

MONOGRAFIA "CARACTERÍSTICAS Y PARÁMETROS DE LA SEGURIDAD
PARA LOS SMARTPHONES CON SISTEMA OPERATIVO ANDROID".

RUBEN DARIO OSORIO HERRADA
CARLOS ALBERTO RAMIREZ HERRERA

UNIVERSIDAD TECNOLÓGICA DE PEREIRA
FACULTAD DE INGENIERÍAS
PROGRAMA DE INGENIERÍA DE SISTEMAS Y COMPUTACIÓN
PEREIRA
2011

MONOGRAFIA "CARACTERÍSTICAS Y PARÁMETROS DE LA SEGURIDAD
PARA LOS SMARTPHONES CON SISTEMA OPERATIVO ANDROID".

RUBEN DARIO OSORIO HERRADA
CARLOS ALBERTO RAMIREZ HERRERA

Monografía

Asesor: Omar Iván Trejos
Ingeniero de sistemas y computación

UNIVERSIDAD TECNOLÓGICA DE PEREIRA
FACULTAD DE INGENIERÍAS
PROGRAMA DE INGENIERÍA DE SISTEMAS Y COMPUTACIÓN
PEREIRA
2011

Notas de aceptación

Firma presidente del jurado

Firma del jurado

DEDICATORIA

A nuestros padres por su amor, apoyo, paciencia, comprensión y expectativas en nosotros dos para la culminación de la carrera y de este proyecto de grado, ya que hasta el último momento de la carrera recibimos el apoyo de ellos.

AGRADECIMIENTOS

Queremos agradecer especialmente por su tiempo y dedicación al Ingeniero Omar Iván Trejos, quien fue nuestro asesor y un miembro más a lo largo de este nuestro proyecto.

Queremos dar nuestros agradecimientos por todo el tiempo dedicado, la buena disposición y la atención a los ingenieros Carlos Augusto Meneses y Julio Cesar Chavarro de la facultad de Ingeniería de Sistemas, quienes siempre se mostraron muy atentos a lo largo del desarrollo de este proyecto.

A la Universidad Tecnológica de Pereira, por la formación académica brindada a lo largo de la carrera.

Finalmente a los compañeros de estudio, quienes a lo largo de la carrera nos acompañaron y ayudaron en nuestra formación.

CONTENIDO

	pág.
CAPITULO 1 GENERALIDADES	12
1.1 TITULO.....	12
1.2 DESCRIPCIÓN DEL PROBLEMA.....	12
1.3 JUSTIFICACIÓN DEL PROBLEMA	13
1.4 OBJETIVOS.....	14
1.4.1 Objetivo general	14
1.4.2 Objetivos específicos.....	14
1.5 MARCO DE REFERENCIA.....	15
1.5.1 Marco conceptual	15
1.5.1.1 ¿Qué es Android?.....	15
1.5.1.2 ¿Cómo está compuesto Android?	15
1.5.1.3 Características de Android	16
1.5.1.4 Arquitectura de Android.....	16
1.5.2 Estado del Arte	19
1.5.2.1 Seguridad en dispositivos móviles.....	19
1.5.2.2 Acceso de archivos	19
1.5.2.3 Permisos de aplicación.....	20
1.5.2.4 Encriptación de datos	21
1.5.2.5 Sistema de intrusión detección y prevención	21
1.6 DISEÑO METODOLÓGICO.....	21
1.6.1 Hipótesis.....	21
1.6.2 Tipo de investigación	21
1.6.3 Población.....	21
CAPITULO 2 SMARTPHONES.....	22
2.1 INTRODUCCIÓN	22
2.2 HISTORIA.....	22
2.2.1 Smartphones	22
2.2.2 Android.....	28

2.2.2.1	El gPhone.....	28
2.2.2.2	Lanzamiento de Android.....	29
2.2.2.3	Lego.....	29
2.3	EVOLUCIÓN DEL MERCADO DE SMARTPHONES.....	30
2.4	EL FUTURO QUE VIENE	32
2.4.1	Móvil como medio de pago.....	33
2.4.2	Aplicaciones Bancarias.....	33
2.4.3	Seguimiento de individuos.....	33
2.4.4	Vulnerabilidades por redes WiFi.....	33
2.4.5	Ataques de ingeniería social avanzada.....	33

CAPITULO 3 CARACTERÍSTICAS Y PARÁMETROS DE SEGURIDAD DE		
LOS SMARTPHONES.		34
3.1	KITS DE DESARROLLO DE APLICACIONES (SDKS).....	35
3.1.1	SDK de Android.....	35
3.1.2	SDK de Blackberry	36
3.1.3	SDK de Nokia.....	37
3.1.4	iOS.....	38
3.2	MERCADOS DE APLICACIONES	39
3.2.1	App Store de Apple.....	39
3.2.2	Android Market	40
3.2.3	OVI Store de Nokia.....	41
3.2.4	App Store de BlackBerry	42
3.3	EN RIESGO: UN ESTUDIO DE AMENZAS MOVILES ENCUENTRA	
VULNERABILIDADES DE SEGURIDAD TODO EL TIEMPO AL MAXIMO		
PARA DISPOSITIVOS MOVILES		44
3.3.1	Conclusiones del informe	46
3.3.1.1	La ansiedad App Store	46
3.3.1.2	Preocupaciones Wi-Fi	46
3.3.1.3	Las amenazas de texto	46
3.3.1.4	La pérdida y el robo de dispositivos.....	46
3.3.1.5	Conductas de riesgo adolescente	46

3.3.1.6 "El peligro Droid"	46
3.4 APLICACIONES MÁS SEGURAS DE ANDROID.....	47
3.5 MALWARE Y PROTECCIÓN CONTRA ROBO.....	48
3.5.1 Gestión de contraseñas	49
3.6 ATAQUES REALIZADOS A ANDROID 2010 - 2011	50
3.6.1 Google Android.....	50
3.6.2 Enero de 2010: Phising de dólares	51
3.6.3 Marzo 2010: El primer Android "Botnet".....	51
3.6.4 Julio 2010: Spyware GPS de seguimiento Envuelto en el juego "Tap Snake"	51
3.6.5 Agosto 2010: El primer troyano SMS (Short MessageService) de Android.....	52
3.6.6 Noviembre de 2010: El Experimento "AngryBirds".....	52
3.6.7 Diciembre de 2010: Android Toma la Corona como objetivo principal en malware móvil	53
3.6.8 Enero / Febrero 2011: La tormenta sigue con la amenaza en China.....	54
3.6.8.1 Adrd	54
3.6.8.2 PjApps.....	55
3.6.9 Marzo 2011: Myournet / DroidDream ofrece pesadillas a los usuarios Android.....	55
3.6.10 Abril 2011: La Broma en usted	58

CAPITULO 4: CONCLUSIONES, RECOMENDACIONES Y REFERENCIAS

BIBLIOGRÁFICAS.....	60
4.1 ERRORES MÁS COMUNES	60
4.2 APORTES.....	61
4.3 RECOMENDACIONES	63
4.3.1 Para los consumidores.	63
4.3.2 Para las empresas, agencias gubernamentales y pymes.	63
4.4 CONCLUSIONES	64
4.5 BIBLIOGRAFÍA	68

TABLA DE FIGURAS

	pág.
Figura 1. Diagrama de Android	17
Figura 2. Smartphones.....	23
Figura 3. Smartphone Simon	24
Figura 4. Nokia 9210.....	25
Figura 5. Ericsson GS88	25
Figura 6. HTC Dream G1	27
Figura 7. SDK de Android	35
Figura 8. SDK de Blackberry.....	36
Figura 9. Web Runtime de Nokia	37
Figura 10. SDK de iOS.....	38
Figura 11. App Store de Apple	40
Figura 12. Android Market.....	41
Figura 13. OviStore de Nokia	42
Figura 14. App Store de Blackberry	43

TABLA DE GRÁFICOS

	pág.
Gráfico 1. Frecuencia de uso por mes Android vs iPhone	31
Gráfico 2. Evolución de mercado de las plataformas para Smartphone	32

TABLA DE TABLAS

pág.

Tabla 1. Comparacion de características entre diferentes plataformas.	59
--	----

CAPITULO 1 GENERALIDADES

1.1 TITULO

Monografía “Características y parámetros de la seguridad para los Smartphones con sistema operativo Android”.

1.2 DESCRIPCIÓN DEL PROBLEMA

Según la página www.tendencias21.net para el 2014 habrán 1700 millones de Smartphones alrededor de todo el mundo, debido a esto, y con base a comScore quien dice que la adquisición de Smartphones aumentó en un 10 por ciento comparado con el año pasado, son cada vez más las personas que acceden a este tipo de dispositivos, aumentando así también en un 65% la creación de malware como lo afirma un informe de virología móvil realizado por Kaspersky Lab, generando estos programas maliciosos, accesos indeseables a la información y la comunicación en los Smartphones¹.

Gracias al número creciente de acceso a los Smartphones², la cantidad de transmisiones aumenta a un ritmo muy acelerado, en consecuencia se hace cada vez más difícil tener un control efectivo que permita a las personas comunicarse sin tener que preocuparse por programas maliciosos.

Alrededor de 5.323 Millones de personas utilizan los dispositivos móviles³ para transmitir información valiosa como por ejemplo información personal y cuentas bancarias, lo que conlleva a que ciertas personas quieran sacar provecho de esto tratando de acceder a estas transmisiones, esto requiere que solo las

¹ Constanza Maecha. Zona Movilidad. 08 de Mayo de 2011. Según kaspersky-lab en 2010 se detectó un 65% más de malware para Smartphones [en línea]. Disponible en internet:

http://www.juniper.net/es/es/company/press-center/press-releases/2011/pr_2011_05_11-18_00.html

² Gartner. 11 de Agosto de 2011. Gartner Says Sales of Mobile Devices in Second Quarter of 2011 Grew 16.5 percent Year-on-Year; Smartphone Sales Grew 74 Percent. [En línea]. Disponible en internet:

<http://www.gartner.com/it/page.jsp?id=1764714>

³ International Telecommunication Union. Global Mobile Cellular 00-10 estadistic. [En línea]. Disponible en internet: <http://www.itu.int/ITU-D/ict/statistics/>

personas las cuales están dentro de la comunicación puedan acceder a esta información.

Con lo mencionado anteriormente, el problema que se quiere abordar con esta monografía es la falta de conocimiento en la vulnerabilidad y fortalezas de los Smartphones con sistema operativo Android, desde la perspectiva del currículo de Ingeniería de Sistemas y Computación de la Universidad Tecnológica de Pereira.

1.3 JUSTIFICACIÓN DEL PROBLEMA

Debido a los riesgos que pareciera tener la transmisión de información entre dispositivos Smartphones, se necesita que los métodos en dichas transmisiones se refinan a un punto que permitan un nivel aceptable de seguridad.

Es por eso que se requiere conocer cuáles son los ataques más comunes a los dispositivos Smartphones, para poder evitar futuros ataques o interceptaciones en las comunicaciones. Esta clasificación puede servir también para determinar cuáles son los errores más comunes de los usuarios de los Smartphones a la hora de utilizar estos dispositivos.

La penetración del sistema operativo Android y su incremento de uso⁴ sugieren la necesidad de pensar en proponer metodologías y sistemas que garanticen un nivel aceptable de seguridad en la transmisión de datos en dispositivos con este sistema operativo.

Por lo tanto, debido al creciente número de Smartphones en la actualidad se espera, con el desarrollo de esta monografía, poder determinar las características y parámetros de la seguridad para los Smartphones con sistema operativo Android lo cual justifica la presente propuesta.

⁴ Gartner. Op. Cit. P. 12

1.4 OBJETIVOS

1.4.1 Objetivo general. Desarrollar una monografía que condense las principales características y parámetros de la seguridad en transmisión de datos para los Smartphones con sistema operativo Android.

1.4.2 Objetivos específicos

- Realizar el estudio sobre los ataques más comunes a los Smartphones con sistema operativo Android.
- Identificar los errores más comunes hechos por las personas, que posibilitan intrusiones a las comunicaciones entre dispositivos Android.
- Identificar las aplicaciones que actualmente brindan más seguridad para los Smartphones Android.
- Establecer parámetros y características de seguridad del sistema operativo Android.
- Establecer unos aportes conceptuales a partir de la información estudiada y asimilada.
- Desarrollar un documento que condense la experiencia de manera sistemática.

1.5 MARCO DE REFERENCIA

1.5.1 Marco conceptual

1.5.1.1 ¿Qué es Android?. Android es una pila de software de código abierto para teléfonos móviles y otros dispositivos⁵ desarrollado por la Open Handset Alliance (OHA), un conglomerado de desarrolladores de hardware, software y operadores de servicio⁶. Fue diseñado originalmente para teléfonos inteligentes, pero ahora se ha visto este sistema operativo funcionando en microondas y lavadoras⁷.

1.5.1.2 ¿Cómo está compuesto Android?⁸. La plataforma de Android está compuesta de varias capas: El kernel de Linux, librerías nativas, la máquina virtual de Dalvik y un framework de aplicación. El kernel de Linux proporciona los servicios básicos del sistema operativo básico y de abstracción de hardware para las pilas de software superior. Las librerías nativas apoyan las diversas funcionalidades de los buscadores web, procesamiento de datos multimedia, acceso a bases de datos y la recepción de GPS optimizado para un entorno de recursos limitados de hardware. Los registros basados en la máquina virtual de Dalvik ejecutan código java con una demanda de memoria baja. En la parte superior de las capas, Android proporciona un framework de programación basado en componentes para que los usuarios puedan crear fácilmente sus propias aplicaciones.

⁵Android Open Source Project. [En línea]. [Consultado el 3 de septiembre de 2011]. Disponible en: <http://source.android.com/about/philosophy.html>

⁶Open Handset Alliance. [En línea]. [Consultado el 3 de septiembre de 2011]. Disponible en: <http://www.openhandsetalliance.com/>

⁷Alex Aliaga. 12 de Marzo de 2010. Android en un microondas. [En línea]. Disponible en internet en: <http://www.linuxzone.es/2010/03/12/android-en-un-microondas/>

⁸Wook Shin, Shinsaku Kiyomoto, Kazuhide Fukushima, and Toshiaki Tanaka. Introduction. En: Towards Formal Analysis of the Permission-based Security Model for Android [Base de datos en línea]. P. 6. [Citado el 1 de septiembre de 2011]. Disponible en IEEE Xplore Digital Library.

