Uso de dispositivos móviles y BYOD: Su impacto en la seguridad

Lic. Nicolás Macia - Lic. Einar Lanfranco - Lic. Paula Venosa - Lic. Alejandro Sabolansky
A.P.U. Carlos Damián Piazza Orlando - A.P.U. Sebastian Exequiel Pacheco Veliz
[nmacia | einar | pvenosa | asabolansky | cpiazza | spacheco] at linti.unlp.edu.ar

LINTI (Laboratorio de Investigación en Nuevas Tecnologías Informáticas)
Facultad de Informática - UNLP
Calle 50 y 120 – 2do piso – La Plata, Buenos Aires, Argentina

1. Resumen

Los dispositivos móviles son un elemento cada vez mas arraigado en la vida diaria de las personas [1]. Debido a la introducción de estas tecnologías tanto en la vida privada de las personas como en el ámbito laboral de éstas, la seguridad de dichos dispositivos se ha convertido en una preocupación creciente en la sociedad [2].

Entre los alcances esperados de esta línea de I/D/I se encuentra el análisis de distintos problemas de seguridad a los que una persona se expone cuando utiliza estos dispositivos, incluso cuando se les da un uso adecuado. Para esto, se crearán pruebas de concepto que permitan determinar la factibilidad de introducir amenazas en dispositivos móviles y se construirán metodologías de análisis a fin de determinar la existencia o no de las mismas.

Los problemas de seguridad en los dispositivos móviles se extienden a las organizaciones a través de lo que hoy se conoce como BYOD [3] y BYOT [4].

En base al conocimiento adquirido, se espera poder generar conciencia y buenas prácticas, definiendo estrategias y acciones que permitan eliminar o mitigar amenazas tanto para los usuarios como para las organizaciones donde éstos se desempeñan.

Palabras clave: seguridad de la información, concientización, dispositivos móviles, BYOD, BYOT, Android, malware, reversing, políticas de seguridad

2. Contexto

En el Laboratorio de Investigación en Nuevas Tecnologías Informáticas (LINTI) [5] de la Facultad de informática de la Universidad Nacional de La Plata [6], un grupo de docentes/investigadores se dedican a estudiar temas relacionados con la seguridad y privacidad de la información, aplicando los conocimientos en los distintos proyectos en los que participan.

En el marco del proyecto de incentivos Redes, Seguridad y Desarrollo de Aplicaciones para e-educación, e-salud, e-gobierno y e-inclusión", este grupo investiga vulnerabilidades de seguridad actuales que afectan a sistemas, redes y servicios. En particular la línea aquí presentada se enfoca en el estudio de la seguridad de los dispositivos móviles, considerando:

- Problemas de seguridad en el software utilizado
- Problemas de seguridad derivados del mal uso por parte de los usuarios
- Mecanismos de protección y mitigación de problemas
- Implementación de Buenas prácticas y concientización de usuarios.

Este grupo de investigadores forma parte del Centro de excelencia de la UNLP en el tema "Ciberseguridad" [7] , seleccionado por la UIT para el año 2015.

3. Introducción

Los problemas de seguridad a los que los dispositivos móviles están expuestos son similares a los que esta expuesto una computadora, pero se ven agravados ya que cuentan con una mayor exposición al

ser su comunidad de usuarios más amplia, que los utiliza tanto en el ámbito laboral como en el personal.

De acuerdo a [8] [9] [10], un malware [11] que afecte a una computadora o a un móvil puede utilizarse para:

1. Robo de Información personal
2. Espionaje de actividad y comportamiento del usuario (Historial de navegación, mensajes, llamadas, ubicaciones, etc.)
3. Envio de SMS Premium que generen un costo al usuario, suscripción a servicios Pagos
4. Controlar remoto el dispositivo (Bot de una Botnet)
5. Causar comportamiento destructivo al dispositivo (agotamiento de la batería, reinicios no deseados, consumo de RAM y/o CPU, etc.)
6. Enviar Spam mediante SMS o e-mails
7. Robar información personal del usuario y demandando un pago para que el cliente pueda recuperarla (Ransomware)

La problemática presentada se potencia tanto debido al desconocimiento general sobre los problemas de seguridad a los que están expuestos como a la falta de información en las contramedidas que son posibles de adoptar. Si eso lo juntamos con la cantidad de elementos incluidos en los smartphones se dan otros problemas, como los relacionados con el espionaje, puesto que un dispositivo comprometido podría permitir consultar su localización vía GPS, transmitir la información captada por su micrófono o incluso su cámara.

