Seguridad y Prívacídad a partir de la Ubicación Geográfica de Dispositivos iOS

Castro Sotis, Daniel Andrés

2012

Universidad de Buenos Aires
Facultades de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática
Trabajo Final

Tema
Geolocalización

Título
Seguridad y Privacidad a partir de la Ubicación Geográfica de Dispositivos *iOS*

Autor:
Daniel Andrés Castro Solis

Tutor:
Antonio Millé

Cohorte: 2011
Julio de 2012

DECLARACIÓN JURADA DE ORIGEN DE LOS CONTENIDOS

"Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y que se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual".

Daniel Castro S.

Daniel Andrés Castro Solis
Ingeniero de Sistemas
DNI: 94.800.621
Ciudad Autónoma de Buenos Aires - Argentina

RESUMEN

El presente trabajo contiene un análisis de seguridad y privacidad de la posibilidad de obtener, almacenar y distribuir la posición geográfica de una persona o *recurso,* a través de un dispositivo móvil en general y en particular para los dispositivos *iOS*[1] *4.x* de *Apple Inc.*

Para la elaboración de este trabajo fue necesario entender la geolocalización en dispositivos móviles estudiando algunas aplicaciones para conocer el funcionamiento de las mismas y verificar la manera en que éstas protegen al usuario, adicional a esto se estudio la técnica de *geo-tagging* y se evalúo también las implicaciones de seguridad y privacidad de dar a conocer la ubicación geográfica, analizando: mecanismos de obtención de esta información, modalidades actuales de ataque mostrando además algunos casos reales de este tipo de victimas. Todo esto permitió elaborar una propuesta de las configuraciones adecuadas para el manejo de la información de geolocalización y así mitigar los riesgos asociados al hecho de hacer pública nuestra localización. Al final se exponen las conclusiones del trabajo realizado.

Palabras Clave: Seguridad, Privacidad, Geolocalización, Geo-etiquetado (*Geo-Tagging*), Dispositivos *iOS*.

[1] **Dispositivos iOS:** Conjunto de dispositivos MAC con sistema operativo *iOS 4.x* de la compañía *Apple Inc*, entre los cuales se destacan: *iPhone, iPod Touch, iPad.*

CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

INTRODUCCIÓN

La mayoría de los dispositivos móviles existentes en el mercado proporcionan al usuario la posibilidad de Geolocalización es decir de conocer y dar a conocer su ubicación geográfica actual, digo posibilidad porque es una opción del dispositivo que se puede habilitar o deshabilitar a consideración del usuario. La geolocalización particularmente en dispositivos *iOS 4.x* esta inmiscuida en configuraciones de los dispositivos y de aplicaciones web, en sistemas GPS[2] y en diferentes aplicaciones que hacen uso de internet.

Existen muchas aplicaciones que requieren conocer la ubicación actual del dispositivo para su correcto y óptimo funcionamiento entre ellas las de captura de fotografías y videos que registran la ubicación donde fueron creados, mapas de localización, entre otras. En cuanto a aplicaciones web se destacan las redes sociales que utilizan el sistema de geolocalización para incluir esta información en el perfil del usuario y registrar toda su actividad en la red asociada a su ubicación, además de estos muchos otros sitios están incorporando la ubicación del usuario como un dato más que se puede aprovechar para muchos fines, como pueden ser: búsqueda de información más útil para el usuario, proporcionar información turística, guías hoteleras y de restaurantes, carteleras de cine, clasificados, pronóstico del tiempo, publicidad en general, e incluso como mecanismo de autenticación de origen y de autenticación de usuarios, etc. [6] Sin embargo en la actualidad se está usando también en situaciones donde la seguridad y privacidad de los usuarios se ve amenazada.

El objetivo de éste documento es establecer un análisis de las implicaciones de seguridad y privacidad para usuarios que conscientemente o no dan a conocer su ubicación geográfica, y de esta forma proponer un modelo de configuraciones para la funcionalidad de geolocalización, donde el usuario determine de forma sensata cuándo, dónde y hasta qué punto dar a conocer su localización y con esto mitigar el riesgo de ser víctimas de un

[2] **GPS**. Sistema de Posicionamiento Global (*Global Positioning System*). Sistema satelital que permite la geolocalización de objetos en la superficie terrestre con gran precisión. [2]

ataque a nuestra privacidad originado por el conocimiento de nuestra ubicación.

Para el cumplimiento de éste objetivo fue necesario documentarse y entender la técnica de *geo-tagging* inmersa en este tipo de dispositivos, analizar aplicaciones existentes que basan su funcionamiento en la posición geográfica del usuario y otras que permiten obtener la ubicación a partir de la actividad de los usuarios en las redes sociales, estudiar algunos de los mecanismos usados para vulnerar la privacidad a partir del conocimiento de esta información, comprender los riesgos asociados a la localización y así mismo dar a conocer algunos formas de cómo mitigar dichos riesgos.

El documento está estructurado de la siguiente manera: En el primer capítulo contiene definiciones y características de geo-etiquetación o *geo-tagging* y mecanismos para geo-etiquetar archivos digitales. En el segundo capítulo se analizan ejemplos de aplicaciones que usan geolocalización así como también herramientas que permiten extraer coordenadas de localización de archivos digitales. El tercer capítulo muestra un análisis de seguridad y privacidad de la geolocalización, analizando los riesgos asociados y formas para mitigarlos. El capítulo cuarto contiene una propuesta de configuraciones para la geolocalización tanto para los dispositivos móviles como para sitios que hagan uso de la ubicación geográfica y de esta manera mitigar los riesgos asociados al conocimiento de esta información. Finalmente se presentan algunas conclusiones.

SEGURIDAD Y PRIVACIDAD A PARTIR DE LA UBICACIÓN GEOGRÁFICA DE DISPOSITIVOS IOS.

1. *GEO-TAGGING*

En este capítulo se estudia la Geo-etiquetación o *Geo-Tagging* como técnica que permite incorporar la ubicación geográfica en archivos multimedia, si bien ayudara a entender mas sobre ella en capítulos siguientes se profundizara en situaciones en las cuales la privacidad de los usuarios está en riesgo ya sea de forma consciente o inconsciente y en los mecanismos que pueden a ayudar a mitigar dicho riesgo. Si bien el trabajo incluye otros objetivos, esta parte ofrece las bases necesarias para un posterior análisis de las amenazas de seguridad y privacidad del usuario junto con los riesgos asociados al conocimiento de su ubicación geográfica; en segunda instancia ayudara el proceso de *awareness* (concientización) de los usuarios para que entiendan la magnitud del problema antes de que ocurra una mayor proliferación. [4]

Como se mostrara a lo largo de éste documento el geo-etiquetado claramente tiene el potencial de impulsar una nueva generación de servicios personalizados de gran utilidad, sin embargo se debe encontrar el punto de equilibrio que determine hasta donde es adecuado ofrecer la geolocalización sin alterar nuestra privacidad y seguridad. [4] Para entender el geo-etiquetado considero necesario estudiar en general los metadatos para luego ahondar en las etiquetas de geolocalización.

1.1. Metadatos de Archivos Digitales

En la mayoría de los contextos los metadatos se suelen definir en la mayoría de los contextos como “datos sobre datos” o "datos de los datos", es decir datos que describen, caracterizan o proporcionan información acerca de otros datos con el propósito de identificarlos y referenciar de manera estandarizada cualquier información de recursos digitales y no digitales. [14][15]

En archivos digitales, los metadatos pueden ser: titulo, autor, fecha y hora de creación, etc. y adicionalmente en archivos geo-etiquetados el lugar de creación, representado como latitud, longitud, y en ocasiones altura. Este tipo de información permite un acceso rápido y estructurado logrando búsquedas optimas con criterios variables, particularmente para archivos geo-etiquetados facilitan la búsqueda ordenada y rápida a través del filtrado del lugar donde se crearon. Entre sus características están:

- Facilitan recuperación, autentificación, evaluación, preservación, publicación, comprensión y/o interoperabilidad de información. [14]

- Refinación de consultas a buscadores. Es decir, si se usa información adicional se obtiene resultados más precisos, rápidos y con menos cantidad de filtros.

- Presentación variable de datos. Si hay metadatos, un programa puede seleccionar la forma de presentación más adecuada de los datos (táctil o leída). Además a través del análisis de los metadatos se puede localizar, enfocar y ampliar automáticamente personas u objetos dentro de las imágenes.

Los metadatos de geolocalización potencian sustancialmente las capacidades de localización, recuperación y búsquedas asociadas al lugar, sin embargo pueden suponer un riesgo para la privacidad mediante el almacenamiento de información inesperada que no sea evidente al abrir un documento. El *geo-tagging* utiliza registros EXIF[3] para asociar lugares en archivos digitales, los cuales incluyen las coordenadas geográficas. [4]

1.2. Geo-etiquetado. Definición y Características

En esta parte se hablara en primera instancia de manera muy general de geolocalización para luego entender el *geo-tagging* como técnica que permite geolocalizar recursos digitales y dispositivos.

[3] *Exchangeable Image File Format.* Formato de archivo de imagen intercambiable.

La **Geolocalización:** Permite conocer nuestra ubicación geográfica automáticamente teniendo o no una conexión a internet, debido a que los dispositivos móviles actualizan constantemente nuestra ubicación, por su portabilidad. [5] "La geolocalización en términos simples es la práctica de asociar un recurso digital con una locación física. ...La información del lugar se calcula con base a coordenadas de latitud y longitud para marcar un lugar específico en cualquier parte del mundo." [7]

El **geo-etiquetado** o ***geo-tagging***, establece una relación entre la creación de archivos digitales y el lugar de creación. Es decir es el mecanismo mediante el cual se añade a los metadatos (*EXIF*) del archivo la localización geográfica donde se creó. Se define a través de coordenadas que incluyen longitud y latitud donde fue creado el archivo multimedia, aunque también puede incluir la altitud, nombre del lugar, código postal, etc. para posteriormente hallar sus coordenadas geográficas. [4][8]

El *geo-tagging* puede ocurrir en el mismo momento de la creación del archivo de forma automática o después mediante software que permite integrar a los metadatos del archivo las coordenadas que se obtuvieron de forma independiente con un receptor GPS, generalmente externo al dispositivo móvil. [8]

Por lo tanto la posibilidad de geo-etiquetado está determinada por la presencia de una entidad que obtenga la ubicación geográfica aproximada del dispositivo móvil, en la actualidad esta característica está integrada en la mayoría de los dispositivos que ofrece el mercado. Para obtener la posición dicha entidad puede utilizar o no un receptor GPS, utilizar las antenas de telefonía celular para tal fin, tomar como referencia los puntos de acceso a *WiFi* o utilizar una combinación de todas o algunas de las opciones anteriores para mayor precisión. Esta parte se detalla más adelante.

Las principales características de la geo-etiquetación son:

- Permite una búsqueda organizada y personalizada, generando en tiempo real resultados que se originan en un determinado lugar; así como también la localización de la misma en un mapa con total

precisión, redes como *Flickr*, *YouTube*[4] y *Twitter*[5], ofrecen esta funcionalidad. Además, archivos digitales que tengan la ubicación, fecha y hora de creación se pueden fácilmente agrupar de forma automática e incluso encontrar nuevos archivos en línea de otros que han visitado el mismo lugar. [4][2]

- Facilita el analizar de metadatos con la ayuda de herramientas, librerías estándar, *plugins* del navegador, entre otros; una de estas herramientas es el programa *Preview* de *Apple* que permite buscar geo-etiquetas y así brindad un acceso directo e interacción con otras aplicaciones como *Google Maps*. [4]

- Permite brindar servicios de geolocalización, es decir actualmente existe gran cantidad de sitios que recolectan, analizan y suministran información de localización geográfica, para posteriormente prestar un servicio. Entre los servicios se destacan: El que ofrecen redes sociales como: *Foursquare*[6], *YouTube*, *Twitter*, que permiten hacer búsquedas relacionadas con lugares, ofrecer servicios personalizados de publicidad, o para ser parte de enormes bases de datos que permitan encontrar y combinar información de distintas fuentes. [4]

- Debido a que la geo-etiquetación permite vincular datos de localización geográfica a contenidos digitales (imágenes, videos, documentos, etc.), logra un impacto en la comunicación relacional. En fotografías digitales permiten conocer su ubicación geográfica; mientras que en el caso de mensajes de texto, se puede llegar a conocer el origen del mensaje lo cual con ciertas adaptaciones podría ser útil como mecanismo de autenticación de origen. [10]

  Otra característica de la geolocalización es que proporciona muchas aplicaciones prácticas, a considerar: **En el ámbito personal**, se utilizan

[4] Sitio oficial: http://youtube.com/
[5] Sitio oficial: http://twitter.com/
[6] Sitio oficial: http://foursquare.com/

en actividades relacionadas con el ocio, que van desde las redes sociales (tradicionales como *Facebook*[7], o específicas como *Foursquare*) hasta la navegación GPS, trazado de rutas en mapas, senderismo, realidad aumentada, obtención de rutas de navegación en automóvil con información de tráfico en tiempo real y sincronización automática de puntos de interés mediante almacenamiento en la nube, etc. **En el ámbito profesional y empresarial**, hay aplicaciones que van desde la seguridad (localización de vehículos, aplicación de geolocalización a seguros de automóviles, etc.) hasta estudios de mercado. [2] Más beneficios para las empresas se encuentran en: [18] y [19]

1.3. Componentes de la Geolocalización

Entre los componentes de la geolocalización se distinguen:

- **Hardware**, Plataforma donde se lleva a cabo la geolocalización, en éste caso particular un dispositivo móvil, sin embargo puede ser un computador, un navegador GPS, una cámara de fotografías, etc. Algunos de estos dispositivos necesitan incorporar un receptor GPS. [2]

- **Software**, Encargado de ejecutar la geolocalización sobre el sistema operativo (concretamente *iOS 4.x.*) del dispositivo y junto con el hardware permite buscar información y localizaciones geográficas. Este componente soporta las aplicaciones y herramientas *on-line* que proporcionan servicio de geolocalización. [2]

- **Conexión a Internet**, "Medio de obtención e intercambio de información y, en ocasiones, sistema de almacenamiento y procesamiento de la misma si es en un sistema *Cloud Computing.* Excepcionalmente, pueden ejecutarse procesos de geolocalización sin una conexión a Internet (*off-line*), cuando los datos necesarios están cargados con antelación en la memoria del dispositivo" o si se utiliza otro mecanismo como *Wi-Fi* o telefonía celular para obtener la información geográfica. [2]

[7] Sitio oficial: http://www.facebook.com

1.4. Mecanismos de Geo-etiquetado de Archivos Digitales

Debido a las avanzadas funcionalidades incorporadas por los *Smartphone*, en la actualidad equipos como el *iPhone* de *Apple* y otros modelos de los principales fabricantes pueden obtener la posición exacta o muy aproximada del dispositivo en cualquier punto del globo terrestre y cargar instantáneamente fotos geo-etiquetadas, videos, e incluso mensajes de texto a redes sociales. Otra fuente de datos de ubicación son las numerosas *start-ups* o mensajes emergentes de internet que basan su negocio en la expectativa de que los usuarios instalan aplicaciones en sus dispositivos móviles de forma continua y reportan la información de su ubicación actual a los servidores de la empresa. [4][5][6] Las tecnologías más utilizadas para obtener datos de geolocalización son:

- **Receptor GPS Integrado:** A través de la red de satélites GPS, se puede geolocalizar un dispositivo con una precisión de entre 1 y 15 metros, generalmente 3 metros; para lo cual es necesario un receptor GPS, por lo que la tecnología los incorpora en los dispositivos móviles. En la actualidad por ejemplo, las nuevas cámaras vienen con funcionalidad GPS o permiten incorporarlo. Del mismo modo, los teléfonos de gama alta disponen de GPS integrado, incluyendo el *iPhone*, los dispositivos basados en *Android* y otros sistemas operativos. [4][2]

- ***Wi-Fi* – Triangulación[8] de Torres Celular:** Método alternativo no tan preciso para determinar la ubicación que mediante la correlación de la intensidad de la señal con lugares conocidos permite a un usuario o servicio calcular las coordenadas del dispositivo. [4][5] La cobertura y la actualización de las bases de datos determinan su funcionamiento, aportando una precisión proporcional al alcance de la red, que oscila entre 30 y 100 m en redes *Wi-Fi* y de 50 a 500 m en redes de telefonía móvil. [2]

[8] *Triangulación.* Es un método geométrico que permite determinar de forma precisa la posición de un objeto desconocido, usando como referencia la posición de varios puntos conocidos. [2]

