SISTEMA DE SEGURIDAD APLICADO A DISPOSITIVOS MOVILES ANDROID

Ortiz Bohórquez Sergio Darío
sergioortiz2007@gmail.com

Rojas Pinzon Julián Francisco
julianfrancisco@gmail.com

Universidad Piloto de Colombia
Bogotá, Colombia

Resumen– En este artículo se busca recopilar y realizar un análisis de los servicios y sistemas de seguridad aplicados a el sistema operativo Android a su vez se revisan las causales y vulnerabilidades en los dispositivos Smartphone que cuentan con este sistema operativo, por último se revisara un modelo de seguridad que pueda garantizar niveles aceptables de seguridad sobre el sistema operativo Android.

Abstract– This article seeks to collect and analysis of services and safety systems applied to the Android OS turn reviews the causes and vulnerabilities in Smartphone devices that have this operating system finally review a security model can ensure acceptable levels of safety on the Android operating system.

Palabras claves—Android, vulnerabilidades, seguridad, sistema operativo, Smartphone.

Keywords—Android, vulnerabilities, security, operating system, Smartphone.

I. INTRODUCCIÓN

En la actualidad el crecimiento de tecnologías móviles, especialmente en el sistema operativo Android, sumado al crecimiento de plataformas y sistemas de comunicación como redes sociales, atraen la curiosidad e interés comercial de usuarios, empresas y delincuentes, los cuales no son ajenos al potencial que encierran. Estas tecnologías permiten almacenar la información de los usuarios y compartirla en tiempo real, como otras que se basan y se establecen sobre las anteriores generando mejoras en servicios como comercio electrónico, que son creadas para el sistema operativo antes mencionado. Por esto, es importante proponer un sistema de seguridad que permita alertar y prevenir sobre el estado del dispositivo Android frente a las actuales competencias del mercado, que de cierto modo pueden llegar a ser desconcertantes.

II. MATERIALES Y METODOS

Un sistema de seguridad, es un software diseñado para proteger los equipos de diversas formas de malware e intrusiones no autorizadas1. Para hacer frente a los problemas de seguridad que amenazan los dispositivos móviles que hoy por hoy se aplican en la estafa y delincuencia cibernética, es necesario entender los conceptos de seguridad y vulnerabilidad, herramientas, procedimientos, los diferentes tipos de ataques, estructura del sistema operativo Android y los objetivos que hacen de sus víctimas un factor ideal.

Este documento inicia con el levantamiento de información y análisis de

[1]OJA Dan, PARSONS June Damrich. “Conceptos de Computación: Nuevas Perspectivas”, Cenage Learning Editores S.A. 2008, página 158.

los sistemas que actualmente operan y protegen los dispositivos móviles Android, basados en la investigación del estado del arte en donde se identificarán y tipificarán las diferentes amenazas que adolecen los dispositivos, partiendo de esto se diseñará un sistema de seguridad que garantice la confidencialidad y seguridad del dispositivo móvil.

Posteriormente, se revisara un escenario de prueba para validar los diferentes tipos de aplicaciones de seguridad donde se hace un seguimiento a cada uno de los pasos y se documentan los resultados.

Con base en los temas anteriormente mencionados, se plantea como propuesta de investigación diseñar un sistema que busca optimizar la seguridad y confidencialidad de los usuarios de los dispositivos basados en el sistema operativo Android.

III. PORQUE EN DISPOSITIVOS ANDROID?

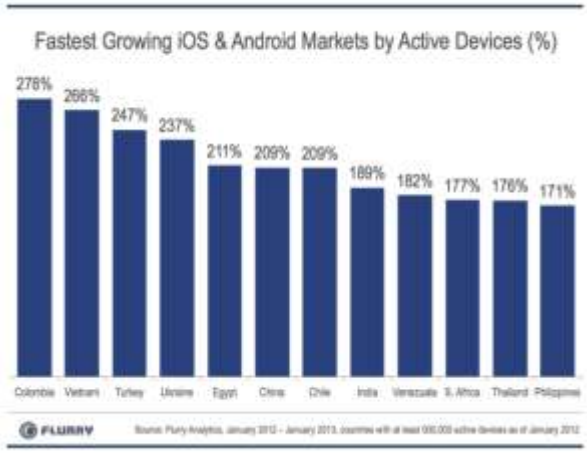
Con el 51% de participación en el mercado actual, el sistema operativo Android ha superado a sus principales competidores como symbian con 11%, IOS con el 24%, Blackberry con el 9% Microsoft con el 2% entre otros2, Colombia ha tenido un crecimiento importante del 278% en adquisición de dispositivos móviles, tanto Android y iOS entre enero de 2012 a enero de 2013, pasando a ser el país líder que más rápido adopta el uso de teléfonos inteligentes3.

