

Seguridad en dispositivos móviles: SmartPhone y Pocket PC

Claudio Caracciolo y Ezequiel Sallis

<http://www.root-secure.com/>

Fecha Publicación: 21/06/2008

Introducción- Situación Actual

El acceso a la información en cualquier momento y lugar se ha vuelto hoy en día parte de nuestras acciones cotidianas. Forma parte de una arista más que el negocio necesita para mantenerse competitivo en el mundo actual. Los dispositivos móviles (Smartphone- Pocket PC) facilitan esta tarea en combinación con las tecnologías de conectividad emergentes y tradicionales (GPRS, EDGE, 3G, 802.11, Bluetooth y otras).

A partir de estas tecnologías, algunas de las funcionalidades corporativas se extienden fuera de los límites de la organización, permitiendo a los usuarios interactuar en donde quiera que se encuentren, como por ejemplo:

- Acceso al Correo Corporativo
- Acceso a los Aplicativos Corporativos
- Sincronización de Calendarios
- Sincronización de Contactos
- Almacenamiento y edición de documentos de ofimática entre otros...

Los Smartphones y las Pocket PC, han ampliado las funciones de las PDA (Personal Digital Assistance) permitiendo utilizar dichos dispositivos tanto para fines personales como corporativos, y en base a ello surgen entonces dos frentes con diferentes tipos de problemáticas:

Problemática I:

En implementaciones corporativas de soluciones móviles, la aplicación de políticas de seguridad apropiadas, al igual que en una estación de trabajo, plantea la misma pregunta:

Cómo evito que el usuario use el dispositivo con fines no relacionados con el negocio?? :-)

Problemática II:

Por lo general, usuarios finales, casi siempre de alta jerarquía, deciden, sin el más mínimo análisis, incorporar estos dispositivos a las redes de la organización o bien incorporar información sensible en las memorias de almacenamiento de estos dispositivos.

Entonces, si bien no es novedad que los dispositivos móviles ya están ocupando un espacio en los entornos corporativos, preguntas como las siguientes rondan de vez en cuando en nuestras cabezas.

- Se han evaluado los riesgos que estas tecnologías pueden introducir en los modelos de seguridad de mi organización?
- Cuáles son los riesgos más representativos en el uso de estas tecnologías?
- Cómo puedo aplicar políticas de seguridad corporativas a dispositivos de uso personal y con información privada dentro?
- Si monitoreo el uso de estas tecnologías, estoy invadiendo la privacidad de los usuarios?
- Conozco todas las tecnologías de conectividad y sistemas operativos que usan los dispositivos móviles?

El objetivo de este artículo es, entonces, ayudarlos a encontrar respuestas a algunas de las preguntas anteriores.

Introducción-Algunos Datos Estadísticos:

Según varias consultoras especializadas, la inserción corporativa de los Smartphones recién empieza, de manera que es bueno estar preparados para lo que viene. Si observamos la **Figura 1**, podremos ver como dichos dispositivos se distribuyen a través de los años según su sistema operativo. Sin duda alguna Symbian OS es el sistema que abarca más del 80% del Mercado, seguido muy de lejos por implementaciones de Linux y Microsoft Windows Mobile. En base a esta información no es asombroso descubrir que más del 80% del código malicioso que afecta a estas tecnologías está desarrollado para Symbian OS.