- **Dirección IP.** No es un mecanismo de geolocalización valido porque es demasiado impreciso, debido a que utiliza el registro de distribución de direcciones IP a proveedores de servicios de internet más no a los clientes como tal. [2]

- **De forma Manual:** Si un dispositivo no geo-etiqueta directamente sus archivos multimedia, la información geográfica también se puede añadir en el post-procesamiento, ya sea mediante la correlación de marcas de tiempo grabadas con un receptor GPS manual, para lo cual existe gran cantidad de software o utilizando un mapa o software de cartografía. Tener en cuenta que geo-etiquetar es insertar en los metadatos las coordenadas y no asociar a los archivos unas coordenadas, por ejemplo al *Tweettear* con una imagen, donde esta adoptaría las coordenadas del lugar donde se hizo el *post* y no de donde se tomo la fotografía. [4][8]

De los mecanismos para geo-etiquetado el más cómodo y utilizado desde mi punto de vista es a través de un dispositivo móvil que disponga de la funcionalidad de geolocalización, que tenga un receptor GPS integrado o que a través de algún otro mecanismo de localización permita obtener la ubicación aproximada y vincularla a los archivos de video, fotos, texto, audio al momento de crearlos o a las publicaciones en las redes sociales; en la mayoría de estos dispositivos el proceso de asociación de la ubicación es automática y el proceso es bastante sencillo, basta con que la opción de localización esté habilitada. [8]

Por ejemplo, *iPhone:* incorpora con alta precisión coordenadas geográficas en fotos, videos y publicaciones hechas con el dispositivo y además permite que las aplicaciones dispongan de esta como un dato más para ofrecer un servicio, a menos que la funcionalidad se desactive. Su exactitud incluso supera a la del GPS, puesto que el dispositivo determina esta posición en combinación con la triangulación de torres celular. [4]

2. APLICACIONES DE GEOLOCALIZACIÓN

Este capítulo está dedicado a la obtención de algunas características de las diferentes configuraciones que utilizan las aplicaciones de geolocalización en general, y así poder hacer un análisis de las mismas para plantear una serie de recomendaciones de seguridad y privacidad, teniendo en cuenta que dichas aplicaciones por su extensión y demanda llevan asociada la problemática de la naturaleza de la información frecuentemente privada o sensible. Por ello, es importante tomar especial consciencia de estos aspectos para que sea posible ejercer un uso responsable y de pleno disfrute de las aplicaciones y herramientas de geolocalización en dispositivos móviles. [2]

2.1. Geolocalización en Dispositivos iOS

Muchos usuarios saben que compartir información sobre la ubicación tiene implicaciones para su vida privada, y por lo tanto los fabricantes de dispositivos y servicios en línea suelen ofrecer diferentes niveles de protección para controlar si, y algunas veces con quién, uno quiere compartir este conocimiento. Sin embargo, muchos otros desconocen que sus archivos contienen información sobre la ubicación. [4]

Por una parte está la configuración del dispositivo móvil donde el usuario decide si desea geo-etiquetar sus archivos, los *post* en redes sociales, y si quiere que las aplicaciones de geolocalización dispongan de su ubicación geográfica para prestarle sus servicios. Y por otra parte está la configuración de seguridad y privacidad de las aplicaciones *on-line* y las aplicaciones de los dispositivos que usan datos de localización. Por lo tanto la configuración referente al dispositivo permite decidir si los archivos contienen datos de geolocalización y las configuraciones de sitios y aplicaciones están orientadas al hecho de que si esa información se hace pública o no.

Acerca de las configuraciones disponibles en los dispositivos móviles se podría decir que en la mayoría de los sistemas operativos la

geolocalización viene habilitada por defecto, sin embargo permiten desactivarla de dos maneras: Primero se puede evitar que la aplicación de la cámara geo-etiquete videos e imágenes y segundo se puede evitar la localización completa a través del GPS en todas las aplicaciones. Además algunos sistemas solicitan confirmación cada vez que se desee acceder a la información de localización. [4][12]

En dispositivos *iOS 4.x* (*iPhone, iPad, iPod* principalmente) que son objeto de estudio de éste trabajo, la geolocalización está activa por defecto y se puede desactivar, en general para todas las aplicaciones o para algunas en especifico, las cuales preguntarán la primera vez que se accede a ellas, si se desea habilitar ésta funcionalidad y así minimizar la publicación de datos privados del usuario. El proceso para desactivar la función de localización en los dispositivos *iOS 4.x* (En versiones anteriores el proceso es diferente), sigue los siguientes pasos: Ingresar a *Ajustes, General, Localización* y elegir si desactivar esta funcionalidad completa para todas las aplicaciones o para alguna en particular. [12]

Figura 1. Pasos para desactivar la localización en dispositivos *iOS 4.x.*

La configuración de la geolocalización tiene muchas limitaciones a considerar:

- No son bastante intuitivos para que los usuarios menos osados conozcan y sean conscientes de las configuraciones y de que pueden estar publicando su ubicación geográfica.

- Solicitan confirmación de activación únicamente la primera vez que se inicia la aplicación, las siguientes veces se da por hecho la utilización de la geolocalización en la aplicación.

- Presentan inconvenientes al desactivarla por completo, pues funcionalidades como GPS también podría quedar desactivado, que en la mayoría de los casos no tiene que ver con la problemática de compartir la localización.

En cuanto a sitios geosociales, sitios de comercio electrónico, *blogs* de cualquier tipo y otros que permiten hacer *post's* con inclusión de imágenes o videos, proveen a los usuarios una opción de configuración de privacidad, cuyas opciones, y sus valores por defecto pueden diferir. *YouTube*, por ejemplo, utiliza geo-información por defecto de los vídeos subidos, mientras que *Flickr* requiere expresamente habilitar la opción (*opt-in*), *Facebook* realiza un proceso que elimina las geo-etiquetas antes de subirlas a su sitio, *Twitter* si mantiene las geo-etiquetas pero solicita al usuario que configure las opciones de privacidad, para que establezca si desea hacer pública su localización. Tratando de sacarle más provecho a la geolocalización sitios como *Foursquare* trataron de utilizarla para autenticar (identificando usuarios que actualmente no están es sus casas), sin embargo genero muchos problemas asociados a la privacidad de los usuarios. [4]

2.2. *Aplicaciones para Dispositivos iOS*

En la actualidad para una persona publicar información que tenga su ubicación geográfica es bastante sencillo, tanto que en ocasiones se hace de forma automática y sin conocimiento de ello. Esto ocurre principalmente por dos razones: los dispositivos móviles y las aplicaciones de geolocalización; los primeros debido a su penetración en el mercado, los múltiples mecanismos, como ya se vio, que permiten la localización geográfica del dispositivo, desarrollo de la banda ancha móvil, capacidad de procesamiento elevado, entre otras, que generaron el desarrollo de gran

cantidad de aplicaciones en general y otras especificas para geolocalización que se adaptan a los recursos y características del dispositivo.

Entre las aplicaciones de geolocalización más destacadas están aquellas que permiten integrar prácticamente cualquier tipo de información geográfica en las populares redes sociales: *Facebook, Twitter* o *Tuenti*[9], etc. y en las más recientes, las llamadas redes sociales de geolocalización: *Foursquare, Gowalla*[10], entre otras. [2]

A continuación, se describen, clasifican y analizan aplicaciones que incorporan geolocalización, con el propósito de estudiar las configuraciones de geolocalización a nivel de dispositivo, aplicación o sitio geosocial. La mayoría de éstas están disponibles para diferentes sistemas operativos como: *Android* de *Google*, *Blackberry* de RIM, *Windows Mobile* y *Windows Phone* de *Microsoft,* para todos o para algunos de ellos, sin embargo todas están disponibles para dispositivos *iOS* de *Apple* [2]

2.2.1. Aplicaciones con funcionalidad de Geolocalización.

En esta categoría se engloban las aplicaciones que haciendo uso de la funcionalidad de geolocalización prestan un determinado servicio a los usuarios de dispositivos móviles, a partir del conocimiento de su ubicación geográfica. Se pueden distinguir principalmente tres categorías: Aplicaciones que incorporan la localización del usuario en imágenes y permiten buscar imágenes geo-etiquetadas, aplicaciones que utilizan la localización del usuario para mostrarle los sitios de interés (restaurantes, tiendas, zoológicos, museos, etc.) cercanos a su ubicación y por último las aplicaciones de búsqueda de información en mapas. [2]

En las siguientes tablas se muestra un listado de las aplicaciones más representativas en cada categoría con una breve descripción de su funcionalidad. La mayoría de las aplicaciones se tomaron del *App Store* de *iTunes* de *Apple,* donde se puede encontrar muchas otras aplicaciones. [31]

---

[9] Disponible en: http://sitios.tuenti.com
[10] Disponible en: http://gowalla.com/

- Geo-etiquetado de Imágenes

Aplicación	Funcionalidad
Google Street View	Visualizar panorámicas de calles en *Google Maps* y *Google Earth*.
Street Slide	Visualizar panorámicas de calles en *Bing Maps*.
360 Panorama	Permite tomar panorámicas y postearlas en las redes sociales. [31]
Panoramio	Compartir fotografías geo-etiquetadas. Pertenece a *Google*.
Flickr[11].	Buscar y publicar fotografías geo-etiquetadas.
Instagram	Permite buscar y compartir fotografías, se integra con las redes sociales. [31]

Tabla 1. Aplicaciones de Geo-etiquetado de Imágenes. [2][31]

- Puntos de interés

Aplicación	Funcionalidad
Bliquo. "Buscador de ocio urbano"	Permite consultar, comentar y evaluar directorios especializados de restaurantes, discotecas, bares, etc., [2]
Google Places Directory.	Búsqueda de puntos de interés de *Google* que se integra con *Google Maps*. [2]
Blink Hotels, iHotel	Permite buscar y reservar hoteles, con el mejor precio. [31]
TVtrip GUIDE	Proporciona información de diversos puntos de interés, incluyendo además realidad aumentada y mapas offline. [31]
AroundMe, Where M.I, Where, Buzzd.	Proporcionan información de diversos puntos de interés.

Tabla 2. Aplicaciones para buscar puntos de interés. [2][31]

- Mapas y Navegación GPS

Aplicación	Funcionalidad
Google Maps, Google Earth.	Servicios del sistema de información geográfica de *Google*, incorpora guía turística e imágenes 3D. [31]
Map My Tracks.	Servicio de Mapas y Navegación GPS que permite grabar recorridos geo-localizados, e integrarlos en otros servicios y redes sociales. [2]
Plan de Ruta	Permite planificar un viaje en coche o a pie marcando puntos de interés. [31]

[11] Disponible en: http://www.flickr.com/

TomTom Navigator y TomTom Places	Navegador GPS que soporta varios idiomas, mapas para distintas zonas geográficas, puntos de interés personalizados, y datos de tráfico en tiempo real. [2]
Galileo Offline Maps	Colección de mapas online con *caching* que guarda los mapas que se han visto, dejándolos disponibles cuando no se tiene conexión. [31]
Google Maps Navigator	Navegación GPS integrada con mapas y funcionalidades de *Google Maps*, que facilita información de tráfico en tiempo real. [2]
Waze	Navegación GPS con información colaborativa de tráfico e incidencias en la carretera. [2]

Tabla 3. Aplicaciones de Mapas y Navegación GPS. [2]

2.2.2. *Aplicaciones para Geolocalizar Dispositivos iOS*

Aplicaciones que permiten ubicar dispositivos móviles de forma remota en tiempo real, para lo cual es necesaria cierta información del dispositivo móvil o del usuario.

- ***FootPrints.*** Permite saber la ubicación exacta o muy aproximada de donde se encuentra un determinado dispositivo móvil y por ende su usuario, se puede utilizar por ejemplo para localizar a nuestros hijos o averiguar la posición de un grupo de amigos. *FootPrints*, envía la información de la localización geográfica del dispositivo a otro configurado como nodo central, de forma constante, sin consumir excesiva batería y a través de una configuración sencilla. [20]

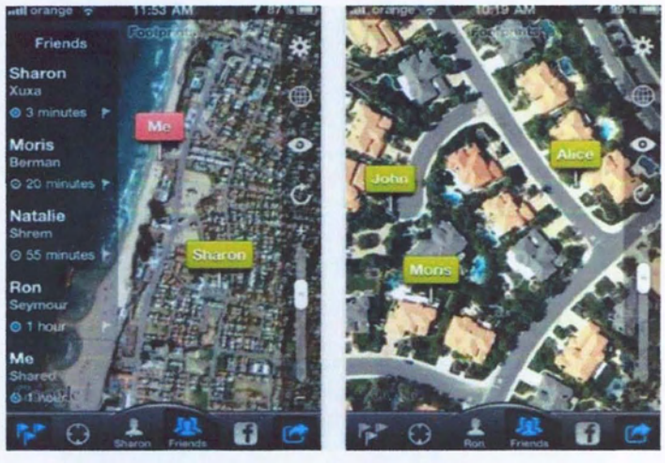


Figura 2. Capturas de *FootPrints*. [20]

- **Buscar mi *iPhone*.** De *Apple*. Aplicación que ayuda a encontrar dispositivos móviles y a proteger los datos desde cualquier otro dispositivo *iOS*. La aplicación es gratuita, de fácil instalación y configuración que requiere del ID de Apple para conectarse. Necesita ser instalada en mínimo dos dispositivos para a través de uno localizar al otro dispositivo *iOS*. *Buscar mi iPhone* utiliza un mapa para informar la localización del dispositivo, permite mostrar mensajes o reproducir sonidos, además permite bloquear remotamente el equipo o todos los datos. [31]

Figura 3. Busca mi *iPhone*. Fuente: sitio oficial *iTunes* de *Apple*. [31]

2.2.3. Redes sociales y Geosociales

Aplicaciones sociales que además de permitir establecer vínculos entre personas facilitan a los usuarios localizar en tiempo real a las personas de una misma red en una zona determinada y, además, combinar esos datos con servicios comerciales. Actualmente existen muchas redes sociales que van desde las más tradicionales como *Facebook* o *Twitter* hasta las específicas para móviles (*Foursquare*) basadas en geolocalización. [2][27][29]

Estos son algunos ejemplos de aquellas que usan exhaustivamente o adaptan sus funcionalidades a este tipo de tecnología con el fin de ofrecer nuevos servicios a sus usuarios: [13]

Red Social	Objetivo	En Español?
Foursquare	Recomendar lugares a los que se asiste físicamente	No
Facebook	Interactuar entre miembros de la red compartiendo además su ubicación.	Sí
Twitter	Ubicar mensajes de texto en el lugar en que se escribieron	Sí
Gowalla	Compartir lugares, eventos y rutas a los que se asiste físicamente, similar a *Foursquare*.	No
Yelp	Almacenar y compartir nuestros locales favoritos	No
Google Buzz	Ubicar mensajes de texto en el lugar en que se escribieron	Sí
Google Latitude	Monitorizar y compartir nuestra posición en tiempo real	Sí
Ipoki	Monitorizar y compartir nuestra posición en tiempo real	Sí
Tuenti sitios	Almacenar y compartir nuestras zonas de ocio favoritas	Sí

Tabla 4. Ejemplos de redes sociales basadas en Geolocalización para dispositivos móviles. [13]

A continuación se detallan algunas configuraciones y observaciones sobre la seguridad y privacidad que ofrecen a sus usuarios algunas de ellas.

- ***Foursquare.*** Plataforma social móvil basada en la geolocalización, que permite a sus usuarios compartir el lugar en donde se encuentra físicamente con sus amigos, haciendo *check-ins* (acción de indicar el lugar en dónde se está físicamente) a través de la aplicación o SMS de un teléfono inteligente con conexión a Internet y GPS, mientras ganan puntos, *badgets* (insignias) virtuales y concede al usuario el título de "mayor" de aquella ubicación que más frecuente. [27][29][16]

  Su funcionalidad clave es permitir conocer cuáles son los lugares (monumentos, tiendas, restaurantes, bares, museos, iglesias etc.) más visitados por los integrantes de la red social y qué opiniones y recomendaciones se hicieron sobre los mismos; convirtiéndose en una guía de experiencias en determinados lugares del mundo real; donde sus usuarios pueden encontrar información sobre lugares que desean visitar y ver sugerencias pertinentes sobre lugares cercanos.

Transformándose también en una poderosa herramienta de marketing para los negocios. [27][28][29]

El objetivo es fidelizar a sus clientes a través de promociones por el uso de la red. En [19] se detallan los beneficios que ofrece *Foursquare* a empresas.