Los usuarios de estos dispositivos, han generado un aumento en el almacenamiento de sus datos en línea como el: 94% de información de contactos, 85.7% almacenamiento de mensajes SMS, 75.9% de almacenamiento de fotos personales, el 48.7% de correos electrónicos, el 31.7% de contraseñas y datos personales.

Como se puede observar, los usuarios de estos dispositivos móviles almacena y comparte su información en tiempo real posibilitando la sustracción de datos para robos y otros tipos de ataques.

Esto genera un interés en delincuentes y empresas que buscan adueñarse de esta información para lucro propio. Empresas de algunos países de Latinoamérica en sus procesos de contratación verifican la información de las personas publicada en Facebook y otras redes sociales para poder otorgar un cargo dentro de la compañía.

Gráfico 1. *Rápido crecimiento en el mercado con dispositivos iOS y Android*



Fuente: blog.flurry.com Análisis Enero 2012 a 2013

Frente a la creciente información almacenada y al presente mercado, han crecido proporcionalmente las acciones maliciosas. Entre los años 2010, 2011 y 2012 se han tenido un 40% de suscripciones a SMS, a servicios Premium donde el atacante busca que la víctima se suscriba de manera inadvertida y genere pagos legales. El 32% de los ataques convierten los dispositivos en zombis y un 28% de robo de información es por medio de spyware. A su

[2]Fuente GARTNER http://www.gartner.com/newsroom/id/2120015

[3]Fuente FLURRY http://blog.flurry.com/bid/94352/China-Knocks-Off-U-S-to-Become-Top-Smartphone-Tablet-Market

vez, se han creado una gran cantidad de firmas digitales que certifican el correcto funcionamiento de aplicaciones, garantizando la seguridad de las mismas. Aun así se han detectado dentro del código malicioso de las aplicaciones publicadas en google play, código malicioso que ha pasado por el equipo de seguridad de la empresa como también a las entidades que pagan para que analicen este código.

Como conclusión a los estudios realizados, podemos observar que el sistema operativo Android es la plataforma más utilizada en los presentes dispositivos móviles y abarca una importante cantidad del mercado internacional. Esto demuestra la necesidad de un sistema que garantice la seguridad de sus usuarios.

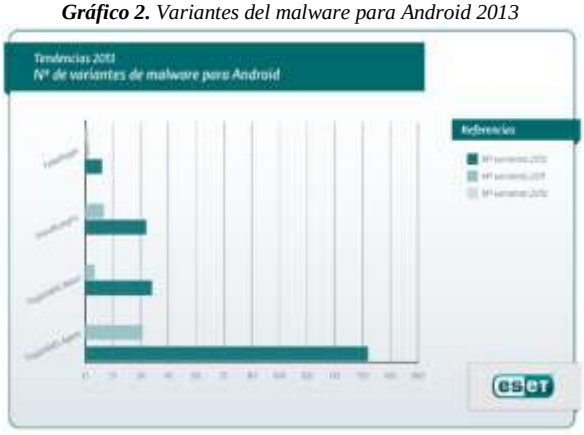
IV. MALWARE, TROJAN SMS EN SISTEMA OPERATIVO ANDROID

Puesto que el modelo de seguridad de Android es sencillo y basado en los estándares del sistema operativo Linux, las aplicaciones que se instalan, muestran una lista de acciones que pretenden efectuar (solicitud de permisos). El usuario tiene la opción de aprobar o rechazar dicha solicitud. La aprobación implementará las limitaciones declaradas y la cancelación bloqueará la instalación. A su vez, no es posible controlar los permisos tras la instalación ni durante la ejecución de la aplicación. Este modelo presenta las siguientes desventajas:

