Consideraciones de seguridad en terminales 'smartphone'

Los terminales de telefonía móvil han pasando de ser meros utensilios para conversar e intercambiar mensajes SMS, a convertirse en micro-ordenadores con capacidades avanzadas de cómputo, que proporcionan acceso a Internet, correo-e, intranets, y todo tipo de documentos, así como muchas otras funciones por venir. Los denominados *smartphones*, están abriendo una nueva ventana a las TI que las empresas pueden y deben aprovechar para extender los servicios de información a empleados móviles, pero esta nueva tecnología debe ser integrada en las compañías de forma segura, minimizando el riesgo que actualmente generan y siempre cubriendo una necesidad de negocio.

Miguel Ángel Domínguez

Sin duda los *smartphones* abren una nueva ventana a las TI que las empresas pueden y deben aprovechar para extender los servicios de información a empleados móviles. Symbian, Windows Mobile Smartphone y Blackberry son tres sistemas operativos que han permitido la evolución de la telefonía móvil basada en *smartphone*.

A modo de breve repaso cabe precisar que Symbian es una empresa participada por Nokia, Ericsson y Motorola. Los *smartphones* basados en Symbian están liderados por Nokia y SonyEricsson; por su lado, Windows Mobile Smartphone está basado en Windows CE y posee una arquitectura similar a otros sistemas Windows (registro, Pocket IE, Word Mobile), teniendo en mente la restricciones de memoria y capacidad de cómputo de los terminales. Por su parte, Blackberry –creado por RIM (Research In Motion)–, está formado por una plataforma que incorpora los dispositivos *smartphone*, software de escritorio y un servidor Blackberry Enterprise Server (BES) como nodo central de la arquitectura.

Blackberry está orientado principalmente a entornos empresariales, mientras que Symbian y Windows Mobile fueron introducidos en entornos de usuario final, y posteriormente se han ido adaptando al mercado empresarial a través de la incorporación de soluciones de operador y de terceras empresas que proporcionan integración con software de acceso a datos y servicios corporativos. Estos sistemas operativos proporcionan servicios de comunicaciones (GSM, GPRS, TCP/IP, WAP y Bluetooth), y *frameworks* para el desarrollo de aplicaciones de usuario (correo-e, calendario, ...) y de terceros en lenguajes de programación como C++, J2ME, o C#. En definitiva, favorecen la integración de los dispositivos móviles como instrumentos de trabajo para empleados móviles, con las ventajas de negocio e inconvenientes de seguridad que esto implica. **(Figura 1)**

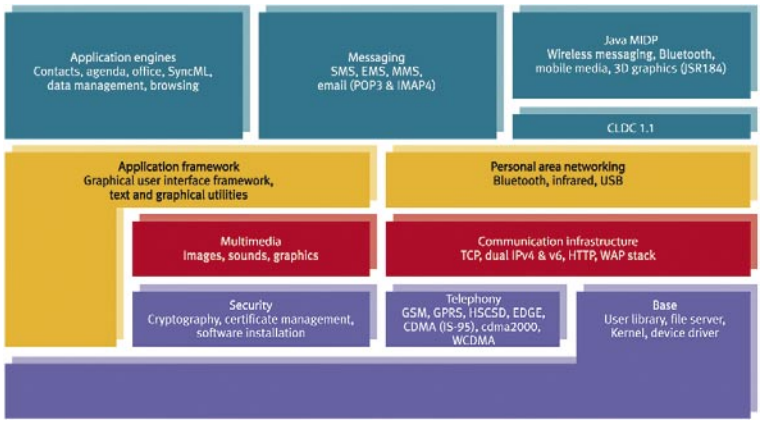

Figura 1: Arquitectura Symbian Smartphone

El desarrollo de aplicaciones para terminales *smartphone* crea un nuevo nicho de mercado para empresas de software ante la necesidad de integrar dichos dispositivos dentro de los procesos de negocio de las compañías. Esto, a su vez, introduce riesgos relacionados con la seguridad en la programación de estas aplicaciones.

