Universidad de Valladolid
E.T.S Ingeniería Informática
Grado en Ingeniería Informática
Mención de Ingeniería de Software

Seguridad en Sistemas Móviles

Bayón Sanz, Miguel
Curso 2020/2021

Índice

1. Introducción

Debido a la inmensa expansión de las telecomunicaciones en todos los aspectos de la vida, tanto para el uso cotidiano como para el trabajo, se ha generado un nuevo campo donde es necesario protegerse de ciertos ataques que pueden poner en peligro nuestra información, seguridad y bienestar. Esto, añadido a que hoy en día todo el mundo tiene un móvil con información confidencial o sumamente importante como sus cuentas bancarias o su dirección postal, hace de estos dispositivos el principal objetivo de las amenazas cibernéticas.

Todo esto hace que sea necesario revisar la seguridad de los dispositivos móviles en todos los aspectos relacionados con este:

1. Confidencialidad: protección de datos y de información intercambiada entre un emisor y uno o más destinatarios frente a terceros
2. Integridad: propiedad que busca mantener los datos libres de modificaciones no autorizadas.
3. Disponibilidad:propiedad que permite a un sistema informático mantenerse trabajando sin sufrir ninguna degradación en cuanto a accesos.
4. Autenticidad: propiedad que permite demostrar cuál es el origen real de la información recibida.
5. Trazabilidad: propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

Además, se considera dispositivo móvil todo dispositivo de uso personal o profesional de tamaño reducido que permite la gestión de información y el acceso a redes de comunicaciones, tanto de voz como de datos, y que habitualmente dispone de capacidades de telefonía y agendas electrónicas.

En los últimos años, se han venido recibiendo amenazas en la seguridad de estos dispositivos mediante ataques que se centran en las diferentes vulnerabilidades en los móviles. Resulta conveniente conocer un mínimo sobre estos ataques para poder analizar tanto riesgos y amenazas como vulnerabilidades a los que se exponen estos sistemas.

2. Dispositivos móviles: capacidades y funcionalidad

Actualmente, los sistemas móviles ofrecen una gama de funcionalidades igual o superior al de algunos sistemas informáticos comunes, llegando a incluir herramientas menos comunes como Bluetooth, acelerómetros, GPS, antenas de comunicación (para telefonía e Internet) o pantallas táctiles; y herramientas más comunes como son cámaras, micrófonos o entradas USB y de auriculares.

Por otro lado, es importante mencionar que los sistemas operativos utilizados en móviles son actualmente especializados en estos mismos, destacando sobre otros el sistema Android y el sistema iOS, los actuales líderes del mercado, aunque existen también otros que se han descatalogado o que no son tan conocidos, como Windows Mobile o los basados en Linux.

A pesar de que hasta ahora se han mencionado solamente los móviles dentro de estos sistemas móviles, también cabe destacar que otros dispositivos como las tablets Android o los iPad de Apple entran en estas categorías al coincidir plenamente en la descripción dada sobre los dispositivos móviles y contienen los mismos sistemas operativos.

En cuestiones de Software, los dispositivos móviles son capaces de manejar información transmitida a través de llamadas, correo electrónico, redes sociales, navegadores, mensajería instantánea, servicios de pago electrónico, localización, etc. Al estar la información tan centralizada, cualquier ataque dirigido a uno de estos dispositivos supondría un gran problema tanto para particulares como para profesionales y empresas, y por esto mismo muchas compañías optan por restringir las aplicaciones y las comunicaciones de los sistemas móviles, definiendo listas blancas y negras de Software, conexiones, teléfonos, información almacenada...

3. Amenazas para los sistemas móviles

Son muchos los ataques que se realizan a los dispositivos que nos incumben, pero muchas de las vulnerabilidades y las amenazas que los rodean son conocidas al ser comunes con los clásicos sistemas informáticos. Según el CCN-CERT, los sistemas operativos dedicados para móviles están cada vez más ocupados en mejorar su seguridad, siendo capaces en la actualidad de encontrar y parar hasta un 73 % de las amenazas.

La importancia de la seguridad en los dispositivos quedó reflejada 2009 en eventos realizados como el Pwn2Own, que premiaban a los participantes que encontrasen nuevas vulnerabilidades en los terminales más comunes de la época, como eran la Blackberry, iPhone, Android o Windows Phone.

