ANÁLISIS DE VULNERABILIDADES Y SEGURIDAD DE DISPOSITIVOS MÓVILES CON SISTEMA OPERATIVO iOS 6.1.4

JEYSON ANDRÉS GUZMÁN
LEONEL ALBERTO FORERO

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE POSTGRADOS
ESPECIALIZACION EN SEGURIDAD INFORMATICA
BOGOTÁ D.C.
2013

ANÁLISIS DE VULNERABILIDADES Y SEGURIDAD DE DISPOSITIVOS MÓVILES CON SISTEMA OPERATIVO iOS 6.1.4

JEYSON ANDRÉS GUZMÁN
LEONEL ALBERTO FORERO

Proyecto de grado para optar al título de
"Especialista en Seguridad Informática"

Asesor Temático
CÉSAR IVÁN RODRÍGUEZ
Docente

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE POSTGRADOS
ESPECIALIZACION DE SEGURIDAD INFORMATICA
BOGOTÁ D.C.
2013

Nota de Aceptación

_____
_____
_____
_____
_____
_____

_____
Presidente del Jurado

_____
Jurado

_____
Jurado

Bogotá D.C., 2 de Octubre de 2013

Dedicamos este proyecto a nuestras familias y amistades, las cuales no ayudaron con su apoyo incondicional a ampliar nuestros conocimientos y estar más cerca de nuestras metas profesionales. Esto fue posible primero que nadie con la ayuda de Dios, gracias por otorgarnos la sabiduría y la salud para logarlo. Gracias a los intercambios y exposiciones de ideas con nuestros compañeros y amigos de estudios durante el proceso de Especialización. Gracias a nuestros maestros por compartir sus conocimientos y experiencias, particularmente al Ph.D Pedro Díaz y a nuestro asesor Cesar Iván Rodríguez y a todos los demás no mencionados… Dios los Bendiga.

CONTENIDO

LISTA DE FIGURAS

pág.

LISTA DE TABLAS

pág.

LISTA DE ANEXOS

pág.

GLOSARIO

ACL: listas de Control de Acceso, proveen de un nivel adicional de seguridad a los ficheros extendiendo el clásico esquema de permisos[1].

AES: Advanced Encryption Standard (AES), también conocido como **Rijndael** (pronunciado "*Rain Doll*" en inglés), es un esquema de **cifrado por bloques** adoptado como un estándar de cifrado por el gobierno de los Estados Unidos. El AES fue anunciado por el Instituto Nacional de Estándares y Tecnología (NIST) como FIPS PUB 197 de los Estados Unidos (FIPS 197) el 26 de noviembre de 2001 después de un proceso de estandarización que duró 5 años. Se transformó en un estándar efectivo el 26 de mayo de 2002. Desde 2006, el AES es uno de los algoritmos más populares usados en criptografía simétrica[2].

ANDROID: es un sistema operativo de dispositivos móviles. Con Android se puede utilizar todas las aplicaciones de, además de que hay más de 600.000 aplicaciones y juegos disponibles en Google Juega para mantenerte entretenido, junto a millones de canciones y libros, y miles de películas. Dispositivos con Android ya están listo, y sólo se vuelven más inteligentes, con nuevas características que no encontrará en cualquier otra plataforma, lo que le permite centrarse en lo que es importante y que le pone en control de su experiencia móvil[3].

ASIMETRÍA: es aquella que utiliza dos claves diferentes para cada usuario, una para cifrar que se le llama clave pública y otra para descifrar que es la clave privada.

APK: es la extensión de los archivos de instalación para el sistema operativo de Google (Android). Ejemplo: whatsapp.apk.

APPSTORE: es un espacio que permite puede navegar por las aplicaciones de Mac por categorías, como juegos, productividad, música y mucho más. O hacer una búsqueda rápida de algo específico. Lea las descripciones de desarrolladores y críticas de usuarios a través de capturas de pantalla. Cuando usted encuentra una aplicación que te gusta, haz clic para comprarlo. La AppStore tiene aplicaciones para casi todo y todos[4].

---

[1]MICROSOFT. Definiciones y conceptos. [en línea]. Bogotá: [citado 26 junio, 2013]. Disponible en Internet : < URL: http://msdn.microsoft.com/en-us/library/windows/desktop/aa374872(v=vs.85).aspx>

[2]MEZA, Jorge Iván. Definiciones. [en línea]. Bogotá: [citado 23 junio, 2013]. Disponible en Internet : < URL: <http://blog.jorgeivanmeza.com/2010/10/cifrado-y-descifrado-simetrico-con-rijndael-aes-utilizando-cmono/>

[3]DIAZ, J. Sistema Androide. [en línea]. Bogotá: [citado 26 junio, 2013]. Disponible en Internet : < URL: Tomado de: https://sites.google.com/site/androtechrd/ >

[4] APPLE. Que es una AppStore. [en línea]. Bogotá: [citado 26 junio, 2013]. Disponible en Internet : < URL: Tomado de: http://www.apple.com/osx/apps/app-store.html>

BIT: señal electrónica que puede estar encendida (1) o apagada (0). Es la unidad más pequeña de información que utiliza un ordenador[5].

BOOT: proceso inicial de un dispositivo en donde se carga la configuración (BIOS), los dispositivos de hardware y se busca el sistema operativo en la secuencia de arranque[6].

CIFRAR: método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo[7].

CONFIDENCIALIDAD: la confidencialidad es una propiedad de la información mediante la cual se garantizará el acceso a la misma solo por parte de las personas que estén autorizadas[8].

CPU: acrónimo de Central Processing Unit (unidad de proceso central)[9].

CRACKER: este utiliza sus conocimientos para invadir sistemas, descifrar claves y contraseñas de programas y algoritmos de encriptación, ya sea para poder correr juegos sin un CD-ROM, o generar una clave de registro falsa para un determinado programa, robar datos personales, o cometer otros ilícitos informáticos[10].

CRACK: en el caso de seguridad informática es el permanente intento de violación de seguridad de los sistemas informáticos, con fines justificados o no. En el caso de crack de programas la definición es la de creador de cracks, literalmente romper, que son programitas destinados a la desprotección de programas comerciales para que puedan ser usados sin límite[11].

CYDIA: aplicación creada por Jay Freeman (conocido como Saurik en la escena) que sirve como plataforma para abrir la configuración del iPhone o iPod, así como instalar aplicaciones que permiten la descarga de aplicaciones de forma no legítima, exactamente iguales a las que podemos encontrar pagando en la App Store de Apple[12].

---

[5] FORERO, Julio. Que es el BIT. [en línea]. Bogotá: [citado11 julio, 2013]. Disponible en Internet < URL: http://www.masadelante.com/faqs/bit>

[6] ROMERO, Luis. Boot. [en línea]. Bogotá: [citado 26 junio, 2013]. Disponible en Internet : < URL : http://www.alegsa.com.ar/Dic/boot.php>

[7] RONCANCIO, Luis. Crifrado. [en línea]. Bogotá: [citado 11 julio, 2013]. Disponible en Internet < URL: http://www.mitecnologico.com/Main/Cifrado>

[8] DEFINICION ABC. Confidencialidad. [en línea]. Bogotá: [citado17 julio, 2013]. Disponible en Internet < URL:http://www.definicionabc.com/comunicacion/confidencialidad.php>

[9] FORERO., op.cit.p.2.

[10] GOMEZ, Héctor. Cracker. [en línea]. Bogotá: [citado2 agosto, 2013]. Disponible en Internet < URL::http://www.informatica-hoy.com.ar/aprender-informatica/Que-es-un-Cracker.php>

[11] MICROSOFT.,op,cit.,p. 2.

[12] IPHONEOSX. Cydia. [en línea]. Bogotá: [citado11 julio, 2013]. Disponible en Internet < URL: http://iphoneosx.com/cydia/>

DES: (Data Encryption Standard, estándar de cifrado de datos) es un algoritmo desarrollado originalmente por IBM a requerimiento del NBS (National Bureau of Standards, Oficina Nacional de Estandarización, en la actualidad denominado NIST, National Institute of Standards and Technology, Instituto Nacional de Estandarización y Tecnología) de EE.UU[13].

DFU: (Device Firmware Upgrade) Modo de actualización de los dispositivos basados en iOS de Apple Inc.[14].

DISPONIBILIDAD: la disponibilidad de la información está directamente relacionada con la flexibilidad empresarial. Los desastres pueden destruir grandes volúmenes de datos y trabajo y tener efectos devastadores en la disponibilidad del negocio[15].

DRIVE-BY-DOWNLOAD: permite infectar masivamente a los usuarios simplemente ingresando a un sitio web determinado. Mediante esta técnica, los creadores y diseminadores de malware propagan sus creaciones aprovechando las vulnerabilidades existentes en diferentes sitios web e inyectando código dañino entre su código original[16].

EMPAREJAMIENTO: el emparejamiento de dispositivos en Bluetooth se entiende como una relación de confianza. El objetivo es que dos dispositivos Bluetooth se puedan comunicar si están emparejados, si hay una relación de confianza entre los mismos. La primera vez que dos dispositivos intentan comunicarse, tiene lugar el procedimiento denominado emparejamiento que permite crear una clave de enlace común de una forma segura. Este procedimiento requiere que el usuario de cada dispositivo introduzca un código de seguridad Bluetooth (código PIN, Personal Identification Number) de hasta 16 bytes de longitud que debe ser el mismo en los dos casos[17].

ENCRIPCIÓN: es un proceso para convertir la información a un formato más seguro. En otras palabras, los datos que están en un formato claro, o sea entendible, se convierten mediante un proceso matemático a un formato encriptado o codificado, o sea ininteligible. Una vez que llegan a su destino, se decodifican para poder ser legibles de nuevo, se descifran[18].

---

[13] SOTELO, Luis. Los DES. [en línea]. Bogotá: [citado 2 agosto, 2013]. Disponible en Internet < URL: http://www.tierradelazaro.com/public/libros/des.pdf>

[14] FONTALVO; Gilma. Los DFU. [en línea]. Bogotá: [citado 22 julio, 2013]. Disponible en Internet < URL: http://theiphonewiki.com/wiki/DFU_Mode>

[15] MONTOYA, José. Definiciones. [en línea]. Bogotá: [citado11 junio, 2013]. Disponible en Internet < URL: http://www-03.ibm.com/systems/es/information_infrastructure/solutions/information_availability/>

[16] ESET.LA. Drive-By-Download. [en línea]. Bogotá: [citado30 julio, 2013]. Disponible en Internet < URL: http://www.eset-la.com/centro-amenazas/articulo/drive-by-download-infeccion-web/1792>

[17] ARRIETA. Marlen. Emparejamiento. [en línea]. Bogotá: [citado11 agosto, 2013]. Disponible en Internet < URL: http://www.seguridadmobile.com/bluetooth/seguridad-bluetooth/sniffar-emparejamiento-Bluetooth.html>

[18] ENCICLOPEDIA EN LINEA. Encripción. [en línea]. Bogotá: [citado11 julio, 2013]. Disponible en Internet < URL: http://enciclopedia.us.es/index.php/Heur%C3%ADstica>

EXCHANGE: software propietario de colaboración entre usuarios, desarrollado por Microsoft[19].

FDD: (Frecuency Division Duplex) es un multiplexor de frecuencia utilizada en los transceptores radio que utiliza dos canales, uno de bajada y otro de subida con una cierta separación en el espectro para evitar interferencias entre ellos[20].

FIREWALL: elemento de Hardware o Software que funciona como cortafuegos entre redes, permitiendo o denegando las transmisiones de una red a la otra. Un uso típico es situarlo entre una red local y la red Internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial[21].

FRAUDES ELECTRÓNICOS: es una manera de estafar a las personas a través de Internet. Con la finalidad de obtener información confidencial, especialmente de cuentas e instituciones bancarias[22].

FROYO: es una versión de un sistema operativo de Google para dispositivos móviles[23].

GOOGLE PLAY: permite descubrir y comprar aplicaciones y juegos en tu dispositivo Android o en la Web, estés donde estés. Encuentra tu aplicación favorita[24].

GPS: (Sistema de Posicionamiento Global) es un sistema que proporciona una dirección disponible nueva, única e instantánea para cada punto de la superficie del planeta. De origen militar, en la actualidad emite también una señal para usos civiles. Aunque GPS no es una tecnología genérica sino una concreción de los sistemas de posicionamiento mediante radiofrecuencia propiedad del Departamento de Defensa de los EE UU, en la práctica hoy por hoy constituye un nuevo estándar internacional que permite determinar ubicaciones y distancias. Asociado a otras tecnologías, el GPS permite, también, localizar objetos y personas[25].

---

[19]: MIGRACIONES. Exchange. Bogotá: [citado 21 agosto, 2013]. Disponible en Internet < URL: http://www.migraciones.gob.pe/Informacion/INF%20TEC%20SOFTWARE.pdf{En Línea} {Visitado>

[20]: WIKITE. FDD. Bogotá: [citado 12 agosto, 2013]. Disponible en Internet < URL: http://es.wikitel.info/wiki/FDD>

[21]: CASTRO. Julián. Bogotá: [citado 2 julio, 2013]. Disponible en Internet < URL: http://www.desarrolloweb.com/articulos/513.php>

[22] BANCOVIMIENDA. Fraudes informáticos. Bogotá: [citado 28 julio, 2013]. Disponible en Internet < URL: http://www.bancovimenca.com/html/fraude_electronico.html>

[23]DIARIOS EL PAÍS. Froyo. Bogotá: [citado 2 julio, 2013]. Disponible en Internet < URL: :http://tecnologia.elpais.com/tecnologia/2010/05/21/actualidad/1274432462_850215.html>

[24]GOOGLE. Google play. Bogotá: [citado 2 agosto, 2013]. Disponible en Internet < URL: http://play.google.com/intl/es/about/index.html#utm_source=HA_Desktop_CO&utm_medium=GDN&utm_campaign=gplaunch>

[25]: QPS. Que es una GPS. Bogotá: [citado 12 junio, 2013]. Disponible en Internet < URL: http://www.gps.gov/spanish.php >

HANDOVERS: sistema de comunicación móvil para celulares el cual se basa en la transferencia de una estación base a otra cuando la calidad de enlace no es la más óptima[26].

HACKER: toda aquella persona con elevados conocimientos informáticos independientemente de la finalidad con que los use[27].

HOME-BANKING: es un servicio que brindan la gran mayoría de los bancos importantes, públicos y privados, de manera gratuita, a través de sus páginas Web. Es factible su ingreso y operatividad las 24 horas de todos los días, los únicos requisitos son, poseer una cuenta corriente o caja de ahorro y obtener una clave personal. Se pueden realizar casi todas las operaciones que se hacen en los cajeros automáticos, incluso hay más posibilidades[28].

ICMP: controla si un paquete no puede alcanzar su destino, si su vida ha expirado, si el encabezamiento lleva un valor no permitido, si es un paquete de eco o respuesta, etc.[29].