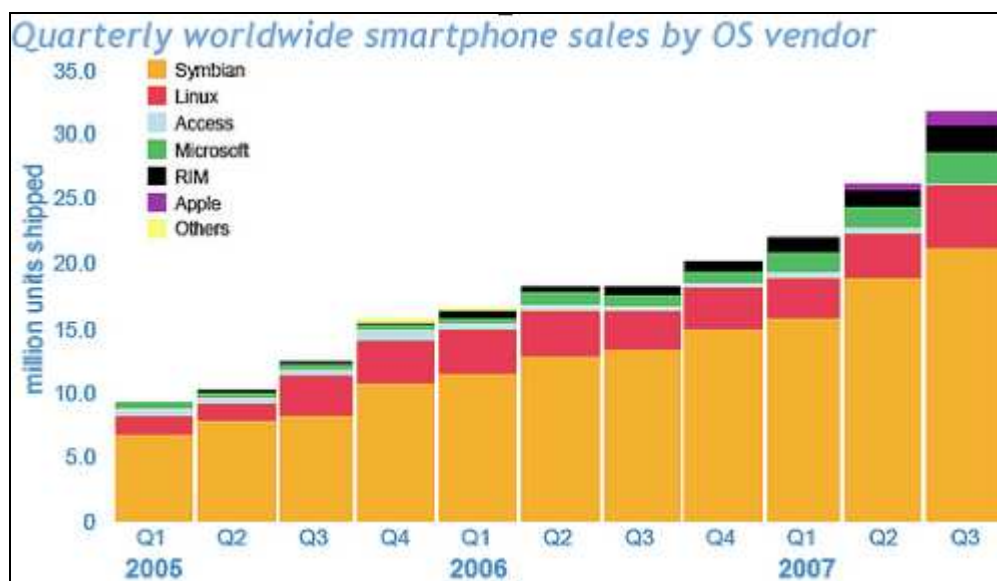


Figura 1

En la **Figura 2** podremos observar cómo se distribuyen estas tecnologías según su localización geográfica, y veremos que la misma se reparte de manera homogénea en la mayoría de los lugares de planeta, salvo en los Estados Unidos donde la historia cambia bastante.

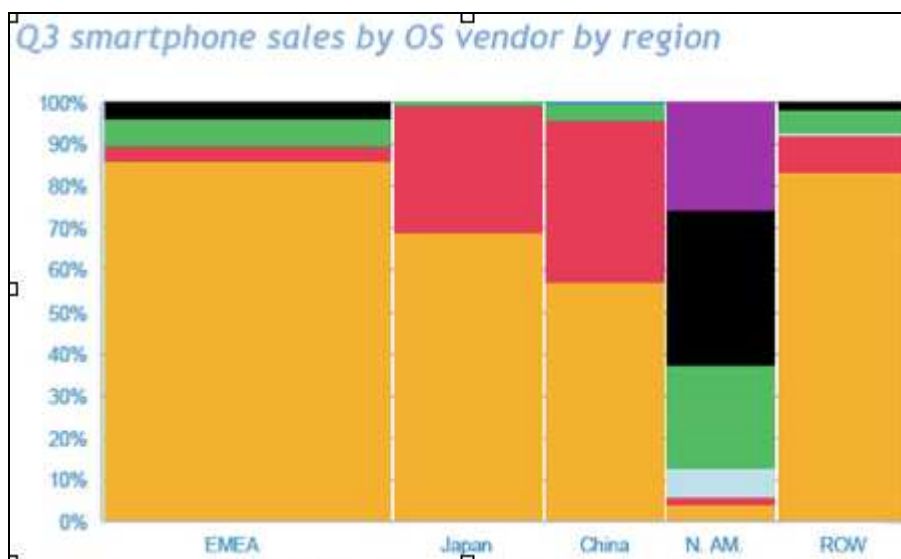


Figura 2

Symbian OS se posiciona entre los primeros, mientras que Windows Mobile, Blackberry y Iphone se reparten la torta (**Figura 3**).

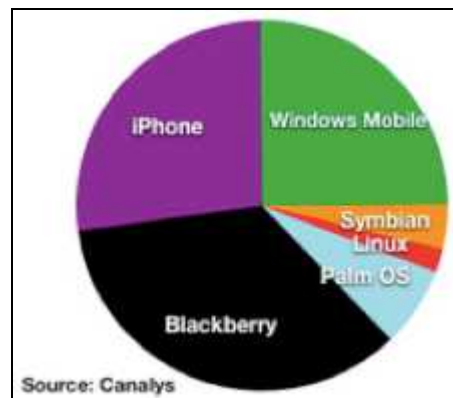


Figura 3

Por último, si analizamos las conductas respecto de la utilización de estos dispositivos por parte de los usuarios, podremos ver que:

- 85% Utiliza estos dispositivos para almacenar el día a día del negocio
- 85% Las utiliza para almacenar contactos y direcciones relacionadas con el negocio
- 33% Las utiliza para almacenar números de pin y contraseñas.
- 32% Para recibir y enviar correo
- 25% Para llevar el detalle de sus cuentas bancarias
- 25% Para almacenar información corporativa

Riesgos habituales en estas tecnologías

Si bien los ataques a estos dispositivos parecen tener muchos orígenes y causantes, como veremos más adelante, creemos que para un mejor entendimiento deberíamos centrarnos en tres perspectivas principales:

- *Debilidades Inherentes a la Tecnología*
- *Debilidades Inherentes a las Aplicaciones*
- *Debilidades Inherentes al Factor Humano*

De más está decir que parte del camino ya fue recorrido, ya que dichas perspectivas podrían aplicarse también a muchos otros aspectos y tecnologías relacionadas con seguridad de la información, sobre las cuales seguramente venimos trabajando.

