PUNTO SEGURIDAD, SEGURIDAD EN TIC | NÚMERO 7 | AGOSTO 2010 | ISSN EN TRÁMITE | REVISTA BIMESTRAL

Dispositivos móviles

Editorial

La revista **.Seguridad** como un esfuerzo de la Subdirección de la Seguridad de la Información por crear una cultura de la seguridad en cómputo, vuelve con la publicación de su número 7.

Esta edición está dedicada a la seguridad en los dispositivos móviles. La mayoría de nosotros ya contamos con algún tipo de dispositivo móvil que nos permiten no solo la comunicación a distancia, sino también el manejo de datos en grandes cantidades. El hecho de que gran parte de los actuales usuarios de Internet naveguen a través de estos dispositivos así como de la cantidad de información manejada en ellos, hace que los maleantes se vean atraídos a atacarlos. En este número te mostramos algunos riegos del uso de los dispositivos móviles así como recomendaciones que te hacemos para defenderte. Esperamos disfrutes de esta edición.

Rocío del Pilar Soto Astorga
Departamento de Seguridad en Cómputo

Anaid Guevara Soriano

¿Qué es un dispositivo móvil?

Los dispositivos móviles son aparatos de tamaño pequeño que cuentan con características tales como las mostradas en la Figura 1:

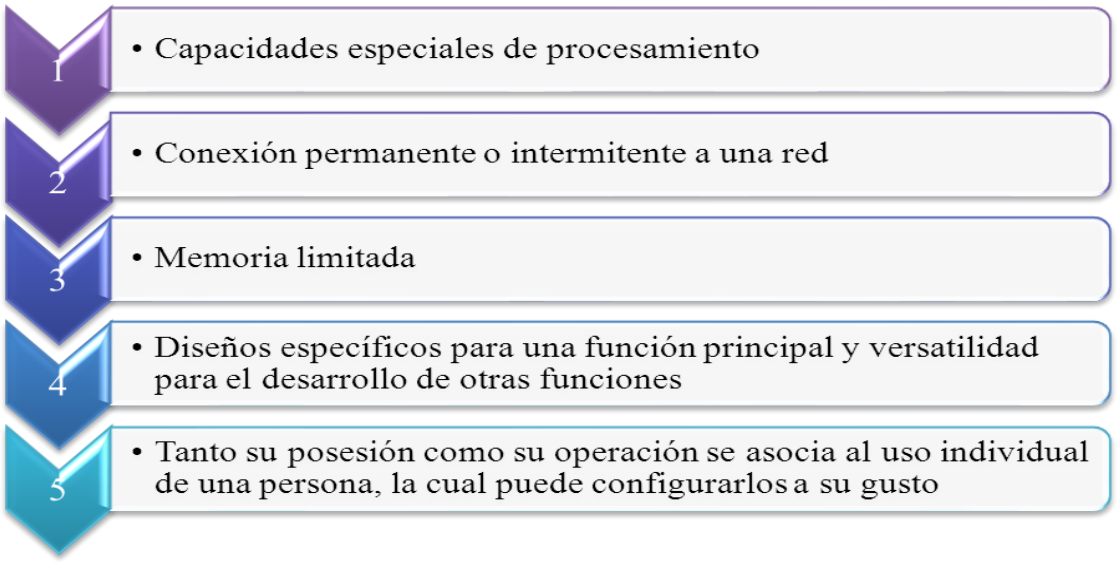

Fig. 1. Características de los dispositivos móviles

Una característica importante es el concepto de movilidad, los dispositivos móviles son pequeños para poder portarse y ser fácilmente empleados durante su transporte. En muchas ocasiones pueden ser sincronizados con algún sistema de la computadora para actualizar aplicaciones y datos.

Otra característica es el que se pueda conectar a una red inalámbrica, por ejemplo, un teléfono móvil, los comunicadores de bolsillos o PDAs[1]. Este tipo de dispositivos se comportan como si estuvieran directamente conectados a una red mediante un cable, dando la impresión al usuario que los datos están almacenados en el propio dispositivo.

[1] *Personal Digital Assistant* o Ayudante Personal Digital, es un dispositivo portátil que combina las funciones de una PC con teléfono/fax, Internet y conexiones de red.

