Privacidad y Seguridad en las Redes Sociales

VS

Sergio de Luz para www.redeszone.net

Índice de contenidos

Introducción o resumen del trabajo.

En los últimos años, las redes sociales como Facebook o Twitter han crecido rápidamente, las redes sociales son muy útiles para hablar con amigos que hacía mucho tiempo que no teníamos contacto, o antiguos compañeros de clase.

También nos permiten crear eventos para quedar o salir, sin tener que llamarnos todos por teléfono y por tanto, ahorrarnos dinero en la factura del móvil. También sirve para establecer nuevas relaciones con otros, basados en rasgos compartidos como comunidades, hobbies, intereses y círculos de amistad.

Las ventajas de las redes sociales las conoce todo el mundo, lo que poca gente sabe, es que la privacidad y la seguridad en las redes sociales, está reñida con la sociabilidad y el uso que se les puede dar. Si tenemos un perfil demasiado estricto, no se podrán comunicar amigos de nuestros amigos y eso podría perjudicarnos "socialmente", sin embargo si tenemos un perfil abierto, se podrá comunicar todo el mundo, ver todas las fotos, todos los comentarios, es decir, la privacidad es nula pero sin embargo la sociabilidad es máxima, justo lo que la gente quiere conseguir en las redes sociales.

Debemos tomar como premisa, que las redes sociales son seguras ante el ataque de hackers, porque si no este artículo, no acabaría nunca, hablando de los grandes gazapos de todas las redes sociales y su nulo interés por corregir los fallos antes de sacarlo al público, al fin y al cabo qué más da, la gente sólo quiere subir sus fotos y cotillear los perfiles de los demás, nadie se va a parar a pensar que si pones "usuario" y la clave 10 veces (ataque fuerza bruta) puedes seguir metiendo más y más claves hasta dar con la buena. O que el Login se realice mediante http por el puerto 80 sin ningún tipo de cifrado. Y ya ni hablar, de que la sesión entera tampoco es cifrada con todos los datos de carácter personal (nuestros y de los demás), que circulan por ella.

Cuando le dices a un amigo, que vas a subir las fotos de la última fiesta al blog personal con contraseña, te dice que no, que es más seguro y mejor subirlo al Tuenti. La gente confía en las redes sociales, pero no son conscientes de la inmensa información que ellas recogen de todo el mundo. Cuando subes una foto a Facebook, si luego la quieres borrar, se eliminará del perfil, pero la foto queda en los servidores de Facebook como veremos más adelante.

Las redes sociales han crecido exponencialmente, y ellas almacenan muchísima información privada de sus usuarios y sus interacciones. Esta información es privada y va dirigida a unas determinadas personas. Sin embargo con toda la información que almacenan, no es de extrañar que las redes sociales también atraigan a personas malintencionadas, para acosar, difamar, hacer spam y phising.

A pesar de los riesgos, muchos mecanismos de control de acceso y privacidad son débiles contra estos atacantes.

En este artículo hablaremos sobre la seguridad y privacidad en las redes sociales, y nos hacemos la pregunta: ¿cuáles deberían ser los objetivos de los diseños de seguridad y privacidad?

Cuando evaluamos los objetivos, entramos en el conflicto de privacidad contra funcionalidad y sociabilidad. Debe haber un equilibrio entre ellas.

Desarrollo de la temática:

Principales funcionalidades de las redes sociales:

Hay varias diferencias entre unas redes sociales y otras, pero todas ellas tienen un punto en común: la comunicación con nuestros amigos, y también con desconocidos.

Una red social es la representación digital de sus usuarios, sus relaciones sociales, sus fotos mensajes etc.

Con dicha res social podemos crear un perfil de uno mismo para mantener relaciones sociales con otra gente que también tiene un perfil, mejorar las relaciones existentes entre nosotros y también nos ayuda a tener nuevas relaciones sociales, basadas en intereses comunes como localización geográfica, actividades etc.