1.5.1.3 Características de Android⁹.

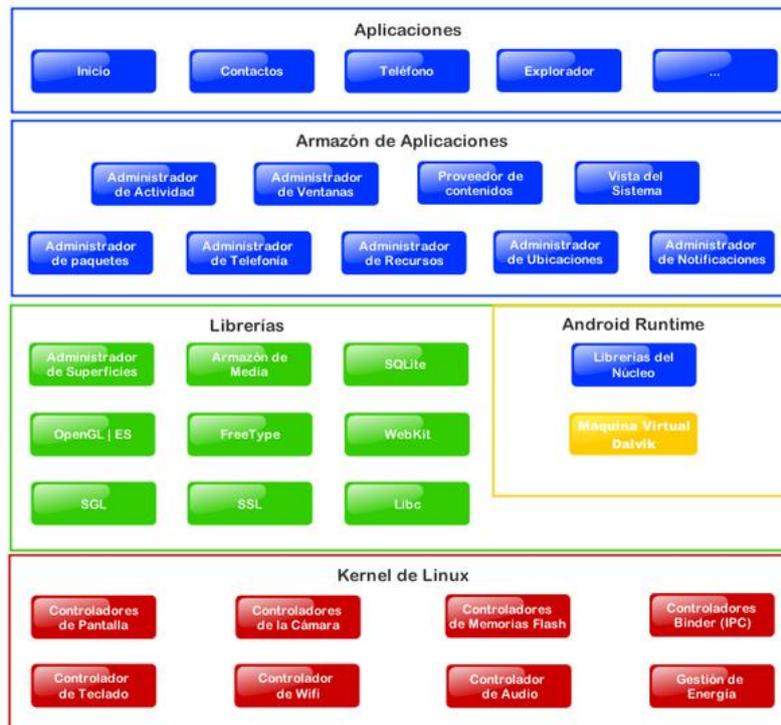
- Framework de aplicaciones. Permite el reemplazo y la reutilización de los componentes.
- Navegador integrado. Basado en el motor Open Source Webkit.
- SQLite. Base de datos para almacenamiento estructurado que se integra directamente con las aplicaciones.
- Gráficos Optimizados. Equipado con una librería personalizada de gráficos en 2D; Gráficos 3D basados en la especificación OpenGL ES 1.0.
- Entorno de desarrollo. Incluye un dispositivo emulador, herramientas para debugging, memoria y perfiles de rendimiento.
- Multimedia. Soporte para medios con formatos comunes de audio, video e imágenes planas (MPEG4, H.264, MP3, AAC, AMR, JPG, PNG, GIF).
- Máquina Virtual Dalvik. Base de llamadas de instancias muy similar a Java, optimizada para dispositivos móviles.
- Telefonía GSM. Dependiente del terminal.
- Bluetooth, EDGE, 3g y Wi-fi. Dependiente del terminal.
- Cámara, GPS, brújula y acelerómetro. Dependiente del terminal.
- Pantalla Táctil.

1.5.1.4 Arquitectura de Android¹⁰. La siguiente foto muestra los mayores componentes del sistema operativo Android. Cada sección se describe con más detalle.

⁹Android Developers. What is android ?.[En línea]. Disponible en: <http://developer.android.com/guide/basics/what-is-android.html>

¹⁰ Ibíd.

Figura 1. Diagrama de Android



Fuente: http://kronox.org/imagenes/diagrama_android.png

La figura 1 muestra la composición de Google Android, a través de sus características principales.

- Aplicaciones¹¹. Android posee un conjunto de aplicaciones básicas, como un cliente de correo electrónico, programa de SMS, calendario, mapas, navegador, contactos y otros. Todas las aplicaciones están escritas con el lenguaje de programación java.
- Framework de aplicaciones¹². Al proporcionar una plataforma de desarrollo abierto, Android ofrece a los desarrolladores la capacidad de crear aplicaciones muy ricas e innovadoras. Los desarrolladores son libres para tomar ventaja de los dispositivos de hardware, información de acceso a la ubicación, ejecutar servicios en segundo plano, establecer alarmas, añadir las notificaciones de la barra de estado, y mucho, mucho más.

¹¹Ibíd.

¹²Ibíd.

Los desarrolladores tienen pleno acceso a la API (Interfaz de programación de aplicaciones) de un mismo framework utilizado por el núcleo de aplicaciones. La arquitectura de la aplicación está diseñada para simplificar la reutilización de componentes, y cualquier aplicación puede publicar sus capacidades y cualquier otra aplicación podrá entonces hacer uso de esas capacidades (sujeto a restricciones de seguridad impuestas por el framework). Este mismo mecanismo permite que los componentes se reemplacen por el usuario.

- Librerías¹³. Android incluye un conjunto de librerías de C/C++ usadas por varios componentes del sistema Android. Estas capacidades son expuestas a los desarrolladores a través del framework de aplicaciones para Android.
- Runtime de Android¹⁴. Android incluye un conjunto de librerías núcleo que proporcionan la mayor parte de la funcionalidad disponible en las librerías núcleo del lenguaje de programación Java.

Cada aplicación de Android corre en su propio proceso, con su propia instancia de la máquina virtual de Dalvik. Dalvik ha sido escrita para que un dispositivo pueda correr varias máquinas virtuales de manera eficiente. La máquina virtual de Dalvik ejecuta archivos ejecutables en el Dalvik (.dex) formato que está optimizado para memoria mínima. La memoria virtual está basada en registros y corre clases compiladas por un compilador de lenguaje java que ha sido transformado en el formato .dex por la herramienta incluida "dx".

- Kernel de Linux¹⁵. Android se basa en la versión 2.6 de Linux para el núcleo de servicios del sistema tales como la seguridad, la gestión de memoria, gestión de procesos, pila de red y el modelo controlador. El kernel también actúa como una capa de abstracción entre el hardware y el resto de la pila de software.

¹³ Ibíd.

¹⁴ Ibíd.

¹⁵ Ibíd.

1.5.2 Estado del Arte

1.5.2.1 Seguridad en dispositivos móviles¹⁶. Los dispositivos móviles disponen de crecientes incentivos para ser atacados por los cibercriminales. Su uso está generalizado y en continua expansión, contienen una vasta cantidad de información personal y confidencial, y son usados (o tienen la capacidad) para realizar prácticamente todo tipo de transacciones online.

Un aspecto interesante en lo referente a la seguridad en estos dispositivos móviles son sus canales de comunicación. En este sentido están más expuestos que los tradicionales PCs ya que las amenazas pueden venir por: SMS, Bluetooth, Wi-Fi, navegadores web, aplicaciones, y correo electrónico, hecho que puede propiciar la propagación de código malicioso orientado a este tipo de plataformas.

Se trata de dispositivos realmente personales. Precisamente es esta capacidad de personalización que disponen lo que los convierte en más peligrosos. Es común que exista un PC para toda la familia, pero también es común que cada miembro de la familia disponga de un teléfono móvil que lo llevará consigo todo el tiempo. El hecho de que todavía existan mínimas muestras de malware para móviles, la falta de concienciación por parte del usuario, y la limitación de la batería para ejecutar aplicaciones complejas como soluciones antivirus, son factores que actualmente juegan en contra del uso de los mismos.

1.5.2.2 Acceso de archivos¹⁷. Los archivos en Android (de aplicación y del sistema) están sujetos a mecanismo de permisos de Linux. Cada archivo está asociado con los ID de usuario y de grupo del propietario y tres tuplas de permisos: lectura, escritura y ejecución (rwx). El kernel de Linux hace cumplir estos permisos e impone la primera tupla al propietario, mientras la segunda

¹⁶ Consejo Nacional Consultivo de Cyber-Seguridad. Seguridad en dispositivos móviles. En: Malware para smartphones. P. 12

¹⁷ WookShabtai, A.; Fledel, Y.; Kanonov, U.; Elovici, Y.; Dolev, S.; Glezer, C. *Android Security Mechanisms*. En: Google Android: A Comprehensive Security Assessment [Base de datos en línea]. P. 36. [Citado el 5 de septiembre de 2011]. Disponible en IEEE Xplore Digital Library.

afecta al usuario que pertenece al grupo del propietario, y la tercera afecta al resto de los usuarios.

Generalmente, cualquiera de los usuarios “system” o “root” controlan los archivos del sistema en Android, mientras que una aplicación específica de usuario controla los archivos de aplicación. Asignando diferentes usuarios para cada aplicación y para los archivos de sistema, con las debidas configuraciones de permisos, se provee la seguridad necesitada para el acceso de archivos. Estas acciones son necesarias porque los archivos de aplicación no serán accesibles para otras aplicaciones (a menos que ellas usen la opción shared UserID o que sean puestas como globalmente legibles o escribibles).

Adicionalmente, Linux maneja muchas funcionalidades del sistema como pseudo archivos. Consecuentemente, el mecanismo de acceso de archivos efectivamente permite permisos de configuración en los controladores, terminales, sensores de hardware, cambios en los estados de poder, audio, lecturas de entrada directas, y muchas más.

1.5.2.3 Permisos de aplicación¹⁸. El mecanismo de permisos de Android para las aplicaciones hace cumplir las restricciones sobre ciertas operaciones que una aplicación puede desarrollar. Android tiene aproximadamente 100 permisos built-in que controlan las operaciones de rango desde el marcado del teléfono, tomar fotos, uso de internet, el presionado de teclas, e incluso deshabilitar permanentemente el teléfono. Cualquier aplicación Android puede declarar permisos adicionales. Para obtener un permiso, una aplicación debe requerirla explícitamente.

¹⁸WookShabtai, A.; Fledel, Y.; Kanonov, U.; Elovici, Y.; Dolev, S.; Glezer, C. *Application permissions*. En: Google Android: A Comprehensive Security Assessment [Base de datos en línea]. P. 37. [Citado el 5 de septiembre de 2011]. Disponible en IEEE Xplore Digital Library.

1.5.2.4 Encriptación de datos¹⁹. La encriptación de datos es una excelente manera contra la exposición de datos privados. Debido a que solo el propietario conoce la clave para descifrar los datos, la información está segura, incluso cuando un atacante roba el dispositivo y tiene completo acceso, porque él o ella no pueden descifrar la encriptación en una cantidad de tiempo razonable. Encriptar datos importantes manejados por el núcleo de aplicaciones requerirá desarrolladores para modificar esas aplicaciones.

1.5.2.5 Sistema de intrusión detección y prevención²⁰. Un IDS (Sistema de Detección de Intrusos) basado en usuario, puede contra-atacar el drenaje malicioso en la batería, memoria o CPU detectando cambios anormales en los niveles de los recursos. En práctica, cualquier malware tiene como objetivo ser indetectable, así que el IDS continuamente debería mantener y validar el uso normal del perfil.

1.6 DISEÑO METODOLÓGICO

1.6.1 Hipótesis. Es posible impulsar el desarrollo de nuevas herramientas para evitar ataques en la comunicación de dispositivos Smartphone a partir del estudio sobre la seguridad de dichos dispositivos móviles.

1.6.2 Tipo de investigación. Debido a las características de este estudio, donde se pretende mostrar cualidades y defectos de los Smartphones Android, es una investigación cualitativa.

1.6.3 Población. Comunidad académica del programa Ingeniería de Sistemas y Computación.

¹⁹WookShabtai, A.; Fledel, Y.; Kanonov, U.; Elovici, Y.; Dolev, S.; Glezer, C. *Data encryption*. En: Google Android: A Comprehensive Security Assessment [Base de datos en línea]. P. 42. [Citado el 5 de septiembre de 2011]. Disponible en IEEE Xplore Digital Library.

²⁰Shabtai, A. ; Fledel, Y. ; Kanonov, U. ; Elovici, Y. ; Dolev, S. ; Glezer, C. *Android Intrusion-detection/prevention system*. En: Google Android: A Comprehensive Security Assessment [Base de datos en línea]. P. 43. [Citado el 5 de septiembre de 2011]. Disponible en IEEE Xplore Digital Library.

CAPITULO 2 SMARTPHONES

2.1 INTRODUCCIÓN

Los dispositivos móviles se han estado transformando hasta prácticamente coincidir en cuanto a funcionalidades con los ordenadores personales, todo esto conlleva a un incremento en la utilización de estos dispositivos en cualquier tipo de tarea. Por otra parte, se incrementan también los riesgos causados al acelerado uso de estas tecnologías, concebidas en muchos casos sin tener en cuenta la seguridad.

Se ha decidido hacer un acercamiento desde muchos puntos de vista para tratar de tener una visión completa de este fenómeno y hacer un soporte para intentar pronosticar algunas inclinaciones futuras y corroborar alguna de las anteriores. De esta manera, se han tenido en cuenta características técnicas (particulares de cada plataforma), económicas e históricas (desde su creación donde los desarrollos eran primordialmente pruebas de consideración o simples muestras de creatividad, hasta la reciente innovación de aplicaciones con fines específicamente engañosos).

2.2 HISTORIA

2.2.1 Smartphones. Se les llama Smartphone a los dispositivos que a partir de la funcionalidad de un teléfono móvil, han evolucionado hasta estar más cercanos, en la actualidad, de un ordenador personal portátil. Es normal hoy en día que esta clase de teléfonos dispongan de agenda, GPS, reproductor de vídeos y música, muchas opciones de conectividad y un número muy grande de funcionalidades que hasta hace unos años eran inimaginables para estos dispositivos.

Figura 2. Smartphones



Fuente <http://www.compubun.com/wordpress/wp-content/subidas/smartphone.jpg>

En la figura 2 se observan algunos de los diferentes Smartphones existentes en el mercado, se puede ver la diversidad de diseños y cada uno tiene funcionalidades únicas.

Simon fue el primer teléfono móvil que se catalogó como Smartphone, y se creó en el año de 1992 por BELLSOUTH e IBM. Fue planeado principalmente como una idea que se quería dar a conocer en la feria de tecnología COMDEX, y salió a la venta un año más tarde. Simon fue el primer dispositivo en el que se adaptaron mas funciones que las de un teléfono móvil convencional en ese tiempo; éste teléfono tenía funciones como correo electrónico, fax, calendario, calculadora e incluso un lector de tarjetas PCMCIA.

Figura 3. Smartphone Simon



Fuente <http://thewinnger.files.wordpress.com/2011/04/first-smart-phone.jpg>

En la figura 3 se observa el diseño del primer Smartphone llamado Simon, el cual fue descrito anteriormente.

Pasados 4 años de la salida de Simon, Nokia contraatacó y lanzó a la venta el modelo Nokia 9000. Este modelo fue fundamentalmente una unión de funcionalidades entre PDA (Personal Digital Assistant) y las propiedades de un teléfono inalámbrico normal. Y fue Nokia quien introdujo en sus modelos posteriores los primeros en incluir ciertas características esenciales que se usan hoy en día para que un dispositivo sea tenido en cuenta como un Smartphone, como pantalla a color y la incorporación de conectividad Wi-Fi entre otros. Cabe resaltar el modelo Nokia 9210 Communicator el cual fue el primer dispositivo en acoger el sistema operativo SymbianOS.

Figura 4. Nokia 9210

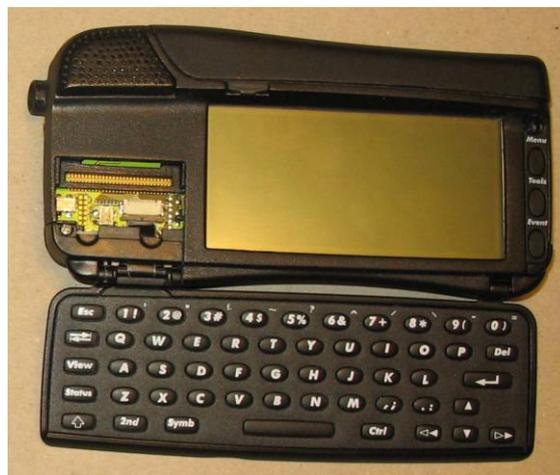


Fuente http://pdadb.net/img/nokia_9210i.jpg

En la figura 4 se observa el modelo 9210 de Nokia el cual fue el primer Smartphone en adaptar el sistema operativo SymbianOS.

Ericsson lanzó su teléfono GS88 en el año 1997, el cual fue el primer dispositivo nombrado explícitamente como Smartphone. La pantalla táctil fue incluida después en sus modelos.

