Estudio de troyanos en dispositivos móviles

D. Fuentes, J.A. Álvarez, J.A. Ortega, J.Torres
Departamento de Lenguajes y Sistemas Informáticos
Escuela Técnica Superior de Ingeniería Informática
Universidad de Sevilla
Avda. Reina Mercedes, s/n 41012
{dfuentes, jaalvarez}@us.es, {ortega,torres}@lsi.us.es

Resumen

A finales de 2007 había en el mundo 3.300 millones de móviles según un estudio de la Unión Internacional de Telecomunicaciones (UTI), lo que supone aproximadamente un teléfono móvil cada dos personas. Si a esto unimos el incremento de capacidades de sensorización de dichos dispositivos, hace que hoy en día la mayoría de las personas se encuentren comunicadas y puedan aprovechar la potencia de sus terminales para conseguir funcionalidades avanzadas: navegación vía GPS, comunicación a Internet, realizar fotografías,... Según Gartner Inc., en 2009 un 29% de los dispositivos móviles en el mundo serán PDAs y Smartphones, con un 90% de predominio de los sistemas operativos Symbian y Microsoft Windows Mobile. Además, actualmente 33 millones de usuarios ya usan los dispositivos móviles para realizar compras y se prevé que en 2010 llega a 103.8 millones. Por otra parte el spam, el número de SMS con intenciones fraudulentas, las numerosas descargas de melodías, fondos para móviles, etc, están aumentando de una manera increíble. Según los datos proporcionados de la firma Ferris Research, se estima que los estadounidenses propietarios de teléfonos móviles reciban unos 1.500 millones de SMS no solicitados a lo largo de 2008. Dicha cifra es el doble de lo que se recibió en 2006. Y eso no es lo peor, sino las posibles infecciones que todos estos mensajes pueden contener en su interior.

En los dispositivos móviles, cada servicio que permita conectar con otro dispositivo puede ser fuente para la intrusión de un virus u otra amenaza. Pueden existir otros caminos que den lugar a la intrusión de un software malicioso, como son las tarjetas de memoria extraíble o la sincronización de una PDA con un PC. La mayoría de los usuarios pueden acceder con sus dispositivos móviles a Internet y debido a ello, también son posible blanco de estas amenazas. Nuestro estudio analizará con detalle todas estas posibles fuentes de infección, advertencias o consejos de prevención y software actual de protección para nuestros dispositivos móviles.

En este artículo nos centraremos en los ataques con troyanos, cuyo objetivo fundamental (además de su propia propagación) es la obtención de información de un usuario de forma maliciosa sin que este pueda percibir el robo. Para ello, se analizará la seguridad en estos dispositivos móviles mediante una experiencia práctica en la que se introducirá un troyano en el terminal de un usuario para conseguir la información de los contactos almacenados en el terminal. El troyano se instalará en la máquina del usuario atacado sin que este pueda ser consciente de ello puesto que irá camuflado dentro de una imagen (aunque también podría ir junto a un archivo de audio o vídeo). El programa una vez instalado, quedará de forma permanente ejecutándose en la PDA atacada a la espera de que un segundo usuario malicioso envíe un mensaje SMS con una estructura predeterminada cuyo contenido será procesado a través de un parser programado dentro del troyano, que devolverá todos los contactos dentro de tantos mensajes SMS como sean necesarios. Una vez analizado el problema, se propondrá una solución que tratará de solventar las posibles consecuencias del ataque a la privacidad del usuario. Por último, como conclusión se realizará una reflexión sobre los resultados obtenidos en el estudio, aconsejando al lector sobre la importancia de la seguridad en los dispositivos móviles en una sociedad en la que los más diversos adelantos tecnológicos ocupan un lugar cada vez más cotidiano y habitual.

1 Introducción

Los dispositivos móviles representan hoy en día la tecnología más extendida y cambiante en el mundo. Ni siquiera los ordenadores personales consiguen superar el ritmo de crecimiento, mejora y aceptación de esta tecnología al alza. Además, al crecer el número de servicios y prestaciones, cada vez se hacen más imprescindibles en nuestro día a día, debido a que ya no sólo proporcionan el servicio básico de

la comunicación por voz, sino contienen otras formas de comunicarse como la mensajería instantánea, mensajería multimedia, bluetooth, NFC o correo electrónico. Para tener una idea de este vertiginoso crecimiento, según el IDC en España el 27% de los trabajadores usan la tecnología móvil como parte de su trabajo, y según una encuesta dada a conocer en el Mobile World Congress 2008 de Barcelona, el 20% de los usuarios españoles considera sustituir su conexión fija a Internet por acceso UMTS.

