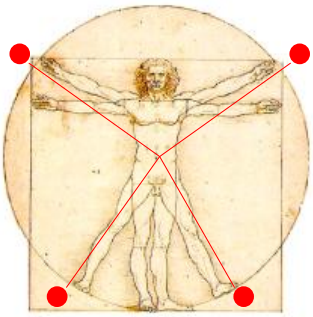
TECNOLOGÍ@ y *DESARROLLO*

Revista de Ciencia, Tecnología y Medio Ambiente

VOLUMEN XV. AÑO 2017

SEPARATA



LA PRIVACIDAD EN LA SOCIEDAD DE LA INFORMACIÓN

Pablo Casais Solano y Antonio J. Reinoso

UNIVERSIDAD ALFONSO X EL SABIO
Escuela Politécnica Superior
Villanueva de la Cañada (Madrid)

Escuela Politécnica Superior.
Universidad Alfonso X el Sabio.
28691, Villanueva de la Cañada (Madrid).
ISSN: 1696-8085
Editor: Javier Morales Pérez – tecnologia@uax.es

LA PRIVACIDAD EN LA SOCIEDAD DE LA INFORMACIÓN

Pablo Casais Solano[a] y Antonio J. Reinoso[b]

[a)] Máster en Ingeniería Informática,
79 Great Arthur House, Golden Lane Estate, EC1Y 0RQ, Londres (RU).
pcasais@ieee.org

[b)]Doctor Ingeniero en Informática
Adjunto a la Jefatura de Estudios
Departamento de Ingenierías TIC, Escuela Politécnica Superior, Universidad Alfonso X el Sabio.
Avda. De la Universidad nº1, Villanueva de la Cañada, 28691, Madrid. España.
areinpei@myuax.com

RESUMEN: A lo largo de la historia podemos observar un cambio en la consideración de la privacidad que se ha acelerado en nuestros días. Con el uso masivo de las tecnologías de la información los ciudadanos han ganado en comodidad y capacidad de comunicación. Sin embargo la acumulación de datos sensibles en sistemas ajenos ha hecho que surjan nuevas amenazas a la vida privada de los individuos. El objetivo de este artículo es analizar las amenazas a las que los ciudadanos se encuentran sometidos y evaluar qué mecanismos se encuentran disponibles para que un usuario pueda recuperar la privacidad de sus datos renunciando en lo mínimo posible a las comodidades que ofrecen los servicios digitales.

Palabras-clave: Amenazas a la privacidad, Tecnologías de la Información, Espionaje Gubernamental, Espionaje Corporativo, Perfilado de clientes, Cibercrimen.

Abstract*: Along history we can observe a change regarding privacy which has accelerated in the last years. With the massive use of information technologies citizens won in comfort and communication possibilities. However by accumulating sensible data in systems outside their control has created new threats to the private life of individuals. The objective of this article is to analyse the threats to citizens and evaluate the mechanism that are available to help users recover their data giving as little as possible on the comforts offered by digital services.*

Keywords*: Privacy Threats, Information Technologies, Government Espionage, Corporate Snooping, Client profiling, Cybercrime*

El único sistema seguro es aquel que está apagado en el interior de un bloque de hormigón protegido en una habitación sellada rodeada por guardias armados
Gene Spafford.

1. Introducción

La privacidad es uno de los derechos básicos de los seres humanos tal como recoge la Declaración Universal de Derechos Humanos de las Naciones Unidas en sus artículos 12 y 19 (Asamblea General de las Naciones Unidas, 1948) así como en el artículo 18 de la Constitución Española (Cortes Generales, 1978). Su importancia es tal que algunos autores llegan a decir que "la persona que pierde su intimidad, lo pierde todo" (Kundera, 1985). Sin embargo lejos de lo que podríamos pensar el concepto de privacidad no es algo estático sino que ha ido evolucionando a lo largo del tiempo. El historiador Manuel García Morente en su libro Idea de la Hispanidad (García Morente, 2008) realiza un interesante recorrido desde la Edad Media, donde las relaciones privadas y los privilegios son la norma, a las sociedades actuales donde los privilegios han sido abolidos y la esfera pública domina las relaciones entre individuos.

Este proceso de "publificación" (tal como lo define García Morente) implica que ciertas relaciones anteriormente íntimas pasan a ser consideradas públicas. El objetivo inicial de este proceso es lograr que los ciudadanos puedan actuar en igualdad tanto en sus relaciones con otros ciudadanos como con la autoridad. Los ciudadanos pasan a representar diferentes roles (cliente, vendedor, funcionario, solicitante, etc.) según la situación en la que se encuentren. Estos roles tratan de ayudar al ciudadano despojándole de sus características privadas dándole un barniz de igualdad.

Sin embargo para que las relaciones entre individuos sean eficaces es necesario no sólo que ambos se reconozcan en sus roles sino que tengan cierta información del otro. Por ejemplo en el caso del vendedor para lograr una relación más eficaz es necesario que posea cierta información acerca de los gustos o intereses del cliente para así poder atenderle mejor. Este proceso es lo que denominamos como "personalización de los roles" o "creación de perfiles" y en él uno de los participantes de la relación trata de convencer al otro para que le dé información personal a fin de poder proveerle un servicio más eficaz. Este proceso que se da de forma habitual en las relaciones entre personas (ejemplo de ello son los casos en los que un comerciante después de ciertas compras nos recuerda y nos ofrece directamente el producto que solemos comprar) se industrializa al aplicar los métodos de procesado masivo de datos que ofrecen las tecnologías de la información.