- ***Facebook.*** Es la red social más utilizada por la mayoría de la gente, tiene la base de datos de usuarios más extensa de todas e incluye múltiples servicios como fotos, videos, círculos de amigos, eventos, juegos, aplicaciones, chat... [3] Aunque desconocido para muchos usuarios esta red ofrece gran cantidad de controles de seguridad los cuales pueden ayudar a combatir intromisiones no deseadas. El problema es implementar estas opciones de privacidad, pues pueden resultar muy confusas para personas no familiarizadas con la tecnológica o las aplicaciones disponibles para dispositivos móviles no cuentan con ellas dado que se someten a las configuraciones de seguridad y privacidad de la cuenta que el usuario establezca en el sitio oficial de la red. Las opciones de configuración que incluye son: [9][24]

  - ✓ **Cambiar la visibilidad del perfil**. Impide que cualquiera tenga acceso a nuestros datos. Estableciendo diferentes formas de hacerlo, desde el momento de la publicación se establece: quién podrá ver e interactuar con cierta información; las opciones de geoposicionamiento por las cuales nuestros amigos pueden etiquetarnos en sitios en los que hemos estado; también se puede controlar la visibilidad de nuestro perfil en los buscadores y evitar que los *bots* de búsqueda lo indexen. La visibilidad se puede establecer tanto para aplicaciones que se utiliza y aplicaciones de amigos ya que pueden acceder y utilizar nuestra información. [9][24]

  - ✓ **Elegir la privacidad de tu muro:** Sirve para regular quien puede ver nuestras publicaciones y fotografías, impedir que aparezcamos etiquetados en publicaciones solicitando nuestra aprobación para

hacerlo. Además se puede establecer quién puede hacer publicaciones en nuestro muro. [9]

- ✓ **Organizar los contactos:** Permite organizarlos en listas, para otorgar privilegios sobre nuestra cuenta a grupos de amigos. Este paso, aunque no es el más rápido, es bastante simple y será muy útil, pues se puede establecer el nivel de privacidad de los grupos (cerrado, abierto o secreto), compartir nuestras publicaciones únicamente con ciertos grupos que nosotros decidamos y además se puede filtrar las publicaciones que aparecen en la página de inicio seleccionando el grupo del que queremos ver las publicaciones en cada momento. [9][24]

- ✓ **Bloquear un contacto:** Permite ocultar ciertas publicaciones de amigos que no nos interesan de forma totalmente imperceptible para el usuario silenciado, podemos ser más drásticos y bloquear o eliminar al usuario de nuestra lista, y además podemos bloquear las invitaciones de aplicaciones o a eventos, y bloquear una aplicación. [9]

Inmersa en *Facebook* se encuentra ***Facebook Places***[12], que permite compartir la posición del usuario en tiempo real con sus amigos a partir de la geolocalización de dispositivos móviles; los usuarios pueden añadir lugares a sus visitas, favoreciendo el enriquecimiento del contenido de la comunidad a través de la participación. Además tiene plena integración con su red social principal, *Facebook*, lo que hace que se convierta en una herramienta ideal para aquellos usuarios que deseen disfrutar de la misma experiencia que tendrían con *Foursquare*, desde una misma aplicación. [2][29]

[12] Disponible en: http://www.facebook.com/places/

Figura 4. *Facebook Places* inmersa en *Facebook*.

- ***Twitter.*** Más que una red social es un micro blog conectado a una red social donde los usuarios comparten información de diversos tipos e intercambian opiniones sin importar realmente la relación que puedan tener, sin embargo hay datos que conviene manejar con cuidado. [9][3].

  Permite **Configurar la privacidad de la cuenta:** en la que se establece la visibilidad de los datos personales, se protege los *tweets* o publicaciones y se controla la geolocalización. Además permite elegir: si se quiere que nos encuentren por correo electrónico o por el número de teléfono, si elegimos o no mostrar la ubicación en los *tweets*, o si borramos las ubicaciones de *tweets* antiguos, si utilizamos o no una conexión segura a través del protocolo *HTTPS* y también al igual que otras redes sociales permite bloquear a un *follower* o seguidor y dar de baja aplicaciones. [9]

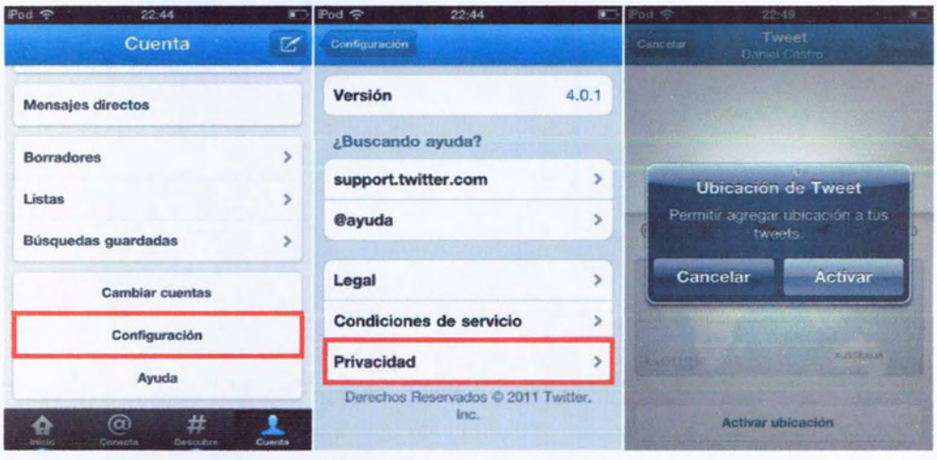


Figura 5. Configuraciones de Seguridad y Privacidad de *Twitter*.

La red social *Twitter* tiene inmerso a ***Twitter Places***[13], que haciendo uso de la funcionalidad de geolocalización o especificación explícita (el usuario ingresa su ubicación) permite a los usuarios, definir el lugar exacto asociado a un mensaje concreto. Además se integra fácilmente con las redes sociales *Foursquare* y *Gowalla*. [2]

- ***Google Latitude***[14]. Servicio de geolocalización de *Google* que integra la mayoría de sus servicios. Se trata de una aplicación de manejo sencillo e intuitivo que permite ubicar sobre un mapa a las personas que forman parte de la red de contactos de *Latitude* y así saber dónde se encuentran. Para que un usuario de *Google Latitude* pueda ser localizado deberá tener instalado en su teléfono móvil la aplicación, formar parte de la red de contactos *Latitude* y tener una cuenta en *Google* o en *Gmail.* [2][29]

- ***Youtube.*** Sitio web especializado en la reproducción de videos digitales. Cualquier usuario puede crear un perfil personalizado en *Youtube,* con su propio canal de videos y subir sus videos de manera muy sencilla. Si los videos tienen datos de geolocalización se mantendrán puesto que este sitio no tiene ningún control sobre esta información, ni tiene alertas para informar al usuario de este hecho. [3]

- ***Tuenti.*** Red social española con gran cantidad de usuarios que, funciona mediante invitaciones, es decir, una persona no puede registrarse sin la previa invitación de un usuario de *Tuenti.* Ofrece servicios similares a los que ofrece *Facebook* pero con menos opciones de configuración de privacidad que limita un poco sus posibilidades pero simplifica el proceso. [9][3]

  Entre las opciones más importantes que ofrece están: la visibilidad y accesibilidad al perfil y de la información que decidamos mostrar, nos da también la posibilidad de eliminar o bloquear a amigos, eliminar nuestras

[13] Disponible en: http://support.twitter.com/entries/194473-twitter-places-and-how-to-use-them
[14] Disponible en: http://m.google.com/latitude

etiquetas en fotos ajenas y podemos decidir si no queremos volver a ser etiquetados. [9]

2.2.4. Aplicaciones de Realidad Aumentada

El aumento de la velocidad de transmisión de las redes de telefonía móvil, la capacidad de procesamiento, la popularidad de los dispositivos móviles, han logrado un avance significativo en aplicaciones móviles que haciendo uso de la funcionalidad de geolocalización y de otras tecnologías de detección de movimiento y orientación permiten enriquecer la visión del mundo real, asociando a la visión del usuario, información virtual que se extrae de diversas fuentes de internet. [2]

Si bien esta tecnología está aun en crecimiento, ya existen gran cantidad de aplicaciones que hacen uso de ella, cuya característica fundamental es hacer un compilado de información y combinarla con lo que el usuario está mirando a través de la cámara del dispositivo y de esta forma: aumentar la cantidad de información que él captura, tomar decisiones acertadas en menos tiempo, minimizar riesgos y tiempo al conducir, encontrar lugares lo antes posible, conocer precios sin necesidad de preguntarlos y demás.

Algunas aplicaciones de realidad aumentada para dispositivos *iOS* se muestran en la Tabla 5. Las mismas se tomaron de: [2][30] donde se puede encontrar más información de las mismas.

Aplicación	Funcionalidad
Layar	Compila Información Diversa.
Wikitude	Información de turismo, guías de viaje y navegación paso a paso y demás haciendo uso de Wikipedia
Car Finder	Graba el lugar donde se estaciono el automóvil y ayuda e encontrarlo luego.
Spyglass	Puede servir como brújula y ayuda además a rastrear la ubicación del sol, la luna, etc.
ZipReality Real Estate	Catalogo de precios de viviendas.
Metro Ar	Permite encontrar las estaciones de metro más cercanas.

Tabla 5. Aplicaciones de Realidad Aumentada.

2.3. Problemas de las Aplicaciones de Geolocalización

Según reporte de la firma de seguridad informática ISACA: "Geolocalización: Riesgo, Problemas y Estrategias" casi el 60% de los usuarios de *smartphones* en Estados Unidos utilizan aplicaciones de localización, a pesar de la preocupación que genera la privacidad, así como la seguridad personal. Indicando que las principales inquietudes son el uso de la información por parte de anunciantes para propósitos de marketing, además del riesgo de que otras personas sepan demasiado de sus actividades.

En teoría, La mayoría de las aplicaciones para *smartphones* informan a los usuarios a qué características del mismo accederán una vez instaladas para su funcionamiento y, dependiendo de eso, la descarga o no. Como dicen: bajo su propio riesgo. Sin embargo el estudio "Aplicaciones para *iPhone* y aspectos de privacidad" ha demostrado que, aunque advierten acceder a ciertas características y usar determinada información, en realidad hacen mucho más que eso, por ejemplo enviar a un servidor remoto los identificadores únicos del dispositivo (UDID) en el peor de los casos compartir datos privados de localización e identificación de sus usuarios sin advertirles. El investigador indica que, en algunos casos, el UDID del *iPhone* puede ser utilizado para obtener la identidad del dueño del dispositivo y que también se podría permitir que las páginas web y aplicaciones que visita y utiliza sean monitoreadas. [25]

Según informe de *ESET* muchas de las aplicaciones móviles de las redes sociales almacenan las credenciales de acceso y otra información sensible sin ningún tipo de protección por parte de la aplicación que pueden conllevar serios problemas para la seguridad y privacidad del usuario. La falla se presenta en aplicaciones como: *Facebook, Mobile* de *Dropbox, LinkedIn,* al almacenar la información sensible en un tipo de archivo *plist* sin cifrado. La situación puede ser mas critica si el archivo *plist* se comparte con aplicaciones de terceros que requieren del acceso a esta red social como un software para compartir fotos. El problema es potencialmente peligroso puesto que gente mal intencionada puede aprovechar esta vulnerabilidad y

construir aplicaciones para robar información privada de los usuarios, ya sean aplicaciones móviles para computadores convencionales que se activarán cuando los dispositivos móviles se conecten a éstos. [26]

Además de lo expuesto se puede citar los siguientes inconvenientes de los *sets* de configuración:

- La mayoría de las aplicaciones a nivel del sitio de la red social proporcionan un mayor control de las configuraciones, sin embargo a nivel de las aplicaciones disponibles para dispositivos móviles, estas opciones son bastante dispendiosas o directamente no están como el caso de la aplicación utilizada para *Facebook*, dejando establecida entonces la privacidad y seguridad como en el sitio oficial, aumentando el riesgo de compartir información privada e impidiendo que el usuario sea consciente de la actividad social generara desde su dispositivo móvil.

- Muchas redes sociales incluidas *Twitter y Facebook* establecen determinadas relaciones con aplicaciones de otros fabricantes, por lo cual, si no se configura adecuadamente el acceso a la información personal cada vez que se añada una aplicación se permitirá el acceso a dicha información a la aplicación, sus fabricantes, buscadores, anuncios de publicidad, amigos. A pesar de su gravedad no existen configuraciones adecuadas e intuitivas, haciéndolas accesibles únicamente a usuarios con mucha experiencia. [9] Además de los juegos un ejemplo de estas aplicaciones es: ***Picfog*** que permite buscar imágenes de *Twitter* por la ubicación geográfica en tiempo real. [4]

  Otro inconveniente es que casi todas las configuraciones están habilitadas por defecto y no existen configuraciones específicas, lo que la mayoría de los usuarios desconoce provocando que publiquen información personal privada de manera innecesaria. Algunos ejemplos son: *Twitter que* tiene perfiles públicos por defecto y *Tuenti* que vincula la visibilidad de las fotografías con la del perfil es decir si se expone el perfil, también se expone las fotografías. [9]

- Por último además de la inadecuada relación entre usabilidad y cantidad de controles (e.d. simplificar el proceso sin arriesgar la seguridad y privacidad); es la dificultad de acceso a una opción de configuración, por ejemplo en *LinkedIn*. "Hacemos clic sobre ***Configuración***, y entramos en ***Edita tu perfil publico>>***. En la ventana que se abre a continuación vamos a la zona inferior de la barra lateral de la derecha y abrimos el menú de visibilidad del perfil público en el que podremos marcar las opciones que se adapten a nuestras necesidades." [9]

2.4. Herramientas de Geolocalización

A continuación se describen de forma breve algunas herramientas existentes más conocidas que permiten leer, modificar, insertar información de geolocalización en archivos digitales. Si bien estas herramientas no están disponibles para dispositivos móviles son de gran utilidad para concientizarlos de la problemática utilizándolas como mecanismos de protección nuestra.

- ***Plug ins.*** Aplicaciones que se puede incluir a los navegadores web y permiten obtener la información geográfica de las fotografías que es encuentran en la red. Su incorporación y manejo es muy sencillo, permitiendo revelar información sensible con un par de clics. Este tipo de aplicativos se encuentras disponibles para *browsers* como: *Google Chrome*, *Internet Explorer*, *Mozilla*, *Safari*, entre otros y la mayoría representan en algún servicio de mapas.

  EXIF Viewer junto con *Opanda IExif* son los aplicativos más utilizados para leer los metadatos de imágenes, se pueden incorporar en *Chrome, IExplorer, Mozilla.*

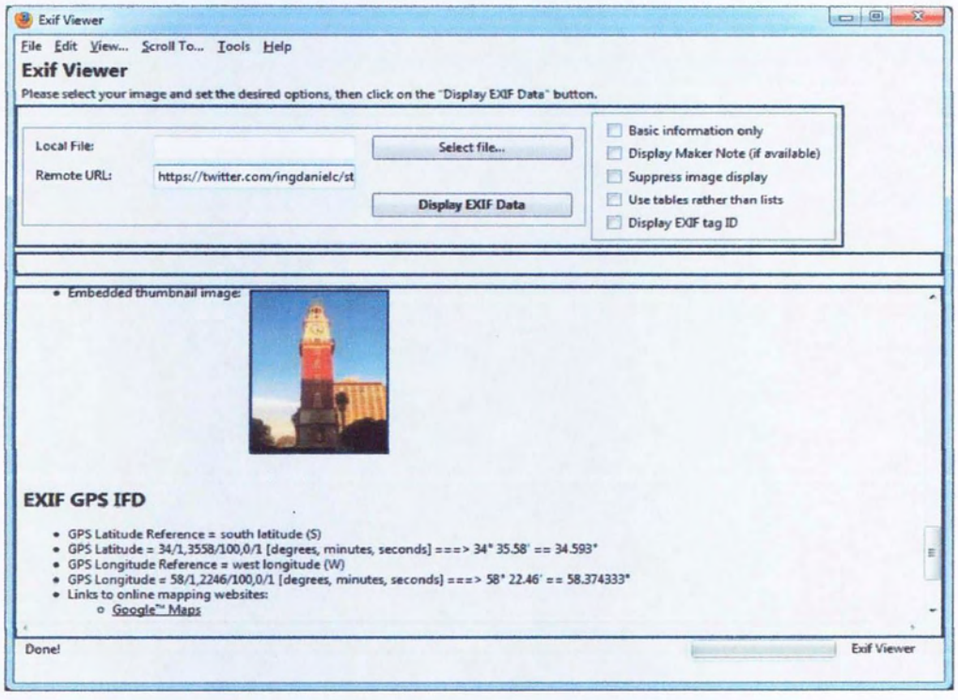


Figura 6. Resultado obtenido con *EXIF Viewer* sobre *Mozilla*.

