Universidad de Costa Rica

Escuela de Ciencias de la Computación e Informática

Sistemas Operativos

Profesor:

Diego Villalba

Tema:

“Seguridad en el Sistema Operativo Android”

Estudiante:

Esteban Solís
A96097

II Semestre
2013

Introducción

Debido a la gran cantidad de usuarios con los que cuenta, el sistema operativo Android se ha convertido en uno de los principales blancos de ataques contra la seguridad, por lo cual en este trabajo se investigará cómo funciona la seguridad de dicho sistema, además de diferentes formas en las que ha sido atacado, la forma de defenderse antes estos ataques, la evolución en dichos ataques, así como las mejoras que se han hecho para su protección, los pasos para realizar una copia de seguridad y por último; sus ventajas y desventajas con su competidor más fuerte del mercado: el sistema operativo de Apple iOS, así como la forma que utilizan principalmente para defenderse de los ataques.

El modelo de seguridad de Android presenta tres aspectos principales:

1-Permisos: las aplicaciones requieren algunos permisos para acceder a ciertos recursos del sistema, los cuales son mostrados al usuario al momento de la instalación para que el usuario decida si continuar o no. Las aplicaciones vienen por defecto sin permisos. Algunos ejemplos son:

•ACCESS_COARSE_LOCATION: permite acceder a la ubicación de red WI-FI y móvil.

•CAMERA: permite acceder a la cámara.

•INTERNET: permite solicitudes de red.

•WRITE_EXTERNAL_STORAGE: permite escribir en la tarjeta de memoria.

2-Firmas de la aplicación: todas las aplicaciones para plataforma Android deben ser firmadas.

3-IDs de usuario de la aplicación: como en Linux, Android asigna un ID de usuario a cada aplicación instalada para determinar sus permisos.

[Adobe Flash Platform, Seguridad en dispositivos Android].

Primero se va a explicar como trabaja la seguridad en Android, para ello debemos saber que Android consiste en una infraestructura de aplicaciones, bibliotecas de las mismas y una máquina virtual Dalvik con compilación en tiempo de ejecución, todo esto funcionando sobre un kernel de Linux. Android tiene una serie de servicios de sistemas operativos, como lo son la gestión de procesos y memoria, una pila de red, controladores, una capa de abstracción de hardware y por supuesto dispositivos de seguridad, esto gracias a los beneficios que brinda su kernel.
Recintos de seguridad: sirven para ejecutar la separación y permisos de comunicación entre aplicaciones para procesar las solicitudes de acceso de una aplicación a los recursos del dispositivo. Aprovecha las facilidades de Linux como la seguridad a nivel de procesos, los ID de usuario y permisos para ejecutar ciertas aplicaciones. A diferencia de Linux, Android asocia un ID de usuario a una aplicación, en vez de a un usuario específico.