1) *Debilidades Inherentes a la Tecnología*

Cada uno de los diferentes tipos de Smartphone's - Pocket PC vienen con su propio sistema operativo dedicado, similares en algunos aspectos a los habitualmente utilizados en las estaciones de trabajo, pero muy diferentes en otros de ellos. Cada uno de estos sistemas operativos pueden introducir, además de nuevas funcionalidades, nuevos agujeros de seguridad que permitan la ejecución de código arbitrario o la denegación de servicio, tanto sea de manera remota como local.

Por otro lado, e independientemente del sistema operativo, muchos de estos sistemas introducen bugs a nivel de diseño en sus sistemas de **control de acceso**, permitiendo el ingreso no autorizado mediante técnicas de evasión o bien, el ataque directo a pobres implementaciones criptográficas.

Desde el punto de vista de capacidad de almacenamiento de datos, cada fabricante ha decidido implementar diferentes medios y tamaños.

Discos de Estado Sólido (Flash)

- *SD*
- *MiniSD*
- *MicroSD*
- *Memory Stick*
- *Otros*

Independientemente de su tipo y forma, todos estos medios son vulnerables a la ya conocida **remanencia de datos**, lo que da lugar a la recuperación con cierta facilidad de archivos que el usuario creía eliminados. De todos los Smartphones y Pocket PC sólo un dispositivo implementa a nivel de OS la posibilidad de Borrado seguro de los datos almacenado en el equipo.

Con respecto a la remanencia de datos pueden darse varias situaciones a tener en cuenta donde suelen centrarse los ataques:

- *Reutilización de los equipos dentro de la organización*
- *Venta del equipo por parte del Usuario*
- *Donación de los equipos por política corporativa*
- *Otros*

Como recomendación general, todos los equipos móviles (al igual que las estaciones de trabajo) deben someterse a procesos de borrado seguro de los datos de la organización. Dentro de las técnicas de borrado seguro más comunes, podemos mencionar:

- *Wipe (Existen varios niveles)*
- *Degaussing*
- *Destrucción Física*

2) Debilidades Inherentes a las Aplicaciones

Uno de los puntos más interesantes es el gran crecimiento que ha tenido la navegación Web desde estos dispositivos con el correr del tiempo. Lejos quedaron los formatos poco amigables y de pobre interacción. Hoy en día la experiencia es muy parecida a la navegación desde una PC, tan similar que casi se sufren los mismos problemas, y es aquí en donde entra la seguridad de los navegadores móviles.

- *Pocket Internet Explorer*
- *Opera Mini*
- *Mínimo (Firefox coming soon...)*

Debilidades del Tipo de XSS y similares no están ausentes en estas plataformas, pudiendo permitir a un potencial atacante el acceso a información de manera no autorizada como así también el secuestro de sesiones previamente establecidas.

Otro punto importante a tener en cuenta es la plataforma de desarrollo J2ME (Java 2 Platform Micro Edition), la cual provee un ambiente de ejecución de aplicaciones Java para dispositivos de bajos recursos. A las aplicaciones Java para los dispositivos Móviles se las conocen con el nombre de MIDlets y existen al momento en dos versiones, MIDP 1.0 y MIDP 2.0.

MIDP 1.0 Posee algunas debilidades desde el punto de vista de la seguridad, ya que si bien, como es habitual en la tecnología Java, todo es verificado a nivel de Sandbox, la verificación del bytecode no es completa ya que esto consumiría muchos más recursos que los que los smartphones poseen, haciendo a la aplicación difícil de utilizar. Por otro lado, las comunicaciones en la versión 1.0 están limitadas solo al protocolo HTTP lo que implica que cualquier tipo de comunicación que se realice correrá el riesgo de ser monitoreada con éxito por parte de un potencial atacante.

MIDP 2.0 Posee en cambio mejoras desde el punto de vista de seguridad con respecto a su antecesor. A diferencia de **MIDP 1.0**, quien proveía un acceso limitado a los recursos del sistema, esta tecnología provee mayor funcionalidad, lo que podría significar que un compromiso en el sistema tenga mayor impacto.

Es bueno aclarar que no todos los Smartphones, como así también no todas las Pocket PC, tienen pleno soporte para la ejecución de aplicaciones de este tipo.

3) Debilidades Inherentes al Factor Humano

Generalmente escuchamos que el factor humano es el eslabón mas débil en la cadena de seguridad de la información... Y en el caso de la utilización de las tecnologías móviles, tampoco es la excepción..., lo realmente curioso es que si bien todos estamos de acuerdo con lo arriba expuesto, son muy pocas las organizaciones que realmente realizan acciones formales y efectivas al respecto.