> ***El desarrollo de aplicaciones para terminales smartphone crea un nuevo nicho de mercado ante la necesidad de integrar dichos dispositivos dentro de los procesos de negocio de las compañías, pero a su vez introduce riesgos relacionados con la seguridad en la programación de estas aplicaciones.***

En este ámbito conviene señalar que un concepto importante de seguridad para el software es la validación y certificación de código a través de firmas digitales. Este concepto, llamado de diferentes formas dependiendo del fabricante, lenguaje de programación y proceso de verificación de código que se realice (Symbian Signed[1], JavaVerified[2] o M2M[3]), permite a los usuarios validar que las aplicaciones descargadas de Internet e instaladas en sus *smartphones*, provienen de fuentes fiables.

Así, el proceso seguido por Symbian Signed y Java Verified consiste en una auditoría del código por parte de una empresa evaluadora y, una vez aprobado el código, éste es firmado digitalmente por una autoridad de certificación para garantizar su autenticidad e integridad. Microsoft, con M2M (Mobile2Market), permite certificar aplicaciones como diseñadas para Windows Mobile, proporcionando servicios de firma digital, en tanto que RIM, por su parte, también incorpora el concepto de firma digital en aplicaciones Blackberry, con la diferencia de que estas firmas son pistas de auditoría de quien desarrolló la aplicación, pero no se realiza ninguna verificación o auditoría del código.

J2ME[4] (Java 2 Micro Edition) es la plataforma de programación adoptada por la mayoría de desarrolladores de aplicaciones para *smartphone*. J2ME, presente en Symbian, Windows Mobile y Blackberry, facilita la incorporación de seguridad a las aplicaciones mediante soporte a SSL y criptografía. El modelo de seguridad de J2ME se basa a nivel de máquina virtual, en el verificador de clases (las aplicaciones no pueden dañar el dispositivo), y a nivel de CDLC (*Connected Limited Device Configuration*) y MIDP (*Mobile Information Device Profile*), en la *sandbox* (ejecución en un entorno controlado). Cabe destacar que este es un modelo de seguridad granular que define conjuntos de permisos y dos dominios de seguridad: Untrusted (*sandbox*) y Trusted (mediante firmas digitales). JavaVerified es el proceso para firmar los MIDlets (aplicaciones desarrolladas con MIDP) y lo gestiona el UTI (*Unified Testing Initiative*) formado por Sun, Motorola, Nokia, Siemens y SonyEricsson. Según este modelo,

Tipología de ataques Bluetooth[6]

Emparejamiento *(Pairing y Bonding)*

Problemas de implementación en los procesos de autenticación y autorización que permiten el robo de información, realizar llamadas o enviar SMS/MMS.

BlueBug

Descarga no autorizada de información, envío y lectura de SMS, establecimiento o redireccion de llamadas, etc., mediante el establecimiento de una conexión serie plana y explotando los comandos AT, sin pasar por el protocolo OBEX.

BlueJacking

Envío anónimo de mensajes usando Bluetooth. Se basa en abusar del protocolo de emparejamiento (*pairing protocol*). El problema de seguridad surge cuando un atacante (*bluejacker*), utilizando esta técnica, consigue que la victima finalice el proceso de emparejamiento, y por tanto tener acceso a la información del dispositivo.

BlueSnarfing

Se conecta al dispositivo sin alertar al propietario de la petición y consigue acceso a partes de los datos almacenados (agenda, calendario,...)

Criptografía

Antes de poder establecer una comunicación, dos dispositivos Bluetooth han de intercambiar una clave secreta generada a partir de que en ambos se teclee idéntico PIN. El sistema engaña al dispositivo víctima haciéndole creer que ha perdido la clave, forzando así al comienzo de una nueva comunicación siempre que se desee.

Figura 2: Ataques a Bluetooth

sólo aplicaciones firmadas pueden acceder a funciones y APIs privilegiadas en el *smartphone.*

Todas estas características generan nuevas oportunidades y mejoran los procesos de negocio, pero a la vez introducen amenazas que ponen en peligro tanto el terminal *smartphone* como los recursos de información de la compañía, ya que aparecen nuevos puntos de entrada para ataques por parte de *hackers* y todo tipo de código malicioso.