Los conceptos de móvil y sin cables muchas veces se confunden. Un PDA con datos en él y aplicaciones para gestionarlos, puede ser móvil pero no tiene por qué ser inalámbrico, ya que puede necesitar un cable para conectarse a la computadora y obtener o enviar datos y aplicaciones.

Por otro lado, un teléfono móvil equipado con un pequeño navegador puede hacer uso de Internet (ver figura 2b), considerándose inalámbrico, pero no móvil ya que no dispone de un *valor agregado que aporte como característica extra alguna función en las aplicaciones del dispositivo cuando éste no está conectado a otros sistemas tales como: Computadoras, cámaras*, etc. Si el PDA es capaz de conectarse a una red para obtener datos "en medio de la calle", entonces también se considera inalámbrico.

Fig. 2a. Ejemplo de un dispositivo móvil no inalámbrico

Fig. 2b. Dispositivo inalámbrico que no dispone de un valor añadido, no aporta ninguna función cuando no está conectado a otros sistemas.

Algunas de las características que hacen que estos dispositivos sean diferentes de las computadoras se muestran en la Figura 3:

Fig. 3. Características de los dispositivos móviles

¿Cuáles son los dispositivos móviles?

Algunos de los ejemplos de estos dispositivos son los siguientes:

- Paginadores.
- Comunicadores de bolsillo.
- *Internet Screen Phones.*
- Sistemas de navegación de automóviles.
- Sistemas de entretenimiento.
- Sistemas de televisión e Internet (WebTV).
- Teléfonos móviles.
- Organizadores y asistentes personales digitales (*Personal Digital Assistant*).

El mundo de "lo móvil" está de moda, no hay más que visualizar a nuestro alrededor para darnos cuenta. Un ejemplo muy común son los usuarios de telefonía móvil debido a que éstos se han multiplicado hasta límites no previstos, convirtiéndose en el mayor y más difundido exponente de ese mercado. No obstante, no es sólo el teléfono, también están los reproductores MP3, las consolas de juegos, las agendas y asistentes personales y las computadoras portátiles o mejor conocidas como laptops.

A ese mundo en miniatura hay que añadir, un nuevo integrante que, en los últimos años, está experimentando un crecimiento considerable. Hablamos de los sistemas informáticos móviles, conocidos con términos como *palm-size pc, handheld, pocket* y similares. Sus características técnicas limitan hasta cierto punto las posibilidades de estos sistemas respecto a un equipo de cómputo corriente, pero hay que tener en cuenta que muchos de ellos tienen una potencia de procesamiento y capacidad similares a los equipos de sobremesa de hace pocos años. La diferencia clara y a la vista, es que esa potencia y capacidad ahora puede transportarse en un bolsillo.

Evolución

Tanto los dispositivos como los sistemas operativos que hacen posible su funcionamiento han ido evolucionando según las necesidades de los usuarios finales. En la actualidad existen principalmente dos tipos de dispositivos móviles: los que cuentan con un teclado y aquellos que están basados en una pantalla táctil, para la introducción de datos.

Los teclados de sistemas móviles son, necesariamente, de tamaño reducido, lo que pudiera hacer que su uso no sea demasiado cómodo, aunque todo depende de nuestras manos y dedos (muchas personas se encuentran con el problema de no poder evitar pulsar varias teclas al mismo tiempo, ya que éstas son más pequeñas que sus propios dedos).

Al sustituir todo el teclado por un lápiz que se utiliza sobre la propia pantalla, el peso y tamaño del dispositivo se pueden reducir, así como el consumo de energía, lo cual contribuye a la mayor duración de las baterías. Se plantea, sin embargo, el problema de la introducción de datos. Existen básicamente dos opciones: utilizar un teclado en pantalla, sobre el cual se puede ir pulsando con el propio lápiz, o bien reconocer la escritura directa del usuario.

Uno de los mayores problemas que plantean los dispositivos de tamaño pequeño, como los PDA, es el mecanismo a utilizar para que el usuario pueda introducir información. Si las dimensiones no son suficientes para incluir un teclado útil, las soluciones posibles son varias: reconocimiento de escritura, un teclado en pantalla o incluso un teclado externo.

