



GUÍA DE SEGURIDAD DE LAS TIC (CCN-STIC-450)

Seguridad en dispositivos móviles

MARZO 2013

Edita:



© Centro Criptológico Nacional, 2013
NIPO 002-13-026-6

Fecha de Edición: mayo de 2013

Raúl Siles, fundador y analista de seguridad de Taddong S.L., ha participado en la elaboración y modificación del presente documento y sus anexos.

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

Una de las funciones más destacables del Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración, materializada en la existencia de la serie de documentos CCN-STIC.

Disponer de un marco de referencia que establezca las condiciones necesarias de confianza en el uso de los medios electrónicos es, además, uno de los principios que establece la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en su artículo 42.2 sobre el Esquema Nacional de Seguridad (ENS).

Precisamente el Real Decreto 3/2010 de 8 de Enero de desarrollo del Esquema Nacional de Seguridad fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Mayo de 2013



Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1	INTRODUCCIÓN	4
2	OBJETO.....	5
3	ALCANCE.....	5
4	DISPOSITIVOS MÓVILES: CAPACIDADES Y FUNCIONALIDAD	5
5	AMENAZAS Y VULNERABILIDADES DE SEGURIDAD EN DISPOSITIVOS MÓVILES	7
5.1	ACCESO FÍSICO AL DISPOSITIVO MÓVIL.....	8
5.2	SISTEMA OPERATIVO DEL DISPOSITIVO MÓVIL.....	9
5.3	ALMACENAMIENTO DE INFORMACIÓN	10
5.4	LOCALIZACIÓN	10
5.5	COMUNICACIONES	11
5.5.1	BLUETOOTH.....	11
5.5.2	WIFI.....	12
5.5.3	GSM (2G): SMS	13
5.5.4	GSM (2G): COMUNICACIONES DE VOZ.....	17
5.5.5	GSM (2G): COMUNICACIONES DE DATOS.....	19
5.5.6	UMTS (3G): COMUNICACIONES DE VOZ Y DATOS	19
5.5.7	NFC (NEAR FIELD COMMUNICATION)	19
5.6	SOFTWARE Y APLICACIONES CLIENTE	20
5.7	MALWARE EN DISPOSITIVOS MÓVILES.....	22
5.8	MALWARE Y <i>JAILBREAK</i> EN DISPOSITIVOS MÓVILES	25
5.9	VULNERABILIDADES Y AMENAZAS MULTIPLATAFORMA	28
6	RECOMENDACIONES DE SEGURIDAD EN DISPOSITIVOS MÓVILES.....	29
6.1	ACCESO FÍSICO AL DISPOSITIVO MÓVIL.....	30
6.2	SISTEMA OPERATIVO DEL DISPOSITIVO MÓVIL.....	32
6.3	CONFIGURACIÓN Y PERSONALIZACIÓN DEL DISPOSITIVO MÓVIL.....	33
6.4	ALMACENAMIENTO DE INFORMACIÓN	33
6.5	LOCALIZACIÓN	35
6.6	COMUNICACIONES BLUETOOTH.....	35
6.7	COMUNICACIONES WIFI	36
6.8	COMUNICACIONES DE TELEFONÍA MÓVIL.....	37
6.9	SOFTWARE Y APLICACIONES CLIENTE	38
6.10	DETECCIÓN DE MALWARE EN DISPOSITIVOS MÓVILES.....	41
6.11	PROPAGACIÓN DE MALWARE HACIA OTROS DISPOSITIVOS	41
6.12	TRAZABILIDAD	41
6.13	SOFTWARE DE GESTIÓN Y SEGURIDAD	42
7	REFERENCIAS.....	43

1 INTRODUCCIÓN

1. El desarrollo de los dispositivos móviles y de las tecnologías inalámbricas en los últimos años ha revolucionado la forma de trabajar y comunicarse. El uso creciente de estas tecnologías sitúa a los dispositivos móviles como uno de los objetivos principales de las ciberamenazas.
2. La proliferación de dispositivos móviles en los últimos años, junto al aumento de las capacidades, prestaciones y posibilidades de utilización de los mismos, hace necesario evaluar en profundidad la seguridad ofrecida por este tipo de dispositivos, así como de los mecanismos de protección de la información que gestionan, dentro de los entornos de Tecnologías de la Información y las Comunicaciones (TIC).
3. El término seguridad es empleado en la presente guía considerando las cinco dimensiones de la seguridad de la información, confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad, tal y como se define en el Esquema Nacional de Seguridad (ENS) [Ref.- 1].
4. Se considera dispositivo móvil aquel dispositivo de uso personal o profesional de reducido tamaño 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, como por ejemplo teléfonos móviles, *smartphones* (teléfonos móviles avanzados o inteligentes) y agendas electrónicas (PDA), independientemente de si disponen de teclado o pantalla táctil.
5. Un estudio de la Asociación Europea de Publicidad Interactiva, (EIAA) denominado Mediascope Europe, publicado el 23 de febrero de 2010 en su séptima edición [Ref.- 2], confirma que los españoles dedican casi 5,5 horas semanales de media a conectarse a Internet a través de dispositivos móviles; en el caso de Europa, la media es de 6,4 horas.
6. Otros datos derivados del estudio confirman que “Respecto al uso que los usuarios dan a Internet en sus dispositivos móviles, comentaron que el 74 por ciento se conecta a redes sociales, el 82 por ciento realiza algún tipo de búsqueda y el 85 por ciento hace uso de su email al menos una vez al mes.” [Ref.- 3].
7. Pese a que los dispositivos móviles se utilizan para comunicaciones personales, privadas y relevantes, y almacenan información sensible, el nivel de percepción de la amenaza de seguridad real existente no ha tenido trascendencia en los usuarios finales y las organizaciones.
8. El presente documento realiza un análisis detallado de las últimas y principales amenazas y vulnerabilidades de seguridad en dispositivos móviles durante los últimos años (2008-2010), complementando las amenazas, vulnerabilidades y malware descubiertos en las plataformas móviles desde el año 2000 [Ref.- 59], como por ejemplo, Caribe (o Cabir), Skulls, CommWarrior, Doomboot o Cardtrap.
9. El análisis se centra únicamente en las amenazas específicas asociadas a las tecnologías empleadas por los dispositivos móviles o a los propios dispositivos, sin profundizar en detalle en las amenazas genéricas existentes en dichas tecnologías o que afectan igualmente a otros tipos de equipamiento informático.

2 OBJETO

10. El propósito del presente documento es proporcionar la información necesaria para la evaluación y análisis de los riesgos, amenazas, y vulnerabilidades de seguridad a las que están expuestos los dispositivos móviles en la actualidad.
11. Adicionalmente, la guía presenta una lista de recomendaciones de seguridad generales cuyo objetivo es proteger los dispositivos móviles, sus comunicaciones y la información y datos que gestionan y almacenan.
12. Los detalles específicos de aplicación e implementación de las recomendaciones de seguridad presentadas se describen en otras guías de esta misma serie, centradas en los aspectos prácticos para llevar a cabo la configuración segura de los dispositivos en función de su tipo y versión de sistema operativo.
13. La serie CCN-STIC-450, “Seguridad en dispositivos móviles”, se ha estructurado en dos niveles: una guía genérica centrada en el análisis de seguridad de dispositivos móviles (este documento), complementada por guías específicas para los principales sistemas operativos empleados en dispositivos móviles. Por este motivo, tras la lectura de la presente guía se recomienda la lectura y aplicación de las guías de seguridad asociadas a los sistemas operativos (y versiones concretas) de los dispositivos móviles a proteger:
 - CCN-STIC-451 - Seguridad en Windows Mobile v6.1
 - CCN-STIC-452 - Seguridad en Windows Mobile v6.5
 - CCN-STIC-453 - Seguridad en Android v2.1

Nota: esta serie de guías están diseñadas considerando como requisito la necesidad de encontrar un equilibrio entre seguridad y funcionalidad en relación a las capacidades disponibles en los dispositivos móviles a proteger, con el objetivo de poder hacer uso de la mayoría de características disponibles en los mismos de forma segura.

3 ALCANCE

14. Las Autoridades responsables de la aplicación de la Política de Seguridad de las TIC (STIC) determinarán su análisis y aplicación a los dispositivos móviles ya existentes o futuros bajo su responsabilidad.

4 DISPOSITIVOS MÓVILES: CAPACIDADES Y FUNCIONALIDAD

15. Los dispositivos móviles, especialmente aquellos más avanzados disponibles en la actualidad, ofrecen capacidades y funcionalidades similares a las de otros dispositivos de computación más tradicionales, como ordenadores portátiles, de sobremesa o estaciones de trabajo. En algunos casos, incluso superan a éstos al incluir elementos adicionales, como *Bluetooth*, acelerómetros, GPS y/o cámara de fotos y vídeo.
16. Estas capacidades vienen determinadas por el hardware y software empleado por el terminal. A nivel hardware, las principales capacidades a considerar en los dispositivos móviles más avanzados son:
 - Almacenamiento: disco duro o memoria interna, y soporte para tarjetas de memoria externas.

- Comunicaciones (de voz y datos): infrarrojos (IrDa), Bluetooth (802.15), WiFi (Wireless Fidelity, 802.11), GSM (2G), GPRS (2.5G), EDGE, UMTS (3G), HSDPA, etc.
 - Localización: GPS.
 - Acelerómetro, para detectar la dirección, velocidad e intensidad de los movimientos del dispositivo.
 - Multimedia: micrófono, altavoz, conexiones de auriculares, cámara (fotos y/o vídeo).
 - Interfaces de usuario avanzados, mediante pantallas táctiles o teclados completos de tamaño reducido.
17. Cabe destacar que los dispositivos móviles actuales disponen de conexión a redes de datos (privadas o Internet), con capacidades de comunicación de datos permanentes las 24 horas a través de las redes de telefonía 3G.
18. A nivel software, es necesario tener en cuenta tanto el sistema operativo que gobierna el dispositivo, como el software y aplicaciones disponibles para dicho sistema operativo. Los sistemas operativos más comúnmente empleados en la actualidad en dispositivos móviles (incluyendo el fabricante) son:
- Microsoft - Windows Mobile: versiones 6.1 y 6.5
 - Microsoft – Windows Phone 7 (finales de 2010)
 - Nokia - Symbian: versiones 7 - 9.5
 - RIM (Research In Motion) - BlackBerry: versiones 3.x - 5.x
 - Google - Android: versiones 1.6 y 2.1
 - Apple - iPhone e iPod Touch: versiones 2.x y 3.x
 - Palm – WebOS (Linux): versiones 1.0.x-1.4
19. En los próximos años nuevos dispositivos se englobarán bajo la categoría de dispositivos móviles, tales como *tablet PCs* o el iPad de Apple, viéndose afectados por amenazas similares a las descritas y sobre los que aplicarán las recomendaciones de seguridad de la presente guía.
20. Los dispositivos móviles más avanzados existentes en la actualidad disponen de múltiples capacidades en función del software y aplicaciones disponibles, como por ejemplo acceso a los servicios de telefonía (mensajes de texto y multimedia, voz y datos), acceso completo a redes de datos (redes privadas o Internet), incluyendo la gestión del correo electrónico, acceso a redes sociales, navegación web, mensajería instantánea, servicios de localización (mediante el GPS y las redes de datos), servicios de pago electrónico, acceso y edición de documentos, realización de presentaciones, etc.
21. En base a las capacidades hardware y software de los dispositivos móviles, los elementos relevantes a tener en cuenta en toda política de seguridad, que permitan definir las reglas, principios y prácticas de utilización, son:
- Los dispositivos móviles deben integrarse dentro de la política de seguridad de la organización, ya que por defecto no son seguros, y no deben considerarse

únicamente teléfonos, al disponer de capacidades avanzadas similares a las de otros equipos informáticos más avanzados o de mayor tamaño.

- Definición de qué tipo de dispositivos móviles están permitidos en la organización (preferentemente en función de sus capacidades de protección y mecanismos de seguridad), indicando tipo de dispositivo, fabricante y modelo.
- Definición del tipo de información que los dispositivos móviles pueden almacenar, gestionar y transferir, según la clasificación de la información en la organización (pública, privada, secreto, etc.).
- Definición del tipo de redes de datos y tipo de comunicaciones a las que los dispositivos móviles pueden tener acceso: Internet, comunicaciones de voz, SMS, redes públicas o privadas, etc. Debe especificarse si se permiten conexiones simultáneas cuando el dispositivo está conectado a una red corporativa o privada.
- Definición de los dispositivos móviles permitidos en función de su propietario: dispositivo personal, dispositivo perteneciente a la organización, o ambos.
- Definición de la política de uso aceptable para ambos tipos de dispositivos, personales y corporativos.
- Listado específico del software y las aplicaciones permitidas (y/o prohibidas) en los dispositivos móviles. En su defecto, listado del tipo de aplicaciones permitidas: internas, comerciales, gratuitas y/o de código libre.
- Listado de software de seguridad requerido en los dispositivos móviles.

5 AMENAZAS Y VULNERABILIDADES DE SEGURIDAD EN DISPOSITIVOS MÓVILES

22. Existen numerosas amenazas y vulnerabilidades asociadas a los dispositivos móviles que ponen en riesgo la seguridad tanto del propio dispositivo como de la información que gestiona. Algunas de ellas son comunes a otros equipos, como ordenadores portátiles o de sobremesa, estaciones de trabajo, y servidores, mientras que otras son propias de este tipo de dispositivos.
23. Los informes de ciberamenazas y tendencias publicados por el CCN-CERT en los años 2009 y 2010 describen las vulnerabilidades que han facilitado la expansión de código malicioso (*malware*) en dispositivos móviles, así como los ataques que tienen como objetivo principal este tipo de dispositivos [Ref.- 4] [Ref.- 5] [Ref.- 18].
24. La importancia de la seguridad de los dispositivos móviles en la industria se refleja también en conferencias de seguridad como *CanSecWest*, dónde en 2009, añadieron estos dispositivos al concurso *Pwn2Own*, que insta a los participantes a descubrir nuevas vulnerabilidades en los terminales más comunes en el mercado (BlackBerry, Android, iPhone, Symbian y Windows Mobile), a cambio de suculentos premios y fama [Ref.- 16]. Este concurso ha sido celebrado de nuevo en el año 2010 [Ref.- 17].
25. La aparición de nuevas plataformas tecnológicas móviles, nuevas aplicaciones y nuevos servicios, así como su conexión a través de redes de comunicaciones públicas y privadas, abren la puerta a novedosas investigaciones de seguridad centradas en el descubrimiento de vulnerabilidades en estos nuevos entornos.

26. Los riesgos de seguridad asociados a los dispositivos móviles son múltiples [Ref.- 69], desde la pérdida o robo del dispositivo, afectando a su disponibilidad, hasta la obtención de la información almacenada y enviada o recibida por el dispositivo, afectando a su confidencialidad, pasando por la suplantación del propietario del dispositivo, lo que afectaría a su integridad.

5.1 ACCESO FÍSICO AL DISPOSITIVO MÓVIL

27. La amenaza de acceso físico a un dispositivo móvil por parte de un intruso, incluso por un breve periodo de tiempo, sigue siendo uno de los vectores de ataque principales, tanto para el acceso a la información que el terminal almacena, como para la instalación de software de espionaje encubierto o malicioso.
28. Por otro lado, debido a su tamaño, portabilidad y uso frecuente fuera de la oficina, siempre existe la amenaza o riesgo de que el dispositivo móvil se pierda o sea robado de forma permanente, conllevando pérdidas económicas notables asociadas al valor del propio terminal y de la información que éste contiene o que puede acceder remotamente.
29. Existe software comercial de espionaje, orientado inicialmente a la monitorización de parejas, cónyuges, amigos o compañeros de trabajo, pero que puede igualmente ser utilizado por un atacante. Este software permite acceder a la lista de llamadas y mensajes de texto enviados y recibidos, recibir notificaciones cuando éstas tienen lugar o cuando el teléfono se enciende, interceptar las llamadas, recibir notificaciones de la localización de la víctima, etc. Este software permanece oculto en el dispositivo, indetectable, realizando la función para la que ha sido diseñado.
30. El software de *Spy Phone* [Ref.- 19] emplea únicamente las características de la telefonía tradicional y puede ser instalado en móviles Nokia basados en Symbian 9.x y 8.1, convirtiéndolos en dispositivos de escucha y espionaje. El atacante, tras obtener el IMEI (*International Mobile Equipment Identity*, o identificador único del terminal) del teléfono víctima e instalar el software, configura su número de teléfono como número privilegiado. A partir de ese momento, el teléfono víctima funciona de forma normal, excepto al recibir llamadas del número del atacante (o privilegiado). Éstas serán contestadas de forma inapreciable, sin ningún tipo de indicación ni visual ni sonora, por lo que el atacante puede escuchar todo lo que ocurre en el entorno de la víctima cercano al terminal. Adicionalmente, el software puede ser reconfigurado a través de mensajes SMS silenciosos.
31. Otras herramientas con características similares hacen uso de la conexión de datos y del acceso del terminal a Internet para su monitorización, como *Mobile Spy* o *FlexySPY* [Ref.- 19], compatibles con dispositivos de última generación como iPhone, BlackBerry, Android, Windows Mobile o Symbian.
32. La instalación de software espía no siempre requiere acceso físico al dispositivo, sino que puede llevarse a cabo a través de actualizaciones remotas, tal como sucedió a los usuarios de BlackBerry en los Emiratos Árabes Unidos al recibir una mejora de software por parte de la operadora Etisalat [Ref.- 20]. Ésta, en lugar de mejorar el rendimiento del dispositivo como prometía, permitía la monitorización de los mensajes de los usuarios.
33. El acceso al dispositivo y a su información está protegido habitualmente mediante un PIN o código de acceso. Desafortunadamente, la mayoría de dispositivos móviles implementan códigos de acceso de cuatro dígitos, que potencialmente pueden ser fácilmente adivinables o utilizan valores por defecto conocidos, como 0000 ó 1234.

