Sociedad Andaluza para el Desarrollo de las Telecomunicaciones
CONSEJERÍA DE EMPLEO, EMPRESA Y COMERCIO

seguridad+ Y CONFIANZA DIGITAL | AndalucíaCERT CENTRO DE SEGURIDAD TIC

Informe de divulgación

Seguridad en Aplicaciones Móviles

Tipo de documento:	*Informe*
Autor del documento:	*AndalucíaCERT*
Código del Documento:	*CERT-IF-9831-160316*
Edición:	*0*
Categoría	*Uso Interno*
Fecha de elaboración:	*16/03/2016*
Nº de Páginas	*1 de 14*

1 TABLA DE CONTENIDOS

2 OBJETIVO

El objetivo de esta publicación es ofrecer una fotografía general del mercado de aplicaciones móviles en los sistemas operativos más utilizados desde el punto de vista de la seguridad de la información.

3 ALCANCE

Este documento ofrece información básica sobre la situación actual de las aplicaciones móviles:

- estado del arte
- principales plataformas
- puntos de ataque
- desarrollo seguro de aplicaciones
- entre otros conceptos.

El público objetivo de esta información es el personal de la Junta de Andalucía y organismos atendidos por AndalucíaCERT. También puede difundirse al público en general.

4 APPS MÓVILES: PANORAMA ACTUAL

En la actualidad, vivimos un incremento exponencial de las nuevas aplicaciones móviles que están llegando tanto a las tiendas oficiales como a través de otros medios no oficiales. El desarrollo de estas aplicaciones se centra, en la mayor parte de los casos, en las prestaciones y no en la seguridad.

Los desarrolladores no se preocupan de la plataforma subyacente sobre la que están desarrollando, incluso la mayor parte de los usuarios ni siquiera se plantean el problema de la seguridad en las aplicaciones que utilizan a diario, por lo que son un fácil objetivo de ingeniería social. El *Smartphone* de hoy es igual que PC's de escritorio de hace no más de 10 años pero con mejores gráficos, más memoria y mejor conectividad.

Según el informe *Trustwave 2015 Global Security*, se han investigado 574 posibles incidentes de compromiso de la información en 15 países. Cerca del 43% eran empresas del sector *retail*, y la mayor parte de dichos incidentes fueron vulnerabilidades en aplicaciones de comercio electrónico y puntos de pago. El resultado de atacar estos sectores desemboca en que la información objetivo ha sido en un 96% el registro de clientes (pagos con tarjeta, información personalmente identificable,...).

De los informes de *Kaspersky Lab* y *Cisco*, se estima que aproximadamente entre el 98% y 99% de los programas maliciosos móviles afectan a Android.

A lo largo de los siguientes apartados, se ofrece una visión de los puntos de ataque que sufren las aplicaciones móviles hoy día y un análisis de las diferencias existentes entre aplicaciones móviles de los dos sistemas operativos más utilizados: iOS y Android.

5 APPS MÓVILES: PUNTOS DE ATAQUE

Los dispositivos móviles ofrecen nuevas funcionalidades y almacenan gran cantidad de datos, generalmente confidenciales. Ya no sólo se guardan los números de teléfono de nuestros contactos, el registro de llamadas o los SMS, sino que también almacenamos gran cantidad de información personal, como pueden ser cuentas bancarias, documentos o imágenes personales. Este hecho provoca que exista interés malintencionado por disponer de dicha información almacenada y si a esto añadimos que la complejidad de los dispositivos móviles está provocando que aparezcan agujeros de seguridad, es indispensable estar alerta para garantizar la seguridad de la información de los dispositivos.