Figura 5. Ericsson GS88



Fuente <http://www.broimg.de/pics/nev9LUeqmfMjpTKZdTT2oJmUF.jpg>

La figura 5 muestra el Ericsson GS88 el cual fue el primer dispositivo móvil nombrado explícitamente Smartphone.

Un año más tarde, se origina un alza importante en cuanto a la venta de diferentes modelos de Smartphone. La salida al mercado de teléfonos móviles con sistema operativo Windows CE y la venta también del primer modelo de Blackberry en 2002 gracias a Research in Motion (RIM) fueron unos de los hechos más importantes, este último lo fue gracias, en gran parte, a la mejora que hace del manejo del correo electrónico.

A lo largo de estos años, los dispositivos de los muchos fabricantes han estado evolucionando e introduciendo nuevas funcionalidades, haciendo que la mayoría de características que se conocen hoy en día, en estándares de mercado que determinan lo que hoy en día conocemos como un teléfono inteligente (Smartphone).

Apple Inc. en el 2007, introdujo su primera generación de Smartphone los cuales llamó iPhone. Estos dispositivos se convertirían en uno de los primeros que permitió ser controlado completamente por una pantalla táctil, a partir de esto, marcarían un punto de inclinación en esta parte del mercado. A lo largo de estos últimos años, Apple ha lanzado nuevas versiones de su iPhone los cuales soportan 3G y permite la descarga de aplicaciones desde su propia comunidad más conocida como App Store.

En el 2008 se da a conocer Android, una plataforma de código abierto hecha solo para Smartphones, el cual se basó en Linux, en una modificación de su Kernel. Esta plataforma se transformó en emblema del consorcio Open Handset Alliance, hecho y fomentado por Google en el año 2007 y además “está compuesto por varios fabricantes, desarrolladores y operadores (Intel, HTC, Dell, ARM, Motorola, entre otros) con el propósito de desarrollar estándares abiertos para dispositivos móviles”²¹.

El HTC Dream fue el primer dispositivo en implementar Android, distribuido por T-Mobile como G1. El software que se instaló en este dispositivo estaba integrado con las aplicaciones de Google; Maps, Calendar, Gmail, y el

²¹Consejo Nacional Consultivo de Cyber – Seguridad. Malware en Smartphones. En: Historia. P.7.

navegador Chrome. Algo muy novedoso es el uso de aplicaciones de terceros (gratuitas y de pago) gracias a Android Market.

Figura 6. HTC Dream G1



Fuente <http://www.traderfoxsuperstore.com/images/HTC.G1Dream.jpg>

En la figura 6 se muestra el primer dispositivo en implementar Android, el cual incluía muchas de las funcionalidades actuales.

RIM y su Blackberry App World, Nokia con su OviStore (mayo 2009), Palm y Palm App Catalog (junio 2009) o Microsoft con Windows Marketplace for Mobile (octubre 2009) son una muestra de que muchos fabricantes usan la línea de crear comunidades para la gestión de sus aplicativos.

“En enero de 2010, Google lanzó al mercado su dispositivo NexusOne basado en Android OS versión 2.2, distribuido en España mediante el operador Vodafone”.²²

²²Ibíd.

2.2.2 Android²³. Ya en julio de 2005, cuando Google parecía tener tanto dinero que no sabía qué hacer con él, en silencio se fue sobre la compra de un montón de empresas que recién comenzaban.

Algunos de estos nunca vieron la luz del día, como por ejemplo Dodgeball, un servicio que permitía mensajería a un grupo de amigos al igual que Twitter, nunca ha aparecido en los establos de Google.

Pero al mismo tiempo, también compró una empresa poco conocida llamada AndroidInc, co-fundada por Andy Rubin, ahora director de plataformas móviles de Google.

Poco se sabía de esta compañía, incluso dentro de su propia industria, de hecho, todo lo que estaba disponible en cuanto a descripción fue que era “que desarrollo software para teléfonos móviles”.

En 2003, antes de involucrarse con Android, Rubin realizó una entrevista con Business Week:

“Rubin dijo que había un enorme potencial en el desarrollo de dispositivos móviles inteligentes que son más conscientes de la ubicación de su propietario y sus preferencias”.

“Si las personas son inteligentes, esa información empieza a ser agregada a los productos de consumo’, dijo Rubin”.

2.2.2.1 El gPhone. En el lanzamiento del iPhone, los rumores de Google empezaron a aumentar con la traída de su propio teléfono, para ayudar a aprovechar su creciente búsqueda de funciones móviles.

Numerosos reportes de Google pregonando sus mercancías a todos los principales fabricantes y compañías empezaron a circular. Se creía que el nuevo equipo seria diseñado para trabajar en servicios basados en locación e

²³ Traducción tomada del texto: A Complete History of Android. Disponible en: <http://www.techradar.com/news/phone-and-communications/mobile-phones/a-complete-history-of-android-470327>

implementando un conjunto de ideas de Google Labs, así como los mapas favoritos de siempre y correo electrónico.

2.2.2.2 Lanzamiento de Android. Surgió una gran sorpresa en el mundo, no solo habían estado trabajando en un teléfono, habían estado desarrollando el núcleo de un completo sistema operativo de código abierto para rivalizar empresas como Symbian, Microsoft y otros.

¿Y todas esas reuniones clandestinas? Los inicios de lo que hoy conocemos como Open Handset Alliance (OHA), incluyendo HTC, LG, Samsung, T-Mobile y una gran cantidad de otros nombres.

Y lo que muchas personas no se dan cuenta, especialmente aquellos quienes lo llamaron “El Android de Google”, es que la nueva plataforma nació fuera de este grupo, Google incorpora la ayuda de otros.

Pero eso no es estrictamente cierto, Google es claramente la principal fuerza motriz detrás del nuevo sistema, pero todas las facciones de la OHA están de pie para hacerlo bien desde el éxito del sistema operativo.

Muchas personas tuvieron problemas entendiendo los beneficios de lo que Google Android actualmente tenía, y lo que lo hizo especial comparado con los sistemas operativos rivales allá afuera.

2.2.2.3 Lego. La mejor manera de describirlo fue haciendo todas las secciones del sistema como bloques de Lego. Donde antes los desarrolladores podrían haber luchado por romper las partes de un sistema operativo móvil, e incluso si tenían éxito, encontrarían que, hacer hablar una parte del sistema con otra era muy difícil, ya que habían sido empacados en sus propios programas pequeños.

Pero con Android, las reglas fueron cambiadas. ¿Querer hacer una aplicación GPS que usaba SMS para actualizar la ubicación? Las dos secciones encajarían muy bien. ¿Si desea agregar en alguna locación información de la internet? Solo basta con meter el pedazo web.

Puede que no sea tan sencillo, pero para la comunidad de desarrolladores, representó un gran paso. Mientras que lo anterior puede haber sido posible a través de cosas como Linux para Móviles (LiMO), Google Android tiene como objetivo proporcionar lo mismo en una escala mayor y más unificada, así trayendo una mayor audiencia en el futuro.

La teoría detrás del sistema es muy similar a la que ha hecho que Google sea un éxito hasta ahora, la publicidad móvil y las ganancias pueden llegar a convertirse en palabras de moda para tal plataforma, y necesitarán aprovecharlo bien para hacer de Android un éxito de Google y la OHA.

2.3 EVOLUCIÓN DEL MERCADO DE SMARTPHONES.

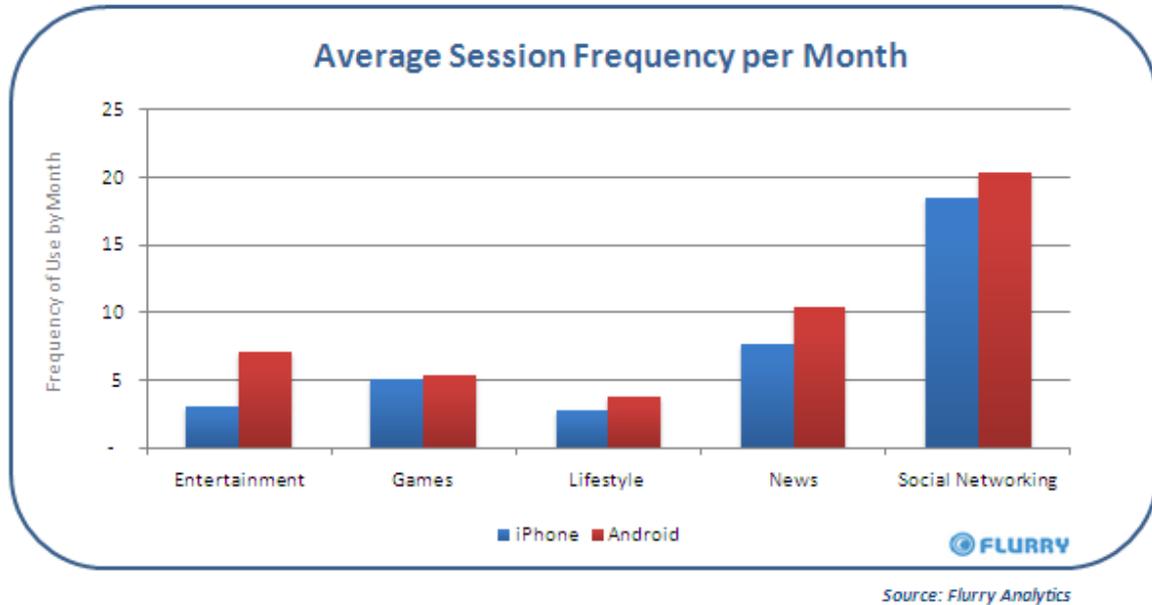
El éxito de los Smartphone ha logrado un grado muy alto de penetración en el mercado para todo tipo de usuarios, esto lleva a consecuencias que no se pueden evitar. El camino que ha tenido su acelerada evolución tal vez no fue el esperado.

En 2006 la consultora Gartner predijo que el vencedor de la batalla comercial en el 2010 sería Windows Mobile, quitando el trono a Nokia. Nada más lejos de la realidad; Nokia, a pesar de tener un porcentaje de penetración de mercado importante, parece de capa caída y sus modelos parecen desfasados en comparación con su competencia.²⁴

Cuando iPhone llegó al mercado a mediados de 2007 comenzó la revolución de los Smartphone, todo esto gracias a la batalla entre iPhone y los dispositivos basados en Android.

²⁴Consejo Nacional Consultivo de Cyber – Seguridad. Malware en Smartphones. En: Evolución del mercado de Smartphones. P.9.

Gráfico 1. Frecuencia de uso por mes Android vs iPhone



Fuente

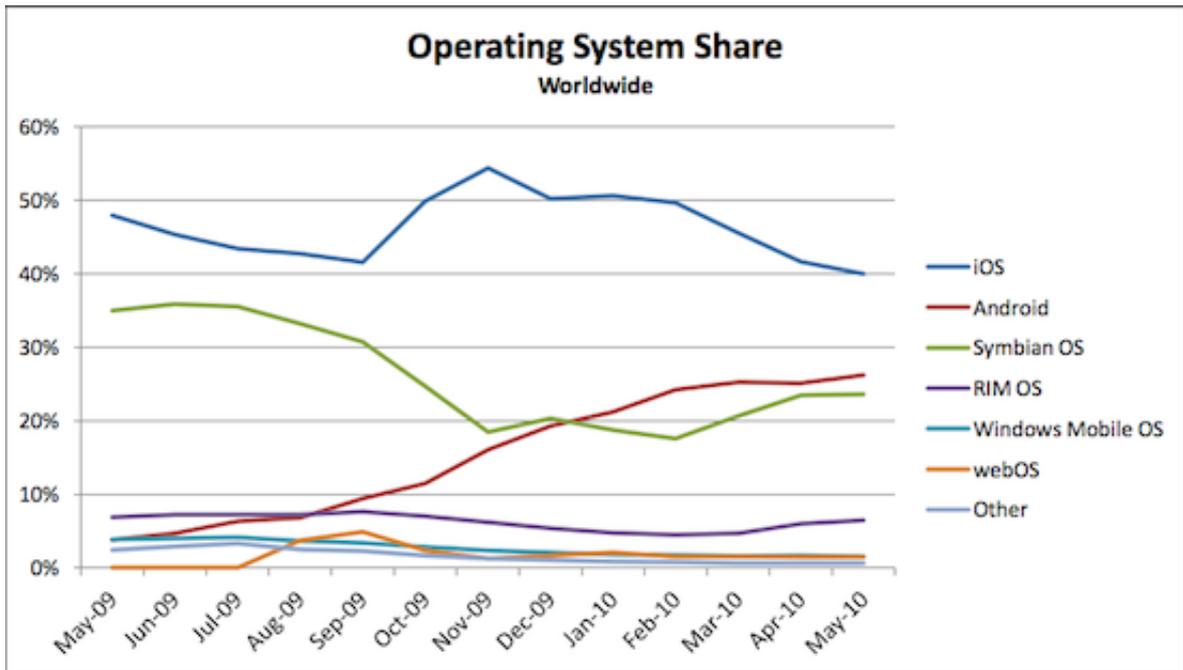
http://blog.flurry.com/Portals/41620/images//iPhone_vs_Android_UsePerMonth_byCategory.png

El Gráfico 1 describe la frecuencia de uso por mes entre Smartphones iPhone y Smartphones Android. Se observa como Android supera en muchos aspectos a iPhone.

La introducción de las pantallas táctiles transformó el mercado, ya que atrajo a los usuarios por medio de una interfaz fácil e intuitiva, debido también a que su superficie de visualización es mucho más amplia y usable que permitió distintas funciones entre las que están la navegación web y la reproducción de archivos multimedia con muy buena calidad.

El desarrollo paralelo del hardware de los dispositivos móviles, hace que actualmente sea muy común encontrar terminales con procesadores de 1 GHz y más de 512 MB de RAM, con funcionalidades como acelerómetros, bluetooth, brújula o GPS, lo que brinda a los desarrolladores una gama amplia de posibilidades que aun no son desconocidas.

Grafico 2. Evolución de mercado de las plataformas para Smartphone



Fuente

http://gigapple.files.wordpress.com/2010/07/admob_mobile_os_0610.png?w=550&h=314

En el Gráfico 2 se puede observar inclinación correspondiente a los dispositivos con Android, los fabricantes instalan cada vez más este Sistema Operativo. El iOS aunque aún mantiene su liderazgo su tendencia esta en baja, y Blackberry solo llega a tener un 9%.

2.4 EL FUTURO QUE VIENE

Los creadores de malware mejoran continuamente sus tácticas y no hay ninguna duda de que el malware para dispositivos móviles seguirá evolucionando, por lo que hay que estar preparado para futuras infecciones:

2.4.1 Móvil como medio de pago. Los avances que se están realizando con el chip NFC (Near Field Communication) son bastante grandes. “NFC es una tecnología de comunicación inalámbrica que permite transmitir datos entre dispositivos a unos 5-10 centímetros, y se puede utilizar para realizar pagos, transferir información, etc. Las ventajas de comunicación con el chip NFC radican en la velocidad de emparejamiento, el consumo, y su compatibilidad con RFID”²⁵ (Radio Frequency Identification). Algunos de los dispositivos de Google y el iPhone 6 incluirán este chip, al igual que Nokia quien ya lo hace en algunos modelos.

2.4.2 Aplicaciones Bancarias. Los bancos están creando cada vez más sus propias aplicaciones para dispositivos móviles. La posibilidad de que malware para dispositivos móviles que utilicen mejores técnicas para interceptar llamadas que capturen información sensible es muy alta.