La posibilidad de conectar un teclado externo al PDA, aunque factible y en existencia, no resulta lo más adecuado cuando lo que se quiere es movilidad, puesto que habría que acarrear no sólo con el dispositivo principal sino, además, con el teclado y posiblemente los cables de conexión. Si necesitamos un teclado físico para introducir datos con cierta agilidad, seguramente la mejor opción es optar por un PDA que lo incluya como parte integral del dispositivo.

El teclado en pantalla, en el que se pulsa con la punta de un pequeño lápiz, es una eficaz alternativa al teclado físico representando, un considerable ahorro de espacio, peso y, en menor medida, energía.

Así mismo, también se tiene el método que podría considerarse más natural: la escritura directa sobre la pantalla del dispositivo. Para que esto sea posible, no obstante, el PDA debe contar con un software de reconocimiento de caracteres suficientemente eficiente ya que, de lo contrario, se perderá más tiempo en efectuar correcciones que en la propia introducción de datos.

La familia de dispositivos que utiliza el sistema Palm OS (sistema operativo hecho por *PalmSource*, Inc. para computadoras de mano (PDAs) fabricados por varios licenciatarios.) se caracteriza por reconocer un conjunto de caracteres bien definido, conocido como Graffiti, que el usuario del PDA debe aprender. Se trata de un alfabeto sencillo que contribuye a que el *software* de reconocimiento sea más efectivo al haber menos posibilidades de error. La mayoría de los Palm OS acepta la introducción de caracteres escritos en pantalla sólo en una reducida área de ésta.

En contraposición a las Palm, otros dispositivos, como los Pocket PC, tienen un *software* de reconocimiento de la escritura natural, lo que significa que no hay necesidad de aprender ningún conjunto de trazos. La efectividad depende de la precisión con que dicho *software* es capaz de reconocer la escritura de cada usuario.

Referencias:

http://leo.ugr.es/J2ME/INTRO/intro_4.htm
http://www.alegsa.com.ar/Dic/dispositivo%20movil.php
http://www.slideshare.net/Jmaquino/dispositivos-moviles
http://www.idg.es/pcworld/De-Palms_-Pockets-y-otros_Informatica-movil-_I_/art113968.htm

Alejandro Reyes Plata

Los grandes avances tecnológicos de los últimos años han hecho posible que en la actualidad podamos manejar una gran cantidad de información en dispositivos que caben en la palma de la mano. De esta forma, estos nuevos aparatos han permitido que el hombre se desempeñe de una manera más eficiente y productiva en varios aspectos de su vida.

Los dispositivos móviles han evolucionado de tal forma que algunos los consideran computadoras de bolsillo debido a sus características y funciones. Estas características han provocado que los usuarios se vean atraídos a la posibilidad de manejar muchos aspectos de su vida diaria a través de los dispositivos móviles, debido a que son una herramienta muy poderosa que permite realizar acciones como navegar en Internet a grandes velocidades, manejo de correo electrónico, chatear, revisar tus redes sociales, tomar fotografías y video con una gran calidad, juegos, agenda electrónica, GPS, ver televisión y algunos incluso, permiten levantar un propio servidor Web. Es decir, la cantidad de aplicaciones que estos aparatos poseen, superan en gran medida las expectativas que se tenían de ellos. Para personas dedicadas a los negocios, los dispositivos móviles son un arma muy poderosa, el aumento en la capacidad de almacenamiento de los móviles actualmente supera los 16 Gigas, lo cual permite almacenar mayor cantidad de información de todo tipo tanto personal como laboral.

Ahora debemos detenernos a pensar en lo que pasaría si alguien con intensiones nada éticas y maliciosas se llegará a apoderar de nuestro dispositivo móvil, si somos de las personas que acostumbramos sacarle el mayor provecho a nuestro móviles seguramente corremos un gran riesgo. Supongamos el hipotético caso en el que extraviamos nuestro dispositivo móvil y una persona que se dedica a la extorsión lo encuentra. Al revisar nuestro aparato puede ver mensajes de texto que describen mucho de nuestra personalidad, observa las imágenes que almacenamos las cuales le brindan información de los lugares que visitamos, nuestras amistades, la ropa que vestimos, nuestros gustos, el auto que manejamos el lugar donde vivimos, etc. No es difícil pensar la enorme utilidad que esta información representa para secuestradores o extorsionadores.