Pero, ¿qué quieren los atacantes? ¿Cuál suele ser el objetivo de los ataques?:

- *Credenciales*. Del dispositivo o de servicios externos (e-mail, bancos, etc.)
- *Datos personales*. Nombre completo, número de seguridad social, datos de la agenda de direcciones, datos de localización, etc.
- *Datos del titular de la tarjeta de crédito*. Número de tarjeta, expiración, CVV.
- *Acceso al dispositivo*. Espiar las conexiones, usar el dispositivo para *botnet* o *spamming*, robar secretos comerciales u otra información sensible.
- *Almacén de datos*. Base de datos de aplicaciones o claves, sistema de archivos de la aplicación, cache, ficheros de configuración.
- *Binarios*. Ingeniería inversa para entender el binario, encontrar vulnerabilidades que puedan explotarse, credenciales embebidas, algoritmos de generación de claves.
- *Plataforma*. Bloqueo de funciones, instalación de *malware*, *botnets* móviles, decisiones de la arquitectura de la aplicación basada en la plataforma.

En la mayoría de los casos, el atacante consigue acceso físico al dispositivo o convence al usuario para que realice al terminal un "*jailbreaks* " o "*rooteo*" (conceptos explicados posteriormente). Una vez que el dispositivo está "rooteado", es más fácil para el atacante instalar el código malicioso, ya que al estar "rooteado" el dispositivo pierde las restricciones de seguridad del sistema.

6 APPS MÓVILES: TIPOS DE ATAQUE

A continuación, se explicarán los diferentes ataques según su tipología: ataques que se pueden ejecutar desde cualquier tipo de aplicación y ataques que se pueden ejecutar a través del navegador web.

6.1 Ataques al software: malware

Malware es un código que tiene un objetivo malicioso en el dispositivo donde se instala y se ejecuta sin el consentimiento del usuario. Su modo de funcionamiento puede ser automático o controlado remotamente. Los principales tipos de malware son:

- ***Virus.*** Programa malicioso que infecta a otros archivos del sistema con la intención de modificarlos o hacerlos inservibles. Una vez un archivo se infecta, pasa a ser un nuevo portador del virus (nueva fuente de infección). De forma genérica, estos archivos deben ser ejecutados por el usuario y su objetivo puede variar desde el robo de contraseñas hasta realizar ataques de denegación de servicio.
- ***Gusano.*** Código malicioso autorreplicable que aprovecha las vulnerabilidades de la red para propagarse. De la misma forma que el virus, tiene un objetivo oculto.
- ***Troyano.*** Código oculto dentro de otra aplicación. Busca pasar inadvertido por el usuario al instalarse en el sistema cuando se ejecuta la aplicación. Después, sin consentimiento del usuario, realizará distintas acciones ya sea de forma instantánea o programada para ejecutarse posteriormente.
- ***Backdoor.*** Código cuyo objetivo es abrir un acceso al terminal para el atacante ignorando cualquier proceso de autenticación, provocando que el dispositivo infectado pueda ser controlado remotamente por el atacante.
- ***Spyware.*** Aplicación que recoge información sin el consentimiento del usuario, siendo su objetivo vender esta información a un tercero interesado, como empresas de publicidad.
- ***Keylogger.*** Aplicación encargada de almacenar todas las pulsaciones de teclado. Por lo tanto, captura información confidencial, como el número de tarjeta de crédito o contraseñas.
- ***Hijacker.*** Programa que realiza cambios en la configuración del navegador web. Cambiando por ejemplo páginas de inicio por páginas de publicidad.
- ***Dialer.*** Código que de manera oculta realiza llamadas a teléfonos con tarifas especiales, obteniendo el atacante beneficios económicos.

Actualmente, puede encontrarse malware en la mayoría de las plataformas. La peligrosidad del mismo recae en el desconocimiento por parte de los/as usuarios/as de los peligros a los que están sometidos los dispositivos móviles, para los cuales, de forma general, no se toman las mismas medidas de seguridad que cuando se encuentran delante de un ordenador.

Una práctica muy peligrosa y común a la hora de desarrollar software es reutilizar trozos de código o software de otros desarrolladores, como librerías externas. Esto implica que no siempre los desarrolladores conocen al 100% el código fuente de su programa. En consecuencia, debido a una librería externa desconocida, puede que la aplicación quede comprometida.

