pueden ser Gran Bretaña, Canadá, Australia o Nueva Zelanda. Su finalidad específica dentro de WINDSTOP es, como ya se indició anteriormente, entrar en las redes internas de Google y Yahoo. Sin embargo no es el único elemento que compone WindStop ni el que proporciona más selectores fuertes. Se conoce la existencia de al menos otro más denominado INCENSER operado por GCHQ[11] (Government Communications Headquarters) y la NSA bajo el nombre DS-300. La forma de operar de este proyecto es desconocida y así como los detalles sobre su funcionamiento. No obstante, pese a la carencia sobre los detalles específicos del mismo, en la siguiente ilustración, filtrada gracias a Edward Snowden, se puede comprobar como la mayoría del volumen es generado por INCENSER y no por MUSCULAR lo que nos puede dar una idea de la ingente cantidad de información que manejan.



Illustración 3: Compartiva de selectores producidos por Muscular DS-200B con Incenser DS-300

3.5. TEMPORA

3.5.1 INTRODUCCION

Al igual que la NSA el GCHQ dispone de sus programas de vigilancia propios, en los que también colabora la agencia estadounidense. De todos ellos, el más importante y conocido es Tempora. Se trata de un programa de vigilancia clandestina establecido en 2011[12] que intercepta los cables de fibra óptica que componen la troncal de internet para tener acceso a los datos personales de los usuarios de internet. A diferencia de otros programas no se precisa de ningún tipo de orden judicial para acceder sino que existen acuerdos con diversos proveedores de internet.

3.5.2 DATOS RECOGIDOS

Como se puede intuir los datos recogidos no tienen límites, el hecho de interceptar directamente los cables de información hace que el GCHQ disponga de todos los datos que circulan por los mismos independiente de a que persona, organización o servicio pertenezca. Uno de los grandes problemas a los que se enfrenta Tempora es el guardado de esa cantidad de datos. Según los documentos, hasta el momento es posible almacenar un total de 3 días de datos y hasta 30 días de metadatos.

3.5.3 FUNCIONAMIENTO

Según los mismos documentos, en la actualidad Tempora está conectado a 200 cables de fibra óptica y es capaz de procesar la información de 46 de ellos a la vez. Sabiendo que cada cable tiene como mínimo una capacidad de 10Gbps eso hace un total de aproximadamente 21 petabytes al día. Es evidente que no toda esta información será almacenada y mucho menos consultada. Según las propias fuentes, se disponen de “filtros” que ayudan a seleccionar que información visualizar y cual descartar directamente por no resultar provechosa. Además, se dispone de un método para la auditoría así que en todo momento puede consultarse los logs para comprobar que el acceso a cierta información por parte de un técnico estaba justificada.

La conexión con estos operadores de internet se ha hecho bajo estricto secreto y en ningún caso las mismas tenían la opción a negarse. Es evidente que tampoco pueden desvelar que la información de sus usuarios está siendo interceptada por el gobierno británico. Aunque en un principio la listas de estos operadores permaneció en secreto, revelaciones posteriores[13] han sacado a luz quienes son y el nombre en clave que reciben

- British Telecommunications (codename "Remedy")
- Interoute (codename "Streetcar")
- Level 3 (codename "Little")
- Global Crossing (codename "Pinnage")
- Verizon Business (codename "Dacron")
- Viatel (codename "Vitreous")
- Vodafone Cable (codename "Gerontic")

CAPÍTULO 4

4. 1 TABLAS COMPARATIVA

	PRISM	XKEYSCORE
Año de creación	2007	2008
Fecha filtración	Hecho público el 6 Junio 2013	Hecho público Julio 2013
País /Agencia	EE.UU/NSA	EE.UU/NSA
¿Quienes son los objetivos de la vigilancia?	Cualquier persona no americana.	Cualquier persona.
¿Que tipo de datos es recogido?	Datos y contenidos de comunicación en línea. Se incluyen email, vídeos, fotos, datos almacenados, transferencias de archivos,	No recolecta datos, pero utiliza diversas fuentes propias de la NSA como fuente de datos
¿Que compañías están involucradas?	Microsoft, Yahoo, Google, Facebook, PalTalk, Youtube, Skype,AOL, Apple	Ninguna compañía involucrada directamente
¿Como se recogen los datos?	Es supuesto que PRISM tiene de alguna forma acceso (directo o indirecto) a los datos de las compañías citadas	A través de las distintas fuentes, principalmente F6, FORNSAT y SSO
¿Como se usan los datos?	Son una de las fuentes principales para la creación de informes de inteligencia de la NSA	Creación de informes de inteligencia, detección de anomalías y tracking de objetivos.
¿Datos o Metadatos?	Datos	Trabaja con datos, pero pueden ser indexados en tablas de metadatos
¿Permite búsquedas?	Se trata de un programa que permite hacer búsquedas y consultar datos en tiempo real	La idea con la que parte XkeyScore es como plataforma unificada de búsquedas de la NSA

