

Convergencia vírica



La telefonía móvil es un invento que ha revolucionado nuestras vidas, qué duda cabe. Desde 1947, cuando se hicieron los primeros experimentos, hasta nuestros días, pasando por el famoso “ladrillo” DynaTAC 8000X de Motorola presentado en 1984, los cambios han sido muchos, y todos encaminados a mejorar la comunicación, el tamaño y las prestaciones de los teléfonos.

Uno de los problemas que se plantearon cuando la telefonía móvil pasó a ser popular en los años 90 fue la necesidad de establecer un sistema que pudiera asegurar la confidencialidad de las llamadas efectuadas a través de móviles. En los sistemas antiguos, la telefonía no era más que un sistema de radio, más o menos complejo, pero la comunicación podía ser escuchada con suma facilidad, bastaba con que se interceptara la señal.

Entre otras cosas, las tecnologías digitales vinieron a intentar solucionar estos problemas, ya que establecía un sistema de cifrado de las llamadas, facilitado mucho al ser un sistema digital y no analógico. Los terminales establecen la comunicación con la estación base de manera cifrada, de manera que un intento de interceptación no debería tener éxito. Por un lado, la tecnología GSM en Europa y CDMA en América y Asia implementaron las mejoras que se veían necesarias en torno a la confidencialidad de las llamadas.

Sin embargo, estos sistemas de cifrado se han visto rotos hace tiempo, y no es especialmente difícil para un atacante el romper esas claves y en poco tiempo (un par de minutos deben bastar) se puede escuchar la conversación teóricamente segura. Pero esto no viene al caso, estamos hablando de una técnica de hacking que intenta escuchar sin autorización una conversación telefónica entre dos personas, delito contemplado en prácticamente todas las legislaciones del mundo.

En los últimos años nos estamos encontrando con que los terminales móviles no son solo teléfonos. Son complejos ordenadores en miniatura, con capacidades asombrosas si los comparamos no ya con el DynaTAC 800X, sino con los modelos que se ofrecían al público hace solamente un par de años. La similitud entre el ordenador personal y el teléfono es cada vez mayor, y los teléfonos podrán ser (y muchos ya lo son) terminales de ordenador con funciones equivalentes a sus hermanos mayores de sobremesa.

Sin embargo, esta convergencia no solo se dirige hacia las funcionalidades, sino también hacia los problemas. Si en un ordenador personal nos vemos desbordados por el spam, en los móviles ya se deja notar el spam a través de mensajes SMS, y si el teléfono es capaz de recibir correo electrónico, el spam también será un problema en el teléfono.

Cuando la convergencia llegue a un punto en el que se dude entre un ordenador de sobremesa y un móvil (que no portátil), nos encontraremos en una encrucijada muy importante, sobre todo con lo que respecta a la seguridad. Los sistemas telefónicos actuales están funcionando con especificaciones de red GSM (que data de mediados de los 80), GPRS o en el mejor de los casos, UMTS (que data de

Convergencia vírica



principios de los 2000), pero las funcionalidades de los aparatos serán de última generación, diseñados 10 años después que la red sobre la que trabajan.

Aparte de la seguridad en la conversación (que como ya hemos visto es suficientemente débil), los terminales se enfrentan a la convergencia en el malware. Si en los sistemas de sobremesa estamos inmersos en una ingente maraña de malware, los sistemas móviles van a enfrentarse a esas amenazas tan directamente como sus hermanos mayores.

Y ya no hablamos de los tímidos e infructuosos códigos malignos como Cabir o Skull, que han causado más impacto mediático que daños, sino de códigos malignos destinados a robar identidades, contraseñas o cualquier otra información que pueda ser económicamente útil para los hackers. Si el phishing ha tenido éxito en los ordenadores de sobremesa, no cabe duda de que cuando los usuarios empiecen a llevar a cabo operaciones bancarias a través del móvil, también surgirá phishing para ellos. O los troyanos bancarios, que ocultos en la memoria del teléfono esperarán a que el usuario se conecte a la página del banco para capturar su información.