Aún con todos los avances en seguridad conseguidos hasta la fecha, es importante remarcar que riesgos tan primitivos como la pérdida o el robo del móvil puedan suponer gravísimo riesgo a la hora de mantener la confidencialidad de los datos, pudiendo un atacante obtener información, suplantar la identidad del usuario o incluso robar dinero de su propia cuenta bancaria.

3.1. Acceso físico

El acceso físico ha sido, y sigue siendo, uno de los ataques más potentes y con menos defensas que existen, permitiendo acceder a toda la información almacenada por el aparato o incluso pudiendo instalar Software de espionaje en un breve periodo de conexión física.

Así, algunos programas de espionaje como Pegasus, permitirían acceder a llamadas, capturar mensajes, realizar fotos, obtener ubicaciones, etc. desde un lugar remoto, vulnerando la confidencialidad y la integridad del atacado. Pese a que muchos de estos programas Spyware eran instalados de manera física en los móviles, otros aprovechaban vulnerabilidades de programas instalados para infiltrarse e instalarse de manera no autorizada. Ese es el caso del Spyware mencionado, que fue instalado en el móvil del político catalán Roger Torrent aprovechando una vulnerabilidad de las videollamadas de Whatsapp.

El acceso físico a los dispositivos móviles actualmente cuenta con fuertes métodos de seguridad además del código PIN. El más común, el lector de huella dactilar, resulta irrompible ante ataques indeseados mediante métodos tradicionales y ofrece una capa de seguridad alta tanto para desbloquear el móvil como para, en algunos móviles, bloquear aplicaciones con contenido sensible como aplicaciones bancarias. Sin embargo, estas capas de seguridad suelen tener una alternativa más simple como un pequeño pin o un patrón, y a día de hoy muchos usuarios siguen introduciendo códigos pin tan simples como '0000' o '1234', lo que hace a la otra capa inútil ante ataques clásicos.

3.2. Seguridad de los sistemas operativos

Los sistemas operativos principales (Android e iOS) publican, de forma periódica y frecuente, las vulnerabilidades de sus versiones anteriores para indicar la cobertura de la última versión ante nuevas amenazas. Al hacer esto público, todos los usuarios que no estén actualizados estarán expuestos a riesgos de seguridad públicos, algo ya aprovechado en numerosas ocasiones en el pasado.

Por suerte, esta vulnerabilidad es fácil de evitar simplemente mediante la actualización del sistema operativo a su versión más reciente, siendo el único inconveniente la obsolescencia programada de los dispositivos, que hagan a los dispositivos incompatibles con ciertas versiones del sistema.

El acceso libre a numerosas y variadas aplicaciones, el acceso fácil a la web y la gran variedad de servicios que ofrece un dispositivo en estos años favorece el gran almacenamiento de información del usuario dentro del mismo. Desde información teóricamente banal como listas de tareas hasta información altamente importante como la ya mencionada cuenta bancaria, toda esta información puede describirnos a la perfección ante cualquier persona que tenga acceso a ella.

Existe un peligro potencial de acceso a toda esta información a través del mencionado Spyware, pero otras aplicaciones instaladas a partir de la tienda que ofrezca el sistema operativo (Apple Store y Play Store entre otras) también podría acceder a estas de manera sencilla. El sistema operativo cuenta con métodos de cifrado de información para evitar robo de datos por parte de fuentes no permitidas, pero conviene en todo momento ser consciente de las aplicaciones que tenemos instaladas y de los permisos que nos piden para evitar que adquieran más información de la debida y, ante todo, evitar instalar aplicaciones poco fiables que puedan potencialmente robarnos información para ofrecérsela a terceros.

3.3. GPS y sistemas de geolocalización

Cada vez más, los móviles amplían sus funcionalidades en relación a la ubicación física del usuario. Gracias a estos, una persona podría en cualquier momento encontrar fácilmente un restaurante cercano donde comer, un monumento histórico que visitar o una gasolinera donde repostar, por no hablar de otras aplicaciones que han ido surgiendo y que utilizan la geolocalización para ubicar en un lugar del mapa, por ejemplo, un vídeo subido a una red social o para jugar a juegos que sitúan eventos en las calles de las ciudades.

