Universidad Católica “Ntra. Sra. de la Asunción”

Facultad de Ciencias y Tecnología

Ingeniería Informática

Teoría y Aplicación de la Informática 2

Trabajo Práctico
“Telefonía Móvil, Riegos y Amenazas”

Alumno: Francisco José Milleres Irala Gadea

Profesor: Ing. Juan Eduardo de Urraza

Asunción – Paraguay
2005

Introducción

El brindar a la sociedad los recursos para ampliarse y desarrollarse con nuevas herramientas ha sido el afán desde siempre de aquellos interesados en el área de la Tecnología de la Información. Sin embargo, desde hace unas décadas existen quienes dedican todos sus conocimientos para llevar a la práctica actos maliciosos y perturbadores de la tranquilidad, como los que se conocen hoy en día, los virus, gusanos, accesos no permitidos, etc.
Llevar la tecnología de la computación a dispositivos inalámbricos ha sido un gran avance, sin embargo, no tardo mucho tiempo para que esto se vuelva un foco de vulnerabilidad ante estos ataques. Las nuevas tecnologías inalámbricas brindan movilidad, agilidad, pero también se ve afectada por el miedo al quedar vulnerable.

Keywords

- telefonía móvil
- PDA
- wireless
- seguridad
- antivirus

Virus Telefónicos

Un virus informático es un programa de computadora, como un procesador de textos, una hoja de cálculo o un juego. Los virus ocupan una cantidad mínima de espacio en el disco, se ejecutan sin el conocimiento del usuario y se dedican a auto-replicarse, es decir se hace copias de sí mismo e infecta archivos, sectores de arranque del disco duro y disquetes para poder expandirse lo más rápido posible.

En los últimos meses se ha detectado un nuevo virus para teléfonos móviles que -al contrario de sus antecesores que usaban tecnologías con muchas limitaciones- se vale de los mensajes multimedia (MMS) enviados desde los teléfonos a otros usuarios. El virus se llama "CommWarrior" y se cree que debido a sus características podría llegar a distribuirse de manera global con la misma velocidad que lo hacen los clásicos gusanos de Internet vía correo electrónico.

Primeros virus de celulares

“CommWarrior” al igual que los primeros virus de celulares, se ejecuta bajo el sistema operativo Symbian. Este gusano además de poder propagarse por Bluetooth, también lo puede hacer a través de mensajes MMS, este tipo de mensajes es muy usado actualmente para el envío de las imágenes y videos obtenidos mediante las cámaras fotográficas que han incorporado los últimos modelos de teléfonos. El hecho de que el virus utilice los mensajes MMS amplía la posibilidad de propagación, ya que este tipo de comunicación, consiste en una simple llamada de teléfono a teléfono. El gusano aparenta ser de origen ruso, y las primeras versiones fueron detectadas en un archivo con extensión (.SIS) acompañado del siguiente texto: "Norton AntiVirus. Released now for mobile, install it!".

Evolución de los virus telefónicos

En el mes de junio de 2004 las compañías de seguridad anunciaron el nacimiento del primer virus para celulares llamado “Cabir” que tiene la capacidad de infectar a través de conexiones “Bluetooth” teléfonos que funcionan con el sistema operativo Symbian. Bluetooth es una norma abierta que posibilita la conexión inalámbrica de corto alcance entre computadoras de escritorio y portátiles, agendas digitales personales, teléfonos móviles y otros dispositivos, y posee un rango de transmisión de muy pocos metros.

La acción de Cabir comienza cuando al seleccionar el archivo infectado, en la pantalla del celular aparece la palabra "Caribe”. A partir de ahí cada vez que se enciende el equipo, el gusano se activa y rastrea el área en busca de otros dispositivos que puedan ser infectados; al encontrar otro teléfono con Bluetooth activado, el virus se replica enviándole una copia.

Este virus podría haber ocasionado grandes desastres si se tiene en cuenta la proliferación del uso de telefonía móvil, pero esto no ocurrió. Es debido a que este gusano fue una "prueba de concepto", un tipo de código creado para demostrar que es posible inventarlo, es decir Cabir fue solo un experimento para demostrar que si se quiere se puede.

Prueba de concepto

Debido a que el gusano requiere la tecnología de Bluetooth para propagarse, geográficamente se obliga a un radio de cerca de 30 metros.

Entonces es dependiente en alguien que tenga su Bluetooth encendido dentro de ese rango. Y favoreciendo a su progreso, cualquier usuario inadvertido en la vecindad tendría que aceptar el virus que sería precedido por una advertencia que la fuente del archivo es desconocida.