Ahora supongamos que somos una persona de negocios y que en nuestro móvil, manejamos información de aspectos financieros críticos relacionados con la empresa donde laboramos, información tal como datos de trabajadores, créditos, contratos realizados o por realizar, contactos de altos directivos, supongamos que la empresa de la competencia contrata a un *cracker* (persona que utiliza sus conocimientos informáticos con fines de lucro) para acceder a al información de nuestro dispositivo, si manejamos información muy importante de la empresa esta puede estar en grave riesgo. Y no solo hablamos de pérdidas económicas, sino del riesgo real para la subsistencia de la empresa y la continuidad del negocio, y hasta responsabilidades legales

derivadas en caso que un dispositivo contenga información confidencial, como lo son los registros médicos.

En la actualidad es común que las parejas se tomen fotografías o videos los cuales comparten como muestra de su amor, amistad, etc. Ahora imagínense el escenario en el que los videos o fotografías de nuestro móvil son extraídos por alguien a quien no le somos de su agrado y coloca estas imágenes o videos en sitios Web. En poco tiempo todas las personas de nuestro círculo social se enteran de tan fatal suceso, si estamos en la escuela probablemente no queramos asistir jamás, peor aun si estamos en el trabajo, probablemente renunciaríamos o cambiaríamos de área a Alaska.

En fin, miles de posibles escenarios pueden ocurrir si nuestra información llega a manos no adecuadas ni éticas. Si nos ponemos a pensar en la posibilidad de que ocurran estos escenarios nos daremos cuenta de que es muy alta. Los dispositivos móviles ofrecen una nueva forma de relacionarse con el mundo al compartir fotos, vídeos, ver antiguos compañeros, etc. Pero también existe la parte oscura, chantajes, extorsiones, amenazas, secuestros, acosos, son solo algunos de los riesgos a los que estamos expuestos al manejar tanta información concentrada en un solo punto.

Recomendaciones:

A continuación te mencionaremos algunas prácticas de seguridad que esperemos te sean de utilidad:

- Asegurarse de que nuestro dispositivo móvil tenga habilitado el uso de contraseñas, estas deben de ser robustas y no se deben de compartir con alguien más.
- Considerar el cifrado tanto del dispositivo móvil como de las tarjetas de almacenamiento.
- Si el dispositivo móvil utiliza el *software* "Windows Mobile 5.0" como sistema operativo es posible aprovechar el complemento del "pack" de mensajería y seguridad (MSFP), el cual permite la protección de los siguientes datos:
  - Restablecimiento del dispositivo móvil tras cierto número de intentos de inicio de sesión fallidos
  - Borrado remoto de los datos y restablecimiento del dispositivo a su estado original
- No compartir fotografías, videos, mensajes, etcétera con desconocidos, ni almacenar fotografías o videos que den información acerca de nuestra persona y seres queridos.
- Desactivar el dispositivo *bluetooth* cuando no se esté utilizando, ya que representa una puerta en nuestros dispositivos por donde pudieran acceder intrusos.
- Tener extremo cuidado al conectar nuestro móvil a redes públicas abiertas, pues es en estas redes en donde ocurre la mayor cantidad de ataques hacia nuestra información.

Referencias:

http://www.slideshare.net/chemai64/seguridad-en-dispositivos-mviles
http://www.techweek.es/seguridad/analisis/1006536004801/cuidado-redes-sociales-cloud-computing.1.html
http://blogs.sanchez-crespo.com/ascl/2009/02/09/dispositivos-moviles-%C2%A1que-peligro/
http://blog.coompra.com/2009/10/sexting-y-el-peligro-de-los-moviles/

Rosa Xochitl Sarabia Bautista

La primera vez que se dio a conocer un teléfono celular fue en 1973 por Martin Cooper de Motorola, con un peso de 2 kilos. A finales de 2009, el número de teléfonos celulares registrados en el mundo se estimó en 4.6 mil millones, reflejando la manera en que se ha masificado su uso hoy en día, prácticamente todos tienen uno: desde adultos y adolescentes hasta niños de 8, 9, 10 años.