Las redes sociales también nos proporcionan un espacio personal de gestión de nuestro perfil. Nos permiten, - entre otras cosas -, crear, modificar y cancelar nuestro perfil en dicha red social. También nos permite introducir contenido (fotos o comentarios) y editarlos, todo ello para mejorar la relación con otra gente, ya que automáticamente es actualizada en la red social y estará a la vista de nuestros contactos.

Nos permitirán administrar la lista de contactos que tengamos, podremos agregar personas con nuestros mismos gustos, misma edad, ciudad...para establecer una nueva relación.
Si tenemos gente agregada con la que que ya no hablamos, o simplemente porque no queremos tenerlos en nuestra lista de amigos, podemos eliminarlos, y no tendrán los permisos necesarios para seguir viendo nuestras fotos o comentarios (esto si la configuración de seguridad es para sólo amigos y no abierto para todo el público).

Algunas redes sociales también permiten hacer grupos de gente, por ejemplo podemos crear el grupo amigos y meter allí a todos nuestros amigos con unos permisos sobre nuestro perfil determinados. Si creamos el grupo compañeros de trabajo, puede que no queramos que esa gente vea nuestras fotos personales, pues les aplicamos los permisos necesarios para que no las puedan ver, y tener control total sobre lo que ven y no ven nuestros contactos.

La comunicación con los demás, es la principal característica de las redes sociales, y podemos comunicarnos de varias formas. Podemos poner comentarios en un tablón como si de una especie de blog se tratase, estos comentarios estarán a la vista de todo el mundo, podremos mantener conversación personales de una forma pública.
Si queremos más privacidad, podemos enviar mensajes privados, que sólo leerá el propietario del perfil en cuestión, es como enviar un email, pero mediante la red social.
Otra forma de comunicación es el "Chat", que es como una conversación de messenger, y puede incorporar videollamada.

Algunas redes sociales permiten aplicaciones de terceros, y encontramos por ejemplo los juegos (muy adictivos) de las redes sociales.

Las redes sociales no se limitan sólo a mantener las relaciones existentes (perfiles agregados a nuestro propio perfil), sino que también necesitan (necesitamos) establecer contacto con más gente, y es ahí donde entra en juego el buscador de las redes sociales, donde haremos una búsqueda global por toda la red.
Para encontrar a un usuario deberemos poner su nombre, también podemos acotar su búsqueda por país, provincia, Universidad, colegio, por empresa y por supuesto por sexo y edad. Se nos presentará un listado con toda la gente coincidente, y con la foto principal del perfil podremos decidir si es la persona que buscamos, o de lo contrario nos hemos equivocado y debemos seguir buscando.

También podemos buscar gente que sean "amigos de nuestros amigos", es lo que llamamos un cruce social. Entramos en su perfil y podremos ver a toda la gente que tiene agregada. Un usuario puede restringir que la demás gente vea a quien tiene agregado, pero esto quita sociabilidad (a cambio de una mayor privacidad).

El principal objetivo de una red social es la sociabilidad, por tanto si tenemos el perfil abierto para que puedan ver a nuestros amigos, potenciaremos esa sociabilidad, y esto es lo que entra en conflicto con la privacidad y la seguridad.

Las redes sociales, también pueden llegar a enmascarar las malas relaciones. Cuando un usuario se quita de la lista de amigos de otro usuario, no te aparece ninguna notificación de que te ha desagregado, solamente aparecen notificaciones sobre las relaciones que son buenas. Es decir, enmascaran los sucesos desagradables. [5]

Arquitectura de una red social.

Hay dos formas en las que las redes sociales pueden trabajar, tenemos la arquitectura cliente-servidor donde el servidor será la red social y los clientes nosotros. Y la otra es la arquitectura peer-to-peer, donde la información estará distribuida y no centralizada, como ocurre en el cliente-servidor.

Las redes actuales de hoy en día están centralizadas, basadas en una arquitectura cliente-servidor. Todas las funcionalidades de la red social, como el almacenamiento, edición de los datos, mantenimiento de la web, o el acceso a los servicios que proporcionan la red social, son ofrecidos por la propia red social como Facebook o Tuenti. Esta arquitectura tiene la ventaja de ser sencilla, pero a la vez, es débil a los ataques, como el ataque de denegación de servicio. Si la información que se almacena en el servidor WEB es muy grande, podría provocar el denominado cuello de botella y que todos los usuarios navegaran muy lentamente por la red social. Por eso hay varios servidores en cada uno de los países, varios nodos, aunque están conectados entre sí para el intercambio de información.