Virus Móvil – "Concept Virus"

- Primer Virus Movil del Mundo
- Se adjunta al cuerpo del Mensaje vía Bluetooth
- Se infecta al abrir el archivo adjunto
- Especificamentea algunas series de NOKIA

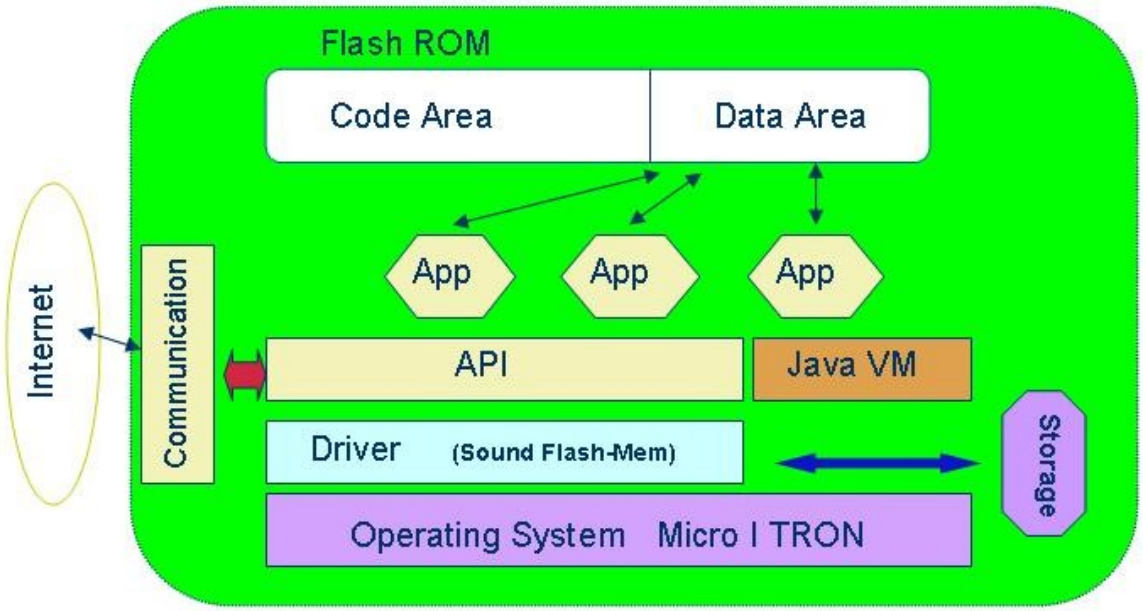
- Primer virus para WinCE en el mundo
- Se copia a si mismo en el archivo abierto
- Se infecta al abrir el archivo infectado
- Solamente a las PDA CE recientes

Ataques Recientes

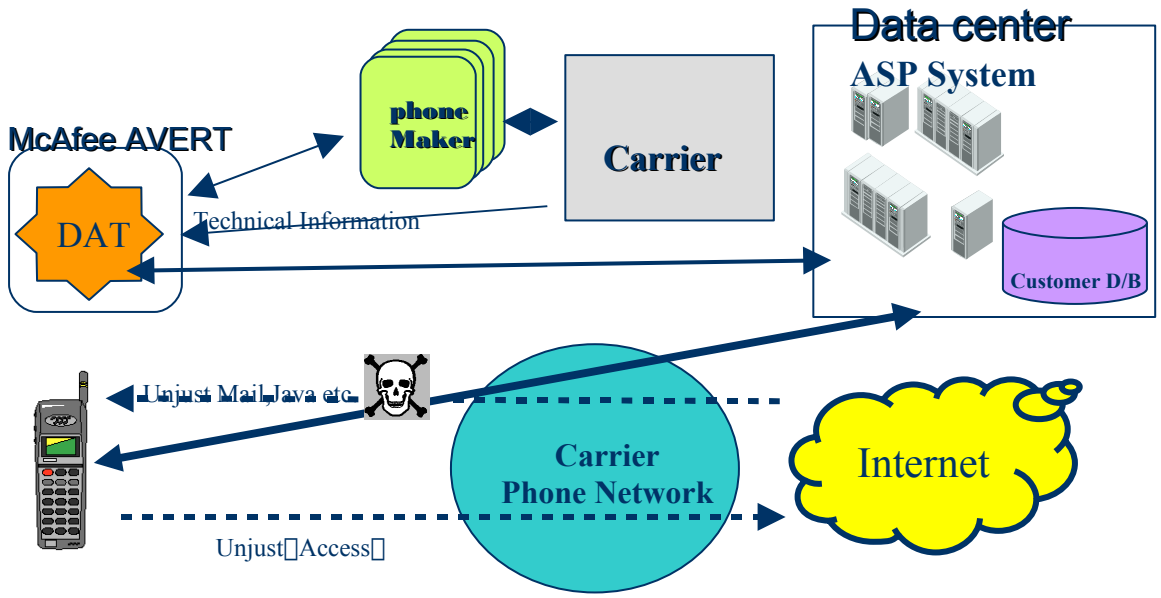
- Cabir. En Junio 20, 2004. Plataforma: Symbian Series 60. Se replica por Bluetooth.
- WinCE DUTS. Julio 17, 2004. Plataforma: Windows CE para las Pocket PCs _. Por file sharing o e-mail.
- WinCE BRADOR. Agosto. 5, 2004. Plataforma: Windows CE para Pocket PCs. Por instalación manual