Debemos reconocer que cada día dependemos más de nuestra PDA o teléfono móvil, le dedicamos más tiempo, lo consultamos más a menudo y sólo tenemos que pararnos a pensar la catástrofe que supondría para nosotros su pérdida. Estamos ante una tecnología cambiante que varía a una velocidad vertiginosa. Los dispositivos móviles que copaban el mercado tan sólo hace unos meses quedan obsoletos porque los actuales nos ofrecen mayores prestaciones. Ya no es necesario que en tu bolsillo tengas un reproductor MP3 para reproducir música, una cámara para realizar fotos o vídeos de alta calidad, un portátil para conectarse a Internet, ver un documento de texto o mandar un correo electrónico puesto que nuestro teléfono móvil ya es capaz de realizar todas estas funciones. Además, ya no sólo usamos nuestro dispositivo móvil para el ocio, sino también para el trabajo y es muy común que cuando un usuario llega a un nuevo puesto la empresa le ofrezca un teléfono móvil o PDA par su uso durante su jornada laboral. El incremento de los dispositivos móviles en las pequeñas, medianas y grandes empresas ha supuesto un también un crecimiento en la productividad en estos últimos años, hasta tal punto que los trabajadores necesitan una formación previa para garantizar un manejo adecuado además de la seguridad en este tipo de dispositivos, cada vez con un mayor cantidad de información.

Como consecuencia de todos los servicios que los nuevos dispositivos ofrecen, se hace imprescindible aumentar la capacidad de almacenamiento (ya sea dentro del terminal o con tarjetas externas) y por tanto también aumenta la información contenida: datos de los contactos, mensajes SMS/MMS almacenados, llamadas grabadas, fotografías o videos son sólo los ejemplos más comunes de información que podemos encontrar en casi cualquier teléfono u otro dispositivo móvil de hoy en día. Por tanto, debemos reflexionar sobre la importancia de la seguridad en los dispositivos móviles en una sociedad en la que los más diversos adelantos tecnológicos ocupan un lugar cada vez más cotidiano y habitual.

1.1 Ataques a dispositivos móviles

En los dispositivos móviles, cada servicio que permita conectar con otro dispositivo puede ser fuente para la intrusión de un virus u otra amenaza. Pueden existir otros caminos, como son las tarjetas de memoria extraíble o la sincronización de una PDA con un PC que pueden transportar al dispositivo la infección. Por tanto, existe un aumento en la probabilidad de un posible ataque a estos dispositivos y cierta preocupación por parte de los usuarios por el peligro de darse cuenta de ello cuando ya sea demasiado tarde. La mayoría de los usuarios pueden acceder con sus dispositivos móviles a Internet y debido a ello, también son posible blanco de estas amenazas. Ejemplo actual es el virus SymbOS/Beselo.A!worm, que se instala a través de varios aparatos Symbian S60 de Nokia. Se contagia a través de SMS y Bluetooth siendo posteriormente enviado a todos los contactos del mismo operador. La infección puede llegar al usuario por diferentes caminos como podemos ver en la Figura_1. A continuación describiremos con más detalle alguno de ellos:

SMS: El SMS, junto al MMS y al Bluetooth son los medios más comunes a través de los cuales los usuarios resultan infectados. La principal desventaja del SMS es su limitado tamaño (160 bytes) y es por ello por lo que no ha habido aún una infección a gran escala vía SMS. El prototipo de troyano descrito en este artículo usará los SMS para el intercambio de información entre el usuario malicioso y el usuario atacado.