La arquitectura peer-to-peer podría ser la próxima generación de redes sociales. Se adoptaría un sistema descentralizado basado en la cooperación de cada uno de los miembros de la red, cada usuario sería cliente de la red social y a la vez servidor de dicha red social, por tanto se almacenarían datos en nuestro equipo. Se apoyaría el intercambio directo de información entre dispositivos, entre usuarios que ya se conocen de antes. La arquitectura P2P puede tener ventaja en redes sociales reales, y proximidad geográfica para proporcionar servicios locales, sin necesidad de internet. El servidor estaría distribuido en cada nodo de almacenamiento, y deberemos tener una "relación social" con ese nodo. El principal problema de esto será, realizar búsquedas de manera global.

En resumen, la arquitectura cliente-servidor, requiere conexión a internet para comunicarse a través del servidor centralizado de nuestra red social. Por otra parte el P2P conectaría localmente, ya que el papel de servidor se distribuye en cada nodo de almacenamiento.

Privacidad y seguridad en las redes sociales.

Para comprender el gran reto que supone equilibrar seguridad y privacidad, con la sociabilidad y usabilidad tenemos que ver los principales estándares de seguridad en la red.

- Confidencialidad: requiere que la información sea accesible únicamente a las entidades autorizadas. Es de vital importancia en las redes sociales porque un mal uso de la información podría traer graves consecuencias en la vida de las personas.
- Integridad (requiere que la información sólo sea modificada por las entidades autorizadas).
- Disponibilidad (requiere que los recursos del sistema estén siempre disponibles).
- No repudio (ofrecer protección a un usuario frente a otro que niegue posteriormente que realizó cierta comunicación). [4]

Todo ello aplicado a las redes sociales.

La protección de los datos es de suma importancia en una red social, ya que la divulgación ilícita y el uso indebido de la información privada de los usuarios, pueden causar indeseables o perjudiciales consecuencias en la vida de las personas.

Pero como las redes sociales no son infalibles, a menudo, sale información sobre que ciertas cosas que deberían estar ocultas no lo están. En Abril, un ingeniero de Google se dio cuenta de un fallo de seguridad, y fue exactamente en el perfil del creador de Facebook [9]

No sólo los administradores de las redes sociales se deben preocupar por la protección de los datos de sus usuarios, sino también las autoridades competentes en este campo, como por ejemplo la LOPD que multan con 300000€ a 600000€ si alguien altera o tiene acceso a los datos personales sin la autorización del propietario de esos datos [4].

La intimidad en el contexto de las redes sociales tiene varios puntos:

- Anonimato de la identidad del usuario:

  La protección de la identidad real de los usuarios, cambia dependiendo de en qué red social estemos registrados. En redes sociales como Facebook, la gente usa su propio nombre como como perfil, para que les sea más fácil localizar a usuarios y sobre todo, que les localicen dentro de la red social.

  A medida que una red social va creciendo, se hace totalmente imposible controlar todos los comentarios, y la divulgación de estos comentarios corren como la pólvora. En noviembre de 2005, cuatro estudiantes de la Universidad del Norte de Kentucky, fueron multados cuando las imágenes de una reunión se publicaron en Facebook. Las imágenes, tomadas en uno de los dormitorios, fueron una prueba visual de que los estudiantes no cumplieron la política de la

universidad del campus. En este ejemplo, los asuntos privados fueron publicados por ellos mismos[2]. No podemos saber el alcance que va a tener algo que ponemos en la red social.

Esto también se puede extrapolar a los videos de Youtube, donde la gente, por ejemplo, sube sus vídeos excediendo la velocidad máxima permitida en una carretera y luego les llega la correspondiente denuncia de la Guardia Civil.