¿Qué riesgos presentan los teléfonos celulares?

Así como la tecnología ha avanzado, los celulares han evolucionado y ya no son sólo teléfonos, los equipos actuales soportan servicios y accesorios adicionales, como los mensajes de texto, correo electrónico, acceso a Internet, juegos, *Bluetooth*, infrarrojo, cámara, mensajes multimedia, reproductor MP3, radio y GPS. Aunque estas son características que pueden resultar útiles y convenientes, los atacantes pueden intentar aprovecharse de ellas. Como resultado, un atacante puede ser capaz de lo siguiente:

- *Uso indebido del servicio*. La mayoría de los planes de teléfonos celulares tienen un número limitado de mensajes de texto para enviar y recibir. Si un atacante utiliza el *spam*, te envía de forma masiva mensajes de texto, se te podrían cobrar con cargos adicionales. Un intruso también podría infectar tu teléfono con código malicioso para poder usar tu servicio. Debido a que el contrato está a tu nombre, tú serás responsable de los cargos.
- *Atraerte a sitios web maliciosos*. Ahora los atacantes están enviando mensajes de texto a teléfonos celulares. Estos mensajes, supuestamente de una compañía legítima, pueden tratar de convencerte de visitar un sitio malicioso al afirmar que hay un problema con tu cuenta o te indique que has sido suscrito a un servicio. Una vez que visitas el sitio, puedes ser engañado para que proporciones información confidencial o descargues un archivo malicioso.
- *Utilizar tu teléfono celular en un ataque*. Los atacantes que llegan a obtener el control del servicio pueden utilizar tu teléfono celular para atacar a otros. Esto no sólo oculta la identidad real del atacante, sino que también le permite aumentar el número de víctimas.
- *Obtener acceso a la información de la cuenta*. En algunas áreas, los teléfonos celulares están siendo capaces de realizar determinadas operaciones (desde el pago de estacionamiento o comestibles hasta la realización de grandes operaciones financieras). Un atacante que llegara a tener acceso a un teléfono que se usa para este tipo de transacciones, puede ser capaz de obtener la información de la cuenta para utilizarla él mismo o venderla.

¿Y los riesgos en los *smartphones*?

Como parte de la evolución tecnológica surgió el llamado *smartphone* (teléfono inteligente), que funciona como un teléfono móvil pero con funcionalidades similares a las de una computadora. Debido a que cuentan con más características, existen diversas maneras de comprometer a estos dispositivos como son:

- *Los ataques desde Internet*. Desde que los *smartphones* son considerados puntos finales de Internet, pueden ser comprometidos de la misma manera que las computadoras por gusanos, virus o caballos de Troya.
- *Infección de una PC comprometida durante la sincronización de datos*. Los usuarios de los *smartphones* suelen sincronizar sus correos electrónicos, calendario, y otros datos con su computadora de escritorio a través de *software* de sincronización. Existen relaciones de confianza entre los *smartphones* y sus respectivas computadoras sincronizadas. Por lo tanto, en última instancia, para infectar un *smartphone*, los atacantes pueden infectar su sincronización con la PC, y entonces el *smartphone* será infectado la siguiente vez que se sincronicen.
- *Infecciones y ataques a smartphones vecinos.* Un *smartphone* comprometido puede escanear e infectar activamente *smartphones* vecinos a través de sus redes inalámbricas de Área Personal[2] como el *Bluetooth*. Dado que los teléfonos inteligentes son dispositivos móviles, pueden infectar nuevas víctimas en distintos lugares. El primer gusano de teléfonos inteligentes, Cabir, utiliza este método.

¿Cómo te puedes proteger?