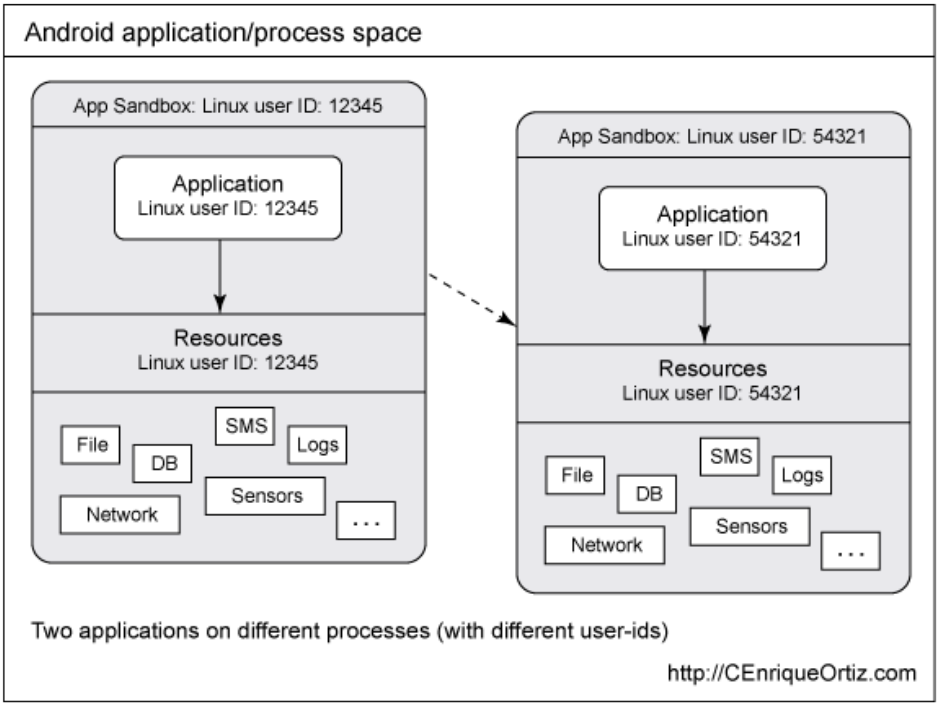


Imagen 1. Recintos de seguridad en dos diferentes aplicaciones de Android.

Cada aplicación de Android se ejecuta en su correspondiente proceso de Linux y tiene un ID único. Estas aplicaciones se ejecutan sin tener permisos asignados, con lo cual no tienen acceso a los recursos del sistema, pero pueden realizar solicitudes de permisos para poder acceder a los recursos que el sistema autorice.
Un mismo proceso puede ejecutar varias aplicaciones distintas.

Firma de la aplicación: asignar una clave privada a una aplicación principalmente para poder identificarla y así saber quién la hizo y si se ha modificado, así como comunicarse con otras aplicaciones. En Android, todas las aplicaciones deben estar firmadas. Si distintas aplicaciones poseen las misma firma, pueden otorgarse permisos entre ellas de acceso a APIs basadas en firmas y si comparten el mismo ID, pueden acceder al código y datos de ambas.

Permisos: se usan para aceptar o negar el acceso a las API y determinados recursos. Son solicitados por las aplicaciones y la respuesta a las solicitudes se dan durante la instalación. La forma de solicitarlos es mediante el atributo <user-permission>:
<uses-permission android:name="string" />
android:name indica el nombre del permiso solicitado.
[Ortiz, Enrique. IBM. Cómo comprender la seguridad en Android]