IEEE: corresponde a las siglas de The Institute of Electrical and Electronics Engineers, el Instituto de Ingenieros Eléctricos y Electrónicos, una asociación técnico-profesional mundial dedicada a la estandarización, entre otras cosas. Es la mayor asociación internacional sin fines de lucro formada por profesionales de las nuevas tecnologías, como ingenieros eléctricos, ingenieros en electrónica, ingenieros en sistemas e ingenieros en telecomunicación[30].

IOS: es un sistema operativo desarrollado por Apple originalmente para su teléfono inteligente iPhone, pero lo emplean otros de sus productos como el iPod Touch, iPad y Apple TV. Apple no permite que iOS esté presente en dispositivos de terceras compañías[31].

INGENIERÍA SOCIAL: la ingeniería social consiste en la manipulación de las personas para que voluntariamente realicen actos que normalmente no harían.[32]

---

[26] IETF. Definición de Handovers. Bogotá: [citado 22 junio, 2013]. Disponible en Internet < URL: http://www.ietf.org/rfc/rfc4068.txt>

[27] SOFTWARE LIBRE. Los Hacker. Bogotá: [citado 11 junio, 2013]. Disponible en Internet < URL: http://www.softwarelibrecr.org/faq/hacker>

[28] RINCON, Lisbeth. Home Banking. Bogotá: [citado 1 junio, 2013]. Disponible en Internet < URL: http://www.bcra.gov.ar/pdfs/snp/SNP0165.pdf>

[29] SUAREZ, Hugo. ICPM. : [citado 12 julio, 2013]. Disponible en Internet < URL: http://neo.lcc.uma.es/evirtual/cdd/tutorial/red/icmp.html >

[30] UTPL. IEEE. Bogotá :[citado 12 junio, 2013]. Disponible en Internet < URL: http://www.utpl.edu.ec/ieee/?p=4

[31] APPLE. Que son los IOS.Bogotá: [citado 30 junio, 2013]. Disponible en Internet < URL: http://www.apple.com/es/ios/what-is/>

[32] ACIS. Ingenieria social. Bogotá: [citado 12 junio, 2013]. Disponible en Internet < URL: http://www.acis.org.co/fileadmin/Base_de_Conocimiento/V_Jornada_de_Seguridad/IngenieraSocial_CarlosBiscione.pdf>

INTEGRIDAD: propiedad que garantiza que el contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada, asegurando su precisión y confiabilidad. La integridad de un mensaje se obtiene adjuntándole otro conjunto de datos de comprobación de la integridad: la huella digital[33].

KERNEL: el kernel o núcleo de Linux se puede definir como el corazón de este sistema operativo. Es el encargado de que el software y el hardware del ordenador puedan trabajar juntos[34].

LOGS: un log es un registro de actividad de un sistema, que generalmente se guarda en un fichero de texto, al que se le van añadiendo líneas a medida que se realizan acciones sobre el sistema[35].

MAC: control de acceso al medio, a su vez, cada tarjeta debe tener con que se puede corregir[36].

MALWARE: software que tiene como propósito explícito infiltrarse o dañar a la computadora. La palabra malware proviene del término en inglés malicious software, y en español es conocido con el nombre de software malicioso[37].

METADATA: son datos altamente estructurados que describen información, describen el contenido, la calidad, la condición y otras características de los datos[38].

MDNS: cuando se utiliza mdns, en lugar de encargar la resolución de nombres a un equipo (servidor DNS), esta labor se distribuye y cada equipo se encarga de la resolución de su propio nombre, a través de un mecanismo multicast (mdns)[39].

MICROSD: es un formato para tarjetas de memoria flash derivado del TransFlash de SanDisk. Es especialmente usado en teléfonos móviles, dispositivos GPS portátiles, reproductores de MP3, consolas de videojuegos y unidades de memoria USB[40].

---

[33] ALVAREZ, Josué. Integridad. Bogotá: [citado 1 junio, 2013]. Disponible en Internet < URL: http://neo.lcc.uma.es/evirtual/cdd/tutorial/red/icmp.html>

[34] UTPL. Op.cit.,p. 2.

[35] BECERRA, Luis. Logs. Bogotá: [citado 13 junio, 2013]. Disponible en Internet < URL: http://www.desarrolloweb.com/faq/408.php>

[36] SOFTWARE LIBRE.op.cit.,p. 1

[37] CORREDOR. Malvare. Bogotá: [citado 15 junio, 2013]. Disponible en Internet < URL: http://aprenderinternet.about.com/od/SeguridadPrivacidad/a/Que-Es-Malware.htm>

[38] INEGI. Metadata. Bogotá: [citado 5 junio, 2013]. Disponible en Internet < URL: http://antares.inegi.gob.mx/metadatos/metadat1.htm>

[39] MOLINA, Alberto. MDNS. Bogotá: [citado 12 junio, 2013]. Disponible en Internet < URL: http://albertomolina.wordpress.com/2008/07/07/utilizando-mdns-en-una-red-local/>

[40] ALEQSA.Microsd. Bogotá: [citado 9 junio, 2013]. Disponible en Internet < URL: http://www.alegsa.com.ar/Dic/microsd.php>

MP3: es una abreviación para "MPEG-1 Audio Layer 3", que es un formato de compresión digital de audio; popularmente se le llama mp3 a las canciones mismas o grabaciones que emplean este formato[41].

NIST: instituto Nacional de Estándares y Tecnología de los Estados Unidos.

OS: por sus siglas en inglés (Operation system) es el software encargado de ejercer el control y coordinar el uso del hardware entre diferentes programas de aplicación y los diferentes usuarios. Es un administrador de los recursos de hardware del sistema[42].

PDA: (Personal Digital Assistant o Ayudante personal digital) es un dispositivo de pequeño tamaño que combina un ordenador, teléfono/fax, Internet y conexiones de red[43].

PUTTY: programa gratuito cliente Telnet y SSH, para conectarse a servidores remotos por línea de comandos[44].

RIM: Research In Motion Limited (RIM) NASDAQ: RIM es una compañía canadiense de dispositivos inalámbricos más conocido como el promotor del dispositivo de comunicación de mano BlackBerry[45].

ROOT: en sistemas operativos Linux el usuario root es el "súper usuario" que permite hacer diversas modificaciones en el sistema; cambiar configuraciones, borrar archivos protegidos, etc.[46].

RSA: (Rivest, Shamir, Adelman). Algoritmo de encriptación de clave pública desarrollado por las tres personas mencionadas[47].

SD: la memoria Secure Digital (también conocida como SD o Tarjeta SD) es un tipo de tarjeta de memoria creada por Matsushita Electronic, SanDisk y Toshiba en enero de 2000[48].

---

[41] MISSRESPUESTAS. Mp3. Bogotá: [citado 1 junio, 2013]. Disponible en Internet < URL : http://www.misrespuestas.com/que-es-mp3.html>

[42] EURAM. Os. Bogotá: [citado 12 junio, 2013]. Disponible en Internet < URL http://www.euram.com.ni/pverdes/verdes_informatica/informatica_al_dia/que_es_un_so_144.htm >

[43] CONTRERAS, Fabio. PDA. Bogotá: [citado 8 junio, 2013]. Disponible en Internet < URL : http://www.masadelante.com/faqs/que-es-un-pda>

[44] LUGO, G. Que es un Putty. Bogotá: [citado 22 agosto, 2013]. Disponible en Internet < URL : http://www.desarrolloweb.com/articulos/putty.html>

[45] DIAZ, Gabriel. Los RIM. Bogotá: [citado 5 junio, 2013]. Disponible en Internet < URL : http://www.venio.info/pregunta/que-es-rim-548.html>

[46] DURAN, Diana. Root. Bogotá: [citado 6 agosto, 2013]. Disponible en Internet < URL : http://www.poderpda.com/plataformas/android/android-root/>

[47] ALEQSA. Los RSA. Bogotá: [citado 1 junio, 2013]. Disponible en Internet < URL : http://www.alegsa.com.ar/Dic/rsa.php>

[48] KIOSKEA. Los SD. Bogotá: [citado 17 junio, 2013]. Disponible en Internet < URL : http://es.kioskea.net/contents/pc/sd-secure-digital.php3>

SIMETRÍA: se implementa en la criptografía simétrica y consiste en utilizar la misma clave para cifrar y descifrar[49].

SPAM: es el envío masivo, indiscriminado y no solicitado de publicidad a través de email, aunque actualmente las personas se refieren como spam a publicidad que llega a los celulares por medio de mensajes de texto SMS, por ejemplo[50].

SSH: (o Secure Shell) es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y que permite a los usuarios conectarse a un host remotamente[51].

TETHERING: proceso por el que un dispositivo móvil con conexión a internet actúa como pasarela para brindar acceso inalámbrico a la red a otros dispositivos. Haciendo este de enrutador o módem[52].

TCP/IP: siglas de Protocolo de Control de Transmisión/Protocolo de Internet (en inglés Transmission Control Protocol/Internet Protocol), un sistema de protocolos que hacen posibles servicios Telnet, FTP, E-mail, y otros entre ordenadores que no pertenecen a la misma red[53].

TDD: duplexación por división de frecuencia (FDD – Frequency Division Duplexing)[54].

VULNERABILIDAD: hace referencia a una debilidad en un sistema permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones[55].

WIRELESS: (inalámbrico o sin cables) es un término usado para describir las telecomunicaciones en las cuales las ondas electromagnéticas (en lugar de utilizar cables) llevan la señal sobre parte o toda la trayectoria de la comunicación[56].

---

[49] DURAN, Camilo. Simetría. Bogotá: [citado 1 junio, 2013]. Disponible en Internet < URL : http://www.virusprot.com/art1.html>

[50] FIGUEREDO. Hugo. Glosario. Bogotá: [citado 20 junio, 2013]. Disponible en Internet < URL : http://www.internetglosario.com/560/Spam.html>

[51] GARCIA, Josefina. SSH. Bogotá: [citado 16 agosto, 2013]. Disponible en Internet < URL : http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/ch-ssh.html>

[52] HIGUERA, Fanny. Tethering. Bogotá: [citado 1 junio, 2013]. Disponible en Internet < URL : http://www.idamovil.com/que-es-tethering-como-compartir-tu-conexion-de-internet-del-iphone/ >

[53] FIGUEREDO.,op.cit.,p.1

[54] HUGHES. Los TDD. Bogotá: [citado 17 julio, 2013]. Disponible en Internet < URL : http://www.hughes.com/HNS%20Library%20For%20Products%20%20Technology/Administracion_Airlink.pdf>

[55] ALEGSA. Vulnerabilidad. Bogotá: [citado 13 agosto, 2013]. Disponible en Internet < URL : http://www.alegsa.com.ar/Dic/vulnerabilidad.php>

[56] JIMENEZ. Gabriel. Wireless. Bogotá: [citado 17 junio, 2013]. Disponible en Internet < URL : http://www.masadelante.com/faqs/wireless>

WIFI: hace referencia a una de las tecnologías de comunicación inalámbrica mediante ondas más utilizada hoy en día. WIFI, también llamada WLAN (wireless LAN, red inalámbrica) o estándar IEEE 802.11.[57]

WRAPPER: el elemento Wrapper (Wrapper en inglés es Envoltura) permite mostrar cualquier sitio web, dentro de un sitio[58].

ZEROCONF: es una configuración de red que permite asignar una dirección IP en una red de forma automática. También conocido como APIPA[59].

[57] LOPEZ, Gregorio. Wifi. Bogotá: [citado 1 junio, 2013]. Disponible en Internet < URL : http://www.aulaclic.es/articulos/wifi.html>

[58] LUGO. Julio. Los wraper. Bogotá: [citado 1 junio, 2013]. Disponible en Internet < URL : http://joomla.org.ar/tutoriales/uso-de-wrapper-contenido-externo.html >

[59] MORENO, Gisell. Zeroconf. Bogotá: [citado 1 junio, 2013]. Disponible en Internet < URL : http://computer.yourdictionary.com/zeroconf>

RESUMEN

Es evidente el uso frecuente de los Smartphone en la actualidad, se pueden observar en distintas partes como centros comerciales, oficinas, reuniones e instituciones educativas entre otros; utilizados por usuarios de diversas edades, la seguridad de la información juega un factor importante a nivel personal y corporativo, es por esto que mediante lineamientos establecidos por la norma NIST 800-155 (Technical Guide to Information Security Testing and Assessment) desarrollada por el Instituto Nacional de Estándares y Tecnología de los Estados Unidos. Se evidencian una serie de pruebas de vulnerabilidades como test de penetración y análisis que permiten desarrollar una guía de buenas prácticas que se enfocan en la mitigación de las mismas, y a su vez, cumple con los pilares fundamentales en la seguridad de la información como lo es la disponibilidad, integridad y confidencialidad en los Smartphone.

Es preciso conocer las vulnerabilidades en sistemas operativos iOS de Apple para concientizar, educar e informar a los usuarios de estos dispositivos sobre el riesgo latente que existe si no se toman medidas de prevención sobre dichos dispositivos. Medidas que pueden ser implementadas en equipos de tipo corporativos y personales. La guía de mejores prácticas es un aporte para la mitigación de vulnerabilidades de seguridad enfocadas en la protección de la información y del dispositivo móvil como tal. Mediante el uso de herramientas como firewall, antivirus y el cambio de la configuración por defecto del dispositivo, entre otras.

Para llegar a estos aportes es necesario realizar un levantamiento de información previo, mediante la revisión técnica de cada uno de los dos dispositivos utilizados, esto permite evaluar los tipos de conexiones a implementar, cuál es su infraestructura a nivel de redes o protocolos de comunicación y de sistema operativo.

En el desarrollo de este proyecto se analizaron factores de riesgo como: la suplantación de identidad, malware, ingeniería social, fraudes y pérdida o robo del dispositivo. No obstante, se describen algunos procedimientos que permiten ejercer control total sobre el dispositivo móvil, procesos como el Jailbreak sobre iOS, mediante el cual se obtiene acceso total al sistema operativo, en medio de este análisis se informa al usuario las ventajas y desventajas en las que se incurre al realizar este tipo de prácticas.

INTRODUCCIÓN

Los días en que los Smartphone sólo se veían en manos de ejecutivos son parte de la historia, las funciones que ofrecen los sistemas operativos de estos dispositivos y la gran cantidad de aplicaciones disponibles para ellos, hacen que sea cada vez más fácil encontrar personas con su Smartphone en centros comerciales, la calle y en el transporte público.

La protección de la información enfocada a este tipo de dispositivos abre un campo de investigación que tiene incidencia a nivel mundial, es por ello que se genera la necesidad de analizar y determinar cuáles son los puntos más vulnerables y posiblemente aquellos por medio de los cuales será posible acceder y violentar la privacidad del propietario, con el fin de realizar un análisis de vulnerabilidades que permita encontrar las mejores prácticas para la protección de la información en dichos dispositivos, ya que al conocer de primera mano cuales son las falencias y debilidades de los dispositivos será posible establecer medidas para prevenir la pérdida compromiso de información.