MMS: Sin duda uno de los medios más comunes para el contagio. Hoy en día, son muy comunes las descargas de canciones, imágenes o juegos. Podría que ser que unido a alguno de estos archivos se encuentre un troyano que se instale sin que el usuario llegue a darse cuenta y que pueda reenviar toda o parte de la información almacenada en el dispositivo. El tamaño del MMS lo impone el proveedor del servicio, normalmente más de 300KB, lo que parece un tamaño apropiado dar cabida al software malicioso. Ejemplo de ello es el Commwarrior, que con 27 KB, podía ser mandado fácilmente como adjunto a otro archivo. Otro peligro de este método de infección es la variedad de formatos en los que puede ir el software alojado. Mientras que el SMS acepta principalmente texto plano, el MMS puede contener texto, audio (MP3, MIDI), imágenes (JPEG, GIF) o video (MP4, MPEG).

Bluetooth: Tecnología inalámbrica de corto alcance, permite la comunicación de datos y voz de dispositivos separados entre 1 (Clase 3) y 100 m (Clase 2). La especificación de Bluetooth define un canal de comunicación de máximo 720 b/s (1 Mbps de capacidad bruta) con rango óptimo de 10 metros. La frecuencia de radio con la que trabaja está en el rango de 2,4 a 2,48 GHz con posibilidad de transmitir en Full Duplex. La tecnología Bluetooth desarrolla diferentes niveles de seguridad basados en la identificación de los dispositivos implicados (cada dispositivo tiene un identificador unico de 48 bits y puede comunicarse simultáneamente con siete dispositivos como máximo) y es el fabricante el que decide este nivel en cada dispositivo. En los último años, el número de vulnerabilidades vía bluetooth ha aumentado considerablemente. La mayoría de ellas se pueden arreglar bajando el parche correspondiente desde la página web del fabricante. Sin embargo, cuando se trata de una nueva vulnerabilidad, sólo se modifica el software para los próximos dispositivos.

Correo electrónico: este método resulta sumamente peligroso si tenemos en cuenta que se trata un método sin restricciones de tamaño, puede adjuntar varios archivos y el software malicioso puede extenderse con mayor facilidad a otros dispositivos no móviles, principalmente PCs.

USB: La mayoría de terminales del mercado traen consigo un puerto USB mediante el cual pueden conectarse a un PC. Es muy común su uso a la hora de sincronizar las agendas de ambos dispositivos y puede ser justo en este momento cuando una infección puede trasladarse de un dispositivo a otro.

Figura 1: Vías de infección en dispositivos móviles

1.2 Troyanos en dispositivos móviles

¿Qué ocurre si un dispositivo se pierde o es robado? El dispositivo podría contener datos confidenciales y podrían derivarse responsabilidades legales en caso que contuviera información confidencial, como registros médicos. Ya se ha visto que existen multitud de formas en las que un dispositivo móvil puede resultar atacado, pero en este artículo nos centraremos en los ataques con troyanos, en el cual, su objetivo fundamental (además de su propia propagación) es la de obtener información del usuario de forma maliciosa sin que este pueda percibir el robo.

Resulta muy común hoy en día que un usuario pueda descargar en su terminal una melodía, vídeo, imagen o videojuego que haya podido ver como anuncio en algún canal de televisión, página web Internet, revista o prensa en general. Estas descargas se realizan enviando mensajes SMS a números que en principio no nos dan ninguna seguridad de lo que puede llegar a nuestro móvil. Podamos pensar que ya que estamos pagando por el servicio de descarga, esta no puede resultar ser una fuente de infección. Sin embargo, no resulta demasiado difícil enviar un troyano dentro de un archivo de este tipo. Como veremos en nuestra demostración, el troyano irá camuflado dentro de una imagen, pero puede ir junto a cualquier archivo de forma que cuando llega al terminal el software malicioso queda instalado.

Un ejemplo claro de ello es el troyano Mosquito 2,0 (2004), que acompañaba la versión pirateada del juego para dispositivos móviles del mismo nombre. Atacaba a móviles Nokia con sistema operativo Symbian Series 60, que por otro lado era el sistema operativo más usado en Europa. El troyano no afectaba a la funcionalidad del equipo, sin embargo enviaba mensajes SMS a servicios Premium (1€/SMS aproximadamente) mientras el usuario jugaba con una copia ilegal del juego. De hecho, es muy probable que aún existan páginas web donde descargarnos este juego y aunque aparecen dos advertencias antes de instalarlo, algún usuario puede caer en la tentación. Por otro lado, el troyano desparecía con sólo borrar el juego del móvil.

