SEGURIDAD EN DISPOSITIVOS MÓVILES CON SISTEMAS OPERATIVOS ANDROID Y IOS

SAFETY DEVICES MOBILE OPERATING SYSTEM ANDROID AND IOS

Juan Carlos Albarracín Galindo
juancalbarracin@gmail.com
Universidad Pedagógica y Tecnológica de Colombia
Escuela de Ingeniería de Sistemas y Computación
Tunja, Colombia

Leidy Maribel Parra Camargo
leidy.parra30@gmail.com
Universidad Pedagógica y Tecnológica de Colombia
Escuela de Ingeniería de Sistemas y Computación
Tunja, Colombia

Juan José Camargo Vega
jjcamargovega@yahoo.com
Universidad Pedagógica y Tecnológica de Colombia
Escuela de Ingeniería de Sistemas y Computación
Tunja, Colombia

Tipo de Articulo: Investigación

Fecha de recepción
Octubre 10 de 2013
Fecha de Aceptación
Noviembre 8 de 2013

ABSTRACT

This paper presents an analytical perspective of the relevant aspects related to security in the mobile devices with operating systems: Android and IOS; where describes the background, and subsequently to present a conceptualization of fundamental aspects of operating systems under study, as well as a definition of the main attacks carried out on each of the platforms. Finally determine the security mechanisms that can be implemented by the user, in order to minimize potential risks present at the time of use mobile devices.

Keywords

Android,IOS, security, mobile devices.

RESUMEN

Este trabajo presenta una perspectiva de análisis de los aspectos relevantes relacionados con la seguridad en los dispositivos móviles con sistemas operativos:

Android y IOS, donde se describen los antecedentes, y posteriormente presentar una conceptualización de los aspectos fundamentales de los sistemas operativos en estudio, así como una definición de los principales ataques llevados a cabo en cada una de las plataformas.

Finalmente determinar los mecanismos de seguridad que se pueden implementar por el usuario, con el fin de minimizar los posibles riesgos presentes en el momento de los dispositivos móviles de uso.

Palabras clave

Android, IOS, seguridad, dispositivos móviles

INTRODUCCIÓN

Seguridad en los dispositivos móviles se define como “la disciplina que se ocupa de diseñar las normas, procedimientos métodos y técnicas destinados a conseguir un sistema seguro y confiable” según [1]; partiendo de ese concepto se describen los principales aspectos relacionados con la seguridad: tipos de seguridad, propiedades de un sistema de información seguro, análisis de los riesgos, entre otros.

En fundamentals of Information Systems Security [2], ofrece una visión global de los fundamentos de la seguridad, en donde se abre con una discusión de los nuevos riesgos, amenazas y vulnerabilidades asociadas con la transformación de un mundo digital, incluyendo un vistazo a la forma en como los negocios, el gobierno y los individuos que operan hoy en día.

DISPOSITIVOS MÓVILES

Debido a la importancia que han adquirido los dispositivos móviles en el desarrollo tanto tecnológico como empresarial. En [3] se presenta un estudio de las principales problemáticas de seguridad que exhibe el uso de estos en el ámbito empresarial. En primer lugar, el ¿cómo evitar que los usuarios

utilicen el dispositivo con fines que no sean los corporativos?. En segundo lugar se plantean, los riesgos presentes en la incorporación de información sensible en las memorias de almacenamiento de estos dispositivos. Partiendo de lo anterior se determina que las principales debilidades de seguridad en el uso de los mismos son inherentes a: la tecnología, las aplicaciones y al factor humano.

El estudio realizado por [4] señala que actualmente "los dispositivos móviles contienen una gran cantidad de información confidencial de sus propietarios, convirtiéndose en un importante elemento para ellos y transformándose en una extensión de sus propias identidades.", razón por la cual se examina la seguridad en dichos dispositivos, basados en el análisis de los hábitos y riesgos de los usuarios de móviles, tabletas y computadores portátiles.

En [5], menciona que no hace muchos años los dispositivos móviles se encontraban casi exentos de varios riesgos de seguridad al no estar interconectados con la red; pero que con los avances tecnológicos que permiten a dichos dispositivos conectarse y descargar contenido de la red, actualmente se encuentran expuestos a las mismas amenazas de seguridad que los equipos informáticos.

El informe sobre amenazas móviles [6], afirman que "los dispositivos móviles son la tecnología de consumo de más rápido crecimiento", además, señalan que las aplicaciones móviles están convirtiendo a estos dispositivos en una plataforma de computación de uso general y que, como su popularidad van en aumento, también lo hacen los incentivos para los atacantes. Por lo anterior, analizan las principales amenazas que afectan principalmente a las plataformas iOS y Android.