El análisis de vulnerabilidades permite tener una visión más precisa acerca de las características y comportamientos del sistema operativo de Apple, aplicando técnicas que evidencian la protección a la integridad, disponibilidad y confidencialidad de la información en estos prácticos dispositivos.

1. PLANTEAMIENTO DEL PROBLEMA

1.1 DESCRIPCIÓN DEL PROBLEMA

El factor común de los Smartphone es la posibilidad que ofrecen de expandir sus funcionalidad es por medio de la gran cantidad de aplicaciones que hay disponibles para ellos en las tiendas online, además de las posibilidades adicionales como la realización de transacciones online, consultas bancarias, compras y pagos móviles entre otras. Adicionalmente, estos dispositivos permiten a los usuarios llevar consigo gran cantidad de datos e información (que en su mayor parte es de carácter confidencial). Al parecer el crecimiento de la demanda de estos dispositivos se seguirá presentado, tal como la muestra la encuesta realizada por la compañía Ericsson[60] ejecutada el año pasado; en la cual se indaga ¿Cuál dispositivo va a comprar?, generando un resultado muy favorable para los Smartphone.

De acuerdo a los estudios de la compañía Symantec, publicados a través de su página symantec.com, realizados a finales de 2012, los Smartphone ya no solo se utilizan para telefonía como tal,

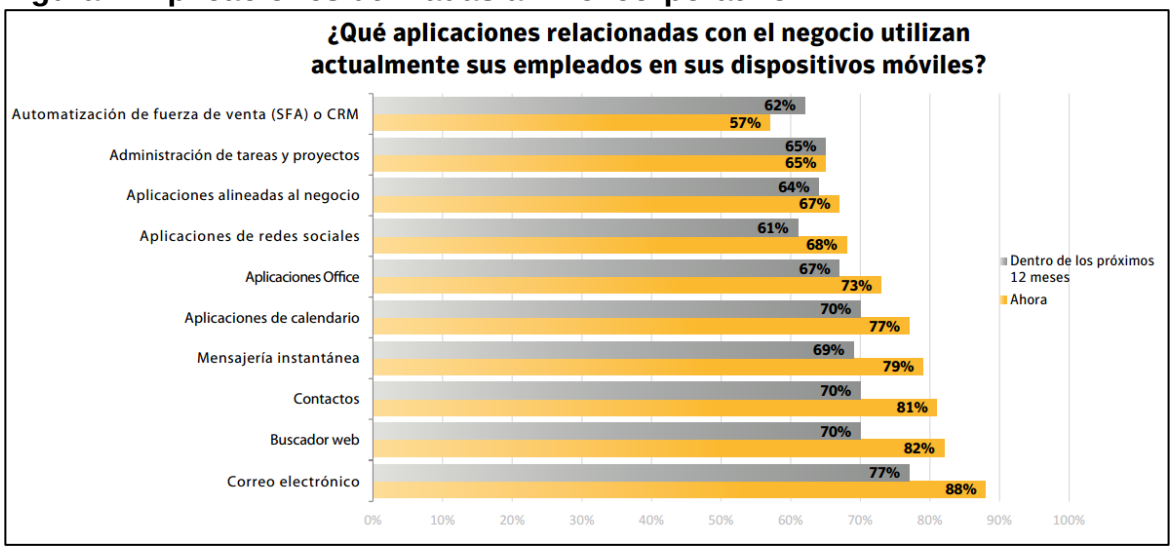
> Para entender por qué las organizaciones están adoptando el cómputo móvil, se preguntó cuáles son los beneficios de negocio más importantes y entre lo que mencionaron se encuentran: aumentar la eficiencia, la agilidad del negocio y las ventas. En conjunto, todos estos elementos beneficiarían a mejorar la rapidez del negocio.[61]

Sin dejar de lado la realización de transacciones online, como consultas bancarias, compras y pagos móviles entre otras.

[60] REVISTA ITNOW. Compañía Ericson. Bogotá: [citado 1 junio, 2013]. Disponible en Internet < URL :http://revistaitnow.com/noticias-itu/on-los-datos-moviles-el-futuro-negocio-de-las-telecomunicaciones-2/>

[61] SYMANTEC . Los Smartphone. Bogotá: [citado 1 junio, 2013]. Disponible en Internet <http://www.symantec.com/content/es/mx/enterprise/images/theme/mobility/America-Latina-2012-State-of-Mobility-Survey-Report-SPA.pdf>

Figura 1. Aplicaciones utilizadas a nivel corporativo



Fuente. SYMANTEC. Aplicaciones. Bogotá: [citado 11 junio, 2013]. Disponible en Internet < URL :http://www.symantec.com/content/es/mx/enterprise/images/theme/mobility/America-Latina-2012-State-of-Mobility-Survey-Report-SPA.pdf>

El hecho de almacenar información que puede ser de vital importancia como contactos, clientes, proveedores, fotografías o mensajes de texto, así como información de alta confidencialidad como contraseñas de bancos, correos electrónicos corporativos o simplemente notas con información personal; hace que estos dispositivos sean un blanco muy atractivo para los atacantes ya que la información anteriormente mencionada está centralizada en un solo dispositivo, un atacante que logre infectar el mismo y acceder a él, puede conocer la vida privada del usuario y utilizar sus datos personales; en el peor de los casos, información financiera y confidencial para espionaje empresarial, fraudes electrónicos, extorsión, entre otros.

1.2 FORMULACIÓN DEL PROBLEMA

A través del desarrollo de un estudio de carácter investigativo/deductivo ¿qué vulnerabilidades que comprometan la seguridad de la información se pueden identificar y demostrar en un documento que contenga las mejores prácticas y recomendaciones para mitigar algunas de ellas en los dispositivos móviles con iOS 6.1.4?

2. JUSTIFICACIÓN

Teniendo en cuenta la falta de conocimiento en términos de seguridad que poseen los usuarios de dichos dispositivos; este campo ha sido vagamente explotado pues apenas comienzan a mostrarse algunos estándares en pro de mejorar los aspectos de protección de la información, modelos y métodos que buscan garantizar la protección de la información, claro está que estos son realizados por grandes compañías de Norteamérica y Europa sin tener en cuenta su acogida en el mercado latinoamericano y particularmente el mercado colombiano (según noticia emitida por eltiempo.com)[62]; de allí la necesidad de elaborar un estudio de carácter investigativo para el territorio colombiano que permita:

- Evidenciar las vulnerabilidades (en cuanto a seguridad de la información concierne), que se presentan en los Smartphone, (si es posible conocer las debilidades, también es posible mitigarlas).

- Establecer el nivel de impacto que pueden proporcionar las vulnerabilidades encontradas frente a la información que estos dispositivos son capaces de almacenar. Ya que actualmente es más frecuente el uso de este sistema operativo y se hace necesaria la identificación de factores en seguridad informática que se pueden ver comprometidos si no se realizan las configuraciones de seguridad pertinentes.

- Elaborar un documento que integre las mejores prácticas para el uso seguro de los Smartphone. Dicho documento es un aporte para los usuarios del sistema operativo iOS 6.1.4 de Apple, en el cual se puede encontrar información detallada para contribuir al aseguramiento de la información en dichos dispositivos.

[62] DIARIO EL TIEMPO. Protección de la Información. Bogotá: [citado 11 junio, 2013]. Disponible en Internet < http://m.eltiempo.com/tecnologia/telecomunicaciones/smartphones-en-colombia/10117907>

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Realizar un análisis de vulnerabilidades a nivel del sistema operativo en los dispositivos móviles con iOS 6.1.4 que permita la generación de un documento que contenga las mejores prácticas y recomendaciones para salvaguardar la información dentro de este tipo de dispositivos.

3.2 OBJETIVOS ESPECÍFICOS

- Revisar la documentación existente sobre las vulnerabilidades a nivel de sistema operativo en los dispositivos móviles Apple con iOS 6.1.4.

- Describir los riesgos a los que se encuentran expuestos los dispositivos móviles Apple con iOS 6.1.4 a nivel de sistema operativo.

- Realizar un análisis de vulnerabilidades a los que se encuentran expuestos los dispositivos móviles Apple con iOS 6.1.4 a nivel de sistema operativo.

4. MARCO REFERENCIAL

4.1 MARCO TEÓRICO

4.1.1 Seguridad Informática. Se refiere a la protección de la información y de sistemas de información de acceso no autorizado, divulgación, alteración, modificación o destrucción para proporcionar confidencialidad integridad y disponibilidad.[63]

Según comenta el libro Seguridad de la Información Redes, Informática y: Sistemas de Información, del Ing. Javier Areitio Bertolín[64] la seguridad de la información es el proceso en el que se da cabida a un creciente número de elementos, entre ellos aspectos tecnológicos, de gestión y organizacionales, recursos humanos, económicos, de negocios de tipo legal y de cumplimento, citando algunos, abarcando no solo aspectos informáticos y de telecomunicaciones sino también aspectos físicos, medioambientales, humanos entre otros.

En un sentido más amplio, según el libro Seguridad Informática Ethical Hacking de la ACISS (Asociación de Auditores, Consultores en la Instalación y Aseguramiento de Sistemas de Información)[65] ; la seguridad informática representa un conjunto de medios y técnicas implementadas para asegurar la integridad y que no se difundan involuntariamente los datos que recorren un Sistema de Información, entendiendo como tal un conjunto de datos y de recursos (físicos, lógicos y humanos) que permiten almacenar y circular la información que contiene.

Ya sea a nivel de empresa, de multinacional, de un usuario privado o incluso de un país, la seguridad de un sistema adquiere importancia directamente proporcional al valor de los datos que contiene.

4.1.2 Confidencialidad. Se refiere a la propiedad de la información que garantiza que está sea accesible únicamente por personal autorizado a acceder a dicha información. Según la Organización Internacional de Estandarización (ISO) en la

[63] CORDERO, Luis. Seguridad informática. Bogotá: [citado 11 junio, 2013]. Disponible en Internet < URL : http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf>
[64] BERTOLINI, Javier. Seguridad de la información redes informática y sistemas de información. Bogotá: Mc Grw Hill, 2001.p. 15.
[65] ACISSI. Seguridad Informática Ethical Hacking, Conocer el ataque para una mejor defensa. Bogotá: Mc Grw Hill, 2008.p. 17.

norma ISO/IEC 13335-1:2004: característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados[66].

En el ámbito de la seguridad informática, se refiere a la protección de datos y de información intercambiada entre un emisor y uno o más destinatarios frente a terceros. En un sistema que garantice la confidencialidad, un tercero que entra en posesión de la información intercambiada entre el remitente y el destinatario no es capaz de extraer cualquier contenido inteligible.

4.1.3 Disponibilidad. Es la característica, cualidad o condición de la información de estar a disposición de quienes tienen el privilegio de acceder a ella, sean personas, procesos o aplicaciones. En general, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que lo requieran; garantizar dicha disponibilidad implica también la prevención de ataques de denegación de servicio (DoS). Para poder manejar con mayor facilidad la seguridad de la información, las empresas o negocios se pueden ayudar con un sistema de gestión permita conocer, administrar y minimizar los posibles riesgos que atenten contra la seguridad informativa del negocio.

Según {ISO/IEC 13335-1:2004}: característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada[67].

4.1.4 Integridad. Se entiende por integridad el servicio de seguridad que garantiza que la información es modificada, incluyendo su creación y borrado, sólo por el personal autorizado. Suelen integrarse varios conceptos análogos en este segundo aspecto de la seguridad: precisión, integridad y autenticidad.

El concepto de integridad significa que el sistema no debe modificar o corromper la información que almacene, o permitir que alguien no autorizado lo haga. Esta propiedad permite asegurar que no se ha falseado la información. Por ejemplo, que los datos recibidos o recuperados son exactamente los que fueron enviados o almacenados, sin que se haya producido ninguna modificación, adición o borrado"[68].

Según {ISO/IEC 13335-1:2004}: el hecho de mantener la exactitud y lógica de la información y sus métodos de proceso propiedad/característica de salvaguardar la exactitud y completitud de los activos[69].

---

[66] MMOSQUERA, Henry. Confidencialidad. Bogotá: [citado 11 junio, 2013]. Disponible en Internet < URL : http://www.iso27000.es/glosario.html#section10c>

[67] MORA, Rogelio. Disponibilidad. Bogotá: [citado 1 agosto, 2013]. Disponible en Internet < URL :http://www.iso27000.es/glosario.html#section10c>

[68] SANCHEZ, José. Ingeniería de Proyectos Informáticos: Actividades y Procedimientos. México: Paidos, 2000.p. 170.

[69] MORA.,op.cit.,p. 2.

4.1.5 Dispositivos móviles. Se puede definir como un dispositivo de tamaño reducido (portable), con ciertas capacidades de procesamiento y almacenamiento de información, conexión permanente o intermitente a una red, que ha sido diseñado específicamente para una función, pero que adicionalmente puede llevar a cabo otras funciones. De acuerdo con esta definición existen multitud de dispositivos móviles, desde los reproductores de audio portátiles hasta los navegadores GPS, pasando por los teléfonos móviles, los PDA o los Tablet PC[70].

Teniendo en cuenta el variado número de niveles de funcionalidad asociado con dispositivos móviles, fue necesario hacer una clasificación de los mismos, por ello en el 2005, T38 y DuPont Global Mobility Innovation Team propusieron los siguientes estándares para la definición de dispositivos móviles.

Dispositivo Móvil de Datos Limitados (Limited Data Mobile Device): teléfonos móviles clásicos. Se caracterizan por tener una pantalla pequeña de tipo texto. Ofrecen servicios de datos generalmente limitados a SMS y acceso WAP.

Dispositivo Móvil de Datos Básicos (Basic Data Mobile Device): se caracterizan por tener una pantalla de mediano tamaño, menú o navegación basada en iconos, y ofrecer acceso a emails, lista de direcciones, SMS, y, en algunos casos, un navegador web básico. Un típico ejemplo de este tipo de dispositivos son los teléfonos inteligentes (Smartphone).

Dispositivo Móvil de Datos Mejorados (Enhanced Data Mobile Device): se caracterizan por tener pantallas de medianas a grandes (por encima de los 240 x 120 pixeles), navegación de tipo stylus, y que ofrecen las mismas características que el "Dispositivo Móvil de Datos Básicos" (Basic Data Mobile Devices) más aplicaciones nativas como aplicaciones de Microsoft Office Mobile (Word, Excel, PowerPoint) y aplicaciones corporativas usuales, en versión móvil, como SAP, portales intranet, etc. Este tipo de dispositivos incluyen los S.O. como Windows Mobile[71].

4.1.6 Criptografía. La criptografía (del griego κρύπτω krypto, «oculto», y γράφως graphos, «escribir», literalmente «escritura oculta») es la técnica, bien sea aplicada al arte o la ciencia, que altera las representaciones lingüísticas de un mensaje para proteger su contenido; en esencia la criptografía trata de enmascarar las representaciones caligráficas de una lengua, de forma discreta[72].