2. Revisión del Estado del Arte.

Una vez presentado el proceso de "personalización de los roles" que se encuentra en marcha actualmente es importante hacer una revisión del Estado del Arte en materia de las amenazas que conlleva este proceso para la privacidad de los ciudadanos. Para empezar, se considera adecuado mencionar que desde un punto de vista puramente técnico a mayor exposición siempre existe un mayor nivel de riesgo. Esta regla que se

utiliza en el campo de la seguridad informática para medir la exposición de un sistema y su superficie de ataque es aplicable igualmente a los datos privados de un usuario que son almacenados en distintos sistemas. El almacenaje de información personal o sensible en sistemas sobre los cuales no se tiene total control supone un incremento del riesgo de que dicha información sea usada en contra de nuestros intereses o robada por delincuentes o gobiernos. Para poder entender mejor el riesgo que supone el mal uso de esta información se analizará el uso que pueden hacer de ella cada uno de estos actores.

2.1. Amenazas del mundo corporativo

El primer actor a analizar son las empresas que ofrecen servicios "gratuitos" en la red. Estas empresas que son las que hoy en día tienen una mayor cuota de mercado en sus sectores suelen tener un modelo de negocio basado en la publicidad. En dicho modelo de negocio el usuario recibe un servicio libre de pago a cambio de aceptar una cierta cantidad de publicidad en dicho servicio. En este modelo de negocio son los anunciantes los que pagan por poder mostrar su publicidad y son los verdaderos clientes del servicio digital. Los usuarios por su parte son el producto que la compañía que ofrece el servicio vende a sus clientes.

En este modelo de negocio la rentabilidad del mismo se mide según el número de visitas o compras realizadas por número de impresiones de la publicidad. Aquellos servicios que logran atraer a sus usuarios a la publicidad mostrada en mayor medida son pues más eficaces y logran un mejor retorno de la inversión para sus clientes. El problema por tanto para los proveedores de servicios es cómo lograr saber qué publicidad deben mostrar a sus usuarios que les pueda resultar interesante. Para resolver dicho problema las empresas tratan de crear perfiles de sus usuarios acumulando datos personales de los mismos a fin de entender cuáles son sus gustos y tendencias.

Estos perfiles digitales inicialmente se almacenaban en forma de "cookies" en el ordenador del cliente y servían para guardar las preferencias del usuario. Sin embargo este mecanismo ofrece poco control a las empresas ya que el usuario puede en cualquier momento borrar o modificar las "cookies". Es por ello que, como muestra el investigador Alejandro Ramos (Ramos, 2014), actualmente las empresas usan técnicas basadas en identificación del navegador o HTTP Etags para identificar a sus usuarios sin necesidad de almacenar cookies en su equipo. Con este proceso además logran poder realizar un seguimiento completo de la actividad de los usuarios aunque no hayan iniciado sesión o se hayan identificado. Esta actitud de tratar de controlar la actividad de los usuarios todo el tiempo es una de las primeras amenazas a la privacidad de los usuarios en la red.

Pero la amenaza a los usuarios no se detiene en el rastreo de toda su actividad. Empresas como Facebook han dado un paso más al empezar a experimentar con sus usuarios. Una

vez que poseen perfiles sobre los usuarios el siguiente movimiento ha sido tratar de modificar la información que estos ven para tratar de producir diferentes respuestas en ellos. En un estudio, realizado sin el consentimiento de sus usuarios, Facebook trató de alterar su estado anímico mediante el filtrado de las publicaciones en su muro (Gorski, 2014). El objetivo de estas manipulaciones es intentar conseguir que el usuario se comporte de acuerdo a las intenciones del prestador de servicios.

2.2. Amenazas gubernamentales

El otro agente que supone una amenaza para la privacidad son los propios gobiernos. En 1971 los países llamados Five Eyes (EE.UU., Canadá, Reino Unido, Australia y Nueva Zelanda) crean la red de espionaje global ECHELON a raíz de la firma del acuerdo UKUSA Security Agreement (National Security Agency, 2010). Dicha red como podemos ver en la Ilustración 1 tiene un alcance mundial y su objetivo era el espionaje de los países del bloque comunista.

Figura 2.1 Estaciones de escucha de los Five Eyes

Una vez terminada la guerra fría en vez de reducir o cerrar esta red de espionaje los Five Eyes proceden a incrementar su capacidad dándole otros usos como el de espionaje industrial. Dos casos públicamente documentados de espionaje a la gran industria europea produjeron en 1994 pérdidas de 6.000 millones de dólares a Airbus (Evans & Leigh, 2003) (Asser, 2000) y de 1.300 millones de dólares a Thomson-Alcatel (Epstein, 1996). En España la red ECHELON espió al ingeniero José Ignacio López de Arriortúa que trabajaba para Volkswagen y la información recabada fue puesta a disposición de su competidor americano General Motors (del Moral, 2001).

Mientras que ECHELON se utilizaba con fines industriales y militares en el mundo civil también han surgido por su parte redes de espionaje. En los Estados Unidos a principios de los años 90 el FBI estadounidense se dotó de su primera generación de software de análisis de la información, un programa comercial llamado Etherpeek (Sanders). Dicho software permite la monitorización y captura de tráfico de red y es capaz de decodificar más de 1.000 protocolos de red en tiempo real. El programa permite la creación de filtros y alarmas que avisan de eventos que suceden en la red, todo esto a través de una interfaz gráfica muy sencilla que permite la creación y edición de filtros gráficamente. Esta potente herramienta junto con el acceso a la red ECHELON fue el primer paso en el ambicioso programa de espionaje civil global de los Five Eyes.