En la monografía [7], señalan que "actualmente está ocurriendo una de las revoluciones más importantes que se han producido en la última década: la posibilidad de disponer y utilizar las tecnologías de la información en cualquier lugar, momento y desde múltiples tipos de dispositivos". Unido a esto, "las tecnologías móviles también han traído consigo diversos riesgos asociados a la privacidad, a la fuga de información - ya sea intencionada o no - o el código malicioso (malware) que, en el último año, ha experimentado un fuerte crecimiento en los dispositivos móviles". Por tal razón, se dan a conocer las soluciones de seguridad que el mercado pone al alcance y que van a permitir hacer un uso más seguro de las tecnologías móviles.

En el trabajo [8], razona sobre la seguridad móvil basado en que en la actualidad los dispositivos móviles se han convertido en una herramienta primordial en la sociedad; además, expone los riesgos a los cuales se enfrentan los usuarios de estos dispositivos y posibles soluciones de seguridad móvil.

Sistemas operativos

En [9], trata los conceptos clave de los sistemas operativos, de manera que ayude a entender al lector los fundamentos fácilmente. Se presentan las definiciones y términos relacionados a los sistemas operativos independientemente de la plataforma.

Según [10] presenta los conceptos básicos de los sistemas operativos, enfocándose en el diseño, las políticas de gestión de recursos y aquellas técnicas que se emplean generalmente para administrar: el procesador, la memoria, las entradas y salidas, entre otros.

Sistema Operativo Android

Los resultados de [11], demuestran cómo Android se ha convertido en la plataforma más popular para dispositivos móviles, a pesar de que este sistema operativo aún posee problemas de rendimiento que pueden llegar a considerarse como críticos. En la investigación se presenta a “AndroScope” como una herramienta para el análisis de rendimiento tanto de la plataforma como de sus aplicaciones.

Para [12] a medida que las empresas fabricantes de dispositivos móviles aumentan la adopción de Android como sistema operativo, las necesidades de rendimiento de la plataforma serán más exigentes, por tal razón se estudió el rendimiento de la plataforma con una aplicación de software de referencia.

Generalidades de Android

Sistema operativo basado en Linux, diseñado principalmente para móviles e inicialmente desarrollado por Android, Inc., una compañía que más tarde fuera comprada por Google. La mayoría del código fuente de este sistema, se encuentra bajo licencia Apache, licencia de software libre y código abierto [20]. En este, se encuentran los drivers necesarios para el acceso al hardware, en concreto, para la gestión de sus dispositivos. En principio, el desarrollador no accederá directamente a esta capa, sino que utilizará una serie de librerías que están en un nivel superior [21]. Estas librerías se encuentran programadas en C; sin embargo, el programar accede a estas desde un API (Application Programming Interface) de Java, lenguaje que se usa para el desarrollo de

Android. Para esto, el sistema incluye una máquina virtual java (JVM), Dalvik, la cual ejecuta archivos .dex en lugar de los .class clásicos de java.

Algunas de las características relevantes que tiene el sistema Android son:

- El framework de aplicaciones que permite el reemplazo y la reutilización de los componentes
- El navegador integrado el cual está basado en el motor open Source Webkit; SQlite base de datos para almacenamiento estructurado que se integra directamente con las aplicaciones
- El soporte para medios con formatos comunes de audio, video e imágenes planas; máquina virtual Dalvik entre otras.

Arquitectura Android

La arquitectura interna de Android está formada básicamente por cinco (5) componentes [22]:

- Aplicaciones: las cuales se incluye Como base un cliente email, programa de SMS, calendario, mapas, navegador, contactos y otros. Todas escritas en lenguaje de programación Java.
- Framework de aplicaciones: los desarrolladores de Android, tienen acceso al código fuente usado en aquellas que son base, esto para que no se generen más componentes distintos, que respondan a la misma acción (reutilización de componentes).
- Librerías: Android incluye en su base de datos un set de librerías C/C++, que son presentadas a todos los desarrolladores a través del framework de las aplicaciones. Algunas son: System C library, bibliotecas de medios, bibliotecas de gráficos, 3D y SQLite, entre otras.
- Runtime de Android: incorpora un set de librerías que aportan la mayor parte de las funcionalidades disponibles en las librerías base del lenguaje de programación Java. Cada aplicación Android corre su propio proceso, con su propia instancia de la máquina virtual Dalvik. Dalvik ejecuta archivos en el formato Dalvik Executable (.dex), el cual está optimizado para memoria mínima.
- Núcleo Linux: Android depende de Linux para los servicios base del sistema como seguridad, gestión de memoria, gestión de procesos, pila de red y modelo de controladores. Este, además actúa como una capa de abstracción entre el hardware y el resto de la pila de software.

Sistema Operativo iOS

[13] ofrece una mirada a profundidad de los métodos y procedimientos para analizar los dispositivos con sistema operativo iOS, además se detalla un conjunto de datos, información y conocimientos de hardware, brindados por la propia empresa Apple para ayudar a los investigadores que estudian estos dispositivos.