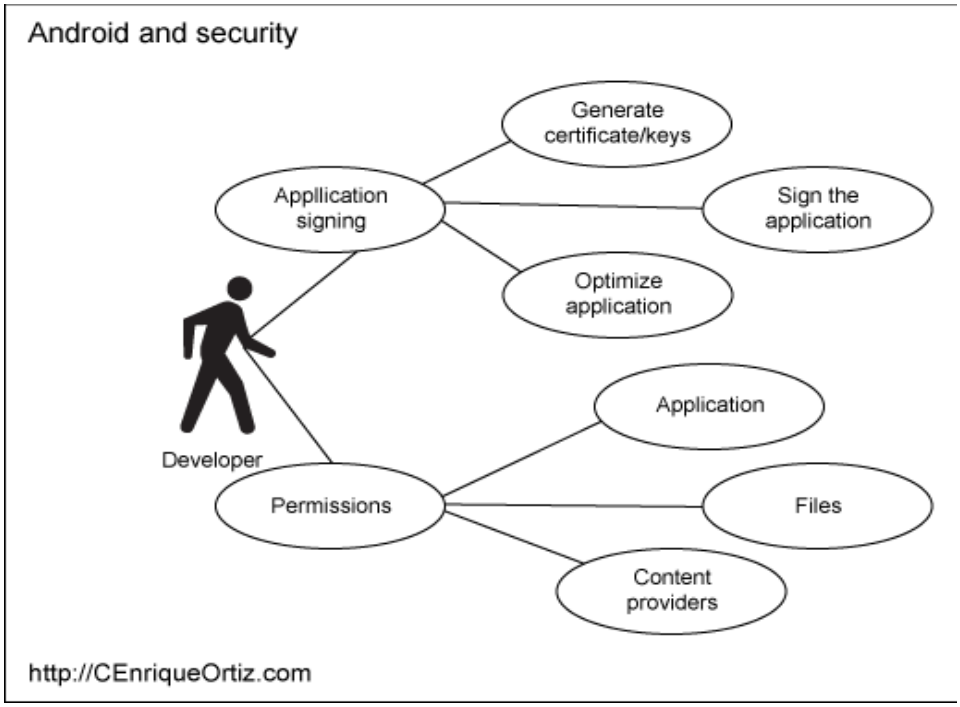


Imagen 2. Zonas de seguridad en la programación de aplicaciones Android.

Capas de seguridad

Android se defiende de las críticas a su seguridad sacando a la luz el mecanismo de defensa interna del sistema operativo, que según miembros de Apple es prácticamente impenetrable, la cual se divide en varias capas de seguridad como se detalla en la siguiente imagen:

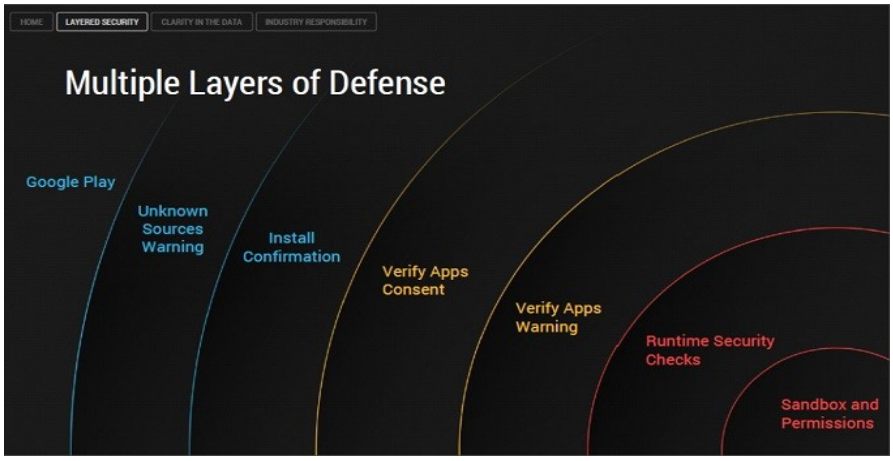
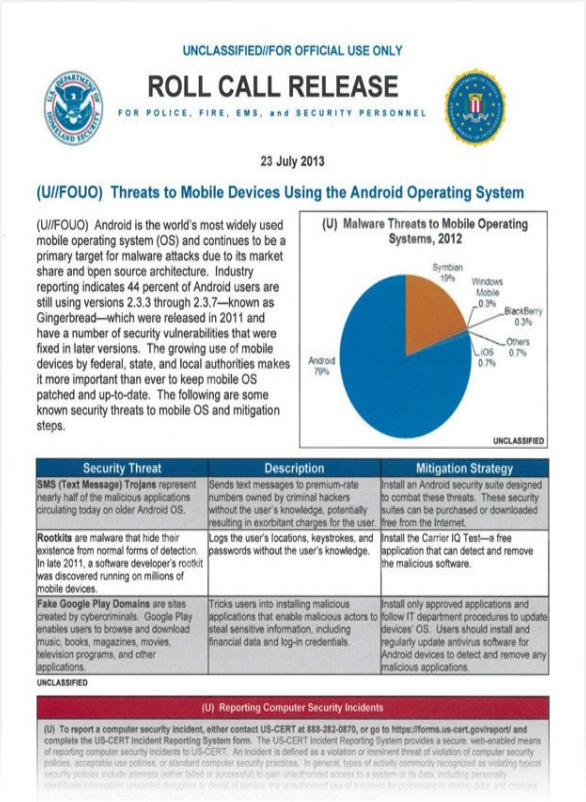