- El usuario toma la decisión de permitir o negar la instalación aceptando los permisos solicitados, donde la descripción de muchos permisos es confusa para los usuarios de los dispositivos incluso para los usuarios más avanzados.
- El sistema operativo permite por medio de la navegación web a cualquier destino sin un software de protección, que se ejecute código malicioso o sea direccionado a sitios en los cuales se puede ver vulnerada su seguridad.
- En ocasiones los programas realizan solicitudes de permisos incluso innecesarios, por lo que los usuarios se acostumbran a solicitudes anómalas y excesivas o en la mayoría de casos no son leídas ni tenidas en cuenta.
- El sistema operativo permite ejecutar código embebido en mensajes SMS.
- Existen casos en los que el usuario acepta cualquier permiso para poder ejecutar un programa y su entusiasmo puede ser aprovechado mediante métodos de ingeniería social.

Un informe de ESET (empresa eslovaca), declara el avance del malware en los dispositivos Android. En el mismo se muestra, una variación del desarrollo por parte de malware hacia trojan SMS que permite efectuar con mayor facilidad ataques orientados a Android.

Gráfico 2. *Variantes del malware para Android 2013*



Fuente: Laboratorio ESET Latinoamérica

A. *Modelo de seguridad Google Android*[4]

Google Ofrece una gran cantidad de aplicaciones y servicios para las diferentes versiones Android las cuales brindan: análisis, escaneo y verificación de los programas instalados junto con otros servicios de seguridad.

Dentro de las aplicaciones Android, se realiza la revisión del diseño donde se verifica toda la ingeniería y los recursos de seguridad a través de controles de seguridad apropiados integrados a la arquitectura del sistema. El equipo de seguridad de google, lleva adelante pruebas de penetración con consultores externos que a su vez evalúan el sistema y las aplicaciones. El equipo de Android realiza constantes exploraciones en busca de errores e incidentes, con el fin de poseer soluciones rápidas y efectivas a los problemas de seguridad que hoy se presentan.

Para lograr estos objetivos, Android proporciona estas características de seguridad clave:

- Seguridad robusta a nivel de sistema operativo a través del kernel Linux.
- Sandbox obligatoria para todas las aplicaciones
- Asegurar la comunicación entre procesos.
- Firma de aplicaciones.
- Permisos definidos por el usuario.

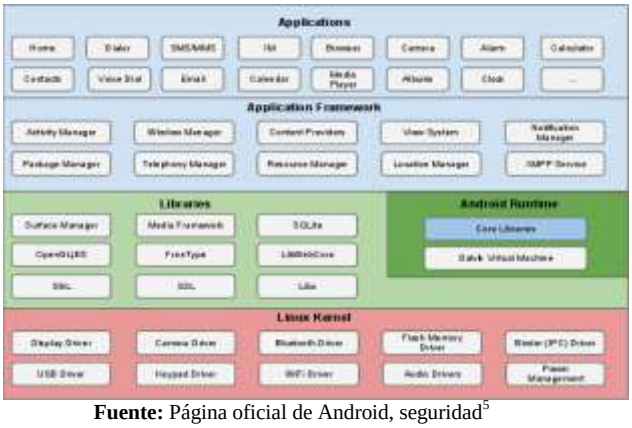


Figura 1. Modelo de Android

Fuente: Página oficial de Android, seguridad[5]

B. *La aplicación Sandbox*

La plataforma Android se aprovecha de la protección basada en el usuario Linux como un medio para identificar y aislar los recursos de aplicaciones. El sistema Android, asigna un ID de usuario único (UID) a cada aplicación y lo ejecuta como ese usuario en un proceso separado. Este enfoque es diferente de otros sistemas operativos (incluyendo la configuración de Linux tradicionales), donde múltiples aplicaciones se ejecutan con los mismos permisos de usuario.