2 Desarrollo

Para comprender el estudio de los troyanos en dispositivos móviles se ha realizado una prueba consistente en la programación de uno de ellos. Así, hemos pretendido demostrar la sencillez con la que un usuario malicioso puede realizar el robo de los datos contenidos en la agenda de otro. La comunicación se realizará mediante SMS con una estructura interna previamente definida mediante la cual el usuario malicioso podrá enviar órdenes a la PDA atacada sin que la otra persona pueda ser consciente de ello.

El prototipo de troyano para PDA se instalará en la máquina de un usuario atacado y devolverá al usuario malicioso los datos de sus contactos. El troyano irá camuflado dentro de una imagen (aunque también se podría implementar con un archivo de audio o vídeo).

Destacar que ya existen programas como *Windows Mobile PRO-X*, de FlexiSPY, que realiza tareas de espionaje en móviles. Esta aplicación permite controlar todos los SMS enviados y recibidos, todos los registros de llamadas y su duración, escuchar conversaciones telefónicas, control remoto del software utilizando las funciones de SMS o descarga directa en el dispositivo sin necesidad de PC o cables. Además, si el dispositivo dispone de GPS, se puede usar como rastreador para recibir las coordenadas de ubicación del dispositivo. Trabaja con todas las versiones de Windows Mobile 2003, excepto PocketPC y su coste aproximado es de 250 euros.

2.1 Implementando un troyano

Para la implementación del prototipo de troyano se ha usado el Kit de desarrollo Microsoft Windows Mobile 6 Professional instalado en el entorno de programación Microsoft Visual Studio 2005. El simulador proporcionado actuará como usuario atacado, es decir, al arrancar el programa en el simulador, se emula la instalación de un software malicioso que permanece ejecutado en segundo plano mientras el usuario sólo observa una fotografía. Por otro lado, para poder realizar el envío y recepción de SMS por parte del usuario malicioso, se ha usado la herramienta Microsoft Cellular Emulator v1.43, que permite realizar llamadas y enviar SMS (entre otros servicios) al emulador de Visual Studio. Así, podemos realizar la simulación de intercambio de SMS en-

tre dispositivos móviles de forma eficiente sin hacer uso de los servicios de alguna compañía teleoperadora.
Las clases principales de Windws Mobile 6 SDK usadas para la demostración fueron:

OutlookSession: permite, entre otras funciones, acceder y modificar los datos de los contactos. En nuestro caso, lo usamos para el robo del nickname y del número de telefóno móvil.

MessageInterceptor: Interceptador de mensajes personalizados. Implementa el canal que permite al troyano permanecer a la espera de algún SMS entrante. El objeto interceptador de la clase *MessageInterceptor* será clave tanto en la implementación del troyano como en la solución propuesta (como veremos en apartados siguientes) puesto que contiene el evento que permite la recepción de SMS es *interceptor MessageReceived()*.

SmsMessage: Clase que implementa la creación y envío de SMS.

2.2 Flujo de información

El funcionamiento en el lado del usuario atacado se muestra en el diagrama de la figura 2:
1. El usuario obtiene la imagen donde va empaquetado el troyano. El archivo puede llegar al terminal por su descarga desde Internet, mediante un servicio MMS o vía Bluetooth.
2. Una vez que el virus se encuentra en el móvil, se instala de forma automática.
3. El programa queda a la espera de recibir órdenes. Dichas instrucciones vendrán de parte del usuario malicioso en forma de SMS con una estructura predeterminada.
4. Si llega SMS con el formato correcto, en nuestro caso con la cabecera *@espia@* se procede al procesamiento de su contenido. En caso contrario, el mensaje pasa a la bandeja de entrada del usuario.
5. A continuación se comprueban los pares etiqueta-valor. En el parser se reconocen los pares *<sms>númeroteléfono*.
6. Se envía de forma automática los datos de los contactos contenidos en la agenda a cada uno de los teléfonos del par *<sms>númeroteléfono*. En la demostración se envía mediante SMS el nombre de cada contacto y su número de teléfono con el formato *nombrecontacto:númeroteléfonomóvil* pero igualmente podrían ser otros datos.
7. Una vez enviados todos los SMS, el troyano queda a la espera de nuevas órdenes.