[70] KOSKEA. Dispositivos móviles. Bogotá: [citado 1 agosto, 2013]. Disponible en Internet < URL :http://es.kioskea.net/contents/389-ordenador-portatil>
[71] Ibid.,p. 2.
[72] ROJAS, MANUEL Criptografía. Bogotá: [citado 12 agosto, 2013]. Disponible en Internet < URL :http://bvs.sld.cu/revistas/aci/vol11_6_03/aci11603.htm>

Aunque no existe un tipo de diseño estándar, tal vez, el más popular es el de Fiestel, que realiza un número finito de interacciones de una manera particular, hasta que finalmente el mensaje es cifrado. Este es el caso del sistema criptográfico simétrico más conocido: DES (Data Encryption Standard); La criptografía de clave pública o asimétrica, también denominada RSA por las siglas de los apellidos de sus inventores Rivest, Shamir y Adelman, es por definición aquella que utiliza dos claves diferentes para cada usuario, una para cifrar que se llama clave pública y otra para descifrar que es la clave privada. El nacimiento de la criptografía asimétrica ocurrió como resultado de la búsqueda de un modo más práctico de intercambiar las llaves simétricas[73.]

4.1.7 Redes 3G. Se conoce con este nombre a la tercera generación de redes de comunicación móvil (para transmisión de voz, datos y video a través de teléfonos móviles), basada en el estándar UMTS (por sus siglas en ingles Universal Mobile Telecommunications System), su tecnología es una evolución de las redes 2G y representan un aumento en la velocidad de transmisión de información y aumento en la prestación de servicios, algunas de las características de estas redes de datos son:

- Velocidad de bit mayor a 2 Mbps, Velocidad variable de bit
- Múltiples servicios con diferentes requerimientos de calidad en una sola conexión.
- Coexistencia de sistemas de segunda y tercera generación y entre sistemas de handovers para aumentar cobertura y balanceo de carga
- Soporte asimétrico de tráfico en el Up link y Down link
- Alta eficiencia espectral
- Coexistencia del modo FDD y TDD

4.2 MARCO HISTÓRICO

4.2.1 Análisis Forense en Dispositivos Móviles con Symbian OS[74]

Autor: C. Agualimpia y R. Hernández.

[73] Ibid.,p. 4.
[74]ARTEMISA. Análisis forense en dispositivos móviles. Bogotá: [citado 12 agosto, 2013]. Disponible en Internet < URL :http://artemisa.unicauca.edu.co/~rhernandez/articulos/Articulo_UPM-Criptored_Symbian_OS_Forensics_UJaveriana.pdf>

Resumen. Este estudio realizado en el 2010, describe algunos métodos de análisis forenses aplicados a dispositivos móviles. Adicionalmente se plantean diferentes alternativas de análisis en dispositivos móviles con el objetivo de evaluar el alcance que se puede tener con algunos de los software forenses más comunes del mercado. Finalmente se concluye con una lista de características deseables en programas forenses para el Sistema Operativo Symbian.

Conclusiones. Se menciona la dificultad que implica el análisis forense a un dispositivo móvil, dadas las grandes diferencias que existen entre dispositivos de diferentes fabricantes así como las numerosas diferencias entre modelos del mismo fabricante. El análisis en dispositivos móviles aparece como una necesidad latente a nivel de las investigaciones actuales en cualquier país del mundo, por esta razón no se deben descuidar los avances y la integración desde el punto de vista científico y tecnológico en este tipo de herramientas; se deben generar convenios a nivel de investigación que involucren a la academia y los entes de policía judicial.

4.2.2 Modelo para medir la madurez de un Smartphone

A Model to Measure the Maturity of Smartphone Security at Software Consultancies[75]

Autor: Mr. Sean Allam

Resumen. Este proyecto de investigación realizado en diciembre de 2009, profundiza en los riesgos introducidos por los teléfonos inteligentes, y a través de estudios de casos múltiples.

El modelo se basa en las recomendaciones de dos marcos principales de seguridad de información, el marco COBIT 4.1 (buenas prácticas para el control de la información) e ISO27002 (estándar para la seguridad de la información). En última instancia, una combinación de riesgos específicos para Smartphone que están integrados con las recomendaciones clave de control, en la prestación de un conjunto de componentes para medir la seguridad.

Conclusiones. Los resultados fueron analizados en conjunto, y luego por separado según los estándares definidos; ya que el usuario es responsable de la seguridad en su dispositivo. Curiosamente parece que hay muy poca percepción de los requisitos de seguridad El resultado de este estudio arrojo que los empleados que son responsables de la seguridad no se preocupan por aplicar estándares que reduzcan las debilidades de seguridad de los teléfonos inteligentes.

[75] SALAZAR. Diana. Modelo para medir madurez. Bogotá: [citado 2 agosto, 2013]. Disponible en Internet < URL :http://ufh.netd.ac.za/jspui/bitstream/10353/281/1/SA%20%28200481118%29%20Dissertation.pdf >

4.2.3 Avances de análisis forenses en Android

Advancements in Android Forensics[76]

Autor: via forensics company

Resumen. Este estudio realizado en el 2011 describe algunos métodos de análisis forenses incluyendo técnicas, arquitectura y comunicación, las contraseñas y sus vulnerabilidades, adquisición física y lógica.
Conclusiones. Se identifican los requerimientos básicos para lograr tener acceso total a un dispositivo móvil. Los requerimientos son: un dispositivo con acceso al Root (usuarios con privilegios para acceder a toda la información y configuración de un sistema) o Shell, depuración USB y en algunos casos el dispositivo no debe ser iniciado en modo normal.

4.2.4 Los ataques móviles están cerca de duplicarse[77]

Autor. IBM Corporation.

Resumen. El informe del 2011 fue elaborado por el equipo de IBM, que viene haciendo este trabajo desde 1997. Sus especialistas analizan más de 50.000 informes de vulnerabilidades, con el objetivo de alertar a empresas sobre los posibles problemas de seguridad.

Conclusiones. Los ataques informáticos a móviles siguen creciendo. Según IBM en su informe X-Force de tendencias y riesgos de mitad de 2011 adicionalmente se indica que su volumen ha crecido y está muy cerca el momento en el que los ataques móviles se dupliquen frente al año anterior.

4.2.5 Pruebas de penetración de Smartphone basados en Android.

Penetration Testing of Android-based Smartphones[78]

Autor. Naresh Kumar (Universidad de Gothenburg)

Resumen. El informe entregado en junio de 2011 evidencia un análisis de seguridad de Android basado en Smartphone. El uso de teléfonos inteligentes está aumentando día tras día con una variedad de aplicaciones. Estas aplicaciones pueden ser muy críticas usualmente como la banca móvil y los sistemas de pago

[76] VIAFORENSICS. Advancements in Android Forensics. Bogotá: [citado 2 agosto, 2013]. Disponible en Internet < URL : http://viaforensics.com/services/mobile-forensics/android-forensics/ >
[77] REVISTA ENTER. Los ataques móviles. Bogotá: [citado 12 agosto, 2013]. Disponible en Internet < URL : http://www.enter.co/seguridad-y-privacidad/los-ataques-moviles-estan-cerca-de- duplicarse-ibm/ >
[78] GUPEA. Penetration Testing of Android-based Smartphones. Bogotá: [citado 12 agosto, 2013]. Disponible en Internet < URL : http://gupea.ub.gu.se/bitstream/2077/27864/1/gupea_2077_27864_1.pdf/

móvil y los usuarios son a menudo inconscientes de los riesgos de seguridad involucrados en tales aplicaciones.

Conclusiones. Se realizó un análisis de vulnerabilidades en tres diferentes versiones de Android. Al hacer esto, fue posible reunir información sobre el Smartphone, tales como si está activo o no, y ver el estado de los diferentes puertos y los servicios que se ejecutan en él. También se evidencio que es posible visualizar los log del OS a través de la red identificando que un atacante puede determinar la versión del sistema operativo mediante estos, que a su vez se puede usar para encontrar fallas de seguridad en el dispositivo conectado.

4.2.6 Examinar la seguridad de los enfoques empleados. Examining the security approaches employed in Apple's iOS and Google's Android[79]
Autor. Symantec

Resumen. El informe presentado durante el 2011 evidencia el incremento en el uso de estos dispositivos, pero también ha expuesto a la empresa a nuevos riesgos de seguridad. Las últimas plataformas móviles fueron diseñadas pensando en la seguridad de los equipos.

Conclusiones. Los dispositivos móviles no prometen solo mejorar considerablemente la productividad, sino que también introducen una serie de nuevos riesgos que deben ser gestionados por las empresas. Se espera que al explicar los modelos de seguridad que subyacen en cada plataforma y los ecosistemas de estos dispositivos, le proporcionemos, al lector, un conocimiento de manera más eficaz para obtener el verdadero valor de estos dispositivos, así como gestionar con más eficacia el riesgo que estos introducen.

4.3 MARCO CONCEPTUAL

4.3.1 Seguridad Digital. Uno de los primeros, delitos informáticos podemos encontrarlo en el que puede ser el cargo más importante del mundo. El ex presidente de EE UU, Ronald Reagan, filtró deliberadamente tecnología defectuosa a la URSS para sabotear sus industrias clave. El código, oculto en el programa, estropeaba el mecanismo que ponía en funcionamiento las bombas, turbinas y válvulas y sometía a los oleoductos a una presión por encima de la que los materiales podían soportar. El efecto fue espectacular. El virus provocó, ante el asombro de los soviéticos, la explosión de un oleoducto siberiano en 1982, el estallido no nuclear más enorme de la historia. El fuego se vio incluso desde los

[79] SYMATEC. Seguridad digital. Bogotá: [citado 12 agosto, 2013]. Disponible en Internet < URL : http://www.symantec.com/content/en/us/about/media/pdfs/symc_mobile_device_security_june2011.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011Jun_worldwide_mobilesecuritywp>

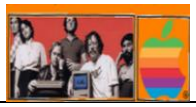
satélites espías de EE UU y la avería, y subsiguiente falta de suministro, afectó seriamente a la economía de la Unión Soviética[80]

Durante la Segunda Guerra Mundial se crean la mayoría de los servicios de inteligencia del mundo con el fin de obtener información valiosa e influyente, creándose grandes redes de espionaje. Como forma de protección surge la contrainteligencia. Con el devenir de los años al incrementarse el alcance de la tecnología, el cuidado de la información se ha vuelto crucial para los hombres, las organizaciones y las sociedades[81].

[80] ROMERO, Giovanni. Historia de la Seguridad digital. Bogotá: [citado 12 agosto, 2013]. Disponible en Internet < URL : http://www.seguridaddigital.info/index.php?option=com_content&task=view&id=23&Itemid=26>
[81] Ibid.,p. 2.

4.3.2 Historia de los Smartphone

Tabla 1 Evolución histórica de los Smartphone[82]

1946 	Primera llamada desde un teléfono móvil que pesaba 36 kilos instalado en el guarda equipaje de un auto con red de AT&T.
1976 	Apple es fundado; Steve Wozniak, Steve Jobs y Ronald Wayne son los propietarios.
1980 	David Potter inicia con los primeros pasos de Symbian.
1984 	RIM es fundado por Mike Lazaridis.
1986	La comisión Europea propone reservar el espectro de los 900 MHz para la red GSM.
1992 	Es presentado el primer dispositivo que se podría llamar Smartphone, (IBM) Simón.
1992 	Palm inc. Es fundada y en un año lanza su primer PDA zoomer.
1993 	Lanzamiento del primer newton de Apple, corriendo newton OS.
1996 	Nokia lanza el Nokia 9000 Communicator (pesaba casi medio kilo) con sistema operativo GEOS (Conocido como zapatófono).
1996 	Lanzamiento de la primera PalmOS.
1996 	Steve Jobs vuelve a Apple después de no tener éxito con NEXT.

[82] ANDROID. Evolución histórica de los Smartphone. Bogotá: [citado 12 agosto, 2013]. Disponible en Internet < URL : http://www.android.es/historia-del-smartphone.html#axzz1dGLIi1ec>

Cuadro 1 (*Continua)*

1997 	Primera vez que se utiliza la palabra Smartphone cuando Ericsson lanzó el prototipo GS88 que nunca se vendió al público.
1998 	Google Inc. es fundada por Sergey Brin y Larry Page.
1999 	Lanzamiento de la primer Blackberry (850) con correo y navegador web.
2000 	Lanzamiento de la primera ipaq (H3100) con sistema PocketPC 2000.
2001 QUALCOMM	Qualcomm monta BREW (Binary Runtime Environment for Wireless), lo más parecido a un Framework más un market, preparado para hacer aplicaciones.
2001 	Primera versión de Symbian instalado en un Nokia 9210.
2001 NTT DoCoMo	Lanzamiento de la primera red 3 G en Japón por NTT DoCoMo.
2003 android	Se crea la compañía de software Android Inc. Por Andy Rubin y Rich Miner, Nick Sears y Chris White.

Cuadro 1 (*Continua)*

2005	**Google compra Android Inc.**
2005 	Apple se asocia con Motorola para desarrollar ROKR, un móvil integro con iTunes.
2005	Apple anuncia que empieza el desarrollo del iPhone ya que no iban muy bien con el ROKR.
2007 	Apple lanza el primer iPhone 2G.
2007 	Google libera la primera versión de Android para desarrolladores.
2007 	Se funda la Open Handset Alliance.
2008 	Nace el primer blog sobre Android.
2008 	Lanzamiento del Android devphone 1, el primer móvil con Google Android fabricado por HTC.
2008 	Apple lanza el iPhone 3G.
2009 	Vodafone anuncia el primer HTC magic en el MWC de Barcelona, y más tarde hacia final de año Motorola anuncia el Droid.
2009	La AppStore de Apple llega a los mil millones de descargas.
2009	Apple lanza el iPhone 3GS
2009	La AppStore alcanza las 100.000 aplicaciones.
2009 	Palm anuncia web OS la evolución de palmos
2009 	Geeksphone anuncia el Geeksphone en el Android.es meetup, el primer móvil con Android fabricado por una empresa española.

Cuadro 1 (*Continua)*

2009	**El Android Market alcanza las 100.000 aplicaciones.**
2009	Más de 100 teléfonos diferentes con Android en el mercado.
2010 	Google anuncia el Nexusone con Android 2.1 y fabricado por HTC. El primer dispositivo que pudo compararse con un iPhone.
2010 	Apple lanza el iPhone 4
2010 	Google anuncia el Nexus S, fabricado por Samsung.
2011	Cada día se activan 500.000 móviles Android.
2011	Apple integra la aplicación Siri en el iPhone
2012 	Android anuncia el lanzamiento de la versión Jelly Bean
2012 	Apple anuncia el lanzamiento del iPhone 5
2013  	Se producen los dos lanzamientos esperados de dos de los fabricantes más grandes del mercado (Apple y Samsung) adicional Apple anuncia la actualización de sistema operativo con iOS 7 realizando cambios importantes a nivel gráfico y de rendimiento.