Imagen 3 . Diferentes capas se defensa en Android.
Ataques en Android

Los ataques ha Android han sido tantos y tan frecuentes que incluso el mismo gobierno de los Estados Unidos ha procedido a emitir una advertencia sobre los riesgos en la seguridad que se corren al utilizar dicho sistema operativo. Se informa que el 79% del software malicioso destinado a dispositivos móviles va dirigido a aquellos que utilizan Android.
[Michan, Miguel. APPLESFERA. El gobierno estadounidense advierte acerca del malware para Android]



UNCLASSIFIED//FOR OFFICIAL USE ONLY

ROLL CALL RELEASE

FOR POLICE, FIRE, EMS, and SECURITY PERSONNEL

23 July 2013

(U//FOUO) Threats to Mobile Devices Using the Android Operating System

(U//FOUO) Android is the world's most widely used mobile operating system (OS) and continues to be a primary target for malware attacks due to its market share and open source architecture. Industry reporting indicates 44 percent of Android users are still using versions 2.3.3 through 2.3.7—known as Gingerbread—which were released in 2011 and have a number of security vulnerabilities that were fixed in later versions. The growing use of mobile devices by federal, state, and local authorities makes it more important than ever to keep mobile OS patched and up-to-date. The following are some known security threats to mobile OS and mitigation steps.

(U) Malware Threats to Mobile Operating Systems, 2012

UNCLASSIFIED

Security Threat	Description	Mitigation Strategy
SMS (Text Message) Trojans represent nearly half of the malicious applications circulating today on older Android OS.	Sends text messages to premium-rate numbers owned by criminal hackers without the user's knowledge, potentially resulting in exorbitant charges for the user.	Install an Android security suite designed to combat these threats. These security suites can be purchased or downloaded free from the Internet.
Rootkits are malware that hide their existence from normal forms of detection. In late 2011, a software developer's rootkit was discovered running on millions of mobile devices.	Logs the user's locations, keystrokes, and passwords without the user's knowledge.	Install the Carrier IQ Test—a free application that can detect and remove the malicious software.
Fake Google Play Domains are sites created by cybercriminals. Google Play enables users to browse and download music, books, magazines, movies, television programs, and other applications.	Tricks users into installing malicious applications that enable malicious actors to steal sensitive information, including financial data and log-in credentials.	Install only approved applications and follow IT department procedures to update devices' OS. Users should install and regularly update antivirus software for Android devices to detect and remove any malicious applications.

UNCLASSIFIED

(U) Reporting Computer Security Incidents

(U) To report a computer security incident, either contact US-CERT at 888-282-0870, or go to https://forms.us-cert.gov/report/ and complete the US-CERT Incident Reporting System form. The US-CERT Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to US-CERT. An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In general, types of activity commonly recognized as violating typical security policies include attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally

Imagen 4. Comunicado del gobierno

Sumado a esto, el director de investigación de Trend Micro, empresa dedicada al desarrollo de software y servicios de seguridad, Rik Ferguson, duda sobre la seguridad de este sistema, ya que según indican en Google, la cantidad de aplicaciones que logran penetrar las capas de seguridad en Android es prácticamente despreciable. Según Ferguson, esto sería impresionante, dado el gran uso que recibe dicho sistema operativo y la gran cantidad de ataques que recibe. Dice también que en la empresa a la cual pertenece se han analizado cerca de 3700000 aplicaciones y actualizaciones, de las cuales, se estima que el 18% son directamente dañinas, el 13% son consideradas de alto riesgo. Casi la mitad de las aplicaciones dañinas fueron tomadas de Google Play.
Afirma que, a pesar de las capas de seguridad que tiene Android, varias de estas quedan en manos del usuario y dado que este muchas veces no lee la información que brinda la aplicación al momento de la instalación o no entiende realmente el riesgo que podría implicar dicha aplicación, pueden burlarse varias capas de defensa.
[Diario Ti, Rik Ferguson, director de investigación en Trend Micro, cuestiona la seguridad de Android].