Esto establece una aplicación Sandbox a nivel de kernel. El kernel aplica la seguridad entre las aplicaciones y el sistema en el nivel de proceso a través de las instalaciones de Linux estándar, como identificadores de usuario y grupo que se asignan. Por defecto, estas no pueden interactuar entre sí y poseen un acceso limitado al sistema operativo. Si una alguna intenta hacer algo malicioso con los datos de lectura de otra aplicación, a continuación, el sistema operativo protege contra esta operación porque la misma no posee privilegios de usuario correspondientes. El sandbox es simple, auditable, y está basada en la separación de usuario de los procesos y permisos de

[4] Fuente: http://source.android.com/tech/security/

[5] Fuente: http://source.android.com/tech/security/

archivo.

Desde que sandbox se encuentra en el kernel, este modelo de seguridad se extiende a código fuente y a las aplicaciones del sistema operativo. Todo el software que está por encima del kernel como se muestra en la Figura 1. Incluidas las bibliotecas del sistema operativo, el marco de aplicación, tiempo de ejecución de aplicaciones, todas se ejecutan desde sandbox. En algunas plataformas, los desarrolladores se ven obligados a un marco específico de desarrollo, un conjunto de APIs, o el lenguaje con el fin de reforzar la seguridad. En Android, no hay restricciones sobre cómo una aplicación puede escribirse para reforzar la seguridad, en este sentido, código nativo es tan seguro como código interpretado.

En algunos sistemas operativos, los errores de corrupción de memoria conducen generalmente a comprometer por completo la seguridad del dispositivo. Este no es el caso de Android, debido a todas las aplicaciones y sus recursos están en el nivel de seguridad del sistema operativo. Un error de corrupción de memoria sólo permitirá la ejecución de código arbitrario, con los permisos establecidos por el sistema operativo.

Al igual que todos los elementos de seguridad, sandbox no es irrompible. Sin embargo, al salir de él, en un dispositivo configurado correctamente, se puede poner en peligro la seguridad del kernel de Linux.

C. Escenario de análisis6.

A continuación, se relacionan los archivos y aplicaciones utilizadas las cuales fueron verificadas en el sitio web virus total y fueron probadas las diferentes herramientas de seguridad que hoy existen en un dispositivo Android.

Para las pruebas se utilizaron las siguientes aplicaciones de seguridad:

- Avast mobile security
- AVG antivirus
- Karpesky mobile security
- Lookout seguridad y antivirus
- Mckafee anivirus & security
- Norton antivirus y seguridad
- NQ security multi-language
- Sophos security
- Trusgo antivirus y seguridad movil
- Webroot secureanywhere
- Bitdefender Antivirus Free
- ESET Mobile Security
- GadgetTrak® Mobile Security

En comparación de las principales herramientas de seguridad se tuvieron en cuenta la calificación que les han dado los usuarios, las veces que se ha descargado, el tamaño descargado, el tamaño instalado y el tamaño que ocupa en ejecución.

Hasta el momento de la revisión, la aplicación más descargada es AVG antivirus con una cantidad mayor a 50 millones de descargas, seguido por Avast y lookout por una cantidad de 10 millones, donde se observa la importancia de avast entre los usuarios de Android.

Grafico 2. Aplicaciones de seguridad más descargadas

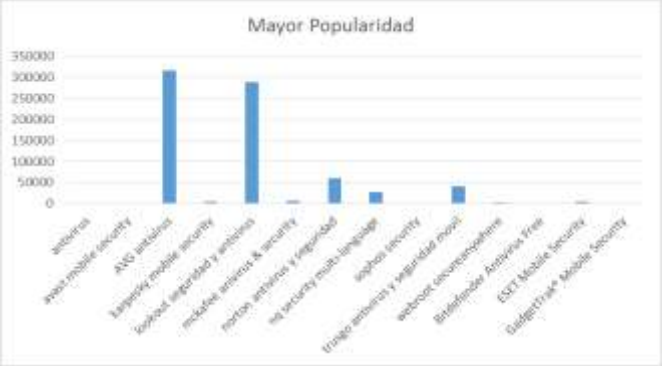
Fuente: autor

6

http://sunbeltsecurity.com/ThreatDisplay.aspx?name=Android.Adware.Wooboo&tid=4761567&cs=B2F819FEDE1090C937C7EE460C22A34E

A continuación verificamos la popularidad que han tenido las aplicaciones anteriormente mostradas.