Fuente. ANDROID. Evolución histórica de los Smartphone. Bogotá: [citado 12 agosto, 2013]. Disponible en Internet < URL : http://www.android.es/historia-del-smartphone.html#axzz1dGLIi1ec>

4.4 MARCO TECNOLÓGICO

Durante la investigación se tendrán en cuenta las siguientes normativas que aplican para Colombia, orientadas al tema de acceso a la información:

Ley 527 de 1999 y Ley 1273 de 2009 afectan de forma directa el análisis de vulnerabilidades en dispositivos móviles, en la medida que se manipule información del fabricante o del usuario como tal, la Ley 527 de 1999 (agosto 18 de 1999) reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y las firmas digitales. Adicionalmente cuenta con otras disposiciones que enmarcan cada uno de los permisos que se deben solicitar para manipulación de mensajes de datos en los capítulos I y II de dicha Ley.

No obstante, se debe tener en cuenta la Ley 1273 de 2009 (enero 5) Diario Oficial No. 47.223 de 5 de enero de 2009 la cual reglamenta "La protección de la información y de los datos" en el capítulo 1 el cual reglamenta los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos. Adicional en el capítulo dos contiene 2 artículos (269i/269j) los cuales tratan los hurtos por medios informáticos y semejantes; mientras que el segundo artículo trata sobre la transferencia no consentida de activos.

La norma técnica NIST 800-115 ofrece una guía técnica de recomendaciones para la evaluación y pruebas de seguridad de la información.

La NIST 800-115 Capítulo 3 establece: Las técnicas de revisión pasiva que examinan sistemas, aplicaciones, redes, políticas y procedimientos para descubrir vulnerabilidades de seguridad. También reúne información para facilitar y optimizar otras técnicas de evaluación. Las técnicas de examen son pasivas, suponen un riesgo mínimo para sistemas y redes. Este capítulo cubre varias técnicas comunes de revisión, documentación, registro, conjunto de reglas y revisión de la configuración del sistema rastreo de red y comprobación de integridad de archivos.

La NIST 800-115 Capítulo 4 establece: Técnicas de identificación y análisis, que se centran en la identificación de dispositivos activos así como sus puertos y servicios asociados; además del análisis de las posibles vulnerabilidades. Esta información se utiliza para seguir explorando los dispositivos para validar la existencia de las vulnerabilidades.

La NIST 800-115 Capítulo 5 establece: Las técnicas de validación de vulnerabilidades de destino, que utilizan información generada a partir de identificación de destino y análisis para seguir explorando más a fondo la existencia de posibles vulnerabilidades. El objetivo es demostrar que existe una vulnerabilidad y demostrar los riesgos de seguridad que se producen cuando se explota dicha vulnerabilidad. Implica el mayor nivel de riesgo en la evaluación,

dado que estas técnicas tienen más potencial de impacto en el sistema de destino o red que otras técnicas.

4.5 ALCANCE

El desarrollo del proyecto contempla los siguientes alcances enmarcados en la investigación descriptiva y deductiva como metodología de proyecto y la norma internacional NIST 800-115 capítulos 3, 4 y 5 (esta norma es una guía sobre las prácticas que se deben realizar a nivel de seguridad para el aseguramiento de la información) como metodología de la ingeniería para los dispositivos Apple con iOS 6.1.4.

1. Revisión de la documentación existente sobre las vulnerabilidades a nivel de sistema operativo en los dispositivos Apple con iOS 6.1.4.

2. Descripción de las vulnerabilidades y riesgos a los que se encuentran expuestos los dispositivos móviles con iOS 6.1.4.

3. Análisis de las vulnerabilidades y riesgos a los que se encuentran expuestos los dispositivos móviles.

4. Aplicación de técnicas de validación de vulnerabilidades a los dispositivos móviles (Penetration Test).

5. Elaboración de un documento que contenga las mejoras prácticas enfocadas a la protección de la información en los dispositivos móviles con iOS 6.1.4.

5. METODOLOGÍA DE LA INVESTIGACIÓN

La metodología de investigación es de carácter cualitativo porque no se plantea una hipótesis sino que se elabora una serie de conclusiones partiendo de los antecedentes de investigaciones similares dentro del campo de la seguridad informática y el análisis de riesgos en sistemas operativos de Smartphone específicamente Apple iOS 6.1.4.

5.1 POBLACIÓN Y MUESTRA

La población estadística del estudio contempla los dispositivos que soportan Sistemas Operativos iOS de Apple, estos son

Tabla 2 Lista de dispositivos que usan iOS.

Dispositivo
iPhone
iPad
iPod Touch
Apple TV

Fuente. Autores

La muestra estadística se seleccionó tomando solamente uno de los dispositivos que usan el sistema operativo a analizar. Este fue el iPhone 5 dada la facilidad de acceso al mismo.

5.2 UNIDAD DE ANÁLISIS

La unidad de análisis implementada en este trabajo investigativo está enfocada a los dispositivos móviles de Apple con iOS 6.1.4 y a sus usuarios, puesto que son un factor importante que interactúa de forma directa con dichos dispositivos, adicionalmente es un análisis que busca garantizar los pilares fundamentales de la seguridad informática, es por esto que se vislumbra la necesidad de evaluar el tipo de información que se almacena y procesa en un Smartphone de este tipo

5.3 ETAPAS O FASES

Revisión documental en sistemas Apple iOS 6.1.4
Riesgos En Smartphone
Riesgo para los Usuarios.
Exploración de Vulnerabilidades
Vulnerabilidades en sistemas Apple iOS 6.1.4

6. RESULTADOS Y DISCUSIÓN

6.1 REVISIÓN DOCUMENTAL DE SISTEMAS APPLE IOS 6.1.4

Dando ejecución al primer objetivo específico de este proyecto con el cual se busca revisar la documentación existente sobre las vulnerabilidades a nivel de sistema operativo en los dispositivos móviles con iOS 6.1.4 se determina que la revisión documental busca verificar aspectos técnicos, políticas y procedimientos actuales aplicados de los dispositivos con sistema iOS 6.1, los cuales constituyen la postura de seguridad sugerida por el fabricante frente a los equipos analizados, dentro de los documentos consultados, es posible integrar políticas de seguridad, arquitecturas, procedimientos operativos; planes de seguridad, memorandos internos y planes de respuesta a incidentes.

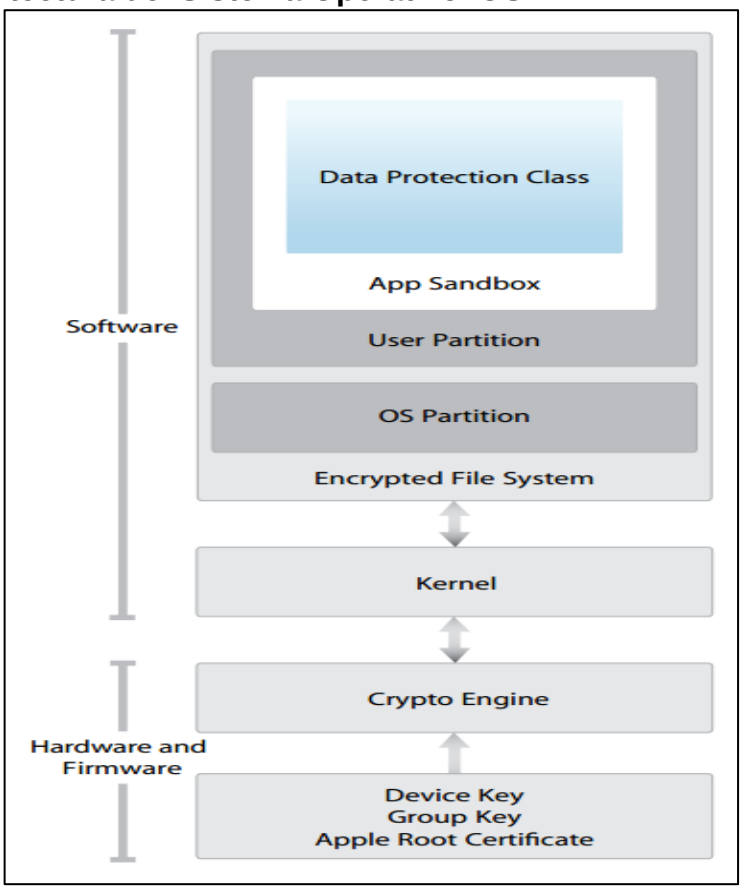
Es de aclarar que la revisión de la documentación no garantiza que los controles de seguridad se aplican correctamente, por ello fue necesario explorar, explotar y probar los controles establecidos por la NIST 800-115 en busca de la optimización de los mismos determinado su eficacia.

6.1.1 Arquitectura del Sistema Operativo iOS[83]. Existe una estrecha integración de hardware y software en los dispositivos IOS que permite la validación de las actividades a través de todas las capas del dispositivo. De arranque inicial de instalación del software iOS ya través de aplicaciones de terceros, se analiza cada paso para garantizar que cada actividad es de confianza y utiliza adecuadamente los recursos.

Una vez que el sistema está en funcionamiento, esta arquitectura de seguridad integrada depende de la integridad y confiabilidad de XNU, el kernel de iOS. XNU cumple funciones de seguridad en tiempo de ejecución y es esencial para ser capaz de confiar en las funciones y aplicaciones de alto nivel.
Para asegurarse de mantener loa integridad de los archivos del sistema estos se encuentran cifrados, y separados por particiones para Sistema Operativo y datos de usuario, esto garantiza que cualquier mala manipulación por parte del usuario no afectara el kernel del sistema.

[83] RUIZ, Martha. Arquitectura del sistema operativo. Bogotá: [citado 12 agosto, 2013]. Disponible en Internet < URL : http://images.apple.com/iphone/business/docs/iOS_Security_Oct12.pdf>

Figura 2. Arquitectura del Sistema Operativo iOS



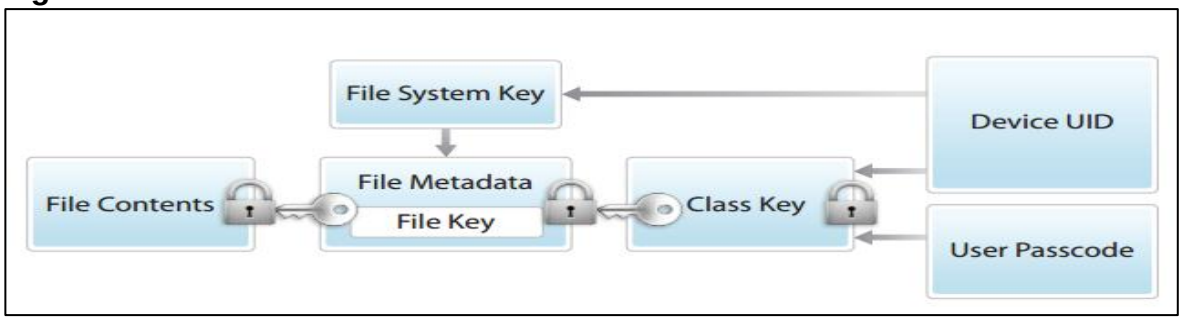
Fuente. SYMANTEC. Arquitectura del sistema. : Bogotá: [citado 12 agosto, 2013]. Disponible en Internet < URL : http://www.symantec.com/content/es/mx/enterprise/images/theme/mobility/America-Latina-2012-State-of-Mobility-Survey-Report-SPA.pdf>

6.1.2 Protección de Aplicaciones. Una vez que el kernel iOS ha arrancado, se controla que los procesos de usuario y las aplicaciones se pueden ejecutar. Para asegurarse de que todas las aplicaciones provienen de una fuente conocida y aprobada y no han sido manipulados, iOS requiere que todo el código ejecutable se firmó con un certificado emitido por Apple. Las aplicaciones suministradas con el dispositivo, como Mail y Safari, están firmados por Apple. Aplicaciones de terceros también deben ser validadas y firmadas con un certificado emitido por Apple. La firma de código obligatoria se extiende el concepto de cadena de confianza desde el sistema operativo a las aplicaciones, y evita las aplicaciones de terceros de código sin firmar utilicen los recursos de forma inadecuada.

6.1.3 Cifrado y Protección de Datos. El contenido de un archivo se cifra con una clave por archivo, que se envuelve con una clave de clase y se almacena en los metadatos de un archivo, que es a su vez cifrada con la clave de sistema de

archivos (mediante el algoritmo AES). La clave de clase está protegida con el UID hardware y, para algunas clases, con códigos de acceso del usuario. Esta jerarquía proporciona flexibilidad y rendimiento. Por ejemplo, cambiar la clase de un archivo sólo requiere reemplazar su clave por archivo, y un cambio de código de acceso sólo requiere rearmar la clave de clase.

Figura 3. Cifrado iOS



Fuente. SYMANTEC. Arquitectura del sistema. : Bogotá: [citado 12 agosto, 2013]. Disponible en Internet < URL : http://www.symantec.com/content/es/mx/enterprise/images/theme/mobility/America-Latina-2012-State-of-Mobility-Survey-Report-SPA.pdf>

La protección depende de la calidad del código de acceso, iOS permite claves sencillas de 4 cifras numéricas o las más seguras que son alfanuméricas.
Cabe resaltar que la Protección de Datos descrita arriba no se activa si no se habilita el código de acceso.

Figura 4. Código de Acceso iOS

Fuente. Autores

6.1.4 Seguridad de red. iOS soporta los protocolos de cifrado de conexión comúnmente conocidos, Secure Socket Layer (SSL v3) así como Transport Layer Security (TLS v1.1, TLS v1.2).

Para las conexiones mediante VPN y Wi-Fi, la protección depende de cómo esté configurada la red a la que se desea conectar, sin embargo, iOS soporta los protocolos VPN/Wi-Fi estándar de la industria. Para el caso del Bluetooth en iOS ha sido diseñado para proporcionar una funcionalidad útil sin mayor acceso innecesario a los datos privados, en otras palabras, no funciona para la trasmisión de datos, solamente para funciones de conexiones a dispositivos y streaming.

6.1.5 Acceso al Dispositivo. Adicional a la protección criptográfica descrita anteriormente, iOS permite proteger el acceso a la interfaz de usuario del dispositivo por medio de una contraseña. La interfaz gráfica de iOS mantiene un estándar de tiempo después de ingresar de un código de acceso inválido, lo que reduce drásticamente la posibilidad de un ataque de fuerza bruta a través de la pantalla de bloqueo. Además, los usuarios pueden optar por que el dispositivo sea borrado automáticamente después de 10 intentos fallidos de contraseña.

Los dispositivos iOS pueden ser borrados remotamente por un administrador o un usuario. La eliminación remota de forma instantánea se logra con seguridad descartando la clave de cifrado de almacenamiento por bloques del sistema de archivos, haciendo que todos los datos queden totalmente ilegibles. Este barrido puede ser iniciado por MDM (Mobile Device Management), Exchange, o iCloud.