6.2 Ataques en la web

En este punto se verán algunas vulnerabilidades que pueden afectar a los navegadores web y los mecanismos de seguridad existentes. Aunque existe gran cantidad de ataques que afectan a páginas web, este comunicado se centrará en los dos que más relevancia tienen cuando se habla de dispositivos móviles: "*web spoofing o phishing" y "clickjacking".*

- ***Web spoofing o phishing***.
  Es un tipo de ataque que consiste en suplantar una página web y engañar al usuario para conseguir robar información confidencial de manera fraudulenta, ya sean contraseñas, información bancaria, etc.
  Esta web tendrá un aspecto lo más idéntico posible a la original, para que el usuario a simple vista no pueda detectar que está siendo víctima de este ataque. Además es difícil percatarse ya que la única diferencia será la dirección web, que en el caso de los móviles, al tener limitaciones en el tamaño de la pantalla, no se suele ver entera.
  Se debe recalcar que la mayor atención deberá prestarse a los datos bancarios, antes de seguir algún enlace en el navegador móvil se deberá comprobar que enlaza con el sitio correcto. Una buena medida sería acceder al banco escribiendo directamente su dirección web y evitar así acceder al mismo a través de los enlaces que se puedan encontrar en los correos electrónicos.

- ***Clickjacking***
  Clickjacking es una técnica que engaña al usuario para que haga clic sobre elementos de una página web que no haría voluntariamente.
  Se lleva a cabo superponiendo dos páginas: La principal es la que contiene un elemento que le interesa al usuario como una confirmación, un enlace de descarga... la otra capa superpuesta es la que el atacante coloca para que sea pulsada por el usuario sin la intención del mismo.

7 APPS MÓVILES: SEGURIDAD EN APLICACIONES ANDROID

Lo primero que debe conocerse de las aplicaciones de Android es que casi en su totalidad están programadas en Java. Android dispone de un conjunto de librerías (C & C++) usadas por varios componentes del sistema como el *Application Framework*. Dentro de la arquitectura del sistema se pueden encontrar dos opciones: ***DVM*** *(Dalvik Virtual Machine)* y ***ART*** *(Android Runtime).*

Las aplicaciones tienen componentes que el sistema puede instanciar y ejecutar por separado cuando sea necesario. Estos componentes son de 4 tipos: Actividades, Servicios, Receptores de mensajes de difusión y Proveedores de contenido, pero no es objetivo de este comunicado entrar en profundidad.

Para centrarse en el tema de seguridad se busca proteger los datos de los usuarios, recursos del sistema incluyendo las comunicaciones y proporcionar aislamiento de las aplicaciones. Para conseguir esto Android provee las siguientes características:

- *Robusta seguridad a nivel de sistema operativo gracias al kernel de linux*.
  El sistema operativo permite limitar el código nativo que se ejecuta en los dispositivos, por ejemplo, si alguna aplicación trata de explotar una vulnerabilidad, el sistema impedirá que las zonas de memoria reservadas por otras aplicaciones se vean afectadas. El kernel también provee un mecanismo de seguridad para las comunicaciones entre procesos.
  Como el sistema operativo es multiusuario, es objetivo para la seguridad aislar los recursos de una aplicación respecto a otras, previniendo que entre distintos usuarios puedan leerse los ficheros, agotar su memoria o recursos de procesamiento el uno del otro.

- *Necesidad de ejecutar todas las aplicaciones en un entorno sandbox*.
  Se ofrece al usuario como una ventaja para identificar y aislar los recursos de las aplicaciones. Android asigna un identificador único a cada aplicación que ejecuta, otorgándole un espacio de memoria reservado para ello, permitiendo establecer mayor seguridad entre las aplicaciones y el sistema. Por defecto, las aplicaciones no pueden interactuar entre sí y poseen un acceso limitado al sistema operativo, por ejemplo, en el caso de que una aplicación trate de invadir el espacio asignado a otra, el sistema operativo se encarga de evitarlo gracias a los permisos y privilegios establecidos para cada aplicación.