Todo esto hace que los usuarios de dispositivos móviles se «olviden» cada vez más de apagar la geolocalización por GPS, manteniéndose en todo momento localizado y pudiendo tener un gran problema de privacidad en caso de que esa ubicación sea accedida de manera fraudulenta.

Estas aplicaciones de las que hemos hablado suponen un problema para la privacidad de los usuarios, debido a que el robo de información en dichas aplicaciones podría implicar la obtención de la ubicación geográfica del usuario y revelar datos como la dirección del hogar. Todo esto suponiendo que la aplicación es fiable, pero si un usuario, como se dijo antes, instalase una aplicación que tuviese como intención oculta el robo de información del usuario y la aplicación se hiciese con los datos de localización y los mandase a sus servidores, podría hacer con esa información lo que quisiera.

3.4. Comunicación inalámbrica

Los móviles actuales cuentan con múltiples vías de comunicación que pasan desde los ya poco utilizados SMS hasta el Bluetooth, el Wi-Fi o el 4G (incluido el 5G dentro de poco). Cada uno de estos supone, de manera individual, una puerta de entrada para las diferentes amenazas existentes para los dispositivos, algunos de ellos permitiendo evitar cortafuegos u otras medidas de seguridad de nuestros pequeños sistemas.

3.4.1. Bluetooth

La tecnología Bluetooth ha sido estudiada desde su creación en el ámbito de la seguridad y ataques y, aún así, sigue siendo una amenaza por las debilidades de las que consta.

Un dispositivo que utilice esta tecnología está expuesto, entre otras cosas, a la captura de sus datos por parte de un tercero (lastimando su confidencialidad), a ataques sobre el pin de autenticación para la suplantación del dispositivo emparejado (afectando su integridad) y a ataques de denegación de servicio (limitando su disponibilidad).

Son muchos los ataques que se han realizado a través de este tipo de comunicación, siendo uno de los más recientes el BLURtooth, uno capaz de aprovecharse de las debilidades encontradas en las versiones 4.0 y 5.1 de Bluetooth y del que aún no se ha encontrado ninguna solución por parte de los diseñadores y desarrolladores de dicha tecnología.

BLURtooth se aprovecha de una vulnerabilidad en el estándar CTKD para hacerse pasar por un dispositivo ya conectado con el móvil, utilizando además su pin de autenticación para acceder a todo aquello a lo que el dispositivo original podía acceder, como pueda ser la agenda telefónica o la voz en el caso de los auriculares inalámbricos.

3.4.2. Wi-Fi

La conexión por Wi-Fi, sobre todo cuando esta conexión está expuesta para el uso público, siempre ha supuesto un grave peligro para todo tipo de dispositivos.

La ausencia de mecanismos de autentificación y cifrado en una conexión Wi-Fi puede facilitar ataques orientados a la captura e interceptación de datos por parte de un tercero (afectando a la confidencialidad), a la inyección de tráfico, a la suplantación de la red (ultrajando la integridad) y a la denegación de servicio (afectando a la disponibilidad).

3.4.3. SMS

Uno de los sistemas actualmente menos usados por usuarios para mensajería, el SMS (con sus sucesores, el EMS y el MMS), también fue utilizado en su momento para realizar una serie de ataques a dispositivos móviles. En 2009, se detectaron varios casos de ataque de denegación de servicio a dispositivos Android, iPhone y Windows Phone, llegando en algunos casos a ser también ataques a la confidencialidad al conseguir la transferencia de ficheros y ejecución de código sin intervención del usuario.

En el caso de iPhone, se llegó a publicar una vulnerabilidad relacionada con la decodificación de los mensajes SMS, a través del cual se podría provocar una denegación de servicio o incluso una toma del control del dispositivo mediante ejecución remota de código, de nuevo, sin necesidad de ningún tipo de intervención por parte del usuario. Debido a esto, Apple se vio obligado a lanzar rápidamente una nueva actualización que cubriese esta debilidad, demostrando la importancia de nuevo de mantener los dispositivos actualizados en todo momento.

