Inseguridad en Smartphone Apps

Simón Roses Femerling
Fundador y CEO de Vulnex

El abaratamiento de los *smartphones* -potentes ordenadores de bolsillo permanentemente conectados a Internet- ha disparado el consumo de Apps entre los usuarios. IDC predice que en 2015 se venderán 982 millones de estos dispositivos y Morgan Stanley estima que en 2012 se venderán más *smartphones* que PC en todo el mundo.

Con este gran mercado potencial miles de desarrolladores, desde programadores en solitario hasta conocidas casas de desarrollo, se han lanzado a la publicación de aplicaciones móviles. Por ejemplo, en Google Play -antiguamente Google Market-, sólo en United Kingdom (UK) se lanzaron de media 701 Apps diarios durante todo 2011.

Desarrollar y publicar Apps en cualquiera de las tres plataformas líderes (iPhone, Android y Windows Phone 7) es muy sencillo y rápido y, por ello, todos estos programadores se centran en lanzar nuevas aplicaciones o actualizaciones de anteriores de forma constante, con el fin de obtener cuota de mercado y, por supuesto, ganar dinero. De hecho, medios especializados hablan de que la Web ha muerto y que hoy únicamente importa tener una buena App.

En la Figura 1 podemos apreciar la cantidad de Apps que tienen las tres plataformas principales. En cuanto a número de descargas, en febrero de 2011 ascendió a 18 billones de Apps en iPhone y en diciembre 2011 se alcanzaban los 10 billones de Apps en Android.

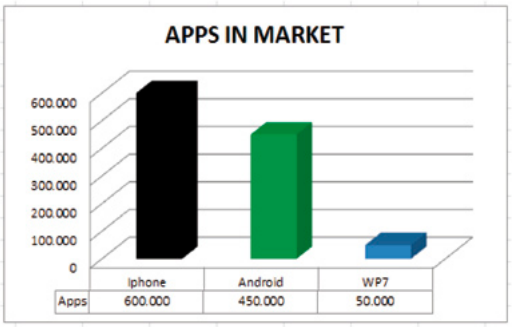


Figura 1. Número de Apps disponibles en sus respectivos mercados.

Por desgracia, en esta frenética actividad se tiende a sacrificar seguridad y privacidad: demasiadas de estas Apps, con millones de usuarios, son inseguras, llegando a comprometer la seguridad del dispositivo y los datos del propio usuario.

Desde Vulnex, empresa española altamente especializada en ciberseguridad, se han analizado más de 100 top Apps de iPhone y Android con el objetivo de determinar su postura de Seguridad, y cuyos resultados se resumen en este artículo. El lector podrá encontrar más información sobre la investigación en la web de la compañía (www.vulnex.com).

Mapa de vulnerabilidades en Apps

En el estudio citado, realizado en más de 100 top Apps, se identificaron diversas clases de vulnerabilidades, siendo algunas de éstas clasificadas graves, como por ejemplo, contraseñas en texto claro o canales inseguros.

Muchas de estas vulnerabilidades son ampliamente conocidas en las aplicaciones web y existe mucha literatura sobre cómo mitigarlas, por lo que no se entiende que se vuelvan a cometer los mismos errores en aplicaciones para *smartphones*.

En la Figura 2, se expone un mapa de las clases de vulnerabilidades identificadas en Apps. A pesar de que el título hace referencia a Android, también aplica a iPhone.

