Mecanismo de actualizaciones de Android vs SO de escritorio

Dedicado a la seguridad informática, no pude resistir mucho tiempo después de comprar mi primer smartphone basado en Android y comenzar a investigar cómo funcionan las actualizaciones de dicho sistema operativo y, debo decir, estoy sorprendido.

Autor: Raúl Batista
Versión: 1.01 (20110522)
Publicado: http://www.segu-info.com.ar/articulos/

Introducción

Usualmente con una PC con Windows, Linux o un Mac OS, cuando se libran correcciones para el propio sistema operativo que solucionan vulnerabilidades de seguridad, el equipo las descarga de forma automática, a través de un administrador o, si se prefiere, en forma manual. Los denominados "parches" corrigen esos “agujeros” que suelen aprovechar los atacantes, mediante la utilización de *exploits* o malware, para comprometer el sistema pero, sobre todo, la información.

El modelo de actualización de parches para Android es distinto: **hay intermediarios**. Llegué a esta conclusión, preliminar por cierto, luego de recolectar distinto tipo de información sobre el modelo de actualizaciones y, finalmente decidí consultar al reconocido especialista en seguridad de la información Ezequiel Sallis, Director Director de Investigación y Desarrollo de la empresa Root-Secure [1].

Preguntas y respuestas

Pregunta: A raíz de charlas con algunos compañeros de trabajo (personal de sistemas) usuarios de Android y de esta noticia publicada en Hispasec [2], surgen algunas dudas en como son las correcciones de las vulnerabilidades, los parches, del SO Android. Las correcciones / parches de seguridad ¿solo los hace Google?

Ezequiel Sallis: La respuesta es **sí**, oficialmente Google libera nuevas versiones del SO con correcciones de seguridad, bugs y nuevas funcionalidades, independientemente de esto, al ser un SO de código abierto alguien con conocimiento podría realizar modificaciones no oficiales y solucionar problemas de seguridad, aunque hasta ahora por lo menos que yo sepa no ha sucedido.

P: ¿Se liberan parches individuales que se aplican al SO o siempre liberan una versión actualizada de todo el SO Android (ej. 2.2 a 2.2.1)?

ES: No, no se liberan parches por separado, siempre están incluidos en las nuevas versiones de los SO, tal y como mencionas en el ejemplo de la pregunta.

P: Una vez que hay un parche de seguridad, ¿se actualiza automáticamente en el teléfono? o ¿se debe hacer manualmente?

Para que pueda ser utilizado, el parche ¿debe pasar de Google al fabricante del teléfono celular?, ¿a la compañía telefónica?, ¿directamente puede descargarse desde Google? O ¿Google realizar *push* sobre el teléfono?

Según esa noticia que comento antes, el parche o actualización pasa de Google al fabricante y de allí al usuario, cuando el fabricante lo decida.

ES: La liberación del SO está a cargo de Google. Luego de esto cada fabricante puede tomarlo y enviarlo a los teléfonos OTA (Over the Air) o, a través de software propietario de cada fabricante, como por ejemplo KIES de Samsung [3], una aplicación de escritorio que se encarga de las actualizaciones y otras actividades de los teléfonos y Tablet Samsung con Android.

P: Al parecer, los fabricantes no liberan las nuevas versiones de Android para todos los modelos de aparatos, entonces ¿muchos aparatos van quedando con cada vez más vulnerabilidades sin solucionar?

ES: Efectivamente, esta acción tiene que ver con los temas de fragmentación, ya que por diferentes razones (hardware, argumentos comerciales, y otros) los fabricantes deciden muchas veces que un modelo *X* no recibirá la actualización de la próxima versión de Android. Esto representa un gran problema ya que muchos teléfonos están condenados de por vida, salvo que el dueño decida bajar la actualización de un foro especializado y lo instale bajo su propia responsabilidad.

En la última conferencia de Google I/O [4] la semana pasada los fabricantes se comprometieron con Google a brindar una ventana de tiempo de 18 meses [5] por lo menos, lo que es mejor de lo que había hasta el momento, que era bastante anárquico.

También en la última Google I/O decidieron sacar una nueva versión (sin fecha aún) que unirá a Android para *tablets* y para *smartphones,* en vez de tener un SO para cada uno como hasta el momento.