2.4.3 Seguimiento de individuos. Ahora que muchos dispositivos móviles tienen incorporados GPS, sería de vital importancia desarrollar aplicaciones que al ser consultadas, entreguen una señal para ubicarla como coordenada en el GPS, que puedan detectar los servidores las personas atacantes.

2.4.4 Vulnerabilidades por redes Wi-Fi. Hoy en día los dispositivos móviles integran conexión a las redes Wi-Fi, no es descabellada la idea de que puedan existir gusanos que exploren los sistemas que tienen una determinada red Wi-Fi, e infiltren códigos maliciosos a estos sistemas explotando sus vulnerabilidades.

2.4.5 Ataques de ingeniería social avanzada. Puede existir malware que cambie la agenda personal de un usuario, esto puede ser muy útil para suplantar una identidad, asociando un número a otra persona, utilizando ingeniería social orientada.

²⁵Consejo Nacional Consultivo de Cyber – Seguridad. Malware en Smartphones. En: El futuro que viene. P.31.

CAPITULO 3 CARACTERÍSTICAS Y PARÁMETROS DE SEGURIDAD DE LOS SMARTPHONES.

De acuerdo a los riesgos que se han planteado, se hace fácil pensar en que el efecto del uso de los Smartphones en la sociedad actual va mucho más orientado a ciertas sensaciones de inseguridad.

Debido a que los Smartphones son dispositivos más pequeños, se tiene la sensación de que tenemos un control físico total sobre éste y que serán menos accesibles para los intrusos. Esta falsa sensación de seguridad, además del uso de funcionalidades tales como contenido multimedia privado, redes sociales y correo electrónico, trae como consecuencia que el dispositivo móvil contenga información privada la cual el usuario no se percata o pasa por alto.

Esta falsa sensación antes mencionada, hace que muchos de los usuarios ni siquiera cambien la configuración de seguridad que el dispositivo móvil trae por defecto.

Hay muchas circunstancias que hacen que aparezcan nuevas amenazas. La contraseña es, la mayoría de los casos, la única herramienta de seguridad en la mayoría de los Smartphones. La seguridad en los Smartphones depende mucho de la seguridad y la confiabilidad de las aplicaciones que estén disponibles para instalar.

Es importante tener métodos de cifrado, para que llegado el caso de robo o pérdida del dispositivo no se permita el acceso a la información. Esto es muy importante debido a que existen empresas en las que se unen las políticas de seguridad con el uso de estos dispositivos, así que mantener la información asegurada es de vital importancia.

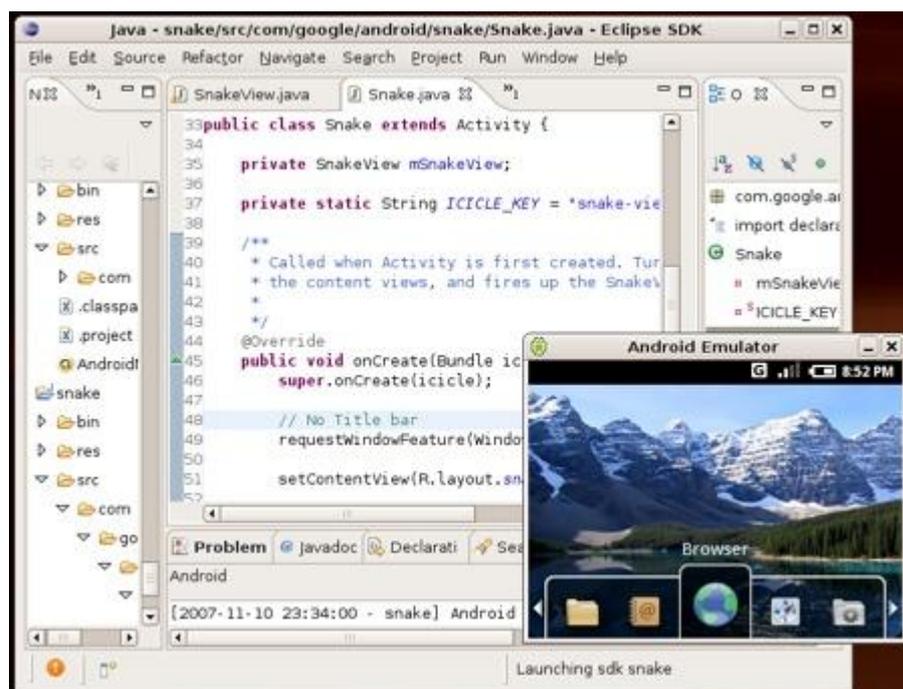
La seguridad de los Smartphones abarca desde el kernel del sistema operativo hasta en el modelo distribución de cada una de sus aplicaciones, y terminando en cada uno de los entornos de desarrollos existentes de cada plataforma, así que la seguridad no se puede ver solo desde el punto de vista del usuario que tiene en funcionamiento el Smartphone.

3.1 KITS DE DESARROLLO DE APLICACIONES (SDKS)

Para la creación de aplicaciones, las plataformas móviles como Blackberry, iPhone y Android brindan entornos de desarrollo o SDKs (SDK, del inglés Software Development Kit). Cada SDK tiene sus características propias, muchas de ellas han sido realizadas con el fin de mejorar la seguridad, como son el cifrado, la restricción de acceso al hardware o la administración de memoria. Los principales SDK de cada plataforma son:

3.1.1 SDK de Android. Impulsado por Google. El lenguaje que utiliza la plataforma Android para la creación de sus aplicaciones es Java, esto hace que dichas aplicaciones se ejecuten sobre una maquina virtual especial llamada Dalvik. No obstante, se pueden utilizar distintos entornos de desarrollo, pero la plataforma de código libre Eclipse es la más elegida para este trabajo. El hecho de que la plataforma sea abierta es lo que marca la diferencia de Android frente a la competencia.

Figura 7. SDK de Android

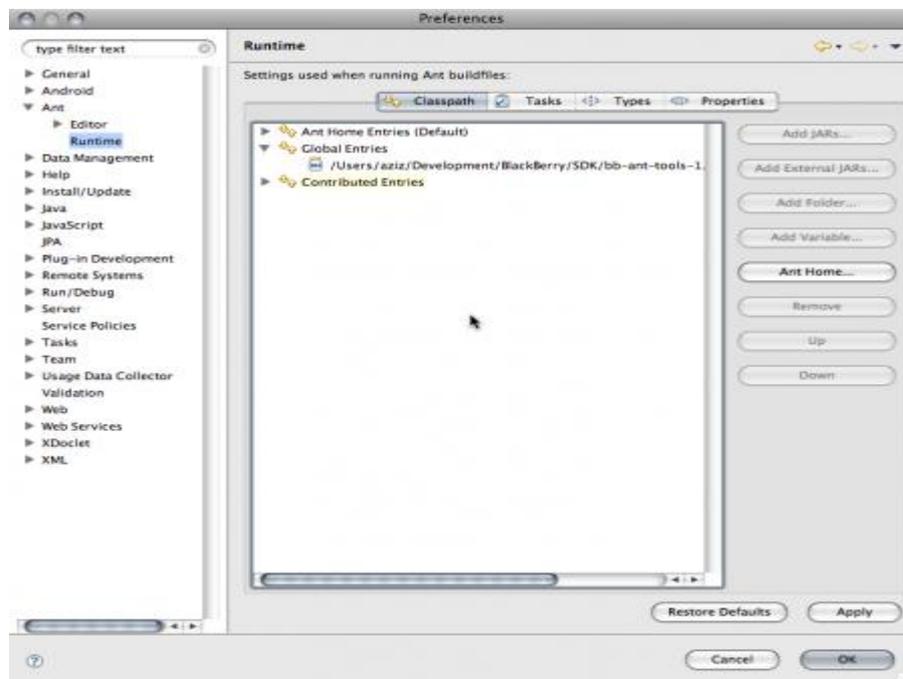


Fuente <http://www.visualbeta.es/647/movil/android-sdk-ya-disponible/>

En la Figura 7 se muestra el entorno de desarrollo Eclipse funcionando en una plataforma Linux. También se observan unas líneas de código en Java así como cada una de las opciones disponibles del editor en la parte superior de la foto.

3.1.2 SDK de Blackberry. Suministrado por RIM (Research In Motion), el promotor del dispositivo móvil Blackberry. El Sistema Operativo es titular y el entorno para la creación de aplicaciones es JavaME. Las aplicaciones que se crean requieren ser empaquetadas para conservar la seguridad que brinda el sistema operativo. Las aplicaciones se firman de modo digital para que puedan vincularse a una cuenta de desarrollador.

Figura 8. SDK de Blackberry

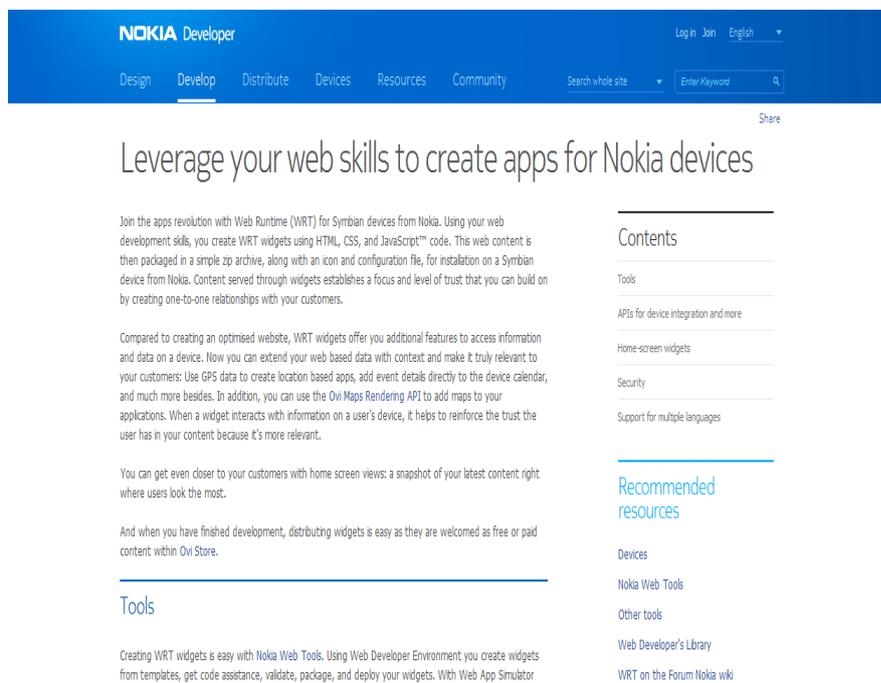


Fuente <http://azizuysal.com/2009/07/06/blackberry-development-on-mac-os-x/>

La figura 8 muestra el SDK de Blackberry corriendo sobre una máquina con sistema operativo Mac-os-x.

3.1.3 SDK de Nokia. Antes Nokia utilizaba el entorno de desarrollo para Symbian para la creación de aplicaciones en su plataforma. Ahora la compañía Nokia hace uso de la plataforma WRT (Web RunTime), que es más accesible para los desarrolladores.

Figura 9. Web Runtime de Nokia



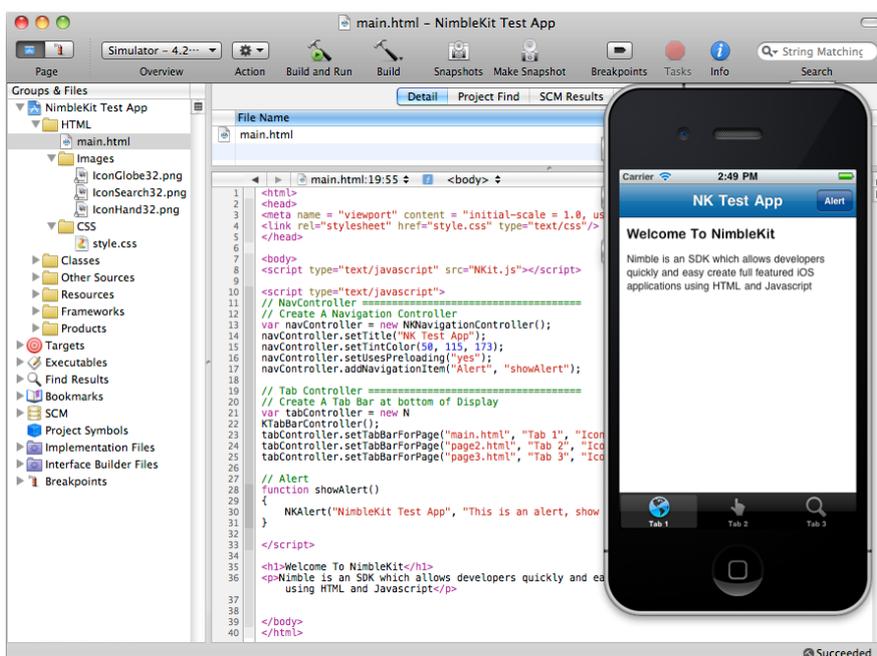
Fuente

http://www.developer.nokia.com/Develop/Web/Web_runtime.xhtml

La figura 9 muestra una breve descripción acerca del sitio y de lo que es WRT de Nokia, un contenido de la página para navegar por ella y recursos recomendados, además de un enlace de descarga para la herramienta de desarrollo de aplicaciones (el Nokia Web Tools).

3.1.4 iOS. El iPhone necesita ser cerrado para mantener su seguridad y estabilidad. Por ello Apple proporciona su kit de herramientas de desarrollo para iOS. La última versión iOS4 ha abierto algunas restricciones en la licencia permitiendo el uso de entornos de desarrollo intermedios, abriéndose así a plataformas como Flash, Java, Silverlight o Mono²⁶.

Figura 10. SDK de iOS



Fuente <http://nimblekit.com/assets/img/xcodeshotlarge.png>

NimbleKit mostrado en la figura 10, es el SDK de iPhone el cual permite a sus desarrolladores crear aplicaciones con todas las funciones. Este SDK permite HTML y Javascript.

Como prueba de concepto, en un artículo de la BBC²⁷ informan de cómo conociendo solo unos conceptos básicos de programación en Java crearon un juego a partir de piezas estándar de herramientas de software que utilizan los programadores para crear programas dirigidos a teléfonos. El objetivo del juego

²⁶ Consejo Nacional Consultivo de Cyber – Seguridad. Malware en Smartphones. En: Kits de desarrollo de aplicaciones. P.14-15.

²⁷ Ward Mark. 9 de agosto de 2010. Smartphone security put on test. [En línea]. [Consultada el 14 de Septiembre de 2011]. Disponible en internet en: <http://www.bbc.co.uk/news/technology-10912376>

era recopilar contactos, copiar mensajes de texto y detectar la localización del teléfono, todo esto se hacía sin que el usuario se diera cuenta, toda esta información era enviada a una cuenta de correo especialmente configurada. El spyware tomó 250 líneas de las 1500 que conformaban el juego completo. El código fue descargado a un móvil, pero no fue puesto en una tienda de aplicaciones.