- Qdial. Ago. 12, 2004. Plataforma: Symbian Series 60. bajando el Jueguito del Mosquito o por file-sharing
- Skulls. 21, 2004. Plataforma: Symbian Series 60. vía download desde el sitio de shareware de Symbian.
- Velasco. Dic. 29, 2004. Plataforma: Symbian Series 60. vía Bluetooth.
- Locknut (Gavno). Feb. 1, 2005; Plataforma: Symbian Series 60. vía download oculto entre los patch de Symbian
- Dampig y Comwar. Marzo 7, 2005. Plataforma: Symbian Series 60. vía Bluetooth ambos.
- 31 de agosto: El Reproductor de MP3, 5GB Zen Neeons , se infecto con Wullik.B (también conocido como Rays.A)
- 27 de agosto: el virus Commwarrior.B por Bluetooth o MMS , en el lobby del Hotel Hilton Bracknell .
- En el concierto de rock *Live 8, mediante Bluetooth*
- En la final del Mundial de Atletismo en Helsinki , también por Bluetooth.

Estructura Dentro del Sistema del Telefono



Overview del Servicio de Telefonía



Antivirus para Celulares

Para contrarrestar esta evolución en los virus que afectan a la telefonía móvil la empresa de seguridad finlandesa F-Secure ya creó un programa de seguridad para proteger a los teléfonos celulares. Muchos expertos en seguridad creen que los virus telefónicos eventualmente se convertirán en una molestia tan grande como los que afectan al sistema operativo Windows.

Algunos Antivirus..

En Junio de 2004 F-Secure crea un programa de seguridad para proteger el teléfono.
En mayo del 2005, Symantec lanza “Mobile Security 4.0” para Symbian

Introducción a Symbian

Symbian es un sistema operativo creado por un consorcio propiedad de Nokia, Motorola, Panasonic, Sony Ericsson, Psion y, recientemente, Siemens
Symbian posee ciertas características que influyen de manera determinante en el desarrollo de aplicaciones. Primero, Symbian es un SO basado en ROM, no siempre ha habido posibilidades de grabar datos en la memoria del teléfono, aunque ahora generalmente se disponga de memorias flash. Segundo, ha sido diseñado para ahorrar batería.

El Micro-kernel de Symbian

Symbian esta basado en un micro kernel. Una mínima porción del sistema tiene privilegios de kernel, el resto se ejecuta con privilegios de usuario, en modo de servidores. Una de las tareas del kernel es manejar las interrupciones y prioridades. En Symbian, cada aplicación corre en sus propios procesos y tiene acceso solo a su propio espacio de memoria. Este diseño hace que las aplicaciones para Symbian sean orientadas a “single threads” y no múltiples.

Aplicaciones para Symbian

Sin embargo no todo iba a ser inconvenientes. El sistema posee componentes que permiten el diseño de aplicaciones multiplataforma, esto es diferentes tamaños de pantalla, color, resolución, teclados, etc. La mayoría de estos componentes han sido diseñados en C++.

Características del Symbian

Todas características permiten que los aparatos con Symbian puedan estar en funcionamiento constante sin necesidad de ser preseteado, preservando la información del usuario y funcionando correctamente (probado en laboratorio). Aunque esto ultimo se esta comprometiendo debido a la complejidad de los últimos aparatos con Symbian y a la multitud de programas externos al SO.