34. En algunos dispositivos, como el iPhone, el disponer de acceso físico permite eliminar el código de acceso (o PIN) mediante el uso de un cable USB y el software adecuado, sin aplicarse ningún mecanismo de autenticación durante el proceso [Ref.- 48]. Esta técnica es empleada habitualmente en el análisis forense de estos dispositivos, o puede deberse a nuevas vulnerabilidades descubiertas en los dispositivos, como el iPhone [Ref.- 78].
35. Otras soluciones de análisis forense permiten el mismo tipo de acceso a la información del terminal sin autenticación, mediante cables JTAG o mediante soluciones como *Paraben's CSI (Cell Seizure Investigator) Stick* para terminales Motorola, Samsung y LG.

5.2 SISTEMA OPERATIVO DEL DISPOSITIVO MÓVIL

36. Los fabricantes del sistema operativo que gobierna los dispositivos móviles, como Windows Mobile, iPhone o Android, publican periódicamente vulnerabilidades de seguridad asociadas a los componentes y librerías básicas del sistema.
37. Si el dispositivo móvil no es actualizado de forma frecuente con las últimas actualizaciones de seguridad, el dispositivo estará expuesto a vulnerabilidades públicamente conocidas, tanto locales como remotas.
38. Este tipo de vulnerabilidades han sido empleadas en el pasado por atacantes y malware para disponer de acceso completo al dispositivo mediante la ejecución de código, la realización de ataques de denegación de servicio, o el robo de información.
39. Por ejemplo, algunas de las vulnerabilidades más conocidas han afectado al navegador web *Pocket IE* o el sistema MMS (*Multimedia Messaging Service*) en Windows Mobile, el navegador web *Safari* y la librería de imágenes TIFF o la librería *WebKit* del iPhone (ver apartado "5.8. Malware y *jailbreak* en dispositivos móviles") [Ref.- 59].
40. La siguiente lista proporciona algunos enlaces a las alertas y actualizaciones de seguridad de los principales fabricantes de los sistemas operativos disponibles en los dispositivos móviles:
 - Microsoft Windows Mobile security updates:
<http://www.microsoft.com/windowsmobile/en-us/help/security/updates.msp>
 - BlackBerry RIM Bulletins and Information:
<http://na.blackberry.com/eng/ataglance/security/news.jsp>
 - Android Security Announcements:
<http://groups.google.com/group/android-security-announce>
 - Apple security updates:
<http://support.apple.com/kb/ht1222>
 - Palm WebOS software update information:
http://kb.palm.com/wps/portal/kb/common/article/22767_en.html
41. Desafortunadamente, los recursos que publican las actualizaciones de seguridad de algunos fabricantes son difíciles de localizar, proporcionan un número reducido de actualizaciones, y/o limitan los detalles de las vulnerabilidades existentes.

42. Adicionalmente a las actualizaciones facilitadas por el fabricante del sistema operativo, es frecuente encontrar actualizaciones publicadas por parte del fabricante del hardware cuando ambos son diferentes, como por ejemplo dispositivos HTC basados en Windows Mobile [Ref.- 60].

5.3 ALMACENAMIENTO DE INFORMACIÓN

43. Los dispositivos móviles más avanzados almacenan cantidades elevadas de información, tanto asociada a la configuración del sistema, como a las múltiples aplicaciones instaladas y a los diferentes servicios accesibles a través de los terminales, así como datos personales o corporativos de su propietario.
44. Entre los datos almacenados se incluyen por ejemplo credenciales de acceso a servicios web e Internet, credenciales de cuentas de correo electrónico, mensajes de correo electrónico y telefonía (SMS/MMS), información de llamadas de telefonía y VoIP, documentos privados y confidenciales, la agenda de contactos, el calendario con información de eventos y actividades, fotografías, vídeos, grabaciones de voz, listas de tareas, etc.
45. Una de las principales amenazas de seguridad en los dispositivos móviles actuales es el acceso a toda esta información por parte de un atacante, ya sea por disponer de acceso físico al dispositivo (de forma temporal o permanente), o por disponer de acceso remoto al terminal a través de una vulnerabilidad en alguno de sus componentes, o mediante una aplicación previamente instalada.
46. *SpyPhone* [Ref.- 46] es una aplicación desarrollada para el iPhone de Apple que permite la obtención de información confidencial y personal almacenada en este tipo de dispositivos, incluso si no ha sido aplicado el *jailbreak* (ver apartado 5.8), afectando directamente a la privacidad del usuario.
47. Los ejemplos de información obtenida por esta aplicación incluyen números de teléfono, lista de contactos, configuración de las cuentas de correo electrónico (salvo las contraseñas), las pulsaciones de teclado, búsquedas a través del navegador web, histórico de *YouTube*, las coordenadas recientes de localización a través del GPS, detalles de las conexiones a redes inalámbricas, capturas de pantalla, etc [Ref.- 47].
48. Esta aplicación demuestra el riesgo asociado a la instalación de software aprobado por la tienda de distribución de aplicaciones oficial del fabricante (analizadas posteriormente), dónde cualquier aplicación, haciendo uso de las librerías estándar, puede pasar los filtros de aprobación para su publicación y extraer información privada del usuario.
49. La información almacenada en el dispositivo puede ser protegida empleando mecanismos de cifrado, pero siempre debe tenerse en cuenta que el sistema operativo debe disponer de las capacidades necesarias para acceder a dicha información en tiempo real una vez se dispone de acceso al terminal. Es decir, pese al uso de cifrado en los soportes de almacenamiento, si un atacante consigue acceso al dispositivo, por ejemplo porque disponga del código de acceso o PIN, podrá acceder a los datos almacenados.

5.4 LOCALIZACIÓN

50. La disponibilidad de GPS en la mayoría de dispositivos móviles permite la creación y utilización de nuevos servicios basados en la localización física del usuario en cualquier

- lugar del mundo, como por ejemplo, la búsqueda de negocios o recursos cercanos al lugar en el que nos encontramos.
51. Este hecho tiene implicaciones directas en la privacidad del usuario en el caso en el que un atacante pudiera obtener información detallada de su ubicación en todo momento.
 52. Las aplicaciones sociales basadas en la localización (*Location-based social applications*, LBSAs) suponen un riesgo para la privacidad de los usuarios, ya que se basan en la obtención de las coordenadas de la ubicación geográfica del usuario, para posteriormente procesarlas y ofrecer sus servicios.
 53. En concreto, los dispositivos móviles actúan como clientes y envían su localización a servidores potencialmente no fiables. Los servidores disponen de la lógica de la aplicación para procesar la información de localización y ofrecer el servicio. Por tanto, los servidores recogen y almacenan cantidades elevadas de datos de localización de todos los usuarios.

5.5 COMUNICACIONES

54. Las amenazas de seguridad en dispositivos móviles emplean nuevos vectores de ataque a través de los mecanismos de comunicación empleados para la transferencia de información propios de estos dispositivos, como GSM (y el servicio SMS), GPRS y 3G o *Bluetooth*, así como vectores más tradicionales, como Wi-Fi, el acceso a Internet (TCP/IP) y la navegación web.
55. Las múltiples posibilidades de conexión de este tipo de dispositivos, tanto a redes privadas como públicas, permite la realización de ataques directos contra los mismos sin necesidad de tener que evitar controles de seguridad corporativos como cortafuegos perimetrales o sistemas de detección de intrusos.
56. Por otro lado las posibilidades de comunicación simultánea de los dispositivos a diferentes redes, como por ejemplo Internet y una red de datos privada, hace que los terminales actúen de pasarela entre diferentes infraestructuras, lo que facilita la realización de ataques y la propagación de malware entre entornos diferentes.
57. Asimismo, y aunque no se analizan en detalle en el presente documento, es necesario tener en cuenta las implicaciones de seguridad de las nuevas tecnologías de comunicaciones que serán incorporadas en este tipo de dispositivos en los próximos años, como WiMAX, LTE (*Long Term Evolution* o 4G) o *Radio Frequency Identification* (RFID).

5.5.1 BLUETOOTH

58. La tecnología *Bluetooth* (802.15) ha sido objeto de múltiples análisis de seguridad y ataques en los últimos años, pero no por ello deja de seguir constituyendo un vector de ataque activo en los dispositivos móviles.
59. Un dispositivo con conectividad *Bluetooth*, en función de su configuración de seguridad, está expuesto entre otros a la captura de datos por parte de un tercero, afectando a la confidencialidad de las comunicaciones, ataques sobre el PIN empleado durante la autenticación y ataques de suplantación de dispositivos emparejados, afectando a la integridad, incluyendo ataques a través de conexiones o redes no fiables como las asociadas al marketing de proximidad, y ataques de denegación de servicio, afectando a su disponibilidad.

60. Concretamente, en el entorno de los dispositivos móviles, han existido numerosos especímenes de malware en el pasado que se propagaban mediante las capacidades de comunicación *Bluetooth* de los terminales, como *Caribe* (2004) o *Comm Warrior*.
61. Las características y funcionalidades añadidas en ocasiones por los fabricantes de los dispositivos móviles con el objetivo de mejorar las prestaciones del sistema operativo empleado pueden dar lugar a nuevas vulnerabilidades.
62. Los dispositivos móviles (como HTC) con Windows Mobile incorporan el servicio HTC BT FTP (HTC *Bluetooth* OBEX FTP), sobre la pila *Bluetooth* estándar de comunicaciones de Microsoft, para la transferencia de ficheros a través de *Bluetooth*.
63. Este servicio permite el acceso y modificación de ficheros en la carpeta específica asociada al servicio (por ejemplo, "My Device\My Documents\Compartimiento de *Bluetooth*"). Sin embargo, en 2009, una nueva vulnerabilidad de desplazamiento por directorios fue descubierta por Alberto Moreno Tablado para Windows Mobile 6 y 6.1 en dispositivos como HTC (CVE-2009-0244) [Ref.- 12], siendo posible obtener y manipular cualquier fichero del dispositivo, independientemente de su ubicación en el sistema de ficheros, e incluso ejecutar código.
64. Pese a que el servicio HTC BT FTP sólo está disponible para dispositivos emparejados, debe tenerse en cuenta que existen ataques para la captura de las claves de enlace *Bluetooth*, y la suplantación de otros dispositivos, que permitirían evitar esta restricción [Ref.- 55].

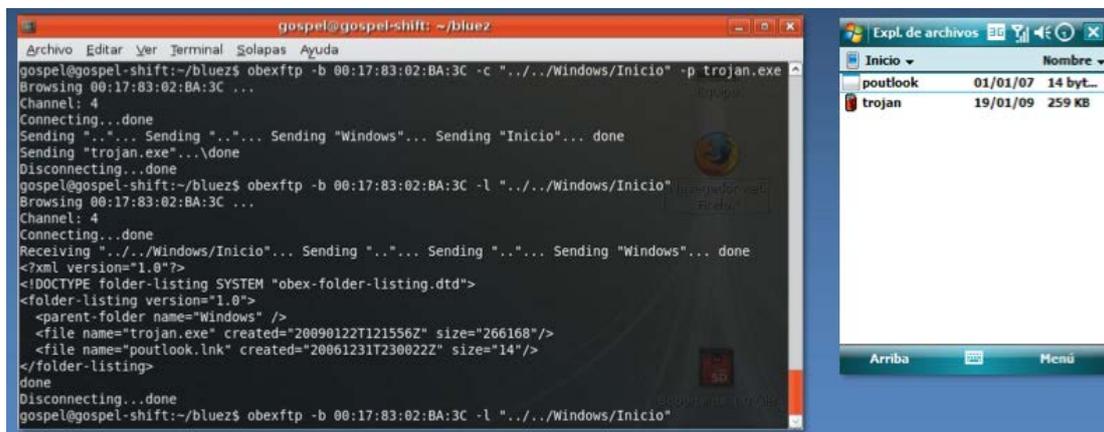


Figura 1. Acceso a cualquier carpeta a través de Bluetooth en dispositivos HTC [Ref.- 12].

5.5.2 WIFI

65. Los dispositivos móviles están expuestos a la totalidad de las vulnerabilidades, amenazas y riesgos asociados a cualquier dispositivo informático con capacidades de comunicación a través de redes inalámbricas WiFi (802.11).
66. Uno de los mayores riesgos de seguridad asociado a las comunicaciones de datos inalámbricas a través de redes WiFi es la conexión a redes públicas y abiertas, con un nivel de seguridad reducido o inexistente (sin mecanismos de autenticación y cifrado), no supervisadas por la organización propietaria del dispositivo, como por ejemplo *hotspots* WiFi disponibles en hoteles, aeropuertos o centros de conferencias.

67. Un dispositivo con conectividad WiFi, en función de los mecanismos de seguridad implantados en la red inalámbrica, está expuesto entre otros a la captura e interceptación de datos por parte de un tercero, afectando a la confidencialidad de las comunicaciones, ataques de inyección de tráfico y ataques de suplantación de la red, afectando a la integridad, y a ataques de denegación de servicio, afectando a su disponibilidad.
68. Adicionalmente, una de las vulnerabilidades propias de los dispositivos móviles es la incorrecta integración por parte de los fabricantes de diferentes tecnologías de comunicación inalámbricas en un mismo dispositivo, desconociendo los requisitos de diseño de cada una de ellas.
69. La mayoría de dispositivos móviles actuales proporcionan conectividad mediante *Bluetooth* y WiFi. La asignación de las direcciones físicas (o direcciones MAC) para cada una de estas tecnologías se lleva a cabo de forma correlativa en muchos casos, es decir, el dispositivo móvil posee la dirección 00:01:02:0A:0B:0C en el interfaz *Bluetooth*, y la dirección (siguiente) 00:01:02:0A:0B:0D en el interfaz WiFi.
70. Este hecho, propio del proceso de fabricación y registro de los dispositivos móviles, introduce una nueva vulnerabilidad inexistente al emplear las tecnologías de forma independiente.
71. La dirección física del dispositivo en *Bluetooth* se emplea como un secreto, y es necesaria para establecer cualquier comunicación con él. Cuando el dispositivo es configurado en modo no visible, situación recomendable desde el punto de vista de seguridad, la dirección se oculta.
72. Sin embargo, la dirección de un dispositivo en WiFi puede obtenerse de forma trivial mediante la captura del tráfico inalámbrico, ya que está disponible en las cabeceras de cualquier trama transmitida, situación que no puede ser evitada ni empleando los estándares WiFi de seguridad más avanzados, como *WPA2 Enterprise*.
73. La práctica común de asignar direcciones correlativas expone por tanto la dirección *Bluetooth* del dispositivo una vez se conoce la dirección WiFi, introduciendo una nueva vulnerabilidad independiente de la tecnología o implementación de la pila de comunicaciones *Bluetooth*.

5.5.3 GSM (2G): SMS

74. La funcionalidad de SMS (*Short Message Service*) de los dispositivos móviles permite el envío de mensajes cortos empleando la infraestructura GSM (*Global System for Mobile communications*, o 2G) empleada para las comunicaciones de voz de la telefonía móvil (mediante conmutación de circuitos).
75. La especificación y la implementación del módulo SMS de los dispositivos móviles no soporta únicamente el intercambio de mensajes de texto, sino que también puede gestionar datos binarios, como tonos de llamada, y ficheros multimedia (audio, vídeo e imágenes), sobre todo en sus variantes avanzadas: EMS (*Enhanced Messaging Service*) y MMS (*Multimedia Message Service*).
76. En el caso de dispositivos basados en Android, iPhone y Windows Mobile, durante el año 2009 se publicaron vulnerabilidades de denegación de servicio, y en algunos casos, de transferencia de ficheros y ejecución de código sin la intervención del usuario.
77. En verano de 2009 se publicó una vulnerabilidad en dispositivos iPhone (CVE-2009-2204) que afectaba a la decodificación de mensajes SMS [Ref.- 23]. Un atacante podía

- enviar un mensaje SMS malicioso y provocar una denegación de servicio en el terminal víctima, o incluso tomar control del mismo mediante la ejecución remota de código. Charlie Miller y Collin Mulliner publicaron su descubrimiento en la conferencia *Blackhat*, demostrando como el envío de múltiples SMS permitía controlar dispositivos remotamente. Este ataque sólo necesita que el teléfono esté encendido, no requiere ninguna intervención por parte del usuario y éste sólo se percataría de la recepción de un SMS anormal, con un único carácter.
78. Esta vulnerabilidad obligó a Apple a distribuir una nueva actualización del sistema operativo del iPhone, versión 3.0.1, que afectaba al módulo de telefonía del terminal. Este tipo de amenazas reflejan la importancia que mantener los dispositivos actualizados frente a las últimas vulnerabilidades descubiertas y con la última versión facilitada por el fabricante.
 79. El proceso *CommCenter* del iPhone se encarga de gestionar los mensajes SMS y las llamadas de teléfono. Debido a que ejecuta como *root* (máximos privilegios sobre el dispositivo) y no está confinado a un entorno de ejecución restringido (*sandbox*), una vulnerabilidad en el mismo (como la mencionada) permite disponer de control completo del dispositivo.
 80. La investigación realizada reveló vulnerabilidades similares en los módulos SMS de Windows Mobile, donde de nuevo era posible tomar control remoto de los dispositivos vulnerables, y de Android (e iPhone, de nuevo), donde mediante el envío de una serie de mensajes SMS era posible desconectar el terminal de la red de telefonía, permitiendo ataques continuados de denegación de servicio sin el usuario ser consciente de ello. En el caso de Android, el proceso que gestiona los mensajes SMS es una aplicación Java.



Figura 2. Ataque de denegación de servicio sobre Android [Ref.- 23].

