Seguridad en dispositivos móviles: un enfoque práctico

Lic. Nicolás Macia
nmacia at info.unlp.edu.ar

Lic. Einar Lanfranco
einar at info.unlp.edu.ar

Lic Paula Venosa
pvenosa at info.unlp.edu.ar

Carlos Damián Piazza Orlando
carlitos-tkd@hotmail.com

Sebastian Exequiel Pacheco Veliz
sebaspev@hotmail.com

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

Resumen

Hoy en día, los dispositivos móviles son un elemento común en la vida diaria de las personas [1]. Los problemas de seguridad a los que estos dispositivos están expuestos son similares a los que esta expuesto una PC [2]. Inclusive, se dan a otros problemas 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 [3].

El problema de la inseguridad en dichos dispositivos se extiende a las organizaciones a través de lo hoy llamado BYOD[1][4] y BYOT[2] [5].

Entre los alcances esperados de esta línea de I/D/I están los de analizar los distintos problemas de seguridad a los que una persona se expone utilizando este tipo de dispositivos, incluso cuando se les da un uso adecuado, creando pruebas de concepto que permitan ejemplificar los problemas posibles y metodologías de análisis que permitan determinar la existencia o no de amenazas de este tipo en los dispositivos móviles.

En base al conocimiento adquirido, también se espera poder generar conciencia y buenas prácticas basada en el estudio de las tecnologías abordadas tanto para usuarios como para organizaciones en las que estos se desempeñan.

Palabras clave: Seguridad de la información, Concientización, dispositivos móviles, Smartphone, Android, blackberry, SDK

Contexto

La línea de investigación presentada está inserta en el proyecto de incentivos "Redes, Seguridad y Desarrollo de Aplicaciones para e-educación, e-salud, e-gobierno y e-inclusión" del LINTI[3] de la Facultad de Informática de la Universidad Nacional de La Plata[4] (UNLP). En el marco de este proyecto un grupo de docentes/investigadores del LINTI trabajan en el estudio y aplicación de estándares y tecnologías vinculadas a la seguridad y privacidad en redes y aplicaciones, incluyendo en esta línea

[1] Bring your own devices

[2] Bring your own technology

[3] http://www.linti.unlp.edu.ar

[4] http://www.info.unlp.edu.ar

también la concientización y capacitación en temas vinculados a la seguridad de la información en el ámbito académico.

Introducción

A partir del uso masivo de dispositivos móviles, tanto en el ámbito personal como en el laboral, las organizaciones están empezando a considerar con más detenimiento el suceso y los potenciales problemas de seguridad que los afectan. En relación a ésto el fenómeno BYOD [4] constituye una de las amenazas actuales más preocupantes [2].

Desde la aparición y uso de los smartphones han ido surgiendo distintas prácticas cuyo objetivo es que el usuario aproveche al máximo el potencial del dispositivo o que obtenga un control total del mismo salteando ciertas restricciones impuestas por el fabricante/desarrollador, entre las que podemos mencionar: jailbreak de un teléfono iphone [6], rootear un teléfono android [7], instalación de aplicaciones desde fuentes no oficiales en android [8], sin tener en cuenta la importancia de garantizar la seguridad de los datos que en los mismos transmiten y almacenan. Al decir datos podemos estar refiriéndonos tanto a información privada del dueño del smartphone como así también información propia de la organización puesto que el usuario usa el teléfono para conectarse a servicios provistos por la misma, lo cual se refiere con el nombre de BYOD.

Un smartphone comprometido, automáticamente pone en riesgo:

- La clave de la/s red/es a la que el dispositivo se conecta
- El usuario de la cuenta de correo utilizada
- El usuario de la cuenta de mensajería instantánea utilizada
- Accesos VPN que puedan haber configurados
- Información de contactos personales
- Información de acceso en distintas aplicaciones: facebook, linkedin, etc

Distintos problemas de seguridad relacionados con estas tecnologías que han tomado trascendencia pública, los cuales, no sólo podrían estar relacionados con el compromiso de los datos personales de los mismos sino también con ataques dirigidos contra la privacidad o inclusive espionaje [3]. A modo de ejemplo podemos mencionar una campaña de ciberesionaje ha logrado infiltrarse en redes informáticas de organizaciones diplomáticas, gubernamentales y de investigaciones científicas conocida como “Octubre Rojo” o “Rocra” [9] (por Red October), activa desde mayo de 2007, la cual, además de los blancos de ataques tradicionales (estaciones de trabajo), puede robar datos de dispositivos móviles como smartphones incluyendo iPhone, Nokia y Windows Mobile.

En la actualidad, el tema aquí abordado resulta de interés dado que aún no se cuenta con información completa y precisa relacionada a que medidas a

adoptar, tanto por parte de los usuarios como por parte de las organizaciones, a fin de preservar la seguridad de la información contenida en los dispositivos móviles[10]. Además, también es de vital importancia el estudio de metodologías y técnicas de análisis que permitan determinar la existencia o no de amenazas reales sobre los dispositivos móviles analizados.