Se pueden agregar los problemas propios tanto de las distintas plataformas como las aplicaciones que corren en ellas. Para citar un caso, Android, el sistema operativo para dispositivos móviles más utilizado en la actualidad [12] posee un gran número de versiones, algunas de ellas, hoy en día, sin actualizaciones. De acuerdo a un relevamiento realizado a fines de Febrero de 2015 [13], el 58,7 % de los celulares Android no tiene soporte y debería ser actualizado como mínimo a la versión 4.4 (KitKat)

Además las actualizaciones se ven demoradas debido a que, en primer lugar, Google libera nuevas versiones; luego los fabricantes las adaptan para sus dispositivos; y finalmente las empresas de telecomunicaciones lo vuelven a modificar agregando personalizaciones, como ser el logo de la empresa. Una vez finalizado este proceso, el sistema operativo queda liberado. Esto resulta en una convergencia lenta y en algunos equipos hasta imposible, lo que deja algunos equipos vulnerables frente a ataques que explotan vulnerabilidades ya corregidas en versiones posteriores del sistema.

Por otro lado, desde la aparición de los Smartphones han ido surgiendo distintas prácticas cuyo objetivo es que el usuario obtenga un control total de su equipo, salteando ciertas restricciones impuestas por el fabricante/desarrollador. Entre estas prácticas podemos mencionar: rootear un teléfono Android [14], instalar aplicaciones no oficiales, jailbreak de iPhone, etc. Estas prácticas se realizan sin tener en cuenta el impacto que tienen sobre la seguridad de los datos almacenados y transmitidos [15].

Por lo anteriormente detallado, el fenómeno BYOD constituye una de las amenazas actuales más preocupantes para las organizaciones [16].

Algunos de los problemas de seguridad pueden mitigarse mediante el uso de software de tipo MDM [17] el cual permite permite asegurar, monitorear y administrar dispositivos móviles de manera centralizada. Esto solo puede aplicarse en forma compulsiva obre los dispositivos que son propiedad de la organización, pero no así sobre los dispositivos personales de los integrantes.

Al carecer de la posibilidad de gestionar los equipos, los activos de la organización pueden verse comprometidos tanto cuando circula información por equipos en poder de los miembros de la organización sin el pertinente estado de seguridad, como ante la perdida o robo de uno de estos dispositivos. Por ejemplo si el dispositivo no posee un PIN o no está protegido por una contraseña segura, un atacante puede obtener acceso directo al dispositivo, su contenido, e incluso todo el contenido que continua llegando a través de los servicios que continúen activos. Medidas parciales, como un equipo protegido por contraseña, no lo hacen completamente inmune, puesto que es posible extraer la tarjeta de memoria y si la misma no está fuertemente cifrada, el atacante tendrá acceso a sus datos.

Debido a todo lo mencionado, un dispositivo privado no debe ser considerado fiable para su uso con

información de la organización hasta que una adecuada revisión confirme que el mismo cumple todos los requisitos especificados en la política de seguridad organizacional.

4. Líneas de Investigación, Desarrollo e Innovación

Sobre los ejes de investigación, inicialmente planteados: seguridad en dispositivos móviles, análisis forense y concientización de usuarios, en una primer etapa: se realizaron pruebas para manipular comunicaciones, se analizaron distintas herramientas de tracking y monitoreo y se elaboraron buenas prácticas de uso [18].

Siguiendo con esta línea, se continuaron las pruebas sobre nuevas versiones y plataformas, se analizó malware existente y su comportamiento y se estudió la aplicabilidad de buenas practicas en usuarios y organizaciones.

5. Resultados y Objetivos

Entre los resultados alcanzados al momento, se pueden enumerar los siguientes:

- POC Android para manipular comunicaciones SMS. Analisis de cambios en la API de mensajería introducidos por Android 4.4.
- Análisis de peligrosidad de aplicaciones. Decompilación. De-ofuscación, análisis de pila. Análisis de código fuente.
- Armado de una suite de aplicaciones para el estudio de APKs Android [19]
- Análisis de herramientas de monitoreo y seguimiento de dispositivos móviles.
- Descripción de buenas prácticas en el uso diario de dispositivos móviles, incluyendo situaciones de robo.

Entre los objetivos que se pretenden alcanzar se pueden enumerar:

- Estudiar de distintos malwares y sus variantes. Conseguir muestras. Realizar ingeniería inversa. Análisis de comportamiento. Vectores de ataque.
- Analizar problemas en Blackberry debido a la posibilidad ejecutar aplicaciones Android. Realizar pruebas de comportamiento de aplicaciones maliciosas (APKs) dentro del entorno de Blackberry. Generar buenas prácticas.
- Analizar y entender mecanismos provistos por distintas tecnologías para preservar la seguridad general del sistema (boot seguro, firma de aplicaciones, etc)
- Desarrollar una aplicación que permita recolectar información relacionada al nivel de seguridad de los dispositivos y concientice usuarios informando malas prácticas de uso.
- Definir un documento de guía para políticas organizacionales de seguridad de dispositivos móviles personales considerando BYOD.
- Comprender y utilizar distintas herramientas de extracción de datos, a partir de las cuales se puedan obtener evidencias relacionadas con incidentes de seguridad que afectan el normal funcionamiento de los dispositivo involucrados.