Todo lo que ponemos en la red, se queda en la red, por tanto debemos tener cuidado de que lo que ponemos no nos perjudique ni nos meta en situaciones problemáticas.
Sin embargo en redes sociales como Twitter, normalmente la gente puede poner pseudónimos o direcciones de tu propia página web como perfil.

– Privacidad del espacio personal:

La visibilidad del perfil de usuario de una red social a otra varía, en algunas redes se pueden encontrar perfiles haciendo una búsqueda en Google, como por ejemplo Facebook o Twitter; sin embargo en la red social Tuenti esto no es posible, está totalmente cerrada a la gente registrada en la página web.

En esta parte también entramos en los perfiles que puede o no ver la gente. Dependiendo de una red social u otra, los permisos por defecto con públicos o privados. Facebook tiene un enfoque diferente por defecto, los usuarios que forman parte de la misma subred pueden ver los perfiles de los demás, a menos que un perfil haya decidido denegar el permiso a los de su subred. Como hemos comentado anteriormente, la mayoría de las redes sociales permiten ver a los amigos agregados de los perfiles que estamos viendo.

Como ya hemos dicho, en la mayoría de redes, se pueden ver la lista de amigos que tenemos, aunque hay excepciones ya sea porque la propia red social te da la opción de esconder la lista de amigos o porque has hackeado el perfil para que no salga.

– Privacidad de la comunicación del usuario:

A parte de los datos que proporcionamos a las redes sociales, como nuestras fotos, nuestros comentarios etc. Un usuario de la red social divulga datos adicionales, como por ejemplo el tiempo de conexión, la dirección IP que usa (y por supuesto, su localización geográfica), los perfiles visitados, los mensajes recibidos y enviados, es decir, todo un log de información personal sobre lo que

hemos hecho mientras estábamos en la red social. Todo esto debe ser privado, recordemos que una dirección IP en un espacio de tiempo es única, identifica a una sola persona, y es ilegal su publicación sin el consentimiento del usuario.

Todo esto se resume en que la privacidad ha de estar presente tanto en la red social como en el intercambio de información (fotos, mensajes etc.), y también los logs que se registran en dicha red social.
Las entidades no autorizadas, no deben saber el contenido de los datos privados enviados y recibidos a través de la red social.

Este aspecto de la privacidad de los datos implica la confidencialidad de los datos y el anonimato de los propietarios, debiendo haber un control de acceso. El acceso a la información sobre un usuario sólo puede ser concedida por el propio usuario. Las entidades no autorizadas, tampoco deben poder enlazar los datos privados con el perfil del propietario.

Tipos de ataques a las redes sociales

La autenticación e integridad de los datos es una tarea de gran importancia en una red social.

Debemos tener en cuenta que la mayoría de las redes están basadas en relaciones ya preexistentes en la realidad, un perfil en la red social, es una persona en la vida real, por tanto las redes sociales deben intentar que esto no cambie.

Cualquier intento de desviar un modelo social online, de su correspondiente red social de la vida real, será considerado un tipo de ataque y debe ser detectado y corregido. Hay dos principales "ataques" a las redes sociales:

La primera de ellas es el robo de identidad, que es el mayor problema de las redes sociales. Por ejemplo un atacante puede crear perfiles falsos, otro ataque es hacerse pasar por la otra persona para dañarla. También se pueden hacer pasar por personajes famosos, para calumniarlos o sacarse un beneficio. Esto puede perjudicar la reputación de las redes sociales, por ello en algunas ocasiones cuando se duda de la legitimidad del perfil, la persona que está detrás de ese perfil debe mostrar su autenticidad (por ejemplo en Tuenti cuando se denuncia a alguien por perfil falso, se le pide el DNI para demostrar su autenticidad, - si piensas que esto es un ataque contra la intimidad de la persona si no le muestras el DNI, no pasa nada, siempre puedes no enseñarlo - y que eliminen tu perfil.

Las redes sociales deben cumplir que la mala conducta sea erradicada, porque algunas redes sociales se usan como herramientas de trabajo para ayudar a sus empleados (otro requisito es la disponibilidad, es decir, que siempre estén disponibles).