Haciendo “malware ficción”, pueden pensarse en infinidad de problemas que se pueden plantear en un escenario de móviles de ultimísima generación, con conexiones permanentes de banda ancha a varios megabytes por segundo. El tamaño del código malicioso puede dejar de ser un problema, ya que las tarjetas de almacenamiento son casi básicas en los teléfonos nuevos. Imaginémonos un código que llega por bluetooth, y se propaga también por bluetooth. Una vez instalado en el teléfono, los problemas podrían ser numerosos:

- Acceso y modificación de la agenda de teléfonos. Quizá para molestar, pero podría darse el caso de cambiar números de teléfono por otros, como por ejemplo el de la banca telefónica, o bien redirigiendo llamadas a un número de teléfono de coste adicional en un país en el que sea difícil intervenir.
- Modificación de los datos de conexiones. Y vuelta a la conexión con la banca telefónica... sería un caso del phishing pero adaptado a los móviles.
- Interacción con otros dispositivos Bluetooth. Se comentó hace tiempo la posibilidad de que los coches pudieran ser infectados por conexiones bluetooth, cosa que nunca llegó a verificarse, pero ¿por qué no hacer que los orgullosos propietarios de impresoras con conexión bluetooth se vean desbordados con cientos de páginas impresas con caracteres sin sentido enviadas por un código malicioso a la impresora?
- Perturbaciones en las funciones añadidas de los móviles. Quizá pueda ser algo tan simple y molesto como hacer que el GPS incorporado en el terminal haga que nos perdamos o que tomemos direcciones prohibidas, o nos deje en mitad del recorrido sin indicaciones.
- Adware. Un código malicioso que interrumpa la comunicación telefónica para mostrar un anuncio a los interlocutores. Molesto y efectivo.

Convergencia vírica



- Zombis telefónicos. La instalación de un bot en un teléfono, que consigue dejar a merced del propietario del código el dispositivo infectado, para envío de spam, ataques de denegación de servicios...
- Falseamiento de sistemas de pago y verificación. Ya existen sistemas de pago mediante el teléfono móvil, como Mobipay, que podrían verse afectados por malware, o al menos falseados sus datos, al igual que los sistemas de verificación de transacciones de tarjetas de crédito a través del móvil.

¿Queremos llegar al extremo? Un código que, aprovechándose del GPS del sistema (o simplemente las funciones de localización GSM), pueda servir para localizar exactamente al usuario. Aquí entramos en las barreras de la seguridad personal, en el que no solo se pierde la intimidad de las comunicaciones, sino que puede ser controlado cada movimiento del portador del teléfono. Los delincuentes pueden llegar a más que un ataque informático con todos esos datos.

Los operadores de telefonía poco podrán hacer en estos casos. Cualquier intento de búsqueda de códigos maliciosos fracasaría al estar cifrada la comunicación, romper esa cifra supondría quebrantar la ley y para colmo no ayudaría porque el peligro no está en esa comunicación, sino en el terminal.

La única manera de introducir códigos maliciosos en los terminales antiguos (al menos teóricamente) sería una llamada, un mensaje o directamente por el teclado, que en la práctica se demostró imposible. Los teléfonos que siguieron ya podían conectarse a los ordenadores personales mediante cable, infrarrojos o Bluetooth, en donde ya sí que es factible la introducción de código. Y muy fácil.

Basta con acercarse a un aeropuerto, por ejemplo (lo ideal es cerca de la sala VIP; donde se encontrarán teléfonos más caros y más modernos) e iniciar una búsqueda de dispositivos Bluetooth. El momento en que yo me encontré con menos teléfonos dispuestos a conectarse con mi ordenador fue de madrugada, en el que había no menos de 10. Imaginémosnos en una hora punta, o los días de salida de vacaciones.

Está claro que en el futuro la protección contra amenazas va a ser un elemento básico en los terminales móviles. Y no solo contra virus, sino contra las amenazas que pueden poner en peligro los datos del usuario. Y no hablo de los MP3 de la tarjeta SD del teléfono, sino de las contraseñas del banco. La protección deberá basarse en la vigilancia de dos puntos básicos:

- Protección de archivos y mensajes entrantes de correo y multimedia contra todo tipo de malware.
- Protección de comunicaciones no telefónicas, como puede ser la infrarroja o Bluetooth.

Así, el sistema podrá tener un punto de seguridad muy elevado, a la que habrá que añadir la necesidad de comprender el teléfono y sus funciones, de qué hace y cómo lo hace. Pero en sistemas cuya documentación pesa y ocupa mucho más que el

Convergencia vírica



propio dispositivo, pocos compradores tecnológicos compulsivos van a hacer uso del manual aparte de ver cómo se cambian las melodías o se bajan nuevos juegos.

A finales de los años 80, cuando los problemas por los primeros virus para PC empezaron a surgir, se empezaron a implementar soluciones que a duras penas sirven hoy en día. Las empresas desarrolladoras de sistemas de telefonía y las de seguridad deben hacer un esfuerzo en común para que los errores cometidos a lo largo de 20 años de historia del malware no se repitan en los próximos 20 meses de historia de la telefonía móvil.

Fernando de la Cuadra
Editor Técnico Internacional
Panda Software (<http://www.pandasoftware.com>)
E-mail: Fdelacuadra@pandasoftware.com