	MUSCULAR	TEMPORA
Año de creación	Julio 2009	2010
Fecha filtración	Hecho público Octubre 2013	Hecho público Junio 2013
País/Agencia	EE.UU/NSA RU/GCHQ	Reino Unido/GCHQ
¿Quienes son los objetivos de la vigilancia?	Tráfico interno de los servidores de Google y Yahoo!	Cualquier persona.
¿Que tipo de datos es recogido?	Selectores de los datos internos generados por los usuarios en estos dos proveedores de servicios	Cualquier tipo de datos y selector que atraviese los canales de los que está extrayendo información
¿Que compañías están involucradas?	Yahoo! Y Google	British Telecommunications Interoute Level 3 Global Crossing Verizon Business Viatel Vodafone Cable
¿Como se recogen los datos?	A través de un punto de acceso en los cables que conectan los centros de datos. Este punto de acceso es proporcionado por un servidor desconocido	El GCHQ tiene aproximadamente 200 puntos de acceso a los cables de red de las principales operadoras del Reino Unido
¿Como se usan los datos?	Generación de marcadores dentro del programa WINDSTOP	Creación de informes de inteligencia, detección de anomalías y tracking de objetivos.
¿Datos o Metadatos?	Datos y Metadatos almacenados de 3 a 5 días	Trabaja con datos y metadatos. Los datos tienen una vida de aproximadamente 3 días y los metadatos de 30
¿Permite búsquedas?	Permite búsquedas aunque no se sabe si en tiempo real	Permite en búsquedas en tiempo real durante el intervalo de tiempo que los datos están almacenados

CAPÍTULO 5

5.1 INTRODUCCIÓN

En el presente capítulo discutiremos sobre las diferentes herramientas y estrategias que pueden emplear los usuarios para evitar el control al que son sometidos por parte de los gobiernos. Cada una de las medidas presentadas en esta sección tendrá un objetivo específico y cubrirá desde la protección del usuario basada en aspectos puramente técnicos hasta otro nivel superior de abstracción como es el plano social. Es importante señalar que la aplicación de estas medidas no garantizará que nuestra privacidad no haya sido vulnerada, pero al menos supondrá una dificultad añadida para cualquier programa que trate de captar datos que hayamos generados en la red.

5.2 COMUNICACIONES ENCRIPTADAS

La primera forma que tenemos para protegernos es encriptar todo el tráfico que generamos. Esto quiere decir que cualquier tipo de conexión que hagamos desde nuestro dispositivo hacia internet nunca vaya en claro. Es cierto que organismos como la NSA tienen como objetivos comunicaciones cifradas y es bastante probable que dispongan de exploits que aprovechen vulnerabilidades en las implementaciones de los protocolos de cifrado de las comunicaciones. Sin embargo, siempre es mejor cifrar nuestros datos. Dos grandes protocolos para llevar a cabo esta tarea son TSL/SSL e IPsec

- Transport Layer Security (TLS - RFC 2246) se basa en SSLv3. Se trata de un protocolo de Capa 4 que se ejecuta directamente sobre TCP. Utiliza PKI para proporcionar la autenticación de usuario, así como la manipulación de las claves simétricas necesarias para permitir confidencialidad. Está diseñado para prevenir el espionaje, manipulación y falsificación de mensajes. TLS se puede utilizar en dos métodos que son la *autenticación mutua* y la *autenticación por parte del servidor*. En el primer caso, ambas partes tienen que disponer de sus certificados verificados tal y como se recoge en una infraestructura PKI con objeto de realizar una conexión. Por el contrario, en el modo de servidor, éste es el único elemento que interviene en la sesión, que ha de disponer de dicho certificado. Es el caso más típico y lo podemos encontrar en todos los navegadores web cuando accedemos a través del

protocolo HTTPS.