Hasta aquí actúa el troyano instalado en el lado del terminal víctima del ataque. El proceso del lado del usuario malicioso se describe en el diagrama de la figura 3:
1. El usuario malicioso envía una orden al troyano mediante un mensaje SMS al usuario atacado con el formato adecuado, que en la aplicación de prueba se trata de @espia@*<sms>númeroteléfono<sms>númeroteléfono*....
2. Queda a la espera de la respuesta del troyano.
3. Comienza a recibir mensajes SMS con la estructura *nombrecontacto:númeroteléfonomóvil-nombrecontacto:númeroteléfonomóvil-*... Los mensajes son procesados mediante un segundo parser en el cuál el usuario malicioso decidirá cómo procesar la información obtenida.
Se termina el proceso hasta que el usuario decida enviar un nuevo SMS con órdenes que den lugar a que se inicie de nuevo el proceso de ataque.

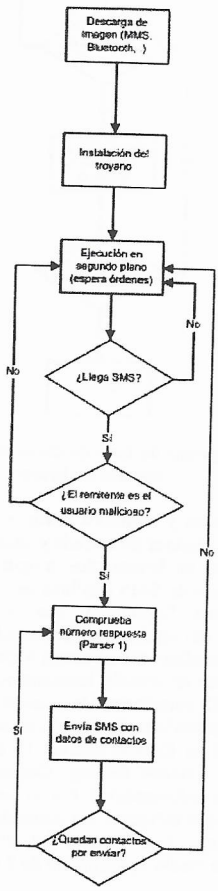

Figura 2: Diagrama de flujo de datos en el dispositivo del usuario malicioso

2.3 Resultado de la experiencia

Evidentemente, todo el proceso se lleva a cabo sin que el usuario atacado sea consciente de ello puesto que el troyano permanecerá ejecutándose en segundo plano. Además, los

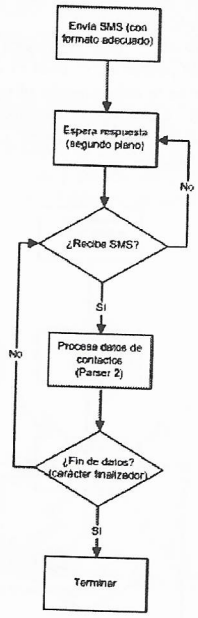

Figura 3: Diagrama de flujo de datos en el dispositivo del usuario malicioso

mensajes enviados y recibidos desde el dispositivo atacado no pasan a los buzones de entrada y salida respectivamente, de manera que no levantamos ningún tipo de sospecha. Además, el envío de SMS conlleva un coste económico que podemos estimar. Suponemos que la longitud media del nombre o nick del contacto es 10 caracteres y sabemos que el número de teléfono móvil ocupa 9 caracteres. Incluyendo los caracteres de separación tenemos que por cada contacto se consumen 12 caracteres. Un usuario normal puede tener de forma aproximada en la agenda de su móvil 100 contactos y los SMS en España cuestan 15 céntimos de euro de media (según Viviane Reding, Comisaría Europea de la Sociedad de la Información). Por lo tanto, cada vez que el usuario malicioso solicitara los datos de los contactos de la agenda del dispositivo víctima del ataque supondría a su dueño un coste medio aproximado de 8.62 euros.

En las pruebas realizadas sobre una PDA HTC P3300 se ha comprobado que efectivamente el dispositivo (una vez el troyano instalado) cuando es atacado no avisa de ninguna forma de la entrada o salida de información vía SMS, es decir, no guarda copia de dichos mensajes en las bandejas de entrada o salida de SMS. Sin embargo, cuando recibe un mensaje del usuario malicioso con las órdenes al troyano se enciende la pantalla aunque sigue sin mostrar nada.

2.4 Solución propuesta

Hemos implementado un troyano que ha permitido fácilmente conseguir información sobre los contactos de un dispositivo infectado. También hemos comprobado que el robo de información pasa totalmente inadvertido para el usuario del terminal atacado.