- ***Creepy***. Es una aplicación desarrollada por Yiannis Kakavas que permite obtener de forma automática información de geolocalización de los usuarios de redes sociales como *Twitter, Flickr, Foursquare* (solamente las confirmaciones que son publicadas a *Twitter*) y servicios de alojamiento de imágenes, para lo cual traza los caminos recorridos por el usuario, usando la posición de GPS, que acompaña a los mensajes y fotos. [22][23]

  La información se presenta en un mapa como *Google Maps, Virtual Maps, Bing Maps, Open Street Maps*, dentro de la aplicación en el que todos los datos recuperados se muestran acompañados de la información pertinente (es decir, lo que se envió desde ese lugar específico) para proporcionar un contexto a la presentación. [22]

  Las fuentes de la información de geolocalización son: publicaciones de *Twitter* desde dispositivos móviles, IP del dispositivo desde el que se hace *post*, geo-etiquetas de archivos digitales incluidos en la actividad de la red social. [22] Pudiendo llegar a obtenerse información especialmente sensible de publicaciones hechas inconscientemente,

como es el caso de las fotos en cuyo interior (sus metadatos) se encuentra almacenada la ubicación GPS de donde fue tomada. [23]

La comunidad *GragonJAR* publico en su sitio el artículo: "*Cómo localizar usuarios de Twitter y Flickr a través de sus fotos*", [23] en el que se analiza la información de geolocalización de dos famosos colombianos @Juanes, @Shakira. En el artículo se muestra como utilizar la aplicación y que información se puede llegar a obtener, corroborando la misma a través de herramientas que permiten leer los metadatos de archivos digitales.

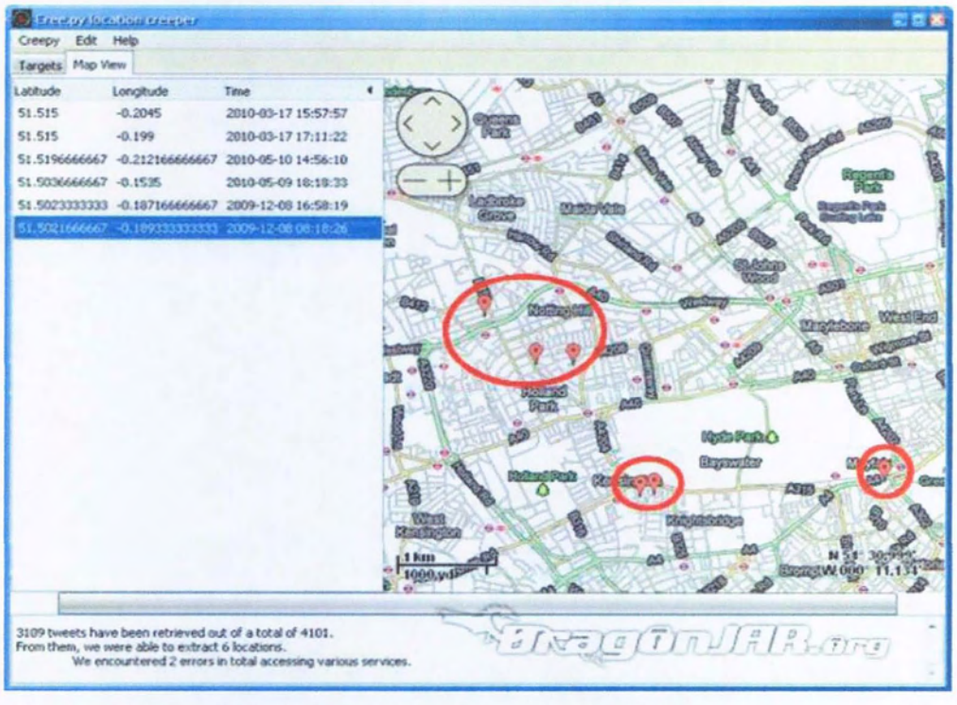


Figura 7. Resultado del análisis de cuenta de *Twitter* con Greepy. [23]

- ***GeoSetter.*** Programa que permite geo-etiquetar, leer o modificar las etiquetas de geolocalización de archivos digitales de forma fácil, completa y con alta precisión, además permite incluir distintos metadatos (IPTC/XMP/EXIF) a los archivos. La precisión es a criterio del usuario, pues es él quien decide que localización incluir, apoyándose en servicios de mapas disponibles en la web. Algunas de sus características son: [8]

  - ✓ Lee y escribe los formatos JPEG, TIFF, y varios formatos de distintas marcas de cámaras.

- ✓ A través de un mapa de *Google Maps* muestra las coordenadas geográficas existentes y la dirección de la imagen.
- ✓ Permite actualizar los datos geográficos a través de un mapa o introduciendo directamente los valores conocidos.
- ✓ Incorpora la funcionalidad de exportación a *Google Earth* (KML). [8]

- **Sitios Web con funcionalidad de Geolocalización.** Muchos sitios web prestan el servicio de localización geográfica, permitiendo consultar los metadatos de archivos digitales, o a través de mapas consultar la ubicación muy aproximada de distintos lugares. Entre los sitios que permiten leer los metadatos de archivos digitales están:

  - ✓ ***Jeffrey`s Exif Viewer y Mapquest.*** Permiten consultar la ubicación geográfica de una fotografía, mapeando el resultado en un mapa. http://regex.info/exif.cgi, http://www.mapquest.com/?q=-34.59967,-58.40133&zoom=8
  - ✓ ***PicFog***, Permite a cualquier persona buscar todas las imágenes que aparecen en *Twitter* por palabra clave y ubicación geográfica en tiempo real. [4]
  - ✓ ***Endomondo***. Servicio que permite llevar un registro de actividades deportivas o de vida diaria referenciadas con datos GPS.
  - ✓ ***PleaseRobMe:*** (Por favor, róbame) Permite obtener la información de localización de todos los usuarios de *Twitter y Foursquare* según la vayan compartiendo, además de permitirnos buscar información de localización sobre un usuario o cerca de un sitio determinado. *PleaseRobMe.com* [28]

Estas son algunas de las herramientas más populares que permiten manipular información de geolocalización de manera muy sencilla; otra aplicación que vale la pena destacar es FOCA, una herramienta muy completa que permite entre otras cosas analizar metadatos a imágenes y documentos.

3. SEGURIDAD Y PRIVACIDAD

La información de geolocalización al igual que la mayoría de la información de las personas necesita un trato adecuado y de no hacerlo tiene consecuencias graves para su privacidad.

En este capítulo se estudiara algunos escenarios vulnerables con el objetivo de ver la facilidad con que se puede poner en riesgo y causar ansiedad a las personas porque su seguridad y privacidad se ha visto amenazada en cualquier momento por alguna mala práctica que se ha dado a su información, además se muestra algunos casos reales y de actualidad donde la geolocalización ha sido protagonista.

3.1. Escenarios Vulnerables – Modalidades de Operación

El propósito aquí es exponer algunos escenarios que demuestran lo fácil que es correlacionar los datos de geolocalización con la correspondiente información que está a disposición del público para comprometer la seguridad y privacidad de los usuarios, lo que supone prestar especial atención a la hora de utilizar funcionalidades de la geolocalización. [4]

El primer escenario se presenta en sitios que ofrecen el servicio de publicidad a través de anuncios con la posibilidad de agregarle fotografías. Muchos de estos sitios tienen su negocio centrado en la venta de artículos, el inconveniente que se presenta es con las imágenes geo-etiquetadas y que los usuarios pueden o no ser conscientes de ello. [4].

En dichos anuncios se ofrecen también a la venta bienes, servicios y objetos de valor (vehículos, joyas, viviendas, equipos electrónicos, etc.) con imágenes que muestran en algunos casos la localización del artículo que está a la venta, lo cual permite verificar de forma sencilla la geolocalización de la foto mediante la comparación de la imagen con otros servicios como *Google Street View, Google Maps,* o cualquier otro servicio de mapas de internet. Estos lugares se convierten en un blanco potencial para los ladrones. Además, muchos ofrecen detalles acerca de cuándo y cómo el

dueño quiere ser contactado ("por favor llamar únicamente en las noches"), lo que permite la especulación acerca de cuando la persona no va a estar en su casa. [4]

Una situación que se debe rescatar es que para determinar la localización más exacta del lugar donde se encuentran dichos objetos es necesario tener un número mayor de imágenes del mismo lugar con geo-etiquetas. Es por eso que anuncios con varias fotografías permiten estimar más precisamente la dirección postal a través de un promedio de las geo-etiquetas y es más fácil aun si hay muchos anuncios en la misma localidad. Se ha demostrado que la exactitud que proporcionan las imágenes geo-etiquetadas creadas con dispositivos como el *iPhone* está alrededor de + / - 1 metro resultando ser mayor que lo que la gente espera. Finalmente se puede destacar que muchos usuarios nos son conscientes de que las fotografías de sus anuncios están geo-etiquetadas y por lo tanto muestran información de su ubicación. [4]

Un segundo escenario se presenta en *blogs* o en redes sociales donde muchas personas incluso celebridades comparten información actualizada sobre sus vidas, y la mayoría de estos sitios permiten subir imágenes. Un sitio muy popular como lo es *Twitter* permite subir fotografías geo-etiquetadas, o hacer link a imágenes externas. Dichas imágenes se pueden convertir en una amenaza para los usuarios si quieren mantener en secreto algunos momentos de sus vidas. La amenaza aumenta debido a que sitios como estos también permiten en la mayoría de los casos hacer comentarios sobre dichas imágenes o publicar algo de interés en su portal que puede incluir la información de geolocalización, que gracias a la cantidad de este tipo de información y a internet se puede conocer exactamente los lugares en donde están o frecuentan dichas personas, construyendo así una línea de tiempo de las actividades más importantes para ellas. [4]

Un tercer escenario muestra que la privacidad de las personas se ve amenazada también por subir videos que contienen datos de geolocalización. Según estudio hecho a *YouTube* se comprueba que se puede de forma semiautomática identificar domicilios de personas que

normalmente viven en un área determinada que están actualmente de vacaciones. [4] Lo que podría ofrecer oportunidades para los ladrones.

El mecanismo que siguieron fue elaborar un *script* utilizando la API[15] de *YouTube* que, dada la posición de una casa, un radio (distancia aproximada de un lugar de vacaciones) y una palabra clave (por ejemplo "niños" ya que muchas personas publican videos caseros de sus hijos), se encuentra una serie de videos correspondientes, luego para todos los vídeos encontrados, el *script* obtiene los nombres asociados a usuarios de *YouTube* y descarga todos los videos que están a una distancia temporal de cierta distancia y se han subido en la misma semana. Seleccionando rápidamente a través de estos videos, se puede encontrar videos del lugar de vacaciones (por el contenido geo-etiquetado) y con fecha de creación actual. Esto permitiría suponer que estas personas están de vacaciones y no en su casa. Sin embargo con los demás videos asociados a la cuenta de *YouTube* de estas personas, se puede descubrir que tienen videos del lugar donde viven y que la ubicación no coincide con la de los videos del lugar donde están actualmente, esto junto con comentarios que suelen hacerse permiten asegurar que efectivamente estas personas están de vacaciones o fuera de la ciudad y que sus casas posiblemente están deshabitadas. [4]

Finalmente podría decirse que las posibilidades para atacar la seguridad y privacidad de las personas por conocimiento de su ubicación actual son muchas como ya se vio y que combinándose con otras alternativas más comunes como la ingeniería social, suplantación de identidad podría ser potencialmente peligroso. A continuación se presentan algunos casos de actualidad donde la privacidad y seguridad de las personas se ha visto comprometida por hacer uso del *geo-tagging* de forma inadecuada.

3.2. Casos Reales y de Actualidad

A continuación se expone de forma muy general dos casos reales y de actualidad donde la privacidad de los usuarios se ha vulnerado y un caso

[15] *Application Programming Interface*, Interfaces de Programación de Aplicaciones

en el que el geo-etiquetado es protagonista en una detención policial. Los ejemplos sirven como alerta a la hora de establecer configuraciones para hacer uso adecuado de la geolocalización.

- En agosto del 2010 *Clarin* publicó "*UN PELIGRO. Adam Savage, conductor del popular programa estadounidense "Mythbusters", publicó en Twitter una foto geo-etiquetada de su auto estacionado frente a su casa*", La imagen contenía una geo-etiqueta con información exacta del lugar donde se tomó la foto, revelando la dirección de su casa inconscientemente. Además el mensaje de la imagen decía "Voy al trabajo". Toda esta información pone en riesgo la seguridad del famoso, puesto que ladrones o personas mal intencionadas podrían darle un inadecuado uso a los mismos. [10][11]

- Este caso publicado en la página de *ESET* en marzo de 2012 sucede a través de la red social *Foursquare* que brinda la facilidad de comunicación para algunas personas, pero para otras puede resultar poco agradable; como es el caso de *Joel Postman*. "Un día, luego de realizar un *check in* en un bar para tomar un café, escucha que la persona detrás de la barra pregunta: - ¿Hay algún *Joel Postman* acá? Tienes una llamada telefónica. *Joel* recordó que no le había comentado a nadie que iría a ese bar, excepto ese *check in* que realizó antes de ingresar. Tomó el teléfono y respondió tímidamente. La persona del otro lado de la línea, con una voz temerosa, añade: - La muerte te puede encontrar en cualquier parte, incluso en este bar. Y luego agrega: Ingresa a ifidie.org". [16]

  "Lo que al principio parecía una amenaza de muerte, terminó como una especie de campaña de marketing", según *Joel Postman*. El sitio web *ifidie.org*, almacena confidencialmente notas y archivos privados que se entregan a sus destinatarios únicamente si el autor muere. [16]

- Este último caso se trata de una publicación en infobae: "El FBI atrapó a un peligroso hacker gracias a foto de su novia" Un activista que atacó los sitios web de la policía de Houston y Los Ángeles, cometió el error de

publicar en *Twitter* una imagen geo-etiquetada. Así fue encontrado por las autoridades de EE.UU. Higinio O. Ochoa III un programador de 30 años de Galveston, Texas que se mantenía en las sombras y se escondía bajo el alias *w0rmer*, hasta que un día decidió mostrar los atributos de sus novia y publicó una foto de su escote en su cuenta *@AnonW0rmer*. El FBI logro conocer la ubicación del departamento gracias a los metadatos del archivo incorporados por el *iPhone* con el que se creó la imagen, que evidentemente tenía habilitada la funcionalidad de geolocalización de lo cual no se percato el joven pirata. [17]

Los investigadores después de chequear varias fotografías y el perfil de *Facebook* de *Ochoa* lograron determinar que uno de sus contactos: *Kylie Gardner,* era la novia del w*0rmer* y con esto el FBI comprobó que *Gardner* era la de la fotografía y que Ochoa era w*0rmer.* Finalmente con esta información el FBI logró arrestar al pirata. [17]

4. RIESGOS DE SEGURIDAD Y PRIVACIDAD

El conocimiento de la geolocalización de individuos tiene asociado múltiples riesgos, dependiendo del contexto en que se encuentre. Esta parte del documento pretende mostrar aquellas situaciones que amenazan la seguridad y privacidad de usuarios y que incluso pueden llegar a causar agresiones personales.