Tenemos dos tipos de atacantes:

Los atacantes internos, que ya están registrados en la red y parecen que son usuarios normales de la red social, pero actúan de una manera maliciosa, por ejemplo crear programas de terceros para dañar la red social, o también atacantes de nuestra propia red inalámbrica. Es decir, todos los que intentan dañar la red social desde dentro.

También encontramos atacantes externos, intrusos, que no están en la red social, pero que pueden dañarla con ataques externos a los servidores o infraestructuras, como la denegación de servicio.

Conflicto del diseño

Como hemos dicho antes, hay un conflicto entre la seguridad y privacidad de las redes sociales, y su usabilidad y sociabilidad.

Para apoyar la búsqueda social, hay que mostrar cierta información de los distintos perfiles que coinciden en uno que nosotros hemos buscado. Esto ocurre tanto en la búsqueda global como en la búsqueda transversal.
Cuantos más datos muestren, la búsqueda será más precisa y eficiente.

Por tanto, ya hemos vuelto a entrar en el conflicto, si mostramos más potenciamos el encontrar correctamente a un individuo pero la privacidad de la gente queda en entredicho. Sin embargo si no mostramos muy poca información, buscar a alguien se hará una tarea tediosa.

Pero esto va más allá del entorno doméstico, imaginemos que recorremos varios perfiles y descubrimos, que dos empleados de distintas empresas rivales son amigos. Esto podría acarrear problemas para ellos.

La principal función de estas redes, es facilitar y potenciar la interacción social. En algunas ocasiones, tenemos la necesidad de crearnos dos perfiles distintos, uno personal y el otro para el trabajo. Esto no es del todo seguro, porque si da la casualidad de que un amigo del trabajo y un amigo personal son (entre ellos) conocidos. Puede haber una fuga de información no deseada, pero esta fuga está completamente fuera del campo de actuación de la persona en cuestión porque no depende él, y todos los esfuerzos que él ha hecho de crearse dos perfiles y dar los permisos mínimos, no valen para nada. A parte de que puede que tarde bastante tiempo en enterarse que hay información circulando por la red.

Por ejemplo, si un usuario usa un seudónimo, y luego una amiga etiqueta una foto con su nombre real a ese seudónimo, ya estaría revelando su identidad real, por tanto todos los esfuerzos de proteger su intimidad habrían sido en vano.

De nada nos va a servir tener una buena configuración de privacidad o de si todo el tráfico está cifrado, si luego no pensamos en lo que se puede extraer de todo lo que ponemos [2].

Minería de Datos VS Privacidad

La ingente cantidad de datos que se suben a las redes sociales, son una importante fuente para el análisis social, lo que puede contribuir a ver como evoluciona la sociedad, pero también puede ser un gran estudio de marketing.

Los datos recogidos, también pueden servir para mejorar la propia red social, con configuraciones o complementos demandados por los usuarios.

Como siempre, estamos ante una encrucijada, mejorar el sistema tal y como quieren los usuarios, o apostar por la privacidad, y no recoger estos datos para proteger su privacidad. Aunque ocultemos los datos y en teoría, sean anónimos, está demostrado que la mayoría de las identidades reales de los usuarios se puede recuperar.

Cliente-servidor vs arquitecturas P2P

La arquitectura cliente-servidor tiene varias ventajas sobre la arquitectura P2P, en el cumplimiento de uno de los objetivos principales de una red social. Los usuarios no se limitan sólo a las relaciones que ya tienen sino que pueden encontrar a ex-compañeros de clase en las redes sociales (siempre y cuando estén en la misma red social). Es más fácil encontrar a alguien en el servidor de la red social, realizando una búsqueda a través de una serie determinada de datos como puede ser el nombre, la edad o el colegio en el que estuvieron. La minería de datos es más eficaz en un servidor centralizado, sin embargo, todos los datos se almacenan en los servidores de la red social elegida, y se pueden usar para distintos fines para los que fueron recogidos, y por tanto, violar la privacidad de los usuarios.

Por otra parte, los datos almacenados en las bases de datos de las distintas redes sociales pueden ser robados por piratas informáticos, y toda la información que hay sobre todos los usuarios pueden eliminarla, modificarla o copiarla, para sus propios beneficios.