Es bien conocido que los usuarios de estas tecnologías corren riesgos de robo o pérdida de los equipos más que lo habitualmente sucede con otras tecnologías, por ejemplo solo en Chicago se dejan olvidados 160.000 dispositivos en taxis por año. La pérdida física de éstos implica un potencial compromiso contra la confidencialidad, la integridad y la disponibilidad de la información de los usuarios y de la Organización si no se toman las medidas adecuadas a tiempo y si no se tienen procedimientos de respuesta que contemplen a estos tipos de incidentes también.

Dispositivos - Características Generales

Antes de comenzar con las descripciones de los riesgos y de los ataques más habituales que afectan a estas tecnologías, es bueno hacer un repaso sobre cuáles son los sistemas operativos más representativos a nivel corporativo y conocer algunas de sus características.

Palm OS

Mencionado en primer lugar no por capricho, sino por ser este dispositivo uno de los primeros organizadores personales que irrumpieron en las Empresas, y no necesariamente como parte de una implementación corporativa sino más bien como iniciativa de los usuarios personales que se vieron atraídos por estas tecnologías. Algunos de los modelos que pueden verse hoy en día son los TX y los Lifedrives con disco de hasta 4 GB, ambos con conectividad Bluetooth y WI-FI. Estos dispositivos han evolucionado de handhelds a Smartphones, dando ingreso a los ya conocidos modelos TREO con conectividad Bluetooth listos para las 3G, llamativos por su diseño armonioso y la facilidad del uso.

Mobile OS

El sistema operativo de Microsoft para dispositivos móviles, hoy está en su Versión 6.0 aunque aún existen gran cantidad de dispositivos que utilizan la 5.0-2003. El sistema operativo cuenta tanto con versiones

Smartphone (Teclado QWERTY) como Pocket PC (Pantalla Táctil). La gran variedad de dispositivos que lo implementan permiten conectividad con redes GPRS, EDGE, 3G ,802.11, Bluetooth e infrarrojo. Generan una fuerte atracción a los usuarios por las similitudes con el sistema operativo de las estaciones de trabajo, como así también con las herramientas de ofimática.

Symbian OS

El más implementado en smartphones y celulares en promedio a nivel mundial (70%). Sony y Nokia son las empresas más importantes que implementan versiones de este sistema en sus dispositivos, lo cual justifica fácilmente esta gran inmersión en el mercado. Como consecuencia del éxito de este sistema operativo, más del 80% del código malicioso existente para dispositivos móviles está dirigido a estas plataformas.

Blackberry RIM OS

Sin duda alguna uno de los revolucionarios del mercado, permitiendo que el correo corporativo sea accesible a través de un celular... Hoy en día sigue existiendo dicha competencia y hace muy pocos años que otras tecnologías se han puesto a la altura e intentan competir contra esta funcionalidad. El sistema operativo implementado en las Blackberry posee una de las características esenciales que ningún otro sistema incluía hasta hace muy poco tiempo, esto es la implementación de un Firewall de salida, así es... poseen un dispositivo de filtrado de conexiones salientes. El Sistema Operativo es provisto por RIM (Research in Motion), y los dispositivos se dividen básicamente en tres categorías:

- ***Business Phone***
- ***Handeld Phone***
- ***Blackberry Enable Devices***

Apple OS X (Iphone)

Revolucionario e Innovador son las dos palabras que veíamos en los periódicos y en los blogs al ser presentado al mercado. Si bien este dispositivo no está orientado hacia líneas corporativas, el nivel de inserción que tiene en los Estados Unidos y en otros países donde aún no fue oficialmente lanzado pero en los que, sin embargo, ya se encuentra funcionando, hace pensar que muchas redes corporativas los tienen o los tendrán conviviendo pronto y no en forma planificada. Además de haber desatado una carrera por romper los controles de seguridad que lo ataban a un único proveedor de servicios de telefonía, se le han descubierto y explotado ya varias vulnerabilidades críticas que harían subir los niveles de riesgo debido a que la mayoría de los usuarios están relacionados a determinadas escalas jerárquicas.

Si bien todas tienen diferentes características, prestaciones y niveles de integración con las redes corporativas, hay algo que tienen en común:

Todas tienen Vulnerabilidades

En mayor o menor medida el uso de estos dispositivos, sin la implementación de adecuados controles y conciencia por parte de los usuarios finales, introduce riesgos en la organización que no pueden dejar de ser analizados.

Algunos Ataques a Dispositivos Móviles (sólo algunos...)