Grafico 3. Aplicaciones de seguridad con mayor popularidad



Fuente: autor

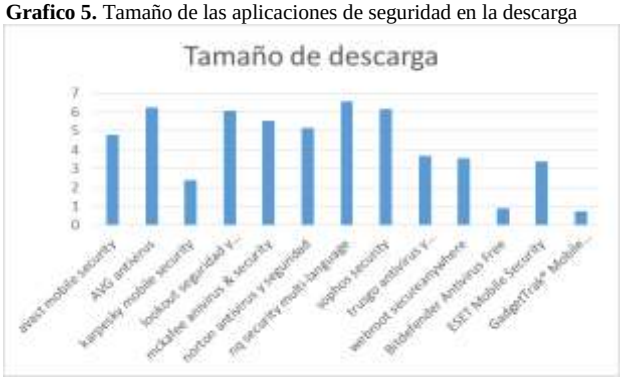
En consecuencia podemos observar, que AVG continúa liderando la votación de sus usuarios con una cantidad de trescientos mil usuarios seguido por Lookout con una cantidad de doscientos cincuenta mil usuarios votando afirmativamente, mientras que los demás antivirus no tienen una gran aceptación por los usuarios de google.

Grafico 4. Aplicaciones de seguridad con menor popularidad

Fuente: autor

Continuando con los niveles de popularidad, podemos observar en el grafico anterior que la aplicación con mayor votación en contra es Lookuot con catorce mil votos, seguido por AVG con diez mil votos mientras que las demás aplicaciones están por debajo de los cinco mil votos negativos.

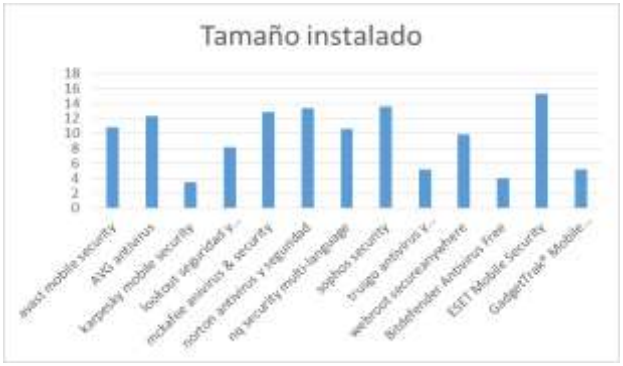
Grafico 5. Tamaño de las aplicaciones de seguridad en la descarga



Fuente: autor

Las aplicaciones evaluadas presentan un tamaño de descarga no superior a 7MB originalmente, pero el 36% tienen herramientas adicionales que se deben descargar por separado aumentando el tamaño en descarga, instalación y ejecución, donde posiblemente en dispositivos móviles anteriores pueden llegar a no funcionar adecuadamente.

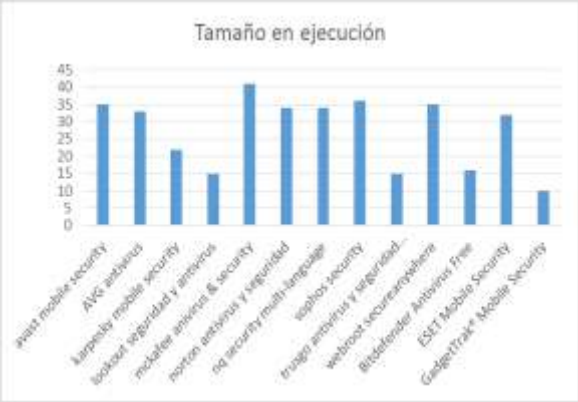
Grafico 6. Tamaño de las aplicaciones de seguridad cuando están instaladas



Fuente: autor

El tamaño instalado como se muestra en la gráfica anterior, no supera los 16MB lo cual hace que el usuario pueda seguir utilizando el almacenamiento interno si es necesario. Al igual que en el segmento anterior, las aplicaciones que tienen complementos, pueden llegar a ocupar un tamaño de 25MB, y no ocupan un tamaño mayor e ineficiente en un dispositivo Android.

Grafico 7. Tamaño de las aplicaciones de seguridad en ejecución.