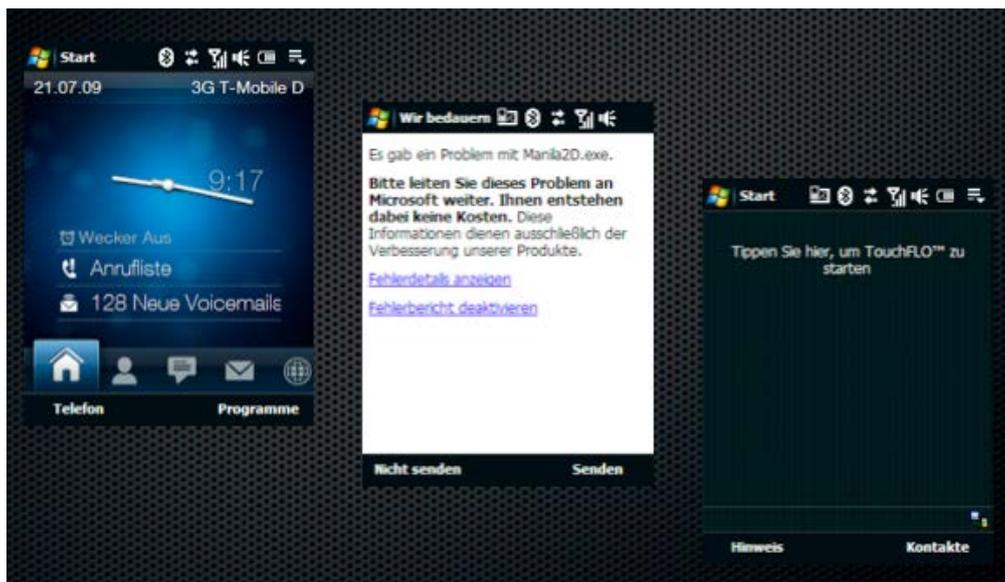


Figura 3. Ataque de denegación de servicio sobre Windows Mobile [Ref.- 23].

81. Durante la misma conferencia, Zane Lackey y Luis Miras [Ref.- 24] presentaron el resultado de su investigación en la implementación SMS de diferentes dispositivos móviles, incluyendo EMS y MMS. El estudio identificó múltiples vulnerabilidades de denegación de servicio en Android, en aplicaciones MMS del iPhone, y en configuraciones WAP realizadas por distribuidores y operadoras sobre Windows Mobile.
82. La investigación destaca adicionalmente la ausencia de medidas de seguridad en los mensajes administrativos intercambiados entre la infraestructura del operador de telefonía móvil y los terminales de los usuarios, como por ejemplo las notificaciones de mensajes en el buzón de voz, permitiendo a un atacante generar mensajes falsos de este tipo.
83. Más crítica aún es la funcionalidad de provisión OTA (*Over the Air*), que permite a las operadoras modificar la configuración de los terminales a través de mensajes SMS. Aunque estas actualizaciones solicitan confirmación del usuario, combinadas con técnicas de ingeniería social, ya que el usuario no puede diferenciar si el mensaje es legítimo o no, permitirían a un atacante reconfigurar el dispositivo víctima.



Figura 4. Recepción de una nueva configuración a través de OTA [Ref.- 24].

84. El análisis realizado sobre mensajes multimedia MMS, refleja la posibilidad de redirigir el dispositivo víctima hacia un servidor del atacante para obtener los contenidos del mensaje, evitando así los mecanismos de filtrado de contenidos de la operadora (antivirus, malware, spam, etc) y permitiendo falsear la identidad (número de teléfono) del emisor. Adicionalmente esta redirección permitiría al atacante identificar el tipo de dispositivo móvil víctima (*fingerprinting*) mediante las cabeceras HTTP.
85. El impacto de este tipo de vulnerabilidades en tecnologías de comunicación tan extendidas como SMS es enorme, ya que la funcionalidad SMS está siempre activa en los terminales. Potencialmente es posible atacar cualquier dispositivo móvil vulnerable a nivel mundial con sólo conocer su número de teléfono, y existen notables carencias en los mecanismos de protección y software de seguridad específico para tráfico SMS.
86. El envío de mensajes SMS también fue empleado en Europa en 2009 para la propagación de enlaces a sitios web maliciosos. Este ataque combinaba el uso de SMS, con las capacidades de acceso a Internet de los terminales y la ingeniería social, instando al usuario a visitar una página web a través de la cual se pretendía infectar a la víctima con el troyano *Ambler*, propio de entornos Windows [Ref.- 25]. El mensaje recibido por la víctima (traducido) era similar al siguiente:
- “Alguien ha publicado toda tu información personal y bancaria en <http://enlace_al_sitio_web_malicioso>. Debes eliminarla cuanto antes.”*
87. Curiosamente, el troyano *Ambler* fue empleado de nuevo en la propagación de malware desde dispositivos móviles BlackBerry, y su modo de almacenamiento USB, hacia los equipos a los que éstos se conectan [Ref.- 26], amenaza comentada posteriormente en el apartado “5.9. Vulnerabilidades y amenazas multiplataforma”. El troyano es ejecutado mediante la funcionalidad *autorun* de Windows, mecanismo también empleado por el troyano para infectar otros dispositivos de almacenamiento USB. Sus acciones maliciosas afectan a Internet Explorer y Outlook y se centran en el robo de credenciales e información sensible.



Figura 5. Propagación del troyano *Ambler* desde BlackBerry hacia equipos Windows [Ref.- 26].

88. Durante el año 2010 se han identificado nuevas vulnerabilidades de seguridad asociadas a la posibilidad de incluir contenidos web (HTML y Javascript) en mensajes SMS.
89. Los dispositivos Palm con WebOS son vulnerables a la recepción de mensajes SMS que contienen *iframes* e inyección de código HTML [Ref.- 76], ya que dichos contenidos no son filtrados adecuadamente por el terminal. Mediante el envío de SMS maliciosos, y con la simple lectura del mensaje por parte del usuario, un atacante puede abrir conexiones con sitios web maliciosos, descargar ficheros, forzar la descarga continua de contenidos,

- solicitar la instalación de una nueva autoridad certificadora raíz (root CA) en el dispositivo, e incluso, apagar la radio GSM o borrar todos los contenidos del terminal (modo Palm Demo) a través de códigos GSM específicos.
90. Las capacidades de previsualización de mensajes SMS de Windows Mobile 6.5 en dispositivos HTC son vulnerables a la inyección de contenidos web y *Cross-Site Scripting* (XSS) [Ref.- 77], permitiendo a un atacante efectuar redirecciones a sitios web, o ejecutar código Javascript.
 91. Para mitigar este tipo de ataques es necesario deshabilitar la funcionalidad vulnerable, deshabilitando la opción "*Show Message*" en la configuración de notificaciones de Windows Mobile, o aplicar la actualización de seguridad que soluciona el problema facilitada por HTC.
 92. *Juniper Research* estima que el mercado de pagos mediante dispositivos móviles (micropagos, pagos por SMS, etc.) alcanzará los seis billones de dólares a nivel mundial en 2013, previsión que potenciará el blanqueo de grandes sumas económicas de forma rápida y encubierta a través de este medio.
 93. El uso de las tecnologías GSM para servicios de banca electrónica desde dispositivos móviles [Ref.- 53], especialmente en países emergentes dónde la disponibilidad de otro tipo de comunicaciones de datos está más limitada, constituye una amenaza con impacto económico directo en el usuario final.

5.5.4 GSM (2G): COMUNICACIONES DE VOZ

94. Las amenazas de seguridad se han extendido recientemente a la infraestructura de comunicaciones de voz GSM (afectando igualmente a las comunicaciones SMS) mediante ataques activos basados en la suplantación de la propia red de telefonía móvil.
95. El coste de reproducir una celda o estación base GSM con capacidad de cursar llamadas reales se ha reducido drásticamente, permitiendo ataques de interceptación o *MitM* (*Man-in-the-Middle*). El ataque se basa en suplantar una celda GSM empleando tecnologías 2G, ya que en éstas la autenticación se realiza en un solo sentido, es decir, desde la tarjeta SIM del terminal hacia la red. GSM (o 2G) no implementa un mecanismo de autenticación mutua que requiera que la red se deba autenticar también frente a la tarjeta SIM.
96. Los terminales se conectan automáticamente, sin ninguna intervención por parte del usuario, a la celda que ofrece mayor intensidad de señal, lo que permite a un atacante posicionarse como la celda preferente para los terminales cercanos.
97. Pese a que la intensidad de la señal es el factor más determinante, según el escenario, pueden existir otros factores a considerar en el proceso de selección de celda, como el operador de la misma (en función del operador principal del terminal) y el tipo de conectividad ofrecido (2G y/o 3G).
98. Este ataque permitiría a un intruso disponer de control completo de las comunicaciones móviles del dispositivo, como por ejemplo redirigir llamadas salientes, manipular la recepción y envío de mensajes SMS, etc.
99. Por otro lado, recientes investigaciones reflejan la posibilidad de capturar y descifrar el tráfico de voz GSM (interceptación pasiva). Las técnicas para romper el algoritmo de cifrado más comúnmente empleado en redes GSM, A5/1, fueron publicadas desde un

- punto de vista práctico en diciembre de 2009 en la conferencia alemana de seguridad CCC [Ref.- 27] por Karsten Nohl.
100. El estudio, basado en el uso de *rainbowtables* (tablas precalculadas) para deducir la clave empleada en una conversación, permite reducir enormemente el tiempo y coste de la infraestructura necesaria para llevar a cabo este ataque.
 101. En tecnologías 3G (o UMTS) existe un mecanismo de autenticación mutua entre el terminal y la red, por lo que no es posible realizar el ataque de suplantación de celda. Además, debido al uso de un algoritmo de cifrado diferente en 3G, denominado A5/3, tampoco aplica el ataque mencionado centrado en descifrar el tráfico.
 102. Sin embargo, dado que todos los terminales disponen de capacidades GSM, un atacante puede forzar que funcionen en 2G y no en 3G, conectándose por tanto a la celda del atacante o empleando el algoritmo de cifrado A5/1, vulnerable.
 103. Por ejemplo, los dispositivos móviles se conectan a través de la red 2G cuando la red 3G no está disponible (por falta de cobertura o por un ataque de denegación de servicio que sature la señal en el rango de frecuencias empleado), viéndose expuestos a los ataques de suplantación de la red y captura de tráfico mencionados.
 104. Adicionalmente, debe tenerse en cuenta que muchos operadores y proveedores de telefonía móvil emplean la misma clave pre-compartida entre el terminal del usuario y la red tanto para las comunicaciones 2G como 3G. Por tanto, si el dispositivo hace uso de ambas redes, y un atacante obtiene la clave mediante los ataques descritos sobre 2G, también podrá descifrar el tráfico de 3G.
 105. Se estima que la tecnología GSM es empleada a nivel mundial a finales del año 2009 por 4 billones de usuarios de teléfonos móviles [Ref.- 52], de ahí la criticidad y el impacto asociado a este tipo de ataques.
 106. La solución más viable para evitar la captura de tráfico en infraestructuras GSM pasa por cambiar el algoritmo de cifrado al empleado en infraestructuras de telefonía 3G, denominado A5/3 o *Kasumi*. Circunstancialmente, en enero de 2010, un estudio teórico centrado en descifrar el algoritmo A5/3 fue publicado por O. Dunkelman, N. Keller y A. Shamir (la S de RSA) [Ref.- 28]. Su aplicación práctica es inviable actualmente ya que requiere la captura de grandes cantidades de tráfico para poder derivar la clave asociada a una conversación, pero denota posibles debilidades en el algoritmo de cifrado de referencia en la actualidad para asegurar la confidencialidad de las comunicaciones móviles.
 107. La utilización de un algoritmo de cifrado robusto, como A5/3, sin embargo, no evita la vulnerabilidad de suplantación de celda durante el proceso de autenticación. Para ello es necesario no hacer uso de la tecnología GSM (2G) y emplear en su lugar UMTS (3G).
 108. Asimismo, debe tenerse en cuenta que en algunos países, los operadores de telefonía móvil no hacen uso de ninguno de los mecanismos de cifrado disponibles en el estándar GSM para las comunicaciones de voz o el envío de SMS [Ref.- 53].
 109. Por otro lado, el buzón de voz asociado a un teléfono móvil puede ser accedido desde cualquier teléfono mediante un PIN o código de acceso, por lo que éste es el único elemento de protección frente al acceso no autorizado a los mensajes de voz confidenciales que se almacenan en dicho buzón.
 110. Incluso para aquellos operadores dónde sólo se permite acceder al buzón de voz desde el propio terminal asociado al mismo, debe tenerse en cuenta que la autenticación se

realiza mediante el número llamante (conocido como “*caller ID*”), y que éste puede ser fácilmente falsificado por un atacante, suplantando al dispositivo auténtico (tanto en llamadas de voz como en mensajes de texto, SMS).

111. Por último, debe tenerse en cuenta que la confidencialidad de las comunicaciones de voz asociadas a un dispositivo móvil no sólo puede verse vulnerada a través de debilidades en las redes de telefonía, sino también mediante la utilización de software malicioso que permita capturar el audio existente alrededor del dispositivo a través de su micrófono.

5.5.5 GSM (2G): COMUNICACIONES DE DATOS

112. La telefonía móvil GSM (2G) permite el establecimiento de comunicaciones de datos casi permanentes las 24 horas del día mediante los estándares GPRS (*General Packet Radio Service*, conocido como 2.5G) y EDGE (*Enhanced Data Rates for GSM Evolution*, conocido como 2.75G), empleados por estaciones base sin capacidades UMTS (3G).
113. Los algoritmos de cifrado empleados por GPRS y EDGE para la transmisión de datos (mediante conmutación de paquetes) son diferentes a los empleados en las comunicaciones de voz (A5), y se denominan GEA1 y GEA2.
114. Pese a que no se conocen vulnerabilidades sobre dichos algoritmos de cifrado, la vulnerabilidad de autenticación existente en GSM previamente analizada, dónde un atacante podría suplantar a una estación base, sigue estando presente.
115. Adicionalmente, las comunicaciones de datos a través de GPRS y EDGE emplean los estándares TCP/IP, por lo que los dispositivos móviles están expuestos a todas las amenazas de seguridad existentes en estos entornos y redes.

5.5.6 UMTS (3G): COMUNICACIONES DE VOZ Y DATOS

116. Las tecnologías de comunicaciones móviles UMTS (*Universal Mobile Telecommunications System*, o 3G) permiten a los dispositivos móviles disponer de conexiones de datos de banda ancha casi permanentes las 24 horas del día.
117. Salvo los ataques teóricos sobre el algoritmo de cifrado empleado en tecnologías 3G (A5/3), mencionados previamente, no se conocen vulnerabilidades asociadas a este tipo de tecnología, aunque debe tenerse en cuenta que cualquier intercambio de información se basa en la confianza que el usuario tiene en el proveedor de telefonía móvil, encargado de cursar todo el tráfico desde y hacia el dispositivo a través de su infraestructura de red.

5.5.7 NFC (NEAR FIELD COMMUNICATION)

118. Nuevas tecnologías inalámbricas, como NFC (*Near Field Communication*) [Ref.- 42] irrumpirán en el año 2010 en el mundo de los dispositivos móviles para convertirlos en medios de pago habituales.
119. La tecnología NFC emplea un rango de radio frecuencia no licenciado, concretamente, 13,56 Mhz. NFC establece comunicaciones de corto alcance (unos pocos centímetros) con un ancho de banda de hasta 424 Kbps.
120. NFC permite almacenar los datos de una tarjeta de crédito en la tarjeta SIM del terminal móvil, habilitando la realización de pagos en tiendas sin disponer de tarjeta de débito o crédito, o dinero en efectivo.

121. Tras introducir el comerciante el importe de la transacción en el terminal punto de venta compatible NFC, el pago se realiza cuando el usuario aproxima su dispositivo móvil a dicho terminal.
122. El primer proyecto piloto en un entorno real en Europa tendrá lugar en Sitges, con la participación de 500 comercios y unos 1.500 habitantes [Ref.- 43].

5.6 SOFTWARE Y APLICACIONES CLIENTE

123. Las plataformas de los dispositivos móviles modernos disponen de sistemas operativos completos, con un abanico de funcionalidad y aplicaciones muy amplio, que permiten extender las capacidades del terminal: Internet, productividad, ocio, *suites* de aplicaciones, juegos, etc.
124. Los fabricantes fomentan tanto la existencia de kits o entornos de desarrollo de software para su plataforma por parte de terceros, como la distribución de las nuevas aplicaciones desarrolladas, creando un negocio con beneficios relevantes para todas las partes.
125. Las técnicas de ataque principales empleadas en Internet en la actualidad contra los usuarios y sus ordenadores, como *phishing*, ingeniería social o ataques a través de la web y web 2.0 (donde gran cantidad de contenidos son generados por los usuarios), se están extendiendo a los dispositivos móviles.
126. Mediante los dispositivos móviles es posible acceder a todos los entornos y servicios que facilitan ataques avanzados y lucrativos, como por ejemplo la banca online (*phishing*), compras electrónicas, acceso al correo electrónico (e-mail), y disponer de aplicaciones móviles específicas para interactuar con las principales redes sociales en Internet, como *Facebook*, *Twitter*, *MySpace*, *Linkedin* o *Tuenti*.
127. Algunos ataques contra este tipo de redes, como por ejemplos gusanos avanzados como *Koobface* [Ref.- 44], afectan tanto a los equipos tradicionales como a los dispositivos móviles.
128. Otras vulnerabilidades afectan directamente a los dispositivos móviles, como las debilidades en la autenticación de mensajes de texto SMS, y la integración de estos mensajes con servicios como *Twitter* o la banca electrónica, lo que fomenta ataques basados en el envío de mensajes SMS manipulados, falseando el emisor de los mismos.
129. Una de las carencias ampliamente conocidas asociada a la navegación web en los dispositivos móviles es la limitación de éstos para realizar una validación adecuada de los certificados SSL/TLS empleados en las conexiones web cifradas (HTTPS). La interacción con el usuario, en el caso de ser necesario, para mostrarle toda la información necesaria para validar la existencia de una conexión segura, y determinar su legitimidad, se ve limitada por la reducida pantalla del terminal o el interfaz empleado por la versión móvil del navegador web [Ref.- 5].
130. Desde el punto de vista corporativo, uno de los riesgos de seguridad principales es la descarga, instalación y ejecución de aplicaciones por parte de los usuarios no certificadas o autorizadas por la organización.
131. Por otro lado, y con el objetivo de disminuir los costes de telefonía móvil, especialmente para llamadas internacionales o de larga distancia, comienza a ser muy común disponer de software y funcionalidad de voz sobre IP (VoIP) en los terminales, con aplicaciones propietarias como *Skype*, *Fring* o soluciones VoIP estándar basadas en los protocolos SIP/RTP.