Blackjacking (RIM OS)

Esta técnica está relacionada con la implementación de las infraestructuras de Blackberry típicamente en las empresas. Si quisiéramos tener el servicio directamente en nuestra empresa, básicamente conectaríamos el BES (Blackberry Enterprise Server) en nuestras oficinas. El tema está en que la mayoría de los proveedores no analizan la situación desde el punto de vista de la seguridad de la compañía y terminan colocando estos dispositivos en la red LAN de la empresa con conectividad hacia el exterior para que pueda comunicarse el BES con los celulares... por qué en la LAN? Porque el BES necesita acceder al servidor de correo electrónico corporativo para poder redireccionar los correos. Pero el problema es obvio, tenemos un equipo público conectado directamente al exterior.

Hace ya un par de años atrás se desarrolló una herramienta que puede ser instalada en las Blackberry conocida como BBproxy, que permite establecer una conexión a un IP y a un puerto determinado a fin de cumplir las funciones de Proxy entre esa conexión que estableció y la comunicación con el BES correspondiente... No se entendió? Básicamente sucede lo siguiente: imaginemos el siguiente escenario, somos los atacantes y tenemos nuestra PC y una blackberry perteneciente a una compañía X a la cual queremos atacar. En nuestra pc conectada a Internet con una IP pública, abrimos un puerto a la escucha de nuevas conexiones (por ejemplo con el viejo y buen amigo Netcat), luego en la Blackberry instalamos el soft mencionado y le configuramos la IP y el puerto de nuestra PC. La Blackberry se conectará a nosotros, pero a su vez estará conectada al servicio de BES de la compañía X, por lo cual, a partir de este momento, podríamos enviar comandos desde nuestra PC a la red interna de la compañía X utilizando como Proxy de esa conexión a la blackberry que tenemos en nuestro poder...fácil, no? Gracias a que en la mayoría de las implementaciones el BES está en la LAN interna de las empresas, estaríamos ahora ubicados directamente adentro, es por esto que no es una buena idea ubicar estos servidores dentro de la LAN. Si bien existe desde hace mucho la posibilidad de separar el BES en dos equipos físicamente, esto no es muy común de encontrar. Si los separasen en dos como dicen los manuales, básicamente podríamos colocar un BES router en la DMZ de la empresa y el BES en la LAN de manera que el único expuesto sea el BES Router, quien se encarga de redireccionar los correos, muy similar a una implementación de un servidor de correo donde tenemos un SMTP Relay en nuestra DMZ.

Blueline (Motorola PEBL U6/Motorola V3)

Motorola sufrió mucho los duros golpes por las implementaciones de Bluetooth en sus primeros pasos, por lo cual ha desarrollado muchísimas mejoras a dicha implementación. Sin embargo, como decimos siempre, no hay nada 100% seguro y han vuelto a ser vulnerables en los dos mencionados dispositivos. Pero existe una diferencia elemental, primero es que es realmente poco probable que este ataque tenga éxito inmediato, ya que necesita que se cumplan varias condiciones particulares... Bien, en que consiste? Es un excelente ataque que combina técnicas de Ingeniería Social con bugs de la implementación, ya que básicamente se basa en la falsificación de la interfase del celular camuflando un pedido de autorización de conexión entrante real con un mensaje que fácilmente haga que el usuario presione "OK". A partir de dicho momento, cuando el usuario acepta un mensaje engañoso enviado por nosotros, estaremos en condiciones de realizar un ataque a partir de la ejecución de comandos AT sobre el teléfono...

A través del ataque Blueline trataremos de ejecutar comandos AT a partir de la conexión al Perfil de Pasarela de Voz (Voice Gateway Profile) el cual es accesible a través del canal 3 y particularmente requiere autorización pero no autenticación.

Los modelos PEBL U6 y RAZR V3, deniegan automáticamente los intentos de conexión provenientes de otro dispositivo Bluetooth no conocido (que no aparece en el histórico de dispositivos conectados anteriormente).

Para llevar a cabo el ataque, primero debemos aprovecharnos de la variación del ataque *Helomoto* contra los dispositivos mencionados, de manera de plantar un dispositivo en los históricos de conexión de las víctimas debido a que, al ser vulnerables, no nos pedirán autenticación...

```
root@secure#hciconfig hci0 up (levantamos la interfase BT)
```

```
root@secure#hciconfig hci0 scan (scaneamos en busca de dispositivos BT)
```

```
root@secure#sdptool browse hciconfig 00:17:84:47:74:94 (navegamos los servicios en busca del servicio de pasarela de Gateway de voz)
```

```
root@secure#./helomoto plant 00:17:84:47:74:94 (realizamos el ataque Helomoto contra la mac de la víctima)
```