En este escenario, los problemas de seguridad se pueden englobar en varios aspectos:

– Errores de desarrollo del software por parte de fabricantes, operadores y terceros que introducen agujeros de seguridad.

– Errores u omisiones en la configuración de las plataformas de seguridad por parte de administradores que abren puertas a atacantes externos o internos.

– Desconocimiento de los peligros de seguridad que pueden conllevar ciertas acciones (p.e., comerciales con *smartphone* acceden al correo corporativo y descargan aplicaciones de Internet sin firmar y que contienen virus y troyanos).

Estos riesgos pueden suponer pérdidas económicas para la empresa debido a fraudes (envío de SMS/MMS, llamadas,...) o a robo/alteración de información sensible y/o personal (correo-e, agenda, etc.), efectos estos que repercuten en el deterioro de la imagen de la compañía, en pérdida de competitividad o incluso puede conllevar sanciones legales.

El primero de estos peligros lo encontramos en la implementación incorrecta de la pila Bluetooth[5] en terminales de Nokia y SonyEricsson (p.e. Nokia 6310i o SonyEricsson T610). Estos errores en el desarrollo introducen vulnerabilidades que han permitido acceso a funciones y datos privados en los terminales Smartphone. La figura 2 muestra algunos ataques que afectan a dispositivos con Bluetooth. **(Figura 2)**

J2ME no está exenta de problemas de seguridad. En octubre de 2004, se publicó una alerta comunicando múltiples vulnerabilidades en J2ME[7], vinculadas a errores de implementación en el verificador de clases de la máquina virtual (KVM) que incorporan dispositivos *smartphone* con soporte a Java. Estas vulnerabilidades permiten a un MIDlet malicioso evadir las medidas de seguridad impuestas por la *sandbox* y el verificador de clases y, por tanto, acceder al dispositivo ejecutando acciones no autorizadas.

La política de utilización y gestión de los terminales smartphone deberían considerar aspectos relacionados con el uso de software de administración para controlar los dispositivos de forma centralizada y en concordancia con la política de seguridad corporativa.

Además de los problemas en el desarrollo de plataformas y aplicaciones, hay que tener en cuenta que muchos usuarios (directivos, comerciales, operarios, etc.) tienen escaso conocimiento de la tecnología subyacente y son víctimas a diario de ataques de ingeniería social por parte de virus, gusanos y troyanos (*malware*). En junio del pasado año apareció el primer gusano capaz de atacar teléfonos con Symbian. Denominado Cabir[8]: utiliza Bluetooth para propagarse y llega por MMS en forma de un fichero llamado caribe.sis. Cuando el usuario lo ejecuta, y se instala en el dispositivo, el gusano se activa. Actualmente existen múltiples mutaciones de este gusano que han aumentado su virulencia y métodos de propagación.

Por tanto, no es en absoluto descabellado pensar que el crecimiento mundial de la telefonía móvil facilita la posibilidad de crear un gusano capaz de propagarse a todos los sistemas vulnerables causando el máximo daño antes de poder reaccionar (Warhol Worm). Viene al caso recordar la premonitoria frase de Andy Warhol: *"In the future, everybody will have 15 minutes of fame".*

En Windows Mobile, el virus WinCE4.Duts[9], es una prueba de concepto que muestra los problemas de seguridad de este sistema operativo. Entra otras cosas, permite ejecutar un *keylogger* (captura teclas pulsadas; p.e., contraseñas), el control remoto del dispositivo y la ocultación de procesos. Aunque Pocket IE está más limitado en funcionalidad que su versión para PC, han aparecido vulnerabilidades de DoS y acceso a ficheros locales, y es de esperar que con el incremento de funcionalidades las vulnerabilidades vayan en aumento.