132. Estas soluciones permiten realizar o recibir llamadas de voz sin emplear la infraestructura de telefonía móvil tradicional, haciendo uso en su lugar de otras redes de datos basadas en TCP/IP, como por ejemplo redes inalámbricas WiFi, cuyo coste de acceso es nulo o muy reducido.
133. En los últimos años los patrones sociales de comunicación han cambiado, siendo muy frecuente el uso de redes sociales en Internet para estar en contacto con conocidos, tanto a nivel personal como de negocios, y en concreto las redes sociales móviles, es decir, el acceso a las plataformas de las redes sociales a través de dispositivos móviles y sus conexiones de datos a Internet. Las redes sociales móviles son empleadas en la actualidad por millones de usuarios sólo en Europa [Ref.- 9].
134. La mayoría de dispositivos móviles modernos incluyen por defecto aplicaciones que permiten el acceso a las redes sociales, como *Facebook*, *Twitter* o *MySpace*, dónde el usuario puede tanto consumir como publicar contenidos.
135. Esta integración permite compartir información entre la aplicación web de la red social y las capacidades de telefonía del terminal, englobando los datos de contacto del teléfono y de la red social, y manteniéndolos sincronizados. Así el usuario puede seleccionar como comunicarse con cada uno de sus contactos (SMS, *chat*, *e-mail*, red social, etc.) y obtener detalles de ellos (estado *online*, qué está haciendo, o dónde, gracias a las capacidades de localización), así como compartir información multimedia en tiempo real.
136. Este tipo de aplicaciones y plataformas, identificados como uno de los principales medios de comunicaciones personales y empresariales en la actualidad, tienen asociados riesgos y amenazas de seguridad, principalmente debido a la revelación pública, o semi-pública, de cantidades elevadas de información personal o profesional, que afecta principalmente a la privacidad del usuario.
137. Los principales riesgos y amenazas de las redes sociales móviles son [Ref.- 9]:
- Robo de identidad, mediante el robo de credenciales o el secuestro de la sesión del usuario, disponiendo de acceso completo a la cuenta de la víctima. Igualmente, existe la amenaza de suplantación de la identidad de una persona a través de perfiles sociales falsos, lo que conlleva un uso malintencionado de datos personales y/o profesionales.
 - Distribución de malware a través de la red social debido a vulnerabilidades de seguridad en la misma, o técnicas de ingeniería social. El objetivo es comprometer el dispositivo móvil para acceder a su información, así como emplearlo para la distribución del propio malware.
 - Revelación de información corporativa sensible, debido a la interconexión entre redes sociales personales y profesionales, pudiendo afectar a la publicación de secretos y, por tanto, a la reputación de la organización.
 - Localización física del usuario, empleando las capacidades de localización de los dispositivos móviles y su integración con la funcionalidad de las redes sociales, siendo posible conocer la ubicación geográfica de un usuario en todo momento, lo que permite ataques contra la seguridad física como secuestros, chantajes, acosos, etc.
138. Los riesgos sobre la privacidad no están sólo asociados al uso de redes sociales, sino que la utilización extensiva de los dispositivos móviles deja trazas de su uso, la identidad del usuario y sus transacciones, tanto en los servicios, como en las plataformas y redes de

- comunicaciones empleadas. En algunos casos basta con tan sólo llevar el dispositivo en el bolsillo, debido a las múltiples tecnologías inalámbricas implementadas.
139. Cada vez es más habitual el uso en dispositivos móviles en nuevas aplicaciones asociadas a servicios críticos, como por ejemplo, pasarelas hacia medios de pago para la compra de bienes o servicios, pago de medios de transporte o estacionamiento, o la gestión de activos financieros.
 140. Hasta el momento, la amenaza principal en dispositivos móviles se centraba en el robo de información personal, pero estas nuevas aplicaciones abren las puertas a nuevas amenazas de fraude, más lucrativas para los atacantes.
 141. Por ejemplo, *Paypal* anunció en el año 2008 la posibilidad de realizar pagos a través de dispositivos BlackBerry [Ref.- 5], mientras que hay países como Brasil, Filipinas (GCASH) o España (SEPOMO) donde los dispositivos móviles son empleados como medio de pago a través del uso de mensajes SMS que permiten llevar a cabo la confirmación de la transacción (micro-pagos), que se cargará en la factura del móvil del usuario.
 142. Actualmente, los dispositivos móviles se están estableciendo como un canal alternativo seguro de autenticación electrónica (fuera de banda) para el acceso a servicios y pagos tanto en Internet como en comercios [Ref.- 10], como por ejemplo la banca electrónica.
 143. La tecnología principal empleada para la autenticación de dos factores a través de dispositivos móviles son los mensajes SMS, mediante los que el usuario recibe un PIN temporal o token para llevar a cabo la transacción, como por ejemplo, una transferencia bancaria.
 144. Al analizar la seguridad de este tipo de mecanismos de autenticación se deben tener en cuenta las vulnerabilidades sobre las comunicaciones de telefonía móvil analizadas previamente, y concretamente sobre los mensajes SMS.

5.7 MALWARE EN DISPOSITIVOS MÓVILES

145. Las capacidades de comunicación, la posibilidad de sincronización con otros equipos, como ordenadores de sobremesa o portátiles, y la integración con soportes de almacenamiento externo son vías para la propagación de software malicioso (*malware*) hacia o desde los dispositivos móviles.
146. La amenaza de *malware* sobre dispositivos móviles venía representada hace unos años principalmente por troyanos para la plataforma Symbian, debido a su popularidad.
147. Las primeras aplicaciones maliciosas dirigidas a las plataformas móviles más recientes, como iPhone y Android, aparecieron durante el año 2009. Pese a que en el caso del iPhone solo podían infectar a los usuarios que habían realizado el *jailbreak* del terminal (proceso analizado posteriormente en el apartado 5.8), en el caso de Android podían afectar potencialmente a todos los usuarios.
148. En 2009 apareció el primer gusano distribuido por SMS (incluyendo mensajes multimedia, MMS), denominado *Sexy View*, *Sexy Space*, EXY o YXE [Ref.- 38], que empleaba enlaces web en el contenido del mensaje y técnicas de ingeniería social para llevar a cabo la instalación de software malicioso (paquete SIS) en los terminales Symbian objetivo.

149. Concretamente, éste afectó a dispositivos basados en Symbian S60 (3ª edición) en China y Oriente Medio. Para la propagación empleaba la lista de contactos de los teléfonos afectados, y, su efectividad en conseguir que los usuarios pulsaran el enlace web malicioso se basaba en la confianza que los usuarios tienen en los mensajes de texto recibidos de sus conocidos, sin ser conscientes de que el mensaje podía no haber sido enviado por ellos.
150. Adicionalmente, esta amenaza está directamente relacionada con la distribución de *software* malicioso “legítimo” para dispositivos móviles. El paquete SIS, remitido por tres compañías Chinas, había sido firmado por Symbian, por lo que los terminales víctima no generaban ninguna alerta de seguridad durante el proceso de instalación.
151. Parece que la firma de este malware se realizó a través del proceso automático *Express Signing* de Symbian, en el que no existe necesariamente ninguna verificación manual del software a firmar.
152. El gusano remitía información del teléfono vía web al atacante, como el modelo de teléfono, el IMEI (*International Mobile Equipment Identity*) y el IMSI (*International Mobile Subscriber Identity*) y, adicionalmente, sus acciones conllevan un impacto económico en las víctimas, que debían pagar por los SMS enviados, uno por cada entrada en la lista de contactos.

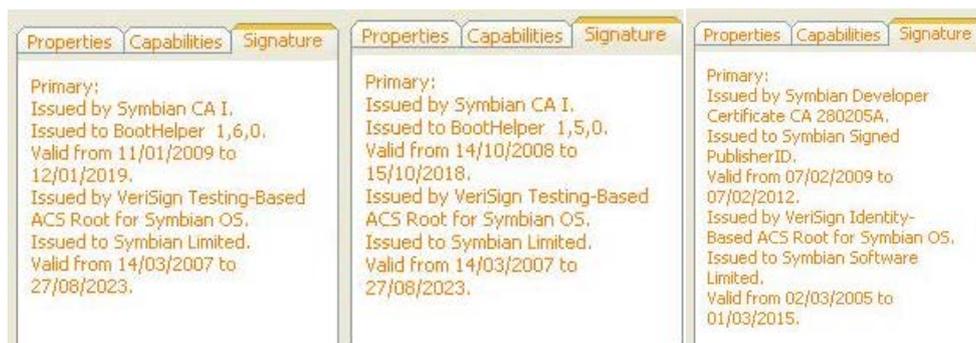


Figura 6. Certificados firmados por Symbian del gusano YXE o EXY.A, B y C [Ref.- 37].

153. Una nueva variante de este malware reapareció en febrero de 2010, con el nombre de *LanPackage*, simulando una mejora en el sistema de idiomas del terminal. El método de infección y propagación empleado fue el mismo que en las variantes previas. De nuevo, el *malware* presentaba un certificado digital válido firmado por Symbian, confirmándose la prevalencia de este tipo de amenaza.

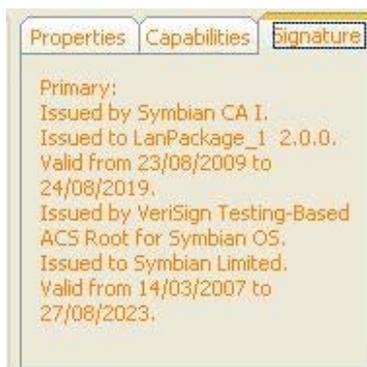


Figura 7. Certificado firmado por Symbian de la nueva variante, SymbOS.Exy.E [Ref.- 37].

154. Pese a que los certificados asociados a este *malware* fueron revocados por Symbian tras el primer incidente, muchos usuarios en China se han visto afectados de nuevo por este segundo caso, debido a que las capacidades de comprobación de certificados revocados están deshabilitadas en sus dispositivos (ver apartado 6.9 de recomendaciones).
155. Las amenazas relacionadas con el envío de SMS masivos se ratifican con otros dos tipos de incidentes de seguridad. Por un lado, la existencia de troyanos multiplataforma para el envío de SMS y distribuidos a través de ICQ en junio de 2009 [Ref.- 39]. Al estar desarrollados como un *MIDlet* de Java, pueden ser ejecutados por numerosos dispositivos móviles, ya que la mayoría de ellos disponen de soporte para Java.
156. Por otro lado, el uso de SMS para la distribución de ataques de *Vishing* (VoIP phishing), dónde se insta a la víctima a llamar a un número de teléfono, que en lugar de pertenecer al supuesto emisor, pertenece y es usado por el atacante para la obtención de información sensible [Ref.- 40], existiendo incluso herramientas para llevar a cabo este tipo de ataques.
157. Adicionalmente, los dispositivos móviles están expuestos tanto a la recepción como al envío de SPAM, tanto asociado al correo electrónico (al igual que otros equipos informáticos), como a mensajes SMS o al buzón de voz. En el caso del envío no autorizado de SPAM mediante mensajes SMS desde el dispositivo móvil, el ataque tendrá repercusiones económicas en la víctima, que se reflejarán en la factura de telefonía (cargándose en la misma el coste de envío de todos los mensajes generados).
158. La aparición de software malicioso para dispositivos móviles cada vez más sofisticado y dañino, incluso con funcionalidad de gusano, hace que las *botnets* constituidas por dispositivos móviles sean cada vez una amenaza más real, dadas sus capacidades permanentes de conexión a redes de datos como Internet a través de tecnologías 3G y 3.5G (UMTS/WCDMA/HSDPA). El malware para el control remoto del dispositivo puede ser distribuido empleando múltiples métodos: SMS, troyanos, e-mails, sitios web maliciosos o comprometidos, mensajería instantánea, etc.
159. Una de las amenazas de mayor expansión en los ordenadores de propósito general, los *rootkits*, tendrán incluso mayor impacto en los dispositivos móviles. Éstos últimos son tan complejos tecnológicamente como los primeros, pero carecen de las capacidades de protección y detección más avanzadas de éstos, lo que dificulta la detección de este tipo de malware, diseñado para permanecer oculto.
160. El impacto de un *rootkit* en un dispositivo móvil es muy elevado, con amplias consecuencias sociales dada su vinculación casi permanente con su propietario, permitiendo a un atacante disponer del control del dispositivo, robar los datos personales

que éste almacena, interceptar y redirigir llamadas, emplear el micrófono para realizar escuchas, capturar las pulsaciones de teclado, grabar imágenes y video a través de su cámara, localizar la ubicación de la víctima a través del GPS o inutilizar el terminal mediante una denegación de servicio al consumir su batería en poco tiempo.

161. En febrero de 2010 un estudio de Rutgers University [Ref.- 41] alertó de las amenazas asociadas a la distribución de *rootkits* en dispositivos móviles, con el objetivo de concienciar sobre los riesgos y mejorar el estado del arte de los mecanismos de defensa en estos dispositivos.

5.8 MALWARE Y JAILBREAK EN DISPOSITIVOS MÓVILES

162. Los dispositivos móviles con mayores capacidades, y sus sistemas operativos asociados, ofrecen funcionalidades adicionales a los usuarios más avanzados. Debido a que algunos de estos sistemas ejecutan un sistema Windows, Unix o *BSD completo, es posible disponer de acceso total al dispositivo, su sistema de ficheros, y los procesos que son ejecutados por el mismo.
163. Por defecto el fabricante, por ejemplo Apple en el caso del iPhone, establece una serie de restricciones en el diseño del dispositivo y el sistema operativo para que este acceso completo no esté disponible para el usuario.
164. El iPhone de Apple presenta un sistema operativo restringido que sólo permite la instalación de *software* previamente aprobado. En el caso del iPhone, el proceso que permite al usuario disponer de control completo de su dispositivo se conoce como *jailbreak*. En el caso de Android, dicho proceso se conoce como *root* o *rooted*.
165. El *jailbreak* es un proceso que permite al usuario acceder a partes del sistema operativo restringidas por el fabricante, y por tanto disponer de toda la funcionalidad existente, vulnerando los mecanismos de protección del terminal, y permitiendo la instalación de cualquier software o aplicación compatible con el dispositivo. Por estos motivos es identificado por los usuarios como algo positivo que proporciona mayor flexibilidad en la gestión del terminal.
166. El proceso de *jailbreak* invalida los mecanismos de verificación de código, encargados de comprobar que cualquier aplicación, antes de ser ejecutada, ha sido firmada por Apple y es por tanto considerada legítima o fiable.
167. Este escenario facilita la instalación de software y aplicaciones desde fuentes no fiables y sin verificar, y por tanto, de aplicaciones maliciosas o *malware*.
168. Se estima que el número de dispositivos iPhone sobre los que se ha aplicado el *jailbreak* en el año 2010 es de un 6-8% del total de iPhones disponibles.
169. El proceso de publicación de aplicaciones en los repositorios oficiales, como la *iPhone App Store* [Ref.- 13] de Apple, es muy riguroso e impone ciertos requisitos a los desarrolladores, como que la aplicación esté firmada digitalmente por Apple, que no establezca comunicaciones externas hacia el desarrollador, o que no utilice APIs no soportadas. Estas restricciones hacen que la distribución de software malicioso a través de este medio esté limitada.
170. El repositorio oficial de aplicaciones para Android, *Android Market* [Ref.- 14], también impone restricciones, como la necesidad de que las aplicaciones estén firmadas digitalmente para así poder identificar al autor, aunque no son tan estrictas ni sus actividades tan estrechamente monitorizadas como en el caso de la *App Store*. En este

- caso no es necesario disponer de un terminal modificado, *rooted* (o *jailbreak*), para su instalación. Ciertas aplicaciones de pago para Android pueden ser definidas con protección frente a copia, de forma que no puedan ser copiadas entre dispositivos y haya que pagar por cada nueva instalación.
171. Otros fabricantes también disponen de sus repositorios o tiendas virtuales de aplicaciones, como el *Windows Marketplace* de Microsoft para Windows Mobile [Ref.- 45], o el *BlackBerry App World* de RIM [Ref.- 70].
 172. En el caso de Android, comparado con el iPhone, es más sencillo instalar aplicaciones provenientes de fuentes diferentes a la oficial. Pese a ello, es necesario que el usuario especifique que quiere evitar esa restricción mediante una opción disponible que debe ser habilitada a tal efecto, y que tiene asociado un mensaje o aviso de seguridad alertando sobre el riesgo de permitir la instalación de software desde sitios externos.
 173. Los dispositivos dónde se ha aplicado el *jailbreak* permiten disponer de capacidades de acceso remoto, por ejemplo, mediante SSH. Pese a que para acceder al terminal es necesario autenticarse, el dispositivo dispone de contraseñas por defecto públicamente conocidas, que si no son modificadas por el usuario, permitirían a un atacante obtener control completo del terminal.
 174. El gusano *Ikee* [Ref.- 29] y el gusano *Duh* [Ref.- 30], bastante más dañino, explotaban este acceso en modelos de iPhone sobre los que se había realizado el *jailbreak*, empleando la contraseña por defecto (“*alpine*”) del usuario más privilegiado (“*root*”).
 175. Este acceso permitía tanto la propagación del *malware* como la realización de otras acciones fraudulentas. Debe tenerse en cuenta que la propagación de este tipo de *malware*, considerando las capacidades de comunicación de datos 3G y WiFi de los dispositivos móviles, es muy efectiva.
 176. *Ikee* afectó a usuarios en Australia y simplemente modificaba el fondo de escritorio del terminal con una foto del cantante Rick Asley, deshabilitando posteriormente el servicio SSH para evitar futuras infecciones, y continuar su propagación hacia otras posibles víctimas. Su código fuente fue liberado posteriormente, lo que facilitó la aparición de nuevas variantes más dañinas [Ref.- 31].
 177. Sin embargo, *Duh* (también conocido como *iBotnet* [Ref.- 32]) presentaba comportamientos propios de las *botnets*. Durante la fase de propagación escaneaba la red local y rangos de ISPs en múltiples países Europeos (Holanda, Portugal, etc) y Australia.
 178. Una vez infectaba un terminal, cambiaba la clave de “*alpine*” a “*ohshit*”, para posteriormente establecer una conexión hacia un servidor web de control remoto ubicado en Lituania, del que descargaba nuevos ficheros y ejecutables, y al que también enviaba información extraída del dispositivo.
 179. Finalmente, implementaba un ataque de *phishing* mediante la modificación del fichero de resolución de nombres, dirigido a usuarios holandeses para la captura de credenciales del banco ING [Ref.- 33].
 180. El precursor de estos gusanos, a comienzos de noviembre de 2009, fue un *hacker* Holandés, que tras escanear la red de datos de la operadora T-Mobile en Holanda en busca de los iPhones disponibles y con el *jailbreak* aplicado, tomó control de los dispositivos víctima empleando el mismo vector de ataque que los gusanos mencionados.
 181. Posteriormente, el atacante notificaba al usuario del problema de seguridad, y ofrecía al propietario del terminal la solución para eliminar la vulnerabilidad por un precio de cinco

euros [Ref.- 34]. A los pocos días, se publicó una herramienta que permitía la ejecución de ataques similares y la extracción de toda la información del iPhone víctima de forma encubierta [Ref.- 35].