“Los desarrolladores tienen que ser responsables e informar de los datos a los que tendrán acceso sus aplicaciones. Pero en muchas ocasiones ni siquiera ellos conocerán toda la funcionalidad de su código al usar aplicaciones de terceras partes. Sin duda el control de las aplicaciones disponibles para estos dispositivos será clave para mantener la seguridad del usuario final”.²⁸

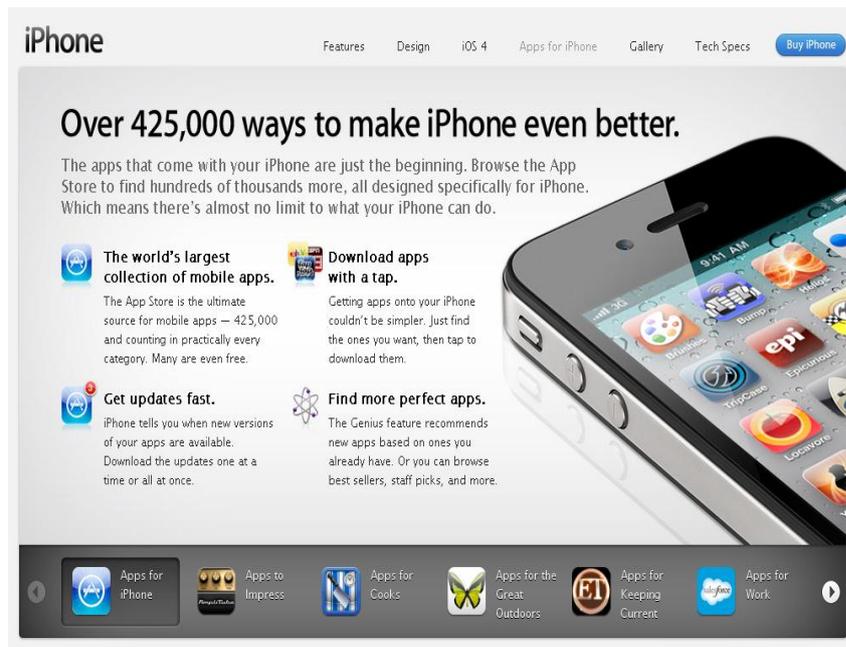
3.2 MERCADOS DE APLICACIONES

Los fabricantes de teléfonos móviles copiaron el modelo de tienda de aplicaciones (App Store) de Apple. Este modelo consiste en trasladar la seguridad de las aplicaciones para móviles a un punto central de distribución, una vez en este punto cada fabricante asigna sus propias normas de distribución de aplicaciones para sus dispositivos. De esta forma se intenta vigilar que las aplicaciones distribuidas estén libres de código malicioso.

3.2.1 App Store de Apple. Las aplicaciones que se crean y quieren estar disponibles en el sitio web, tienen que ser aprobadas por Apple. Asimismo, los desarrolladores deben crear una cuenta como tal y pagar una tarifa anual. Apple comprueba que la aplicación funcione tal y como se anuncia así como que la aplicación no desestabilice el dispositivo móvil.

²⁸Consejo Nacional Consultivo de Cyber – Seguridad.Op. Cit., P. 39.

Figura 11. App Store de Apple



Fuente <http://www.apple.com/iphone/apps-for-iphone/>

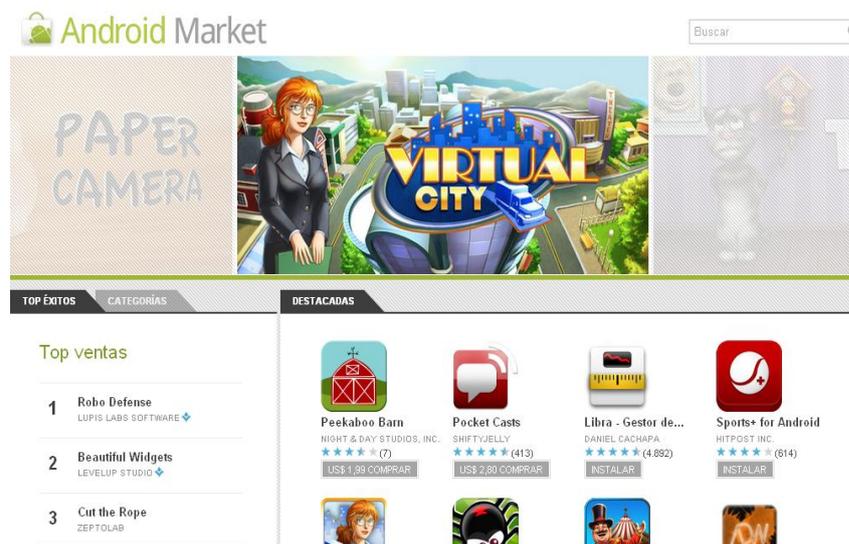
En el AppStore de iPhone (Figura 11) se puede encontrar cual es la aplicación de la semana, esto para ir al pendiente de que es lo nuevo y más utilizado que los desarrolladores crean, así como también se pueden encontrar aplicaciones para el trabajo, para estudiantes, para música, entre otros.

3.2.2 Android Market. Por otro lado, Google no veta las aplicaciones que se suban al mercado de Android. Google dispone de reglas específicas, pero la responsabilidad del software recae sobre el usuario. Para proteger al Android de los ataques malintencionados se utiliza un modelo de seguridad que se basa en “capacidades”. “Cada aplicación Android debe indicar al Sistema Operativo del móvil las capacidades que necesita. Al instalar una aplicación, el sistema operativo listará las capacidades que la aplicación necesita para ejecutarse, pero es responsabilidad del usuario decidir si estas capacidades son consistentes con la funcionalidad de la aplicación”²⁹.

²⁹Consejo Nacional Consultivo de Cyber – Seguridad. Malware en Smartphones. En: Mercados de aplicaciones. P.15-16.

Por su parte, las aplicaciones que Google encuentre con código malicioso las podrá deshabilitar de forma remota. Así mismo, cuando el teléfono quiere interactuar con las aplicaciones, se necesita de los permisos que los desarrolladores hayan declarado para estas.

Figura 12. Android Market



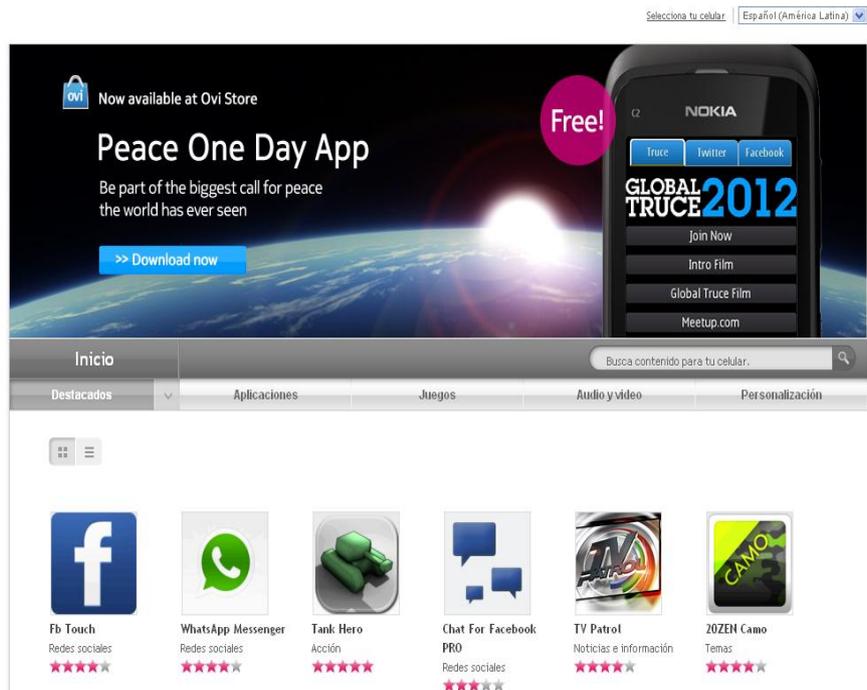
Fuente <https://market.android.com/?hl=es>

El Android Market en la Figura 12 puede ser visto en español, la página permite saber cuáles son las aplicaciones más destacadas y cuáles van en la punta en el top de ventas, así como las destacadas en el top gratis. Para la facilidad de búsqueda en aplicaciones, la pagina cuenta con una sección de categorías, conformada por juegos y aplicaciones.

3.2.3 OVI Store de Nokia. Propietaria, similar a Apple, pueden vetar las aplicaciones de su tienda³⁰.

³⁰Ibid.

Figura 13. OviStore de Nokia



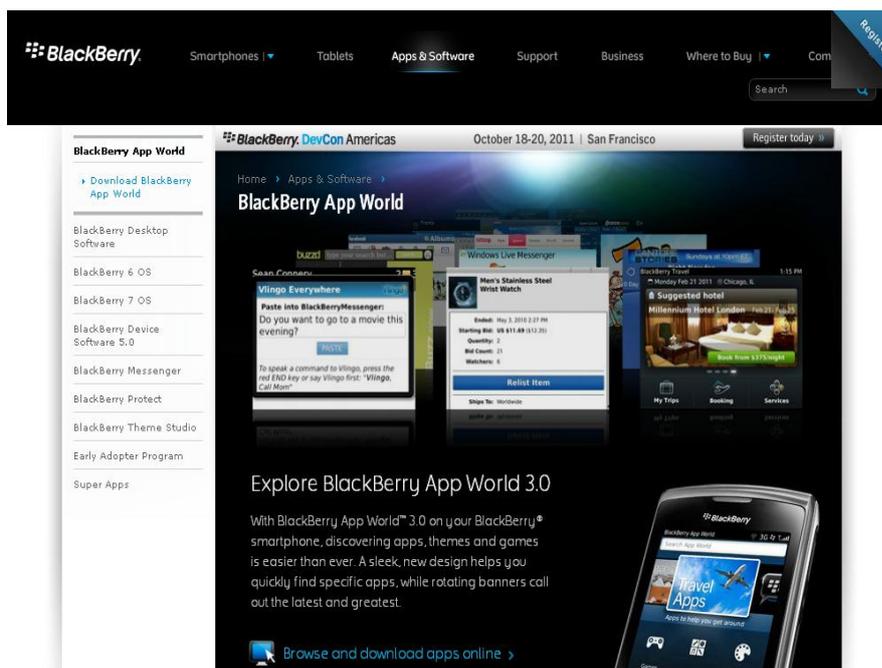
Fuente <http://store.ovi.com/?&lang=es> 419

El OviStore de Nokia Figura 13 puede ser visto en más de 10 idiomas. Cuenta también al igual que el Android Market con una sección de aplicaciones destacadas.

3.2.4 App Store de Blackberry. Propietaria, similar a Apple, pueden vetar las aplicaciones de su tienda³¹.

³¹Ibid.

Figura 14. App Store de Blackberry



Fuente <http://us.blackberry.com/apps-software/appworld/>

El App Store de Blackberry mostrado en la figura 14, ofrece App World, un software que permite búsquedas más sencillas de aplicaciones como fondos, juegos, entre otras.

En resumen, “el modelo de software de Apple, Blackberry y Nokia es cerrado en contraposición al modelo abierto de Android. Los tres primeros asumen la responsabilidad de las aplicaciones albergadas en su mercado, mientras que en Android esta responsabilidad se otorga a los propios desarrolladores. Hasta ahora, se ha demostrado que cada modelo tiene sus pros y sus contras, y que ninguno de ellos ha evitado la entrada de malware en sus dispositivos”³².

Para tener aplicaciones más seguras, se necesita de las buenas prácticas de programación por parte de los desarrolladores y también se necesita que el usuario se informe primero del contenido que quiere descargar a su dispositivo móvil a través de las páginas oficiales antes de instalarlo.

³²Ibid.

“Cabe destacar que la diversidad de tecnologías móviles, en comparación con la dominación de plataformas Windows en PC, puede jugar en contra de una gran proliferación de código malicioso en este entorno, ya que los creadores de malware deberán escribir el código malicioso apropiado para cada plataforma”³³.

Ahora con los Smartphones no solo se tiene un teléfono para recibir y realizar llamadas, ahora se tiene un teléfono del cual se puede acceder a internet para pagar cuentas bancarias, ver un video, enviar o recibir un correo y en fin muchas de las funcionalidades que posee un computador.

3.3 EN RIESGO: UN ESTUDIO DE AMENAZAS MOVILES ENCUENTRA VULNERABILIDADES DE SEGURIDAD TODO EL TIEMPO AL MAXIMO PARA DISPOSITIVOS MOVILES³⁴

En un estudio de amenaza global móvil dado a conocer el 10 de mayo de 2011, Juniper Networks (NYSE: JNPR) encontró que los dispositivos móviles empresariales y de consumo están expuestos a un número récord de amenazas de seguridad, incluyendo un aumento del 400 por ciento de malware para Android , así como altos ataques orientados a Wi-Fi. A través de un examen minucioso de las hazañas de los últimos programas maliciosos, el estudio describe las nuevas áreas de interés y ofrece recomendaciones claras sobre las tecnologías esenciales de seguridad y prácticas para ayudar a los consumidores, las empresas / pymes, entidades y las entidades del gobierno contra las vulnerabilidades a los dispositivos móviles.

Con los Smartphones listos para eclipsar a los PCs como el método preferido de la computación tanto personal como profesional, los ciber-delincuentes han dirigido su atención a los dispositivos móviles. Al mismo tiempo, la brecha entre las capacidades de los hackers y las defensas de una organización se está

³³Ibid.

³⁴ Traducción tomada del texto: At Risk: Global mobile threat study finds security vulnerabilities at all time highs for mobile devices. Disponible en: http://www.juniper.net/us/en/company/press-center/press-releases/2011/pr_2011_05_10-09_00.html

ampliando. Estas tendencias ponen en relieve la necesidad de una mayor conciencia sobre la seguridad móvil, así como más rigidez, y mejores políticas y soluciones integradas de seguridad móvil.

"En los últimos 18 meses se han producido imparables bombardeos de amenazas de interés periodístico, y aunque la mayoría se habían dirigido a computadoras de escritorio tradicionales, los hackers están fijando sus ojos en los dispositivos móviles. La consolidación de los sistemas operativos y en la puesta masiva y creciente de poderosos dispositivos móviles es tentador para los hackers atacar estos dispositivos ", Jeff Wilson, analista principal, dice en el artículo Security at Infonetics Research. "En una encuesta reciente de las grandes empresas, encontramos que casi el 40 por ciento consideraron a los Smartphones como el tipo de dispositivo que mas representa una amenaza de seguridad. Las empresas necesitan herramientas de seguridad que proporcionan protección integral: desde el núcleo de la red a la amplia gama de puntos finales que todos los departamentos de TI se ven obligados a administrar y proteger. "

El informe, "Malicious Mobile Threats Report 2010/2011", fue compilado por Juniper Networks Global Threat Center (GTC), una organización única dedicada a la realización de la seguridad "around-the-clock", la vulnerabilidad y la investigación de malware diseñado específicamente para plataformas y tecnologías de dispositivos móviles. El GTC examina cada vez más sofisticados ataques desde 2010 y 2011, como por ejemplo, Myournet/DroidDream, Tap Snake y Geinimi, así como las aplicaciones piratas de los " Walk and Text ", nuevas amenazas para la ciber-delincuencia móvil, y el potencial para la explotación y el mal uso de los dispositivos móviles y de datos.

3.3.1 Conclusiones del informe:

3.3.1.1 La ansiedad App Store. El único gran punto de distribución de malware móvil es la descarga de la aplicación, sin embargo, la gran mayoría de los usuarios de Smartphones no están empleando un antivirus en sus dispositivos móviles para escanear en busca de malware.