En [14], se describe la arquitectura del sistema operativo iOS, además detalla cada una de las capas que lo componen y presentan el SDK (siglas de Software Development Kit) del sistema operativo iOS que proporciona los recursos necesarios para desarrollar aplicaciones nativas de iOS.

Generalidades de iOS

Desarrollado por Apple Inc., inicialmente solo para el teléfono inteligente de la compañía (iPhone), luego fue extendido a otros dispositivos como el iPod Touch, iPad y el Apple TV. Se deriva de Mac OS X, el cual está basado en Darwin BSD.

iOS cuenta con (4) cuatro capas de abstracción: el núcleo del sistema operativo, los "Servicios Principales", los "Medios" y "Cocoa Touch" [23].

Las principales características que posee iOS son [24]:

- Interfaz de usuario: se basa en el concepto de manipulación mediante gestos multi-touch. Los elementos de esta se componen por deslizadores, interruptores y botones. La respuesta es inmediata y fluida en las aplicaciones. La interacción con el sistema operativo se realiza mediante movimientos como deslizar y tocar.
- SpringBoard: es la pantalla principal, donde se ubican los iconos de Aplicaciones y el Dock en la parte inferior de la pantalla se pueden anclar aplicaciones de uso frecuente.
- Aplicaciones: iOS incluye múltiples aplicaciones entre las que se destacan: phone (video conferencia y teléfono), email, safari (navegador web), mensajes, calendario, fotos, cámara, iTunes, App Store (tienda de aplicaciones), Nike + iPod, Siri (asistente por control de voz), entre otras.
- Soporte multitarea: el sistema operativo permite le ejecución de aplicaciones en segundo plano, permitiendo la posibilidad de utilizar varias a la vez.

Arquitectura iOS

Se basa en capas, en donde las más altas se encargan de contener las tecnologías y servicios de mayor importancia para el desarrollo de las aplicaciones; los servicios básicos son controlados por las más bajas [25]

- Cocoa Touch: es la capa de mayor relevancia en el desarrollo de aplicaciones para este sistema operativo, basándose en un conjunto de Frameworks proporcionados por el API de Cocoa; en donde se destacan: UIKit encargado de contener todas las clases que son necesarias para el desarrollo de una interfaz de usuario y Foundation que define algunos servicios del sistema operativo.
- Media: se proveen los servicios gráficos y multimedia.
- Core Services: domina los servicios fundamentales necesarios para la ejecución de las aplicaciones.
- Core OS: constituye las características de bajo nivel, como lo son: drivers, manejo de memoria, seguridad ficheros del sistema.

DISPOSITIVOS MÓVILES

Son aparatos de tamaño pequeño, que se caracteriza por poseer capacidades de procesamiento, memoria limitada y una conexión que puede ser permanente o interrumpida hacía alguna red; dispositivo que se ha diseñado con un fin específico pero que además puede llevar a cabo otro tipo de funciones más generales [15]. Una característica fundamental en este tipo de dispositivos es que deben ser lo suficientemente pequeños para ser transportados y empleados durante su traslado, de una manera fácil; así como también la gran capacidad de comunicación, que le permitirá acceder a la información y servicios independientemente del lugar en donde se encuentre.

Al momento de tratar el concepto de dispositivo móvil, se piensa en un teléfono móvil, pero es importante resaltar que actualmente existe en el mercado una gran variedad de estos dispositivos.

TIPOS DE DISPOSITIVOS MÓVILES

A continuación se presentan algunos de los dispositivos móviles existentes en el mercado:

Asistente Digital Personal (PDA)

Las PDA son agendas personales electrónicas que se caracterizan por su capacidad para el almacenamiento de datos, lo anterior debido a que poseen la cantidad de memoria necesaria para esta función [16]; teniendo en cuenta el éxito que tuvieron en los últimos años, este

tipo de dispositivos continúan presentes en el mercado, pero su uso se ha trasladado en su gran mayoría al ámbito empresarial, en donde se hacen muy útiles debido a sus aplicaciones de información geográfica, paquetes ofimáticos, clientes de correo electrónico, navegadores web entre las principales [17].

Teléfono móvil Inteligente (SmartPhone).

Este tipo de dispositivos se presentan actualmente como los más ligeros, portables y cómodos [18], la principal función que cumplen es la de realizar y recibir llamadas; adicionalmente los "Smartphone" se hacen cada vez más atractivos para el usuario, debido a que permiten la instalación y ejecución de aplicaciones, de gran utilidad para los compradores, entre las más relevantes se pueden encontrar: cámara fotográfica, grabación de video, gestor de correos electrónicos, chats, redes sociales, GPS, navegador web entre otras.