Otros Virus No-Symbian

Ya existen **virus para celulares**. Se llaman Skulls y Cabir (Cabir, considerado el primer gusano de teléfonos móviles, se propaga utilizando servicios Bluetooth, también bajo Symbian.), pero por ahora no provocan una verdadera alarma porque están diseñados sólo para una clase de celulares, los **smartphones (Sistema operativo de Windows para Celulares)**. Los smartphones son teléfonos con algunas prestaciones de computadora de mano, con lo cual tienen incorporado un sistema operativo similar al de las PC. Es por ello que también pueden sufrir algún ataque de virus.

Hace poco en Japón, mensajes electrónicos no convencionales, enviados **a algunos teléfonos móviles con capacidad de leer en su display los mensajes recibidos en las casillas de correo, ocasionaban que dichos teléfonos realizaran llamadas a números telefónicos disponibles para emergencias** (los 911 de muchos países). El proveedor detuvo todo el servicio hasta limpiar el sistema.

Algunas fallas que ocasionan estos virus son:

Se puede bloquear al teléfono móvil que lo recibe. El teléfono literalmente "se cuelga", y es imposible volver a encenderlo. Pero esto solo funciona con modelos específicos, y de ningún modo puede catalogarse de virus.

Un verdadero virus podría hacer cosas como llamar a la policía por si solo, y enviar un mensaje. O enviarse a otros celulares con mensajes infectados. Puede obtener contraseñas, listas de teléfonos y otra información privada y confidencial, y enviarla a un atacante, o simplemente hacerla desaparecer.

Un envío masivo de mensajes SMS podría ocasionar la caída de todo el sistema telefónico, hasta que los mensajes corruptos fueran eliminados de los servidores.

Sistema Smartphone

Pero los nuevos smartphone (teléfonos inteligentes) como algunos modelos de Nokia, Motorola y Mitsubishi, utilizan sistemas bajo Java o plataformas Palm, Microsoft o Symbian, comunes al menos en Europa.

Y ya existen algunas soluciones antivirales preparadas para el sistema operativo de los smartphone. En verdad, tal vez no falte mucho para que sea obligatorio que los celulares también tengan antivirus y cortafuegos instalados.

Nokia y Symantec han llegado a un acuerdo por el cual los smartphones de la Serie 60 van a llevar instalado de serie un software antivirus especialmente diseñado para proteger los móviles de la multinacional finlandesa de amenazas que pudieran poner en peligro la información que los usuarios guardan en los mismos. El acuerdo establece asimismo que ambas compañías se comprometen a desarrollar conjuntamente nuevas tecnologías que mejoren la seguridad en los smartphones.

Dichos gusanos han utilizado los clientes de correo y los navegadores que incorporan los smartphones para propagarse.

Actualmente, los smartphones equipados con Windows Mobile pueden enviar y recibir documentos de Office, que teóricamente pueden transportar programas con virus.

Dickopf señala que los sistemas operativos de telefonía móvil van por la vía de repetir los errores que se cometieron con los sistemas operativos para computadoras. No hacen más que "implementar nuevas funciones, sin tomar en cuenta los efectos que tendrán en la seguridad", sostiene el experto.

Muchos especialistas siguen la línea de pensamiento de Dickopf. Que cuando se trata de seguridad, los fabricantes de teléfonos móviles están pasando la responsabilidad a las firmas de software antivirus. Y al menos una empresa ya empezó a transitar ese camino:

Nokia anunció que venderá sus smartphone series 60, que incluyen Symbian, con Symantec Mobile Security, un nuevo **software de seguridad especial para celulares**.

Así, en breve, los operadores de celulares deberán tomar los mismos resguardos que los de computadoras de escritorio. Por ahora, parece que alcanza con no usar programas que llegan de sitios desconocidos y con **no abrir archivos adjuntos de extraños**. "Con el tiempo se implementarán antivirus, firewalls, programas de codificación y la certificación digital", concluye Wolf.

Otras Amenazas a Dispositivos Móviles

En USA, Japón y Europa, donde los dispositivos móviles son ampliamente usados, se ha sufrido muchos ataques de virus a través de la red wireless. Se han reportado la recepción de mensajes de textos comerciales no solicitados, phishing (engaños al consumidor para que revele información personal llevándolos a un website falso diseñado para parecer al home page de una empresa de prestigio).