- *Proceso de comunicación interno seguro y necesidad de solicitud de permisos*.
  Sólo es posible realizar operaciones de lectura por defecto, exceptuando carpetas especiales como la asignada a la tarjeta SD. Hay disponible un modo seguro de arranque en el que sólo están disponibles las herramientas del núcleo que fueron instaladas por defecto, asegurando un sistema libre de aplicaciones de terceros.
  Al tener un sistema de ficheros basado en permisos, se asegura que ningún usuario, excepto el autor, puede modificar o alterar el espacio reservado para una aplicación o los ficheros pertenecientes a ella. Cada aplicación se ejecuta bajo los permisos de un usuario específico. A menos que el autor de una aplicación exponga implícitamente sus ficheros a aplicaciones de terceros, éstos no podrán ser leídos. A partir de la versión 3.0 incluye un sistema de ficheros completamente cifrado, opción que podrá configurar el administrador del dispositivo.
  Además, ofrece mejoras en la memoria como utilizar ASLR para aleatorizar los lugares claves de la memoria, evitar desbordamientos de pila, prevenir desbordamiento de enteros, etc.

- *Firmado de aplicaciones*.
  Todas las aplicaciones en Android están encapsuladas en el formato de empaquetado APK, dicho formato es utilizado para la instalación y distribución de aplicaciones. Todos los ficheros *.apk* están firmados con un certificado que permite identificar al autor.
  Durante la instalación se comprueban los permisos que requiere la aplicación y se le pregunta al usuario, acción que no se realizará nunca más. Existen algunas lagunas de seguridad, como que las aplicaciones de manera habitual son firmadas con certificados autofirmados, por lo que no requiere ninguna autoridad certificadora que asegure que dicha aplicación no representa riesgo

para el usuario. La posibilidad de crear permisos personalizados puede suponer un riesgo para la privacidad de los usuarios.

Con uno de los últimos cambios en las políticas de permisos de *Google Play Store*, los usuarios ya no son notificados acerca de ciertos cambios en los permisos solicitados por las aplicaciones.

8 APPS MÓVILES: SEGURIDAD EN APLICACIONES IOS

Todo cambia drásticamente si se habla de la plataforma iOS de Apple. Las diferencias son notables en todos los aspectos. El primero de ellos es que la gran mayoría de las aplicaciones están escritas en Objetive-C o incluso en C. iOS refuerza estrictamente los límites de la aplicación y sandboxing. Las aplicaciones no pueden comunicarse directamente con otras aplicaciones o acceder a directorios que no sean los suyos.

El *Jailbreak* consiste en encontrar un exploit en el kernel además de un espacio de usuario que permita ejecutar código sin firmar. Hay herramientas en internet que ayudan a hacerlo en cuestión de unos minutos e incluso puede ser ocultado para el usuario final.

iOS es el sistema operativo que utilizan los dispositivos de iPhone, iPad y iPod Touch. El sistema operativo maneja el hardware y ofrece las tecnologías necesarias para el desarrollo de aplicaciones nativas. La arquitectura en iOS está estructurada en capas. Las inferiores tienen servicios y tecnologías fundamentales mientras que las superiores se apoyan en las inferiores y ofrecen tecnologías y servicios más sofisticados. Las capas son Cocoa Touch, Media, Core Services y Core OS. Las capas superiores suelen ofrecer abstracciones de las capas inferiores y su uso se simplifica.

Si nos situamos en el ámbito de seguridad, Apple tiene 4 capas de seguridad en iOS para proteger a los usuarios y sus datos: Seguridad en el dispositivo, Seguridad de los datos, Seguridad de red y Seguridad de aplicación. Alineándose con el objetivo de este informe, se profundizará en el apartado de seguridad en las aplicaciones.

Las aplicaciones se ejecutan en un Sandbox que es un entorno donde se supone que la aplicación no es fiable y por tanto queda aislada de otros procesos y recursos disponibles para el sistema operativo. Este sandbox limita los ciclos de CPU, y el acceso a ficheros fuera de su propio directorio. Además, incorpora el firmado de las aplicaciones para velar por el código binario que se permite ejecutar en el dispositivo.

Por último, Apple incorpora un canal de claves *(keychain)* que ofrece un sistema centralizado de almacenamiento y recuperación de claves encriptadas, credenciales de red y otro tipo de información relacionada. Una aplicación no puede acceder a información del *keychain* de otras aplicaciones.