Por tanto, decidimos programar un servicio que utilice los "EventListener" o escuchadores de eventos (de SMS, MMS, GPS, Bluetooth,...) para detectar los accesos a una lista de recursos potencialmente peligrosos si resultan ser objetivo de algún ataque. En el caso de nuestra demostración, se utiliza el evento de recibir SMS que nos proporciona Microsoft Windows Mobile 6 SDK (*MessageReceived()* del objeto de la clase *MessageInterceptor*) para detectar los accesos vía SMS que se producen en nuestro sistema (recordemos que en el programa de prueba la PDA no informaba de los SMS llegados con información para el troyano), y así, avisaremos al usuario de que un nuevo mensaje ha llegado sin importar su contenido o procedencia.

Cuando llegue un nuevo SMS avisará al usuario de la llegada dando información adicional como el número de su remitente y los primeros caracteres del mensaje. A su vez, se dará la oportunidad al usuario de aceptarlo (pasaría al buzón de mensajes recibidos) o eliminarlo según crea conveniente.

Esta es sin duda una solución sencilla y flexible con la que podemos realizar un control más exhaustivo de la entrada y salida de información desde nuestro dispositivo. Sin embargo, se deja al usuario que sea él mismo, basándose en su experiencia y en el contenido del SMS, el que tome la decisión de aceptar el envío o recepción de un mensaje.

3 Conclusiones y trabajos futuros

Actualmente la mayoría de usuarios de dispositivos móviles, al contrario de los usuarios de PC, creen no tener la necesidad de tener instalados en sus máquinas un programa antivirus u otras aplicaciones para proteger sus dispositivos de posibles infecciones. Sin embargo, debido al crecimiento exponencial de los servicios y capacidades de estos dispositivos y a la gran cantidad de información comprometida que contienen se hace casi indispensable tomar algún tipo de medida contra un posible ataque.

En este artículo hemos abordado el caso de ataques a terminales con troyanos, es decir, vulnerabilidades capaces de instalarse en el dispositivo del usuario atacado, captar parte de su información privada y enviarla para un futuro uso malicioso, teniendo en cuenta durante todo el proceso que el usuario no llega a ser consciente del robo y que en ningún momento se daña la funcionalidad del dispositivo.

Se ha desarrollado una demostración en la que se llevaba a cabo el robo de parte de la información de los contactos de la agenda de un dispositivo móvil. Esta demostración se realizó en un principio en los simuladores que proporciona Microsoft Windows Mobile 6 SDK para posteriormente ejecutarlo en una PDA. La solución propuesta en el artículo propone un mayor control en el trasiego de información enviada y recibida desde el dispositivo.

Como trabajos futuros, convendría estudiar el comportamiento de troyanos a la hora de atacar otros servicios de un terminal como Bluetooth, GPS o correo electrónico. Y no sólo con troyanos sino con otros tipos de vulnerabilidades como gusanos o virus que ya podrían afectar a la funcionalidad (software o hardware) del dispositivo.

4 Agradecimientos

Este trabajo ha sido parcialmente subvencionado por los proyectos FAMENET-InCare (TSI2006-13390-C02-02) del Ministerio de Educación y Cultura Español y CUBICO (P06-TIC-02141) de la Junta de Andalucía.

Referencias

[Abelson *et al.*, 1985] Harold Abelson, Gerald Jay Sussman, and Julie Sussman. *Structure and Interpretation of Computer Programs*. MIT Press, Cambridge, Massachusetts, 1985.

[Rebollal *et al.*, 2008] Eduardo López Rebollal, Javier Jaraiz Sánchez. *Seguridad en entornos móviles corporativos*. Revista SIC, Nº 79 Abril 2008.

[Reynolds *et al.*, 2008] Franklin Reynolds. *Camera Phones: A Snapshot of Research and Applications*. IEEE Pervasive Computing, Vol. 7 Nº 2, Abril 2008

[Roy Want, 2008] Roy Want. *You are your cell phone*. IEEE Pervasive Computing, Vol. 7 Nº 2, Abril 2008

[Bose *et al.*, 2006] Abhijit Bose and Kang G. Shin. *On Mobile Viruses Exploiting Messaging and Bluetooth Services*. IEEE 2006

[Bose and Shin *et al.*, 2006] Abhijit Bose, Kang G. Shin. *Proactive Security For Mobile Messaging Networks*. WiSe'06, September 29, 2006.

[Haataja *et al.*, 2005] Haataja, K., "*Two practical attacks against Bluetooth security using new enhanced implementations of security analysis tools*", CNIS 2005, Arizona, USA, November 14-16, 2005