Después del éxito en el despliegue de Etherpeek, el FBI decide aumentar su capacidad de análisis. Para ello empiezan un programa llamado Omnivore que ofrece la capacidad de interceptar correos electrónicos de un individuo. En 1997 crea un conjunto de herramientas llamadas DragonWare para el espionaje digital. Entre las herramientas que forman parte de este paquete se encuentra una evolución de Omnivore llamada Carnivore (Electronic Privacy Information Center, 2005). Este programa se instala en los ISP (Proveedores de Servicio de Internet) y permite la interceptación no sólo de emails sino de todo el tráfico de red de un usuario. El uso de evidencias recogidas mediante DragonWare y Carnivore empiezan a atraer sobre sí gran atención por parte de los grupos en defensa de la privacidad de los individuos por el potencial de violación de la privacidad y el secretismo con el que estos programas son ejecutados. Ante las quejas por las posibles violaciones de la privacidad, la libertad de expresión y los temores a una posible regulación de Internet el FBI decide realizar una serie de comparecencias en las que aclara el control judicial sobre el mismo. Además para intentar darle un perfil más suave se renombra el programa a DCS1000 (Associated Press, 2005).

El éxito de los programas de espionaje de los Five Eyes hizo que otros países se interesasen por alcanzar el mismo nivel de capacidad de interceptación. En 1995, 20 años después de que la red ECHELON fuese creada, Europa decide crear su propio sistema llamado ENFOPOL (Quirantes Sierra, 2002) (Molist & Collado, 1999). Dicho programa permanece aún hoy en día mayormente secreto y sus capacidades son mayormente desconocidas. Por su parte en España, en 2001 durante la presidencia de José María Aznar se encarga el desarrollo de un programa llamado SITEL (Ministerio del Interior, 2007) (Sistema de Interceptación Legal de las Telecomunicaciones). Dicho programa permite el acceso a las comunicaciones entre individuos mediante una interfaz que todos los proveedores de telefonía y servicios digitales en España deben proveer. El programa es entregado tras dos retrasos el 30 de Noviembre de 2003. A pesar de que el programa fue desarrollado durante el mandato de J.M. Aznar el Gobierno niega haberlo usado hasta la presidencia de José Luis Rodríguez Zapatero debido a la falta de un marco legal que diese cobertura a las escuchas (Cervera, 2009).

Volviendo al ámbito internacional mientras el resto de países desarrollaban sus capacidades de interceptación los Five Eyes implementaron el mayor programa de espionaje y monitorización mundial, PRISM. En Junio de 2013 sale a la luz su existencia gracias a las revelaciones de un consultor de la CIA llamado Edward Snowden. Este programa desarrollado y empleado por los Five Eyes va un paso más allá de la mera interceptación al conseguir acceso directo a las bases de datos y al tráfico de los principales servicios de Internet. Gigantes como Google, Microsoft, Apple, Facebook o Yahoo! proveyeron acceso directo a los datos de sus usuarios a los Five Eyes. Pero este programa no se limita al espionaje de los servicios de red social u otros servicios sino que también espía a diferentes compañías y líderes mundiales.

Para entender el alcance de la red espionaje desplegada por Five Eyes podemos ver el siguiente gráfico filtrado por Edward Snowden. En él se muestra la extensa red de espionaje de los Five Eyes en el mundo.

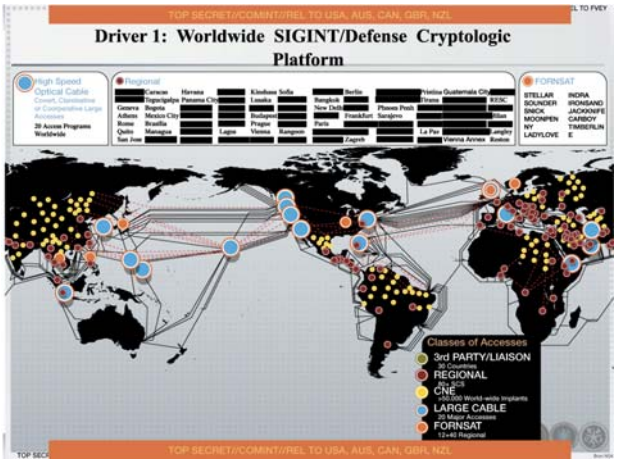


Figura 2.2 Red de señales de los Five Eyes

Esta red masiva de espionaje se extiende hasta extremos increíbles. Recientemente se ha revelado que los servicios de espionaje del Reino Unido espiaron a 1.8 millones de usuarios a través del programa de Yahoo! para webcams (Ackerman & Ball, 2014) Este espionaje masivo ha producido una evidente violación de la privacidad de los usuarios. Tal como indican los informes publicados los analistas de información tuvieron acceso a información sensible incluyendo imágenes sexuales explícitas de los usuarios espiados.

Gracias a Edward Snowden y Chelsea Manning sabemos que hoy en día mediante los programas PRISM, Upstream, FASCIA y la recogida de metadatos de teléfonos móviles los Five Eyes realizan tareas de espionaje masivas de los ciudadanos a nivel mundial (ProPublica, 2014). Los gobiernos de los Five Eyes tratan de justificar este espionaje como un elemento necesario para poder garantizar la seguridad de sus ciudadanos. Sin

embargo el hecho de que el GCHQ británico estuviese espiando y fotografiando a ciudadanos en la intimidad de sus casas a través de sus cámaras web nos da un ejemplo de la gran amenaza que suponen para la privacidad.