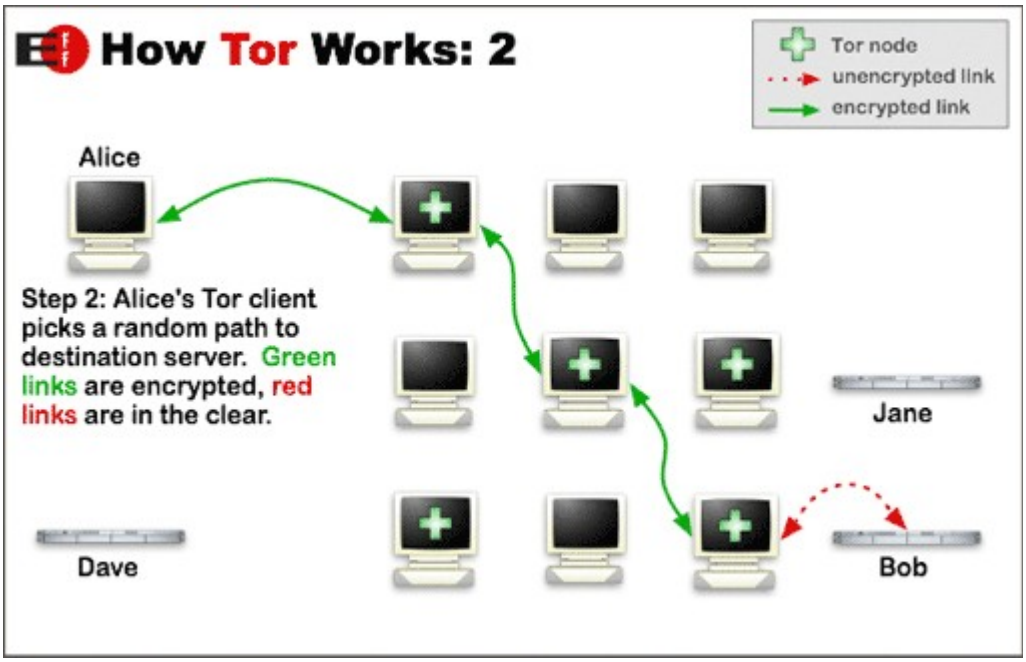
Una de las grandes ventajas de TSL/SSL es que no existe la necesidad de realizar una configuración para utilizarlo. Su uso en navegadores web no requiere instalar ningún software adicional. Por lo tanto, la facilidad de uso unido con el poco mantenimiento requerido es lo que hace TLS / SSL una opción muy popular. El cuello de botella real con TLS / SSL son los requisitos para cumplir PKI. Aunque usemos TSL en su forma más simple (servidor) requerimos en el cliente ciertas características como son el manejo de certificados y la validación de los mismos que hacen que se obtenga un entorno complejo. Por otra parte, el uso de criptografía de clave pública del que hace uso PKI hace que hablemos de un protocolo que requiera altos requisitos computacionales.

- *IPsec* (RFC 2401, 2406, 2409, 2411); es un conjunto de protocolos que se ejecuta en la capa de red (Capa 3). Proporciona confidencialidad, integridad, autenticación del origen de datos y la protección contra la reproducción de cada mensaje mediante el cifrado y la firma de los mismos. IPsec es una combinación de muchos RFCs y define dos protocolos principales para utilizar: *Authentication Header* (AH) y Encapsulating Security Payload (ESP). ESP es la opción preferida, ya que proporciona la autenticación y confidencialidad, mientras que AH no proporciona confidencialidad. Las Asociaciones de Seguridad IPsec (SA) entre dos puntos finales,se establecen de forma dinámica a través de un protocolo de gestión de claves. Esto se hace normalmente a través de protocolos como IKEv1/IKEv2 o IMS-AKA.