Tabletas

Las tabletas actualmente representan un gran porcentaje de los dispositivos móviles existentes en el mercado, su nombre se deriva del término en ingles "Tablet", que hace referencia a un computador portátil. Una de las principales características es la integración de una pantalla táctil que brinda facilidades de interacción con tan solo el contacto con los dedos. Este tipo de dispositivos también permite la ejecución de aplicaciones de gran acogida en el mercado actual. Los principales proveedores en la actualidad de esta tecnología son las empresas Apple y Samsung, que implementan en sus dispositivos los sistemas operativos iOS y Android respectivamente.

Empresas fabricantes de dispositivos móviles y sus sistemas operativos

Entre las principales empresas dedicadas a la producción de Smartphone se encuentran [19], ver tabla 1:

Empresa	Sistema operativo de los dispositivos móviles
Apple	Ios
Samsung	Android
HTC	Android, Windows Phone
Nokia	Windows Phone, Symbian OS
Motorola	Android
Sony	Android

Tabla1. Empresas y sistemas operativos móviles: Fuente los Autores

Principales ataques y amenazas en Android y ios

Con el crecimiento acelerado del negocio de la telefonía móvil en los últimos años, dos (2) empresas se

desatacan en la actualidad debido a la dominación del mismo: Apple con su sistema operativo iOS, y Google con Android; pero de la misma manera que ha crecido dicho negocio los ataques informáticos hacía estos dispositivos también lo han hecho, en donde tan solo en un año se ha pasado de registrar cerca de unos 792 a más de 36000 [26], lo que evidencia que la atención de los delincuentes informáticos actualmente se está desviando hacia esta área tecnológica.

Con la llegada del nuevo servicio en la nube KSN de la compañía Kaspersky Lab diseñado para prestar servicio a los dispositivos móviles con plataforma Android, se facilitó la recopilación de información y estadísticas, que permitieron determinar las amenazas detectadas con mayor frecuencia en dichos dispositivos [27].

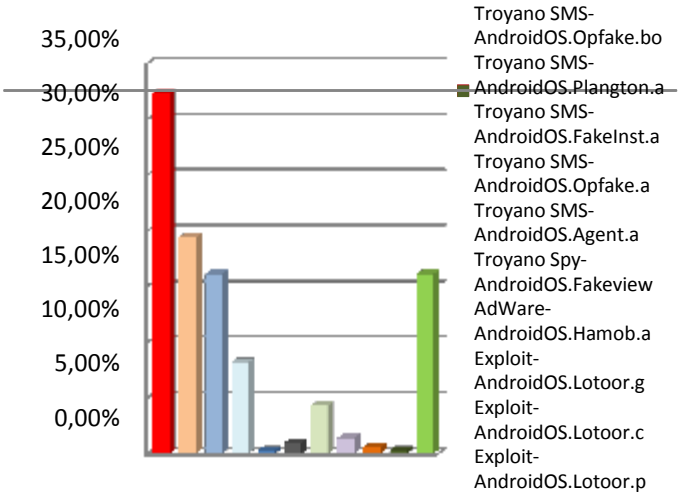

Figura 1. Principales ataques contra el sistema operativo Android. Adaptada de [27]

En la Fig. 1 se muestran las estadísticas capturadas por el servicio KSN, en donde se evidencia que los principales ataques hacia los dispositivos con sistema operativo Android son representados principalmente por: Troyanos SMS, adware y exploits.

- Troyanos SMS: con una incidencia del 76,3% (SMS-AndroidOS.Opfake.bo, SMS-AndroidOS.FakeInst.a, SMS-AndroidOS.Agent.a, SMS-AndroidOS.Plangton.a, SMS-AndroidOS.Opfake.a y SMS-AndroidOS.Fakeview)

Según la Fig. 1, son una categoría de códigos maliciosos para teléfonos móviles que se fundamentan en la capacidad de suscribir a la víctima a números de mensajería Premium, filtrando los SMS provenientes de dichos números con el fin de impedir al usuario percatarse de la infección, de tal forma

que los mensajes relacionados con la cuenta Premium no aparecerán; representado lo anterior un riesgo financiero para el usuario al no poder consultar su saldo o estado de cuenta, debido a que podría incurrir en costosos cargos. Este tipo de ataque representa una de las categorías más antiguas de códigos maliciosos para teléfonos móviles [28].

Los Troyano SMS; generalmente funcionan de la siguiente forma: como primera medida el usuario descarga el malware inadvertidamente, posteriormente el Troyano envía un SMS a un número Premium, sin el consentimiento de la víctima, el SMS es transportado a través de la red de la compañía de telefonía prestadora de la plataforma SMS, en donde el código malicioso bloquea los mensajes de confirmación para finalmente permitir que el cibercriminal genera ganancias ilícitas mediante el aprovechamiento de la cuenta del usuario.

- Adware: según la Fig. 1 este tipo de ataque se presenta con una frecuencia del 4,3%, en donde su ejecución es automática y tiene como objetivo fundamental el mostrar publicidad. Se ocultan en programas ofrecidos gratuitamente que incluyen dentro de sus condiciones de uso, que generalmente no son leídas por el usuario, en donde se acepta que se ejecuten las funciones que muestran dicha publicidad [29].