9 APPS MÓVILES: SEGURIDAD EN OTRAS PLATAFORMAS

En los puntos anteriores se ha hablado de los dos sistemas operativos más utilizados hoy día pero no hay que dejar de lado otros que también tienen actualmente su lugar en el mercado.

Por ejemplo, Windows Phone sigue aumentando su cuota en el mercado. Durante el año 2013 aumentó un 90.9% y actualmente tiene entre el 3% y el 4% de las ventas en el mercado, una posición que se ha ganado sobre todo con la gama Lumia de Nokia.

Centrándonos en la seguridad de este sistema operativo, como en el resto, la mayoría de características de seguridad están activadas por defecto. Microsoft prueba las aplicaciones que se descargan desde la Tienda oficial de Windows Phone y las cifra para asegurarse de que no se instale accidentalmente software malintencionado en el teléfono.

También existen varias formas para proteger la información del dispositivo. Por ejemplo, se puede configurar un PIN de la Cartera, Windows Phone proporciona una capa de seguridad adicional para las compras en su Tienda oficial, y dicho PIN evita también que se puedan realizar pagos no deseados por NFC. También lleva integrado OneDrive (sistema de almacenamiento en la nube de Microsoft) que sube automáticamente las fotos para respaldarlas, y las copias de seguridad del dispositivo completo. De forma gratuita también incorpora un servicio para encontrar el teléfono al igual que Android e iOS.

Otro de los sistemas operativos que más se han visto en estos últimos años, sobre todo en el sector empresarial, es BlackBerry. Apuesta por optimizar la productividad y poner al alcance del mundo corporativo el acceso remoto a la información en forma inalámbrica, rápida y segura. BlackBerry protege la integridad, confidencialidad y autenticidad de los datos corporativos con un esquema de cifrado seguro que cifra los datos mientras se transfieren en el servidor de BlackBerry y los dispositivos móviles.

Para proteger la información almacenada en estos dispositivos es posible aplicar políticas personalizables como ser autenticado por contraseña, que se vuelva a pedir tras un periodo de inactividad, cifrado de datos a través de directivas, mantenimiento de contraseñas de forma segura en el dispositivo mediante el cifrado AES,... Además los administradores del sistema central pueden crear y enviar comandos remotamente para cambiar las contraseñas de los dispositivos, bloquear o borrar información de forma remota en dispositivos perdidos o robados.

Hay más características en seguridad de BlackBerry: en las aplicaciones se firma el código y se usan certificados digitales, utilizan autenticación RSA SecurID en ambos sentidos, usan HTTPS para acceder a datos, S/MIME para que los usuarios puedan firmar y cifrar correos, soporte PGP o compatibilidad con el cifrado de correos de Lotus Notes... entre otras.

Por último, se verá la plataforma SymbianOS que actualmente no está siendo muy utilizada por los usuarios pero no por ello es menos importante a la hora de mencionar como gestiona la seguridad:

- Uso de protocolos TKS, WTLS y IPSec para sus comunicaciones.

- Uso de certificados X.509 a través de repositorios certificados usuario y CA.
- Los desarrolladores obtienen un *ACS Published ID* (certificado digital) de Verisign y la aplicación se envía a Symbian donde el código deberá pasar una evaluación independiente que lo analiza y prueba bajo ciertos criterios.

Se debe nombrar el primer intento por parte de Symbian de diseñar una plataforma de seguridad a partir de la v.9 denominado *Platsec*. Dicha plataforma busca detectar accesos no autorizados al hardware, software o datos y prevenir que los programas actúen de forma ilegítima (malware).

10 APPS MÓVILES: MECANISMOS DE PREVENCIÓN

Se mostrarán ahora algunos mecanismos de prevención en la capa de aplicación. Se empezará por ver el mercado de aplicaciones, se verán mecanismos de seguridad que se pueden utilizar en la web y finalmente se describirán distintos tipos de aplicaciones que pueden aumentar el nivel de seguridad en los dispositivos móviles.