Otro ataque similar, en este caso válido tanto contra iPhone como contra Android, permitía desconectar al móvil de la red móvil, pudiendo así realizar ataques de denegación de servicio contra el usuario.

Por último, es necesario comentar que algunos ataques mucho más sencillos y dirigidos a gente no familiarizada aún con las tecnologías llevan mucho tiempo realizándose, y algo tan sencillo como mandar un SMS con mensaje engañoso que invita a entrar en un link donde se entregue información confidencial o descargue un Malware puede hacer que mucha gente caiga en la trampa.

3.4.4. 2G y 3G

Uno de los grandes ataques realizados sobre las conexiones 2G ha sido la suplantación de la propia red de telefonía móvil: un atacante podría suplantar una celda GSM mediante tecnología 2G sin necesidad de autenticación mutua debido a las propiedades de la tecnología y realizar un ataque del tipo Man-in-the-Middle. Un problema adicional de este tipo de ataques es que los dispositivos se conectan automáticamente a la celda con más señal detectada sin ningún tipo de opción por parte del usuario, de modo que un atacante simplemente necesitaría generar una celda con mayor potencia que las de su alrededor para comenzar su ataque. Así, un atacante podría redirigir llamadas salientes, manipular los SMS enviados y recibidos, leer los datos de navegación de la víctima...

En la tecnología 3G, los ataques basados en la falta de autentificación son inútiles debido a la presencia de estos en los mensajes y a un algoritmo de cifrado mutuo. Sin embargo, un atacante puede forzar a un dispositivo a funcionar bajo la tecnología 2G para aprovecharse de sus debilidades al tener todos los dispositivos capacidades GSM.

Pese a todo, la tecnología 3G tampoco se libra de fallos de seguridad. Un fallo con la clave de validación entre la red y el servidor de comunicaciones ha sido descubierto recientemente y se dice que permite a un atacante observar los movimientos en la conexión del usuario sin que este se dé cuenta, afectando así a su confidencialidad.

3.4.5. NFC

La tecnología NFC ha sido introducida hace pocos años en los móviles para ciertos tipos de comunicaciones relacionados sobre todo con pagos, sustituyendo ampliamente a las tarjetas de crédito y débito. Constituyen un problema menor al tener una distancia física de efectividad muy reducida, pero siguen existiendo algunos tipos de ataque como la interceptación de datos, en los que el atacante utiliza un dispositivo que actúa como intermediador entre emisor y receptor en la comunicación, pudiendo leer y alterar la información emitida.

Existen otros tipos de ataque que aplican actuaciones similares, como el ataque de escucha, en el que una comunicación que no tenga establecido un canal seguro podría ser «escuchado» por dispositivos cercanos, obteniendo toda la información intercambiada.

3.5. Aplicaciones

La gama existente de aplicaciones en las tiendas de los sistemas operativos actuales es sumamente amplia: desde juegos hasta programas de banca online o incluso ampliaciones de funcionalidades del móvil. La ampliación de esa gama es incentivada además por parte de los fabricantes a través de plataformas de desarrollo como Android Studio que facilitan el lanzamiento de nuevas aplicaciones.

Algunos ataques se aprovechan de la integración de estas aplicaciones con servicios anteriores como los SMS para falsear mensajes. Por otro lado, también se aprovechan de las descargas, instalaciones y ejecuciones de aplicaciones no certificadas para introducir Malware en los sistemas móviles.

También, por la amplia expansión de las redes sociales y su integración y aceptación en los móviles como estándar, han aumentado los ataques a móviles para conseguir robos de identidad, distribución de Malware a través de estas redes, revelación de información sensible e incluso la anteriormente mencionada localización física del usuario, implicando todo esto un serio problema en la confidencialidad de los usuarios.

Aún limitando el uso de las redes sociales en los móviles, otro gran problema pasaría por las trazas dejadas por otras aplicaciones durante su uso, pudiendo estas ser rastreadas y utilizadas en contra del propio usuario. A esto hay que añadirle las aplicaciones con micropagos incluidos o cuyo fin es el movimiento de dinero, que pueden generar a su alrededor amenazas de fraude muy lucrativas para el atacante. Para solucionar esto, se está utilizando ampliamente métodos de autentificación de dos factores a través de SMS, por donde se recibe un pin temporal que servirá como confirmación para realizar el pago. Sin embargo, para este último factor de confirmación hay que volver a tener en cuenta las debilidades mostradas por los SMS ante ataques ya conocidos.