- Exploits: son programas que se han diseñado para sacar provecho de las vulnerabilidades de un software, representan el 2,3% (Exploit-AndroidOS.Lotoor.g, Exploit-AndroidOS.Lotoor.c y Exploit-AndroidOS.Lotoor.p) de los ataques a esta plataforma (véase Fig. 1); en la gran mayoría de ocasiones estos ataques se realizan con fines maliciosos. Estas vulnerabilidades no son más que errores en la programación, que pueden ser aprovechados como puerta de entrada de ataques.

Así mismo la empresa de seguridad Symantec en su informe Internet Security Threat Report 2013 [30] presenta las cifras respecto a las vulnerabilidades de seguridad en dispositivos móviles durante al año 2012. En ellas ha quedado reflejado que el sistema operativo iOS tiene un mayor número de vulnerabilidades conocidas en 2012 que Android, aunque éste sigue siendo más atacado con malware.

Dentro de los ataques más conocidos que se realizan al sistema operativo iOS, se encuentran:

- Iphone Exploit Code: básicamente el ataque consiste en colocar el computador del atacante a través del metasploit como un webserver a la escucha de solicitudes de conexión provenientes de los móviles navegando por Internet. Cuando la víctima acceda al webserver, el navegador Safari se cerrará automáticamente, el usuario, podrá abrirlo nuevamente y continuar utilizándolo, sin embargo, en el equipo del atacante se tendrá un Shell remota con permisos privilegiados sobre el sistema, pudiendo acceder a los correos configurados en el equipo, a los contactos, a los archivos de sistemas a fin de modificar los archivos de host o dns [31].

- Ikee.Co Malware.iPhoneOS/Ikee.C@SSH+ Otros: gusano que afecta a móviles iPhone que utilicen la contraseña por defecto del root en el servicio SSH del teléfono, únicamente afecta a terminales a los que se les ha practicado el "jail-break". Cambia la imagen de fondo del terminal. Cuando se ejecuta, detiene remotamente el demonio SSH y elimina el inicio automático en la opción de reiniciar el servicio SSH [32].

- Ikee.Bo Malware.iPhoneOS/Ikee.B@SSH+ Otros: gusano que se propaga a dispositivos iPhone que han sido modificados para permitir la instalación de software no oficial. Consiste en el robo información sensible, bloquea la pantalla y muestra el siguiente texto: "¡El iPhone ha sido hackeado porque es realmente inseguro!", y solicita el pago de 5 euros para la liberación del dispositivo y, además, modifica la contraseña del usuario root [32].

- Aurora Feint: este fue un juego lanzado para la plataforma, su manera de atacar era subiendo los datos de los contactos almacenados en la libreta de direcciones a la base de datos del desarrollador y ocupa estos datos para enviar spam [33].

- Ataques D.O.S. y de Spam en iOS iMessages app: estos ataques consisten en la denegación de servicios, haciendo imposible abrir la aplicación iMessages para leer los mensajes y dejando inutilizado el servicio [34].

- Phishing: este ataque tiene como objetivo intentar obtener de un usuario sus datos, claves, cuentas bancarias, números de tarjeta de crédito, identidades, para luego ser usados de forma fraudulenta; puede producirse de varias formas, desde un mensaje, una web que simula una entidad, una ventana emergente, y la más usada y

conocida por los internautas, la recepción de un correo electrónico [35].

- Cross-site scripting (XSS): es una vulnerabilidad que aprovecha la falta de mecanismos de filtrado en los campos de entrada y permiten el ingreso y envió de datos sin validación alguna, aceptando él envió de scripts completo [36].
- URL spoofing: este tipo de ataque consiste en mostrar una dirección URL falsa en la barra de direcciones de Safari el navegador por defecto de iOS, permitiendo incluso tomar información de la tarjeta de crédito cuando se realizan compras en la tienda de Apple [37].

Soluciones de seguridad para los dispositivos con sistemas operativos Android y IOS

La constante evolución tecnológica ha llevado a que la sociedad actual sea más vulnerable a los ataques informáticos, debido a que hoy en día la dependencia de los dispositivos móviles presenta un crecimiento acelerado en sus cifras, a tal punto que en nuestro país Colombia, se ha alcanzado un aumento en el año 2012 que supera el 270% en activaciones de dispositivos móviles con los sistemas operativos Android y iOS, según se indica en la Fig. 2 adaptada del estudio realizado por [38].