En este anuncio oficial se puede ver la distribución de la fragmentación a la fecha [6]. Por ejemplo, última versión que es la 2.3.3 la tiene solo el 3% de instalación. No confundir con la 3.0 (ya disponible la 3.1), que sólo se encuentra disponible para *tablets*.

P: Respecto de la actualización OTA, ¿la hace el operador de telefonía a partir del paquete que obtenga del fabricante? o ¿directamente el fabricante instala la actualización OTA?

ES: El flujo es el siguiente, Google libera la nueva versión del SO, y se lo envía a los fabricantes (Samsung, HTC, Motorola y otros), los cuales le cargan paquetes de software extras personalizados (interfaces de escritorio y demás), para luego liberarlos a las operadoras de

telefonía celular, que son las responsables de enviar a los dispositivos de los usuario, vía OTA, la misma. Esto último se hace por país y por operadora y es anárquico. Además a esto hay que sumarle que si el fabricante decide no dar la nueva versión a los equipos, las operadora ni siquiera pueden tener la opción de decidir, como por ejemplo en esta decisión de Motorola [7].

P: Entonces, en comparación con el modelo de actualizaciones de parches de seguridad en escritorios de los SO Windows / Linux / MacOS, y el modelo de Android ¿que opinión te merece el modelo de Android, en la práctica? porque, en principio parecería defectuoso o con fallas como la reciente de "el protocolo que usa ClientLogin con Google" donde Javier Rascon de Hispasec dice (subrayo):

> *Este fallo de seguridad está presente en Android 2.3.3 y versiones anteriores. Google ha subsanado el error en la versión 2.3.4, por lo que sería recomendable actualizar a esta versión. Sin embargo, el principal problema ahora es que los usuarios de Android actualicen realmente su versión para no ser vulnerables. Esta responsabilidad suele dejarse en manos del fabricante del terminal, que personaliza las versiones del sistema operativo. Por tanto, es necesario estar al tanto de la actualización de cada fabricante de teléfonos y esto podría demorarse un tiempo indefinido.*
>
> *Mientras tanto, se recomienda no usar Android en redes inalámbricas no cifradas o en las que no se confíe.*

… ¿No dejan demasiados móviles a merced de quien quiera entretenerse explotándolos con vulnerabilidades conocidas?

ES: Exactamente, es un modelo que está afectado por la fragmentación, no solo por las nuevas funcionalidades (que es lo que la mayoría de los usuario quiere) sino también por los aspectos de seguridad, tal cual como comentas.

P: No será que estoy muy apegado a pensar como con la PC, que si me faltan 3 meses de parches y 2 actualizaciones de Adobe Reader y Flash siento que estoy en serio riesgo.

ES: Esto es así, el modelo debería ser el de PC, ya que las amenazas de seguridad son muy similares y están migrando poco a poco a los dispositivos móviles, seguramente se deban que realizar cambios en un futuro ya que este modelo no resistirá demasiado

P: Para finalizar, te pido que analices el siguiente este esquema y verifiques si es correcto:

Parches SO de PCs línea de tiempo – participantes (p)

Dia 0 → Vulnerabilidad descubierta

Día a → Fabricante.SO(p1) de SO decide hacer parche y lo hace

Día a + n → Fabricante.SO(p1) publica parche

Día a + n + 1 → Usuario.SO(p2) sistema del usuario en modo automático se actualiza.

Parches SO Android

Día 0 → Vulnerabilidad descubierta

Día a → Fabricante.Android(p1) de SO decide hacer parche y lo hace.

Dia n → Fabricante.Android(p1) publica nueva versión de SO c/parche.

Día n + x → Fabricante.Teléfono(p2) adapta la nueva versión de SO emparchada y lo publica

Día n + x + y → Operador.Telefono.Celular(p3) envía al usuario por OTA el SO emparchado

Día n + x + y + 1 → Usuario(p) PC en modo automático se actualiza

Dónde:

A = cantidad de días que tomo el fabricante para decidir solucionar una vulnerabilidad.

N = a + cantidad de días para preparar y liberar parche

x = días que demora el fabricante de celular en adaptar el parche

y = días que demora el operador de telefonía en disponer la actualización mediante OTA

Resumiendo

En SO tradicional:

- Existen sólo 2 participantes: fabricante y usuario.
- la demora, fuera de control del usuario, es la del fabricante para decidir y producir el parche
- se produce el parche para todas las versiones con soporte vigente

En SO Android:

- Existen cuatro participantes: fabricanteOS, FabricanteCelular, OperadorCelular, usuario
- la demora, no administrable por el usuario, es la suma de la demora de fabricanteSO, de fabricanteCelular y de operadorCelular
- cualquier participante que decida no actuar interrumpe la posible solución de la vulnerabilidad
- se producen soluciones a vulnerabilidades para versiones nuevas y se dejan abandonadas versiones anteriores.