3.6. Malware en móviles

Las primeras apariciones de Malware dirigidas a los teléfonos con sistemas operativos actuales (Android y iPhone), aunque con versiones anteriores, fueron en 2009, cuando pudieron infectarse tanto móviles Android como iPhone que hubiesen realizado el jailbreak del terminal. Fue en este año cuando apareció un gusano distribuido por SMS llamado YXE, que utilizaba la ingeniería social para que, al pulsar sobre el enlace enviado en el mismo SMS, se instalase Software malicioso. Al instalarse este programa en el dispositivo, aprovecharía su control sobre el móvil para reenviar el SMS a toda la agenda del móvil y, aprovechando que probablemente los receptores conozcan al emisor y se fíen de él, abran el enlace.

Aparte del método de propagación, el Software malicioso reenviaba información sobre el dispositivo en el que estaba instalado al atacante, como el IMEI y el IMSI, teniendo además que pagar la víctima el envío de todos los SMS que produjo el ataque.

Más tarde en 2010, este mismo ataque se replicaría con el nombre de LanPackage, manteniendo el método de propagación e infección.

Las amenazas relacionadas con el reenvío masivo de SMS suponen un problema por dos debilidades distintas: por un lado, se instalan troyanos multiplataforma desarrollados en Java, lenguaje interpretado por todos los dispositivos actuales; por otro, el SMS se puede utilizar para instar a un usuario a llamar a un número de teléfono del atacante para robarle, a través de este, información sensible por medio del Phising.

Actualmente, este problema no esta sujeto únicamente a los SMS: al tener los móviles aplicaciones para leer y mantener actualizado el correo electrónico, este es también otro medio por el que se puede percibir el mismo tipo de ataque. Siguen sin ser excepción en este caso las redes sociales, donde muchas veces se utiliza la misma vía para engañar a otros usuarios en cadena, utilizando los chats instantáneos que tienen integrados.

3.7. Malware y Jailbreak

Algunos sistemas operativos, como es el caso del iPhone de Apple, mantienen unas restricciones duras con respecto a instalación de aplicaciones y descarga de contenido con la excusa de evitar la aparición de virus. Estas limitaciones pueden ser resueltas mediante el proceso jailbreak, teniendo un equivalente en Android llamado root.

Mediante el jailbreak, un usuario sería capaz de acceder a todas las funcionalidades y partes del sistema operativo, rompiendo los mecanismos de protección del terminal y permitiendo la instalación de cualquier aplicación o programa compatible. Esto, debido a las altas restricciones de Apple, fue muy implementado durante varios años por los usuarios.

La gran ventaja pasa a su vez a ser desventaja al invalidar los mecanismos de verificación de código del sistema, que comprueban la legitimidad de las aplicaciones antes de ser instaladas. Con este proceso, también se facilita la entrada e instalación de Software malicioso, evitando así todas las restricciones que impone, en este caso Apple, para que una aplicación se legitime para entrar en su Store.

En el caso de Android, en comparación con Apple, es más fácil instalar aplicaciones sin ningún tipo de legitimidad, desactivando simplemente la opción que impide la instalación de código que contenga estas características. Antes de ser completamente desactivado, Android avisará de la inseguridad que generará el desactivar esta opción.

Una vez realizado el jailbreak en los sistemas iPhone, se podía utilizar herramientas de acceso remoto mediante SSH. Para esto era necesario identificarse, pero la funcionalidad poseía una contraseña por defecto conocida que podía ser utilizada por cualquiera si no era alterada. Los gusanos *Ikee* y *Duh* explotaban esta vulnerabilidad autenticándose como root en el sistema y propagando Malware una vez dentro.

Mientras que el gusano Ikee surgió más como una broma al cambiar el fondo de escrito por una imagen de Rick Astley para, justo después, desactivar el servicio SSH, el gusano Duh, basado en el código del primero una vez se liberó, cambiaba la contraseña del root de SSH, descargaba ficheros y ejecutables de un servidor, enviaba información del dispositivo al mismo servidor y finalizaba realizando un ataque de phishing orientado a usuarios holandeses para la captura de credenciales del banco ING.