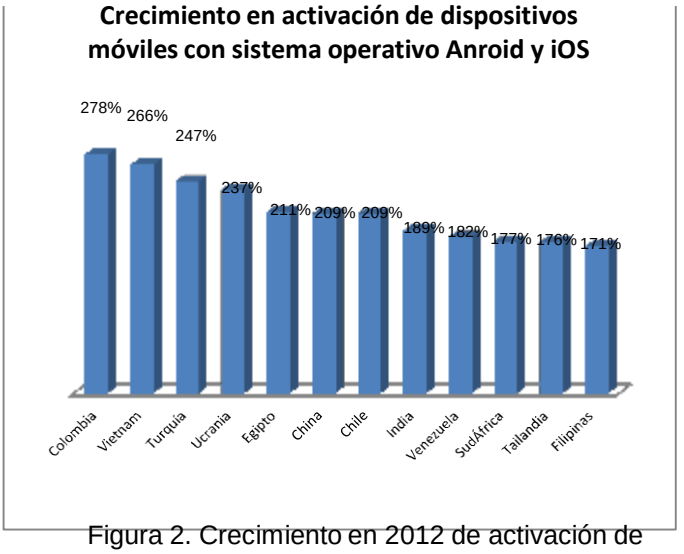

Figura 2. Crecimiento en 2012 de activación de dispositivos móviles. Adaptada de [38].

Lo anterior con el fin de demostrar el por qué en la sección anterior se indicaba que los delincuentes informáticos están enfocando sus actividades hacia este tipo de dispositivos, volviéndolos cada vez más vulnerables. Por esta razón se hace indispensable el conocer las diferentes soluciones de seguridad existentes actualmente, cuyo propósito fundamental es el minimizar el riesgo de que el usuario se vea afectado por cualquiera de los ataques anteriormente descritos.

Para el sistema operativo Android las soluciones para disminuir la posibilidad de ser afectados por un malware, se concentran básicamente en cinco (5) puntos:

1) El primero es estar consciente de que los dispositivos móviles en la actualidad son tan vulnerables a los ataques como cualquier otro tipo de dispositivos, lo que permitirá estar atento a cualquier anomalía que se pueda percibir.
2) El segundo punto es prestar especial atención a las aplicaciones que se van a descargar, en donde los más importante es revisar el tipo de aplicación a ejecutar, con lo que se asegurará el conocer exactamente los recursos de hardware que la misma utilizará.
3) En tercer lugar se sugiere verificar las fuentes de donde provienen las descargas, no todos los desarrolladores de aplicaciones que no están en el Android Market tienen fines criminales, pero las probabilidades de sufrir un ataque malicioso si aumentan con las descargas provenientes de estas fuentes; en donde una posible solución para este punto es restringir la instalación de aplicaciones provenientes de desarrolladores que no sean oficiales para Android Market.
4) Como cuarto, es importante revisar los permisos que solicitan las aplicaciones al momento de ser instaladas, para de esta manera conocer a profundidad cuales son los accesos que podrá llegar a tener la misma y en caso de no estar de acuerdo poder optar por la decisión adecuada a tiempo.
5) Por último y un aspecto fundamental en este contexto es el hacer uso de un antimalware, en los que actualmente muchos de los proveedores más reconocidos de seguridad están enfocando sus esfuerzos, buscando mantenerse un paso delante de los cibercriminales ubicando una diversidad de herramientas (tanto gratuitas como pagas) en el mercado.

Apple tiene un modelo de seguridad de cuatro (4) pilares para disminuir el número de ataques que sufren los dispositivos con el sistema operativo iOS [8]: control de acceso tradicional, iOS proporciona la seguridad tradicional de todos los dispositivos móviles, como configuración de contraseñas para el bloqueo, y otras más avanzadas para el desbloqueo, la cual ante un determinado número de intentos incorrectos para desbloquear el dispositivo; elimina el contenido automáticamente la recuperación de la información se puede realizar mediante copias de seguridad; almacenadas en iTunes, a la cual solo tiene acceso el propietario del dispositivo.

Procedencia de las aplicaciones, como cualquier persona puede desarrollar aplicaciones para iOS y algunas de estas pueden traer consigo malware, Apple dispone App Store, donde se encuentran centralizadas todas las aplicaciones certificadas para móviles con este

sistema operativo. Cifrado, iOS cuenta con un cifrado hibrido, en el cual se usa una aceleración el hardware para compendiar los datos almacenados en la memoria flash.

Aislamiento, iOS aísla cada aplicación del resto instaladas en el dispositivo, lo que impide que estas instalen controladores, malware y conozcan que otras aplicaciones existen.

Para hacer que el sistema de seguridad implementado por iOS funcione, se debe evitar que el dispositivo cuente con Jailbreak, el cual elimina las limitaciones impuestas por Apple en los dispositivos con iOS y que permite a los usuarios acceder al sistema operativo y de esta manera descargar aplicaciones y extensiones que no se encuentran disponibles en el App Store, pues quedan mucho más expuestos al malware y a ataques informáticos.

CONCLUSIONES.