Hoy en día, el fácil acceso a la tecnología permite compartir ideas y experiencias por medio de imágenes, videos, texto y sonidos de manera ágil a través de las redes sociales, enriqueciendo nuestras formas de comunicación, además de beneficiarnos de que la publicidad por ejemplo al igual que otros servicios estén orientados de forma específica a nosotros, a nuestros gustos, al lugar por donde nos movemos, etc. [10] Sin embargo asociado a estos beneficios nos exponernos a muchos riesgos que van desde la pérdida o robo de dispositivos móviles y con ellos de toda la información personal, financiera, de geolocalización, empresarial, etc., hasta sufrir agresiones físicas. A continuación se describen algunos de los riesgos asociados a la geolocalización:

4.1. Riesgos en el Sistema Operativo

El sistema operativo es el elemento más sensible desde el punto de vista de seguridad pues actúa como instrumento de gestión de recursos, gestiona la información almacenada y procesada por el dispositivo. [2] El principal riesgo que presenta el sistema operativo es el **Acceso a la información privada,** que tras aprovechar ciertas vulnerabilidades del mismo se puede acceder a información sensible para el usuario, un ejemplo de esto es la forma que usan los dispositivos *iOS* para almacenar las contraseñas de las redes sociales a través de la utilización de archivos *plist*. [26]

A continuación se exponen las razones más sobresalientes desde el punto de vista del sistema operativo, que ponen en riesgo la información de los dispositivos móviles en especial la información de geolocalización del usuario:

- **Código malicioso o malware** (virus, troyanos, *botnets*, *keyloggers*) que infectan el sistema operativo anfitrión con el fin de inutilizarlo, dañarlo, robar o alterar información privada contenida en el dispositivo móvil. [2] Existen aplicaciones que tras de la funcionalidad que prestan acceden sin autorización a información privada, pudiendo alterarla o en el peor de los casos robarla para enriquecer gigantes bases de datos que pueden ser aprovechadas para fines maliciosos.

- ***Bugs* del Sistema Operativo**, Fallos de seguridad que permiten la intrusión de un atacante, a través del aprovechamiento de vulnerabilidades. Los más peligrosos son aquellos que dan la posibilidad de explotación remota, a través de una red de intercomunicación. Los dispositivos móviles por el hecho de contar con múltiples interfaces de comunicación de red (redes de telefonía, redes Wi-Fi inalámbricas, *Bluetooth*, infrarrojos...), tienen más posibles vectores de ataque en caso de fallo de seguridad. [2]

- **La modificación no autorizada del sistema operativo**, (*jailbreak* en *iOS*, *rooteo* en *Android)* con el fin de acceder a funciones que se encuentran bloqueadas por el fabricante se habilita la instalación de programas no firmados que puede provocar la entrada de software malicioso que, bien suplantando a uno original o no, llegue a infectar el sistema operativo y aplicaciones instaladas. [2]

4.2. Riesgos en Aplicaciones de Geolocalización

Las aplicaciones de geolocalización, al igual que el sistema operativo, son susceptibles de contener fallos de seguridad y suponer un potencial vector de ataque. [2] Algunos de sus riesgos son:

- Por **la naturaleza de la información** que manejan las aplicaciones de geolocalización, se las considera muy sensibles desde el punto de vista de la seguridad. Si la información se integra dentro de redes sociales, aumenta las posibles consecuencias de los fallos de seguridad y privacidad asociados, puesto que se conjuga la información de

geolocalización con toda clase de datos personales. Y además si la información de geolocalización se transmite, "los riesgos para el ciudadano no se limitan a posibles robos de información o datos a través de Internet, sino que pueden llegar incluso a suponer un peligro para su integridad física y personal". [2]

- **Fallos de seguridad**, al igual que el sistema operativo también son susceptibles a este tipo de problema y además tienen una gravedad directamente proporcional a la clase de privilegios del usuario que las ejecuta. [2]

- **Inadecuada configuración** de las funcionalidades de geolocalización, dejándolas habilitadas por defecto inconscientemente, supone alto riesgo para el usuario, pues estaría brindando información innecesariamente.

- **Integración con Redes Sociales.** La información de geolocalización es muy sensible que puede generar serios problemas para las personas, estas situaciones se agravan cuando la localización se integra con las redes sociales siendo necesario establecer restricciones que determinen el ámbito de publicación y disponibilidad de los mismos. La publicación de información de localización de un ciudadano conlleva riesgos que van desde el robo de datos, el hurto o robo físico, a la agresión contra su persona. Por ejemplo suplantación de identidad (crear un perfil igual al de alguien) con el propósito de utilizarlo en estudios de mercado, envío de publicidad, *ciberbullying,* entre otros. [2]

4.3. Riesgos en sitios Web: Redes Geosociales

Los riesgos relacionados con la información de geolocalización aumentan cuando se publican a través de estos sitios y de hecho acá es donde se encuentran los mayores peligros de la geolocalización.

- **Riesgos en la Red de Comunicación.** El principal problema asociado a las conexiones de red es la intercepción de las comunicaciones (ataques

de *man in the middle)*. Debido a la propia arquitectura de Internet, la información, puede ser intervenida o accedida por personas no autorizadas y mal intencionadas. Esta intercepción puede darse por utilizar redes inalámbricas abiertas (libres, sin contraseñas) o con protocolos de protección pero con contraseñas débiles y también por preferir las redes de telefonía móvil de segunda generación sobre las de tercera generación que son mas robustas en cuanto a seguridad. [2]

Junto con la intercepción se encuentran muchos otros tipos de ataques como los que se listan a continuación, tomados de: [2][21] y donde se puede encontrar más información; que ponen en riesgo información privada del usuario de las redes sociales, e incluso pueden llegar a tomar el control total de las mismas.

- ✓ Inyección de código en sitios cruzados o *XSS cross-site scripting*.
- ✓ Perdida de Autenticación y Gestión de Sesiones.
- ✓ Falsificación de petición en sitios cruzados o *CSRF cross-site request forgery*.
- ✓ Redirecciones no validas.
- ✓ Inyección de código SQL o *SQL Injection* e inyección de comandos de SO.
- ✓ Secuestro de clic o *clickjacking*.
- ✓ Falsificación de la información en formularios o *form tampering*. [2][21]

- **Facilidad de búsqueda y correlación de la información.** Aumenta el riesgo de los individuos, y es un peligro para un público mucho más amplio, ya que incluso las personas que conscientemente optan por no informar su ubicación, es posible que ésta se haga pública a través de una publicación o etiquetación involuntaria de fotos o vídeos de terceros y que están fuera del propio control del usuario. [4]

- **Fuga de datos.** El principal riesgo de seguridad por el uso de geo-etiquetación, es la fuga inconsciente de datos de ubicación a través de redes sociales, que ocurre por desconocimiento del funcionamiento y del tipo de configuración en dispositivos móviles. [2][10]

Como se dijo la fuga se da por las **configuraciones deficientes de privacidad** en aplicaciones *on-line* específicamente en servicios y redes sociales ricas en información geo-etiquetada. Una configuración deficiente seria dejar habilitada una opción por defecto permitiendo que personas ajenas a nuestros círculos sociales, incluso mal intencionadas tengan acceso a datos de ubicación, aprovechándose de esto para realizar acciones criminales, técnica conocida como Ingeniería Social. [10]. También se presenta por el fácil acceso a las **Interfaces de Programación de Aplicaciones (API's).** que ofrecen algunas redes sociales como *Twitter* y *YouTube* acompañado con ciertas habilidades de programación pueden permitir extraer datos valiosos de los usuarios de esos sitios. Por ejemplo, se podría buscar fotos geo-etiquetadas acompañadas de textos como "de vacaciones" o las que se hayan sacado en un barrio específico. [11]

- **Tratamiento irresponsable de datos** llevado a cabo por las empresas: cesión de datos de usuarios sin su consentimiento, utilización indebida de datos para estudios de mercado fuera de las cláusulas de privacidad, vulneración de la configuración de privacidad de los usuarios. [2]

Es importante dejar claro que los datos relacionados a nuestra ubicación tienen carácter "privado", por el simple hecho de brindar información relacionada con lugares que frecuentamos o con actividades que realizamos cotidianamente. Por ejemplo, a través de mensajes o fotografías geo-etiquetadas se podrían conocer el comportamiento o rutinas de una persona y así generar un mapa ilustrativo de sus actividades diarias, de los lugares de convivencia con su familia y amigos, así como la ubicación de sus pertenencias, que puede incluso poner en riesgo su integridad. [10]

5. SUGERENCIAS DE SEGURIDAD Y PRIVACIDAD PARA MITIGAR RIESGOS DE GEOLOCALIZACIÓN

El desarrollo de aplicaciones de geolocalización debe ir acompañado de mecanismos de control que garanticen la seguridad y privacidad de los usuarios y que eviten o disminuyan los riesgos asociados por el inadecuado manejo e incluso manejo sin autorización de su información. [4]

Al igual que otros datos privados del usuario como su identificación, sus contactos, su domicilio, etc., si la ubicación de los lugares que frecuenta o de sitios en los que permanece se vuelven públicos o son muy fáciles de obtener (por ejemplo: la ubicación inmersa en una imagen comprometedora que incluye sujetos identificables) incrementa la amenaza de comprometer su privacidad, es en estos casos donde la ubicación toma gran relevancia. [4] Es decir como simple dato la ubicación no representa mayor problema, sin embargo en un entorno como internet que: contiene una enorme cantidad de imágenes, vídeos y en general archivos digitales con datos de localización suficientes para el montaje de ataques sistemáticos de privacidad, permite hacer búsquedas exhaustivas basadas en localización e inferir información a partir de la correlación de diferentes fuentes, brinda la disponibilidad de muchos otros servicios basados en geolocalización, que a su vez permite correlacionar los hallazgos con la ubicación gracias además a la facilidad con que los *smartphone* generar datos geo-etiquetados por las funcionalidades que incorporan; dicho esto entonces podemos sostener que en un entorno como éste sí representa un potencial problema para la privacidad de los usuarios. [4]

Tomando como base el desconocimiento, la dificultad de acceso y de configuración que la mayoría de usuarios de *smartphone* tienen sobre la funcionalidad de geolocalización, este capítulo tiene como objetivo enumerar un conjunto de sugerencias de configuraciones para la funcionalidad de geolocalización en dispositivos móviles como los de *Apple*; si bien se podrían adaptar para otros sistemas operativos estas configuraciones están pensadas para *iOS 4.x*. Las configuraciones están orientadas a usuarios sin

experiencia en el tema y serán de fácil acceso para promover su utilización sin la necesidad de pasar por interminables y confusas pantallas de menús.

Este conjunto de sugerencias están basadas en otros trabajos que pretendieron establecer pautas similares, de los cuales he elaborado una recopilación y estructuración de las más importantes que según mi criterio debe tener la funcionalidad de geolocalización para mitigar la amenaza de la seguridad y privacidad de los usuarios, a éste compilado agrego además algunos aspectos que surgieron del desarrollo de éste trabajo. A continuación se describen las sugerencias de seguridad y privacidad que pueden ayudar a aprovechar al máximo los beneficios de la geolocalización minimizando los riesgos:

- Se sugiere a nivel general establecer una estrategia unificada entre proveedores para configurar la funcionalidad de geolocalización en el sistema operativo, aplicaciones, herramientas, sitios web, y demás que permita reducir la exposición innecesaria de información confidencial como datos geo-etiquetados, ubicaciones, etc., para aumentar la seguridad y privacidad de los usuarios; para lo cual se recomienda que todas las configuraciones estén deshabilitadas de inicio (política *opt-in)* y que sea el usuario quien decida conscientemente habilitarlas, esto evitaría además que se usen sin conocimiento ni consentimiento del usuario. [4]

5.1. Sugerencias a nivel de Sistema Operativo

En éste apartado se exponen sugerencias y buenas prácticas de seguridad y privacidad para la funcionalidad de geolocalización en el sistema operativo *iOS*.

- Mantener siempre actualizado el sistema operativo y utilizar software original, cuya procedencia sea conocida y certificada. Evitando modificaciones no autorizadas del software o hardware, puesto que pueden ocasionar problemas de seguridad no contemplados por el fabricante. [2]

- Utilizar un sistema antivirus siempre actualizado y un sistema de protección de red de tipo cortafuegos para proteger el sistema. [2]

- Leer del instructivo las configuraciones y recomendaciones de la funcionalidad de geolocalización para conocer su funcionamiento y poder configurarla adecuadamente. [10]

- Configurar adecuadamente las opciones de localización, preferiblemente solo si se va a utilizar una aplicación que haga uso de ella, de la misma manera la precisión GPS deberá utilizarse a criterio del usuario únicamente en las aplicaciones que lo requieran y tener en cuenta que la geolocalización a través de redes *Wi-Fi* inalámbricas se debe evitar al máximo posible. [2]

- El sistema operativo debe tener la capacidad de permitir regular al usuario la precisión de la geolocalización que desea incluir en archivos digitales y al hacer *post* en sitios web, evitando valores por defecto y que sea el usuario quien decida al respecto dependiendo de la utilidad.

- Establecer contraseñas para asegurar el acceso de los dispositivos, pues existe el riesgo de extravío o robo del mismo y por lo tanto de la información. Se recomienda utilizar contraseñas fuertes, (números, letras mayúsculas y minúsculas, símbolos; con longitud mínima de 8 caracteres) y cambiarlas con cierta periodicidad. También opcionalmente se recomienda incluir una contraseña cada vez que se utilice el dispositivo, siempre y cuando no sea molesto. [10][2]

- Con el propósito de disminuir los riesgos asociados al robo o perdida del dispositivo móvil es recomendable primero realizar una copia de seguridad de la información del dispositivo y mantenerla actualizada, segundo establecer contraseñas (según recomendación anterior) y tercero utilizar aplicaciones de seguridad que impidan la utilización del dispositivo si se apaga o se cambia de SIM y que borren de forma remota la información privada. [2]

- Se podría implementar un mecanismo criptográfico para los metadatos de contenido digital especialmente para los de geolocalización, y así proporcionar al usuario mayor control sobre los mismos en aplicaciones y sitios web, mitigando las implicaciones de privacidad y seguridad.

5.2. Sugerencias a nivel de Aplicaciones de Geolocalización

Para obtener el mejor provecho de la gran cantidad de aplicaciones y herramientas que hacen uso de geolocalización se sugiere a desarrolladores y usuarios finales tener en cuenta:

5.2.1. Sugerencias para desarrolladores

- La configuración debe ser bastante intuitiva y de fácil acceso, preferiblemente se debe mostrar cuando las aplicaciones requieran hacer uso de la funcionalidad encontrando un adecuado equilibrio entre la usabilidad y los controles.

- Construir políticas de seguridad, ética y uso de las funcionalidades de geolocalización siendo lo más específicos posible para que puedan ser entendidos por usuarios no experimentados.

- La geolocalización para todas las aplicaciones debe estar inicialmente deshabilitada, igualmente para la opción de geo-etiquetación de medios digitales como audio, video, documentos, imágenes; permitiendo que el usuario sea quien decide si habilitarlas o no al momento de él requerirlo. [10]

- Cuando el usuario decida activar o desactivar la funcionalidad de geolocalización y geo-etiquetación debe poder hacerlo únicamente para las aplicaciones que él quiere y no en general para todas, esto permite tener más control al usuario de las aplicaciones que utiliza. Por ejemplo al momento de tomar una fotografía se puede decidir si agregar o no geo-etiquetas sin embargo esta decisión no implica para los videos.

- Cada vez que el usuario acceda a una aplicación se deberá preguntar si desea hacer uso de éstas funcionalidades, el nivel de precisión (resolución de ubicación) de las mismas [4], si desea conocer más sobre las implicaciones de seguridad y privacidad y si desea habilitarlas de forma permanente para la aplicación. En caso de habilitarla permanentemente se debe notificar que está haciendo uso de ese servicio al ingresar a la aplicación. De esta manera se logra que usuarios que no tienen conocimiento publiquen información privada de forma inconsciente.

  En cuanto a la resolución de ubicación, el dispositivo podría eliminar un número correspondiente de los dígitos menos significativos de cualquier sistema de coordenadas, lo que ofrecería a los usuarios más control. Por ejemplo se podría decidir si quiere publicar su país, región, ciudad, domicilio. [4]

- Como complemento de la anterior característica, si se decide activar o desactivar la geolocalización y geo-etiquetación para una aplicación en particular se debe permitir elegir en qué casos concretos y que módulos de la aplicación van hacer uso o no de estas funcionalidades. En general se debe evitar el todo o nada. [4]

5.2.2. Sugerencias para usuarios finales

- Si se decide instalar una aplicación ya sea para acceder a una red social o para integrarla a la misma, se debe revisar la licencia antes de aceptarla con el propósito de conocer a que información accederá la aplicación.