Líneas de Investigación, Desarrollo e Innovación

A partir de la problemática planteada en la sección anterior, hemos partido de las siguientes hipótesis:

- En los últimos tiempos se han reportado distintos problemas de seguridad en los smartphones .
- Las prácticas que se llevan a cabo para facilitar/promover el uso de los smartphones exponen a los mismos a amenazas de seguridad.
- En términos de seguridad proactiva, se pueden determinar buenas prácticas que conlleven a minimizar los riesgos existentes en el uso de smartphones.
- Para poder analizar causas y efectos de un incidente de seguridad es necesario conocer metodologías adecuadas de extracción de datos y análisis.

Partiendo de esta base, los ejes del tema que se está investigando son:

- Seguridad en dispositivos móviles
- Concientización de usuarios
- Análisis forense de dispositivos móviles

Resultados y Objetivos

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

- Realización de una POC android para manipular comunicaciones SMS.
- Análisis de herramientas de tracking de dispositivos móviles en distintos tipos de tecnologías (android, iphone, blackberry)
- Análisis de herramientas de monitoreo de dispositivos móviles en distintos tipos de tecnologías (android, iphone, blackberry)
- Descripción de buenas prácticas tanto en su uso como ante situaciones de robo de un dispositivo móvil.

Entre los objetivos que se quieren alcanzar podemos enumerar:

- Realizar un análisis en profundidad considerando distintos tipos de usos y/o configuraciones que puedan desencadenar situaciones indeseables, en las distintas tecnologías de smartphones.
- Analizar y entender distintos mecanismos provistos por distintas tecnologías para preservar la seguridad general del

sistema (BOOT SEGURO, FIRMAR APPS, ETC)

- Utilizar los SDK de las distintas tecnologías para la creación de POCs que ayuden a crear conciencia.

- Definir buenas prácticas para preservar la seguridad de la información que se almacena en los dispositivos móviles.

- 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.

- Incursionar en metodologías de reversing de binarios [11] que se ejecutan en las distintas plataformas.

Formación de Recursos Humanos

Como parte del trabajo del grupo de investigación de Redes y Seguridad del LINTI, el tema de seguridad en dispositivos móviles está siendo abordado por los alumnos Carlos Damián Piazza Orlando y Sebastian Exequiel Pacheco Veliz en el marco de la definición de su tesina de grado de la Licenciatura en Sistemas, en conjunto con los profesores Nicolás Macia, Paula Venosa y Einar Lanfranco, quienes además son integrantes del equipo de atención de incidentes de seguridad en la UNLP, CERTunlp[5].

Esta linea de investigación también forma parte de las tareas realizadas por el equipo de respuesta de incidentes CERTunlp.

En lo que refiere a concientización en seguridad de la información, el grupo ha realizado varias experiencias y capacitado a diferentes perfiles (entre ellos usuarios en general, alumnos, docentes, usuarios gerenciales). La tesis "Una herramienta para concientización sobre seguridad en Internet" del alumno Gerónimo Acevedo, dirigida por las Prof. Paula Venosa y Claudia Banchof, finalizada en el año 2013, es también un resultado alcanzado en esta línea de trabajo en lo que hace a la formación de recursos humanos [12][13].

Referencias

[1] "The State of Broadband 2013: Universalizing Broadband"-Boradban comision ITU UNESCO http://tools.cisco.com/search/results/display?url=http%3a%2f%2fwww.cisco.com%2fassets%2fcsr%2fpdf%2fState_of_Broadband.pdf&pos=6&query=smartphone+argentina

[2] "423 Vulnerabilidades en android- Resultado de Busqueda en la National Vulnerability Database" - http://web.nvd.nist.gov/view/vuln/search-results?query=android&search_type=all&cves=on

[3]"Vulnerabilidad en la firma de APKs"http://www.genbeta.com/seguridad

[5] http://www.cert.unlp.edu.ar

/en-que-consiste-la-vulnerabilidad-de-android-y-como-podemos-protegernos

[4]"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

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

[6] "¿Qué es jailbreak?" - http://www.jailbreakme.com/#moreinfo

[7] "¿Qué es rootear un android?" - http://yosoyandroid.com/diccionario-android/que-es-root-y-para-que-sirve/

[8] "¿Cómo autorizar la instalación de apks no oficiales?" http://www.androidjefe.com/instalacion-bloqueada-android-porque-como-desbloquear/

[9] "Descripción del estudio sobre Rocra" - http://www.viruslist.com/sp/weblog?discuss=208188760&return=1

[10] "A survey of mobile phone sensing" - Lane, N.D.; Miluzzo, E. ; Hong Lu ; Peebles, D. ; Choudhury, T. ; Campbell, A.T. , Communications Magazine, IEEE

[11] http://en.wikipedia.org/wiki/Reverse_engineering

[12] "FoCoS: una herramienta para concientización sobre seguridad en Internet" – Gerónimo Acevedo -http://catalogo.info.unlp.edu.ar/meran/opac-detail.pl?id1=6304#.UzbknFSnPz4

[13] "Redes Sociales Open Source: una comunidad para Caperucita" , Claudia Banchoff, Gerónimo Acevedo, Paula Venosa, TE&ET 2012,ISBN 978-987-28186-0-9