3.3.1.2 Preocupaciones Wi-Fi. Los dispositivos móviles son cada vez más susceptibles a los ataques de Wi-Fi, incluyendo aplicaciones que permiten a un atacante acceder fácilmente al correo electrónico de la víctima y a las aplicaciones de redes sociales.

3.3.1.3 Las amenazas de texto. El 17 por ciento de todas las infecciones reportadas se debieron a troyanos SMS que envían mensajes SMS a números de pago, a menudo a un costo irrecuperable para el usuario o empresa.

3.3.1.4 La pérdida y el robo de dispositivos. 1 de cada 20 dispositivos de los clientes de Juniper se perdieron o fueron robados, lo que requiere localizar, bloquear o borrar los comandos que son emitidos.

3.3.1.5 Conductas de riesgo adolescente. Un 20 por ciento de los adolescentes admite el envío de material inapropiado o explícito desde un dispositivo móvil.

3.3.1.6 "El peligro Droid". El número de ataques de malware Android ha aumentado en un 400 por ciento desde el verano de 2010.

"Estos resultados reflejan una tormenta perfecta de usuarios que no están informados o desinteresados en la seguridad, la descarga de aplicaciones disponibles de fuentes desconocidas y sin vetar en la ausencia completa de soluciones de seguridad para dispositivos móviles", dijo Dan Hoffman, evangelista jefe de seguridad móvil de Juniper Networks. "Los procesos de la aplicación de la App Store de remover de forma reactiva las aplicaciones

identificadas como maliciosas después de haber sido instaladas por miles de usuarios es insuficiente como medio para controlar la proliferación de malware. Hay pasos específicos que los usuarios deben tomar para mitigar los ataques móviles. Tanto las empresas como los consumidores necesitan ser conscientes de los crecientes riesgos asociados con la comodidad de tener Internet en la palma de sus manos. "

3.4 APLICACIONES MÁS SEGURAS DE ANDROID³⁵.

Gracias al hecho de que el sistema operativo Android permite realizar múltiples tareas más amplias que otros sistemas operativos populares de Smartphones, los dispositivos Android son capaces de soportar una amplia gama de funcionalidades de seguridad móvil que funcionan en un segundo plano de manera permanente, tales como copias de seguridad automáticas y los escaneos de antivirus.

Sin embargo, vale la pena tener en cuenta que la mayoría de las medidas esenciales de seguridad para su dispositivo Android, como la protección para el propio dispositivo con contraseña y establecer el auto-bloqueo después de un período específico de tiempo, no requieren de una aplicación – Ambas características pueden ser accedidas por Configuración -> Ubicación y seguridad.

Y con la llegada de Android 2.2, los dispositivos Android ahora ofrecen varias opciones de desbloqueo, que incluye un PIN numérico, una contraseña o un patrón gráfico (la última de las cuales se ha descubierto recientemente para ser fácilmente comprometida, según una investigación de la Universidad de Pennsylvania).

Si desea tener la protección de la contraseña de su dispositivo en un solo paso, aplicaciones como App Protector Pro (\$ 1.99), Carrot App Lock Pro (\$

³⁵ Traducción tomada del texto: Top 25 Android security apps. Disponible en: <http://www.esecurityplanet.com/trends/article.php/3935711/Top-25-Android-Security-Apps.htm>

1.50), Seal (€ 2.19) y Android Protector (gratis) también le permite proteger con contraseña las aplicaciones en de manera individual.

Y con el creciente número de aplicaciones disponibles en el Android Market, sin duda lo que sigue a continuación no es una lista exhaustiva, pero es la intención de darle un buen sentido de algunas de las opciones disponibles en la búsqueda de una mayor protección para su Smartphone Android - y por los datos que residen en él.

3.5 MALWARE Y PROTECCIÓN CONTRA ROBO

En la mayoría de los casos, no es necesario buscar soluciones distintas para el escaneo del anti-virus y la protección contra robo, ya que varios desarrolladores ofrecen una amplia gama de funciones de seguridad dentro de una sola aplicación para Android. Cada producto ofrece una amplia gama de funcionalidad ligeramente diferente - y vale la pena tener en cuenta que, dado que todas estas aplicaciones son relativamente nuevas, dependiendo de sus características es probable que también evolucionen.

El Lookout security suite (gratis) ofrece protección anti-virus, funcionalidad de debackup (para los contactos, fotos, video, correo electrónico y mensajes de texto), y un localizador de dispositivo perdido, que puede ser usado para mostrar la ubicación del dispositivo en un mapa online, sonará una alarma desde el propio dispositivo, y / o borrar de forma remota todos los datos en el dispositivo. Toda la funcionalidad de la aplicación se pueden manejar de forma remota desde la interfaz basada en Web

En este punto, Lookout parece ser la opción más completa - a pesar de que es seguro asumir que la funcionalidad de sus competidores probablemente crecerá para igualar o superar a Lookout en el tiempo.

La aplicación SMobileSystems' Security Shield (\$ 29.99) ofrece un escaneo de anti-virus, localizador, bloqueo del dispositivo remoto, y la limpieza remota del dispositivo. Para SMB y usuarios empresariales, SMobileSystems también

ofrece una amplia gama de soluciones de gestión de dispositivos para Android, Windows Mobile, Symbian Series 60 y Smartphones BlackBerry.

WaveSecure (\$ 19.90/año), el cual fue recientemente adquirida por McAfee, no ofrece protección anti-virus en este momento, aunque proporciona la funcionalidad de backup y restauración, así como la capacidad de localizar, bloquear o limpiar un dispositivo de forma remota. Cuando se bloquea de forma remota, el dispositivo también puede ser activado para mostrar un mensaje personalizable, tales como un número de teléfono para llamar en caso de que el dispositivo sea hallado.

Y DroidSecurity bien llamado antivirus (gratis) y antivirus Pro (\$ 9,99) proporcionan la funcionalidad de exploración de antecedentes de anti-virus - mientras que una opción FindrChromeextension (gratuito) añade la posibilidad de determinar la ubicación del dispositivo a través de GPS, y para bloquear o borrar todos los datos de el dispositivo de forma remota.

3.5.1 Gestión de contraseñas. Para gestionar todas las contraseñas de forma centralizada, LastPass (\$12.00/año) combina una aplicación de Android con el navegador de Firefox para PC, Safari, Chrome e Internet Explorer. Una contraseña maestra proporciona acceso a una bóveda de contraseña basado en la nube, y la aplicación y la extensión puede rellenar contraseñas en los sitios de forma automática, tanto en el PC como en el Smartphone Android.

El independiente SplashID (\$ 9.95) una aplicación de gestión de contraseñas se puede utilizar para almacenar contraseñas, tarjetas de crédito, PINs y más en un dispositivo Android, protegidos con cifrado Blowfish de 256 bits. Opcionalmente el desktop software (\$ 19.95) se puede utilizar para sincronizar datos del celular con una PC. Al igual que con LastPass, la aplicación Android se puede utilizar para rellenar las contraseñas por usted en un navegador móvil de propiedad.

Del mismo modo, la aplicación Callpod'sKeeper (\$ 29.99/año) ofrece encriptación de tipo militar, junto con el backup de datos en la nube, así como

para sincronizar los datos por Wi-Fi con el software de escritorio empresarial - en última instancia, LastPass, SplashID y Keeper son lo suficientemente similares que vale la pena la descarga de un trial gratuito de cada uno para decidir qué interfaz es mejor para los usuarios antes de hacer una compra.

Como alternativa, una opción mucho más barata y totalmente funcional es KeePassDroid (gratis), un puerto Android administrador de contraseñas open source de KeePass, que utiliza la aplicación gratuita DropBox para sincronizar los datos almacenados.

3.6 ATAQUES REALIZADOS A ANDROID 2010 - 2011³⁶

3.6.1 Google Android. El sistema operativo para móviles de Google (Android), como la fuerza dominante en el creciente mercado de dispositivos móviles, fue el objetivo más grande de malware y desarrolladores de exploits en 2010. Capaces de investigar, descubrir y aprovechar las debilidades, en ambos modelos de seguridad de Android y en el ecosistema abierto impulsado por el Android Market. Personas malintencionadas tomaron ventaja de un mercado con poca supervisión y un largo y potencial número de nuevos usuarios que fueron en gran parte sin educación, inconscientes o desinteresados en la seguridad móvil, y fueron introducidos a una gran cantidad de aplicaciones en su primera vez. Era, en efecto, una tormenta perfecta, que continua ocurriendo en 2011.

³⁶ Traducción tomada del texto: Malicious Mobile Threats Report 2010/2011. En: Google Android. P. 6-9 Disponible en: <http://www.juniper.net/us/en/dm/interop/go/>

3.6.2 Enero de 2010: Phising de dólares. A principios de enero de 2010, la primera aplicación de phising de banco apareció en el mercado de Android, la tienda oficial de aplicaciones para Android, cuando un desarrollador con el nombre de "Droid09" publicó una aplicación que pretendía ser un cliente bancario para acceder cuentas financieras en línea pidiendo al usuario sus credenciales de inicio de sesión, solo para enviarlas a una ubicación desconocida.

3.6.3 Marzo 2010: El primer Android "Botnet". En marzo de 2010, otro ataque altamente publicitado hacia Android tuvo lugar. El proveedor de servicios móviles Vodafone estaba enviando sin saberlo, dispositivos desde su fabricante de teléfonos móviles con tarjetas Secure Digital (SD) precargada con la Botnet Mariposa (Botnet es un término que hace referencia a un conjunto de robots informáticos o bots, que se ejecutan de manera autónoma y automática) que afectó a sistemas Windows.

Cuando un usuario desempaquetaba el nuevo dispositivo y lo conectaba mediante un cable USB a un PC basado en Windows para transferir archivos o sincronizar el dispositivo, la función de la tarjeta SD "autorun" iniciaría e infectaría el ordenador del usuario con el botnet.

3.6.4 Julio 2010: Spyware GPS de seguimiento Envuelto en el juego "Tap Snake". A finales de julio de 2010, el juego "Tap Snake" -en realidad era una aplicación spyware insidiosa- fue lanzada en el Android Market.

Para el usuario ocasional, no era más que un simple juego donde el usuario guiaba a la serpiente alrededor de los obstáculos pulsando la dirección en la que les gustaría que la serpiente se mueva.

En realidad, la "Tap Snake" era un spyware que podía monitorear la ubicación del dispositivo móvil a través del dispositivo GPS.

Fue acompañado por otra aplicación "GPS spy", que podía ser instalado en el dispositivo de un atacante Android y luego se utilizaba para acceder al portal

web en el que el juego "Tap Snake" cargaba la ubicación del dispositivo móvil infectado de la víctima, con fines de vigilancia.

3.6.5 Agosto 2010: El primer troyano SMS (Short Message Service) de Android. "Fake Player" fue el primer troyano SMS conocido en los dispositivos Android, y recorrió el mundo en agosto de 2010, que afectando a muchos usuarios rusos. La aplicación pretende ser un reproductor multimedia que envía mensajes SMS a números de tarificación adicional ruso a una tasa de 6,00 USD por mensaje. Mientras que el "Fake Player" nunca fue lanzado en el diario oficial de Android Market, ha seguido siendo actualizado dos veces al mes desde su lanzamiento original. La actualización más reciente se produjo en medio de octubre de 2010.

3.6.6 Noviembre de 2010: El Experimento "AngryBirds". Poco después de la última actualización conocida de "Fake Player", los investigadores de seguridad Jon Oberheide y ZachLanier dieron a conocer un notable exploit de Android en una conferencia de seguridad de Intel en Oregon.

Oberheide y Lanier mostraron que las iteraciones actuales del modelo de seguridad para Android incluyen una falla de seguridad que permite que una aplicación sea invisible para descargar aplicaciones adicionales o archivos APK (paquete para el sistema operativo Android), sin que se le avise al usuario sobre los permisos para descargar aplicaciones o aún sabiendo que las aplicaciones se están instalando. Con el fin de ilustrar cómo el Android Market y tiendas similares de aplicaciones pueden ser utilizadas contra un usuario de telefonía sin saberlo, Oberheide y Lanier eligieron el popular juego de "Angry Birds" como su mecanismo de entrega. Su prueba de concepto de malware no contenía ningún código malicioso actual, simplemente se retrataba a sí mismo como niveles de bonus para "Angry Birds" que, una vez instalado, abriría mas niveles para el jugador. En realidad, nada relacionado con "Angry Birds" se incluyó alguna vez en la aplicación. Sin embargo, Oberheide y Lanier probaron que los usuarios podían ser engañados en la descarga de esta aplicación, y que la aplicación podía descargar e instalar aplicaciones adicionales sin

preguntar al usuario para aprobar dichas instalaciones, o para verificar y estar de acuerdo con los permisos necesarios para que las aplicaciones de fondo fueran instaladas.

3.6.7 Diciembre de 2010: Android Toma la Corona como objetivo principal en malware móvil. En los últimos años, ha sido una práctica común para los creadores de malware piratear las aplicaciones de Symbian y de Windows Mobile para luego empacar código malicioso dentro de estas aplicaciones. Sin embargo, en diciembre de 2010, los investigadores descubrieron que una serie de aplicaciones para Android, descargadas de la página oficial de Android Market, fueron distribuidas a través de repositorios chinos de aplicaciones de terceros y las tiendas de aplicaciones. Las aplicaciones legítimas fueron desempaquetadas y el código malicioso, conocido como "Geinimi", se añadió a un máximo de 24 aplicaciones diferentes.

Las aplicaciones modificadas fueron luego re empaquetadas, apareciendo como la aplicación original para el usuario ocasional.

Las aplicaciones Geinimi infectadas se publicaron entonces en los sitios web chinos usados para distribuir software y aplicaciones para dispositivos móviles. En muchos casos, varias versiones de las aplicaciones pirateadas estaban disponibles, algunas eran maliciosas y otras no.

A menos que el usuario preste atención a los permisos que se aprueban en el momento de la instalación de la aplicación, no se darían cuenta de que nuevas capacidades maliciosas estaban siendo añadidas de otra manera hacia actividades inocuas.

Geinimi no sólo apalancaba aplicaciones pirateadas de Android para la distribución de malware, sino que también incluían un comando botnet bastante extenso y control de funcionalidad, incluían los primeros intentos de cifrado de las comunicaciones, y la ofuscación de código malicioso introducido directamente en la aplicación. Mientras que Geinimi monitoreaba las comunicaciones, cosechaba datos de identificación de los dispositivos móviles,

monitoreaba la ubicación de los datos, y enumeraba listas de las aplicaciones instaladas, también utilizaba un cifrado estándar de datos relativamente débil (DES del inglés Data Encryption Standard) para cifrar las cadenas en el código que revelaría la intención maliciosa cuando fueran analizados. El mismo sistema de cifrado DES se usó para cifrar el tráfico HTTP para el comando y las funciones de control.

3.6.8 Enero / Febrero 2011: La tormenta sigue con la amenaza en China. En las semanas siguientes al descubrimiento de Geinimi, los investigadores descubrieron dos nuevas familias de aplicaciones maliciosas que seguían el mismo enfoque y el método de difusión. Ambos "aDrD" y "pJapps" son familias diferentes de aplicaciones legítimas que fueron pirateadas en Android Market, descodificadas, empaçadas con códigos maliciosos, y luego re empaçadas para su difusión en las tiendas de aplicaciones de China. En conjunto, aDrD y pJapps representaron más de 75 aplicaciones diferentes pirateadas y troyanas.