- *Seguir las guías generales para la protección de dispositivos portátiles*. Tomar las precauciones necesarias para proteger a los teléfonos celulares de la misma manera que protegerías a una computadora.
- *Tener cuidado al publicar el número de celular y correo electrónico*. Los atacantes suelen utilizar *software* para examinar los sitios web en busca de direcciones de correo electrónico. Estas direcciones se convierten en objetivos para los ataques y el *spam*. Los números de los celulares también pueden ser obtenidos de forma automática. Al limitar el número de personas que tienen acceso a esta información, se limita el riesgo de convertirse en víctima.
- *No seguir los enlaces enviados por correos electrónicos o mensajes de texto*. Sospechar de las URLs enviadas en correos electrónicos o mensajes de texto no solicitados. Aunque los vínculos pueden parecer legítimos, en realidad pueden dirigir a un sitio web malicioso.

[2] WPAN – Wireless Personal Area Networks

- *Tener cuidado con el software descargable.* Existen muchos sitios que ofrecen juegos y otro tipo de *software* que se pueden descargar al teléfono celular. Este *software* puede incluir código malicioso. Si vas a obtener archivos de un sitio supuestamente seguro, hay que buscar un certificado del sitio web. Si se descarga un archivo desde un sitio web, hay que considerar la posibilidad de guardarlo en la computadora y escanearlo de forma manual para detectar algún virus antes de abrirlo.
- *Evaluar la configuración de seguridad.* Asegúrate de que se están aprovechando las características de seguridad que ofrecen los dispositivos. Los atacantes pueden aprovecharse de las conexiones *Bluetooth* para acceder o descargar información en el dispositivo. Deshabilitar el *Bluetooth* cuando no se esté utilizando para evitar el acceso no autorizado es una buena práctica de seguridad que debes llevar a cabo.
-

Estas son sólo algunas medidas de seguridad que, aunque no evitan que los dispositivos sean atacados, disminuyen el riesgo de verse comprometidos.

Referencias:

http://en.wikipedia.org/wiki/Mobile_phone
http://www.us-cert.gov/cas/tips/ST06-007.html
http://en.wikipedia.org/wiki/Mobile_phone
http://research.microsoft.com/en-us/um/people/helenw/papers/smartphone.pdf

Sergio Andrés Becerril López

La utilización de dispositivos móviles en los últimos años se ha incrementado tremendamente. No solo los teléfonos celulares (en sus modalidades de "teléfono" y "*smartphone*") se han vuelto ubicuos; verdaderamente, toda una cantidad de dispositivos móviles para múltiples propósitos se ha vuelto disponible, desde los ya conocidos PDA (*Personal Digital Assistant,* Asistente Personal Digital), hasta dispositivos increíblemente especializados (como, por ejemplo, los navegadores basados en GPS).

Imagen 1. iPad, de Apple

Al mismo tiempo que se diversifican, los dispositivos aumentan cada vez más su capacidad y habilidades. Un lector de libros electrónicos de primera generación apenas tenía espacio para unas cuantas decenas de libros; hoy en día, su capacidad puede llegar a superar muchas bibliotecas personales. Igualmente, los lectores actuales pueden realizar tareas de conectividad a alguna red de datos móvil, por 3G o *WiFi*; esto hubiera sido impensable hace apenas 10 años.

Como ejemplo, tenemos la *iPad*, de Apple. Apenas 2 meses después de su lanzamiento, la compañía indica que ha vendido más de 2 millones de dispositivos – entre aquellos con y sin acceso a redes 3G. Sin embargo, todos los modelos cuentan con conectividad por *WiFi*, y vienen integrados con navegador de Internet, cliente de correo y numerosas aplicaciones que hacen uso de Internet – y miles más están disponibles a unos cuantos clics de distancia en la tienda *iTunes* de Apple.

Estos dispositivos buscan, en las palabras de Steve Jobs, fundador y líder de la compañía, "ser dispositivos fáciles de usar, mas no ser computadoras personales". Sin embargo, las capacidades del dispositivo le permiten ser visto como una herramienta de trabajo, de entretenimiento personal y más.

Y es que la conectividad es precisamente la principal ventaja de estos dispositivos. El acceso a los recursos en cualquier lugar, a cualquier hora, es uno de los atractivos más importantes; y es, precisamente, el origen de la mayoría de problemas de seguridad con estos dispositivos.