Otra gran desventaja del jailbreak era la incapacidad de actualizar el sistema operativo al considerarse usuario «no oficial» hasta varios días más tarde, tiempo durante el cual, como se dijo anteriormente, están expuestos a ataques de vulnerabilidades conocidas y solucionadas en el nuevo parche.

4. Recomendaciones de seguridad en móviles

Para evitar o mitigar todos los ataques y vulnerabilidades anteriormente descritas, existen una serie de pautas que, dependiendo del dispositivo y la tecnología, pueden ser implementadas. Esto podría proteger no solo la integridad del dispositivo y sus capacidades sino que también la información que gestiona y que almacena.

Hay que tener en cuenta que, con el crecimiento de los ataques, los dispositivos móviles comenzaron a integrar antivirus y aplicaciones de seguridad que combaten eficientemente gran parte de las amenazas. Sin embargo, añadir esta capa extra de seguridad permitirá asegurar la integridad y confidencialidad del dispositivo perfectamente.

4.1. Acceso físico

La norma siempre, en estos casos y como siempre ha sido, es no dejar el móvil desatendido y menos aún si está desbloqueado. Con la configuración y los cables necesarios, un atacante podría en muy pocos segundos instalar una aplicación maliciosa o comprometer la seguridad del dispositivo. De la misma manera, si nos robasen el dispositivo tendrían muchas más posibilidades de robar información peligrosa del mismo sin las complicaciones del otro escenario.

Obviamente, otra de las normas para estas situaciones es tener un bloqueo con pin, patrón o alguna de las formas de identificación que permiten los móviles modernos (detección facial, huella dactilar). A su vez, cuanto más complicado sea este código, más difícil de adivinar será. Conviene también activar el bloqueo de pantalla automáticamente tras un tiempo, siendo recomendado 1 minuto para esto.

Además, es importante mantener siempre el código PIN de la tarjeta del móvil activada. Esta ofrece una gran capa de seguridad si se enciende desde cero el móvil, al dar tan solo 3 oportunidades de desbloquear con el PIN antes de activar el código PUK (Personal Unblocking Key). Estos datos deben ser tratados siempre como confidenciales y no ser compartidos jamás.

Desde el punto de vista de la seguridad, se desaconseja totalmente que el móvil muestre información o notificaciones mientras tenga el bloqueo activado, de modo que si alguien pretende hacerse con información del dispositivo, tenga obligatoriamente que intentar desbloquear el sistema. Además, si el sistema tiene una opción de borrado total de información tras múltiples intentos de desbloqueo, se aconseja totalmente activar dicha opción para mayor protección de datos.

Por último, en caso de extravío o robo se recomienda cambiar inmediatamente las contraseñas de todos los servicios utilizados dentro del móvil y cancelar los servicios de telefonía del dispositivo para evitar pérdidas enormes de información y consumos costosos o malintencionados de servicios por parte del atacante.

4.2. Sistemas operativos

Desde el punto de vista de la seguridad se recomienda altamente desactivar todo servicio (GPS, Bluetooth, Wi-Fi) que no esté siendo utilizado para reducir los vectores de ataque.

También conviene recordar que la actualización de los sistemas operativos al momento de salida son cruciales para evitar ataques conocidos, aunque también conviene a veces comprobar si aquellas vulnerabilidades que dice solucionar la actualización nos afectan antes de actualizar.

4.3. Configuración del dispositivo

Una vez iniciado un móvil por primera vez, conviene entrar en su configuración y modificar ciertas opciones optimizadas a la facilidad de uso y al disfrute en vez de a la seguridad del mismo. Además, hay que tener muy en cuenta que ejecutar técnicas como jailbreak en los dispositivos reduce drásticamente la seguridad permitiendo, como dijimos antes, realizar nuevos ataques por medio de SSH, por ejemplo.

4.4. Almacenamiento de información

Una medida para proteger la información contenida dentro del móvil es la utilización de sistemas de cifrado de datos. Actualmente, los propios sistemas operativos permiten el cifrado de datos con claves biométricas, lo cual es una gran capa de seguridad. Cabe indicar que, si el móvil cuenta con una tarjeta SD extraíble, también sería de especial importancia cifrar esa información.