3.6.8.1 Adrd. Mientras aDrD reunía grandes cantidades de información de identificación de dispositivos móviles, también trataban de identificar la puerta de enlace para el protocolo de aplicación inalámbrica (WAP) así se podría cambiar la configuración Wap para enrutar el tráfico a través de una puerta de enlace específica. Esto elevó artificialmente el perfil de búsqueda de sitios que contienen otras aplicaciones infectadas aDrD, promoviendo un mayor número de descargas. El aDrD también tenía la capacidad para llegar a la Internet y descargar versiones actualizadas de sí mismo al dispositivo.

3.6.8.2 PJApps. PJApps es similar en el tipo de infección y el método de difusión al Geinimi y el aDrD. Cuando un dispositivo se infecta con el pJapps, inmediatamente intenta registrarse con un servidor en línea mediante la obtención y el envío de la información de identificación del dispositivo móvil a una URL. Una vez el dispositivo se ha registrado, es configurado para descargar comandos desde una dirección URL diferente que ordena al dispositivo para enviar mensajes SMS a números de tarificación adicional, consulte a un servicio en línea para determinar si el número del dispositivo se encuentra en una lista negra en cualquier lugar, realizar spam SMS, descarga de aplicaciones adicionales para el dispositivo, vaya a un sitio web después de la comprobación de la existencia de una lista de determinados navegadores Android, y establecer una serie de favoritos del navegador.

3.6.9 Marzo 2011: Myournet / DroidDream ofrece pesadillas a los usuarios Android. Ya que los investigadores todavía estaban tratando de descubrir el alcance de aDrD y pJapps, el Android Market, una vez más fue golpeado con una venganza por "Myournet", también conocido como "DroidDream".

Myournet / DroidDream eran también una serie de aplicaciones legítimas que fueron pirateadas fuera del Android Market, decodificadas, y luego llenas con códigos maliciosos. La diferencia entre Myournet / DroidDream y Geinimi, aDrD y pJapps, fue el método de difusión. En el caso de Myournet /DroidDream, tres cuentas diferentes de desarrollador se crearon y más de 55 aplicaciones infectadas se encontraron en el interior del Android Market. Las aplicaciones infectadas se sabe que han existido en el Android Market por al menos cuatro días, y fueron descargadas de entre 50.000 y 250.000 veces en exclusiva a los dispositivos Android.

Myournet inicialmente fue nombrado después de que la primera cuenta de desarrollador identificada, estuviera colocando estas aplicaciones maliciosas. Inmediatamente después de establecerse en ese nombre, la industria de la seguridad en telefonía móvil, comenzó a llamar a la familia de programas

maliciosos DroidDream porque era considerado como la madre de todo el malware en Android. En muchos casos, tenían razón.

Myournet / DroidDream comenzó su reinado de terror, intentando aprovechar el "rageinthecage" exploit que permite el acceso root en el dispositivo móvil. "Rooting" un dispositivo Android permite que una aplicación gane acceso a los sistemas y servicios que de alguna manera no están disponibles para una aplicación normal. Una vez que Myournet / DroidDream ha arraigado con éxito el dispositivo, instala otro archivo APK que fue ofuscado en el código de la solicitud original. Esto entonces le permitía a la aplicación ser instalada en el fondo sin absolutamente ninguna intervención o conocimiento del usuario.

La aplicación recién instalada tenía Myournet / DroidDream con acceso ilimitado a una gran cantidad de usuarios sensibles y a la información de identificación del dispositivo, que era recolectada y luego enviada a un servidor de terceros en California. A continuación, la aplicación infectada facilitaría la descarga e instalación de aplicaciones adicionales en el dispositivo, una vez más llevado a cabo sin la interacción o conocimiento del usuario.

Myournet / DroidDream marcó la primera vez que el malware de Android había sido puesto a disposición y distribución a través del Android Market a gran escala. La táctica demostró que el enfoque abierto de Google hacia su Android Market, lamentablemente podría permitir aplicaciones maliciosas en el ecosistema, con el potencial de afectar a un gran número de usuarios de forma rápida.

Los usuarios que sospechaban que estaban infectados con malware tenían sólo un recurso para revertir los efectos de la infección, y era realizando un restablecimiento (reset) de sus dispositivos, posibilitando la pérdida de grandes cantidades de datos y la configuración de su equipo en caso tal de no tener una buena copia de seguridad o una herramienta de restauración. El impacto de más de 50.000 usuarios realizando un restablecimiento de sus dispositivos móviles, probablemente tomaría un impuesto sobre los proveedores de servicio, sin duda, atendiendo miles de llamadas de servicios de apoyo.

Google lanzó una aplicación que podría revertir los efectos de las infecciones Myournet/DroidDream, así los usuarios no se verían obligados a realizar un restablecimiento completo en su dispositivo. De este modo, Google lanzó el Android Market de herramientas de seguridad, fue lanzado de forma automática a los dispositivos móviles que habían sido infectados con Myournet / DroidDream. Google determina que dispositivos descargaron las aplicaciones refiriéndose a la cuenta de caja del usuario. Incluso después de instalar esta actualización, la vulnerabilidad subyacente responsable del rooting se mantiene, lo que acentúa la necesidad de una solución antimalware que vaya tomando lugar para evitar futuras infecciones relacionadas con el rooting.

La herramienta de seguridad de Android Market fue puesta de forma automática en el dispositivo móvil del usuario, una vez instalado, realiza una serie de actividades para eliminar los efectos de la infección Myournet / DroidDream, y luego se retira a si mismo del dispositivo. Por lo tanto, no era necesario para los usuarios hacer otra cosa más que esperar a la actualización para ser puesta a su equipo y para comenzar automáticamente la limpieza de la infección. Google publicó la herramienta de seguridad del Android Market, con estrictas instrucciones que indicaban que no era necesario descargar manualmente la aplicación. Sin embargo, sólo unos pocos días más tarde, una versión de la herramienta de seguridad de Android Market que había sido pirateada del Android Market, descodificada, y llenada de códigos maliciosos, se estaba difundiendo en las tiendas de aplicaciones de terceros con sede en China.

La versión corrupta de la herramienta de seguridad de Android Market en las tiendas de aplicaciones chinas tenía una capacidad adicional más allá de las diseñadas por Google. Esta nueva versión pirateada y troyana de la herramienta de seguridad de Android Market recolectó información sensible de de los dispositivos y los envió a un servidor en línea. Una vez que el dispositivo móvil se comprobó en el servidor en línea, comenzó a recibir órdenes para enviar mensajes SMS a números de pago que sólo eran efectivos en el interior de China y en redes de proveedores de servicios de este mismo país.

3.6.10 Abril 2011: La Broma en usted. Más recientemente, el mundo de Android vio a la aplicación decimocuarta clasificada en la lista de "101 mejores aplicaciones Android", "Walk and Text", pirateada fuera del Android Market. Sin embargo, este caso fue un poco diferente, el desarrollador que pirateó y reempacó la aplicación lo hizo sólo para ridiculizar a los usuarios que instalaron estas aplicaciones piratas.

Parece que varias horas después de que una nueva versión de la popular aplicación "Walk and Text" golpeará el Android Market, ya había sido pirateado y compartido en las tiendas de aplicaciones de terceros. Un desarrollador aprovechó esta versión pirata de la aplicación fuera de una tienda de aplicaciones de terceros y decidió seguir la rutina de sus predecesores, la deconstrucción de la aplicación, y el relleno con su propio código malicioso.

En el caso de la aplicación maliciosa "Walk and Text", tan pronto como un usuario instalara la aplicación que había sido "cargada en el sitio", comenzaba el envío de mensajes SMS a todos los contactos del usuario almacenados en el dispositivo móvil con un mensaje que decía, "hey, acabo de descargar [sic] una aplicación pirata de la Internet, Walk and Text para Android. Soy [sic] estúpido y barato, costó [sic] sólo 1 dólar [sic]. No lo [sic] robes como lo hice yo! "

Tabla 1. Comparacion de características entre diferentes plataformas.³⁷

Basis of Comparison	iOS 5 (iPhone)	Android 2.3 (Gingerbread)	Windows Phone 7 (Mango)	Blackberry 7 OS
Unified Notifications	✓	✓	✓	✓
Phone-to-Phone Messaging	✓	✗	✗	✓
Newspaper/Magazine Subscriptions	✓	✗	✗	✗
Advanced Reminder System	✓	✗	✗	✗
System-Wide Twitter Integration	✓	✗	✓	✗
Quick Camera Access	✓	✗	✓	✗
Photo Editing Tools	✓	✓	✗	✗
Tabbed Browsing	✓	✗	✓	✓
Reader View	✓	✗	✗	✗
Rich Text Email	✓	✗	✓	✓
PC-Free Setup, Updates	✓	✓	✓	✓
Wi-Fi Sync	✓	✗	✓	✓
Online Gaming Community	✓	✗	✓	✗

Fuente <http://img.actualidadiphone.com/wp-content/uploads/2011/06/Screenshot-2011-06-10-at-20.53.25.png>

En la tabla 1 se puede observar diferentes características entre varias plataformas para Smartphones, de las cuales se observa que el IOS 5 cuenta con todas ellas, esto no quiere decir que las demás no las tengan, sino que se deben instalar aplicaciones para que cuenten con estas funcionalidades.

³⁷ Gnzl. 12 de junio de 2011. Comparativa: iOS 5 vs Android Gingerbread, WP7 Mango y Blackberry 7. [En línea]. Disponible en: <http://www.actualidadiphone.com/2011/06/12/comparativa-ios-5-vs-android-gingerbread-wp7-mango-y-blackberry-7/>

CAPITULO 4: CONCLUSIONES, RECOMENDACIONES Y REFERENCIAS BIBLIOGRÁFICAS.

4.1 ERRORES MÁS COMUNES

Debido a su masividad, los Smartphones se convirtieron en un objetivo de ataque bastante atractivo para los desarrolladores de malware ya que tienen la gran facilidad de comunicarse con el internet, esto es una gran ventaja para los desarrolladores de códigos maliciosos porque a través de este medio se pueden difundir fácil y rápidamente dichos códigos.

Los ataques a los Smartphones tienen gran variedad, desde los que solo hacen que se desgaste la batería hasta ataques que pueden dejar el dispositivo sin servicio. Virus, spam y contagio de portátil a dispositivo móvil pertenecen a la larga lista de vulnerabilidades que poseen los dispositivos móviles. Así como existen muchas formas de atacar los Smartphones, existen también errores muy comunes a la hora de utilizar los servicios propios u asociados de los Smartphone. Como por ejemplo:

- Dejar abiertas las conexiones a tecnologías como Wi-fi y Bluetooth después de haberlas utilizado.
- Dejar el equipo sin contraseña, así cuando este es robado esta persona puede acceder a toda la información en el Smartphone.
- No clasificar la información antes de ingresarla al Smartphone, como por ejemplo meter estados de cuentas o avances financieros en el celular, así es más factible de que roben esta información.
- No encriptar los datos en los Smartphones, ni instalar un programa antivirus es un error común a nivel empresarial.
- El uso de software ilegal y la no verificación de donde provienen las aplicaciones que se instalan en el Smartphone, esto es importante ya que

se encontró una aplicación la cual decía que su desarrollador era un importante cantante del pop.

4.2 APORTES

El avance en la tecnología móvil ha permitido que los usuarios ahora puedan apreciar imágenes, con textura, profundidad y color en sus teléfonos celulares, ya sea solo para guardarla o para personalizar dicho dispositivo. Esta característica de visualización hizo que también se pensara en estilos para la fabricación de celulares, estilos que van desde modelos deportivos hasta de altos ejecutivos. Pero lo más importante es que estos teléfonos adoptaron la habilidad de correr sistemas operativos y de ampliar su capacidad de almacenamiento, para poder así guardar cualquier tipo de archivo que sea soportado por el dispositivo, como lo son el audio, el video y el texto.

Los Smartphones se han convertido en un elemento muy importante para el uso de todo tipo de personas, desde solo entretenimiento u ocio, escuchando música mientras se hace deporte, hasta ganando tiempo en el pago de deudas o la realización de consultas y transacciones a través de dichos dispositivos para los ejecutivos o trabajadores de compañías.

Al hacer estos dispositivos con mejores características como almacenamiento o nuevas funcionalidades, también se hace necesario empezar a mejorar las barreras de seguridad que son evadidas por los desarrolladores de códigos maliciosos. Ya sea colocando mas filtros a la hora de subir alguna aplicación, o simplemente incentivando al programador a hacer uso de las confirmaciones del usuario.

Los teléfonos móviles han ido cambiando su apariencia y se han convertido para algunos en una adquisición de lujo. Las pantallas de gran tamaño en los Smartphone ahora permiten tener una mejor visualización de lo que se está haciendo en el celular con alta calidad en el detalle. Así como las diferentes características que permiten y facilitan tareas cotidianas como los pagos a

través de internet, consultas web, recordatorios, comparaciones de precios, entre otros.

Con respecto a la seguridad de los Smartphones, no importa el número de medidas que se tengan, nunca se estará completamente protegido de las amenazas que constantemente atacan a los usuarios de estos dispositivos. A pesar de esto es bueno tomar cierto tipo de medidas para estar protegidos de los ataques más comunes.

Los Smartphones al estar compitiendo ya con los computadores personales, se tiende a guardar información de vital importancia en estos dispositivos, es así que surgen una gran cantidad de ataques por parte de piratas que desean obtener información de las cuales se puedan lucrar, o que por simple diversión hacen ataques o programas maliciosos que perjudican a todos los usuarios de los Smartphones.

Es factible no estar de acuerdo con el sistema de seguridad de Android Market, debido a que todas las aplicaciones pueden ser subidas a esta plataforma sin ninguna restricción, y cualquier persona las tendrá disponibles para su uso personal, y será éste quien determine si esta aplicación es o no segura para la función para la cual fue programada. Esto no es una buena política debido a que existen una gran cantidad de usuarios inexpertos en este tema y son ellos quienes más afectados se ven por los programas maliciosos subidos a esta plataforma.

Es importante que las personas se den cuenta de que los Smartphones, al tener acceso internet se tiene un dispositivo, que a pesar de su tamaño, se tiene todo un mundo en sus manos, y que es muy probable el hecho de que por este medio se realicen una gran cantidad de ataques.

Con la tecnología evolucionando cada vez más rápido, los nuevos modelos de Smartphones tendrán cada vez mas aplicaciones que faciliten el diario vivir de las personas, esto llevará a que los creadores de malware sean aun mas difíciles de controlar debido a que las personas, van a tender a guardar información más valiosa en sus dispositivos móviles, así que es importante que

las personas sigan las reglas de seguridad de cada fabricante para evitar ataques malintencionados y se disminuya el robo de información importante que sucede diariamente en el mundo.

4.3 RECOMENDACIONES

Con el fin de protegerse contra las crecientes amenazas de malware para dispositivos móviles, se recomienda lo siguiente:

4.3.1 Para los consumidores.

- Instalar en el dispositivo una solución antimalware para protegerlo contra las aplicaciones maliciosas, spyware, tarjetas SD infectadas, y los ataques de malware basados en el dispositivo.
- Use en el dispositivo un firewall personal para proteger las interfaces del dispositivo.
- Se requiere una contraseña robusta de protección para el acceso al dispositivo
- Implementar software anti-spam para proteger contra comunicaciones de voz y de SMS / MMS.
- Para los padres, un software de monitoreo para supervisar y controlar el uso de dispositivos móviles para la protección contra el acoso cibernético, el uso inadecuado o de explotación, y otras amenazas.