Evolución del malware en dispositivos móviles

El desarrollo de malware a venido en aumento principalmente en dispositivos que utilizan Android, en gran parte debido al poco conocimiento que tienen los usuarios sobre temas relacionados a la seguridad.
Los desarrolladores de malware se han aprovechado de aplicaciones tan comunes como el simple juego "Snake", tradicional desde los primeros dispositivos móviles, para acceder la localización del dispositivo. Una versión de este juego llamada Top Snake fue el primer caso de malware detectado por la empresa Symantec. Dicha versión se encontraba como una aplicación legítima en el market de Google, pero extrañamente dentro de los permisos que solicitaba se encontraban ACCESS_COARSE_LOCATION y ACCESS_FINE_LOCATION; con los cuales se tendría acceso a la localización del dispositivo, lo cual es evidentemente innecesario para dicha aplicación.

También tenemos el primer caso que tuvo un efecto considerable para los usuarios de Android, el Fake Player, el cual es supuesto un reproductor multimedia pero dicha funcionalidad no se encontraba en el código. Entre sus permisos se encontraba SEND_SMS, con lo cual enviar mensajes de texto a números especiales.

Con el caso Geinimi, cambió el esquema referente al malware hasta ese momento. Se valía de aplicaciones legítimas para distribuirlas por markets ilegales infectando el código. Entre sus permisos se encontraban: CALL_PHONE, SEND_SMS, READ_CONTACTS, WRITE_SMS y RECEIVE_SMS. Fue el primer caso de ofuscación de código. Enviaba información privada a direcciones web.

HongTouTou
Se infectaba de la misma manera que Geimini. Solicitaba permisos tales como: **WRITE_APN_SETTINGS, RECEIVE_BOOT_COMPLETED, ACCESS_NETWORK_STATE, READ_PHONE_STATE, WRITE_EXTERNAL_STORAGE e INTERNET, MODIFY_PHONE_STATE.** Se usaba para enviar ciertos datos privados a un servidor remoto.
[Guerrero, Sebastián. Security by default. Evolución del malware en dispositivos Android].

Seguridad Android versus seguridad iOS

Hay diferentes versiones sobre cual de los dos sistemas es más vulnerable a los ataques, veremos algunas de ellas. Lo que si está claro es que ambos tienen sus riesgos pero el sistema operativo de Google es mucho más atacado por software malintencionado que el de Apple.
En iOS, una aplicación no puede buscar, ver o modificar códigos o datos de otra, con lo cual, las aplicaciones no pueden acceder al núcleo o a los recursos sensibles del dispositivo. En cambio, en Android, aunque las aplicaciones no pueden verse o modificarse entre ellas, sí pueden examinar sus códigos y compartir acceso a dispositivos externos.
En cuanto a la administración de riesgos, en iOS es más difícil el abuso por parte del malware, pero ambas plataformas son vulnerables a los ataques vía navegador. Desde el punto de vista de reducción de riesgos, Android es más flexible, ya que los escáneres antimalware pueden detectar aplicaciones maliciosas en Android pero no en iOS.

Controles de seguridad
Ambos sistemas soportan los controles de seguridad que piden las empresas. También la limpieza remota pero no se implementa de igual manera ni es igualmente eficaz. En iOS se eliminan las aplicaciones instaladas por medio de un sistema de administración de dispositivos móviles y deja intacto todo lo demás. En Android, se requiere una aplicación externa y se puede limpiar ya sea todo el dispositivo o sólo cierta parte. Se es total, se resetea el dispositivo y dejará los ajustes de fábrica.
Las dos plataformas pueden usar encriptación para proteger los datos.
La principal diferencia en seguridad que tienen es el control que tienen con las aplicaciones de usuario; mientras Apple tiene fuertes controles y exigencias de aprobación y de certificados emitidos por ellos mismos. En cambio Google es más abierto en ese sentido, dando mayores facilidades a los desarrolladores, además de poder conseguir aplicaciones en otros sitios.
Esta diferencia es la que ha hecho que los dispositivos que utilizan iOS no hayan sido atacados de la forma en que ha pasado con los que usan Android, lo que ha hecho que Google tome acciones al respecto y tome controles para sacar el malware de su sitio, pero aún así sigue siendo el blanco de los ataques.
[Phifer, Lisa. Search data center. Android vs iOS: características, políticas y controles de seguridad].