En La utilización de los dispositivos móviles, y en especial de Smartphone, con fines de negocio incrementa de forma acelerada día a día, sin embargo se debe tener en cuenta que como éstos manejan información trascendental, existe una gran motivación por parte de los ciberdelincuentes para atacarlos y obtener la información que poseen; por lo cual, es de suma importancia que los usuarios conozcan los peligros y riesgos a los que se ven expuestos al utilizar sus Smartphone.

En un país como el nuestro, en donde, el uso de los dispositivos móviles se ha convertido en parte fundamental para el desarrollo de las actividades cotidianas, es importante conocer los riesgos que se presentan con la adopción de esta tecnología, con el fin de acoger las medidas necesarias para aprovechar al máximo las facilidades que brindan sin poner en riesgo la información que contienen los mismos.

Se evidencia que los dispositivos con sistema operativo Android, actualmente son los que presentan mayor incidencia de ataques informáticos, por lo cual los usuarios deben prestar atención a los mecanismos existentes para proteger la información contenida en los mismos; para prevenir los ataques de tipo Troyanos SMS, se deben verificar los permisos que tienen las aplicaciones que se instalan; para los Adware y Exploits se recomienda la utilización de un anti-virus.

REFERENCIAS

[1] P. A. López, Seguridad informática, 1st ed., vol. 1. Editex, 2010.

[2] D. Kim and M. Solomon, Fundamentals of Information Systems Security, 1st ed., vol. 1. Jones & Bartlett Learning, 2010.

[3] C. Caracciolo and S. Ezequiel, "Seguridad en Dispositivos Móviles; Smartphone-Pocket PC," 2011 [En linea]. Disponible en: http://ebookbrowse.com/seguridad-en-dispositivos-moviles-smartphone-y-pocket-pc-pdf-d89717861. [Revisado: 02-JUN-2013].

[4] Kaspersky Lab, "SEGURIDAD EN DISPOSITIVOS MÓVILES EN ESPAÑA," 2012 [En linea]. Disponible en: http://webcache.googleusercontent.com/search?q=cache:CCbX6tJY878J:https://www.inteco.es/file/pEdja0pwhXbAyyRDEuknZg+&cd=1&hl=es&ct=clnk&gl=co. [Revisado: 02-JUN-2013].

[5] INTECO, "Estudio sobre seguridad en dispositivos móviles y smartphones," 2012.

[6] L. M. Security. 2011 Mobile Threat Report. [En linea]. Disponible en: https://www.lookout.com/resources/reports/mobile-threat-report. Revisado: 11-May-2013].

[7] INTECO. Monográfico de Seguridad: seguridad en dispositivos móviles [En linea]. Disponible en: http://cert.inteco.es/extfrontinteco/img/File/demostrador/monografico_seg_disp_momovil.pdf [Revisado: 11-May-2013].

[8] J. V. A. Lagunes, "Seguridad en dispositivos móviles," Facultad de Contaduría y Administración, Universidad Veracruzana, Veracruz, 2012.

[9] A. Sibsankar and A. Alex A.,Operating Systems. Pearson Education India, 2010.

[10] C. Santiago, G. Carmelo Rubén , Q. Alexis , S. Francisco José , and S. José Miguel, Fundamentos de sistemas operativos: teoría y ejercicios resueltos. Editorial Paraninfo, 2007.

[11] Myeongjin Cho, Ho Jin Lee, Minseong Kim, and Seon Wook Kim, "AndroScope: An Insightful Performance Analyzer for All Software Layers of the Android-Based Systems," ETRI Journal, vol. 35, no. 2, pp. 259–269, Apr. 2013.

[12] Hyeon-Ju Yoon, "A Study on the Performance of Android Platform," International Journal on Computer

Science & Engineering, vol. 4, no. 4, pp. 532–537, Apr. 2012.

[13] A. Hoog and K. Strzempka, iPhone and iOS Forensics: Investigation, Analysis and Mobile Security for Apple iPhone, iPad and iOS Devices. Elsevier, 2011.

[14] "iOS Technology Overview: Introduction". [En linea]. Disponible en: http://developer.apple.com/library/ios/#documentation/Miscellaneous/Conceptual/iPhoneOSTechOverview/Introduction/Introduction.html#//apple_ref/doc/uid/TP40007898. [Revisado: 11-May-2013].

[15] A. Baz , F. Irene , Á. María , and G. Rosana, "Dispositivos móviles ," 2009.

[16] "Introducción a los dispositivos móviles," http://developer.apple.com/library/ios/#documentation/Miscellaneous/Conceptual/iPhoneOSTechOverview/Introduction/Introduction.html#//apple_ref/doc/uid/TP4000789

[17] Guachun Andrés."42 programas para tu PDA Palm OS." [En linea]. Disponible en: http://www.pdaexpertos.com/Articulos/Experiencias_de_Usuarios/42-programas-pda-palm-os.shtml [Revisado: 11-May-2013].