En Mayo, Facebook identificó al hacker que había robado más de 1,5 millones de cuentas y que intentó venderlas en foros de hacking a bajo precio. Como veis, ninguna

red social es completamente segura, aunque la seguridad empieza por nosotros mismos. [6]

En Julio, Facebook implementó un botón para eliminar nuestra cuenta, de una forma rápida y sencilla. Pero no es oro todo lo que reluce, porque en las condiciones de uso del servicio, todas las fotos y todo lo que subes a Facebook, pasa a ser de su propiedad. Es decir, que puede que eliminen tu perfil, pero las fotos siguen quedando en sus servidores. [7]

Recientemente, ha salido un nuevo caso de fotos borradas que todavía siguen estando en los servidores. Arstechnica.com, medio de referencia sobre tecnología, habla que muchos usuarios se han quejado sobre fotos que borraron hace mucho tiempo y aún continúan. Qué casualidad, que en cuanto la noticia vio la luz, las fotos desaparecieron por arte de magia. [8]

Aunque la política de privacidad de Facebook asegura que no comparten información personal con las empresas que se anuncian en dicha comunidad virtual, la ha dicho que en algunos casos habían enviado el nombre de usuario a dichos anunciantes y que era un fallo que ya estaba corregido. [12]

En la arquitectura P2P la seguridad se ve reforzada porque no está centralizada, se elimina el servidor de la red social central, lo almacenan los propios usuarios, quienes pueden cifrar sus propios datos para evitar miradas indiscretas, y también reforzar el control de acceso a esos datos.

En un sistema centralizado, también puedes subir los datos cifrados, pero esto no es totalmente cierto, porque la propia red social puede prohibirte subirlos de este modo, y si hay un vacío en sus condiciones, siempre pueden modificar sus condiciones de uso. De todas formas, siempre sabrán quien está relacionado con quien basándose en las direcciones IP de los usuarios.

Un sistema P2P con cifrado de datos es la mejor combinación de privacidad que puede haber, pero el problema está en que todavía no se puede recrear eficientemente todo lo que hacen los sistemas centralizados.

Un ejemplo de red social P2P es Diáspora. Una Red Social que están terminando de desarrollar cuatro universitarios estadounidenses, ofrecen un nuevo concepto de comunicación social, que tiene como primer objetivo garantizar la privacidad de nuestros datos, un tema muy importante pero que al parecer, importa poco. Diáspora ofrecerá una plataforma P2P, es decir, que nuestros datos no salen de nuestros PCs, lo que nos posibilita decidir qué información compartimos, con quien y en qué momento

queremos desaparecer, algo que a día de hoy es casi imposible en las redes sociales cliente-servidor como Facebook. [14]

Direcciones de investigación

Aunque eliminar completamente los conflictos de diseño para las redes puede ser imposible, necesitamos investigar y explorar en otras direcciones.

Algunas redes, sólo se basan en si aceptamos a los demás como amigos o no, no tienen término medio. Y esto es diferente en la vida real.

Para capturar los máximos aspectos de las relaciones sociales en la vida real debemos incluir:

- Tipos de relaciones: pueden clasificarse como amigos o compañeros y luego están los denominados "seguidores".
- Confianza: muestra la confianza que un usuario deposita en sus compañeros agregados ya sea en un tema específico o en todo.
- Intensidad de la interacción entre usuarios: mide la calidad y cantidad de interacciones entre los distintos usuarios.

Un modelo relacional, puede proveer a la red social más privacidad y seguridad en muchos aspectos.

Lo primero, sería compartir diferente información con nuestros amigos y compañeros. Debemos tener cuidado con las posibles confusiones, y asignar determinados permisos a cada grupo.

Lo segundo, son las relaciones de confianza entre los usuarios, que no son iguales. No podemos tener una relación de confianza binaria (sí o no), siempre hay término medio. Por tanto, si no podemos dar un permiso adecuado a cada situación, podríamos tener una brecha de seguridad en la relación.