- Utilizar únicamente aplicaciones de geolocalización actualizadas y de confianza, obtenidas a través de los canales de distribución pertinentes. Entre ellos se incluyen páginas web oficiales y tiendas de aplicaciones o *Store Applications*. [2]

- Distintas aplicaciones tienen la capacidad de almacenar ubicaciones para acceder a ellas rápidamente, a dichas etiquetas se debe evitar ponerles nombres que contengan información extra, por ejemplo: "Mi Casa", "Trabajo de mi hermano", "oficina", "casa de mi novia", etc. [10]

- Prestar atención a los permisos al momento de instalar una aplicación y vigilar en sus actualizaciones los posibles cambios en los mismos, considerando que se deben asignar los mínimos necesarios para evitar que la información se comprometa. [2]

- Puesto que las aplicaciones pueden tener muchas vulnerabilidades es recomendable mantener el dispositivo bloqueado al conectarlo en computadores que no sean de confianza y solo utilizarlas para cargar la batería. [26]

- "Establecer, en la configuración de la aplicación, en qué momento se permite la utilización de funciones de geolocalización, y con quién se va a compartir dicha información". [2]

- La mayoría de las aplicaciones que incorporan funcionalidad de geolocalización, utilizan a las redes sociales como medio para difundirse estableciendo relaciones a nivel de datos que es convenientes revisar, y de esta manera controlar la publicación de información, resultado de la interacción con la aplicación. [2]

5.3. Sugerencias a nivel de Sitios Web: Redes Geosociales

5.3.1. Sugerencias para desarrolladores

- Al momento de subir archivos digitales a sitios web de geolocalización solicitar si eliminar, bloquear o configurar la resolución de la localización (similar al de las aplicaciones) si se decide mostrar. El navegador entonces adaptaría las geo-etiquetas si existen de acuerdo a la elección del usuario, antes de proceder. *Facebook* por ejemplo elimina los

metadatos de los archivos para evitar ataques relacionados a la geolocalización, proporcionando mayor protección, *Flickr* bloquea el acceso a geo-etiquetas a menos que el usuario lo permita de forma explícita. Sin embargo muchos sitios (de publicidad, comercio electrónico, redes sociales, blogs) todavía no aplican ninguna medida ante esta situación dejando subir contenido geo-etiquetado. [4][11]

- Las API's que ofrecen sitios como *Flickr* y *YouTube* se deberían configurar reduciendo la resolución para ofrecer un mayor nivel de privacidad, sin restringir la geo-tecnología en sus capacidades. [4]

- Considerar que muchos sitios no tienen control sobre la asociación de links que contienen archivos digitales geo-etiquetados, lo que implica que de forma indirecta tienen información de geolocalización. [4]

5.3.2. Sugerencias para usuarios finales

- Verificar la autenticidad del certificado del sitio al que se accede, mas sí presta servicios de geolocalización.

- Siempre que sea posible y si no se desea que la navegación sea inteligente y permita buscar información personalizada, se recomienda configurar el navegar web para que no dé a conocer la localización física.

- Verificar que el navegador web utilizado junto con sus complementos, y *plugins* estén actualizados, con el fin de prevenir ataques web y explotación de vulnerabilidades. [2]

- Siempre que sea posible conectarse a redes de confianza y que cuenten con protocolos adecuados de seguridad, evitando utilizar al máximo redes *Wi-Fi* inalámbricas abiertas y redes gratuitas, en cuanto a redes móviles preferir las de tercera generación sobre las de segunda generación. [2]

- "Leer con detenimiento y comprender las cláusulas de privacidad de los servicios de geolocalización y las redes geosociales". [2]

- Se recomienda revisar periódicamente la privacidad de la cuenta; los sitios en general y las redes sociales en particular tienen varias alternativas para poder personalizar las opciones de seguridad y de esta manera conocer la configuración para tener mayor control sobre la actividad social. [16]

- Si se decide publicar la geolocalización se debe evaluar el contexto para poder adecuar la precisión o resolución de la misma. Es posible que en ocasiones baste con la ciudad en lugar de publicar el domicilio. [2]

- Es prudente hacerse amigo únicamente de personas que realmente se conoce y como regla general desconfiar de todo el mundo, en redes de geolocalización, un contacto desconocido puede tener implicaciones mayores para la seguridad del usuario. [16]

- No expongas a miembros de la familia (especialmente a los pequeños) en *posts* de las redes, como por ejemplo, incluyendo la ubicación de los lugares que frecuentan (hogar, escuelas, casas de amigos y demás); podría ser una práctica delicada que estaría brindando demasiada información. [16]

- Si se decide publicar información geo-etiquetada se debe prever que esté disponible únicamente para personas de confianza, para lo cual se recomienda elegir con cuidado el grupo de usuarios que podrán ver la información generada por las aplicaciones o redes geosociales. La mayoría de las redes sociales permiten crear grupos de amigos y de esta manera restringir las publicaciones y la información a dichos grupos privados. [10][2]

- Evitar incluir información referente a lugares en que se encuentra un usuario en un momento dado. Para ello, conviene no anunciar los

desplazamientos habituales, los períodos de vacaciones, salidas y en general evitar hacer *check in* en lugares llamativos como casas de cambios, bancos, casa, entre otros que pueden facilitar a delincuentes localizarte. [16]

- Antes de publicar contenido digital recuerda que éste puede dar información de los sitios que más frecuentas, horarios de visita y ubicación geográfica. [10]

- Si se decide instalar aplicaciones dentro de la red social es importante saber que permisos se les otorga además de hacer una revisión periódica de las actividades que estas realizan y de la información que utilizan sin que sean solicitadas por el usuario. [9]

En general éstas son algunas de las acciones más comunes que, a pesar de lo obvio que parezcan, muchos usuarios todavía siguen utilizando y pueden poner su seguridad en riesgo. Tener presente que el empleo de tecnologías innovadoras o emergentes siempre debe ir acompañado de medidas básicas de seguridad, ser consciente del tipo de información que se genera, transforma, almacena o comunica, sin olvidar los riesgos que implica. Contribuir a mantener una cultura de seguridad de la información que propicie un ambiente de confianza en las nuevas tecnologías y sus aplicaciones. [10][16] Informarse e informar a los amigos de los riesgos que pueden existir, pues como dice *Sommer* en [4] *"Proteger la privacidad no es sólo una cuestión de estar informado y ser responsable en el plano personal. Un amigo puede sacar una foto geo-etiquetada de nuestra casa y subirla. Hay que educarse y educar a los amigos, pero en definitiva no se tiene control alguno".*

6. CONCLUSIONES

Con la realización del presente trabajo se logró hacer una lista bastante completa de sugerencias para el buen uso de la funcionalidad de la geolocalización sin correr ningún riesgo, el cual presento como principal aporte, dicho resultado se obtuvo primero del análisis que se hizo a algunas aplicaciones, en específico al conjunto de configuraciones de seguridad y privacidad de la geolocalización con el propósito de encontrar ciertas limitaciones y problemas en las mismas que podrían convertirse en potenciales amenazas, segundo por la recopilación y estructuración de la información recolectada de diversos trabajos que tratan la problemática. Junto a las sugerencias se presenta una parte teórica, aspectos de seguridad y privacidad y también los riesgos asociados a la problemática con el propósito de concientizar al usuario del alcance que podría tener la amenaza de publicar información privada y así lograr un adecuado uso de ésta tecnología. Del desarrollo de este trabajo se puede concluir lo siguiente:

- El nivel de seguridad con respecto a las funcionalidades de geolocalización está determinado primero por la configuración del dispositivo móvil donde el usuario decide si geo-etiquetar archivos de audio, video y demás, los post que hace en las redes sociales y si quiere que las aplicaciones de geolocalización dispongan de su ubicación geográfica para prestarle mejores servicios. Y segundo por la configuración de seguridad y privacidad de las aplicaciones *on-line* y las aplicaciones de los dispositivos que usan datos de localización. Por lo tanto la configuración referente al dispositivo permite decidir si los archivos contienen datos de geolocalización y las configuraciones de sitios y aplicaciones están orientadas al hecho de que si esa información se hace pública o no. Se podría decir entonces que la seguridad depende de uno o de ambos tipos de configuración además del nivel de consciencia que tengan los usuarios del problema puesto que la solución no es dejar de utilizar la geolocalización ni publicar nuestra localización sino determinar e identificar los eslabones débiles del ciclo y prestarles mayor atención.

- Las principales razones que ponen en riesgo la seguridad y privacidad de los usuarios de dispositivos móviles son primero la publicación de información geo-etiquetada de forma innecesaria, segundo los avanzados desarrollos que permiten realizar búsquedas sistemáticas y estructuradas de información utilizando como parámetro la geolocalización que aprovechando la cantidad de fuentes de datos privados y de información se puede inferir con gran facilidad, tercero la elevada capacidad de los dispositivos móviles de capturar la geolocalización del usuario e incluirla en archivos digitales o en actividad web, cuarto las configuraciones deficientes de la funcionalidad de geolocalización.

- Los riesgos que suponen una amenaza a la seguridad y privacidad de los usuarios de dispositivos móviles van desde la pérdida o robo de los dispositivos y con ellos de toda la información personal, financiera, empresarial, de geolocalización, etc. hasta llegar a sufrir agresiones que afecten la integridad de los usuarios, sin embargo se logro determinar que la principal preocupación es la fuga datos de localización convirtiéndose en la mayor amenazan la seguridad y privacidad para el usuario.

- La publicación de información de localización (con alta precisión) por parte de los usuarios de dispositivos móviles puede darse principalmente por: se desea y se es consciente de la publicación de la ubicación, se tiene conocimiento de la existencia de la información pero no de las consecuencias, las aplicaciones no tienen un set de configuración adecuado e intuitivo que permita publicar sin poner en riesgo la seguridad y privacidad; o simplemente se desconoce que los archivos digitales tienen la ubicación geográfica del lugar donde se crearon y otros datos privados que podrían causar situaciones riesgosas.

- Unas adecuadas, completas e intuitivas opciones de configuración de la funcionalidad de geolocalización son la mejor manera de evitar situaciones incomodas, acompañada de un nivel de consciencia

aceptable por parte de los usuarios de las consecuencias y riesgos por el uso inadecuado, riesgos que podrían clasificarse como medianamente altos, por lo cual surge la necesidad de un proceso de educación como primer paso para adoptar una tecnología emergente y así aprovecharla al máximo.

- En la actualidad la mayoría de las aplicaciones de geolocalización y las redes sociales tienen como objetivo recolectar la mayor cantidad de información personal incluida la información geográfica en lo cual los usuarios colaboran mucho sin tener las suficientes precauciones del caso antes de hacerlo por desconocimiento o por dificultad; de ahí la necesidad entonces de que las configuraciones sean pensadas con el ánimo de proteger al usuario eliminando los valores por defecto y que al contrario sea el usuario quien decida explícitamente si quiere exponerse a los riesgos.

- La geolocalización en dispositivos móviles afecta principalmente la confidencialidad (la integridad y disponibilidad casi no se ven afectadas) de la información, puesto que si no se utiliza de forma adecuada y si no se es consciente de sus riesgos se puede estar permitiendo el acceso a información privada a personas no autorizadas, que si son malintencionadas podría convertirse en una seria amenaza que ponga en entredicho la seguridad y privacidad de los usuarios.

7. BIBLIOGRAFIA GENERAL

[1]. Nissnbaum, Helen. Privacidad amenazada, Tecnología, política y la integridad de la vida social. Editorial Océano de México. Primera Edición 2011.

[2]. Pérez, Pablo. Gutiérrez, Cristina. Álvarez, Eduardo. De la Fuente, Susana. García, Laura. Observatorio de la Seguridad de la Información de INTECO. Guía sobre privacidad y seguridad de las herramientas de geolocalización. Edición Marzo de 2011.
http://www.inteco.es/Seguridad/Observatorio/guias/Guia_Geolocalizacion
Último Acceso: Abril 29 de 2012

[3]. Jimeno Garcia, Maria. Míguez Pérez, Carlos. Heredia Soler, Ernest. Caballero Velasco María. Destripa la Red. Editorial Anaya. Edición 2011.

8. FUENTES

[4]. Friedland, Gerald. Sommer, Robin. *Cybercasing the Joint: On the Privacy Implications of Geo-Tagging.*
http://www.icsi.berkeley.edu/pubs/networking/cybercasinghotsec10.pdf
Último Acceso: Abril 29 de 2012

[5]. Qué es Geolocalización?
http://www.parchegeek.com/%C2%BFque-es-geolocalizacion
Último Acceso: Octubre 29 de 2011

[6]. Informática Hoy. Qué es geolocalización?
http://www.informatica-hoy.com.ar/aprender-informatica/Que-es-geolocalizacion.php
Último Acceso: Octubre 29 de 2011

[7]. Geomatrix. Tecnologías para el Desarrollo. Qué es Geolocalización?
http://geomatrixdominicana.com/index.php?option=com_content&view=article&id=45:que-es-geolocalizacion&catid=18:articulos&itemid=1
Último Acceso Octubre 28 de 2011

[8]. *Geotagging*: Cómo subir sus fotos a un mapa del Google-Earth!
http://www.guia4x4.com.ar/images/geotagging/geottaging_para_imprimir.pdf
Último Acceso: Octubre 29 de 2011

[9]. Privacidad y seguridad en Redes Sociales.
http://recursostic.educacion.es/observatorio/web/es/internet/recursos-online/1015-daniel-ortega-carrasco
Último Acceso: Abril 29 de 2012

[10]. Espinosa Madrigal, Carmina Cecilia. Canales, Israel Andrade. Geoetiquetación: Los riesgos de hacer pública tu ubicación. Julio 30 de 2011.
http://revista.seguridad.unam.mx/numero-11/geoetiquetaci%C3%B3n-los-riesgos-de-hacer-p%C3%BAblica-tu-ubicaci%C3%B3n
Último Acceso: Marzo 13 de 2012

[11]. Clarín. "Nuevo peligro del mundo online: Las Geoetiquetas". Agosto 14 de 2010.
http://www.clarin.com/internet/Nuevo-peligro-mundo-online-geoetiquetadas_0_315568651.html
Último Acceso: Marzo 13 de 2012

[12]. El geoetiquetado: qué es y como desactivarlo.
http://www.trucoswindows.net/forowindows/trucos-moviles/103979-geoetiquetado-desactivarlo.html
Último Acceso: Marzo 13 de 2012

[13]. Muniz, Javier. Geolocalización en las redes sociales. Abril 10 de 2010
http://www.genbeta.com/a-fondo/geolocalizacion-en-las-redes-sociales
Último Acceso: Abril 29 de 2012

[14]. SEDIC. Introducción a los Metadatos. Estándares y Aplicación.
http://www.sedic.es/autoformacion/metadatos/tema1.htm
Último Acceso: Abril 17 de 2012

[15]. Corporación Universitaria para el Desarrollo de Internet. Introducción a los Metadatos.
http://www.google.com.ar/url?sa=t&rct=j&q=metadatos&source=web&cd=8&sqi=2&ved=0CGsQFjAH&url=http%3A%2F%2Ffiles.tecnologiaenelaula.webnode.es%2F200000147-3ea773fa15%2FIntroduccion%2520a%2520los%2520metadatos.pdf&ei=00qOT4z-LYz-8ASxlaWwDg&usg=AFQjCNFWqLgxtEdzh0WhOI0EEZsj766nJg
Último Acceso: Abril 17 de 2012

[16]. Labaca Castro, Raphael. 4 Acciones que no deberías realizar en *Foursquare.* Marzo 6 de 2012.
http://blogs.eset-la.com/laboratorio/2012/03/06/4-acciones-no-deberias-realizar-foursquare/
Último Acceso: Abril 23 de 2012

[17]. Infobae.com. El FBI atrapó a un peligroso hacker gracias a foto de su novia. Marzo de 2012.
http://www.infobae.com/notas/642702-El-FBI-atrapo-a-un-peligroso-hacker-gracias-a-foto-de-su-novia.html
Último Acceso: Abril 23 de 2012

[18]. Alcocer, Alberto. Las Redes Sociales de Geolocalización, Generadoras de Negocio para las Empresas. Julio 3 de 2011.
http://www.societic.com/2011/07/las-redes-sociales-de-geolocalizacion-generadoras-de-negocio-para-las-empresas/
Último Acceso: Abril 29 de 2012

[19]. Alcocer, Alberto. *Foursquare* y sus beneficios para las empresas. Julio 14 de 2010.
http://www.societic.com/2010/07/fousquare-y-sus-beneficios-para-las-empresas/
Último Acceso: Abril 29 de 2012

[20]. Polo, Juan Diego. *Footprints* – Determina la localización geográfica del *iPhone/Android* de tus hijos. Mayo 5 de 2011.
http://wwwhatsnew.com/2011/05/05/footprints-determina-la-localizacion-geografica-de-tu-iphoneandroid/
Último Acceso: Febrero 18 de 2012

[21]. *OWASP. The Open Web Application Security Project*
https://www.owasp.org/index.php/Main_Page
Último Acceso: Agosto 4 de 2012

[22]. Revela la localización con redes sociales a través de *Creepy.*
http://www.taringa.net/posts/linux/10304384/Revela-la-localizacion-con-redes-sociales-a-traves-de-Creepy.html
Último Acceso: Abril 29 de 2012