  Las grandes ventajas que tiene IPsec es que nos evita el uso de una PKI. A su vez, el hecho de que esté en la capa 3 de red, hace que protejamos cualquier protocolo o aplicación que esté sobre esta capa. Por contra, a diferencia de TSL/SSL su configuración es más compleja y suele tener problemas con los routers que hacen NAT ya que no tiene acceso a los puertos de la capa 4 debido a que están encapsulados como el payload de la capa 3.

5.3 OCULTAMIENTO

Como vimos en el apartado anterior, encriptar las comunicaciones es una buena idea, pero puede ser que en ocasiones requiramos ir un paso más allá y ocultar nuestra presencia en la red para no poder ser rastreados y garantizar nuestro anonimato. Es aquí donde proyectos como Tor cobran sentido. En una conexión común cuando un usuario se conecta a un sitio web, el dispositivo intenta conectarse directamente a esa máquina por la ruta más directa. Es una cuestión de eficiencia y de velocidad. En este escenario, nuestra red con nuestra IP pública, consta como punto de origen de las comunicaciones con lo que será posible desde el servicio rastrearnos. La idea con la que parte Tor es romper esa línea entre el origen y el servidor remoto. La conexión va pasando por una serie de nodos secretos que cifran los datos que se envían y se reciben y solo al llegar al último de estos, es cuando se descifran y se envían al destino con lo que este último será capaz de responder correctamente a la petición de origen.



Illustración 4: Esquema de funcionamiento de la red Tor

Es importante señalar que el recorrido a través de los nodos que se hace hasta conectar con un servidor es creado de manera aleatoria para cada usuario. De esta forma conseguimos no poder tener la certeza de quien es el usuario que está enviando su información por una serie

de nodos determinados. Por otra parte, y aunque es un hecho ampliamente confundido, es importante señalar que Tor en ningún caso proporciona confidencialidad, únicamente anonimato. Este aspecto se entiende mejor observando la ilustración que acompaña a esta sección y al hecho de que la comunicación entre el último nodo y “Bob” se realiza sin cifrar. Un atacante que interceptara esta comunicación sería capaz de observar todo el contenido que hemos transmitido perdiéndose así la propiedad de la confidencialidad de la que hablábamos aunque nuestro anonimato si que seguiría existiendo. Es recomendado que cuando trabajamos con Tor no utilicemos ningún plugin o extensión en nuestro navegador y que desactivemos Javascript ya que pueden producir conexiones ante terceros con las que se nos pueda identificar y perder así el anonimato.

5.4 DATOS ENCRIPTADOS

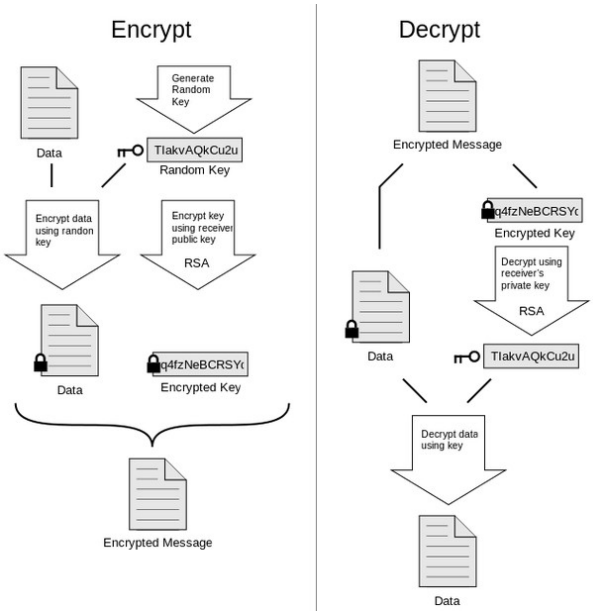
Ya hemos hablado de la importancia de mantener las comunicaciones encriptadas. Parece lógico pensar que es necesario trasladar ese concepto de las comunicaciones a los ficheros locales que tengamos almacenados. Nunca debemos olvidar que nuestro sistema no es solo vulnerable mientras enviamos o recibimos información sino que las diversas agencias de inteligencia (al igual que piratas informáticos) disponen de los conocimientos y las herramientas para acceder a nuestros dispositivos. Existen en el mercado diversas herramientas que permiten el cifrado de los mismos. No es objeto del presente trabajo hacer un análisis exhaustivo sobre todas la que existen. Existirán muchos factores que influyan en la elección de la misma, como puede ser el sistema operativo, si se encarga de cifrar todo el sistema operativo o solo unos ficheros específicos o si el descifrado de hace bajo demanda o al arrancar el equipo.