11.1 Mercado de aplicaciones

En los dispositivos móviles actuales, casi toda la seguridad se ha centrado en la creación de un punto centralizado y fiable para descargar y gestionar las aplicaciones. Se trata de lo que denominamos Mercado de Aplicaciones. Cada mercado de aplicaciones puede tener políticas más o menos restrictivas, ya sea respecto al tipo de contenido, o a su potencial peligrosidad.

Puede haber mercados que permiten todas las aplicaciones, indiferentemente de quién las haya publicado y de su funcionalidad, y mercados que tienen un control para limitar las aplicaciones accesibles, esto está ligado a la existencia de un proceso previo de revisión. En estos mercados, el control elimina aplicaciones que puedan causar un mal funcionamiento del sistema o que directamente sean maliciosas. El problema es que cada aplicación tiene que ser revisada por completo antes de ser publicada, lo que ralentiza su publicación.

Los dos más conocidos son el Android Market y la Appstore. Estos mercados de aplicaciones también pueden permitir una actualización de las aplicaciones. Ésta debe ser una tarea realizada periódicamente, ya que las nuevas aplicaciones, aparte de mejoras en el rendimiento y funcionalidad, suelen solucionar vulnerabilidades detectadas que podrían ser explotadas.

11.2 Navegador web

Por defecto, todos los sistemas operativos incorporan una aplicación encargada de la navegación web. Estos navegadores, al igual que los navegadores de los PC's, pueden ejecutar código muy complejo a nivel de usuario, con el nivel de privilegios que éste tenga establecido. Los lenguajes más utilizados son HTML/DHTML y JavaScript. Además, el contenido multimedia puede ser directamente abierto desde aquí, ejecutando otras aplicaciones que también pueden tener vulnerabilidades.

No obstante, no hay protección a nivel de usuario que sea infalible ya que por ejemplo existen técnicas de ataque *man in the middle* que no dependen de la intervención del usuario, por lo que debería vigilarse las páginas a las que se accede y las ejecuciones de código.

Una buena medida podría ser el uso del protocolo HTTPS que crea un canal seguro sobre una red insegura garantizando protección contra distintos tipos de ataques. Esta seguridad se basa en utilizar cifrado, certificados digitales y una autoridad de certificación, que actúan como *tercera parte de confianza*, en las que tanto la web como el usuario final deben confiar.

11.3 Aplicaciones de seguridad

Hay aplicaciones que pueden contribuir a aumentar el nivel de seguridad del sistema añadiendo nuevas capas de seguridad como métodos de autenticación adicionales más restrictivos, sistemas de copia de seguridad, cifrado de datos, aplicaciones antivirus o cortafuegos...

Por ejemplo, una acción imprescindible cuando se trabaja con información es realizar copias de seguridad. En los dispositivos móviles se almacena hoy día mucha información, pero es complicado ya que cada aplicación puede almacenar los datos internamente. Por esto, es importante disponer de una aplicación que facilite y automatice este proceso.

Respecto al cifrado y ya que se almacena información delicada como documentos oficiales o datos bancarios, resulta útil añadir una capa más de seguridad y cifrar estos datos. Así se garantiza que, en caso de pérdida, la información sea ilegible para alguien no autorizado.

Igual de recomendable que es tener un antivirus en un equipo PC, lo es tenerlo en los dispositivos móviles. Debido al gran crecimiento de los malware creados para sistemas móviles, empiezan a ser necesarias aplicaciones que analicen los ficheros para evitar infecciones.

Alguna de estas aplicaciones, a modo de ejemplo, es CONAN, que es una aplicación gratuita que ayuda a proteger el dispositivo móvil Android. Permite conocer el estado de seguridad del dispositivo mostrando soluciones a posibles riesgos a los que esté expuesto y proporcionando algunos consejos que ayudan a mejorar la seguridad del mismo.