Es importante mencionar que el cifrado genera un impacto directo en el rendimiento del sistema, aunque los sistemas modernos cada vez sufren menos ese impacto.

También es recomendable contar con una copia de seguridad actualizada de los datos contenidos en el móvil, y por razones obvias es altamente recomendable no almacenar contraseñas, información sobre cuentas, datos sensibles o códigos PIN de ningún servicio en el móvil.

4.5. Bluetooth

En adición a la recomendación anterior de desconectar todo servicio que no se vaya a utilizar, acerca del Bluetooth se recomienda también activarlo en modo oculto cuando se vaya a utilizar. También es recomendable cambiar el nombre de la conexión ofrecido por defecto, debido a que suele incluir información sobre el dispositivo que puede ayudar a ubicarlo si se está haciendo un rastreo de dispositivos. Tampoco se recomienda en ningún caso que el nombre describa a la persona o empresa a la que pertenezca.

El proceso de emparejamiento por el sistema Bluetooth es especialmente delicado y conviene hacerlo en lugares privados o con poca gente debido a la posibilidad de obtención del código de emparejamiento por parte de un atacante.

Conviene también utilizar las versiones más actualizadas de la tecnología Bluetooth, que contienen sistemas de emparejamiento más seguros. También, aunque los creadores de la tecnología recomienden el uso de 4 caracteres para el pin de emparejamiento, desde el punto de vista de seguridad se hace hincapié en que una contraseña larga es siempre más segura, pudiendo en esta tecnología usar hasta 16 caracteres alfanuméricos.

4.6. Wi-Fi

Además de la recomendación anterior sobre desconectar servicios que no estén en uso, si se va a utilizar el servicio Wi-Fi se recomienda, ante todo, utilizar solo aquellas conexiones que tengan un nivel de seguridad alto, recomendando el sistema WPA2 antes que WPA o WEP. Además, si contamos con el control de esta señal Wi-Fi, sería aconsejable que la contraseña sea larga (más de 20 caracteres) y difícilmente adivinable.

Si es necesario conectarse a una red Wi-Fi insegura, se recomienda utilizar tecnologías VPN, capaces de cifrar la información transmitida en la comunicación y minimizando la capacidad de ataques. Esto, además, se recomienda en cualquier otro tipo de conexión.

Por lo general, los móviles cuentan con un registro de todas las conexiones Wi-Fi junto con sus contraseñas (si las tienen) para poder conectarse de nuevo automáticamente en caso de volver a encontrarlas. Se recomienda configurar al móvil para que no se realice esa conexión de manera automática. De la misma manera, se recomienda borrar de esa lista todas aquellas señales a las que se haya conectado de manera temporal o que no sean conexiones habituales con una seguridad adecuada.

4.7. Comunicaciones de telefonía móvil

Tal y como se lleva diciendo hasta ahora, la comunicación por datos móviles debe ser desactivada si no está siendo usada, aunque en este caso sería solo para casos concretos donde su uso no es relevante (debido a la necesidad en algunos casos de mantener la conexión).

Es importante al utilizar esta tecnología no asumir la confidencialidad de la conversación. Para proteger la confidencialidad, pueden utilizarse productos de cifrado de extremo a extremo y que protejan la información transmitida.

La recepción de SMS supone un problema grave en sí, y para minimizar su amenaza, se recomienda tanto mantener el sistema operativo actualizado siempre que se pueda como no abrir los mensajes siempre que no sean esperados o solicitados, algo similar a los correos electrónicos recibidos en un sistema de mensajería.

A la hora de conectarse a través de datos móviles a Internet, se recomienda utilizar la tecnología 3G o superior antes que la 2G debido a la cantidad menor de amenazas que suponen aquellos frente a este último.

4.8. Aplicaciones

Se recomienda instalar única y exclusivamente aplicaciones ubicadas en la tienda oficial del fabricante (Apple Store o Play Store). Por supuesto, por las mismas razones, se desaconseja totalmente el uso de jailbreak.

Almacenar contraseñas en el móvil para que inicie automáticamente las aplicaciones resulta más inseguro que insertar cada vez la contraseña, recomendándose siempre esta segunda opción.