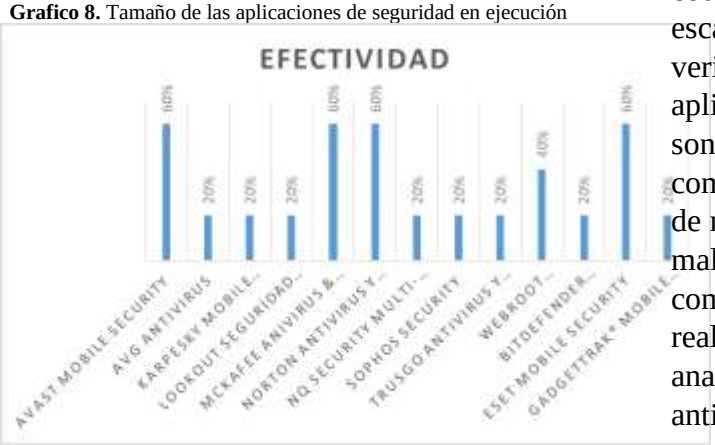


Fuente: autor

Los tamaños de ejecución observados, tomando como sistema base un dispositivo con memoria RAM de 512MB no llega a ocupar más del 9% y con los complementos pueden ocupar un 14% de ejecución y uso de la memoria RAM del sistema.

V. ANÁLISIS DE EFECTIVIDAD DE LAS HERRAMIENTAS ANTERIORMENTE MENCIONADAS

Grafico 8. Tamaño de las aplicaciones de seguridad en ejecución



Fuente: autor.

Frente a la evaluación de detección y análisis de archivos, aplicaciones y el sistema encontramos que el máximo de efectividad es del 60% puesto que no todas las aplicaciones tienen en sus bases de datos los mismos archivos y que para algunas de las aplicaciones no se realizan verificaciones de archivos comprimidos permitiendo el almacenamiento de archivos con códigos maliciosos y demás.

Figura 9. Listado de funcionalidades de las aplicaciones de seguridad

Controles de seguridad	Avast	AVG	aspersk	lookout	McAfee	Norton	NQ	Sophos	TrustGo	WebRoo	itdefend	ESET	adgetTra
Control flujo de datos entrada y salida	X												
control remoto	X									X			
Anti robo	X	X	X		X	X	X	X	X	X	X	X	X
Analisis y correccion de URL	X				X	X	X	X		X			
analisis de aplicaciones	X	X	X	X	X		X	X	X	X	X	X	
analisis web	X	X	X	X	X	X			X	X	X		
analisis de mensajes SMS, correo, QR	X	X	X	X	X	X		X	X	X			
analisis memoria y aplicaciones instaladas	X	X	X	X	X	X	X	X	X	X		X	
acceso remoto mediante SMS	X				X			X				X	
Analisis y caracteristicas de aplicaciones	X	X		X	X	X	X	X	X	X	X	X	
analisis de URL en cache Bloqueo USSD	X	X						X		X		X	
funciona cuando se ejecutan tareas	X												
cortafuegos, telefonos root, analisis de trafico de red	X												
aviso configuraciones no seguras de las aplicaciones		X			X	X							
proteccion de contactos		X	X		X								
analisis bajo demanda	X	X		X		X		X				X	
Bloqueo llamadas	X		X					X		X			
Bloqueo o informe de cambio de SIM						X		X		X			X
Backups							X		X				X

Fuente: autor

VI. CONCLUSIONES DEL ANÁLISIS DE LAS HERRAMIENTAS DE SEGURIDAD DE ANDROID.

Como conclusión no hay una herramienta que sea completa para los dispositivos Android, debido a que en algunos casos como se ha demostrado anteriormente no escanean los archivos comprimidos, lo que permite almacenar archivos con virus o código malicioso, los archivos de Android escaneados no son completamente verificados mientras que si verifican las aplicaciones instaladas. A su vez, no todas son completas debido a que necesitan complementos para poder prevenir ataques de malware, mensajes sms troyanos, códigos maliciosos, que se presentan continuamente como se ha observado en los estudios realizados anteriormente por empresas analistas y desarrolladoras de motores de antivirus.