2.3. Amenazas de delincuentes

El tercer agente que supone una amenaza para la privacidad de los ciudadanos son los delincuentes informáticos. Dado que las empresas están cada vez guardando una mayor cantidad de datos de los usuarios para sus procesos de negocio se crea un efecto llamada sobre los delincuentes que quieren obtener acceso a dicha información. El robo de información sensible es un negocio gigantesco, según un informe de McAffee las pérdidas provocadas por los cibercrímenes en 2013 estarían entre 375 y 575 miles de millones dólares (Pemper, 2014). En función de la motivación del daño que se pretende infligir y el destinatario del mismo se pueden clasificar las amenazas en dos tipos:

El primer tipo de ataques son las denegaciones de servicio (DoS o DDoS cuando son distribuidas). El objetivo de este tipo de ataques es lograr saturar los servidores de la víctima de forma que sean incapaces de responder a peticiones de los usuarios. Esta técnica ha sido usado en 2013 con diversos fines: desde ataques a países como el ataque sufrido por Colombia en el día de la Independencia a raíz de su reforma educativa (Hassan, 2011), a simples litigios entre compañías como fue el ataque realizado por CyberBunker contra Spamhaus que llego a ralentizar Internet a nivel mundial debido al nivel de tráfico generado (Jenkins, 2013).

El segundo tipo de ataques son los actos de cibercrimen, ciberguerra o ciberespionaje. Los atacantes se dividen entre ciberdelicuentes cuyo objetivo es el robo de información para su posterior venta; y los conocidos como APT (Advanced Persistent Threats) o Amenazas Persistentes Avanzadas que realizan actos de ciberespionaje o ciberguerra. En el caso de los APT Sus miembros tienen objetivos específicos en compañías o agencias gubernamentales y su objetivo es la infiltración con el fin de conseguir una “cabeza de playa” desde la cual poder después llevar a cabo sus actividades. Dichas actividades pueden ser desde espionaje, robo de documentos sensibles o sabotaje.

2.3.1. Ataques de denegación de servicio

Los ataques de DDoS empezaron organizándose con herramientas colaborativas tipo Loic que permitían sincronizar las peticiones de múltiples ordenadores para tratar de saturar los servidores. De ahí se pasó al uso de Botnets que son alquiladas o dirigidas para lanzar cantidades de peticiones masivas desde ordenadores comerciales. Por último es importante detallar el uso de amplificadores en este tipo de ataques. En ciertos protocolos bien por fallos de diseño o por errores de configuración se pueden realizar solicitudes en nombre de otros y lograr que el servicio devuelva la respuesta a la

víctima. Si las respuestas son muy superiores en número al número de consultas se utiliza estos errores para amplificar el tráfico que soporta la víctima.

En comparativa con el año 2012 en 2013 tenemos:

- El BPS de los ataques ha crecido pasando los ataques mayores de 1 Gb/s de un 33.1% a un 53.9 %.
- El ataque medio ha crecido en tamaño un 78% sin embargo el número de paquetes se ha reducido en un 34% lo que indica un menor número de participantes.
- Grandes incrementos en los mayores segmentos de los ataques pasando los ataques mayores de 10 Gb/s de un 2.3% a un 4.06 %, los mayores de 20 Gb/s se han multiplicado por 4.5 veces y los de 2 a 10 Gb/s han pasado de un 14.78% a un 37.13 %.
- El mayor ataque jamás registrado alcanzó los 191 Gb/s con un pico de 300 Gb/s.
- La duración de los ataques se está reduciendo: el 87.5% de los ataques duran menos de 1 hora.

A continuación en la Ilustración 3 podemos ver cómo ha variado el reparto de los DDoS acorde a su tamaño en los últimos tres años.

Figura 2.3 Distribución de ataques DDoS por tamaño

Los ataques de DoS o DDoS gran proporción de ellos es lo que hemos denominado hacktivismo. Durante 2013 el grupo Anonymous solicitó que se considerasen los DDoS como una forma de protesta legítima dentro del derecho de manifestación y de reunión (Kersey, 2013) adaptado al mundo digital. La diferencia es que mientras los perjuicios provocados por las protestas físicas tienen un alcance limitado no sucede lo mismo con la “protesta digital”. Según estudios realizados por proveedores de servicios como Akamai un 60% de los servicios atacados sufren una degradación en los mismos. Dicha degradación puede afectar a sus usuarios y provocar pérdida al optar estos por servicios

alternativos. También en un 27% de los casos directamente el servicio deja de funcionar con los mismos efectos para los usuarios. Es por tanto el DDoS un ataque que puede provocar considerables pérdidas a un servicio web.

2.3.2. Cibercrímenes

Como se mencionó anteriormente la otra fuente de ataques sucedidos son los denominados cibercrímenes. Este tipo de actos suponen casi el 50% de los ataques de 2013. En su mayoría este tipo de ataques están enfocados al robo de información de usuarios del servicio. En la Ilustración 4 se pueden ver los mayores robos de información que se llevaron a cabo en 2013.

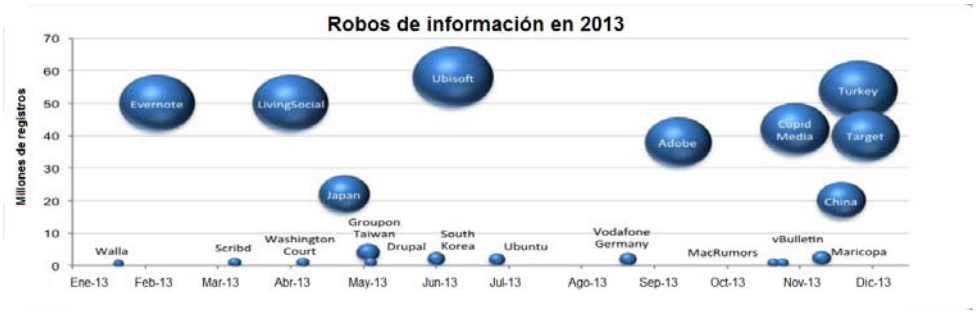


Figura 2.4 Robos de información en 2013 por cantidad de registros robados

Estos robos de información supusieron que unos 392 millones de registros de usuarios se encuentren ahora mismo en manos de criminales. Los datos de tarjetas de crédito son vendidos en portales de los mercados underground de internet (Krebs, Cards Stolen in Target Breach Flood Underground Markets, 2013). Otros datos personales son usados por los criminales para realizar robos de identidad. En 2012 un 25% de los usuarios cuyos datos fueron robados sufrieron también robos de identidad (Javelin Strategy Research, 2013).