Se recomienda desactivar en las aplicaciones instaladas los permisos que no sean estrictamente necesarios para el correcto funcionamiento de la misma. Así mismo, se recomienda controlar e incluso limitar el número de aplicaciones instaladas, dado que no todas las aplicaciones que han pasado las restricciones de las tiendas oficiales tienen por qué ser legítimas.

Al igual que en los navegadores para ordenadores de sobremesa, se recomienda tener una serie de precauciones generales con los navegadores diseñados para móvil, siendo las más importantes desactivar Javascript y plug-ins y activando solo los necesarios en momentos necesarios, activar la detección de sitios sospechosos del navegador, deshabilitar el autocompletado de contraseña del navegador y eliminar las contraseñas y credenciales guardadas.

Por supuesto, se recomienda pensar fríamente y con responsabilidad qué tipo de información, tanto personal como profesional, se va a compartir por redes sociales y otras aplicaciones web que pueda derivar en la obtención ilegítima de dichos datos.

4.9. Trazabilidad

Para rastrear actividades sospechosas en el móvil en caso de posible ataque, se recomienda activar los registros de eventos y la obtención de logs (mensajes).

4.10. Software de seguridad

Los móviles cuentan cada vez más con un antivirus o un sistema de seguridad integrado desde el primer encendido. Sin embargo, en otros casos, estos vienen con la seguridad básica del sistema operativo. Existen múltiples antivirus en las tiendas oficiales de los fabricantes (Avast, Panda, McCaffee...) accesibles para todos los usuarios por su carácter gratuito que permiten otra capa de seguridad ante cualquier tipo de ataque.

5. Bibliografía

[1] *Esquema Nacional de Seguridad*. dirección: https://www.ccn-cert.cni.es/publico/ens/ens/index.html#!1067.

[2] *BOE 29/01/2010: Sobre la Seguridad en el Ámbito de la Administración Electrónica*. dirección: www.boe.es/boe/dias/2010/01/29/pdfs/BOE-A-2010-1330.pdf.

[3] *Informe de amenazas del año 2019 del CCN-CERT*. dirección: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4625-ccn-cert-ia-03-20-informe-anual-2019-dispositivos-y-comunicaciones-moviles-1/file.html.

[4] *El País: Así funciona Pegasus: el software de espionaje más célebre del mundo*. dirección: https://elpais.com/tecnologia/2020-07-18/asi-funciona-pegasus-el-software-de-espionaje-mas-celebre-del-mundo.html.

[5] *Android Security Team*. dirección: https://groups.google.com/g/android-security-announce/c/aEba2l7U23A.

[6] *Actualizaciones de seguridad de Apple*. dirección: https://support.apple.com/es-es/HT201222.

[7] *Mobile Malware Attacks and Defense*. dirección: http://www.syngress.com/hacking-and-penetration-testing/Mobile-Malware-Attacks-and-Defense/.

[8] *El Español: Hackers descubren cómo conectarse a nuestros móviles por Bluetooth, y aún no hay solución*. dirección: https://www.elespanol.com/omicrono/tecnologia/20200911/hackers-descubren-conectar-moviles-bluetooth-no-parches/519948285_0.html.

[9] *Fuzzing the Phone in your Phone (Black Hat USA 2009)*. dirección: www.blackhat.com/presentations/bh-usa-09/MILLER/BHUSA09-Miller-FuzzingPhone-PAPER.pdf.

[10] *Security flaw shows 3G, 4G LTE networks are just as prone to stingray phone tracking*. dirección: https://www.zdnet.com/article/stingray-security-flaw-cell-networks-phone-tracking-surveillance/.

[11] *Security Concerns with NFC Technology*. dirección: http://nearfieldcommunication.org/nfc-security.html.

[12] *Reference about YXE*. dirección: https://www.f-secure.com/v-descs/worm_symbos_yxe.shtml.

[13] *Internet Storm Center: sms-vishing for your bank info*. dirección: https://isc.sans.edu/diary/sms-vishing+for+your+bank+info/4507.

[14] *PDF: Guía de Seguridad de las TIC (CCN-STIC-450) - Seguridad en dispositivos móviles*.