VII. DISEÑO DE MODELO DE SEGURIDAD DE ANDROID

Siguiendo los problemas de seguridad que como muestra google la mayoría se deben a los usuarios, por descuido y los diferentes

tipos de ataques que se presentan en los dispositivos Android hemos realizado el diseño de un modelo de seguridad aprovechando las ventajas y desventajas de las presentes aplicaciones que actualmente hay en el mercado, sumando las técnicas de un sistema de detección de intrusos y según el comportamiento del sistema operativo.

A continuación y fomentando las practicas desarrolladas durante la especialización, presentamos el modelo de seguridad diseñado con el fin de optimizar la seguridad de los dispositivos basados en el sistema operativo Android, mejorando los errores que se pueden presentar por el descuido de los usuarios.

A. Agente de análisis del sistema

En esta parte del modelo, verificamos el estado actual del usuario administrador con el fin de detectar si el equipo ha sido modificado o desbloqueado para ejecutar funciones que únicamente puede realizar como administrador. Por parte en la comunicación del dispositivo, se establece el agente de análisis de datos entrantes y salientes para evitar que la información se desvíe, salga sin autorización, entre información que pueda alterar el sistema, etc. Por otro lado, verificará y realizará la detección de actualizaciones del sistema operativo.

B. Análisis y protección de aplicaciones

En este punto el modelo, actuaremos con la revisión de las aplicaciones al momento de ser instaladas y en su presente ejecución monitoreando los permisos que se le otorgan a las mismas, las actualizaciones de análisis de código de seguridad junto con la debida verificación de los certificados de aplicaciones generados para identificar y confirmar la integridad. Basados en estudios de comportamiento del uso del dispositivo, se planea ejecutar verificaciones en segundo plano de las aplicaciones y comportamientos de las mismas. Estas verificaciones, irán de la mano de los permisos que obtiene la aplicación y que en sugerencia por análisis de expertos no deberían tener permisos para modificarlos y optimizar la protección del usuario y su sistema.

C. Escaneo de archivos

Dentro del modelo se plantea, el escaneo de archivos del usuario soportados en un motor de antivirus con el fin de analizar todo tipo de archivo, verificando todas las posibilidades de almacenamiento de malware y analizando archivos comprimidos, evitando que se puedan almacenar archivos y aplicaciones maliciosas que no estén instaladas.

D. Guía de seguridad

Adicional al modelo, se propone una guía de seguridad con ejemplos y consejos para que el usuario tenga en cuenta en el uso de su dispositivo. Esta guía plantea ser visual y con pocas molestias al usuario, con el objetivo de que el mismo entienda, mejore y cambie los hábitos que pueden poner en peligro la información. Por otro lado, para ayudar a la confidencialidad del usuario y poder mejorar el uso de sus credenciales hacia sus aplicaciones, se expone una solución integral de administración donde el usuario pueda tener contraseñas de débiles pero que la aplicación genere contraseñas robustas y así poder proteger las diferentes cuentas que accede.

Todo este modelo de seguridad, se formula acompañado de una base de datos que contenga la información y reglas de seguridad principales para mantener el modelo. Así mismo, será alimentado por expertos en seguridad siendo el objetivo que alcance el uso mundial y gratuito, para que se pueda generar un sistema íntegro y de alta disponibilidad.

E. Centro de análisis y prevención

Basado en el modelo y arquitectura jerárquica de los desarrolladores de debían, a continuación diseñamos la arquitectura de la empresa para el análisis y aseguramiento de las aplicaciones de Android con la finalidad de salvaguardar a los usuarios en buscar de proteger la información y privacidad de mismo.

Este modelo se basa en tres niveles en los cuales se crea una arquitectura donde se analizaran las aplicaciones a fondo en busca de errores, código malicioso, modificaciones del sistema o comportamientos que puedan producir fallos de seguridad o del sistema operativo Android.

VIII. CONCLUSIONES

Los dispositivos Android están cada vez más presentes en el mercado, generando un amplio crecimiento de malware y ataques hacia los dispositivos y teniendo un gran éxito debido a que aprovechan las vulnerabilidades que puede llegar a tener el sistema operativo. Esto es, gracias a la intervención o modificación que puede realizar el usuario sobre el dispositivo móvil con el fin de mejorarlo, porque muchas veces los proveedores de los Smartphone no continúan desarrollando y optimizando el sistema para los equipos que venden en la actualidad, generando un nivel de obsolescencia a un tiempo corto por la cantidad de dispositivos móviles y versiones mejoradas que pueden distribuirse en un año.