La única pauta a seguir que damos es que intentemos que el sistema de cifrado sea de dominio público. Por ejemplo, es más difícil para la NSA colocar una puerta trasera a TLS (dominio público) que a BitLocker, ya que el TLS que implemente programa de cifrado tiene que ser equivalente al que implemente otro programa, mientras BitLocker sólo tiene que ser compatible consigo mismo, dando a la NSA mucha más libertad para hacer cambios. El hecho de que un código sea propietario y no conocido hace que las posibilidades de detectar estas modificaciones en el código en forma de puertas traseras sean mucho más difíciles.

5.5 CORREO CIFRADO

Al igual que hemos hablado de cifrar las comunicaciones y los archivos, hemos de hacer lo propio con los correo que enviemos. Una de las formas más extendida para llevar a cabo el cifrado de los mismos es el uso del programa conocido como PGP o Pretty Good Privacy. Se trata de, un programa desarrollado por Phil Zimmermann que sirve para cifrar contenido y acceder a él mediante una clave pública y firmar documentos digitalmente para autentificarlos. El programa vio la luz en 1991, y desde entonces se ha convertido en una herramienta imprescindible para el cifrado de toda clase de archivos, ya que a pesar de sus más de 20 años de vida, sigue siendo una tecnología de cifrado muy segura. En la actualidad, la tecnología es propiedad de Symantec, pero está disponible a través de una gran cantidad de programas distintos para diferentes plataformas. Además, existe una versión de código abierto cuyo principal representante es la aplicación GnuPG.

El funcionamiento es bastante sencillo y utiliza un esquema híbrido de clave simétrica y clave asimétrica. El proceso de cifrado comienza con la compresión del texto a cifrar y con la creación de una clave de sesión aleatoria única para ese mensaje. Se cifra el texto con esa clave y la clave de sesión generada con la clave pública del destinatario del mensaje. Se envía el mensaje cifrado y la clave de sesión cifrada. Ya en el destino, se procede a obtener la clave de sesión aplicándole la clave privada y una vez obtenida, se descifra el mensaje con la misma.



5.6 MEDIDAS SOCIALES

La medidas explicadas hasta ahora incluían en mayor o menor grado que los usuarios llevaran a cabo algún tipo de solución técnica para protegerse ante la acción de los gobiernos a través de los programas de vigilancia. Existen muchas otras medidas de carácter social que se pueden llevar a cabo para evitar que se recopilen datos sobre los ciudadanos y que pasaremos a estudiar en el presente apartado

5.6.1 NO UTILIZAR SERVICIOS EN LA NUBE

Últimamente los servicios de almacenamiento de fotos, videos y documentos en la nube han aumentado su popularidad. Prácticamente todas las grandes empresas disponen de alguna de estas herramientas, si no todas, como son el caso de Google, con Google Docs u Youtube, o Yahoo! Con Flickr. Proyectos como **Muscular** han dejado claro que los gobiernos están interesados en la información que estas compañías poseen sobre los ciudadanos. Ya sea accediendo directamente a la los servidores de estas grandes empresas o a través de algún ISP lo cierto es que es innegable que se está produciendo el acceso a esta información. La solución a esta problemática pasa por mantener los datos en nuestros propios servidores y centros de datos, o en nuestra propia nube privada manteniendo siempre el tráfico en una intranet corporativa o local. Además, hay que tener siempre en cuenta que si utilizamos los SaaS que ofrecen estas compañías (Office 365, Gmail …) es probable que el trabajo o actividad que estemos realizando sea potencialmente visible a los ojos de terceros.