En el esquema de la plataforma Blackberry, el servidor BES es el nodo central y, por tanto, supone un punto único de fallo en la arquitectura. Es primordial proteger los terminales *smartphone*, pero también es imprescindible que se proteja el servidor BES, los sistemas de mensajería y datos corporativos. RIM hizo especial hincapié en que los sistemas de seguridad incorporados en Blackberry

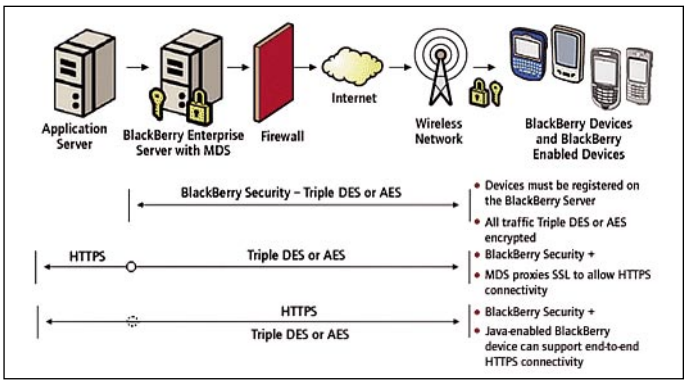

Figura 3: Arquitectura Blackberry

fuesen validados y certificados por normativas de seguridad americanas (FIPS140-2, DoD), así como analizados por empresas del sector especializadas en *hacking* ético. Este hecho demuestra la implicación de RIM en el diseño y desarrollo de un sistema operativo con altas garantías de seguridad.

De todas formas esto no es suficiente; se deben utilizar sistemas de protección perimetral (cortafuegos, IDS, etc.), configurando (control de contraseñas, cifrado de datos, etc.), monitorizando y manteniendo (aplicación de parches) de forma segura los diferentes elementos en la arquitectura para permitir únicamente el acceso a datos y recursos de información a terminales autorizados. **(Figura 3)**

Como ninguno de los sistemas operativos que se han descrito está libre de problemas de seguridad ya sea por una u otra causa, las organizaciones deben ser conscientes de que para poder aprovechar las ventajas que proporcionan los dispositivos *smartphone* y mejorar sus procesos de negocio, es necesario establecer sistemas seguros que salvaguarden sus recursos de información.

De los tres sistemas operativos descritos, Blackberry proporciona capacidades integradas de seguridad, a través de canales cifrados, administración centralizada de terminales con posibilidad de eliminar datos en caso de robo o pérdida del *smartphone*, y protección del correo con cifrado y firma digital S/MIME. En los escenarios españoles, la gran mayoría de las empresas han apostado por terminales Blackberry para proporcionar a sus empleados servicios de acceso a mensajería e información corporativa.

No obstante, Symbian, que es el sistema instalado en el mayor número de terminales *smartphone* (más del 90% en EMEA[10]), está cubriendo la necesidad del mercado empresarial; por un lado, mediante el rediseño de su arquitectura de seguridad en la versión 9.0, que incorpora la nueva plataforma de seguridad PlatSec –basada en potenciar la detección de intentos de acceso no autorizados al hardware, software y datos del teléfono, así como prevenir que los programas actúen de forma no aceptable, ya sea por error o intencionadamente *(malware)*–, y por otro, mediante acuerdos de colaboración con socios tecnológicos centrados en la protección como F-Secure (para software antivirus), Certicom y PointSec (con sus productos de VPN y criptografía, que proporcionan seguridad de extremo a extremo y protección de datos), e incluso Microsoft, con la que en el pasado marzo firmó un acuerdo para incorporar soporte al protocolo ActiveSync de Microsoft Exchange Server 2003.

La tecnología se está adaptando a las necesidades de las empresas incorporando productos de seguridad VPN para protección del canal extremo-a-extremo, cortafuegos personales, antivirus, antispam y cifrado... muchos de ellos aún en fases beta.

Todos estos acuerdos permiten incorporar servicios que las empresas pueden utilizar para conectar a sus empleados de forma segura a los servicios TI corporativos. Microsoft, con su versión de Windows Mobile 5.0, se acerca así mucho más al sector empresarial, añadiendo mayores capacidades de acceso seguro y eficaz a la información (autorización, cifrado extremo a extremo, etc..).