6. Formación de Recursos Humanos

La línea de investigación Seguridad en dispositivos móviles está siendo abordada por los alumnos Carlos Damián Piazza Orlando y Sebastián Exequiel Pacheco Véliz en el marco de la realización de su tesina de grado de la Licenciatura en Sistemas, en conjunto con los docentes Nicolás Macia, Paula Venosa, Einar Lanfranco y Alejandro Sabolansky quienes también forman parte del grupo de seguridad del LINTI de la Facultad de Informática de la UNLP, el CERT.unlp y las cátedras de grado y postgrado Seguridad y privacidad en redes.

El grupo de seguridad del LINTI de la Facultad de Informática de la UNLP trabaja hace varios años realizado varias experiencias de concientización en Seguridad de la Información dirigidas a distintos perfiles. La tesis “Higienización de dispositivos para la preservación de la privacidad” de la alumna Guillermina Belli, y dirigida por las profesoras Paula Venosa y Lía Molinari, finalizada en el año 2014, es también un resultado alcanzado en esta línea de trabajo, siendo uno de sus ejes la concientización de

usuarios respecto a la protección de sus datos como motivador del estudio de técnicas de borrado seguro en discos magnéticos y herramientas usadas para tal fin.

Por otra parte, este grupo de investigadores representa a la UNLP en el Centro de excelencia en el tema "Ciberseguridad" de la UIT, durante el transcurso del año 2015 [20]. Además el mismo comenzó a participar en el año 2014 de la comisión de estudio ITU-T SG17:Security de la UIT [21], donde se abordan temas actuales de seguridad de la información, y en particular algunos relacionados a esta línea de investigación.

Referencias

[1] Más dispositivos móviles que personas http://www.independent.co.uk/life-style/gadgets-and-tech/news/there-are-officially-more-mobile-devices-than-people-in-the-world-9780518.html

[2] El negocio de la ciberdelincuencia http://www.sophos.com/es-es/security-news-trends/security-trends/malware-goes-mobile/business-of-cybercrime.aspx

[3] "BYOD: Bring your own device Why and how you should adopt BYOD" https://www.ibm.com/mobilefirst/us/en/bring-your-own-device/byod.html

[4] "Del BYOD al BYOT: un fenómeno en alza" http://blogthinkbig.com/del-byod-al-byot-un-fenomeno-en-alza/

[5] Laboratorio de Investigación de Nuevas Tecnologías Informáticas - LINTI.Facultad de Informática: `https://www.linti.unlp.edu.ar`

[6] Facultad de Informática: `https://info.unlp.edu.ar`

[7] Centro de excelencia en Ciberseguridad. http://www.itu.int/en/ITU-D/Regional-Presence/Americas/Documents/EVENTS/2015/0225-BR-COE/Agenda-EN.pdf

[8] Proyecto Nemesys http://www.nemesys-project.eu/nemesys/files/document/deliverables/NEMESYS_Deliverable_1.1_v4_rev_final.pdf

[9] Taxonomy: mobile malware threats and detection techniques http://airccj.org/CSCP/vol4/csit42222.pdf

[10] Android Malware Detection System Classification http://www.scialert.net/fulltext/?doi=rjit.2014.325.341&org=10

[11] Reporte de malware 2014 por F-secure https://www.f-secure.com/documents/996508/1030743/Threat_Report_H1_2014.pdf

[12] Android el sistema operativo móvil mas usado http://www.idc.com/prodserv/smartphone-os-market-share.jsp

[13] Android Platform Versions http://developer.android.com/about/dashboards/index.html#Platform

[14] Rooteo en android http://rootear.com/android/telefonos-android-rooteados-directamente

[15] Cuando el malware llega a los dispositivos moviles. http://www.sophos.com/es-es/security-news-trends/security-trends/malware-goes-mobile.aspx

[16] Aumento del BYOD obliga a resolver problemas de seguridad en redes corporativas. http://diarioti.com/aumento-del-byod-obliga-a-resolver-problemas-de-seguridad-en-redes-corporativas/69615

[17] MDM Mobile Device Management http://es.wikipedia.org/wiki/Mobile_device_management

[18] Lic. Nicolás Macia, Lic. Einar Lanfranco, Lic. Paula Venosa, Carlos Damián Piazza Orlando, Sebastian Exequiel Pacheco Veliz. (2014) "Seguridad en dispositivos móviles: un enfoque práctico"WICC ISBN 978-950-34-1084-4

[19] APK http://es.wikipedia.org/wiki/APK_%28formato%29

[20] Grupo de Estudio 17 en la ITU http://www.itu.int/en/ITU-T/studygroups/2013-2016/17/Pages/default.aspx.

[21] ITU. http://www.itu.int