5.6.2 EVITAR SERVICIOS DE IM

Cuando se envía un mensaje a través de una aplicación de mensajería instantánea, suele pensarse erróneamente que el mensaje se dirige directamente al destinatario. Esto no curre así. Por lo general, lo que ocurre es que se envía primero a un servidor, donde se guarda una copia, y luego es enviado al destinatario. Esta copia que queda almacenada en los servidores de la compañía que provee de los servicios supone un peligro para nuestra privacidad. Para solventar este problema, se debería evitar el uso de cualquier servicio de mensajería instantánea pública, tales como, Skype, Google Hangouts o Facebook Messenger. En su lugar se debería ejecutar un servicio propio de mensajería instantánea a

través del protocolo XMPP (Extensible Messaging and Presence Protocol). Hay que tener en cuenta sin embargo que aunque utilicemos un servicio de IM propio, si el destinatario del IM pertenece a una red de IM XMPP externa compatible, como puede ser Google Hangouts, los mensajes terminarán siendo mantenidos en un servidor de terceros de todos modos.

5.6.3 NO UTILIZAR REDES SOCIALES

Una de las conclusiones que quedaron claras tras las divulgación de los documentos secretos de la NSA por parte de Edward Snowden es que la agencia era capaz de obtener información de objetivos a través de su actividad en la red social Facebook. Hoy en día el uso de las redes sociales está muy extendido y la información disponible sobre las personas que se puede encontrar en las mismas es abrumadora. No es de extrañar que los organismos de inteligencia de los diferentes países hayan visto en la misma una fuente de información precisa que es importante explotar. La mejor técnica para prevenir que se recolecten datos nuestros a través de este medio es dejar de utilizar dichas redes.

CAPÍTULO 6

6.1 CONCLUSIONES

Tras la realización de este trabajo, hemos sido conscientes de la verdadera problemática tras los programas de vigilancia de los gobiernos. Su uso está más extendido de lo que la sociedad es consciente y nos queda realmente claro que la información de los programas que aún no han salido a la luz es superior a lo poco que se conoce.

Una de las grandes dificultades con las que nos hemos topado al realizar este trabajo, es la gran falta de información existente en relación a los mismos. Aunque es conocido que Edward Snowden sustrajo gran cantidad de información de la NSA, solo una pequeña parte ha sido publicada. Solo se encuentra accesible a través de la red, diapositivas internas descriptivas de los programas de vigilancia en la que parte de la información está oculta por motivos operativos de las agencias (los datos ocultos tratan sobre operativos reales de la NSA).

Por otra parte, el hecho de que los gobiernos intervengan las comunicaciones de sus ciudadanos y de otros países supera el aspecto de la legalidad y toca de lleno en el aspecto moral de las acciones realizadas por los mismos. Hasta que punto es lícito moralmente acceder de forma indiscriminada a la información privada de los individuos en aras de una seguridad absoluta no queda a nuestro entender justificado.

Ante tal atropello de la privacidad individual y por ende de los derechos y libertades de las que se presuponen al individuo, los ciudadanos pueden y deben tomar medidas al respecto. Aunque somos conscientes de que las medidas planteadas en el presente documento son capaces de impedir que dicha recolección de información se produzca en su totalidad, si que conseguiremos que la efectividad que los gobiernos alcance a través de ella se vea reducida.

[1] http://en.wikipedia.org/wiki/Clifford_Cocks

[1] The Guardian 6 Junio 2013 http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

[2] The Washingnton Post 6 Junio 2013 http://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

[3] La corte para la vigilancia de la inteligencia extranjera o por sus siglas en inglés FISC es quien aprueba las peticiones que solicitan recoger datos de los ciudadanos.

[4] Foreign Intelligence Suerveillance Act. Ley que ha sido aprobada por el congreso de los Estados Unidos para proveer a la comunidad de inteligencia del citado país, con mayores poderes de vigilancia a partir del 11/9. El es documento que hace posible la existencia legal de PRISM

[5] http://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document – página 5

[6] SIGAD son las colecciones de plataformas con las que cuenta las agencias de inteligencias estadounidenses para obtener y analizar datos de inteligencia de diversos orígenes

[7] Diapositivas sobre XkeyScore http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation

[8] Diapositiva con las fuentes de datos de XkeyScore http://www.freesnowden.is/wp-content/uploads/2013/12/xkeyscore-sources-dated-2008.pdf

[9] http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

[10] http://en.wikipedia.org/wiki/File:NSA-MUSCULAR-p22.png

[11] Government Communications Headquarters http://www.gchq.gov.uk/

[12] http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

[13] Listado de las operadoras británicas que operan en Tempora http://www.theguardian.com/business/2013/aug/02/telecoms-bt-vodafone-cables-gchq