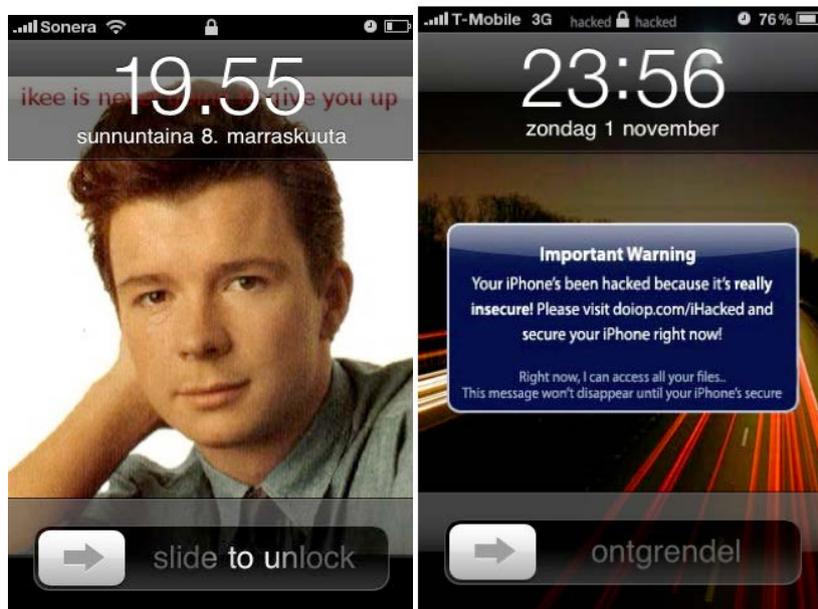


Figura 8. Imágenes resultado de gusanos como Ikee [Ref.- 31] y de su precursor en Holanda [Ref.- 34].

182. A finales de 2009 se descubrió que una nueva aplicación para el acceso a la banca online desde móvil publicada por 09Droid, diseñada para dispositivos Android y disponible en el *Android Marketplace*, recopilaba información bancaria de los usuarios y sus cuentas [Ref.- 36]. Varias entidades financieras alertaron a sus clientes de la existencia de dicha aplicación fraudulenta y de los riesgos de su utilización.
183. El impacto de la distribución de aplicaciones maliciosas en dispositivos sobre los que se ha realizado el *jailbreak*, o que aceptan software de terceros, fue analizado por un estudio realizado en marzo de 2010 [Ref.- 6], dónde se publicó una nueva aplicación móvil para iPhone y Android, y se analizó su descarga y distribución, alcanzando la cifra de casi 2.000 descargas en 24 horas.
184. El objetivo principal del estudio era demostrar como de fácil y probable es la creación de una *botnet*, red de dispositivos víctima controlados por un atacante, compuesta por dispositivos móviles de última generación.
185. Asimismo, el estudio demuestra el riesgo asociado a la instalación de cualquier software proveniente de una fuente no fiable, ya que una vez se ejecuta en el dispositivo, un atacante podría controlar el terminal y acceder a toda la información que éste gestiona, como la lista de contactos, documentos y ficheros almacenados, cuentas registradas para servicios web o redes sociales (*Twitter*, *Facebook*, etc.), mensajes SMS y llamadas, correos electrónicos, contraseñas, etc.
186. Otra implicación de seguridad asociada al proceso de *jailbreak* a tener en cuenta es que la publicación de nuevas actualizaciones por parte del fabricante, como una nueva versión del sistema operativo, no está disponible para los usuarios “no oficiales” (los que han realizado el *jailbreak*) hasta unos días o semanas después, tiempo durante el que están expuestos a las vulnerabilidades solucionadas por la actualización. Este retraso se debe a

que las herramientas empleadas para realizar el *jailbreak* deben ser actualizadas para trabajar con la nueva versión del sistema operativo.

187. Con el objetivo de concienciar a los usuarios, en julio de 2009 Apple publicó un artículo con el impacto que el proceso de *jailbreak* tenía en los mecanismos de seguridad del iPhone [Ref.- 73].

5.9 VULNERABILIDADES Y AMENAZAS MULTIPLATAFORMA

188. Uno de los riesgos inherentes a los dispositivos móviles es la propagación de *malware* desde los mismos hacia los ordenadores empleados para la compartición y transferencia de datos o sincronización. Es fundamental evaluar por tanto la posible propagación de software malicioso desde dispositivos móviles a otros entornos multiplataforma, como son equipos portátiles o de sobremesa.
189. Los dispositivos móviles actuales disponen de capacidades de almacenamiento interno o externo, mediante tarjetas tipo SD (*Secure Digital*), *microSD*, CF (*Compact Flash*), etc.
190. Cuando el dispositivo móvil es conectado a otro equipo para realizar la sincronización de los datos compartidos entre ambos o para transferir cualquier tipo de información, existe el riesgo de que *malware* residente en el dispositivo móvil sea transferido, y por tanto infecte el equipo al que se ha conectado.
191. Las conexiones se realizan habitualmente mediante cable USB, y el dispositivo móvil se ofrece como unidad de disco USB al equipo al que se conecta. Si dicho equipo no está configurado con las restricciones adecuadas de seguridad [Ref.- 11] y, por ejemplo en entornos Windows, ejecutará automáticamente los contenidos de la unidad de disco (es decir, del dispositivo móvil) en el momento de su conexión, se podrá infectar.
192. Esta ejecución automática constituye un vector de ataque ya conocido para la propagación de software malicioso. Uno de los primeros especímenes de *malware* que empleaba esta técnica de propagación e infección entre dispositivos móviles Symbian y ordenadores Windows fue *Cardtrap*, descubierto a finales del año 2005 [Ref.- 59].
193. La infección inicial del dispositivo móvil puede ocurrir a través del uso diario del terminal por parte del usuario, o directamente desde fábrica en dispositivos nuevos. Un ejemplo concreto de este último tipo de amenaza en entornos Windows fue descubierto en marzo de 2010 en dispositivos basados en Android y distribuidos por Vodafone en España.
194. Vodafone distribuyó móviles HTC Magic en Europa con Android 1.5 que contenían en la tarjeta de memoria externa múltiples muestras de *malware* [Ref.- 7], concretamente, *software* cliente de la *botnet* Mariposa (una de las mayores *botnets* descubiertas hasta el año 2010 [Ref.- 8] e investigada por la Guardia Civil), *Confiker* (uno de los gusanos de mayor distribución en entornos Windows en los últimos años) y *Lineage* (una herramienta de robo de contraseñas). La distribución de dicho espécimen de *malware* afectaba a todo aquel equipo Windows al que se conectara el dispositivo móvil mediante USB, y que tuviera activa la auto-ejecución (*autorun*) de unidades de disco. El *malware* no afectaba en este caso al propio dispositivo móvil, pero no existen limitaciones que hubieran evitado que así fuese.
195. El *malware* Mariposa, contenido en el fichero “AUTORUN.EXE”, se hospedaba en una carpeta denominada “NADFOLDER”, con fecha de creación el 1 de marzo de 2010.

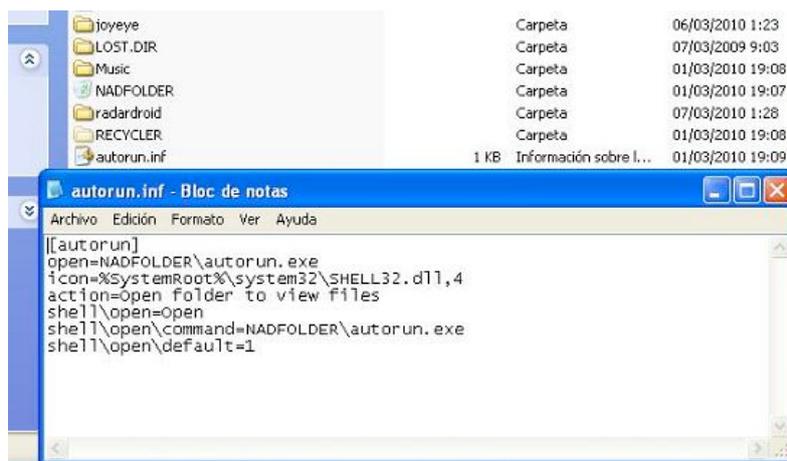


Figura 9. Contenido del fichero autorun.inf de los terminales HTC infectados de Vodafone [Ref.- 7].

196. Tras el incidente inicial, a los pocos días se confirmó otro caso similar en el mismo tipo de dispositivo [Ref.- 21], por lo que Vodafone realizó una investigación del incidente, confirmando la infección de un lote de 3.000 tarjetas de memoria microSD distribuidas con múltiples terminales de la operadora [Ref.- 22].
197. Este incidente enfatiza la necesidad de disponer de un proceso seguro en la fabricación, procesos de calidad y distribución de dispositivos móviles y sus diferentes componentes (como las tarjetas de memoria), desde su concepción en la fábrica hasta su entrega al usuario final.
198. La posibilidad de comprometer ordenadores tradicionales, como equipos portátiles o de sobremesa, a través de dispositivos móviles abre nuevas vías para penetrar el perímetro de seguridad de las organizaciones, que es vulnerado cuando el usuario conecta su terminal al ordenador ubicado en redes internas.

6 RECOMENDACIONES DE SEGURIDAD EN DISPOSITIVOS MÓVILES

199. Con el objetivo de mitigar y/o eliminar las numerosas amenazas y vulnerabilidades asociadas a los dispositivos móviles descritas en el presente informe, existen diferentes recomendaciones de seguridad que pueden ser implementadas en función del tipo de dispositivo y de las tecnologías empleadas.
200. Las recomendaciones descritas pretenden proteger tanto el dispositivo móvil, incluyendo sus capacidades de comunicación y almacenamiento, como la información que gestiona.
201. El interés principal de los atacantes hacia los dispositivos móviles se centra en el robo de información personal y confidencial, la obtención de credenciales y las transacciones financieras y fraude *online*, por lo que cada vez serán más comunes las *suites* de seguridad para dispositivos móviles, con capacidades de antivirus, anti-spam (e-mail y SMS), cortafuegos y cifrado de datos.
202. Asimismo es necesario tener en cuenta las diferencias existentes entre los dispositivos móviles y los ordenadores tradicionales (portátiles o de sobremesa), ya que aunque se enfrentan a amenazas similares, no permiten la aplicación de mecanismos de protección y contramedidas equivalentes.

203. Las principales diferencias entre ambos tipos de dispositivos de cara a la implementación de medidas de seguridad y protección son [Ref.- 51]:

- Recursos limitados, tanto en la capacidad de cómputo como en la capacidad de alimentación eléctrica (batería), lo que afecta directamente a la aplicación de soluciones de detección de malware tradicionales, como antivirus.
- Naturaleza de los ataques, ya que para los atacantes es más interesante hoy en día focalizarse en los ordenadores tradicionales frente a los dispositivos móviles para la obtención masiva de recursos y creación de *botnets* que puedan ser usados con distintos propósitos delictivos. Esto es debido a los recursos de los que disponen, el ancho de banda, latencia de la conexión, y su presencia constante en Internet. Por otro lado, los dispositivos móviles son más interesantes para la realización de ataques dirigidos contra una persona u organización, intrusiones de mayor impacto generalmente y más difíciles de detectar.
- Ausencia de capacidades avanzadas de seguridad en la arquitectura del dispositivo, ya que la mayoría de dispositivos móviles no ofrecen los mecanismos de seguridad existentes en la actualidad en las plataformas de computación tradicionales, como ASLR (Address Space Layout Randomization), NX (Non-Executable memory pages) o TPM (Trusted Platform Module). Algunas plataformas móviles, como por ejemplo iPhone o Android, disponen de algunas de estas capacidades, como NX (en la pila de memoria) o ASLR, respectivamente.
- Limitaciones y particularidades en la utilización del dispositivo y las capacidades de entrada de datos. La utilización de aplicaciones web, común en entornos tradicionales, deriva habitualmente en la existencia de aplicaciones específicas para el acceso al mismo servicio en entornos móviles, con capacidades más reducidas. Por ejemplo, existen numerosas aplicaciones para entornos como Android o iPhone para el acceso a servicios web como Amazon, Facebook, Gmail, Wikipedia, etc.
- Diferencias en el diseño y en los modelos de seguridad disponibles en las diferentes plataformas móviles, por lo que es difícil el desarrollo de mecanismos de protección homogéneos independientes de la plataforma.

204. Se recomienda a las organizaciones planificar el modelo de gestión y seguridad a aplicar sobre los dispositivos móviles durante la fase de diseño, antes de implementar y desplegar la infraestructura de dispositivos móviles en la organización, ya que posteriormente es mucho más complejo y costoso aplicar nuevas medidas de seguridad en cada uno de los terminales existentes.

6.1 ACCESO FÍSICO AL DISPOSITIVO MÓVIL

205. Como recomendación general, no se debe dejar el dispositivo móvil desatendido en ningún momento, ya que una atacante sólo necesita unos segundos para instalar un programa malicioso, o comprometer la seguridad del terminal o tarjeta SIM (*Subscriber Identity Module*). El objetivo es no facilitar el acceso físico al mismo de forma temporal o permanente (pérdida o robo) a un tercero.

206. El dispositivo debe implementar mecanismos de autenticación para el control de acceso por parte de cualquier usuario.

207. El acceso al teléfono debe estar protegido por un código de acceso o PIN, y para la selección del mismo se debe emplear el conjunto de caracteres más amplio posible (números, letras mayúsculas y minúsculas, símbolos de puntuación, etc.) y de una longitud razonable, al menos ocho caracteres. Desafortunadamente, en muchos terminales móviles el PIN está limitado a cuatro dígitos (caracteres numéricos únicamente).
208. Adicionalmente, es posible establecer un código de acceso o PIN asociado al SIM o tarjeta chip de telefonía móvil. En el caso del SIM, tras varios intentos de acceso fallidos (siendo tres intentos el valor estándar) el SIM se bloqueará y no podrá ser utilizado hasta ser desbloqueado mediante el código PUK (*Personal Unblocking Key*).
209. El PIN de acceso al teléfono, a la tarjeta SIM y al buzón de voz, deben ser tratados como un dato secreto y confidencial, y no ser compartidos con nadie, ni reutilizados.
210. Los dispositivos móviles más modernos pueden incluir opciones de autenticación alternativos, como mecanismos biométricos (reconocimiento de la huella dactilar) o autenticación por proximidad, como el Anshin-key de Panasonic. Adicionalmente, es posible combinar múltiples factores de autenticación simultáneamente, incrementando así el nivel de protección de acceso al dispositivo.
211. El dispositivo móvil debe ser configurado para que automáticamente se bloquee el acceso al mismo tras un tiempo de inactividad, por ejemplo entre 1 y 5 minutos, de forma que se solicite al usuario el código de acceso para poder utilizar de nuevo el terminal.
212. El dispositivo no debería mostrar ningún tipo de información mientras está bloqueado, forzando al usuario a introducir el código de acceso para acceder a cualquier dato. Por ejemplo, el iPhone dispone de una opción (desaconsejada desde el punto de vista de seguridad) que permite previsualizar los SMS incluso estando bloqueado el terminal. Windows Mobile también dispone de capacidades de previsualización de mensajes similares, y en otras plataformas como Symbian, existen aplicaciones para añadir esta funcionalidad, como *SMS Preview*.
213. Algunos dispositivos, como el iPhone, permiten ser configurados para eliminar automáticamente todos los datos personales y de configuración almacenados tras diez intentos fallidos de acceso. Desde el punto de vista de seguridad se recomienda habilitar este mecanismo para limitar la posibilidad de acceso a la información almacenada por parte de un intruso. De esta forma, en el caso en el que el dispositivo sea robado por parte de un intruso, si éste desconoce el código de acceso al mismo e intenta adivinarlo, no podrá disponer de acceso a los datos, que serán borrados.
214. Otros dispositivos, como BlackBerry también disponen de mecanismos de protección de la contraseña, eliminando todos los datos del dispositivo tras varios intentos de acceso fallidos. En el caso de BlackBerry, si el terminal está configurado con BES (*BlackBerry Enterprise Server*) es posible resetear la contraseña o eliminar los contenidos de forma remota.
215. En entornos Windows Mobile es posible disponer de este tipo de acceso remoto para eliminar los datos de un dispositivo o bloquearlo a través de un servidor Microsoft Exchange. Para hacer uso de las capacidades remotas es necesario disponer de conectividad con el dispositivo, normalmente a través de la red de telefonía móvil o celular.
216. Microsoft Exchange puede ser empleado también para el borrado de los datos de forma remota en otros dispositivos, como el iPhone, alternativamente a otros servicios propios de este dispositivo, como *iCloud* [Ref.- 64] de Apple. El servicio *iCloud* también permite

- localizar la ubicación física de un iPhone, fijar o cambiar el código de acceso de forma remota en el terminal, o mostrar un mensaje y reproducir un sonido en el dispositivo.
217. De cara a los usuarios de los dispositivos móviles, se recomienda notificar a la mayor brevedad posible la pérdida, extravío o robo del dispositivo a la organización propietaria (en el caso de dispositivos profesionales) y modificar las contraseñas de todos los servicios empleados desde el dispositivo móvil: correo electrónico, redes sociales, banca online, etc.
 218. La temprana notificación durante el proceso de gestión de un incidente de seguridad tras la pérdida del dispositivo es especialmente útil para poder aplicar las soluciones de seguridad de gestión remota mencionadas, como el borrado de datos o el cambio del código de acceso.
 219. Adicionalmente, la notificación temprana permitiría cancelar los servicios de telefonía del terminal para evitar incurrir en gastos adicionales asociados al uso no autorizado del dispositivo móvil. Algunos operadores móviles pueden incluso bloquear el uso del terminal añadiendo su identificador o IMEI (*International Mobile Equipment Identity*) a una base de datos global de dispositivos perdidos o sustraídos y a los que no se permite hacer uso de las infraestructuras de telefonía móvil.