6.1.6 Modificaciones no autorizadas a la arquitectura. Uno de los mayores retos que ha enfrentado Apple Inc. es la gran cantidad de hackers que buscan explotar las capacidades de sus dispositivos; los primeros hackers que buscaban desbloquear la protección del iPhone, indicaron que sus acciones fueron impulsadas porque iOS no permitía ciertas funciones (por ejemplo, MMS, tethering (técnica que permite la conexión a internet utilizando el teléfono móvil como dispositivo de conexión), y personalización entre otras) o aplicaciones de terceros diferentes de las disponibles desde la AppStore.

Algunos piratas informáticos también tomaron la postura de que iOS era inseguro, y querían mostrar a Apple los defectos que tenía, el grupo más notorio es el iPhone Dev Team, quienes idearon el proceso conocido como “Jailbreak” que consiste en remover las limitaciones originales (que están configuradas desde la fábrica en los dispositivos que utilicen el sistema operativo iOS), mediante el uso de kernels (núcleo de sistemas operativos basados en Unix) modificados; dicho procedimiento permite a los usuarios acceder por completo al sistema operativo,

permitiendo descargar aplicaciones, extensiones y temas que no estén disponibles a través de la AppStore (sitio Web autorizado por el fabricante como el único lugar para descargar aplicaciones). Un dispositivo con Jailbreak todavía puede usar la AppStore, iTunes y todas las demás funciones sin inconveniente alguno, el Jailbreak es necesario si el usuario quiere correr software no autorizado por Apple.

Existen (a Agosto de 2013) dos versiones de este procedimiento, el “Jailbreak atado" que requiere que el dispositivo esté conectado a un computador cada vez que inicie, y el “Jailbreak sin ataduras" que permite al dispositivo encender a la totalidad del sistema sin la asistencia de un computador; bajo el Digital Millennium Copyright Act. El proceso de hacer Jailbreak es legal en los Estados Unidos, adicionalmente, Apple anunció que la práctica puede violar la garantía, sin dejar de lado que el hecho de modificar los parámetros de los diseñadores advierte un elevado riesgo de seguridad puesto que permite la interacción de software sin discriminación.

Además de la ejecución del Jailbreak, existen una serie de novedades en seguridad destacadas por el mismo fabricante; la siguiente información fue extraída de los documentos de soporte publicados en las páginas oficiales de Apple[84], claro está que Apple presenta una nota aclaratoria en la que asegura que no entrará en ningún tipo de discusión respecto de las vulnerabilidades encontradas

6.1.7 Vulnerabilidades conocidas. El número de vulnerabilidades que se publican diariamente es elevado, sin embargo, se evidencia que el número de exploits disponibles se encuentran previamente identificados por Apple. No obstante las vulnerabilidades no siempre son materializadas por un exploit. Esto hace necesario el uso de un bug no parchado. Frameworks como Metasploit son una herramienta básica para identificar varias de las vulnerabilidades que se pueden encontrar en este sistema operativo de Apple. Es por esto que se vio la necesidad de identificar varias vulnerabilidades con su respectivo código CVE (Common Vulnerabilities and Exposures) el cual se muestra descrito por años y tipos de vulnerabilidad en la siguiente tabla:

[84]SUPPORT APPLE. ejecución del Jailbreak . . Bogotá: [citado 12 agosto, 2013]. Disponible en Internet < URL : http://support.apple.com/kb/HT4564?viewlocale=es_ES#>

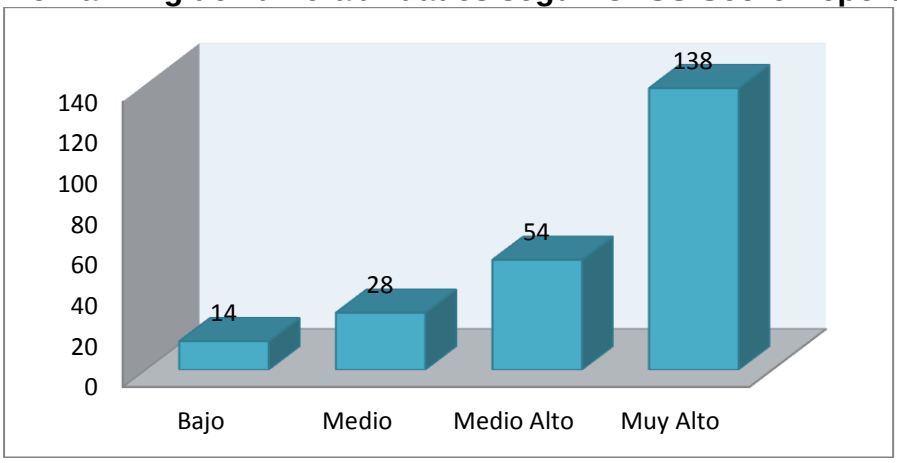
Tabla 3 CVE Anual y por categorías

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
1999	7	1								3					
2000	4	1		1											
2001	12	3	3	3							1	2			
2002	23	7	10	5								2			1
2003	47	7	10	9			1	3			1	4			
2004	66	8	13	10				2		3	2	5			
2005	148	28	45	38	1		2	1		7	4	12			
2006	138	42	72	53	5		1	1		6	5	6			
2007	208	62	99	58	20		13	2	1	19	13	18			6
2008	211	76	102	54	21		12	3		15	29	7	1		10
2009	220	108	96	61	24		17		1	12	23	9	1		16
2010	302	174	165	84	40		12	5		22	27	10	1		8
2011	253	169	169	149	108		9	2		15	23	3			1
2012	283	210	214	117	182		7			16	19	3			
Total	1922	896	998	642	401		74	19	2	118	147	81	3		42
% Of All		46.6	51.9	33.4	20.9	0.0	3.9	1.0	0.1	6.1	7.6	4.2	0.2	0.0	

El sistema de puntuación de vulnerabilidades comunes (CVSS) proporciona un marco abierto para la comunicación de las características y el impacto de las vulnerabilidades de TI. Su modelo cuantitativo garantiza una medición precisa repetible al tiempo que permite ver las características de vulnerabilidad subyacentes que se utilizaron para generar los resultados.

La ilustración 5 muestra el ranking de vulnerabilidades según CVSS Score Report para las vulnerabilidades de iOS 6.4

Ilustración 5 Ranking de vulnerabilidades según CVSS Score Report



6.2 RIESGOS A LOS QUE SE EXPONEN LOS USUARIOS DE LOS SMARTPHONE.

Con la ejecución del segundo objetivo de este proyecto se realiza una descripción de los riesgos a los que se encuentra expuesta la información contenida en los dispositivos móviles Apple con iOS 6.1, esto, apoyado con la revisión de la documentación del capítulo anterior, da una idea de los puntos críticos de atención en cuanto al funcionamiento general del sistema operativo y sus vulnerabilidades más explotadas.

De acuerdo con la investigación que apoya la descripción del problema, la información es el factor clave de riesgo para los Smartphone, no es lo mismo extraviar un Smartphone nuevo, que uno con mucho tiempo de uso e información sensible corporativa o personal. Es por esto, que este capítulo tiene un enfoque de riesgos a nivel de usuario, pues son los que finalmente afectan la información almacenada en los dispositivos y pueden clasificarse en las siguientes categorías:

6.2.1 Pérdida o robo. Si bien es el robo es uno de los hechos de mayor reiteración en el territorio colombiano, un Smartphone es uno de los blancos más atractivos para los delincuentes ya que representa una efectiva de ingresos y un riesgo mínimo.

En estas situaciones, el problema no es la pérdida del dispositivo en sí misma ni la afectación económica del activo que ello implica, sino la imposibilidad de recuperar la información contenida en el dispositivo por falta de respaldo y el mal uso que se le pueda dar a la misma en las manos equivocadas.[85]

[85]ESET. Pérdida o robo de datos. . Bogotá: [citado 12 agosto, 2013]. Disponible en Internet < URL : http://www.eset-la.com/pdf/documento_guia_de_seguridad_para_usuarios_de_smartphone_baj.pdf>

6.2.2 Riesgo Phishing. Es un tipo de ataque informático mediante el cual un elemento externo recopila información (contraseñas, números de tarjeta de crédito, entre otras), usando engaños a través páginas de internet preparadas con antelación o con aplicaciones falsas, mensajes de texto o correos electrónicos, lo que permite la captura de información con la que puede ser posible afectar al usuario.

En el caso de los Smartphone, se puede presentar mediante mensajes de texto, correos electrónicos y hasta en llamadas telefónicas de delincuentes que se hacen pasar por corporaciones para ofrecer premios o descuentos a cambio de información o transacciones bancarias, saldos de telefonía, entre otros.

6.2.3 Riesgo Spyware. Otro de los ataques comunes en el campo de la informática aplica mediante la descarga de software de dudosa procedencia (programas no firmados ni admitidos por el fabricante) lo que puede hacer que en el teléfono se instale software espía que permita a un atacante acceder directamente al sistema y a la información.

Muchos de los programas que pueden ser instalados en los Smartphone y que son de dudosa procedencia, pueden llegar a capturar información sobre el propietario o la información del dispositivo, lo que puede convertirse en un riego latente si se usa el dispositivo para transacciones bancarias por ejemplo.

6.2.4 Ataques de suplantación de identidad. Este tipo de ataque consiste en generar un punto de acceso a una red WiFi sin protección (similar a las encontradas en los centros comerciales), con la intención de que los usuarios se conecten a él para poder obtener los paquetes de datos con información básica del sistema como: versión del sistema operativo, dirección IP, puertos abiertos y servicios activos. Este acceso a redes inalámbricas sin autenticación permiten instalar malware (software malicioso con una intención definida) y ejecutar diferentes tipos de ataques, sin el conocimiento del usuario.

Es común encontrar a personas utilizando Smartphone en redes públicas de universidades, hoteles, clubes, aeropuertos, entre otros; en algunos de estos casos, los delincuentes pueden llegar a suplantar servidores en la red y filtrar información que se transmita en la red, suplantar destinos por resolución DNS entre otros; esto, puede ser muy peligroso pues al trasmitir información sensible en redes públicas se corre el riesgo de ser filtrada por un tercero.

6.2.5 Riesgo Malware y Virus. Son software desarrollado con un propósito específico, muchos de estos desarrollos se orientan en explotar diferentes vulnerabilidades de los sistemas operativos que están contenidos dentro de cada Smartphone, estos pueden desde habilitar accesos a la información hasta dejar

completamente inutilizable el sistema, monitorear lo que se hace en el dispositivo, esclavizarlo y un sinnúmero de riesgos que pueden llegar a comprometer la información del dispositivo.

6.2.6 Riesgo Ingeniería Social. Es una de las técnicas más usadas para la recolección de información en distintos campos de la informática y la tecnología, mediante ella es posible recabar diversos tipos de datos por medio de los cuales es posible llegar a tener acceso a la información del sistema. Un ingeniero social puede llegar a dar con la contraseña de un dispositivo móvil si esta no cumple con un nivel de seguridad complejo que evite su deducción por información personal, como por ejemplo, fechas, números telefónicos etc.

6.2.7 Uso inadecuado o restringido. Este riesgo representa la alerta de seguridad de mayor impacto para los sistemas operativos de los dispositivos Smartphone, consiste en la ejecución de procedimientos y modificaciones del Sistema Operativo no recomendado por los fabricantes (Jailbreak iOS), los cuales violentan gravemente la restricciones del sistema generando un mayor grado de vulnerabilidad a cualesquiera de los riesgos mencionados anteriormente.

6.2.8 Pérdida y replicación de información. Al adquirir un dispositivo de tipo Smartphone, es posible deducir que en este se guardan listas de contactos, historiales de llamadas, SMS y MMS recibidos y enviados, correos electrónicos, fotografías y videos personales, entre otras, que para la mayoría de usuarios es información altamente susceptible e importante y por tanto es necesario mantenerla protegida y fuera del alcance de personas no autorizadas. Uno de los mayores riesgos que sufren los usuarios de este tipo de equipos se ve ligado a la pérdida de los mismos, bien sea por un descuido o por hurto, dejando molestias por la pérdida de la información almacenada allí y más aún si se llegará a tratar de información confidencial que puede llegar usada con fines no deseados.

6.2.9 Fraude. Este riesgo es causado por el envío de información con el fin de participar en promociones, realizar descargas de tonos, fondos, aplicaciones o juegos, visitar páginas web de dudosa procedencia, realizar compras y pagos de productos o servicios, con la idea de estar realizando transacciones monetarias seguras, pero que son aprovechadas por personas que buscan extraer la mayor cantidad de información con fines de lucro personal.

6.2.10 Ciberbullying. El ciberbullying es el uso de los medios telemáticos (Internet, telefonía móvil principalmente) para ejercer acoso psicológico entre personas que generalmente se encuentran dentro del mismo rango de edad. No se trata aquí del acoso o abuso de índole estrictamente sexual ni de los casos en

los que personas adultas intervienen. Se trataría de situaciones en las que acosador y víctima son personas de la misma o similar edad o pertenecen al mismo entorno social, dichas situaciones se constituyen de amenazas, insultos o maltratos verbales.

6.2.11 Sexting. El sexting consiste en la difusión o publicación de contenidos (principalmente fotografías o vídeos) de tipo sexual, producidos por el propio remitente, utilizando para ello el teléfono móvil u otro dispositivo tecnológico; en muchas ocasiones estos contenidos llegan a manos de pedófilos, quienes mediante su utilización pueden llevar adelante acciones de extorsión, amenazando con exhibir dicho material a los familiares o amigos de los involucrados. La extorsión puede arrojar, en algunos casos, daños a la integridad moral y psicológica de las víctimas.

6.2.12 Grooming. El grooming se define como una situación de acoso u hostigamiento hacia un menor procedente de una persona mayor con finalidad sexual explícita o implícita. Se trataría del conjunto de estrategias que un adulto desarrolla para ganarse la confianza del niño o niña a través del dispositivo con el fin de obtener concesiones de índole sexual e incluiría actuaciones que van desde un acercamiento con empleo de empatía y/o de engaños hasta un chantaje para obtener imágenes comprometedoras de la víctima y en casos extremos, pretender un encuentro personal.

Tabla 4 Resumen Riesgos de Usuarios

Resumen Riesgos de Usuarios		
Riesgo	**Factores de Vulnerabilidad**	**Controles**
Pérdida y replicación de información	No existe la cultura de backup	7.1.1 Inventario de activos.
		7.1.2 Propiedad de los activos.
	Desconocimiento de herramientas para realizar backup	7.1.3 Uso aceptable de los activos.
		10.5.1 Copias de seguridad de la información.
	Inseguridad física o del entorno	11.3.1 Uso de contraseñas.
		11.3.2 Equipo de usuario desatendido.
Fraude	Desconocimiento de protocolos seguros de conexión	10.6.1 Controles de red.
		11.4.6 Control de la conexión a la red.