4.3.2 Para las empresas, agencias gubernamentales y pymes.

- Emplear en el dispositivo anti-malware para protegerse contra aplicaciones maliciosas, spyware, tarjetas SD infectadas y los ataques de malware contra el dispositivo móvil.

- Usar clientes SSL VPN para proteger fácilmente los datos en tránsito y garantizar la autenticación de red adecuada y los derechos de acceso.
- Centralizar el bloqueo remoto, limpieza, copias de seguridad y restaurar las instalaciones para los dispositivos perdidos o robados.
- Aplicar totalmente las políticas de seguridad, tales como ordenar el uso de fuertes contraseñas y PINes.
- Aprovechar las herramientas que ayudan a monitorear la actividad del dispositivo para la fuga de datos y el uso inadecuado.
- Centralizar la administración del dispositivo móvil para hacer cumplir e informar las políticas de seguridad.

4.4 CONCLUSIONES

- Los dispositivos móviles se han estado transformando hasta prácticamente coincidir en cuanto a funcionalidades con los ordenadores personales, todo esto conlleva a un incremento en la utilización de estos dispositivos en cualquier tipo de tarea. Por otra parte, se incrementan también los riesgos causados al acelerado uso de estas tecnologías, concebidas en muchos casos sin tener en cuenta la seguridad.
- Se les llama Smartphone a los dispositivos que a partir de la funcionalidad de un teléfono móvil, han evolucionado hasta estar más cercanos, en la actualidad, de un ordenador personal portátil. Es normal hoy en día que esta clase de teléfonos dispongan de agenda, GPS, reproductor de vídeos y música, muchas opciones de conectividad y un número muy grande de funcionalidades que hasta hace unos años eran inimaginables para estos dispositivos.
- La salida al mercado teléfonos móviles con sistema operativo Windows CE y la venta también del primer modelo de Blackberry en 2002 gracias a Research in Motion (RIM) fueron unos de los hechos más importantes, este

ultimo lo fue gracias, en gran parte, a la mejora que hace del manejo del correo electrónico.

- Apple Inc. en el 2007, introdujo su primera generación de Smartphone los cuales llamó iPhone. Estos dispositivos, se convertirían en uno de los primeros que permitió ser controlado completamente por una pantalla táctil, a partir de esto, marcarían un punto de inclinación en ésta parte del mercado. A lo largo de estos últimos años, Apple ha lanzado nuevas versiones de su iPhone los cuales soportan 3G y permite la descarga de aplicaciones desde su propia comunidad más conocida como App Store.
- En el 2008 se da a conocer Android, una plataforma de código abierto hecha solo para Smartphones, el cual se basó en Linux, en una modificación de su Kernel. Ésta plataforma se transformó en emblema del consorcio Open Handset Alliance, hecho y fomentado por Google en el año 2007 y “está compuesto por varios fabricantes, desarrolladores y operadores (Intel, HTC, Dell, ARM, Motorola, entre otros) con el propósito de desarrollar estándares abiertos para dispositivos móviles”.
- RIM y su Blackberry App World, Nokia con su OviStore (mayo 2009), Palm y Palm App Catalog (junio 2009) o Microsoft con Windows Marketplace for Mobile (octubre 2009) son una muestra de que muchos fabricantes usan la línea de crear comunidades para la gestión de sus aplicativos.
- La introducción de las pantallas táctiles transformó el mercado, ya que atrajo a los usuarios por medio de una interfaz fácil e intuitiva, debido también a que su superficie de visualización es mucho más amplia y usable que permitió distintas funciones entre las que están la navegación web y la reproducción de archivos multimedia con muy buena calidad.
- El desarrollo paralelo del hardware de los dispositivos móviles, hace que actualmente sea muy común encontrar terminales con procesadores de 1 GHz y más de 512 MB de RAM, con funcionalidades como acelerómetros, bluetooth, brújula o GPS, lo que brinda a los desarrolladores una gama amplia de posibilidades que aun no son desconocidas.

- Los creadores de malware mejoran continuamente sus tácticas y no hay ninguna duda de que el malware para dispositivos móviles seguirá evolucionando, por lo que hay que estar preparado para futuras infecciones.
- Los bancos están creando cada vez más sus propias aplicaciones para dispositivos móviles. La posibilidad de que malware para dispositivos móviles que utilicen mejores técnicas para interceptar llamadas que capturen información sensible es muy alta.
- Ahora que muchos dispositivos móviles tienen incorporados GPS, sería de vital importancia desarrollar aplicaciones que al ser consultadas, entreguen una señal para ubicarla como coordenada en el GPS, que puedan detectar los servidores las personas atacantes.
- Hoy en día los dispositivos móviles integran conexión a las redes Wi-Fi, no es descabellada la idea de que puedan existir gusanos que exploren los sistemas que tienen una determinada red Wi-Fi, e infiltren códigos maliciosos a estos sistemas explotando sus vulnerabilidades.
- Puede existir malware que cambie la agenda personal de un usuario, esto puede ser muy útil para suplantar una identidad, asociando un número a otra persona, utilizando ingeniería social orientada.
- Debido a que los Smartphones son dispositivos más pequeños, se tiene la sensación de que se tenemos un control físico total sobre éste y que serán menos accesibles para los intrusos. Esta falsa sensación de seguridad, además del uso de funcionalidades tales como contenido multimedia privado, redes sociales y correo electrónico, trae como consecuencia de que el dispositivo móvil contenga información privada la cual el usuario no se percata o pasa por alto.
- La contraseña es, la mayoría de los casos, la única herramienta de seguridad en la mayoría de los Smartphones. La seguridad en los Smartphones depende mucho de la seguridad y la confiabilidad de las aplicaciones que estén disponibles para instalar.

- Es importante tener métodos de cifrado, para que llegado el caso de robo o pérdida del dispositivo no se permita el acceso a la información. Esto es muy importante debido a que existen empresas en las que se unen las políticas de seguridad con el uso de estos dispositivos, así que mantener la información asegurada es de vital importancia.
- La seguridad de los Smartphones abarca desde el kernel del sistema operativo hasta en el modelo distribución de cada una de sus aplicaciones, y terminando en cada uno de los entornos de desarrollos existentes de cada plataforma, así que la seguridad no se puede ver solo desde el punto de vista del usuario que tiene en funcionamiento el Smartphone.
- “El modelo de software de Apple, Blackberry y Nokia es cerrado en contraposición al modelo abierto de Android. Los tres primeros asumen la responsabilidad de las aplicaciones albergadas en su mercado, mientras que en Android esta responsabilidad se otorga a los propios desarrolladores. Hasta ahora, se ha demostrado que cada modelo tiene sus pros y sus contras, y que ninguno de ellos ha evitado la entrada de malware en sus dispositivos
- Para tener aplicaciones más seguras, se necesita de las buenas prácticas de programación por parte de los desarrolladores y también se necesita que el usuario se informe primero del contenido que quiere descargar a su dispositivo móvil a través de las páginas oficiales antes de instalarlo.
- Cabe destacar que la diversidad de tecnologías móviles, en comparación con la dominación de plataformas Windows en PC, puede jugar en contra de una gran proliferación de código malicioso en este entorno, ya que los creadores de malware deberán escribir el código malicioso apropiado para cada plataforma
- Ahora con los Smartphones no solo se tiene un teléfono para recibir y realizar llamadas, ahora se tiene un teléfono del cual puedes acceder a internet para pagar cuentas bancarias, ver un video, enviar o recibir un correo y en fin muchas de las funcionalidades que posee un computador.

- Con los Smartphones listos para eclipsar a los PCs como el método preferido de la computación tanto personal como profesional, los ciberdelincuentes han dirigido su atención a los dispositivos móviles. Al mismo tiempo, la brecha entre las capacidades de los hackers y las defensas de una organización se está ampliando. Estas tendencias ponen en relieve la necesidad de una mayor conciencia sobre la seguridad móvil, así como más rigidez, y mejores políticas y soluciones integradas de seguridad móvil.
- Tanto las empresas como los consumidores necesitan ser conscientes de los crecientes riesgos asociados con la comodidad de tener Internet en la palma de sus manos.
- Con la llegada de Android 2.2, los dispositivos Android ahora ofrecen varias opciones de desbloqueo, que incluye un PIN numérico, una contraseña o un patrón gráfico (la última de las cuales se ha descubierto recientemente para ser fácilmente comprometida, según una investigación de la Universidad de Pennsylvania).
- A menos que el usuario preste atención a los permisos que se aprueban en el momento de la instalación de la aplicación, no se darían cuenta de que nuevas capacidades maliciosas estaban siendo añadidas de otra manera hacia actividades inocuas.

4.5 BIBLIOGRAFÍA

1. Alex Aliaga. 12 de Marzo de 2010. Android en un microondas. [En línea]. Disponible en internet en: <http://www.linuxzone.es/2010/03/12/android-en-un-microondas/>
2. Android Developers. What is android?. [En línea]. Disponible en: <http://developer.android.com/guide/basics/what-is-android.html>
3. Android Open Source Project. [En línea]. [Consultado el 3 de septiembre de 2011]. Disponible en: <http://source.android.com/about/philosophy.html>

4. Consejo Nacional Consultivo de Cyber – Seguridad. Malware en Smartphones. [En línea]. [Consultado el 2 de septiembre de 2011]. Disponible en: <http://www.hispasec.com/laboratorio/Malware%20en%20Smartphones%20NCCS%20.pdf>
5. Constanza Maecha. Zona Movilidad. 08 de Mayo de 2011. Según kaspersky-lab en 2010 se detectó un 65% más de malware para Smartphones [en línea]. Disponible en internet: http://www.juniper.net/es/es/company/press-center/press-releases/2011/pr_2011_05_11-18_00.html
6. Enck, W., Ongtang, M., McDaniel, P. Understanding Android Security. [Online], Pennsylvania State Univ., University Park, PA URL: <http://ieeexplore.ieee.org.ezproxy.utp.edu.co/stamp/stamp.jsp?tp=&arnumber=4768655> .
7. Gartner. 11 de Agosto de 2011. Gartner Says Sales of Mobile Devices in Second Quarter of 2011 Grew 16.5 percent Year-on-Year; Smartphone Sales Grew 74 Percent. [En línea]. Disponible en internet: <http://www.gartner.com/it/page.jsp?id=1764714>
8. Gnzl. 12 de junio de 2011. Comparativa: iOS 5 vs Android Gingerbread, WP7 Mango y Blackberry 7. [En línea]. Disponible en: <http://www.actualidadiphone.com/2011/06/12/comparativa-ios-5-vs-android-gingerbread-wp7-mango-y-blackberry-7/>
9. International Telecommunication Union. Global Mobile Cellular 00-10 estadistic. [En línea]. Disponible en internet: <http://www.itu.int/ITU-D/ict/statistics/>

10. Ittipon Rassameeroj y Yuzuru Tanahashi, Various Approaches in Analyzing Android Applications with its Permission-Based Security Models [online], URL:<http://ieeexplore.ieee.org.ezproxy.utp.edu.co/stamp/stamp.jsp?tp=&arnumber=5978583> .
11. Open Handset Alliance. [En línea]. [Consultado el 3 de septiembre de 2011]. Disponible en: <http://www.openhandsetalliance.com/>
12. Shabtai, A. ; Fledel, Y. ; Kanonov, U. ; Elovici, Y. ; Dolev, S. ; Glezer, C. Google Android: A Comprehensive Security Assessment [online], Security & Privacy, IEEE, Ben-Gurion Univ. of the Negev, Beer-Sheva, Israel URL: <http://ieeexplore.ieee.org.ezproxy.utp.edu.co/stamp/stamp.jsp?tp=&arnumber=5396322&tag=1> .
13. Shabtai, A. ; Fledel, Y. ; Kanonov, U. ; Elovici, Y. ; Dolev, S. ; Glezer, C. *Android Intrusion-detection/prevention system*. En: Google Android: A Comprehensive Security Assessment [Base de datos en línea]. P. 43. [Citado el 5 de septiembre de 2011]. Disponible en IEEE Xplore Digital Library.
14. Traducción tomada del texto: A Complete History of Android. Disponible en: <http://www.techradar.com/news/phone-and-communications/mobile-phones/a-complete-history-of-android-470327>
15. Traducción tomada del texto: At Risk : Global mobile threat study finds security vulnerabilities at all time highs for mobile devices. Disponible en: http://www.juniper.net/us/en/company/press-center/press-releases/2011/pr_2011_05_10-09_00.html

16. Traducción tomada del texto: Malicious Mobile Threats Report 2010/2011.
En: Google Android. P. 6-9 Disponible en:
<http://www.juniper.net/us/en/dm/interop/go/>
17. Traducción tomada del texto: Top 25 Android security apps. Disponible en:
<http://www.esecurityplanet.com/trends/article.php/3935711/Top-25-Android-Security-Apps.htm>
18. Ward Mark. 9 de agosto de 2010. Smartphone security put on test. [En línea]. [Consultada el 14 de Septiembre de 2011]. Disponible en internet en:
<http://www.bbc.co.uk/news/technology-10912376>
19. Wei Tang, Guang Jin, Jiaming He, Xianliang Jiang. Extending Android Security Enforcement with A Security Distance Model [online], College of Information Science and Engineering Ningbo University, Ningbo, Zhejiang, China, URL:
<http://ieeexplore.ieee.org.ezproxy.utp.edu.co/stamp/stamp.jsp?tp=&arnumber=6006288> .
20. Wook Shabtai, A.; Fledel, Y.; Kanonov, U.; Elovici, Y.; Dolev, S.; Glezer, C. *Android Security Mechanisms*. En: Google Android: A Comprehensive Security Assessment [Base de datos en línea]. P. 36. [Citado el 5 de septiembre de 2011]. Disponible en IEEE Xplore Digital Library.
21. Wook Shabtai, A.; Fledel, Y.; Kanonov, U.; Elovici, Y.; Dolev, S.; Glezer, C. *Application permissions*. En: Google Android: A Comprehensive Security Assessment [Base de datos en línea]. P. 37. [Citado el 5 de septiembre de 2011]. Disponible en IEEE Xplore Digital Library.
22. Wook Shabtai, A.; Fledel, Y.; Kanonov, U.; Elovici, Y.; Dolev, S.; Glezer, C. *Data encryption*. En: Google Android: A Comprehensive Security

Assessment [Base de datos en línea]. P. 42. [Citado el 5 de septiembre de 2011]. Disponible en IEEE Xplore Digital Library.

23. Wook Shin, Shinsaku Kiyomoto, Kazuhide Fukushima, y Toshiaki Tanaka. Towards Formal Analysis of the Permission-based Security Model For Android [online], KDDI R&D Laboratories, Saitama, Japan [URL:http://ieeexplore.ieee.org.ezproxy.utp.edu.co/stamp/stamp.jsp?tp=&arnumber=5279458&tag=1](http://ieeexplore.ieee.org.ezproxy.utp.edu.co/stamp/stamp.jsp?tp=&arnumber=5279458&tag=1) .

24. Wook Shin, Shinsaku Kiyomoto, Kazuhide Fukushima, and Toshiaki Tanaka. Introduction. En: Towards Formal Analysis of the Permission-based Security Model for Android [Base de datos en línea]. P. 6. [Citado el 1 de septiembre de 2011]. Disponible en IEEE Xplore Digital Library.