Dentro de sus funciones CONAN analiza si está instalada alguna aplicación maliciosa, verifica que todas las aplicaciones se encuentren correctamente actualizadas y comprueba si la configuración del dispositivo es la correcta. Es una aplicación gratuita y se puede encontrar en la tienda oficial. Otra de sus funciones muy interesantes es la clasificación de los permisos que las aplicaciones declaran necesitar, lo que puede suponer un gran riesgo, ya que la mayoría de los usuarios suele aceptarlos sin conocimiento y en realidad se le está dando acceso a una aplicación de terceros a la información almacenada en el dispositivo como, por ejemplo, acceso a los contactos del mismo.

Por último, también analiza las conexiones de red realizadas por las aplicaciones instaladas advirtiendo al usuario de aquellas que pueden ser potencialmente maliciosas, obteniendo información relevante de estas conexiones como por ejemplo la geolocalización de las direcciones IP.

En el caso de iOS existe gran variedad de aplicaciones orientadas a la seguridad, muchas de ellas focalizadas al control y gestión de las contraseñas como *1Passe*, *Secretum* o *Keeper*.

Buscando algo diferente podemos encontrar aplicaciones como *HiFolder*. Esta aplicación proporciona seguridad desde varios puntos de vista a los dispositivos móviles iOS. En cuanto a la

protección de datos, consta de contraseña de disfraz, que ocultará los datos en caso de que alguien te obligue a introducirla, contraseña para las distintas carpetas, patrón del bloqueo, y función de ocultar archivos. También permite gestionar archivos y hacer fotos, entre otras funciones, desde la aplicación para ahorrar en la transmisión de datos.

En resumen, es un mercado que todos los días sigue creciendo y van apareciendo nuevas aplicaciones que nos ayudan a mantener un nivel de seguridad razonable sobre toda la información que reside en nuestros dispositivos móviles.

11.4 Ingeniería social

Desde AndaluciaCERT consideramos que es otro punto imprescindible en este documento hablar sobre la ingeniería social. Se han visto en estos últimos años filtraciones de fotos de celebridades, artículos de debilidades de sistemas informáticos y hasta coches que han sido objeto de ataques informáticos. Pero muchas veces se olvida hablar del elemento más débil del sistema: el humano.

Por ejemplo un caso conocido es el de Kevin Mitnick, el hacker del teléfono. Buena parte de sus acciones se basaron en su habilidad para extraer información por teléfono a las víctimas. Sus acciones se fundamentaban en cuatro aspecto básicos, comunes en la mayoría de las personas: todos queremos ayudar, el primer movimiento es siempre confianza hacia el otro, no nos gusta decir que no y a todos nos gustan las alabanzas.

Una estrategia habitual de Mitnick era la de hacer ver que ya tenía determinada información. Cuando hablando con otra persona, daba una determinada información de forma incorrecta, como una contraseña o un número de teléfono, el interlocutor le solía corregir, logrando de esta forma gran cantidad de información que sería dificil obtener de otra manera. No importa cuánto esfuerzo pongan las compañías en mejorar sus sistemas informáticos, si el ser humano siempre va a seguir siendo vulnerable y susceptible de ser engañado o dar información por error.

Aplicado a este documento, se podría hablar de varios puntos. Por ejemplo, aplicaciones maravillosas o con más funcionalidades que las que solemos tener, que se pueden descargar directamente desde internet y no a través de la tienda oficial, suelen ser aplicaciones malintencionadas que requerirán más permisos de lo normal y que pueden acceder a información sensible. Incluso hoy día, aplicaciones de uso cotidiano como las más conocidas de redes sociales, van requiriendo más permisos, como por ejemplo el acceso a nuestra libreta de direcciones con la excusa de poder encontrar a tus contactos en dicha red social y poder agregarlos, pero que en última instancia están recabando información sensible y números de teléfono de nuestros compañeros, familia o conocidos.

Por esto, es importante que además de seguir mejorando continuamente en la seguridad de los dispositivos móviles, se invierta tiempo y recursos en poder formar al eslabón más débil, nosotros mismos, en una serie de buenas prácticas a adoptar para prevenir cometer fallos que puedan hacer que nuestra información se vea comprometida.