Cuadro 4 (Continúa)

Riesgo	Factores de Vulnerabilidad	Controles
	No implementación de una aplicación de Antivirus	11.4.7 Control de encaminamiento (routing) de red.
		10.6.2 Seguridad de los servicios de red.
Ciberbullying	Desconocimiento de entidades como el Colcert de la policía donde se pueden denunciar este tipo de eventos	10.4.1 Controles contra el código malicioso.
		10.4.2 Controles contra el código descargado en el cliente.
		11.6.1Campañas de sensibilización.
	Falta de formación en seguridad	11.6.2 Aislamiento de sistemas sensibles.
		12.3.1 Política de uso de los controles criptográficos.
Sexting	Desconocimiento de entidades como el Colcert de la policía donde se pueden denunciar este tipo de practicas	10.4.1 Controles contra el código malicioso.
		10.4.2 Controles contra el código descargado en el cliente.
		11.6.1 Restricción del acceso a la información.
	Falta de formación en seguridad	11.6.2 Aislamiento de sistemas sensibles.
		12.3.1 Política de uso de los controles criptográficos.
		12.3.2 Gestión de claves.
Grooming	Desconocimiento de entidades como el Colcert de la policía donde se pueden denunciar este tipo de prácticas	10.4.1 Controles contra el código malicioso.
		10.4.2 Controles contra el código descargado en el cliente.
		11.6.1 Restricción del acceso a la información.
	Falta de formación en seguridad	11.6.2 Aislamiento de sistemas sensibles.
		12.3.1 Política de uso de los controles criptográficos.

Fuente. Autores

En la siguiente tabla se muestra el análisis de riesgos evaluando la probabilidad de ocurrencia VS el impacto:

Tabla 5 Análisis de Riesgo

Análisis del riesgo				
Probabilidad	ALTO		• Desconocimiento de protocolos seguros de conexión. • No implementación de una aplicación de antivirus.	• No existe la cultura de backup. • Desconocimiento de herramientas para realizar backup. • Inseguridad física o del entorno.
	MEDIO		• Desconocimiento de entidades como el Colcert de la policía donde se pueden denunciar este tipo de prácticas. • Falta de formación en seguridad	• Desconocimiento de entidades como el Colcert de la policía donde se pueden denunciar este tipo de eventos. • Falta de formación en seguridad.
				• Desconocimiento de entidades como el Colcert de la policía donde se pueden denunciar este tipo de eventos. • Falta de formación en seguridad.
	BAJO			
		BAJO	MEDIO	ALTO
		Impacto		

Fuente. Autores

6.3. ANÁLISIS DE VULNERABILIDADES

Posterior a la revisión de documentación, y la identificación de riesgos es posible entrar a realizar un análisis que nos permita, mediante un Penetration Testing apoyado por la norma NIST 800-115, ejecutar las técnicas que nos lleven a explotar las vulnerabilidades evidenciadas en el capítulo 6.1, de acuerdo al conocimiento adquirido en este mismo capítulo sobre la arquitectura de iOS 6.1.4, sus métodos de protección de fábrica y las vulnerabilidades conocidas y publicadas para el Sistema Operativo en mención resumidas en el punto 6.1.7.1.

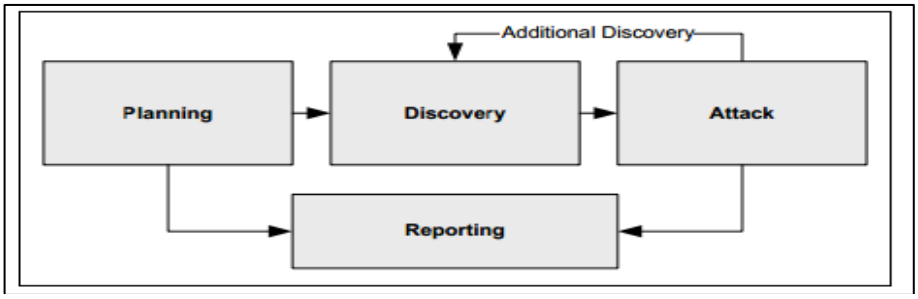
Asimismo, una vez ejecutado el Penetration Testing, se puede estudiar de qué forma la explotación de las vulnerabilidades del sistema puede llegar a apoyar la materialización de los riesgos expuestos en el capítulo 6.2 suponiendo un escenario de fuga de información apoyado en los casos de riesgo planteados en el

capítulo anterior de este documento y condensados en el mapa de calor de la tabla 6.

6.3.1 Penetration Testing a iOS 6.1. El test de penetración incluye dos partes; la primera es iniciar el test que cubre la información obtenida y escaneada. Identificar puertos y servicios de red, lo que conduce a identificar objetivos potenciales. Adicionalmente, con respecto a la identificación de puertos y servicios, se pueden utilizar otras técnicas para conseguir información de objetivos de red.

La figura 6 muestra las fases por medio de las cuales el "National Institute Of Standards and Technology", recomienda ejecutar el proceso de penetración de dispositivos.

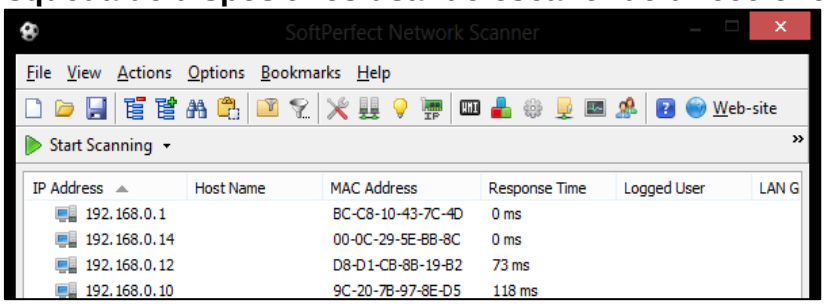
Figura 6. Esquema según la NIST 800-115 para ejecución del Test de Penetración.



Fuente: TECHNICAL GUIDE TO INFORMATION SECURITY TESTING AND ASSESSMENT. National Institute of Standards and Technology. 2008 .p.37.

6.3.1.1 Obtención de información del objetivo. La búsqueda del dispositivo en la red se realizó mediante la aplicación Advanced IP Scanner[86], desde un host en el mismo segmento de red que el iPhone.

Figura 7. Búsqueda de dispositivos usando escáner de direcciones IP



Fuente. Autores

[86] RADMIN. Advanced IP Scanner. Bogotá: [citado 12 agosto, 2013]. Disponible en Internet < URL : http://www.radmin.com/products/ipscanner/>

Usando el Advanced IP Scanner es posible ver que hay un dispositivo con fabricante Apple, Inc., este es el iPhone, además obtenemos información como su dirección física (MAC), dirección IPv4 y nombre del host.

Resultados. Al finalizar el escaneo se encontró el siguiente equipo

Tabla 6 Listado de dispositivos hallados usando escáner de direcciones IP

Dirección Física:	**D8:D1:CB:8B:19:B2**
Hostname:	JAG
Dirección IP:	192.168.0.12

Fuente. Autores

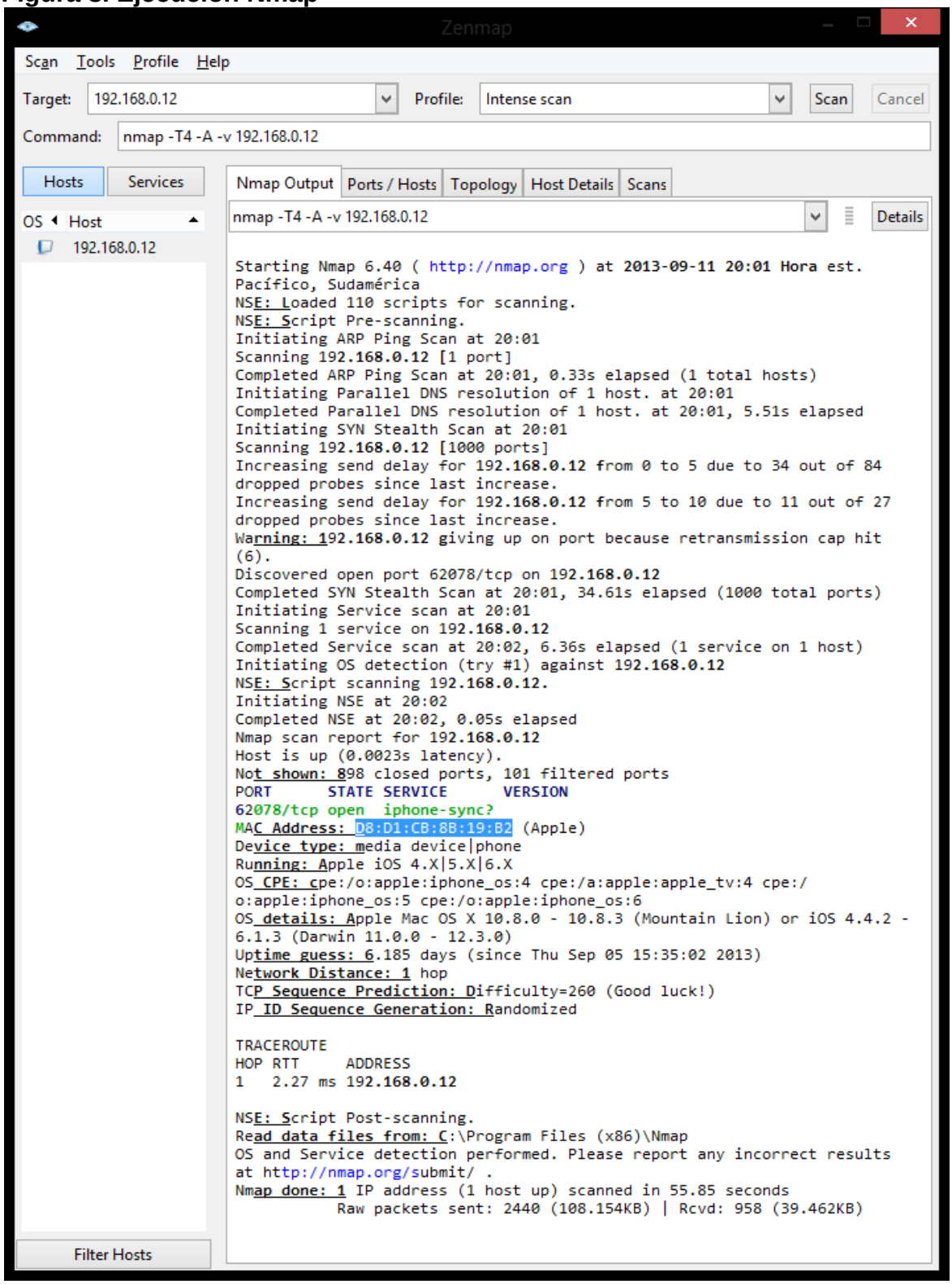
6.3.2 Escaneo del objetivo. Con la información obtenida es posible realizar escaneos tipo sniffing para obtener información detallada; para ello se utilizarán las aplicaciones Nmap [87]y Nessus[88]. Nmap. una aplicación de código abierto que sirve para efectuar rastreo de puertos (escrito originalmente por Gordon Lyon más conocido por su alias Fyodor Vaskovich), se usa para evaluar la seguridad de sistemas informáticos, así como para descubrir servicios o servidores en una red informática.

Por otra parte, Nessus es otra aplicación de escaneo de vulnerabilidades en diversos sistemas operativos su funcionalidad radica en realizar el escaneo en el sistema objetivo, a través de un cliente (basado en consola o gráfico) que muestra el avance y reporte de los escaneos.

6.3.2.1 Ejecución Nmap. Se ejecuta la herramienta hacia el host:

[87] NMAP. Escaneo. Bogotá: [citado 22 agosto, 2013]. Disponible en Internet < URL : http://nmap.org/:es>
[88] TENABLE. Escaneo. Bogotá: [citado 2 agosto, 2013]. Disponible en Internet < URL : http://www.tenable.com/products/nessus>

Figura 8. Ejecución Nmap



Fuente: Los autores

Los resultados son más informativos, se resumen a continuación:

- El dispositivo no tiene bloqueado el protocolo ICMP pues responde a ping y Nmap lo informa como “the host is up”.

- Se encuentra abierto el puerto TCP 62078, este es usado para la sincronización del dispositivo con iTunes vía Wi-Fi.

- Tipo de dispositivo: media device|phone.

- Sistema Operativo: Apple iOS 4.X|5.X|6.X

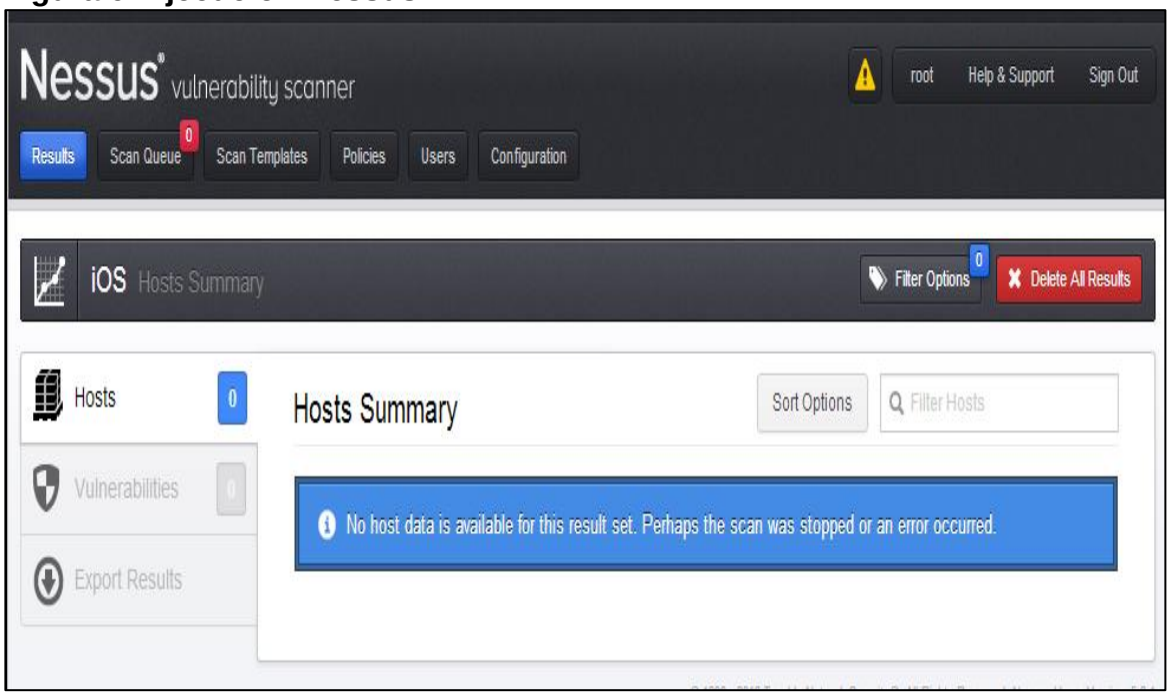
- OS CPE: cpe:/o:apple:iphone_os:4 cpe:/a:apple:apple_tv:4 cpe:/o:apple:iphone_os:5 cpe:/o:apple:iphone_os:6

- OS detalles: Apple Mac OS X 10.8.0 - 10.8.3 (Mountain Lion) or iOS 4.4.2 - 6.1.3 (Darwin 11.0.0 - 12.3.0)

- Dirección MAC: D8:D1:CB:8B:19:B2 (Apple)

6.3.2.2 Ejecución Nessus. Nessus no arroja resultados muy alentadores, ni siquiera puede encontrar el host:

Figura 9. Ejecución Nessus



Fuente: Los autores

Así mismo, no puede validar si existen vulnerabilidades para el mismo:

La información recolectada es de gran utilidad para cruzar contra las vulnerabilidades conocidas y para la posterior explotación.