6.2 SISTEMA OPERATIVO DEL DISPOSITIVO MÓVIL

220. Dada la complejidad y las numerosas funcionalidades implementadas en los dispositivos móviles actuales, se recomienda como norma general deshabilitar toda funcionalidad no requerida o que no esté siendo utilizada, con el objetivo de reducir la superficie de exposición y ataque del dispositivo.
221. Por ejemplo, la mayoría de dispositivos móviles avanzados disponen de un “modo vuelo” que permite al usuario de forma sencilla deshabilitar todas las capacidades de comunicación del terminal (telefonía, GPS, *Bluetooth*, WiFi, etc) cuando éstas no están siendo utilizadas (o no se permite su uso, como durante un vuelo).
222. Es crítico actualizar el *firmware* del dispositivo a la última versión de sistema operativo disponible y soportada por el fabricante, con el objetivo de solucionar todas las vulnerabilidades de seguridad públicamente conocidas.
223. En algunos entornos, el proceso de actualización de los dispositivos móviles debe ir precedido de un análisis detallado previo que permita confirmar si la funcionalidad principal del terminal se ve o no afectada por el nuevo *firmware*. Se recomienda definir y poner en práctica dicho procedimiento para agilizar el proceso de actualización y minimizar el plazo de tiempo en el que todos los dispositivos móviles de la organización disponen de la nueva versión.
224. Para llevar a cabo una correcta configuración de seguridad, puede ser necesaria la utilización de herramientas externas facilitadas por el fabricante, como por ejemplo *iPhone Configuration Utility* (ICU) [Ref.- 50], o la manipulación del registro en dispositivos basados en Windows Mobile.
225. El *Trusted Computing Group* (TCG) ha definido un módulo de seguridad hardware resistente a manipulaciones para dispositivos móviles denominado MTM, *Mobile Trusted Module* [Ref.- 72], similar al TPM, *Trusted Platform Module*, disponible en equipos de sobremesa y portátiles. El objetivo de este módulo es el almacenamiento fiable y seguro

de información de seguridad, y será implantado en el futuro en nuevos dispositivos móviles.

6.3 CONFIGURACIÓN Y PERSONALIZACIÓN DEL DISPOSITIVO MÓVIL

226. La configuración existente por defecto y seleccionada por los fabricantes se centra en promover las capacidades, funcionalidad y facilidad de uso del dispositivo móvil, y no así la seguridad del mismo. Por ello, es necesario modificar la configuración por defecto para aumentar el nivel de protección del terminal.
227. Los riesgos asociados a la configuración y personalización del dispositivo móvil deben evaluarse desde el punto de vista de quién tiene el control del mismo: el propietario o usuario final, o el departamento de seguridad y tecnologías de la información de la organización.
228. En el primer caso, el otorgar capacidades completas de configuración y personalización al usuario final, hace prácticamente imposible poder proteger a los dispositivos frente a la mayoría de amenazas de seguridad analizadas en la presente guía.
229. Para proteger los dispositivos en este caso es necesario contar con la colaboración del usuario, haciéndole partícipe de los riesgos y amenazas de seguridad existentes y concienciándolo y asesorándolo desde el punto de vista de seguridad sobre la configuración y uso más adecuados.
230. En el segundo caso, es necesario el uso de herramientas y plantillas de seguridad que establezcan la configuración de seguridad deseada en todos los dispositivos de forma automática, limitando la posibilidad de modificación de la configuración por parte del usuario, y prohibiendo el desbloqueo del dispositivo mediante técnicas de *jailbreak*.
231. Por ejemplo, Apple dispone de una utilidad denominada *iPhone Configuration Utility* [Ref.- 50] para el iPhone que permite, entre otros, configurar códigos de acceso alfanuméricos (en lugar del PIN de 4 dígitos existente por defecto), limitar las descargas de la *App Store*, permitir el acceso por e-mail sólo a cuentas corporativas (y no personales), así como el bloquear el uso de otras funcionalidades, como la cámara o la posibilidad de navegación web.
232. Se recomienda hacer uso de estas herramientas de configuración especialmente para incrementar el nivel de seguridad de los códigos de acceso al dispositivo y para limitar las aplicaciones que pueden ser instaladas en los mismos.

6.4 ALMACENAMIENTO DE INFORMACIÓN

233. Una de las recomendaciones principales para proteger la confidencialidad, integridad y disponibilidad de la información almacenada en los dispositivos móviles se basa en emplear mecanismos de cifrado de los datos. Adicionalmente, numerosos estándares, legislaciones y regulaciones (HIPAA, SarbOx, PCI DSS) en diferentes países y sectores de la industria exigen este tipo de controles de seguridad.
234. La solución de cifrado debe ser aplicada tanto a las capacidades de almacenamiento internas del dispositivo, como a las tarjetas de memoria externas, debido a la movilidad asociada a ambos tipos de almacenamiento y su exposición a intrusos potencialmente interesados en los datos almacenados.

235. En función de las capacidades de computo del dispositivo móvil, el proceso de cifrado y descifrado de los datos en tiempo real puede conllevar un impacto relevante en el rendimiento del terminal. Sin embargo, la capacidad existente en los dispositivos móviles actuales más avanzados permite emplear cifrado sin afectar al uso normal del terminal.
236. En el caso de soluciones de cifrado aplicadas al dispositivo por completo (*full-disk encryption*), debe tenerse en cuenta que el acceso a la información es posible de forma transparente una vez se dispone de acceso al dispositivo, es decir, se dispone del código de acceso al mismo.
237. El iPhone 3GS es la primera versión de este dispositivo que incluye capacidades de cifrado de la información y datos almacenados en el mismo. Sin embargo, existen técnicas que permiten realizar una copia no cifrada de todos los datos contenidos en el dispositivo [Ref.- 49]. La versión 4 del iPhone incluirá mejoras en la funcionalidad de cifrado de los datos almacenados con el objetivo de evitar esta vulnerabilidad.
238. Adicionalmente, es posible emplear *software* de cifrado independiente del sistema operativo del dispositivo y que sólo protege ciertos datos. Para acceder a los datos protegidos por este *software* es necesario disponer de una contraseña, independiente del código de acceso al dispositivo, que permite gestionar la información más confidencial.
239. Existen soluciones propias del fabricante del sistema operativo, como *Mobile Encryption* [Ref.- 63] en Windows Mobile, las capacidades de cifrado del iPhone 3GS (previamente mencionadas), o la opción de protección de contenidos en BlackBerry, que cifra los datos almacenados con AES (256 bits).
240. Asimismo se dispone de soluciones comerciales para el cifrado de datos en dispositivos móviles, como *PGP Mobile* [Ref.- 61] o *Data Armor* [Ref.- 62] para Windows Mobile, y *Checkpoint Pointsec Mobile Encryption* para Symbian, Windows Mobile y Palm OS.
241. Además del cifrado de los datos e información almacenada en el dispositivo, se recomienda disponer de una copia de seguridad (o *backup*) actualizada de los contenidos del dispositivo móvil.
242. Los fabricantes de dispositivos móviles disponen de *software* que puede ser instalado en un ordenador de sobremesa o portátil para la sincronización y realización de copias de seguridad entre el dispositivo y el ordenador, como por ejemplo iTunes en el caso del iPhone, y ActiveSync (para Windows XP) o el Centro de Dispositivos de Windows Mobile (*Windows Mobile Device Center*, para Windows Vista y Windows 7). En el caso de otros dispositivos, existen soluciones comerciales de otros fabricantes, como por ejemplo *The Missing Sync* o *MyBackup Pro* para Android, o el *BlackBerry Desktop Software* (o *Manager*) para BlackBerry.
243. Como norma general es recomendable que el *software* realice la sincronización y la copia de seguridad del dispositivo móvil de forma automática cada vez que éste se conecte al ordenador, típicamente a través de cable USB, con el objetivo de realizar dicha copia frecuentemente. Según el *software* empleado, existen múltiples opciones para la selección y configuración de los datos a sincronizar y copiar.
244. Asimismo se dispone de servicios “en la nube” que permiten la realización de copias de seguridad y la sincronización de los datos de los dispositivos móviles, como *iCloud* [Ref.- 64] de Apple para el iPhone, *MyPhone* [Ref.- 65] de Microsoft para terminales basados en Windows Mobile, los servicios de sincronización de Google (*Google Sync Services*) [Ref.- 66] para Android, o el servicio de sincronización de BlackBerry integrado en el servidor BES (*BlackBerry Enterprise Server*) para BlackBerry.

245. Por último, es necesario analizar y evaluar el tipo de información almacenada en el dispositivo móvil, no siendo recomendable almacenar información confidencial y sensible, o datos de cuentas, contraseñas o PINs de acceso a otros servicios.

6.5 LOCALIZACIÓN

246. La funcionalidad de localización geográfica a través del GPS, o localización estimada mediante redes inalámbricas WiFi y celdas de telefonía móvil, debe ser deshabilitada cuando no se requiere hacer uso de esta tecnología.

247. Sin embargo, los dispositivos móviles que han sido perdidos o sustraídos pueden ser localizados mediante una combinación de estas tecnologías (WiFi, telefonía móvil, GPS) y el uso de servicios orientados a su localización geográfica.

248. El servicio *iCloud* [Ref.- 64] de Apple permite la localización de dispositivos iPhone, al igual que el servicio *MyPhone* [Ref.- 65] de Microsoft permite la localización de terminales basados en Windows Mobile perdidos o sustraídos.

6.6 COMUNICACIONES BLUETOOTH

249. La funcionalidad de conexión con otros dispositivos mediante *Bluetooth* debe ser deshabilitada cuando no se requiere establecer una conexión mediante esta tecnología.

250. Esta recomendación general, que aplica a la mayoría de tecnologías de comunicación disponibles en los dispositivos móviles (analizadas en los siguientes apartados), permite adicionalmente alargar el uso del dispositivo entre recargas de batería, ya que el consumo de la misma se verá notablemente reducido.

251. El dispositivo móvil deber ser configurado en modo oculto o no visible, con el objetivo de no revelar su dirección física Bluetooth (o BD_ADDR), elemento necesario para establecer cualquier conexión *Bluetooth* con el mismo.

252. Se recomienda modificar los valores existentes por defecto para el nombre del dispositivo, ya que habitualmente éste incluye la marca y modelo de dispositivo, lo que facilita su identificación por parte de un atacante. Asimismo no es recomendable emplear como nombre del dispositivo el nombre de su propietario (persona o empresa), con el objetivo de evitar ataques dirigidos.

253. En el caso de disponer de la suficiente granularidad en la implementación de *Bluetooth* del dispositivo móvil, se recomienda habilitar únicamente los perfiles de *Bluetooth* que se desea utilizar.

254. El proceso de emparejamiento inicial entre dos dispositivos *Bluetooth* es vulnerable a múltiples ataques, tales como la interceptación de tráfico y posibilidad de obtención del PIN empleado, por lo que es necesario ser especialmente cuidadoso al elegir el lugar para llevar a cabo este primer emparejamiento. Se desaconseja realizarlo en lugares públicos e inseguros.

255. Es recomendable emplear dispositivos móviles que implementen las últimas especificaciones de *Bluetooth*, como por ejemplo la versión 2.1 (ratificada en julio de 2007) o posterior, ya que ésta proporciona mecanismos de emparejamiento más seguros, como *Secure Simple Pairing* (SSP).

256. Desafortunadamente, los fabricantes de dispositivos *Bluetooth* establecen o recomiendan el uso de PINs para el emparejamiento de dispositivos de únicamente 4 dígitos. Sin

- embargo, la especificación *Bluetooth* permite el uso de PINs de hasta 16 caracteres alfanuméricos.
257. Se recomienda hacer uso de PINs para el emparejamiento de dispositivos *Bluetooth* que hagan uso de caracteres alfanuméricos y cuya longitud sea de al menos entre 8-12 caracteres. Este tipo de PINs sólo puede ser utilizado si la implementación del dispositivo móvil permite esa longitud y juego de caracteres.
 258. El dispositivo *Bluetooth* debe ser configurado para solicitar confirmación por parte del usuario (autorización) antes de permitir cualquier conexión o hacer uso de cualquiera de los perfiles existentes.
 259. Es necesario concienciar a los usuarios para no aceptar ningún intento de conexión o mensaje *Bluetooth* no solicitados, ya que éstos han sido empleados por especímenes de malware para su propagación a través de *Bluetooth* en el pasado, y pese a que prácticas de uso comunes y aceptadas socialmente, como el *marketing* de proximidad, hacen uso de este tipo de conexiones no solicitadas.
 260. Los dispositivos *Bluetooth* disponen de una base de datos en la que almacenan los datos de emparejamiento de otros dispositivos a los que se han conectado previamente, tales como dirección física y claves de enlace. Es conveniente gestionar esta base de datos, y de forma periódica eliminar de la misma aquellos emparejamientos que no son usados habitualmente o que se prevé no volverán a ser utilizados.
 261. La guía CCN-STIC-418 proporciona más información sobre la seguridad en *Bluetooth* [Ref.- 55].

6.7 COMUNICACIONES WIFI

262. La funcionalidad de conexión a redes inalámbricas WiFi debe ser deshabilitada cuando no se requiere establecer una conexión mediante esta tecnología.
263. Los usuarios deberían hacer uso de las capacidades de conexión WiFi únicamente en redes con un nivel de seguridad adecuado, es decir, que hacen uso de los mecanismos de seguridad WPA o WPA2 (preferiblemente este último), evitando establecer conexiones con redes WiFi públicas sin ninguna seguridad (sin autenticación ni cifrado) o que emplean mecanismos de seguridad WEP.
264. En el caso de redes WiFi basadas en WPA o WPA2 Personal, la clave de acceso a la red WiFi debería ser suficientemente larga (más de 20 caracteres) y difícilmente adivinable. En su defecto, y más recomendable desde el punto de vista de seguridad, se debería emplear WPA o WPA2 Enterprise, solución que emplea mecanismos de autenticación avanzados basados en los protocolos 802.1x y EAP.
265. En el caso de requerir establecer conexiones a través de redes WiFi inseguras, se recomienda hacer uso de tecnologías VPN (*Virtual Private Network*) con el objetivo de cifrar todos los datos recibidos y transmitidos por el dispositivo móvil, minimizando así la posibilidad de ataques de interceptación y modificación del tráfico.
266. Esta recomendación se extiende a cualquier conexión de datos establecida desde el dispositivo móvil, como por ejemplo, conexiones de datos a través de las redes de telefonía móvil (GPRS, EDGE o UMTS; referenciadas en el siguiente apartado).
267. La mayoría de dispositivos disponen de una base de datos en la que almacenan todas y cada una de las redes WiFi a las que se han conectado en el pasado (lista de redes

- preferidas), con el objetivo de poderse volver a conectar a ellas si se encuentran en el área de cobertura. Se recomienda configurar el dispositivo móvil para que no intente conectarse automáticamente a redes inalámbricas WiFi a las que ha estado conectado previamente.
268. Asimismo se debería evitar que el dispositivo almacene información de redes a las que se ha asociado de forma temporal, o borrar esa información manualmente, con el objetivo de evitar una asociación automática posterior. Por tanto, el dispositivo sólo debería almacenar las redes a las que se conecta habitualmente y que presentan un nivel de seguridad adecuado.
269. La guía CCN-STIC-406 proporciona más información sobre la seguridad de redes inalámbricas WiFi [Ref.- 56].

6.8 COMUNICACIONES DE TELEFONÍA MÓVIL

270. La funcionalidad de conexión a redes de datos de telefonía móvil (GPRS, EDGE, o UMTS) debe ser deshabilitada cuando no se requiere establecer una conexión mediante estas tecnologías.

Nota: esta guía considera que las capacidades de comunicación de voz de telefonía de los dispositivos móviles son necesarias para el usuario en todo momento, por lo que no se recomienda deshabilitarlas explícitamente. Sin embargo, puede ser aconsejable desactivar su utilización en entornos y escenarios concretos.