Malware

Lasco (enero, 2005): Lasco.A es un virus y gusano. Corre en los teléfonos que ejecutan Symbian y pertenecen a la plataforma s60. Lasco llega al inbox de los mensajes como un archivo velasco.sis, el cual contiene el gusano. Cuando el usuario instala el archivo, el gusano activa el Bluetooth y comienza a buscar a nuevos dispositivos para infectar. Cuando otro dispositivo Bluetooth comienza a enviarle archivos SIS infectados mientras este se encuentre en alcance.

Caballos de Troya

Gavno: Gavno.a y Gavno.b se enmascaran como parches diseñados para engañar a los usuarios para que los bajen. Aunque muy parecido al Gavno.a, el Gavno.b contiene al gusano Cabir, el cual intenta enviar una copia del troyano a otros teléfonos Symbian a través de Bluetooth. Estos troyanos son los primeros en apuntar a funciones centrales de los teléfonos móviles además de text-messaging, email y libretas de direcciones. Gavno.a tiene unos 2KB y viene disfrazado como un archivo SIS llamado patch.sis. Gavno.b es un poco más grande y viene en un archivo patch_v2.sis.

Sybos/Cardtrap (septiembre, 2005): El troyano incluye una variedad virus que se esparcen de teléfono en teléfono vía Bluetooth o MMS. Puede afectar dispositivos móviles que ejecutan sistemas operativos Symbian s60, así como sistemas operativos Windows. Este intenta saltar a la PC copiando dos gusanos de Windows a la tarjeta de memoria del teléfono. Un usuario que inserta esta tarjeta en una PC y hace clic en uno de los archivos infectados activará un gusano que intenta de propagarse a otras PCs en la red.

Más Amenazas

Bancos en USA pueden estar exponiendo los datos de sus clientes ofreciendo servicios de ATM a través de aplicaciones móviles. El servicio utiliza varias funciones de seguridad, entre esto una autenticación de dos pasos. Pero puede ser posible para un hacker pasar sobre medidas accediendo al código fuente de la aplicación misma, debido a que la mayoría de las aplicaciones están escritas en Java 2 Mobile Edition (J2ME).

T-Mobile instaló un firewall en su red GPRS de USA luego de que un pequeño número de clientes se quejaron de recibir hacker probes cuando se encontraban usando su servicio móvil de alta velocidad.

La empresa SecureTest demostró como hackers pueden irrumpir en una aplicación móvil, modificando el código y usar este para manipular el mismo website. Las pruebas incluyeron un website de apuestas falsa con aplicación para apuestas en carreras de caballos y un Sony Ericsson P900 smartphone, el cual utilizaba herramientas freeware.

Una serie de ataques por input validation en la aplicación web móvil permitió modificar el código de la aplicación J2ME para apuestas del teléfono. Luego la aplicación corrupta fue usada como ruta de acceso al website y modificar el contenido de una base de datos de las apuestas.

Robos de datos personales por las compañías ChoicePoint y Lexis-Nexis mediante el uso de spyware. En febrero, ChoicePoint vendió a otras empresas archivos que incluían el número social de 145000 personas.

Resumen

Las actuales amenazas de virus de computadoras están siendo contrarrestadas por los software de antivirus existentes hoy en día. Los teléfonos celulares se acercan cada vez mas a las computadoras, tal es el caso que los mas sofisticados poseen sistemas operativos avanzados y livianos, como el Symbian, que inclusive proveen control sobre los recursos del dispositivo, así mismo como en los PDA.
Además esta provistos de de tecnologías de comunicación inalámbricas como el Bluetooth, esto además de brindar comodidad, también acarrea problemas, ya ser el caso de acceso no permitido a datos del usuario o infestación de virus o gusanos, o mas bien un dolor de cabeza por la preocupación de que esto le suceda si aún no le ocurrió.
Las firmas mas famosas de antivirus ya han lanzado antivirus basado en el sistema operativo de estos dispositivos, la mayoría de estos aparatos utilizan sistemas Symbian que asegura seguridad y tranquilidad al usuario. Veamos más detalladamente estos problemas y soluciones según estos anuncios.

Bibliografía

- http://www.geocities.com/ogmg.rm/QueSon.html
- http://www.vsantivirus.com/08-03-05.htm
- http://www.mouse.cl/2004/rep/08/24/03.asp
- http://news.bbc.co.uk/hi/spanish/international/newsid_4208000/4208170.stm
- http://www.f-secure.com/weblog/archives/archive-082005.html
- Cell Phone Environment & Virus in Japan - Yoshihiro Kato (McAfee Japan)