[23]. Dragonjar. Cómo localizar usuarios de *twitter* y *flickr* a través de sus fotos.
http://www.dragonjar.org/como-localizar-usuarios-de-twitter-y-flickr-a-traves-de-sus-fotos.xhtml
Último Acceso: Abril 28 de 2012

[24]. Pérez, Sarah. Simples pasos para mantener su seguridad (y su privacidad) en Facebook.
http://www.galileo.or.cr/uploads/media/5_simples_pasos_para_mantener_su_seguridad_y_privacidad_en_Facebook.pdf
Último Acceso: Abril 29 de 2012

[25]. Ocampo, Efraín. *Apps* de *iPhone* tampoco juegan limpio con privacidad.
http://www.bsecure.com.mx/enlinea/apps-de-iphone-tampoco-juegan-limpio-con-privacidad/
Último Acceso: Mayo 29 de 2012

[26]. Goujon, André. Especialista de *Awareness & Research. Plist*: Facebook y otras aplicaciones en móviles susceptibles al robo de contraseñas. Abril 17 de 2012.
http://blogs.eset-la.com/laboratorio/2012/04/17/plist-facebook-moviles-robo-contrasenas/
Último Acceso: Abril 18 de 2012

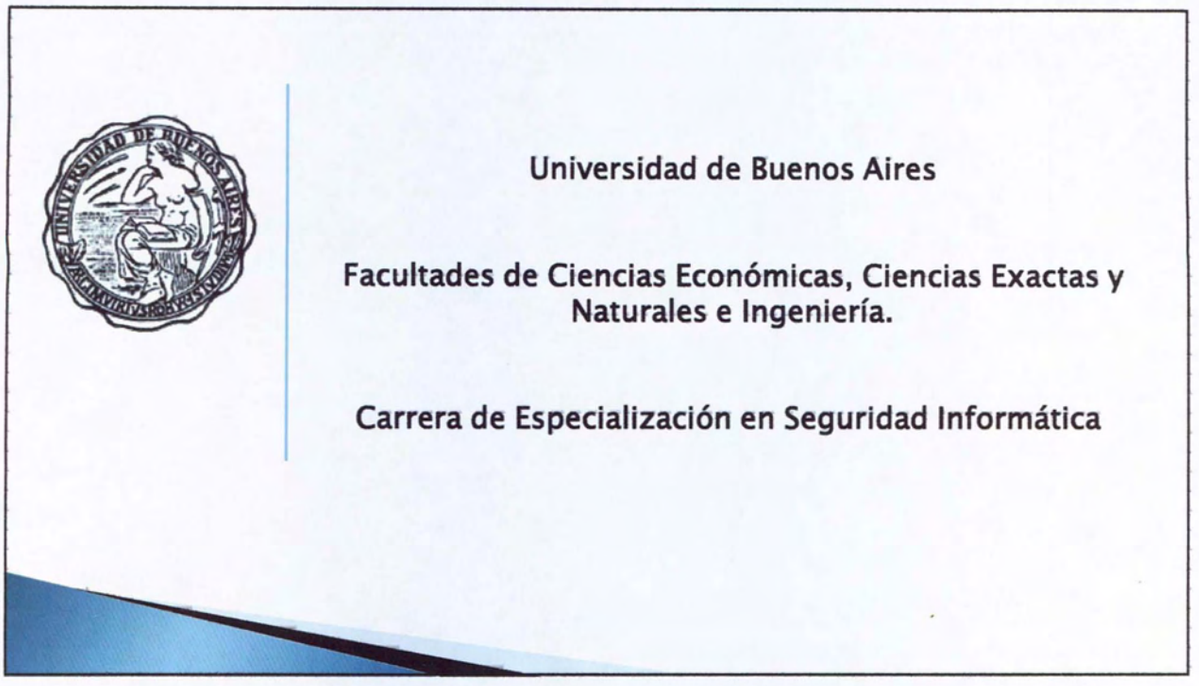
[27]. Webespacio. Villugas, Junny. *Foursquare.* Junio 7 de 2011.
http://myspace.wihe.net/foursquare/
Último Acceso: Abril 29 de 2012

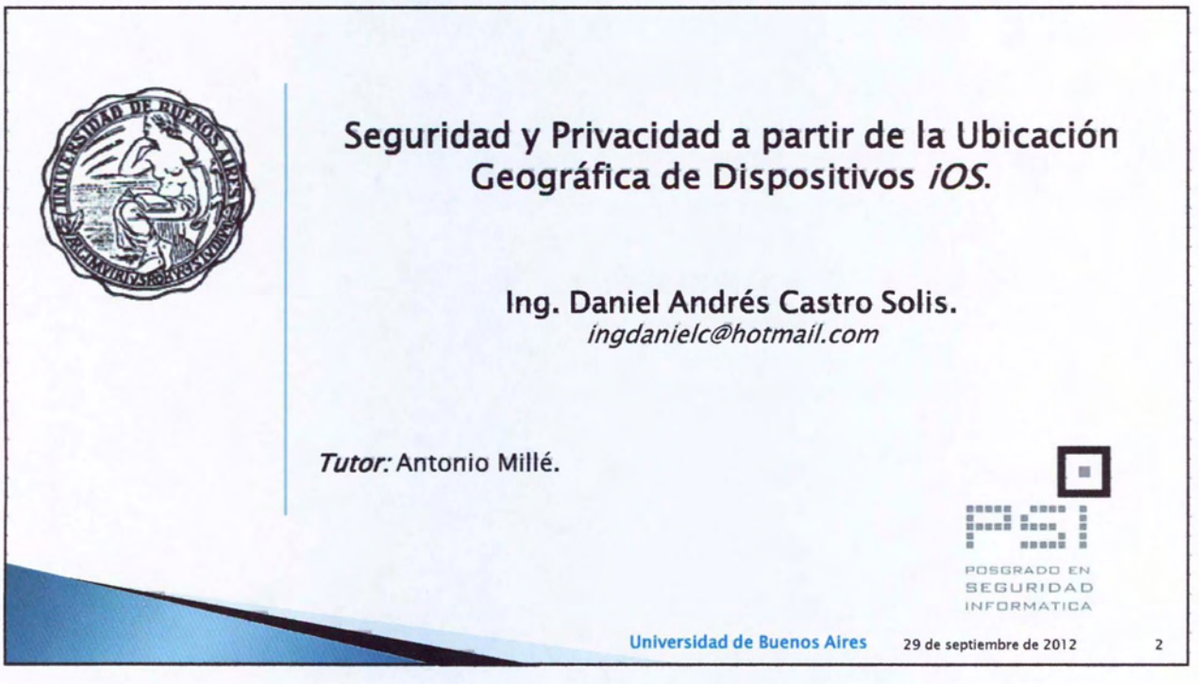
[28]. Social Media Marketing. Las redes sociales basadas en la localización, un nuevo filón para fidelizar clientes. Abril 13 de 2010.
http://www.marketingdirecto.com/actualidad/social-media-marketing/redes-sociales-localizacion-filon-fidelizar-clientes/
Último Acceso: Abril 29 de 2012

[29]. Geolocalización y redes sociales. Febrero 24 de 2012.
http://www.cyldigital.es/articulo/geo-localizacion-y-redes-sociales
Último Acceso: Abril 29 de 2012

[30]. 10 aplicaciones móviles de realidad aumentada que te transportarán al futuro.
http://www.marketingdirecto.com/actualidad/checklists/10-aplicaciones-moviles-de-realidad-aumentada-que-te-transportaran-al-futuro/
Último Acceso: Agosto 3 de 2012

[31]. *App Store* de *Apple.*
http://itunes.apple.com/es/genre/mobile-software-applications/id36?mt=8
Último Acceso: Julio 29 de 2012


Universidad de Buenos Aires
Facultades de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería.
Carrera de Especialización en Seguridad Informática


Seguridad y Privacidad a partir de la Ubicación Geográfica de Dispositivos iOS.
Ing. Daniel Andrés Castro Solis.
ingdanielc@hotmail.com
Tutor: Antonio Millé.
POSGRADO EN SEGURIDAD INFORMATICA
Universidad de Buenos Aires
29 de septiembre de 2012
2

Seguridad y Privacidad a partir de la Ubicación Geográfica de Dispositivos *iOS*.

OBJETIVOS

INTRODUCCIÓN

1. *GEO-TAGGING*
2. APLICACIONES DE GEOLOCALIZACIÓN
3. SEGURIDAD Y PRIVACIDAD
4. RIESGOS DE SEGURIDAD Y PRIVACIDAD
5. SUGERENCIAS DE SEGURIDAD Y PRIVACIDAD PARA MITIGAR RIESGOS DE GEOLOCALIZACIÓN
6. CONCLUSIONES

Seguridad y Privacidad a partir de la Ubicación Geográfica de Dispositivos *iOS*.

OBJETIVOS

INTRODUCCIÓN

1. *GEO-TAGGING*
2. APLICACIONES DE GEOLOCALIZACIÓN
3. SEGURIDAD Y PRIVACIDAD
4. RIESGOS DE SEGURIDAD Y PRIVACIDAD
5. SUGERENCIAS DE SEGURIDAD Y PRIVACIDAD PARA MITIGAR RIESGOS DE GEOLOCALIZACIÓN
6. CONCLUSIONES

Objetivos

- Recolectar y analizar información que permita entender el funcionamiento de geolocalización.
- Comprender el funcionamiento de las aplicaciones existentes que permiten obtener datos de localización geográfica del dispositivo.
- Identificar los riesgos a los que se expone el usuario si se conoce su posición geográfica.
- Hacer un análisis de seguridad y privacidad del usuario y su información a partir del conocimiento de la ubicación del dispositivo desde el cual accede a la web.

5

Universidad de Buenos Aires

Seguridad y Privacidad a partir de la Ubicación Geográfica de Dispositivos *iOS*.

6

Universidad de Buenos Aires 29 de septiembre de 2012

Introducción (1/3)

Windows phone

Universidad de Buenos Aires

7

Introducción (2/3)

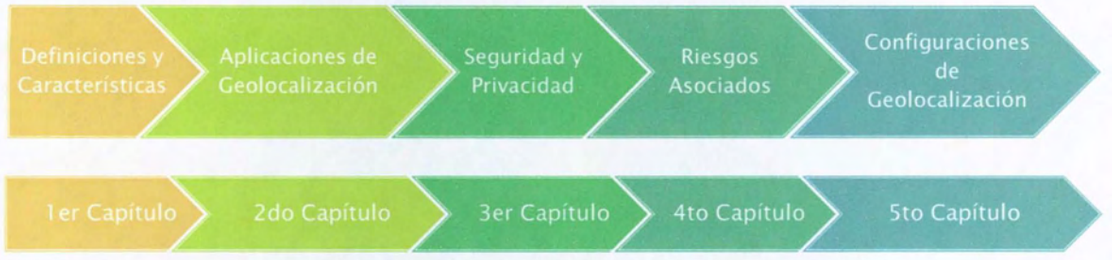
- Documentarse y entender la técnica de *geo-tagging.*
- Estudiar y Analizar aplicaciones existentes que basan su funcionamiento en la posición geográfica del usuario.
- Evaluar las implicaciones de seguridad y privacidad de dar a conocer la ubicación geográfica.
- Comprender los riesgos asociados al hecho de dar a conocer la localización geográfica.

Configuraciones adecuadas para la funcionalidad de geolocalización.

Universidad de Buenos Aires

8

Introducción (3/3)



9

Universidad de Buenos Aires

Seguridad y Privacidad a partir de la Ubicación Geográfica de Dispositivos *iOS*.

10

Universidad de Buenos Aires 29 de septiembre de 2012

Seguridad y Privacidad a partir de la Ubicación Geográfica de Dispositivos *iOS*.

1. *GEO-TAGGING*

Metadatos de Archivos Digitales

Geo-etiquetado. Definición y Características

Componentes de la Geolocalización

Mecanismos de Geo-etiquetado de Archivos Digitales

1. Geo-Tagging. (1/4)

Metadatos de Archivos Digitales

Datos que describen, caracterizan o proporcionan información acerca de otros datos con el propósito de identificarlos y referenciar de manera estandarizada cualquier información de recursos digitales y no digitales. [14][15]

- Facilitan recuperación, autentificación, evaluación, preservación, publicación, comprensión y/o interoperabilidad de información. [14]
- Refinación de consultas a buscadores.
- Presentación variable de datos.

1. Geo-Tagging. (2/4)

Geo-etiquetado. Definición y Características

La **Geolocalización**: Permite conocer nuestra ubicación geográfica automáticamente teniendo o no una conexión a internet, debido a que los dispositivos móviles actualizan constantemente nuestra ubicación, por su portabilidad. [5] "La geolocalización es la práctica de asociar un recurso digital con una locación física. ...La información del lugar se calcula con base a coordenadas de latitud y longitud..." [7]

El **geo-etiquetado** o ***geo-tagging,*** establece una relación entre la creación de archivos digitales y el lugar de creación. Es decir es el mecanismo mediante el cual se añade a los metadatos (*EXIF*) del archivo la localización geográfica donde se creó.

13

Universidad de Buenos Aires

1. Geo-Tagging. (3/4)

Componentes de la Geolocalización

- Hardware.
- Software.
- Conexión a Internet.

14

Universidad de Buenos Aires

1. Geo-Tagging. (4/4)

Mecanismos de Geo-etiquetado de Archivos Digitales

- Receptor GPS Integrado.
- *Wi-Fi* - Triangulación de Torres Celular.
- Dirección IP.
- De forma Manual.

15

Universidad de Buenos Aires

Seguridad y Privacidad a partir de la Ubicación Geográfica de Dispositivos *iOS*.

16

Universidad de Buenos Aires 29 de septiembre de 2012

Seguridad y Privacidad a partir de la Ubicación Geográfica de Dispositivos *iOS*.

2. APLICACIONES DE GEOLOCALIZACIÓN

Geolocalización en Dispositivos iOS

Aplicaciones para Dispositivos iOS

Aplicaciones con funcionalidad de Geolocalización.

Aplicaciones para Geolocalizar Dispositivos iOS

Redes sociales y Geosociales

Aplicaciones de Realidad Aumentada

Problemas de las Aplicaciones de Geolocalización

Herramientas de Geolocalización

17

Universidad de Buenos Aires

2. Aplicaciones de Geolocalización. (1/13)

Geolocalización en Dispositivos iOS

- Habilitada por default y la formas de deshabilitarla.
- Configuraciones poco intuitivas.
- Solicitud de confirmación de activación.
- Inconvenientes al desactivarla por completo.

18

Universidad de Buenos Aires

2. Aplicaciones de Geolocalización. (2/13)

Aplicaciones para Dispositivos iOS

Aplicaciones con funcionalidad de Geolocalización.

- Geo-etiquetado de Imágenes
- Puntos de interés
- Mapas y Navegación GPS

19

Universidad de Buenos Aires

2. Aplicaciones de Geolocalización. (3/13)

Aplicaciones para Dispositivos iOS

Aplicaciones con funcionalidad de Geolocalización.

- Geo-etiquetado de Imágenes

Fuente: *App Store iTunes.* http://store.apple.com/us

20

Universidad de Buenos Aires

2. Aplicaciones de Geolocalización. (4/13)

Aplicaciones para Dispositivos iOS

Aplicaciones con funcionalidad de Geolocalización.

- Puntos de interés

Fuente: *App Store iTunes.* http://store.apple.com/us

Universidad de Buenos Aires

21

2. Aplicaciones de Geolocalización. (5/13)

Aplicaciones para Dispositivos iOS

Aplicaciones con funcionalidad de Geolocalización.

- Mapas y Navegación GPS

Fuente: *App Store iTunes.* http://store.apple.com/us

Universidad de Buenos Aires

22

2. Aplicaciones de Geolocalización. (6/13)

Aplicaciones para Dispositivos iOS

Aplicaciones para Geolocalizar Dispositivos iOS

Footprints: Permite conocer la ubicación exacta o muy aproximada de donde se encuentra un determinado dispositivo móvil.