11 CONCLUSIONES

A lo largo de los apartados anteriores se ha intentado abarcar gran parte de los puntos de interés de la seguridad en aplicaciones móviles: cuáles son los objetivos de estos ataques, qué tipos de ataques existen, cómo pueden prevenirse y algunas aplicaciones de seguridad que pueden complementar nuestros dispositivos móviles para hacerlos más robustos.

Es fundamental darle importancia a este tema ya que cada día trabajamos con más dispositivos móviles y lo más relevante es que cada vez almacenamos en ellos información y datos más confidenciales. Por lo que es conveniente estar siempre actualizado e informado sobre nuevas medidas de seguridad o nuevos ataques o vulnerabilidades que vayan apareciendo y de esta forma, intentar ser más proactivos a la hora de prevenir que nuestra información pueda verse comprometida.

Se han explicado distintos mecanismos de seguridad en los diferentes sistemas operativos, pero ninguno de ellos adquiere al completo su efectividad si los usuarios no tomamos conciencia y seguimos unas buenas prácticas a la hora de utilizar los mismos.

Como conclusión final se podría decir que para evitar el compromiso de toda la información que reside en nuestros dispositivos móviles se debe intentar mantener sistemas operativos y aplicaciones actualizadas, evitar descargar aplicaciones de lugares que no sean las tiendas oficiales, comprobar si los permisos que requieren estas aplicaciones son los adecuados para sus funciones y ser conscientes de que habrá personas que intenten aprovechar nuestro desconocimiento para adquirir información, por lo que debemos ser precavidos para poder disfrutar de la tecnología de una forma segura.

12 GLOSARIO

Retail: Es el sector industrial que entrega productos al consumidor final.

CVV: Es el número de tres dígitos impreso en el panel de firma en la parte posterior de la tarjeta de crédito.

Botnet: Es un término que hace referencia a un conjunto o red de robots informáticos o bots, que se ejecutan de manera autónoma y automática.

Spam: Hace referencia a los mensajes no solicitados, no deseados o con remitente no conocido (correo anónimo), habitualmente de tipo publicitario, generalmente enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor.

ASLR: Técnica de seguridad informática focalizada a la prevención de ataques de desbordamiento (*buffer overflow*).

S/MIME: Es un estándar para criptografía de clave pública y firmado de correo electrónico encapsulado en MIME. Siendo MIME una serie de convenciones o especificaciones dirigidas al intercambio a través de Internet de todo tipo de archivos (texto, audio, vídeo, etc.) de forma transparente para el usuario.

HTTPS : Es un protocolo de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de Hipertexto, es decir, es la versión segura de HTTP.

PGP : Es un programa desarrollado por Phil Zimmermann y cuya finalidad es proteger la información distribuida a través de Internet mediante el uso de criptografía de clave pública, así como facilitar la autenticación de documentos gracias a firmas digitales.

Man in the middle : Es un ataque en el que se adquiere la capacidad de leer, insertar y modificar a voluntad, los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado.

13 DOCUMENTACION DE REFERENCIA

- *https://www.csirtcv.gva.es/es/paginas/seguridad-en-aplicaciones-m%C3%B3viles.html*
- *http://seguridadparaaplicaciones.com/*
- *http://www.eslared.org.ve/walc2012/material/track4/M%F3viles/SeguridadAndroidAospina.pdf*
- *https://www.exabyteinformatica.com/uoc/Informatica/Tecnologia_y_desarrollo_en_dispositivos_moviles/Tecnologia_y_desarrollo_en_dispositivos_moviles_%28Modulo_6%29.pdf*
- *https://www.incibe.es/extfrontinteco/img/File/demostrador/monografico_seg_disp_moviles.pdf*
- *https://www.apple.com/es/business/docs/iOS_Security_Guide_es_Oct14.pdf*
- *http://www.tic.udc.es/~nino/blog/lsi/reports/seguridad-permisos-android.pdf*
- *https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/11-ccn-stic-453-seguridad-en-android/file.html*
- *http://www.cybsec.com/upload/CYBSEC_Seguridad_Blackberry_Sobrero.pdf*
- *http://e-archivo.uc3m.es/bitstream/handle/10016/17873/Memoria%20PFC,%20F.J.Castellanos.pdf?sequence=1*