Además, el mayor número de usuarios en Android ha influído para que suceda esto.

También están quienes consideran que es más seguro el sistema operativo Android por sus ya conocidas capas de seguridad, con las cuales se dice que dificulta en gran medida que un proceso pueda adquirir los permisos que necesita. Se argumenta además que lo inseguro no es el sistema, sino los usuarios de dicho sistema, ya que la mayoría de los casos de ataques se ha dado porque los usuarios no toman las precauciones necesarias de seguridad, ya sea asignando permisos a aplicaciones que no son confiables o descargándolas desde sitios no conocidos.
Dicen además que lo que da seguridad en el iOS es simplemente que en Android se pueden quitar las medidas de seguridad cuando se desee, mientras que en el primero no, pero que si las condiciones fueran las mismas, Android sería igual o inclusive más seguro.
[PC actual, Android es más seguro que iPhone].

Conclusión

El mayor riesgo en la seguridad de cualquier sistema operativo es el usuario, en Android este tiene muchas libertades para manejar la seguridad y puede toma muchas decisiones importantes, lo que hace que sea más fácil de vulnerar que un sistema como iOS, que ejerce mucho más control y no da esa libertad a los usuarios. Por otra parte, Android viene ejerciendo nuevas prácticas para impedir que aplicaciones dañinas o malintencionadas lleguen a su sitio, así como para eliminar las que se encuentren, por lo que se espera que esa mayor vulnerabilidad vaya disminuyendo. Por otra parte, se dificulta un poco saber realmente que tan seguro es iOS interiormente, ya que sabemos que ha sido muy difícil poder atacarle pero probablemente sea por su control con las aplicaciones, en cambio con Android se ha abordado más el asunto y hemos visto como se divide el control de la seguridad internamente y como este ha funcionado de nuena manera.

También se dan muchas críticas a Android por los constantes ataques que recibe, por lo cual es todo un reto a futuro que tienen los desarrolladores de dicho sistema para lograr que Android pueda ser reconocido como un sistema realmente seguro.

Se recomienda leer cuidadosamente cuando se va a instalar cualquier aplicación, en vez de dar “siguiente” sin siquiera haber leído los permisos que requiere la aplicación y esto protegerá en gran medida los dispositivos contra los ataques de malware.

Bibliografía

Adobe Flash Platform, Seguridad en dispositivos Android. Disponible en: http://help.adobe.com/es_ES/as3/dev/WSfffb011ac560372f-10359c2612b317e3655-8000.html.

Diario Ti, Rik Ferguson, director de investigación en Trend Micro, cuestiona la seguridad de Android. Disponible en: http://help.adobe.com/es_ES/as3/dev/WSfffb011ac560372f-10359c2612b317e3655-8000.html]http://diarioti.com/rik-ferguson-director-de-investigacion-en-trend-micro-cuestiona-la-seguridad-de-android/69724.

Guerrero, Sebastián. Security by default. Evolución del malware en dispositivos Android. 28 de febrero de 2011. Disponible en: http://www.securitybydefault.com/2011/02/evolucion-del-malware-en-dispositivos.html.

Michan, Miguel. APPLESFERA. El gobierno estadounidense advierte acerca del malware para Android. 28 de agosto de 2013. Disponible en: http://www.applesfera.com/iphone/el-gobierno-estadounidense-advierte-acerca-del-malware-para-android-con-un-79-de-amenazas-frente-al-0-7-registrado-por-ios.

Ortiz, Enrique. IBM. Cómo comprender la seguridad en Android. 4 de febrero de 2013. Disponible en: http://www.ibm.com/developerworks/ssa/library/x-androidsecurity/.

PC actual, Android es más seguro que iPhone. Disponible en: http://www.pcactual.com/articulo/actualidad/reportajes/13558/android_mas_seguro_que_iphone.html.

Phifer, Lisa. Search data center. Android vs iOS: características, políticas y controles de seguridad. Junio de 2012. Disponible en: http://searchdatacenter.techtarget.com/es/consejo/Android-vs-iOS-caracteristicas-politicas-y-controles-de-seguridad#content.