en esta instancia, en el celular se habrá agregado un dispositivo en la lista de históricos, sin embargo, para finalizar el ataque, deberíamos estar autorizados por el usuario del mismo celular y el problema surge en que cuando requiera dicha conexión le aparecerá en la pantalla que el dispositivo "ATACANTE" desea conectarse y deberá elegir si permite o no la conexión. Es decir que aquí es donde entra en juego la habilidad como ingeniero Social, ya que el próximo paso será camuflar ese mensaje enviando otro más grande que el tamaño de la pantalla, de manera tal que el mensaje, de permitir conexión verdadero quede desfasado hacia abajo y se muestre nuestro mensaje de error personalizado con dos opciones coincidentes con la ubicación de las teclas que queremos que ejecute la víctima.

Entonces, el próximo paso sería:

```
root@secure#hciconfig hci0 name `perl -e 'print  
"Seleccione\x0daceptar\x0dpara\x0ddeshabilitar\x0dMute\x0d\x0d"'` (le enviamos el  
mensaje que utilizaremos para camuflar el verdadero mensaje de autorización de  
conexión)
```

Ahora sí, una vez que el usuario selecciona la opción de aceptar en base al mensaje que le enviamos por pantalla, nuestro dispositivo ya contará con autorización para enviar comandos AT y listar los directorios, efectuar llamadas, etc etc etc... como ya hemos visto en algún artículo anterior ;-)

Bluespam (Palm OS)

No es una técnica nueva pero sí molesta quizás. Es un ataque que nos ha fastidiado y nos sigue complicando si es que nuestro equipo tiene Bluetooth encendido en modo descubrimiento. BlueSpam es un ataque basado en la búsqueda de dispositivos en Modo Descubrimiento, a los cuales luego les enviará mensajes arbitrarios creados por el atacante. Por lo general este ataque es utilizado en lugares donde existe un gran volumen de gente como técnicas de Marketing Directo, sin costos asociados fuera de la adquisición de una Palm. Es decir, que básicamente consiste en enviar Spam sobre Bluetooth...

Cómo es posible esto?, en principio la herramienta de BlueSpam envía los mensajes utilizando el protocolo OBEX, más específicamente OOP (Object Push Obex) y/o OBEX-FTP (Protocolo de transferencia de archivos OBEX), básicamente el protocolo utilizado para enviar tarjetas de contactos entre los teléfonos celulares. Los tipos de archivos que pueden transmitirse por este medio van desde simple archivos de texto hasta imágenes en JPG y GIF o incluso archivos de audio y video, por lo cual, si pensamos en malware para móviles, ésta puede ser una puerta de entrada bastante interesante... Igualmente debemos aclarar que no todos los dispositivos permiten la transferencia de todos los tipos de archivos a través del protocolo OBEX, ya que han implementado “perfiles” que restringen la funcionalidad de manera que algunos dispositivos solo pueden transferir y recibir vcards, otros solo audio, otros imágenes y vcards, y así sucesivamente.

Es interesante remarcar que en sí mismo no es un problema de seguridad, el problema estaría del lado del usuario si acepta la recepción de archivos sin haberlos solicitado, por lo cual podemos decir: “estamos en problemas si dependemos de ellos”

Iphone Exploit Code (Iphone OS)

Como ya mencionamos anteriormente, el foco de este tipo de dispositivos no es el mercado corporativo, sin embargo al ser un dispositivo tan elegante e innovador y que además trae funcionalidades poco comunes de interoperabilidad, como por ejemplo la posibilidad de conectarse a cuentas de MS-Exchange, no es poco común verlo dentro de las empresas... El Iphone ha traído consigo muchas fallas de seguridad que principalmente eran utilizadas para desbloquear el teléfono o para ampliar su funcionalidad, sin embargo, dos vulnerabilidades referentes a Safari han llamado la atención y han sido implementadas en el Framework de Explotación más famoso (metasploit). Básicamente el ataque consiste en colocar la PC del atacante a través del metasploit como un webserver a la escucha de solicitudes de conexión provenientes de estos móviles navegando por Internet. Aquí vuelven a entrar en juego las técnicas de Ingeniería Social para lograr que una víctima llegue inocentemente con, por ejemplo, un mail y un link a nuestro webserver malicioso (*técnica conocida, no?*).