Las diferentes aplicaciones de seguridad que se encuentran en el mercado, no son completas debido a que no realizan un análisis exhaustivo de los archivos que el usuario puede llegar a almacenar. En algunos casos los programas de seguridad, poseen sistemas de información muy completos que toman información de las aplicaciones instaladas pero no todas verifican correctamente, la compresión de archivos y no todas tienen una base de datos con las detecciones que han realizado otros sistemas, ya que se puede observar que cada aplicación detecta de manera diferente las amenazas encontradas.

Es necesario tener instalada una aplicación completa, que debería estar embebida en el sistema operativo o en su defecto que se permita instalar sencillamente, de fácil configuración y que le conceda al usuario liberarse de la seguridad del dispositivo. Esto se debe, a que en el momento de ejecutar nuevas y mejores aplicaciones para los dispositivos móviles, se pueden estar otorgando permisos que el usuario no lee o no entiende y deja a un lado permitiendo la vulneración del sistema. Esta aplicación debe estar constantemente actualizada, con una base de información única que permita detectar las amenazas de cualquier forma y no como las aplicaciones actuales, como se comentó anteriormente y se especifica en este documento.

El modelo de seguridad diseñado, es óptimo para su desarrollo buscando una mejora continua y basándose en diferentes problemáticas y herramientas aprendidas durante la especialización, mejorando considerablemente la seguridad de la plataforma Android. De esta manera, podría ser instalada en versiones anteriores asegurando que todos los dispositivos serian actualizados con el principal objetivo de certificar la seguridad de la información del usuario, posibilitando tener un dispositivo libre de ataques y daños originado por terceros.

REFERENCIAS

[1] HARDFIELD Dave, THOMAS Gavin, DIXON Danielle, PICKARD Anne, Android Tips, Tricks, Apps & Hacks volume 4, Londres Inglaterra, Imagine Publishing Ltd, Richmond House, 2012, sitio web: http://www.littlegreenrobot.co.uk

[2] OJA Dan, PARSONS June Damrich. "Conceptos de Computación: Nuevas Perspectivas", Cenage Learning Editores S.A. 2008, página 158.

[3] SIX Jeff, Application Security for the Android Platform, Estados Unidos, O'Reilly Media, Inc, 2012

[4] BETTS Andy, Android hacking goes mainstream, En: Android magazine. Vol. 23, Marzo 2013 p 8.

[5] BETTS Andy, Hacker Zone amazing android projects, En: Android magazine. Vol. 23, Marzo 2013 p 48-61.

BETTS Andy, Hacker Zone tips and tricks, En: Android Magazine. Vol. 24, Abril 2013, p 46-60

BETTS Andy, Hacker Zone tips and tricks, En: Android Magazine. Vol. 20, Enero 2013, p 62-69

ESET Laboratorio Latinoamérica, "Tendencias 2013: vertiginoso crecimiento de malware para móviles" {En línea}. {Noviembre 2012} disponible en: (http://www.eset-la.com/pdf/prensa/informe/tendencias_2013_vertiginoso_crecimiento_malware_moviles.pdf)

FARAGO Peter, "China Knocks Off U.S. to Become World's Top Smart Device Market", {En linea} {Lunes 18 de febrero 2013}, disponible en: (http://blog.flurry.com/bid/94352/China-Knocks-Off-U-S-to-Become-Top-Smartphone-Tablet-Market)

[6] PHONE USERS 19, "Android Jelly Bean", DALAGA S.A., Buenos Aires, Argentina Viernes, 15 de febrero de 2013, sitio web: http://www.redusers.com

[7] PHONE USERS 21, "Hackear Android", DALAGA S.A., Buenos Aires, Argentina, Jueves, 11 de abril de 2013, sitio web: http://www.redusers.com

Autores:

Ingenieros de Sistemas. En proceso final de obtener el título de la Especialización de Seguridad Informática en la Universidad Piloto de Colombia