Como se ha señalado, la tecnología se está adaptando a las necesidades de las empresas incorporando productos de seguridad VPN para protección del canal de comunicación extremo-a-extremo, cortafuegos personales, antivirus y anti*spam* (F-Secure, Symantec, Trend Micro, Kaspersky..., muchos de ellos aún en fases beta) y cifrado de datos. Estos '*softwares*' permiten reducir algunos de los riesgos de seguridad que se han comentado (virus, troyanos, privacidad e integridad de la información). Pero, ¿qué deben hacer las empresas para adaptarse a la tecnología de los terminales *smartphone* de forma que no se ponga en peligro la continuidad del negocio? Aquí se sugieren algunas:

– Adaptar la política y procedimientos de seguridad introduciendo el nuevo canal de comunicación, determinando los requerimientos de seguridad y las medidas que deben implementarse para salvaguardar los activos de la compañía.

– Implantar estos mecanismos de seguridad para combatir los nuevos peligros y extender las protecciones actuales para abarcar los puntos de entrada que suponen una amenaza a la disponibilidad de los recursos de información y, en definitiva, a la continuidad del negocio.

– Revisar y mantener la plataforma de forma periódica y en concordancia con los objetivos del negocio.

– Formar y concienciar a los empleados (seminarios, mesas de trabajo, avisos, etc.) sobre la correcta utilización de la plataforma de terminales *smartphone*.

Asimismo, la política de utilización y gestión de los terminales *smartphone* deberían considerar aspectos relacionados con:

– No instalar software sin verificar antes que está libre de virus (código firmado).

– No abrir mensajes de correo-e o MMS en los que no se confía o que provienen de fuentes desconocidas.

– No habilitar Bluetooth si no es imprescindible y tenerlo en modo visible el tiempo mínimo necesario.

– Sólo aceptar comunicaciones Bluetooth de terminales en los que se confía.

– Aplicar todas las actualizaciones disponibles para solventar deficiencias en el software base incorporado por el fabricante y el operador.

– No permitir la instalación de aplicaciones que no estén homologadas por la empresa (aplicaciones que hayan sido revisadas y aprobadas por el departamento de TI e incluso por dirección).

– No permitir o bloquear la descarga de aplicaciones desde Internet.

– Utilización de software de administración para controlar los dispositivos *smartphone* de forma centralizada y en concordancia con la política de seguridad corporativa. ■

Miguel Ángel Domínguez Torres
Auditor/Consultor en Seguridad
CISSP, OPST
INTERNET SECURITY AUDITORS
mdominguez@isecauditors.com

REFERENCIAS

(1) Symbian Signed – http://www.symbiansigned.com
(2) Java Verified, UTI (Unified Testing Initiative) – http://javaverified.com/index.jsp
(3) M2M - http://msdn.microsoft.com/mobility/windowsmobile/partners/mobile2market/default.aspx
(4) J2ME (Java 2 Micro Edition) - http://www.microsoft.com/windowsmobile/smartphone/default.mspx
(5) Bluetooth - http://www.bluetooth.com http://www.kjhole.com/Standards/BT/BTdownloads.html
6) Ataques a la pila Bluetooth y Vulnerabilidades en Terminales Nokia y SonyEricsson http://www.thebunker.net/security/bluetooth.htm http://trifinite.org/ http://www.securityfocus.com/bid/13854/info http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0143 http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0681 http://www.securityfocus.com/bid/13782/info
(7) Vulnerabilidades en Dispositivos J2ME - http://www.securityfocus.com/bid/11461/info http://packetstormsecurity.com/hitb04/hitb04-adam-gowdiak.pdf
(8) Cabir - http://www.f-secure.com/v-descs/cabir.shtml
(9) WinCE4.Duts - http://www.vsantivirus.com/dust-a.htm
(10) Previsiones del mercado Smartphone- http://www.pdastreet.com/articles/2004/6/2004-6-3-Overview-Symbian-Smartphone-print.html