Cuando la víctima acceda hasta nuestro webserver, el navegador Safari se cerrará automáticamente, el usuario, podrá levantarlo nuevamente y continuar utilizándolo como así también el resto de las funcionalidades del dispositivo, sin embargo, en nuestro equipo tendremos un Shell remota con permisos privilegiados sobre el sistema, pudiendo acceder a los correos configurados en el equipo, a los contactos, a los archivos de sistemas a fin de modificar los archivos de host o dns de forma de convertirlo en una víctima permanente, etc etc. Cómo es posible el ataque? Básicamente, la implementación de Safari sobre Iphone posee un bug sobre la librería libtiff que permite la ejecución de Buffer Over Flow, lo cual fue corregido en el Firmware 1.1.3...

Software Espía (Symbian OS - RIM OS - Windows Mobile OS)

Como hemos mencionado anteriormente, existe una gran variedad de software malicioso y principalmente está dirigido a Symbian OS, sin embargo hemos tenido la oportunidad de encontrarnos con un Software Comercial que es capaz de asombrarnos una vez más por la peligrosidad de su implementación... Dicho software en particular puede ser instalado en Palm, en Windows Mobile, en Blackberry y vaya uno a saber en cuántas cosas más :)

Básicamente lo que hace esta herramienta es instalar una aplicación que se encargará de monitorear nuestros dispositivos y enviará toda la información que necesitemos a un Sitio Web para que podamos accederla directamente. Cómo?

Supongamos que compramos la herramienta On Line, nos llegará el link de descarga de la herramienta para el OS que nosotros hayamos elegido con la posibilidad de utilizarlo en tantos dispositivos como queramos, pero siempre que respetemos dos cosas importantes:

- Debe ser siempre sobre el mismo OS.
- No pueden estar activos dos equipos a la vez (a menos que compremos otro tipo de licencia obviamente)

Una vez instalado, si pudiéramos revisar las aplicaciones instaladas en nuestro dispositivo, podremos observar cómo se intenta camuflar tras un nombre ficticio, como por ejemplo: actualización de java... de todas maneras, si analizáramos el proceso, veríamos que en realidad no es firmado por el fabricante del Soft que mencionan (obviamente).

Pero bien, qué se puede hacer con esta herramienta?... el software en cuestión permite:

- Recibir todos los correos que lleguen al dispositivo móvil en una consola Web.
- Recibir todos los SMS que lleguen al dispositivo móvil en una consola Web.
- Activar remotamente el móvil en modo micrófono llamándolo a un número especial.
- Rastrear el historial de llamadas del equipo y verificar las actividades GPRS

En el caso particular de Blackberry y gracias a la implementación del Firewall de su OS, para que el programa funcione deberíamos permitir la conexión saliente e indicar que no vuelva a preguntar, por lo cual, el escenario ideal para este tipo de ataques es cuando en un evento regalamos el último modelo de estos equipos a la línea de CEO's de las empresas para que estén al día (y los atacantes al tanto ;-))

Recomendaciones de Seguridad - Buenas Prácticas

Si bien hoy en día la mayoría entiende la necesidad de implementar y mantener políticas de seguridad acordes a las buenas prácticas, muchas veces éstas dejan fuera a las nuevas tecnologías y sus diferentes aplicaciones en el negocio. Es por esto que debe existir una Norma de Seguridad que haga referencia exclusivamente a la utilización de dispositivos móviles, que cuente con el apoyo de la Alta Dirección y contenga entre sus objetivos:

- Proteger los datos sensibles de la organización almacenados en ellos.
- Evitar que sean causa de la infección y distribución de código malicioso dentro de la organización.
- Prevenir que sean estos dispositivos el origen de accesos no autorizados a las redes de la organización.

No solo Smartphones y Pocket PC deberían incluirse dentro de lo que se conoce como dispositivos móviles, sino que también se deberían abarcar por lo menos los siguientes:

- *Notebooks*
- *Dispositivos de Almacenamiento USB*
- *Cámaras Digitales*
- *Reproductores de Audio*
- *PDA*
- *Pocket PC*
- *Smartphones*
- *Teléfonos Celulares Tradicionales*

Entonces, SI o NO a los Smartphones y Pocket PC?

Quizás ésta sea una de las preguntas que se plantean con mayor frecuencia en relación con este tema, el cómo tratar la **autorización o la prohibición** de estos dispositivos con fines personales o del negocio y, si lo autorizo, cómo **lo controlo**. Una de las primeras recomendaciones que podemos dar es la importancia de dejar en claro por parte de la compañía de cuál será la expectativa de privacidad de los usuarios respecto de la utilización de las distintas tecnologías cuando sean provistas por la organización, o bien, cuando ésta sea personal pero se encuentre conectada a las redes corporativas.