Para tener una imagen más clara de los objetivos y métodos de este tipo de delincuencia es útil revisar los 9 principales ataques de 2013 para ver qué tipo de información fue robada:

1. Adobe sufrió el 3 de octubre el robo de información de 58 millones de clientes de su base de datos. Dicha información contenía sus ID de usuario de Adobe junto con sus contraseñas y emails así como datos cifrados de tarjetas de crédito y débito. Además de los 58 millones de usuarios activos también se hicieron con información de hasta casi 100 millones de usuarios inactivos y con código fuente de varios productos de la firma incluyendo el famoso Photoshop.

2. En China el 9 de diciembre un grupo no identificado de hackers consiguió hacerse con los datos de reservas en hoteles de unos 20 millones de usuarios. El atacante filtró la información en un portal chino llamado WeChat con una aplicación en la que introduciendo el número de la tarjeta de identidad de una persona mostraba los registros asociados.

3. La empresa australiana Cupid Media sufrió por su parte un ataque el 20 de noviembre que supuso el robo de la base de datos de sus usuarios que contenía registros de 42 millones de personas. Los datos como se puede ver en las capturas de pantalla de Brian Krebs (http://krebsonsecurity.com/2013/11/cupidmedia-hack-exposed-42m-passwords) incluyen el email, nombre, apellidos, fecha de nacimiento y contraseña.

4. Evernote por su parte sufrió el 2 de marzo una intrusión en sus sistemas que acorde con el comunicado de la compañía (http://blog.evernote.com/blog/2013/03/02/security-notice-servicewide-password-reset) pudo suponer la exposición de los email y contraseñas de 50 millones de usuarios. Sin embargo como aclaran en el comunicado las contraseñas estaban cifradas y se habían utilizado técnica de salteado en ellas.

5. Living Social fue atacada el 26 de abril y según el comunicado de la empresa (https://www.livingsocial.com/createpassword) datos de sus usuarios que incluyen nombres, emails, fechas de nacimiento y contraseñas. Sin embargo al igual que en el caso de Evernote las contraseñas estaban cifradas y salteadas.

6. Target fue el objeto de ataque el 19 de diciembre correspondiendo con el periodo de compras navideñas. Los detalles de las tarjetas de crédito así como información personal de sus clientes fue robada afectando a unos 40 millones de clientes (http://pressroom.target.com/news/target-confirms-unauthorized-access-to-payment-carddata-in-u-s-stores).

7. En Turquía el almacenamiento por parte de partidos políticos de la base de datos de los ciudadanos cedida por el Comité Electoral del país supuso que los datos fuesen robados el 16 de diciembre. Según las noticias un hacker ruso (http://www.hurriyetdailynews.com/russian-hackers-stole-54-million-turkishcitizens-id-data-claim.aspx?pageID=238&nID=59644&NewsCatID=338) fue el autor del robo que afectó a 54 millones de ciudadanos.

8. Ubisoft descubrió que el 2 de julio uno de sus sistemas había sido atacado e información sobre sus usuarios había sido robada afectando a 58 millones de usuarios. En su comunicado oficial (http://blog.ubi.com/security-update-for-all-ubisoft-accountholders) se informa que sólo nombres de usuarios, emails y

contraseñas cifradas fueron robadas. Sin embargo el servidor donde se alojaban los datos de las tarjetas de crédito no fue atacado.

9. Yahoo! Japón reconoció el 18 de mayo que uno de sus servidores había tenido un intercambio anormal de información y que podrían haber sido víctimas de un robo (ver noticia en el Japan Times http://www.japantimes.co.jp/news/2013/05/18/national/yahoo-japan-suspects-vast-id-theft/#.UaGx_5xz4et). Sin embargo la compañía no menciona más detalles sobre el robo en sí.

Una vez vistas las consecuencias de los 9 mayores cibercrímenes de 2013 el siguiente paso es entender cómo se han podido llevar a cabo. Antes de nada hay que destacar que muchas empresas son reacias a publicar información técnica sobre los ataques sufridos ya que dicha información revela parte de su estructura y puede suponer un riesgo. Sin embargo gracias a la excelente labor de divulgadores y expertos en seguridad como Brian Krebs o Paulo Passeri es posible reconstruir bastantes de ellos.

1. En el caso de Adobe, de acuerdo a las investigaciones publicadas por Brian Krebs, fue atacada por un grupo de delincuentes que había anteriormente descubierto una vulnerabilidad en ColdFusion (producto de Adobe para servidores) y la había explotado con éxito (Krebs, Data broker giants hacked by id theft service, 2013) en servidores de la agencia NW3C. Al parecer tras el éxito en dicho ataque los delincuentes decidieron atacar a la propia Adobe con el fin de robar el código fuente de otros productos y poder así descubrir más vulnerabilidades.

2. En China el robo de los datos de millones de clientes de hoteles fue provocado por un problema en la seguridad del proveedor de Wifi CNSWisdom (Li, 2013). La empresa china no ha querido dar más datos sobre el ataque así que el vector usado para el mismo sigue siendo desconocido.