Por último, la intensidad de la interacción entre usuarios puede ser como un poder para la calidad de la relación, para tomar decisiones privadas. Si dos usuarios apenas hablan, significa que no quieren revelar demasiada información acerca de ellos. La intensidad de interacciones puede introducir una nueva forma de caracterizar las redes.

Hay que tener en cuenta la complejidad que supone describir una relación. Esto es completamente inviable para una red social, debido a las descripciones inexactas y

ambiguas, evaluar esto puede tener un alto coste computacional que haga que no sea factible.

Recientemente Facebook ha incorporado una serie de herramientas que ofrecen a sus usuarios **un mayor control sobre su información personal** y les ayudarán a interactuar con círculos más pequeños y selectos de amigos.
La nueva función de 'grupos' facilita a los 500 millones de usuarios interactuar en círculos reducidos de amigos, en lugar de tener fotos y mensajes personales abiertos a familiares, amigos, compañeros del instituto y compañeros de trabajo en un mismo lugar.
Con los grupos, los usuarios de Facebook podrán ahora **reunir a sus amigos en diferentes círculos** y enviar mensajes o mantener conversaciones en línea exclusivas con sus integrantes. [10]

Proteger los grafos sociales

La característica principal de las redes sociales, es conectar a los usuarios entre sí. La información recogida en la red social debe ser protegida. Las relaciones y conexiones entre los distintos perfiles, también ayudan a proteger la propia red social y mitigar los ataques a los grafos sociales.

Un enlace social, se puede haber hecho si un usuario malintencionado, consigue la confianza de un buen usuario de la red social. Ese atacante, se puede ganar la confianza a su vez, de otro amigo de la víctima en cuestión, pero finalmente, ellos se darán cuenta de que es una identidad falsa, porque se conocen en persona. La propia naturaleza de las redes hace difícil a los atacantes forzar vínculos sociales

En muchas redes sociales, es muy fácil para un usuario malintencionado, crearse varios perfiles falsos y pretender ser distintas personas. Si la red social requiriese enseñar la apropiada identificación como el DNI, hacer esto sería mucho más complicado. Sin embargo, la privacidad de los usuarios no puede ser garantizada con el esquema centralizado.

Lo mejor que podemos hacer en estos casos, es utilizar la red de relaciones de la vida real para comprobar la identidad de un usuario. La idea es que la gente se conecte y comunique. Aunque es muy fácil crearse un "nick" sin revelar tu nombre, es difícil cambiar los contactos y amigos.

Aunque los grafos sociales online, dan enormes cantidades de datos de confianza para facilitar el diseño de mecanismos de defensa, las relaciones sociales personales representan mucha información privada sensible de ser mal utilizada. La clave está, en encontrar una forma de preservar la privacidad para utilizar el conocimiento de los grafos sociales.

Ha habido una creciente preocupación cuando dan demasiada información personal por la amenaza de violadores sexuales, recordemos que Tuenti permite hacerse un perfil si eres mayor de 14 años.[5]
El artículo 13 del Reglamento de desarrollo de la LOPD dice que no podrán tener acceso a una red social los menores de 14 años. Facebook, por su parte, hace caso omiso a dicho precepto y permite el registro de usuarios que declaren tener 13 años. Tuenti ha implantado políticas de borrado de perfiles de jóvenes que se detecten como menores de 14 años. No se conocen medidas en este sentido adoptadas por Facebook. [11]

Para mitigar los conflictos de diseño, podemos encontrar y utilizar propiedades cualitativas de las redes sociales de la vida real. A diferencia de las propiedades cuantitativas, las cualitativas se puedes aplicar a cualquier grafo social seguro y no revelar información personal sobre los usuarios individuales.

Basado en el hecho de que es difícil crear links sociales entre nodos honestos y otros no honestos, se propone un nuevo esquema de defensa contra los ataques de usuarios malintencionados. La idea es que los usuarios maliciosos crean demasiados nodos no honestos, el grafo social se hace extraño porque tiene un pequeño cociente de corte, esto es, un pequeño juego de links sociales (los bordes del ataque) cuya eliminación desconecta un gran número de nodos (todos los nodos no honestos) del resto del grafo. Por otro lado, las redes de la vida real no tienden a tener estos cortes (propiedad cualitativa de las redes). Utilizando un tipo especial de camino arbitrario verificable en el grafo social online y las intersecciones entre esos caminos, el pequeño cociente de corte puede ser identificado y el número de nodos no honestos, puede ser, en consecuencia saltado. Creemos que más y más técnicas cualitativas de las redes sociales, combinadas con técnicas criptográficas que preservan la privacidad, pueden ser utilizadas para diseñar nuevos mecanismos de seguridad para redes sin comprometer la privacidad del usuario.