271. No se debe asumir que las conversaciones de voz a través de dispositivos móviles son confidenciales, al igual que no lo son otros medios de comunicación como fax o e-mail, pese al carácter cerrado y propietario de las infraestructuras de los operadores de telefonía móvil.
272. Para proteger la confidencialidad de las comunicaciones y llamadas de voz sobre redes no fiables existe software de cifrado extremo a extremo, como el proporcionado por *Cellcrypt* (para Symbian y BlackBerry) [Ref.- 74], *Sigillu* [Ref.- 75] (multiplataforma) o productos verificados por el Centro Criptológico Nacional (ver CCN-STIC-103 Catálogo de productos con Certificación Criptológica). Las comunicaciones de voz cifradas pueden ser cursadas sobre cualquier red de datos: 2.5G, 3G, 3.5G y WiFi.
273. La recepción de mensajes de texto SMS es el objetivo de múltiples ataques y vulnerabilidades recientes, por lo que, aparte de aplicar las actualizaciones proporcionadas por el fabricante del terminal, es necesario que el usuario sea consciente de los riesgos asociados a la lectura de un mensaje de texto. Se recomienda no abrir ningún mensaje de texto no esperado o solicitado, práctica similar a la empleada para la gestión de correos electrónicos en equipos portátiles y de sobremesa, o dispositivos móviles.
274. Debido a las numerosas vulnerabilidades existentes en los protocolos y estándares de comunicaciones móviles englobados bajo las tecnologías 2G, se recomienda utilizar únicamente las tecnologías de comunicación móviles 3G.
275. Para ello, es necesario configurar el dispositivo móvil para utilizar únicamente la red de telefonía 3G. Algunos dispositivos móviles, como el Nokia N97 [Ref.- 54], basado en Symbian, permiten al usuario utilizar únicamente la red 3G, o ambas redes (2G y 3G) en

su configuración por defecto, aunque se trate de una característica que no es publicitada en sus especificaciones técnicas.

276. Otros dispositivos, como el iPhone de Apple, permiten habilitar o deshabilitar las comunicaciones 3G, pero no así las 2G.
277. Adicionalmente, es posible mitigar algunas de las amenazas y vulnerabilidades descritas eliminando los servicios disponibles a través del operador de telefonía móvil, como por ejemplo la ausencia de capacidades de comunicaciones de datos asociadas al contrato de la tarjeta SIM, la imposibilidad de realizar llamadas de voz internacionales (debido a su elevado coste), o el bloqueo en la recepción de mensajes de texto originados en Internet (fuente principal de SPAM mediante SMS).
278. La guía CCN-STIC-407 proporciona más información sobre seguridad en telefonía móvil [Ref.- 57].

6.9 SOFTWARE Y APLICACIONES CLIENTE

279. Debe tenerse en cuenta que las limitaciones de los dispositivos móviles, con pantallas táctiles reducidas e interfaces de usuario limitados, facilitan la realización de engaños y la manipulación de las acciones del usuario, ya que es más difícil para el usuario disponer de toda la información necesaria para verificar la validez o veracidad de mensajes de aviso, establecimiento de conexiones e interacción con servicios y aplicaciones.
280. Se recomienda instalar únicamente aplicaciones software de la tienda oficial del fabricante del dispositivo. Esta recomendación está directamente relacionada con la prohibición en algunos entornos para realizar el *jailbreak* de los dispositivos móviles.
281. No se deben almacenar las contraseñas de los diferentes servicios y aplicaciones empleados en el propio dispositivo móvil, sino forzar a que el dispositivo solicite la contraseña al usuario en el momento de acceder al servicio o aplicación.
282. Una consideración a tener en cuenta, propia de los dispositivos móviles frente a otros equipos informáticos, y debida mayormente a la limitación de los teclados físicos o táctiles de estos dispositivos, se centra en la dificultad que el usuario tiene a la hora de introducir contraseñas complejas y de longitud elevada. Por este motivo, la tendencia natural del usuario es emplear PINs o códigos de acceso y contraseñas sencillas, como por ejemplo, 4 dígitos.
283. Cada una de las principales plataformas (y sistemas operativos) asociadas a los dispositivos móviles ofrece un modelo y nivel de seguridad diferente respecto a la instalación de nuevo software o aplicaciones cliente:
284. Así por ejemplo, el iPhone no permite la instalación de aplicaciones que no provengan de la *App Store* (salvo que se haya realizado el *jailbreak* del dispositivo). Android sólo permite la instalación de aplicaciones desde el *Android Marketplace* por defecto, pero dispone de una opción de configuración para permitir al usuario la instalación de software desde otras fuentes. BlackBerry sólo permite la instalación de aplicaciones firmadas, pero dispone de una opción de configuración para permitir la instalación de aplicaciones no firmadas. En cualquier caso, la obtención de claves de firma de aplicaciones de BlackBerry tiene un coste reducido, de unos 20 dólares (USD), lo que induce a crear un falso nivel de seguridad.
285. La gestión en la ejecución de software es controlada también por cada una de las plataformas asociadas a los dispositivos móviles de manera muy diferente:

286. Así por ejemplo, el iPhone presenta un número reducido de controles para definir los permisos asociados a la ejecución de una aplicación, mientras que Windows Mobile define tras niveles de ejecución (privilegiado, normal y restringido; equivalentes a disponer de acceso de ejecución completo, limitado a ciertas funcionalidades y accesos a ficheros, o nulo, respectivamente). Android presenta una mayor granularidad para definir los permisos de una aplicación para acceder a las redes de comunicaciones (*Bluetooth*, *Wifi*, celular, etc), al módulo de telefonía (llamadas, SMS y MMS), a los datos de localización, y a los datos personales (calendario, contactos, etc). Estos permisos son definidos por el desarrollador de la aplicación y aceptados por el usuario en el momento de su instalación.
287. Las diferentes plataformas asociadas a los dispositivos móviles presentan diferentes modelos de seguridad para el aislamiento de las aplicaciones (*sandbox*), con el objetivo de que una aplicación maliciosa no pueda comprometer el sistema u otras aplicaciones:
288. Así por ejemplo el iPhone ejecuta múltiples aplicaciones con el mismo nivel de privilegios, con los riesgos de seguridad que ello conlleva. Android, por otro lado, ejecuta cada aplicación con un identificador (de usuario y grupo) único, generado en el momento de su instalación, con el objetivo de limitar el acceso únicamente a la información gestionada por cada aplicación.
289. Adicionalmente se deben aplicar las recomendaciones de seguridad generales para todas aquellas aplicaciones estándar que no son propias de dispositivos móviles, sino que también existen en ordenadores de sobremesa y portátiles, como por ejemplo los navegadores web.
290. Por ejemplo, con el objetivo de proteger las actividades de navegación web se recomienda:
- Deshabilitar las capacidades de ejecución de Javascript del navegador, y habilitarlas (de ser posible) de forma individual para cada sitio web visitado.
 - Deshabilitar el uso de plug-ins para la visualización de documentos ofimáticos o ficheros multimedia (audio y vídeo) en el navegador, o en su defecto, únicamente habilitar aquellos plug-ins que vayan a ser usados frecuentemente.
 - Habilitar la funcionalidad del navegador para la detección de sitios web sospechosos, maliciosos o asociados a phishing (en el caso de disponer de estas capacidades en el navegador web del dispositivo móvil).
 - Deshabilitar la funcionalidad que permite autocompletar la información introducida en campos de formularios de páginas web.
 - Deshabilitar el almacenamiento de contraseñas y credenciales en el navegador web.
291. Por otro lado, y con el objetivo de proteger las comunicaciones de voz sobre redes de datos basadas en voz sobre IP (VoIP), se recomienda consultar la guía CCN-STIC-414, que proporciona más información sobre seguridad en VoIP [Ref.- 58].
292. La protección frente a ataques basados en la distribución de aplicaciones maliciosas correctamente firmadas y aprobadas por el fabricante, como el gusano *Sexy View* distribuido por SMS [Ref.- 38] (analizado previamente), pese a que Symbian revocó los certificados digitales empleados para su firma, requiere de acciones adicionales por parte del usuario

293. Pese a que los certificados digitales empleados en el ataque fueron revocados, éstos no son distribuidos de forma automática a los millones de dispositivos móviles Symbian existentes. La configuración por defecto de la mayoría de terminales Symbian debe modificarse para habilitar la recepción de certificados revocados.
294. Para ello, es necesario acceder a la configuración del gestor de aplicaciones (*Application Manager*), y fijar el valor de “*Online certificate check*” al valor que indica la obligatoriedad de comprobar el estado del certificado: “*Must be passed*”.

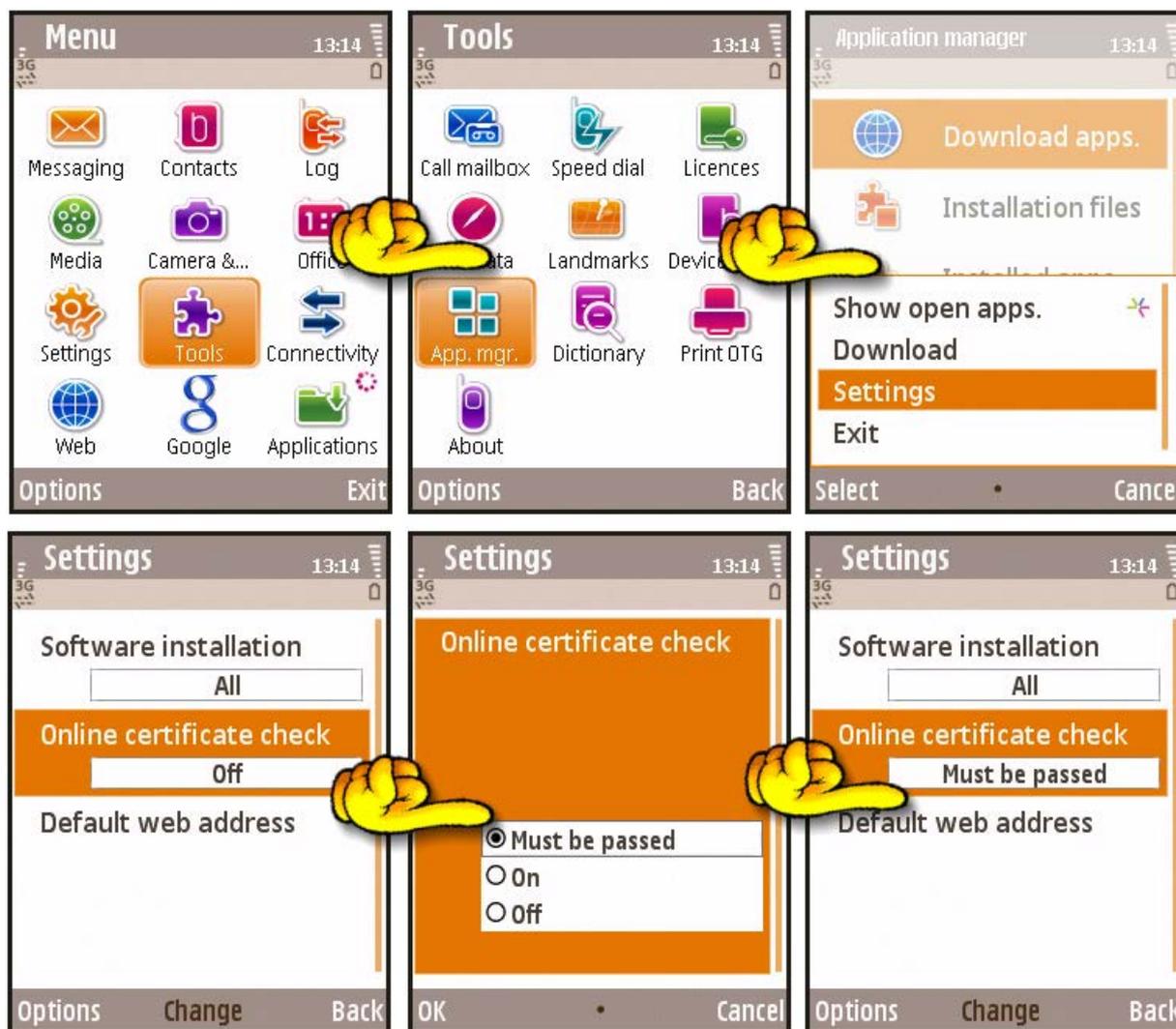


Figura 10. Configuración en Symbian para verificar el estado de los certificados digitales [Ref.- 58].

295. Con respecto al uso de las redes sociales móviles, es fundamental incidir en la importancia de una buena concienciación de seguridad en el usuario del dispositivo móvil, enfatizando el uso responsable de las mismas y de los contenidos publicados por el usuario (mensajes, comentarios, fotos, vídeos, etc.).
296. El usuario es responsable en todo momento de los contenidos que publica sobre él, sus conocidos o su puesto de trabajo, y debe siempre mantener tanto su privacidad, personal y profesional, como la de sus conocidos. En Europa existen numerosas directivas y legislaciones centradas en la protección de datos personales y la privacidad de los ciudadanos [Ref.- 9].

297. Se recomienda por tanto que el usuario analice minuciosamente la información que publica en las redes sociales móviles (sobre el mismo, sus conocidos o empresa), no publicando nunca información sensible.
298. Asimismo el usuario debe seguir otras recomendaciones de seguridad, como hacer uso de pseudónimos en lugar de emplear su nombre real, no aceptar peticiones de amigos desconocidos, verificar su lista de contactos periódicamente, gestionar con cautela la información profesional publicada en redes sociales personales (independizando ambos tipos de redes), no permitir el acceso a los detalles de su perfil sin su consentimiento, no almacenar la contraseña de la red social en su dispositivo, fijar el nivel de privacidad de su perfil de forma restrictiva (limitando quién puede acceder a sus fotos, contactarle o añadir comentarios), y desactivar el uso de servicios de localización cuando no se está haciendo uso de los mismos.

6.10 DETECCIÓN DE MALWARE EN DISPOSITIVOS MÓVILES

299. Los mecanismos de detección de *malware* tradicionales tienen limitaciones notables para su aplicación en dispositivos móviles. La capacidad de procesamiento necesaria para poder comparar ficheros con bases de datos de firmas de gran tamaño, la necesidad de realizar un escaneo continuo y el consumo de recursos requerido, acabarían con la batería de los terminales en poco tiempo.

6.11 PROPAGACIÓN DE MALWARE HACIA OTROS DISPOSITIVOS

300. Se recomienda configurar los ordenadores de sobremesa o portátiles empleados para la conexión y sincronización de dispositivos móviles de forma segura para que no ejecuten ninguna acción automática a nivel del sistema operativo al detectar la presencia del dispositivo móvil, y en concreto, al detectar a éste como una unidad de almacenamiento. Por ejemplo, deshabilitando la funcionalidad de *autorun* en Windows [Ref.- 11].
301. Los dispositivos móviles BlackBerry pueden ser configurados de forma segura para evitar la propagación de *malware* hacia otros equipos de forma automática.
302. Los terminales BlackBerry disponen de un modo de almacenamiento USB dónde actúan como un disco USB externo. Este modo puede estar accesible de forma automática, o únicamente tras introducir una contraseña, configuración ésta que mitiga la posibilidad de propagación a través del mecanismo de ejecución automático en entornos Windows.
303. El modo de almacenamiento USB puede ser deshabilitado en el *BlackBerry Enterprise Server* (BES) si no es necesario disponer de dicha funcionalidad para transferir ficheros, fotos o música a los dispositivos móviles BlackBerry, como por ejemplo en entornos dónde los dispositivos son gestionados “*over the air*” (OTA, es decir, a través de las redes de comunicación inalámbricas).

6.12 TRAZABILIDAD

304. Los dispositivos móviles son cada vez más complejos y generan cantidades relevantes de eventos y registros (*logs*) asociados a su uso y a la ejecución de las diferentes aplicaciones disponibles y funcionalidad propia del sistema operativo.
305. Se recomienda activar las capacidades de trazabilidad, es decir, registro de eventos, y obtener y procesar los *logs* generados, con el objetivo de analizar las actividades llevadas

a cabo por los dispositivos y detectar posibles anomalías, intrusiones e incidentes de seguridad.

306. Cada sistema operativo móvil, y las aplicaciones instaladas sobre éstos, pueden proporcionar diferentes opciones y mecanismos para la generación y el almacenamiento de *logs*. Se recomienda revisar cada uno de ellos para proceder a su activación.
307. Incluso los terminales de telefonía más sencillos permiten mantener un registro de las llamadas realizadas y recibidas, así como de los mensajes SMS intercambiados [Ref.- 71]. Por defecto esta funcionalidad está deshabilitada, por lo que se recomienda su activación antes de comenzar a usar el dispositivo.

6.13 SOFTWARE DE GESTIÓN Y SEGURIDAD

308. La integración de los dispositivos móviles en las infraestructuras y políticas de gestión de las tecnologías de la información y de seguridad de la información de las organizaciones es una necesidad, por lo que los diferentes fabricantes de dispositivos móviles están orientando sus soluciones hacia el ámbito profesional y de negocios frente al uso personal de los terminales.
309. Así por ejemplo, Apple dispone de soluciones de gestión de los dispositivos móviles basadas en Microsoft Exchange para el iPhone, al igual que la propia Microsoft para Windows Mobile, mientras que RIM proporciona soluciones con servidores BES para BlackBerry.
310. Es fundamental por tanto para los departamentos de seguridad de la información emplear soluciones corporativas que permitan una adecuada gestión, inventario y control de los dispositivos móviles, su configuración y nivel de seguridad.
311. Entre el *software* de seguridad que se recomienda instalar en los dispositivos móviles, adicionalmente al *software* existente por defecto, se encuentran aplicaciones de cifrado de datos, cortafuegos, antivirus, sistemas de detección de intrusos, soluciones *anti-spam*, y capacidades VPN. La disponibilidad de este software de seguridad varía en función del tipo de dispositivo, existiendo soluciones comerciales para dispositivos móviles por parte de los principales fabricantes de soluciones de seguridad, como Symantec, McAfee, F-Secure, Credant, Kaspersky, Eset, etc [Ref.- 59].
312. Complementando la política de seguridad definida para los dispositivos móviles de la organización, las recomendaciones de configuración para incrementar su nivel de seguridad, la aplicación de buenas prácticas de uso, y la instalación de aplicaciones de seguridad específicas, se recomienda llevar a cabo de forma periódica auditorías y pruebas de intrusión que tengan como objetivo los dispositivos móviles para evaluar su nivel de protección y grado de seguridad real.
313. Durante el proceso de auditoría debería identificarse no sólo la existencia de dispositivos móviles vulnerables, sino también la presencia de terminales no conformes con la política de seguridad establecida por la organización.