Algunas de estas vulnerabilidades son graves si tenemos en cuenta que, entre las Apps analizadas, se encuentran varias relacionadas con banca *online*, seguridad y comunicaciones. Y es que no podemos olvidar que los *smartphones* almacenan gran cantidad de información sensible e identificable de un usuario, que un atacante

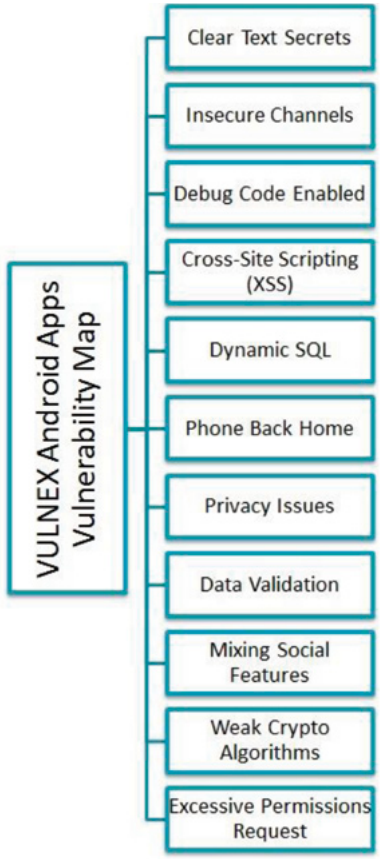
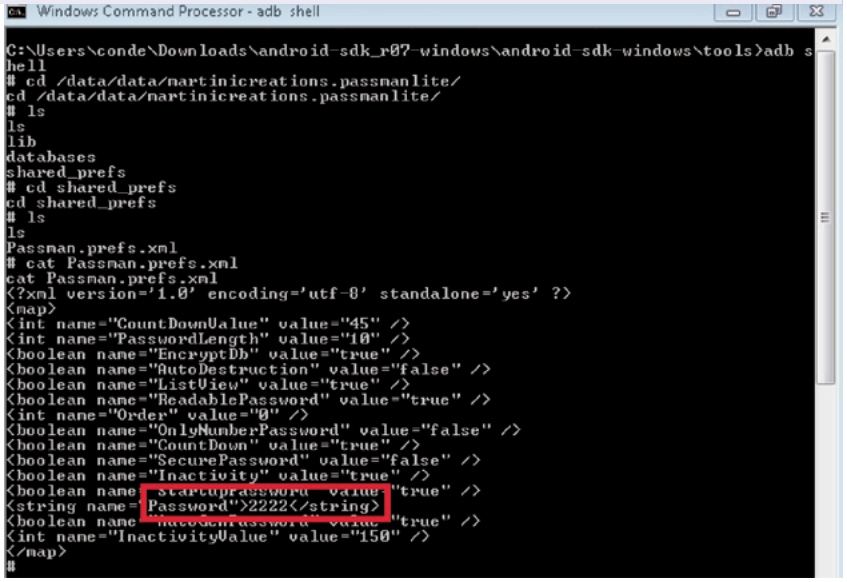


Figura 2. Clases de vulnerabilidades en aplicaciones móviles.

Figura 3. Contraseña en texto claro.



podría conseguir. Es mayor la preocupación cuando vemos que estos dispositivos, *smartphones* y tabletas, se están introduciendo rápidamente en el entorno corporativo y podrían ser utilizados como vector de ataque comprometiendo la seguridad de la organización.

En el análisis hemos encontrado vulnerabilidades ampliamente conocidas como contraseñas sin codificar, envío de información en texto claro sin ningún tipo de protección, *Cross-Site Scripting* (XSS) e inyección de SQL.

Otras vulnerabilidades hacen referencia a la capacidad que tienen las aplicaciones de recoger información del dispositivo (como lista de contactos, *bookmarks*, información de sistema operativo y *hardware*) y enviarla a un servidor remoto. Llama la atención la integración de redes sociales en Apps de banca *online*.