Riesgos

Los riesgos existentes al poseer uno de estos dispositivos son por ejemplo: contenido contaminado, un mensaje de correo electrónico con un archivo adjunto malicioso; incluso una página web inteligentemente diseñada, pueden tomar ventaja de alguna vulnerabilidad conocida o, por supuesto, de alguna todavía no conocida en el sistema operativo de este dispositivo. Esto solo cubre las aplicaciones nativas; existe un riesgo en que alguna de las aplicaciones de terceros, a pesar de los estrictos controles de las compañías, lleve consigo vulnerabilidades en su código que permitan atacar por estos nuevos vectores.

Recordemos que hace ya seis años, en 2004, un grupo de programadores de virus profesionales diseñaron el primer virus para dispositivos Symbian, conocido como *Caribe*. Esto resalta que el potencial de alcanzar a los más de 100 millones de usuarios del sistema operativo móvil es un jugoso fin que muchos atacantes quisiera alcanzar.

Por tanto, conforme crece la popularidad de la *iPad*, así mismo crece su riesgo. Pero este no es el único dispositivo amenazado. Como mencionamos al inicio, los PDAs son probablemente el dispositivo móvil más conocido, aparte de los teléfonos celulares. Estos dispositivos han sido desplazados por equipos más orientados al contenido multimedia que a la productividad empresarial, debido a que esta última puede ser conseguida mediante teléfonos inteligentes. Entonces, en vez de observar usuarios corporativos con una *Palm* o *Pocket* PC, vemos incrementalmente usuarios con *iPods touch*, por ejemplo.
Existe entonces el mismo problema. Una aplicación comprometida puede permitir a los atacantes tomar control del dispositivo, lo que se traduce en lentitud en el mismo, comportamientos anómalos y, posiblemente, fuga de datos.

Este último punto es uno de los más importantes para usuarios de dispositivos móviles. Las estadísticas muestran que uno de los principales problemas con los dispositivos móviles en general es que pueden ser extraviados. Y es que, ¿a cuántos de nosotros no se nos ha perdido algo? Solo porque el aparato en cuestión tenga relación con la tecnología, no quiere decir que nuestras costumbres y hábitos vayan a cambiar. Y efectivamente, muchas compañías lidian diariamente con la realidad de dispositivos perdidos. El problema principal de la pérdida de un dispositivo móvil es encontrarnos en la situación donde otra persona podría tener acceso a nuestra información. Supongamos que

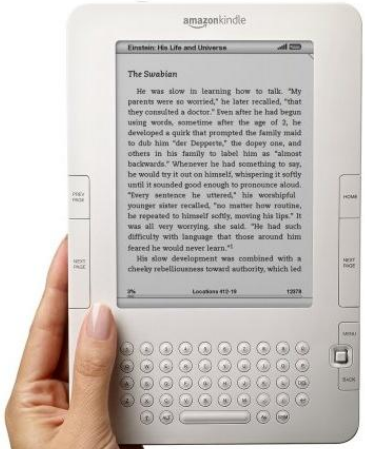

Imagen 2. Kindle de Amazon

guardamos en nuestro PDA la colección de datos personales de todos nuestros contactos: teléfonos, direcciones, correos electrónicos, etc. Es evidente que esta información puede ser de valor para otras personas –en particular– si hablamos de contactos corporativos y algún competidor puede tener una ganancia de esta información.

Pero incluso, la información personal es algo de cuidado. Uno podría pensar que un GPS perdido no tiene mayor problema –exceptuando– el hecho de que estos dispositivos actualmente guardan nuestras rutas previas como una medida de conveniencia para nosotros. Una persona podría utilizar esta información para registrar nuestros movimientos, ubicar personas que hemos visitado y realizar actos delictivos apoyándose de esta información. Igualmente, un lector de libros digitales perdido (o una cámara digital, por ejemplo) podría ser una mina de oro para ingeniería social, ya que permite un conocimiento de todos nuestros gustos y tendencias.

¿Cómo puedo protegerme?