7 REFERENCIAS

314. La siguiente tabla muestra las fuentes de información a las que se hace referencia a lo largo de la presente guía:

Referencia	Título, autor y ubicación
[Ref.- 1]	Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. BOE. URL: http://www.boe.es/boe/dias/2010/01/29/pdfs/BOE-A-2010-1330.pdf
[Ref.- 2]	Séptima edición del estudio Mediascope Europe. Asociación Europea de Publicidad Interactiva (EIAA). 23 de febrero de 2010. Cadena Ser. URL: http://www.cadenaser.com/tecnologia/articulo/espanoles-dedican-horas-internet-television/csrcsrpor/20100223csrcsrtec_2/Tes
[Ref.- 3]	Séptima edición del estudio Mediascope Europe. Asociación Europea de Publicidad Interactiva (EIAA). 23 de febrero de 2010. ABC. URL: http://www.abc.es/hemeroteca/historico-23-02-2010/abc/Medios_Redex/133-horas-semanales-frente-al-ordenador-o-el-movil_1134010983921.html
[Ref.- 4]	“Informe de amenazas CCN-CERT IA-02/09: Seguridad móvil”. CCN-CERT. 2009. URL: (Requiere autenticación) https://www.ccn-cert.cni.es/index.php?option=com_docmanpriv&task=doc_download&gid=88&Itemid=168&lang=es
[Ref.- 5]	“CCN-CERT IA-01/09: Ciberamenazas 2008 y Tendencias 2009”. CCN-CERT. 2009. URL: (Requiere autenticación) https://www.ccn-cert.cni.es/index.php?option=com_docmanpriv&task=doc_download&gid=82&Itemid=168&lang=es
[Ref.- 6]	“Smartphone Weather App Builds A Mobile Botnet”. Kelly Jackson Higgins. DarkReading. Marzo, 2010. URL: http://www.darkreading.com/insiderthreat/security/client/showArticle.jhtml?articleID=223200001
[Ref.- 7]	“Vodafone distributes Mariposa botnet”. Pedro Bustamante. Panda. Marzo, 2010. URL: http://research.pandasecurity.com/vodafone-distributes-mariposa/
[Ref.- 8]	“Botnet Mariposa”. Luis Corrons. Panda. Marzo, 2010. URL: http://pandalabs.pandasecurity.com/mariposa-botnet/
[Ref.- 9]	Online as soon as it happens. ENISA. Febrero, 2010. URL: http://www.enisa.europa.eu/act/ar/deliverables/2010/onlineasithappens
[Ref.- 10]	Security Issues in the Context of Authentication Using Mobile Devices (Mobile eID). ENISA. Noviembre, 2008. URL: http://www.enisa.europa.eu/act/it/eid/mobile-eid
[Ref.- 11]	“How to disable the Autorun functionality in Windows”. Microsoft. Julio, 2009. URL: http://support.microsoft.com/kb/967715
[Ref.- 12]	“HTC / Windows Mobile OBEX FTP Service Directory Traversal Vulnerability”. Alberto Moreno Tablado. CVE-2009-0244. URL: http://www.seguridadmobile.com/windows-mobile/windows-mobile-security/HTC-Windows-Mobile-OBEX-FTP-Service-Directory-Traversal.html
[Ref.- 13]	App Store. Apple. URL: http://www.apple.com/iphone/apps-for-iphone/
[Ref.- 14]	Android Market. Google. URL: http://www.android.com/market/
[Ref.- 15]	“Hunting Mobile Threats in Memory”. Erica Naone. MIT Technology Review. 5 de marzo de 2010. URL: http://www.technologyreview.com/communications/24692/
[Ref.- 16]	“CanSecWest: Pwn2Own 2009”. Terri Forslof. 25 de febrero de 2009. URL: http://dvlabs.tippingpoint.com/blog/2009/02/25/pwn2own-2009
[Ref.- 17]	“CanSecWest: Pwn2Own 2010”. Aaron Portnoy. 15 de febrero de 2010. URL: http://dvlabs.tippingpoint.com/blog/2010/02/15/pwn2own-2010

Referencia	Título, autor y ubicación
[Ref.- 18]	“CCN-CERT IA-03-10: Ciberamenazas 2009 y Tendencias 2010”. CCN-CERT. 2010. URL: (Requiere autenticación) https://www.ccn-cert.cni.es/index.php?option=com_docmanpriv&task=doc_download&gid=122&Itemid=168&lang=es
[Ref.- 19]	Ejemplos de software comercial de espionaje: - Spy Phone. URL: http://spyphone.biz - Mobile Spy. URL: http://www.mobile-spy.com - FlexySPY. URL: http://www.flexispy.com
[Ref.- 20]	“BlackBerry customers revolt after spyware scandal”. Graham Cluley. Sophos. 23 de julio de 2009. URL: http://www.sophos.com/blogs/gc/g/2009/07/23/blackberry-customers-revolt-after-spyware-scandal/
[Ref.- 21]	“Vodafone distributes Mariposa –Part 2”. Pedro Bustamante. Panda Security. Marzo 2010. URL: http://research.pandasecurity.com/vodafone-distributes-mariposa-part-2/
[Ref.- 22]	“Vodafone arreglará 3.000 móviles que pueden verse afectados por el virus 'mariposa’”. El País. 18 de marzo de 2010. URL: http://www.elpais.com/articulo/tecnologia/Vodafone/arreglara/3000/moviles/pueden/verse/afectados/virus/mariposa/elpeputec/20100318elpeputec_12/Tes
[Ref.- 23]	[11] “Fuzzing the Phone in your Phone”. C. Miller, C. Mulliner. Blackhat USA 2009. URL: http://www.blackhat.com/presentations/bh-usa-09/MILLER/BHUSA09-Miller-FuzzingPhone-PAPER.pdf URL: http://www.blackhat.com/presentations/bh-usa-09/MILLER/BHUSA09-Miller-FuzzingPhone-SLIDES.pdf
[Ref.- 24]	[12] “Attacking SMS”. Zane Lackey, Luis Miras. Blackhat USA 2009. URL: http://www.blackhat.com/presentations/bh-usa-09/LACKEY/BHUSA09-Lackey-AttackingSMS-SLIDES.pdf
[Ref.- 25]	“There is some SMiShing going on in the EU”. Internet Storm Center (ISC). Marzo, 2009. URL: http://isc.sans.org/diary.html?storyid=6076 URL: http://hphosts.blogspot.com/2009/03/malicious-sms-sending-victims-to.html
[Ref.- 26]	“Easy as pie: Apple anti-virus is a peach at detecting infected BlackBerries”, Sophos. Tony Ross. 30 de octubre de 2009. URL: http://www.sophos.com/blogs/chetw/g/2009/10/30/apple-antivirus-detecting-infected-blackberries/
[Ref.- 27]	“GSM: SRSLY?”. Karsten Nohl. 26th Chaos Communication Congress (CCC). 27 de diciembre 2009. URL: http://events.ccc.de/congress/2009/Fahrplan/events/3654.en.html
[Ref.- 28]	“A Practical-Time Attack on the A5/3 Cryptosystem Used in Third Generation GSM Telephony”. Orr Dunkelman, Nathan Keller, and Adi Shamir. Weizmann Institute of Science. Enero, 2010. URL: http://eprint.iacr.org/2010/013.pdf
[Ref.- 29]	“First iPhone Worm Spreads Rick Astley Wallpaper”. IDG. Robert McMillan. 8 de noviembre de 2009. URL: http://www.pcworld.com/businesscenter/article/181697/first_iphone_worm_spreads_rick_astley_wallpaper.html
[Ref.- 30]	“Malicious iPhone Worm”. F-Secure. 22 de noviembre de 2009. URL: http://www.f-secure.com/weblog/archives/00001822.html
[Ref.- 31]	“First iPhone Worm Found”. F-Secure. 8 de noviembre de 2009. URL: http://www.f-secure.com/weblog/archives/00001814.html
[Ref.- 32]	“Intego Security Memo: iPhone Worm Creates Botnet, Copies Personal Data”. Intego. 21 de noviembre de 2009. URL: http://blog.intego.com/2009/11/23/intego-security-memo-iphone-worm-creates-botnet-copies-personal-data/
[Ref.- 33]	“New iPhone worm can act like botnet say Experts”. BBC. 23 de noviembre de 2009. URL: http://news.bbc.co.uk/2/hi/technology/8373739.stm

Referencia	Título, autor y ubicación
[Ref.- 34]	<p>“iPhone Ransomware? Dutch Hacker Exploits Jailbroken iPhone Bug and Asks for Money”. The Mac Security Blog. Intego. 3 de noviembre de 2009. URL: http://blog.intego.com/2009/11/03/iphone-ransomware-dutch-hacker-exploits-jailbroken-iphone-bug-and-asks-for-money/</p>
[Ref.- 35]	<p>“Intego Security Memo: Hacker Tool Copies Personal Info from iPhones”. Intego. 11 de noviembre de 2009. URL: http://blog.intego.com/2009/11/11/intego-security-memo-hacker-tool-copies-personal-info-from-iphones/</p>
[Ref.- 36]	<p>“Banking malware found on Android Marketplace”. Graha, Cluley. Sophos. 11 de enero de 2010. URL: http://www.sophos.com/blogs/gc/g/2010/01/11/banking-malware-android-marketplace/</p>
[Ref.- 37]	<p>“A Touch of Mobile Threat Déjà Vu”. Symantec. Irfan Asrar. 25 de febrero de 2010. URL: http://www.symantec.com/connect/blogs/touch-mobile-threat-deja-vu</p>
[Ref.- 38]	<p>““Sexy View” Trojan on Symbian S60 3rd Edition”. F-Secure. 18 de febrero de 2009. URL: http://www.f-secure.com/weblog/archives/00001609.html URL: http://www.f-secure.com/weblog/archives/00001721.html URL: http://www.f-secure.com/weblog/archives/00001732.html URL: http://www.f-secure.com/v-descs/worm_symbols_yxe.shtml</p>
[Ref.- 39]	<p>“Mobile phone trojans”. Bojan Zdrnja. Internet Storm Center. 1 de julio de 2009. URL: http://isc.sans.org/diary.html?storyid=6691</p>
[Ref.- 40]	<p>“AT&T Cell Phone Phish”. Rob VandenBrink & Donald Smith. Internet Storm Center. 10 de septiembre de 2009. URL: http://isc.sans.org/diary.html?storyid=7309 URL: http://isc.sans.org/diary.html?storyid=4507</p>
[Ref.- 41]	<p>“Rutgers Researchers Show New Security Threat Against ‘Smart Phone’ Users”. Rutgers. 22 de febrero de 2010. URL: http://news.rutgers.edu/medrel/news-releases/2010/02/rutgers-researchers-20100222 URL: http://www.cs.rutgers.edu/~vinodg/papers/hotmobile2010/</p>
[Ref.- 42]	<p>NFC (Near Field Communication) Forum. URL: http://www.nfc-forum.org</p>
[Ref.- 43]	<p>““la Caixa” y Telefónica lanzan en Sitges la primera gran experiencia de compras en España con teléfonos móviles NFC y con el sistema de pago Visa”. Telefónica. 11 de febrero de 2010. URL: http://pressoffice.telefonica.com/documentos/nprensa/np_sitges_11022010_0.pdf</p>
[Ref.- 44]	<p>“Twitter Worms - Koobface Diversifies”. Sophos Blog. 17 de julio de 2009. URL: http://www.sophos.com/blogs/sophoslabs/v/post/5431</p>
[Ref.- 45]	<p>“Windows Marketplace for Mobile”. Microsoft. URL: http://www.microsoft.com/windowsmobile/en-us/meet/marketplace.aspx</p>
[Ref.- 46]	<p>SpyPhone. Nicolas Seriot. 2009. URL: http://seriot.ch/blog.php?article=20091203</p>
[Ref.- 47]	<p>“iPhone Privacy”. Nicolas Seriot. Black Hat DC 2010. URL http://seriot.ch/resources/talks_papers/iPhonePrivacy.pdf</p>
[Ref.- 48]	<p>“Removing iPhone 3G[s] Passcode and Encryption”. Jonathan Zdziarski. YouTube. URL: http://www.youtube.com/watch?v=5wS3AMbXRLs</p>
[Ref.- 49]	<p>“What Can you Steal from an iPhone 3Gs in 2 Minutes?”. Jonathan Zdziarski. YouTube. URL: http://www.youtube.com/watch?v=34f47m-1YSg</p>
[Ref.- 50]	<p>iPhone Configuration Utility. Apple. URL: http://www.apple.com/support/iphone/enterprise/</p>
[Ref.- 51]	<p>“When Mobile is Harder Than Fixed (and Vice Versa): Demystifying Security Challenges in Mobile Environments”. Jon Oberheide, Farnam Jahanian. UMICH. 2010.</p>
[Ref.- 52]	<p>“3G Americas Project: Gsm technologies to reach 4 billion mobile connections worldwide”. Agosto, 2009. URL: http://www.3gamericas.org/index.cfm?fuseaction=pressreleasedisplay&pressreleaseid=2451</p>

Referencia	Título, autor y ubicación
[Ref.- 53]	“Stragglers of the Herd Get Eaten: Security Concerns for GSM Mobile Banking Applications”. Michael Paik. NYU. 2010.
[Ref.- 54]	“Nokia N97”. URL: http://europe.nokia.com/find-products/devices/nokia-n97 URL: http://europe.nokia.com/find-products/devices/nokia-n97/specifications
[Ref.- 55]	“Guía CCN-STIC-418: Seguridad en Bluetooth”. CCN-CERT. URL: https://www.ccn-cert.cni.es - Herramientas – Series CCN-STIC
[Ref.- 56]	“Guía CCN-STIC-406: Seguridad en redes inalámbricas”. CCN-CERT. URL: https://www.ccn-cert.cni.es - Herramientas – Series CCN-STIC
[Ref.- 57]	“Guía CCN-STIC-407: Seguridad en telefonía móvil”. CCN-CERT. URL: https://www.ccn-cert.cni.es - Herramientas – Series CCN-STIC
[Ref.- 58]	“Guía CCN-STIC-414: Seguridad en VoIP”. CCN-CERT. URL: https://www.ccn-cert.cni.es - Herramientas – Series CCN-STIC
[Ref.- 59]	“Mobile Malware Attacks and Defense”. Ken Dunhan et. al. Syngress. 2008. ISBN: 9781597492980. URL: http://www.syngress.com/hacking-and-penetration-testing/Mobile-Malware-Attacks-and-Defense/
[Ref.- 60]	“HTC Support & Downloads”. HTC. URL: http://www.htc.com/www/support.aspx
[Ref.- 61]	PGP Mobile. PGP. URL: http://www.pgp.com/products/mobile/index.html
[Ref.- 62]	Data Armor. Mobile Armor. URL: http://www.mobilearmor.com/dataarmor.php
[Ref.- 63]	Mobile Encryption. Windows Mobile. Microsoft. URL: http://msdn.microsoft.com/en-us/library/bb416357.aspx
[Ref.- 64]	iCloud. Apple. URL: http://www.apple.com/icloud/
[Ref.- 65]	MyPhone. Microsoft. URL: http://myphone.microsoft.com
[Ref.- 66]	Google Sync Services. Google. URL: http://www.google.com/sync/android.html
[Ref.- 67]	Paraben CSI Stick: URL: http://www.csistick.com
[Ref.- 68]	Pointsec Mobile Encryption. Checkpoint. URL: http://www.checkpoint.com/products/datasecurity/mobile/index.html
[Ref.- 69]	Guidelines on Cell Phone and PDA Security. SP800-124. NIST. US DoC. URL: http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf
[Ref.- 70]	BlackBerry App World. RIM. URL: http://www.blackberry.com/services/appworld/
[Ref.- 71]	“The Evidence was in your Monthly Cell Phone Bill... Bluetooth?”. Raúl Siles. RaDaJo. URL: http://www.radajo.com/2008/09/evidence-was-in-your-monthly-cell-phone.html
[Ref.- 72]	Mobile Trusted Module (MTM). Trusted Computing Group. URL: http://www.trustedcomputinggroup.org/resources/mobile_phone_work_group_mobile_trusted_module_specification_version_10
[Ref.- 73]	“Unauthorized modification of iPhone OS has been a major source of instability, disruption of services, and other issues”. Apple. 30 de julio de 2009. URL: http://support.apple.com/kb/HT3743
[Ref.- 74]	Cellcrypt. URL: 1. http://www.cellcrypt.com
[Ref.- 75]	Sigillu. URL: http://www.sigillu.com
[Ref.- 76]	“WebOS: Examples of SMS delivered injection flaws”. Intrepidus Group. April, 2010. URL: http://intrepidusgroup.com/insight/2010/04/webos-examples-of-sms-delivered-injection-flaws/ URL: http://intrepidusgroup.com/insight/webos/

Referencia	Título, autor y ubicación
[Ref.- 77]	“XSS and Content Injection in HTC Windows Mobile SMS Preview PopUp”. Michael Mueller. Abril, 2010. URL: http://www.securityfocus.com/archive/1/510897/30/0/threaded
[Ref.- 78]	“iPhone business security framework & iPhone data protection flaw”. Bernd Marienfeldt. Mayo, 2010. URL: http://marienfeldt.wordpress.com/2010/03/22/iphone-business-security-framework/