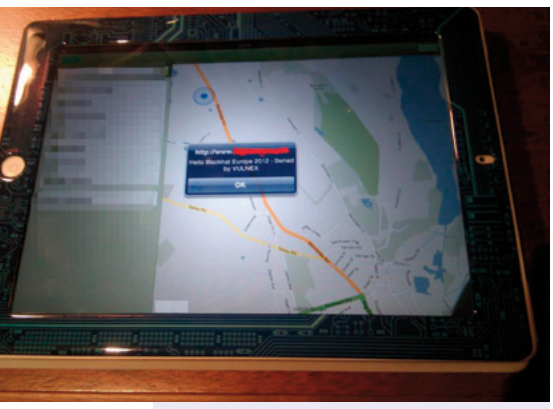


Figura 4. Ataque de Cross-Site Scripting (XSS).

Es recomendable que los desarrolladores de este tipo de aplicaciones no abusen de la solicitud de permisos para su App, ya que podría provocar que los usuarios acepten sin revisar si los permisos son apropiados para la App en cuestión. Esto es importante ya que algunos permisos tienen un impacto económico.

En la Figura 3 tenemos un App de seguridad, CVE-2011-1840, que cifraba la contraseña maestra en texto claro y la almacenaba en un fichero XML de configuración. El desarrollador no protegió adecuadamente la contraseña porque confiaba en la seguridad de la plataforma, grave error. Un atacante o *malware* podría acceder a la contraseña almacenada en el dispositivo.

Sin duda, esta clase de vulnerabilidades puede ser grave y se han identificado algunas aplicaciones afectadas.

Otro ejemplo de vulnerabilidad es la capacidad de inyectar código malicioso mediante un ataque de MITM y que se ejecute en la App. En la Figura 4 se puede ver una demostración de una conocida App, con millones de usuarios, víctima de un ataque de *Cross-Site Scripting* (XSS).

Muchos usuarios utilizan sus dispositivos en lugares públicos como cafés, hoteles y aeropuertos y por eso este tipo de ataques pueden ser muy peligrosos.

El último ejemplo (ver Figura 5) es una conocida App para reproducir vídeos que tiene servidores web, Samba y FTP incluidos para subir ficheros directamente al dispositivo. Por desgracia, la aplicación no hace una correcta validación de datos, y un atacante puede enviar una sentencia maliciosa provocando un error en la App.

Este tipo de errores puede comprometer de forma muy grave la seguridad del dispositivo permitiendo a un atacante ejecutar código malicioso, lo que combinado con otras clases de vulnerabilidades -por ejemplo, de plataforma- podría ser devastador.

Conclusiones

A lo largo de este artículo hemos expuesto algunas clases de vulnerabilidades que afectan a aplicaciones que utilizan con millones de personas, lo que supone un asunto muy serio sobre seguridad y privacidad de las Apps.

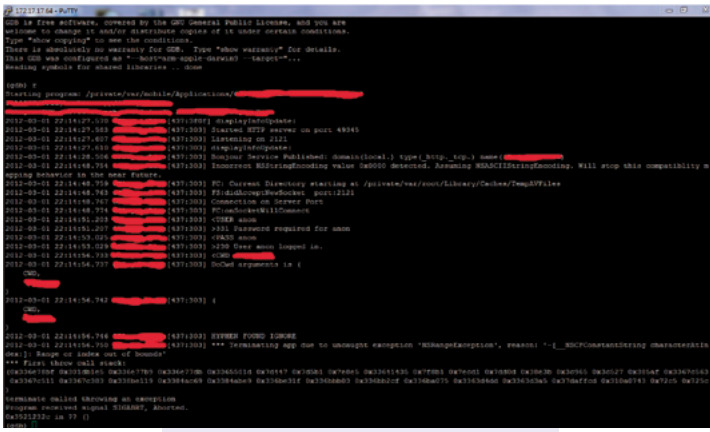


Figura 5. Atacando el servicio FTP de la App.

Las Apps son un mercado imparable y, por ello, deberían seguir un ciclo de desarrollo seguro.

Afortunadamente existen diversos recursos como OWASP Mobile Project (https://www.owasp.org/index.php/OWASP_Mobile_Security_Project), así como las webs de los respectivos fabricantes con información para desarrollar Apps de forma segura.