Conclusiones

Hemos comentado los diseños de seguridad y privacidad en las redes sociales online señalando unas cuantas direcciones de investigación para mitigar los conflictos de diseño entre los distintos diseños y las metas de las redes.

Sin embargo, una última solución requerirá expertos en ciencia social y comunidades de seguridad en la red, cuerpos reguladores, y otras comunidades relevantes para tomar decisiones sobre mecanismos políticos y de seguridad.

Los usuarios no son conscientes de que sus comentarios pueden llegar a cualquier persona de la red social, debemos tener una intimidad. Normalmente cuantos más

contactos se tienen, más popular eres, y por tanto tienes más influencia. Todo lo que pongas en la red social lo verá mucha más gente, y seguro que muchos de ellos ni les conocen en persona [3].

Cualquier usuario de la red social, puede coger toda la información que tenemos y usarla en un futuro cercano para hacernos daño. Lo mejor sería no estar en ninguna red social online, así no tendríamos ningún problema ni de privacidad, ni de seguridad en internet. Las cosas personales son, como la misma palabra indica, "personales", "privadas", y no para ser publicadas en un tablón de internet a la vista de todo el mundo como si de un anuncio se tratara.

Los **despidos del trabajo por comportamientos inadecuados en las redes sociales** aumentan día a día, debido a que las empresas están cada vez más pendientes de lo que sus empleados o candidatos publican en ellas, por cuestión de **imagen y reputación** pero también de **seguridad. [13]**

La seguridad y privacidad en la red social, empieza por nosotros, por los contenidos que subimos y los permisos que otorgamos.

Las redes sociales seguirán innovando, creando nuevos diseños, pero esperemos que también se centren mucho en la seguridad, y sobre todo, la privacidad de sus usuarios.

Bibliografía:

Material de apoyo: Privacy and Security for Online Social Networks: Challenges and Opportunities.

[2] R. Gross and A. Acquisti, "Information Revelation and Privacy in Online Social Networks," Proc. WPES '05, Alexandria, VA, Nov. 2005.
[3] ENISA, "Security Issues and Recommendations for Online Social Networks," Position Paper, Nov. 2007.
[4] Noveria: http://blog.noveria.es/2009/12/12/seguridad-en-el-famoso-sistema-de-aplicacion-tuenti/
[5] http://en.wikipedia.org/wiki/Social_network_service
[6] http://www.softzone.es/2010/05/14/facebook-identifica-al-hacker-que-hackeo-15-millones-de-cuentas/
[7] http://www.softzone.es/2010/07/27/facebook-testea-un-boton-para-que-puedas-borrar-tu-cuenta/
[8] http://www.adslzone.net/article4724-facebook--las-fotos-siguen-visibles-incluso-despues-de-borrarlas.html
[9] http://www.tgdaily.com/security-features/49522-new-privacy-hole-in-facebook-makes-zuckerbergs-party-plans-public

[10] http://www.elmundo.es/elmundo/2010/10/07/navegante/1286442192.html
[11] http://seguridadredessociales.wordpress.com/2010/06/01/a-facebook-y-tuenti-no-se-les-aplican-las-mismas-normas-legales/

[12] http://seguridadredessociales.wordpress.com/2010/06/05/facebook-entrego-datos-personales-de-sus-usuarios-a-anunciantes/

[13] http://seguridad-redes-sociales.blogspot.com/2010/09/descuidos-en-las-redes-sociales-que.html
[14] http://www.configurarequipos.com/actualidad-informatica/2191/diaspora-una-red-social-p2p

Sergio de Luz para www.redeszone.net