Buscar mi *iPhone:* Ayuda a encontrar dispositivos móviles y a proteger los datos desde cualquier otro dispositivo *iOS.*

Fuente: *App Store iTunes.* http://store.apple.com/us

Universidad de Buenos Aires

23

2. Aplicaciones de Geolocalización. (7/13)

Aplicaciones para Dispositivos iOS

Redes sociales y Geosociales

Fuente: *App Store iTunes.* http://store.apple.com/us

Universidad de Buenos Aires

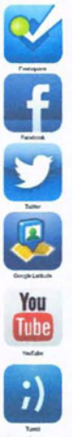
24

2. Aplicaciones de Geolocalización. (8/13)

Aplicaciones para Dispositivos iOS

Redes sociales y Geosociales

- Permiten compartir la ubicación geográfica.
- Visibilidad del perfil.
- Privacidad del perfil.
- Organizar los contactos.
- Bloquear un contacto.



Fuente: *App Store iTunes.* http://store.apple.com/us

Universidad de Buenos Aires

25

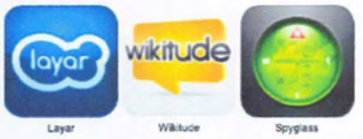
2. Aplicaciones de Geolocalización. (9/13)

Aplicaciones para Dispositivos iOS

Aplicaciones de Realidad Aumentada.

Enriquecen la visión del mundo real, asociándole información virtual que se extrae de diversas fuentes de internet.

- Geolocalización .
- Velocidad de Transmisión.
- Capacidad de Procesamiento.
- Detección de Movimiento y orientación.



Fuente: *App Store iTunes.* http://store.apple.com/us

Universidad de Buenos Aires

26

2. Aplicaciones de Geolocalización. (10/13)

Problemas de las Aplicaciones de Geolocalización

- Enviar a un servidor remoto los identificadores únicos del dispositivo (UDID) o compartir datos privados de localización e identificación.
- Almacenan las credenciales de acceso y otra información sensible sin ningún tipo de protección.
- Disminución de las configuraciones en aplicaciones móviles.

27

Universidad de Buenos Aires

2. Aplicaciones de Geolocalización. (11/13)

Problemas de las Aplicaciones de Geolocalización

- Relaciones con aplicaciones de otros fabricantes.
- Configuraciones habilitadas por defecto.
- Inadecuada relación entre la usabilidad y la cantidad de controles.
  "Clic sobre ***Configuración***, y entramos en ***Edita tu perfil publico>>***. En la ventana que se abre a continuación vamos a la zona inferior de la barra lateral de la derecha y abrimos el menú de visibilidad del perfil público en el que podremos marcar las opciones ..."

28

Universidad de Buenos Aires

2. Aplicaciones de Geolocalización. (12/13)

Herramientas de Geolocalización

Plug ins. Para la extracción de metadatos de archivos digitales. (*EXIF Viewer* junto con *Opanda IExif).*

Creepy. (Yiannis Kakavas) Permite obtener automáticamente información de geolocalización de usuarios de redes sociales como *Twitter, Flickr, Foursquare* y servicios de alojamiento de imágenes, y traza los caminos recorridos por el usuario, usando la posición GPS, de mensajes y fotos.

GeoSetter. Permite geo-etiquetar, leer o modificar etiquetas de geolocalización de archivos digitales de forma fácil, completa y con alta precisión.

29

Universidad de Buenos Aires

2. Aplicaciones de Geolocalización. (13/13)

Herramientas de Geolocalización
Sitios Web con funcionalidad de Geolocalización.

- ***Jeffrey`s Exif Viewer y Mapquest.*** Permiten consultar la ubicación geográfica de una fotografía, mapeando el resultado en un mapa.
- ***PicFog***, Permite buscar todas las imágenes que aparecen en *Twitter* por palabra clave y ubicación geográfica en tiempo real. [4]
- ***Endomondo.*** Permite llevar un registro de actividades deportivas o de vida diaria referenciadas con datos GPS.
- ***PleaseRobMe.*** Permite obtener información de localización de los usuarios de *Twitter y Foursquare* según la vayan compartiendo, [28]

30

Universidad de Buenos Aires

Seguridad y Privacidad a partir de la Ubicación Geográfica de Dispositivos *iOS*.

OBJETIVOS
INTRODUCCIÓN
1. *GEO-TAGGING*
2. APLICACIONES DE GEOLOCALIZACIÓN
3. **SEGURIDAD Y PRIVACIDAD**
4. RIESGOS DE SEGURIDAD Y PRIVACIDAD
5. SUGERENCIAS DE SEGURIDAD Y PRIVACIDAD PARA MITIGAR RIESGOS DE GEOLOCALIZACIÓN
6. CONCLUSIONES

Seguridad y Privacidad a partir de la Ubicación Geográfica de Dispositivos *iOS*.

3. **SEGURIDAD Y PRIVACIDAD**

Escenarios Vulnerables – Modalidades de Operación
Casos Reales y de Actualidad

3. Seguridad y Privacidad. (1/2)

Escenarios Vulnerables – Modalidades de Operación

- Anuncios Publicitarios.
- Blogs y Redes Sociales.
- Videos.

33

Universidad de Buenos Aires

3. Seguridad y Privacidad. (2/2)

Casos Reales y de Actualidad

- Clarín. "*UN PELIGRO. Adam Savage, conductor del popular programa estadounidense "Mythbusters", publicó en Twitter una foto geo-etiquetada de su auto estacionado frente a su casa*"
- ESET. Caso de *Joel Postman* en *Foursquare.*
- Infobae. "El FBI atrapó a un peligroso hacker gracias a foto de su novia".

34

Universidad de Buenos Aires

Seguridad y Privacidad a partir de la Ubicación Geográfica de Dispositivos *iOS*.

OBJETIVOS
INTRODUCCIÓN
1. *GEO-TAGGING*
2. APLICACIONES DE GEOLOCALIZACIÓN
3. SEGURIDAD Y PRIVACIDAD
4. **RIESGOS DE SEGURIDAD Y PRIVACIDAD**
5. SUGERENCIAS DE SEGURIDAD Y PRIVACIDAD PARA MITIGAR RIESGOS DE GEOLOCALIZACIÓN
6. CONCLUSIONES

Seguridad y Privacidad a partir de la Ubicación Geográfica de Dispositivos *iOS*.

4. **RIESGOS DE SEGURIDAD Y PRIVACIDAD**

Riesgos en el Sistema Operativo
Riesgos en Aplicaciones de Geolocalización
Riesgos en sitios Web: Redes Geosociales

4. Riesgos de Seguridad y Privacidad. (1/3)

Riesgos en el Sistema Operativo.

El sistema operativo es el elemento más sensible desde el punto de vista de seguridad pues actúa como instrumento de gestión de recursos, gestiona la información almacenada y procesada por el dispositivo. [2]

Las razones que ponen en riesgo la información de los Dispositivos Móviles:

- Código malicioso o malware.
- *Bugs* del Sistema Operativo.
- Modificación no autorizada del sistema operativo.

37

Universidad de Buenos Aires

4. Riesgos de Seguridad y Privacidad. (2/3)

Riesgos en Aplicaciones de Geolocalización.

- La naturaleza de la información que administran.
- Fallos de seguridad.
- Inadecuada configuración.
- Integración con Redes Sociales.

38

Universidad de Buenos Aires

4. Riesgos de Seguridad y Privacidad. (3/3)

Riesgos en sitios Web: Redes Geosociales.

- Riesgos en la Red de Comunicación.
- Facilidad de búsqueda y correlación de la información.
- Fuga de datos.
  Configuraciones deficientes de privacidad
  Fácil acceso a las Interfaces de Programación de Aplicaciones (API's).
- Tratamiento irresponsable de datos.

39

Universidad de Buenos Aires

Seguridad y Privacidad a partir de la Ubicación Geográfica de Dispositivos *iOS*.

40

Universidad de Buenos Aires 29 de septiembre de 2012

Seguridad y Privacidad a partir de la Ubicación Geográfica de Dispositivos *iOS*.

5. SUGERENCIAS DE SEGURIDAD Y PRIVACIDAD PARA MITIGAR RIESGOS DE GEOLOCALIZACIÓN

Sugerencias a nivel de Sistema Operativo

Sugerencias a nivel de Aplicaciones de Geolocalización

Sugerencias para desarrolladores

Sugerencias para usuarios finales

Sugerencias a nivel de Sitios Web: Redes Geosociales

Sugerencias para desarrolladores

Sugerencias para usuarios finales

Universidad de Buenos Aires

41

5. Sugerencias de Seguridad y Privacidad para Mitigar Riesgos de Geolocalización. (1/11)

Sugerencias a nivel de Sistema Operativo

- Mantener siempre actualizado el sistema operativo y utilizar software original.
- Utilizar un sistema antivirus y mantenerlo actualizado.
- Leer del instructivo las configuraciones y recomendaciones de funcionalidad de geolocalización.
- Configurar adecuadamente las opciones de localización.

Universidad de Buenos Aires

42

5. Sugerencias de Seguridad y Privacidad para Mitigar Riesgos de Geolocalización. (2/11)

Sugerencias a nivel de Sistema Operativo

- El sistema operativo debe tener la capacidad de permitir regular al usuario la precisión de la geolocalización.
- Establecer contraseñas para asegurar el acceso a los Dispositivos.
- Es recomendable realizar una copia de seguridad, establecer contraseñas y utilizar aplicaciones de seguridad.
- Se podría implementar un mecanismo criptográfico para los metadatos de contenido digital.

43

Universidad de Buenos Aires

5. Sugerencias de Seguridad y Privacidad para Mitigar Riesgos de Geolocalización. (3/11)

Sugerencias a nivel de Aplicaciones de Geolocalización

Sugerencias para desarrolladores

- La configuración debe ser bastante intuitiva y de fácil acceso.
- Construir políticas, procedimientos de seguridad, ética y uso de las funcionalidades de geolocalización.
- La geolocalización para todas las aplicaciones debe estar inicialmente deshabilitada.
- Configuraciones (activar o desactivar) de geolocalización y *geo-tagging* por aplicación.

44

Universidad de Buenos Aires

5. Sugerencias de Seguridad y Privacidad para Mitigar Riesgos de Geolocalización. (4/11)

Sugerencias a nivel de Aplicaciones de Geolocalización

Sugerencias para desarrolladores

- Al acceder a una aplicación se deberá preguntar si desea hacer uso de la funcionalidad, con qué nivel de precisión y si desea habilitarla de forma permanente para la aplicación.
- Niveles de la Resolución de ubicación. (País, Región, Ciudad, Domicilio).
- Evitar el todo o nada de la geolocalización.

45

Universidad de Buenos Aires

5. Sugerencias de Seguridad y Privacidad para Mitigar Riesgos de Geolocalización. (5/11)

Sugerencias a nivel de Aplicaciones de Geolocalización

Sugerencias para usuarios finales

- Revisar el contrato o licencia de las aplicaciones antes de instalarlas.
- Utilizar únicamente aplicaciones actualizadas y de confianza, obtenidas a través de canales de distribución pertinentes.
- Si las aplicaciones tienen la capacidad de almacenar ubicaciones se deberán configurar adecuadamente.
- Asignar los permisos mínimos necesarios al momento de instalar una aplicación.

46

Universidad de Buenos Aires

5. Sugerencias de Seguridad y Privacidad para Mitigar Riesgos de Geolocalización. (6/11)

Sugerencias a nivel de Aplicaciones de Geolocalización

Sugerencias para usuarios finales

- Es recomendable mantener el dispositivo bloqueado al conectarlo en computadores que no sean de confianza.
- "Establecer, en la configuración de la aplicación, en qué momento se permite la utilización de funciones de geolocalización, y con quién se va a compartir dicha información".
- La mayoría de las aplicaciones, utilizan las redes sociales como medio para difundirse por lo cual es recomendable revisar qué datos se publican.

47

Universidad de Buenos Aires

5. Sugerencias de Seguridad y Privacidad para Mitigar Riesgos de Geolocalización. (7/11)

Sugerencias a nivel de Sitios Web: Redes Geosociales

Sugerencias para desarrolladores

- Los sitios web de geolocalización al momento de subir archivos digitales deberían tener la capacidad de solicitar si eliminar, bloquear o configurar la resolución de la localización si se decide mostrar.
- Reducir la resolución de localización de las API's que ofrecen sitios como *Flickr* y *YouTube.*
- Considerar que muchos sitios no tienen control sobre la asociación de links que contienen archivos digitales geo-etiquetados.

48

Universidad de Buenos Aires

5. Sugerencias de Seguridad y Privacidad para Mitigar Riesgos de Geolocalización. (8/11)

Sugerencias a nivel de Sitios Web: Redes Geosociales

Sugerencias para usuarios finales

- Verificar la autenticidad del certificado del sitio al que se accede.
- Configurar el *browser* para que no dé a conocer la localización física.
- Verificar que el *browser*, complementos y *plugins* estén actualizados.
- Conectarse a redes de confianza con protocolos de seguridad adecuados.
- "Leer con detenimiento y comprender las cláusulas de privacidad de los servicios de geolocalización y las redes geosociales".

49

Universidad de Buenos Aires

5. Sugerencias de Seguridad y Privacidad para Mitigar Riesgos de Geolocalización. (9/11)

Sugerencias a nivel de Sitios Web: Redes Geosociales

Sugerencias para usuarios finales

- Revisar periódicamente la privacidad de la cuenta de los sitios y de las redes sociales.
- Si se decide publicar la geolocalización se debe evaluar el contexto para poder adecuar la precisión o resolución de la misma.
- Es prudente hacerse amigo únicamente de personas que realmente se conoce y como regla general desconfiar de todo el mundo.
- No exponer a miembros de la familia (especialmente a los pequeños).

50

Universidad de Buenos Aires

5. Sugerencias de Seguridad y Privacidad para Mitigar Riesgos de Geolocalización. (10/11)

Sugerencias a nivel de Sitios Web: Redes Geosociales

Sugerencias para usuarios finales

- Al publicar información geo-etiquetada se debe prever que esté disponible únicamente para personas de confianza.
- Evitar incluir información referente a lugares en que se encuentra un usuario en un momento dado.
- Al instalar aplicaciones dentro de la red social es importante saber que permisos se les otorga además de hacer una revisión periódica de las actividades que éstas realizan y de la información que utilizan.

51

Universidad de Buenos Aires

5. Sugerencias de Seguridad y Privacidad para Mitigar Riesgos de Geolocalización. (11/11)

"Proteger la privacidad no es sólo una cuestión de estar informado y ser responsable en el plano personal. Un amigo puede sacar una foto geo-etiquetada de nuestra casa y subirla. Hay que educarse y educar a los amigos, pero en definitiva no se tiene control alguno".

Robin Sommer.

52

Universidad de Buenos Aires

Seguridad y Privacidad a partir de la Ubicación Geográfica de Dispositivos *iOS*.

OBJETIVOS
INTRODUCCIÓN
1. *GEO-TAGGING*
2. APLICACIONES DE GEOLOCALIZACIÓN
3. SEGURIDAD Y PRIVACIDAD
4. RIESGOS DE SEGURIDAD Y PRIVACIDAD
5. SUGERENCIAS DE SEGURIDAD Y PRIVACIDAD PARA MITIGAR RIESGOS DE GEOLOCALIZACIÓN
6. **CONCLUSIONES**

53

Universidad de Buenos Aires 29 de septiembre de 2012

6. Conclusiones.

- El nivel de seguridad de las funcionalidades de geolocalización está determinada por la configuración de la misma.
- Las principales razones que ponen en riesgo la seguridad y privacidad de los usuarios de dispositivos móviles son:
  - ✓ La Publicación de información geo-etiquetada de forma innecesaria.
  - ✓ Los avanzados desarrollos que permiten realizar búsquedas sistemáticas y estructuradas de información.
  - ✓ La capacidad de los dispositivos para capturar la geolocalización.
  - ✓ Las configuraciones deficientes de la funcionalidad de geolocalización.

54

Universidad de Buenos Aires

6. Conclusiones.

- Los Principales Riesgos de la Geolocalización:
  - ✓ Pérdida o robo de los dispositivos.
  - ✓ Sufrir agresiones que afecten la integridad de los usuarios.
  - ✓ La fuga datos de localización.
- La publicación de información de localización se da principalmente por:
  - ✓ Se desea y se es consciente de la publicación.
  - ✓ Se tiene conocimiento de la existencia de la información pero no de las consecuencias.
  - ✓ Las aplicaciones no tienen un set de configuración adecuado e intuitivo.
  - ✓ Desconoce que los archivos digitales tienen la ubicación geográfica.

55

Universidad de Buenos Aires

Seguridad y Privacidad a partir de la Ubicación Geográfica de Dispositivos *iOS*.

56

Universidad de Buenos Aires 29 de septiembre de 2012


Seguridad y Privacidad a partir de la Ubicación Geográfica de Dispositivos iOS.
Gracias
Universidad de Buenos Aires
29 de septiembre de 2012
57