3. El atacante de Cupid Media según Brian Krebs (Krebs, Cards Stolen in Target Breach Flood Underground Markets, 2013) es el mismo grupo de criminales que atacó a Adobe. En su artículo se menciona como el responsable de la web trata de situar la fecha del ataque mucho antes de cuando sucedió. Probablemente debido a que quiere ocultar la falta de medidas una vez que el ataque de Adobe fue hecho público y se informó de la vulnerabilidad en ColdFusion.

4. Evernote fue hackeada el 2 de marzo y los asaltantes consiguieron hacerse con identificadores de usuario y contraseñas cifradas y salteadas. Sin embargo a pesar de las peticiones la compañía no ha proporcionado ninguna información acerca del ataque en sí por lo que el vector de ataque sigue siendo desconocido.

5. Living Social por su parte fue víctima del robo de su base de datos de usuarios y contraseñas. Dada la mala elección del algoritmo para almacenar los datos (SHA-1) el "dump" de la base de datos fue puesto a la venta por 1 Bitcoin. De acuerdo a información de C|net (Rosenblatt, 2013) el robo pudo haberse producido mediante una inyección SQL en una aplicación web de la compañía.

6. Target por su parte fue víctima de un ataque Malware. Los atacantes a través de un proveedor que carecía de medidas de seguridad fueron capaces de infiltrarse en la red de Target y colocar un malware en los terminales de venta que les ayudó a exfiltrar los datos de las tarjetas de los clientes.

7. En el caso de Turquía aunque no está claro que vector utilizaron los atacantes para acceder a la información lo que sí está claro es la nefasta política de ciberseguridad del país. Máquinas sin antivirus con datos sensibles, funcionarios realizando copias en DVD de material privado y agencias del gobierno cediendo la propiedad de sus bases de datos a entidades privadas hicieron muy fácil la labor de los atacantes (Bisson, 2014).

8. En el caso de Ubisoft después de ciertas especulaciones iniciales acerca de un posible error en el navegador de su servicio UPlay la compañía confirmó que el ataque se produjo en una web interna (Hinkle, 2013). Por el tipo de objetivo atacado lo más posible es que se tratase de una inyección SQL.

9. En el caso de Yahoo! Japón lo único conocido es que hubo un acceso a la base de datos de usuarios desde donde se extrajo información de 22 millones de usuarios (ver http://storageservers.wordpress.com/2013/05/21/yahoo-japan-servers-hacked-to-steal-22-million-user-ids) sin embargo la compañía no ha querido publicar ningún detalle del incidente.

2.3.3. Posibles técnicas de defensa

Como se ha podido observar los frentes de ataque a una compañía en la red son muy numerosos y por tanto la protección ante ellos es un asunto muy complejo. De todas formas es necesario mencionar algunas de las técnicas probadas que ayudan a reducir el impacto de los ataques.

En cuanto a los ataques de DDoS las recomendaciones para tratar de mitigar sus efectos son:

- Tener sistemas que detecten rápidamente el inicio de situaciones anormales de tráfico. La temporalización en este tipo de ataques es crítica si se quieren evitar caídas del sistema

- Ser capaz de levantar reglas rápidamente para bloquear directamente tráfico de ciertos países o segmentos cuando se supere ciertos niveles.

- Disponer de servicios de balanceo de peticiones tipo Akamai que ayuden a filtrar el tráfico.

- Ponerse en contacto inmediatamente con el ISP para intentar bloquear el tráfico en sus rúters y evitar que alcance la red del usuario dónde es más costoso bloquear el tráfico.

Para el otro ataque clave, las SQLi, existen también ciertas recomendaciones que ayudan a reducir su incidencia e impacto:

- Para aplicaciones internas es crucial el uso de librerías y métodos que aseguren las entradas de los usuarios antes de ejecutar las consultas a la base de datos.

- Es también fundamental definir correctamente los roles de la base de datos de forma que dependiendo del usuario se utilicen diferentes conexiones a la base de datos con permisos exclusivos para los datos que necesita consultar.

- En caso de que las aplicaciones sean externas el uso de un WAF (Web Application Firewall) puede ayudar a modelar el uso de las aplicaciones y a bloquear la exfiltración de resultados. El WAF de Imperva permite definir el número y tipo de parámetros de las consultas y sus respuestas de forma que una SQLi puede ser detectada y bloqueada.

En cuanto a políticas de almacenamiento es importante ponerse en la situación en la cual la base de datos ha sido comprometida y desde ahí ver qué medidas pueden limitar la usabilidad de los datos robados. Ejemplos básicos son:

- Las contraseñas deben estar almacenadas usando un algoritmo de hash robusto y con salteo.

- La base de datos de tarjetas de crédito debe estar separada de la de clientes y se debe cumplir con las recomendaciones de la normativa PCI para almacenado de PAN cifrados.

- Es recomendable ofrecer al usuario la posibilidad de autenticarse usando dos factores en vez de simplemente la contraseña.

- Otro aspecto fundamental es tener tareas periódicas de purgado de la base de datos. En los casos de Adobe y Cupid Media el número de usuarios afectados fue mucho mayor debido a la política de estas empresas de no eliminar los datos de

los usuarios que se han dado de baja. Dichos datos son más una carga para la compañía que un activo y deben ser eliminados cuanto antes.

Por último es importante tener en cuenta que en informática la seguridad no es un estado sino un proceso y por tanto es necesario tener establecido un proceso constante de auditorías de seguridad que evalúen la idoneidad de las medidas implementadas.

3. Análisis de los posibles mecanismos de defensa

Una vez que se ha visto que la privacidad de los usuarios se encuentra bajo amenaza constante por parte de los tres agentes mencionados anteriormente es necesario ver qué medidas se encuentran al alcance de los usuarios para tratar de limitar su impacto.