[18] Mediasmash2.0, "¿Qué tipos de dispositivos móviles hay? | Smash Media," ¿Qué tipos de dispositivos móviles hay? | Smash Media, 26-2012. [En linea]. Disponible en: http://smash-media.blogspot.com/2012/04/que-tipos-de-dispositivos-moviles-hay.html. [Revisado: 11-May-2013].

[19] M. S. Vargas , R. Diego de Jesús, R. Gustavo, M. Christian , and R. Hugo, "Análisis estratégico del sector teléfonos móviles inteligentes smartphones," 2012.

[20] A. O. S. Project. Android Open Source Project license [En linea]. Disponible en: http://source.android.com/source/licenses.html. [Revisado: 11-May-2013].

[21] O. H. Alliance. Android [En linea]. Disponible en: http://www.openhandsetalliance.com/android_overview.html. [Revisado: 11-May-2013].

[22] A. Vilchez. Que es Android: Características y Aplicaciones [En linea]. Disponible en: http://www.configurarequipos.com/doc1107.html Revisado: 11-May-2013].

[23] EcuRed. iOS [En linea]. Disponible en: http://www.ecured.cu/index.php/IOS . [Revisado: 11-May-2013].

[24] Apple. Qué es iOS [En linea]. Disponible en: http://www.apple.com/es/ios/what-is/ [Revisado: 11-May-2013].

[25] "Arquitectura iOS - Tecnología iOS." [En linea]. Disponible en: https://sites.google.com/site/tecnologiaiostm/desarrollo-de-aplicaciones/arquitectura-ios Revisado: 11-May-2013].

[26] "Las Empresas Eligen iOS Ante el Aumento de Malware Contra Android," iPadizate. [En linea]. Disponible en: http://www.ipadizate.es/2013/04/17/empresas-eligen-ios-malware-android-69504 /. [Revisado: 12-May-2013].

[27] D. Máslennikov, "Evolución de los programas maliciosos para dispositivos móviles Parte 6," virulist.com, 03-May-2013. [En linea]. Disponible en: http://www.viruslist.com/sp/analysis?pubid=207271207 [Revisado: 12-May-2013].

[28] G. André and R. Pablo, "Troyano SMS Boxer," ESET, Oct. 2012.

[29] J. D. Aycock, Spyware and adware. Springer, 2011.

[30] Symantec, "Internet Security Threat Report 2013", Abril-2013. [En linea]. Available: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf . [Revisado: 14-May-2013].

[31] Independent Security evaluators. "Exploiting the iPhone". [En linea]. Disponible en: http://securityevaluators.com/content/case-studies/iphone// . [Revisado: 03-Jun-2013].

[32] INTECO. [En linea]. Disponible en: http://cert.inteco.es/virusSearch/Actualidad/Actualidad_Virus/Resultados_de_la_bububusq_de_virus_y_bulos/?keyWord=&alert=&virusType=&findAfter=&findBefore=&platform=generic_55&spreadType=&attachment=&spreadText=&md5=&postActiop=getVirusResults&typeSearch=lucene . [Revisado: 03-Jun-2013].

[33] Spencer E. Ante. "El lado oscuro de las aplicaciones para celulares". [En linea]. Disponible en:

http://www.estoyenbaja.com/artDes.php?iA=462 . [Revisado: 03-Jun-2013].

[34] Seguridad Apple. "Ataques D.O.S. y de Spam en iOS iMessages app", 30-Marzo-2013. [En linea]. Disponible en: http://www.seguridadapple.com/2013/03/ataques-dos-y-de-spam-en-ios-imessage.html . [Revisado: 03-Jun-2013].

[35] Seguridad Apple. "Vulnerabilidad de SMS Spoofing en iPhone". [En linea]. Disponible en: http://www.seguridadapple.com/2012/08/vulnerabilidad-de-sms-spoofing-en-iphone.html . [Revisado: 03-Jun-2013].

[36] CVE Details. "Security Vulnerabilities (Cross Site Scripting (XSS))". [En linea]. Disponible en: http://www.cvedetails.com/vulnerability-list/vendor_id-49/product_id-15556/version_id-95758/opxss-1/Apple-Iphone-Os-4.0.1.html. [Revisado: 03-Jun-2013].

[37] Chris Foresman. "Address spoofing vulnerability discovered in Mobile Safari on iOS 5.1". [En linea]. Disponible en: http://arstechnica.com/apple/2012/03/address-spoofing-vulnerability-discovered-in-mobile-safari-on-ios-51/ . [Revisado: 03-Jun-2013].

[38] Flurry Mobile, "China Knocks Off U.S. to Become World's Top Smart Device Market." 2013 [En linea]. Disponible en: http://blog.flurry.com/bid/94352/China-Knocks-Off-U-S-to-Become-World-s-Top-Smart-Device-Market . [Revisado: 03-Jun-2013].