ES: Sublime, excelente análisis que deberíamos comenzar a utilizar todos.

Declaraciones del fabricante

Finalmente encontramos una FAQ en el sitio Android.Developers estas declaraciones [8] que oficialmente explican el tema:

¿Cómo recibirán los arreglos de seguridad los dispositivos basados en Android?

El fabricante de cada dispositivo es responsable de distribuir las actualizaciones para este, incluyendo los arreglos de seguridad. Muchos dispositivos se actualizarán por sí mismos con software que se descarga "Over the Tir" (de forma inalámbrica), mientras que otros dispositivos necesitan que el usuario los actualice manualmente. Cuando los dispositivos basados en Android estén disponibles públicamente, esta FAQ proveerá los enlaces a como los miembros de la Open Handset Alliance publicarán las actualizaciones.

¿Puedo obtener un parche directamente del Proyecto de Plataforma Android?

Android es una plataforma móvil que será liberada como Open Source y disponible en forma gratuita para que la use cualquiera. Esto significa que habrá muchos dispositivos basados en Android disponibles para los consumidores, y la mayoría de ellos serán creados sin el conocimiento o participación del Android Open Source Project. Como los que mantienen otros proyectos Open Source, no podemos crear y liberar parches para el ecosistema completo de los productos que usan Android. En lugar de eso, trabajaremos diligentemente para encontrar y reparar las fallas tan pronto como sea posible y distribuir esos arreglos a los fabricantes de los productos.

Además, agregaremos los arreglos de seguridad a la distribución Open Source de Android y haremos público los cambios en el grupo android-security-announce [9].

Conclusiones

Los sistemas operativos de los móviles inteligentes, *smartphones*, son un gran avance en la simplificación del uso de estas pequeñas computadoras bolsillo. Están en el camino correcto para llegar al público masivo. Quizás de este sector provenga la necesaria simplificación del uso que nunca llegó a las de escritorio.

Pero en el caso analizado del Android OS, las actualizaciones de seguridad representan un paso atrás respecto de la madurez y eficacia conseguidas, después de muchos años, en los sistemas operativos de las escritorio, todos ellos, Windows, Linux y Mac OS.

El mecanismo de actualizaciones de Android debería madurar hacia una reducción de intermediarios y/o garantizarse mayor velocidad y menos discrecionalidad. Deberían tener actualizaciones todos los dispositivos durante un tiempo respetable, mayor al actual.

Mientras tanto lo que cualquier usuario de un celular basado en Android debiera saber es que las fallas de seguridad no necesariamente se corregirán para su modelo de celular, ni tampoco estarán disponibles tan pronto Google la haya corregido. Por ello es que para permanecer seguro uno debiera mantenerse informado respecto de lo que pasa con su modelo, como está afectado por las vulnerabilidades. Incluso saber que debe necesariamente instalar el programa de escritorio para obtener las actualizaciones, en caso que el operador de celular no las envíe OTA.

Agradecimiento

Agradecemos especialmente a Ezequiel Sallis su inmediata y gentil colaboración, sin la cual este artículo no hubiera sido posible.

Referencias

[1] Root-Secure

http://www.root-secure.com

[2] Robo de credenciales en Android [Hispasec]

http://www.hispasec.com/unaaldia/4588/robo-credenciales-android

[3] Kies Samsung

http://www.celularis.com/noticias/samsung-kies-actualizar-android-galaxy-s.php

[4] Google I/O 2011

http://www.google.com/events/io/2011/

[5] Fragmentación

http://appleweblog.com/2011/05/ios-vs-android-fragmentacion

[6] Fragmentación, información oficial:

http://developer.android.com/resources/dashboard/platform-versions.html

[7] Motorola:

https://supportforums.motorola.com/community/manager/softwareupgrades

[8] Android Develovpers FAQ Security

http://developer.android.com/resources/faq/security.html

[9] Android Security Discussions

http://groups.google.com/group/android-security-discuss

[10] Android Security Announces

http://groups.google.com/group/android-security-announce