Ya que la primera fuente de las amenazas son los procesos de "publificación" y de "personalización de los roles" que lleva a los ciudadanos a poner una mayor cantidad de información la primera solución es revisar el grado de exposición digital. En la situación actual gran parte de la información es pública por defecto aumentando así el perfil de exposición. Una revisión sobre los datos compartidos y la necesidad de que se encuentren disponibles para todo el mundo debe ser la primera medida a tomar.

La segunda posible solución es la repatriación de los datos desde servicios basados en modelos de negocio financiados con publicidad a otros más respetuosos con la privacidad. La Free Software Foundation tiene una página web (http://stop-prism.org) donde se pueden encontrar alternativas más respetuosas con la privacidad. Un aspecto interesante de las alternativas libres es el poder hospedar el servicio localmente. Las alternativas libres suelen ofrecer el código fuente, ejecutables y guías de instalación que permiten montar el servicio en una máquina local. Además otra de las ventajas de estas alternativas es que suelen basarse en protocolos "federados". Estos protocolos carecen de un nodo central y en ellos la información se encuentra distribuida entre los diferentes equipos que usan el protocolo. Esto hace más difícil el robo de información de forma masiva ya que ésta no se encuentra almacenada en un punto único. Como ejemplo de este tipo de soluciones auto contenidas, en el trabajo fin de master realizado por uno de los autores de este artículo (Casais Solano, 2014), se demostró que es posible montar un servidor que utilice servicios libres y provea los servicios básicos de la Sociedad de la Información. Sin embargo durante el montaje de dicho servidor se observó que las soluciones libres en su mayoría no se encuentran en un estado de madurez que permiten a gente sin conocimientos avanzados de informática montar sus propios servicios. Después de la realización del experimento con los diversos servicios se llega a la conclusión de que en muchos casos el nivel de conocimientos requerido para su instalación y funcionamiento de una forma segura es muy elevado. Algunos servicios se encuentran tan mal empaquetados que es imposible aun siguiendo sus instrucciones hacerlos funcionar. En otros la falta de detalles sobre como configurar o instalar los

prerrequisitos de la solución elegida supone un grave problema. Además en muchos de los servicios se recomienda el uso de certificados de seguridad SSL pero no se explica detalladamente como conseguirlos o instalarlos correctamente

La tercera posible solución es la legislativa. Leyes como la de Ley Orgánica de Protección de Datos o sentencias como la del Tribunal de Justicia Europeo acerca del Derecho al Olvido son también formas eficaces de provocar cambios en el tratamiento que hacen las empresas de nuestros datos personales. En países como Alemania, Estados Unidos o Inglaterra están apareciendo movimientos políticos que abogan por una legislación que proteja más a los ciudadanos de las intromisiones en su vida privada.

4. Conclusiones

Como se ha mencionado anteriormente las soluciones libres aún no se encuentran en el grado de madurez necesario para que el gran público haga un uso masivo de las mismas. Aral Balkan en su conferencia “Free is a lie” donde habla sobre los costes de la privacidad menciona también que en el campo del software libre existe un gran déficit en cuanto a la experiencia de usuario. Muchos de los servicios probados proporcionan interfaces de gestión demasiado complejas o directamente fuerzan al usuario a editar archivos de configuración manualmente. El exceso de complejidad acaba produciendo que la mayor parte de los usuarios no sean capaces de utilizar estos sistemas aun siendo técnicamente superiores. Es por tanto necesario un cambio de mentalidad con un enfoque mayor en la interacción del usuario y la seguridad y posponer el aumento de las funcionalidades del software existente hasta que estos dos aspectos estén a un mayor nivel.

Sin embargo a pesar de la dificultad para montar los servicios propios, o quizás debido a ello, hay cada vez más servicios públicos de pago basados en software libre que garantizan un tratamiento más ético y respetuoso de los datos de los usuarios. Es importante mencionar en este punto que el criterio geográfico aquí es vital. El más seguro de los servicios montado en cualquiera de los países miembro de los Five Eyes es susceptible de ser interceptado. Esto pone a los servicios basados en la Unión Europea o Suiza en una posición ideal para hacerse con un mercado de usuarios Premium dispuestos a pagar por mantener su privacidad. Esto puede ser un buen germen para lograr servicios europeos de calidad respetuosos con la privacidad.

Por último y como colofón a este artículo es fundamental mencionar tres principios que se revelan como básicos para entender la privacidad:

1. En el mundo corporativo si no pagas por un servicio es tú eres el producto con las consecuencias que ello conlleva.

2. En cuanto a los gobiernos el político Benjamín Franklin dijo que “aquellos que renunciarían a una Libertad esencial para comprar un poco de Seguridad momentánea, no merecen ni Libertad ni Seguridad”.

3. Y en cuanto a los ataques criminales se ha de entender que es un simple problema de riesgo recompensa, mientras se acumulen gran cantidad de datos en sistemas centralizados seguirá siendo rentable para los criminales realizar ataques contra dichos sistemas.

5. Bibliografía

Ackerman, S., & Ball, J. (28 de Febrero de 2014). Optic Nerve: millions of Yahoo webcam images intercepted by GCHQ. Obtenido de http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo

Asamblea General de las Naciones Unidas. (1948). Declaración Universal de Derechos Humanos. Paris. Obtenido de https://www.un.org/es/documents/udhr/index_print.shtml

Asser, M. (Julio de 2000). Echelon: Big brother without a cause? Obtenido de http://news.bbc.co.uk/1/hi/world/europe/820758.stm

Associated Press. (Enero de 2005). FBI Ditches Carnivore Surveillance System. Obtenido de http://www.foxnews.com/story/2005/01/18/fbi-ditches-carnivore-surveillance-system/

Bisson, D. (Enero de 2014). Compromising 54 million ids: The shortcoming of turkish cybersecurity. Obtenido de http://www.informationsecuritybuzz.com/compromising-54-million-ids-shortcomings-turkishcybersecurity/

Casais Solano, P. (2014). La privacidad en la Sociedad de la Información. *MUF-13001*.