Por otro lado, recomendar la utilización de estos dispositivos **únicamente con fines que sirvan al negocio**, debido a que los mismos serán monitoreados a través de los controles implementados con estos fines, puede ayudarnos a evitar unos cuantos dolores de cabeza.

Algunos de los aspectos no deseables por la organización sobre el uso de estas tecnologías y sobre los cuales deberían aplicarse controles son:

- *Instalación no Autorizada de Software*
- *Navegación irrestricta por Internet*
- *Descarga y uso del correo electrónico personal*
- *Conexión a Redes inalámbricas inseguras (WI-FI 802.11)*
- *Establecimiento de relaciones de confianza con equipos no autorizados (Bluetooth)*
- *Abuso de la Red de Voz*
- *Abuso de la Red de Datos*
- *Almacenamiento de información no autorizada (Mp3, Archivos Personales y otros)*

Como existe hoy en día una gran variedad de controles de seguridad creados exclusivamente para estos dispositivos, independientemente de la particularidad de cada uno, se deberían tener en consideración los siguientes factores:

Identificación y Autenticación:

Debe existir formalmente una política de contraseñas para el acceso a estos dispositivos. Al igual que en el entorno corporativo, la contraseña debe tener ciertos componentes que hagan de la misma una contraseña robusta según conocemos de las recomendaciones de los estándares internacionales. Existen sistemas que integran el acceso a estos dispositivos a otros controles como Tokens o Factores biométricos y desde ya, siempre que sea posible, los dobles factores de autenticación serían ideales.

Cifrado de Información Sensible:

Deben existir controles al cifrado de información sensible, tanto sea en la transmisión como en el almacenamiento de la misma. Hoy en día existen algoritmos creados para estos dispositivos (Curva Elíptica y otros), como así también sistemas criptográficos híbridos para la firma y el cifrado de correo electrónico (PGP Versión Mobile).

Software para la Prevención de Código Malicioso:

Si bien la variedad y cantidad de código malicioso no puede compararse con los que afectan sistemas tradicionales, es importante contar con software actualizado que prevenga la infección de virus, gusanos, troyanos o cualquier tipo de malware, tal como lo hacemos en estaciones de trabajo.

Filtrado de Tráfico:

Estos dispositivos deben contar con un firewall personal que prevenga el establecimiento de conexiones entrantes no autorizadas, como así también deberían contar con la capacidad de controlar todas aquellas conexiones salientes (Malware de Conexión Reversa). Si bien el único que posee esta implementación por Default es el RIM OS, existen algunos desarrollos para otras plataformas que por lo menos deberían evaluarse.

Conexiones Seguras:

Toda conexión que transmita información sensible sobre cualquier tipo de medio, debería ser realizada a través de canales seguros (VPN, SSL, TLS, WPA2, Bluetooth Autenticado , autorizado y Cifrado), pero de nada sirve este control si los usuarios no analizan, cuando se comunican telefónicamente con otra persona, el ambiente donde se encuentran parados...

Borrado Seguro:

Como mencionamos anteriormente, es realmente importante asegurar mecanismos de borrado seguro de todos los medios de almacenamiento de nuestros dispositivos a fin de evitar los ataques de Remanencia de Datos... lamentablemente es muy común comprar equipos usados por medios on line y encontrar en ellos mensajes de texto, mails, contactos, etc etc que no han sido borrados adecuadamente o bien, que ni siquiera han sido borrados...

Conclusión

La utilización de dispositivos móviles con fines de negocio incrementa de manera muy favorable la productividad, pero puede transformarse en una nueva vía de ataque si no se implementan los controles adecuados. Lo mismo que sucede con toda nueva tecnología...

Antes de decidir incorporar o no estas tecnologías, se debe analizar los riesgos que pueden introducir en nuestra organización de manera directa e incluso de manera indirecta. Se debe analizar cómo pueden impactar en el modelo actual de seguridad de la organización.

Está claro que no podemos frenar el crecimiento tecnológico de nuestras empresas, tampoco es el objetivo hacerlo, solo debemos asegurar que el crecimiento sea dentro de un marco de riesgos acotados y aceptados por la empresa...

Si bien las Blackberry, las PDA, los celulares y los Smartphone no son los dispositivos de red móviles a los que estábamos acostumbrados a proteger dentro de nuestro espectro de trabajo, hoy en día no podemos ignorarlos si conocemos la potencialidad de sus ataques...

No hay peor incidente de seguridad que aquel que ocurre y no nos enteramos, pero más frustrante es aquel que ocurre, nos enteramos pero no podemos determinar por dónde vino... Desarrollar metodologías de defensa es la única forma de acortar las distancias entre los atacantes y nosotros...