A continuación, listamos una serie de recomendaciones que puedes seguir para asegurar de mejor manera tus dispositivos móviles:

- **Escoger cuidadosamente tus dispositivos**

En general, para cualquier dispositivo existirán siempre varias líneas de producto. Busca aquellas que ofrezcan más y mejores medidas de seguridad –como las que veremos a continuación–.

- **Habilita el cifrado**

Una de las mejores medidas de seguridad es el cifrado de datos. De esta manera, aún cuando nos enfrentemos a herramientas de robo de información o perdamos el aparato, solo alguien que conozca nuestra llave de descifrado podrá acceder a los datos.

- **Requerir autenticación**

Hablando de perder los aparatos, esta es una de las medidas más eficientes de evitar la fuga de datos. Una simple contraseña para utilizar el dispositivo puede ser la diferencia entre información perdida e información liberada.

- **Habilitar administración remota**

En algunos dispositivos, particularmente los más avanzados, es posible borrar de manera remota (mediante nuestra PC) el dispositivo, donde sea que se encuentre. Esto se logra aprovechando la capacidad del dispositivo de conectarse a Internet; en cuanto lo haga, recibirá la señal de "autodestrucción".

- **Cuidar la conectividad**

Es una práctica inteligente habilitar solo aquello que vayamos a utilizar. Por ejemplo, muchos lectores de libros digitales no utilizan la funcionalidad de conexión a Internet porque compran sus

libros desde su PC y con esta misma se sincronizan al dispositivo. Entonces, ¿por qué tenerla prendida?

- **Cuida lo que instalas**

En aquellos dispositivos que lo permiten, instalar aplicaciones debe realizarse con juicio y sentido común. Revisa que las aplicaciones vengan de un lugar con buena reputación y no sean meramente "bajadas de Internet". Vigila bien lo que las aplicaciones desean hacer: hoy en día, los dispositivos nos alertan cuando la aplicación desea conectarse a Internet, anunciar nuestra posición geográfica, etc.

Estos dispositivos seguirán creciendo en popularidad y presencia. Si cuidamos un poco lo que realizamos con ellos nos permitirá explotar al máximo sus capacidades, y nos facilitarán, como lo han venido haciendo, nuestras tareas diarias.

Referencias:

http://www.teleread.com/2009/12/22/statistics-who-reads-ebooks-in-the-us/
http://contacto-latino.com/news/541903/steve-jobs-boasts-of-2-million-ipads-sold-dailytech/
http://googleblog.blogspot.com/2008/09/future-of-mobile.html
http://articles.techrepublic.com.com/5100-22_11-5274902.html
http://www.securelist.com/en/analysis?pubid=170773606

DIRECTORIO

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

Dr. José Narro Robles
Rector

Dr. Sergio Alcocer Martínez de Castro
Secretario General

DIRECCIÓN GENERAL DE SERVICIOS DE
CÓMPUTO ACADÉMICO

Dr. Ignacio de Jesús Ania Briseño
Director

M. en C. Ma. de Lourdes Velázquez Pastrana
Directora de Telecomunicaciones

Ing. Rubén Aquino Luna
Subdirección de Seguridad de la Información
UNAM-CERT

2010 D.R. Universidad Nacional Autónoma de México
Revista elaborada por la
Dirección General de Servicios de Cómputo Académico

CRÉDITOS

PUNTO SEGURIDAD, DEFENSA DIGITAL

M en I. Rocío del Pilar Soto Astorga
Edición

Sergio Andrés Becerril López
Anaid Guevara Soriano
Alejandro Reyes Plata
Rosa Xochitl Sarabia Bautista
Colaboraciones

Ing. Rubén Aquino Luna
Subdirección de Seguridad de la Información
UNAM-CERT

Rocío del Pilar Soto Astorga
Rubén Aquino Luna
Revisión de Contenidos

Act. Guillermo Chávez Sánchez
Coordinación de Edición Digital

Diana Chávez González
Coordinación de la Producción Digital

Lic. Lizbeth Luna González
Dolores Montiel García
L.D.C.V. Carolina Silva Bretón
Diseño Gráfico

Liliana Minerva Mendoza Castillo
Formación

2010 D.R. Universidad Nacional Autónoma de México
Revista elaborada por la
Dirección General de Servicios de Cómputo Académico