Cervera, J. (Noviembre de 2009). SITEL en doce preguntas. Obtenido de http://www.rtve.es/noticias/20091105/sitel-doce-preguntas/299489.shtml

Cortes Generales. (1978). Constitución Española. *BOE-A-1978-31229*, pág. 4. Madrid: BOE. Obtenido de http://www.boe.es/buscar/pdf/1978/BOE-A-1978-31229-consolidado.pdf

del Moral, J. (Septiembre de 2001). Echelon sirvió para espiar a Arriortúa. Obtenido de http://gananzia.com/echelon-sirvio-para-espiar-a-arriortua

Electronic Privacy Information Center. (Enero de 2005). Carnivore. Obtenido de https://epic.org/privacy/carnivore/

Epstein, J. (Enero de 1996). Big surveillance project for the Amazon jungle teeters over scandals. Obtenido de http://www.csmonitor.com/1996/0125/25071.html/%28page%29/2

Evans, R., & Leigh, D. (Junio de 2003). Airbus's secret past. *The Economist*, 55-58. Obtenido de http://www.economist.com/node/1842124

García Morente, M. (2008). *Idea de la Hispanidad.* Madrid: Homo Legens.

Gorski, D. (Junio de 2014). Did Facebook and PNAS violate human research protections in an unethical experiment? Obtenido de http://www.sciencebasedmedicine.org/did-facebook-and-pnas-violate-human-research-protections-in-an-unethical-experiment/

Hassan, A. (16 de Agosto de 2011). Ciberataque de Anonymous contra el gobierno colombiano. Obtenido de http://actualidad.rt.com/ciencias/view/31368-Ciberataque-de-Anonymous-contra-gobierno-colombiano

Hinkle, D. (Julio de 2013). Ubisoft hacked, account info accessed. Obtenido de http://www.joystiq.com/2013/07/02/ubisoft-hacked

Javelin Strategy Research. (2013). More Than 12 Million Identity Fraud Victims in 2012 According to Latest Javelin Strategy & Research Report. Obtenido de https://www.javelinstrategy.com/news/1387/92/1

Jenkins, Q. (28 de Marzo de 2013). Answers about recent DDoS attack on Spamhaus. Obtenido de http://www.spamhaus.org/news/article/695/answersabout-recent-ddos-attack-on-spamhaus

Kersey, B. (Enero de 2013). Anonymous petitions the White House to make DDoS attacks a legal form of protesting. Obtenido de http://www.theverge.com/2013/1/9/3856202/anonymous-wants-ddos-attacks-to-be-protected-under-free-speech

Krebs, B. (20 de Diciembre de 2013). Cards Stolen in Target Breach Flood Underground Markets. Obtenido de http://krebsonsecurity.com/2013/12/cards-stolen-in-target-breach-flood-underground-markets/

Krebs, B. (Diciembre de 2013). Cards Stolen in Target Breach Flood Underground Markets. Obtenido de http://krebsonsecurity.com/2013/12/cards-stolen-intarget-breach-flood-underground-markets/

Krebs, B. (Septiembre de 2013). Data broker giants hacked by id theft service. Obtenido de http://krebsonsecurity.com/2013/09/data-broker-giants-hacked-by-id-theft-service

Kundera, M. (1985). *La insoportable levedad del ser.* Barcelona: Tusquets Editores.

Li, A. (Octubre de 2013). Software loophole puts chinese budget hotel guests privacy at risk. Obtenido de http://www.scmp.com/news/chinainsider/article/1329325/software-loophole-puts-chinesebudget-hotel-guests-privacy-risk

Ministerio del Interior. (Octubre de 2007). Contrato plurianual de soporte a SITEL. (BOE-B-2007-256021(256):12614). doi:65067/07

Molist, M., & Collado, M. (Abril de 1999). Bruselas estudia cómo pinchar Internet. Obtenido de http://ww2.grn.es/merce/enfopol.html

National Security Agency. (Junio de 2010). Declassified UKUSA Signals Intelligence Agreement Documents Available. Obtenido de http://www.nsa.gov/public_info/press_room/2010/ukusa.shtml

Pemper, K. (Junio de 2014). Cyber crime costs global economy 445 billion dollars a year. Obtenido de http://www.reuters.com/article/2014/06/09/us-cybersecurity-mcafee-csis-idUSKBN0EK0SV20140609

ProPublica. (2014). The NSA Revelations All in One Chart. Obtenido de http://projects.propublica.org/nsa-grid/

Quirantes Sierra, A. (Enero de 2002). Zona ENFOPOL. Obtenido de http://www.ugr.es/~aquiran/cripto/enfopol.htm.

Ramos, A. (Julio de 2014). Cazador de mitos: La privacidad en Internet . *Security by default*. Obtenido de http://www.securitybydefault.com/2014/07/cazador-de-mitos-la-privacidad-en.html

Rosenblatt, S. (Abril de 2013). Livingsocial hacked; 50 million affected. Obtenido de http://www.cnet.com/news/livingsocialhacked-50-million-affected/

Sanders, J. (s.f.). Etherpeek. Obtenido de http://www.pcmag.com/article2/0,2817,27055,00.asp