6.3.3 Explotación de Vulnerabilidades en sistemas Apple iOS 6.2.1

6.3.3.1 Preparación de Dispositivo. Por defecto, los dispositivos iPhone no permiten acceder a los archivos internos del mismo a excepción de las fotografías. Para ingresar a los archivos del dispositivo es necesario realizar un procedimiento denominado "Jailbreak" al mismo. Hay que tener en cuenta las recomendaciones de Apple Inc., pues para ellos, el Jailbreaking es considerado un procedimiento grave de piratería, según informan en el artículo HT3743 de su página oficial,[89] en donde argumentan que las modificaciones no autorizadas del iOS suponen una violación al acuerdo de licencia del usuario final del iPhone, por tanto se considera piratería informática.

6.3.3.2 Procedimiento de Jailbreaking. El procedimiento consiste en modificar el firmware mediante una aplicación que puede ejecutarse desde Windows o MacOS. En necesario tener el dispositivo en modo DFU[90]. (El modo DFU es al acrónimo en inglés de Device Firmware Upgrade). El modo DFU permite al usuario restaurar el dispositivo desde cualquier estado de iOS, sea que se encuentre desactualizado, tenga inconvenientes de inicio, se requiera restaurar la configuración de fábrica del mismo, entre otros.

Inicialmente hay que descargar el firmware original del dispositivo, desde la página de Apple Inc.[91]**,** posteriormente, hay que descargar la aplicación **redsn0w 0.9.6rc17**, la cual no dispone de un servidor oficial de descarga, por lo que hay que encontrarla mediante buscadores web; para esta demostración utilizó el Redsn0w para Windows. (Redsn0w es una aplicación diseñada por el equipo Dev-Team[92] que funciona como una herramienta de apoyo para Jailbreak en todos los dispositivos actuales[93]), su funcionamiento es sencillo, utiliza el código Pwnage 2.0[94] para insertarlo aprovechando que el dispositivo queda en espera cuando se coloca en modo de recuperación (DFU).

---

[89] SUPPOR APPLE. Preparación de dispositivos. Bogotá: [citado 12 agosto, 2013]. Disponible en Internet < URL : http://support.apple.com/kb/HT3743?viewlocale=es_ES#>
[90] SOTELO, Juan. Procedimiento de Jailbreaking. Bogotá: [citado 8 agosto, 2013]. Disponible en Internet < URL : http://theiphonewiki.com/wiki/index.php?title=DFU_Mode>
[91] APPLDNLD. Procedimiento de Jailbreaking. Bogotá: [citado 7 agosto, 2013]. Disponible en Internet < URL : http://appldnld.apple.com/iPhone4/061-9853.20101122.Vfgt5/iPhone1,2_4.2.1_8C148_Restore.ipsw>
[92] SOLANO, Gregorio. Procedimiento de Jailbreaking . Bogotá: [citado 2 agosto, 2013]. Disponible en Internet < URL : http://blog.iphone-dev.org/>
[93] GUARZIZO. Sonia. Procedimiento de Jailbreaking. Bogotá: [citado 2 agosto, 2013]. Disponible en Internet < URL : http://theiphonewiki.com/wiki/index.php?title=Redsn0w>
[94] Ibid.,p.2.

Básicamente el sistema de arranque del iPhone incluye un LLB (Cargador de Arranque de bajo nivel por sus siglas en inglés Low Level Bootloader) y los módulos de iBoot que se almacenan en la memoria flash NOR[95] del dispositivo (Memoria Flash desde donde la aplicación de procesamiento inicia) y que suelen estar encriptados mediante RSA.

La vulnerabilidad consiste en que el iPhone asume que si algo está en la memoria NOR, es porque ha pasado necesariamente a través de la verificación de la firma RSA y por lo tanto es código autentico de Apple, lo que es incorrecto, pues el único mecanismo de prevención de la escritura de código no autorizado en la memoria NOR es el núcleo.

Por otra parte, el núcleo del iPhone/iPod touch incluye una extensión diseñada específicamente para escribir en la NOR, llamada AppleImage2NORAccess; dicha extensión realiza una verificación de firmas RSA en los datos que trata de escribir, es decir, cualquier cosa que sea verificada con AppleImage2NORAccess se puede escribir en la memoria flash NOR y quedará con la verificación RSA. Lo que hizo Dev-Team fue firmar el código de Pwnage 2.0 utilizando la extensión AppleImage2NORAccess y ejecutarlo colocando el dispositivo en modo DFU de la misma manera que Apple lo hace en la restauración, y así, poder cargar el código de Pwnage 2.0 en la memoria NOR de tal manera que al iniciar el iPhone lo ejecuta modificando el iOS.

6.3.3.3 Consideraciones del Jailbreaking. Evasi0n es un paquete de software que permite al usuario hacer jailbreak y eliminar las limitaciones impuestas a muchos dispositivos de la marca Apple con el software de Apple iOS. En la actualidad, es capaz de dispositivos IOS jailbreaking ejecutan versiones entre 6.0 a 6.1.2[96]

La explotación que realiza evasi0n es simple, utiliza el demonio de iOS “MobileBackup” que se utiliza para realizar las copias de seguridad desde iTunes. Bajo este principio, lo que evasi0n hace es evasi0n restaurar una copia de seguridad que contiene los archivos necesarios para el jailbreak.

A través de MobileBackup, evasi0n no puede almacenar archivos fuera de /var/Mobile/Media, esto, por la protección por defecto de iOS, por lo tanto, la aplicación crea un enlace "simbólico" (symlink) o un atajo en /var/Mobile/Media llamado .haxx que apunta a /var/Media.

De ese modo, MobileBackup es capaz de escribir archivos en /var/mobile a través del enlace simbólico .haxx. Los archivos copiados conforman la app se lanza en pleno proceso de jailbreak.

[95] Ibid.,p.2.

[96] ROGELES, Mario. Consideraciones del Jailbreaking. Bogotá: [citado 2 agosto, 2013]. Disponible en Internet < URL : http://evasi0n.com/>

Usando el procedimiento del symlink, evasi0n también gana acceso a un archivo de zona horaria, que es otra vez un enlace simbólico que apunta a launchd, un demonio que ejecuta procesos con privilegios de "root". El acceso a launchd ahora es explotado y el archivo de zona horaria se hace accesible a todos los usuarios (no sólo root) cambiando sus permisos. Un procedimiento similar se emplea para hacer un zócalo, que se encarga de las comunicaciones entre launchd y otros procesos accesibles para el usuario, bajo el cual se ejecutan todas las apps en iOS.

Ahora el usuario es notificado a lanzar la aplicación que ha sido copiada al filesystem iOS anteriormente. Esta aplicación, usando el zócalo launchd expuesto, hace que la partición del sistema cambie de sólo lectura a escritura. Evasi0n otra vez ejecuta MobileBackup y escribe varios archivos, uno de los cuales es launchd.conf que contiene una gran cantidad de comandos. Este archivo se ejecuta durante el arranque, lo que hace el jailbreak persistente.

Adicionalmente, uno de los comandos en launchd.conf es responsable de evadir el código de verificación de firmas AppleMobileFileIntegrity, y sustituye la función de comprobación incorporada con una que siempre devuelve true, de este modo, iOS nunca se dará cuenta que hay archivos del sistema operativo modificados. Evasi0n solamente funciona hasta la versión 6.1.2, a partir de la 6.1.3 la vulnerabilidad fue cerrada.

La ejecución del Jailbreak trae consigo ventajas y desventajas[97] que serán descritas a continuación:

- El Sistema Operativo puede presentar inestabilidad, bloquearse de forma inesperada con frecuencia. Las aplicaciones integradas o de otros fabricantes pueden bloquearse o congelase lo que puede provocar pérdida de datos.

- La comunicación por voz y transmisión de datos móvil puede presentar caídas, lentitud o poco fiabilidad, además de datos de ubicación con retardo o imprecisos.

- Los servicios como el buzón de voz visual, YouTube, Tiempo y Bolsa pueden presentar interrupciones o no funcionar. Adicionalmente, las aplicaciones de otros fabricantes que utilizan el servicio de Notificaciones Push de Apple pueden experimentar dificultades a la hora de recibir notificaciones. Otros servicios tipo push, como MobileMe y Exchange, pueden presentar inconvenientes al sincronizar datos con sus servidores respectivos.

- Estas modificaciones pueden abrir brechas de seguridad que pueden permitir a los hackers robar información personal, dañar el dispositivo, atacar la red inalámbrica o introducir malware o virus entre otros.

[97] SUPPOR APPLE.op.cit.,p. 3

- Las modificaciones de iOS pueden provocar el consumo acelerado de la batería.

- En algunos casos, luego de realizar Jailbreaking, el iPhone, iPad o iPod touch pirateado podría dejar de funcionar permanentemente cuando se instale una futura actualización del iOS creada por Apple.

- Posibilidad de instalar Aplicaciones/Modificaciones de terceros a través del administrador de paquetes **Cydia** que se instala una vez se realiza el Jailbreak. Cydia es una aplicación que permite la gestión de paquetes dpkg mediante una interfaz gráfica, permite adquirir software y demás modificaciones que no están disponibles en la AppStore oficial de Apple. Maneja repositorios que administra el usuario, partiendo del principio de administración de paquetes de los Sistemas Operativos Linux.

- Permite habilitar características deshabilitadas de fábrica en el dispositivo por ejemplo: Facetime, YouTube de alta calidad en 3G, fondo de escritorio, porcentaje de la batería, grabación de video, Dual Boot con Android entre otras.

- La personalización de la pantalla de inicio ofrece mayor cantidad de posibilidades pues Cydia dispone de una gran cantidad de temas que se pueden aplicar modificando los sonidos predeterminados, iconos, imagen de inicio entre otros.

- Permite abrir las bandas del iPhone sin necesidad de pedir autorizaciones al operador.

- En la mayoría de los casos es reversible, aunque puede presentar problemas dependiendo la cantidad de paquetes no autorizados se instalen en el dispositivo y que tanto se modifiquen los archivos propios del Sistema Operativo.

- Es posible realizar la instalación de aplicaciones de la AppStore de forma gratuita, descargando versiones crackeadas de las mismas y aplicándolas con aplicaciones específicas para ello.

6.3.3.4 Realización de Jaibreaking. El procedimiento de jailbreak es tan sencillo como la vulnerabilidad explotada. Teniendo el dispositivo conectado al computador, se debe descargar la aplicación evasi0n desde el sitio web http://evasi0n.com/

Figura 10. Evasi0n Jailbreak

Fuente. EVASI0N. Evaders. Bogotá: [citado 11 junio, 2013]. Disponible en Internet < URL :http://www.evasi0n.com >

Luego, de la descarga se debe ejecutar la aplicación que muestra una ventana similar la siguiente:

Figura 11. Descarga Evasi0n

Fuente: los autores

Lo siguiente que se debe hacer es conectar el dispositivo y evasi0n lo reconocerá de forma automática, seguidamente, se debe pulsar el botón jailbreak:

Figura 12. Evasión reconoce el dispositivo

Fuente: los autores

Luego de finalizar el proceso, en el menú principal del dispositivo deberá aparecer un icono con el logotipo de evasi0n y el texto jailbreak:

Figura 13. Pantalla de inicio con el logo de Evasi0n

Fuente: los autores

Sin desconectar el dispositivo, al abrir el icono el procedimiento continuará realizando varios reinicios sobre el dispositivo, finalmente, quedará el icono del administrador de paquetes típico del jailbreak Cydia:

Figura 14. Icono de Cydia

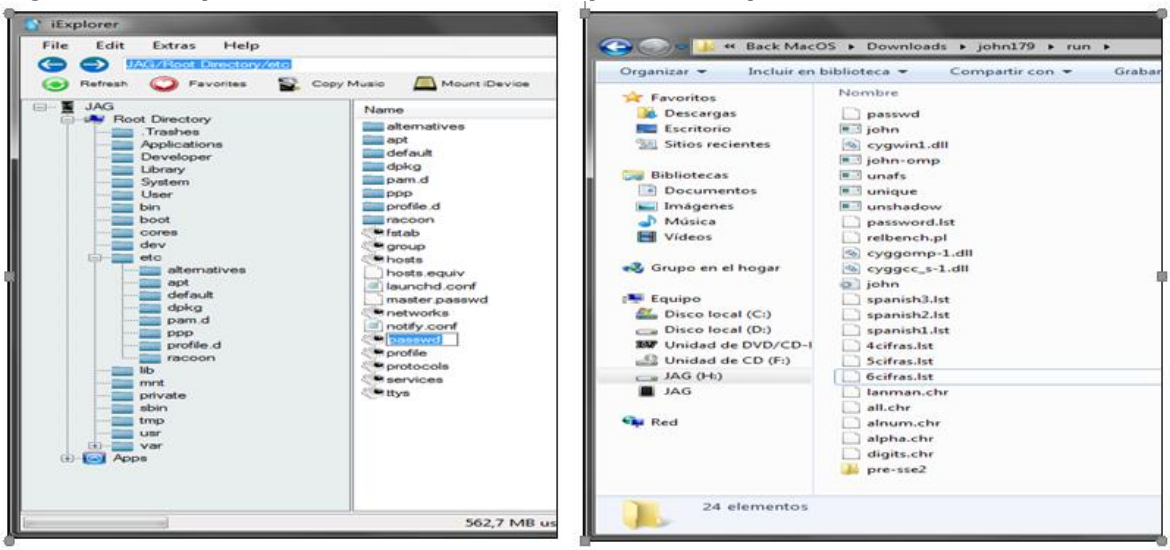
Fuente: los autores

6.3.4 Cracking de Password. iOS se deriva de Mac OS X, que a su vez está basado en Darwin BSD, y por lo tanto es un sistema operativo Unix y como tal almacena los hash de las contraseñas en un archivo passwd, localizado en /etc/passwd, para poder obtener este archivo usaremos la aplicación iExplorer[98]), de libre descarga y disponible para Windows y Mac OS, que permite explorar los archivos internos del dispositivo luego de realizar el Jailbreaking (es posible copiar el archivo passwd para intentar realizar cracking con el programa John the Ripper.[99]

6.3.4.1 Extracción del archivo passwd. Copiar el archivo passwd de la ruta /etc/passwd del iPhone 3G iOS 4.2.1 a la carpeta del programa John the Ripper 1.7.9:

[98] MACROPLANT. Cracking de Password . Bogotá: [citado 2 agosto, 2013]. Disponible en Internet < URL : http://www.macroplant.com/iexplorer/download-pc.php>
[99] Ibid.,p. 2

Figura 15. Copiando la información de password para descifrar

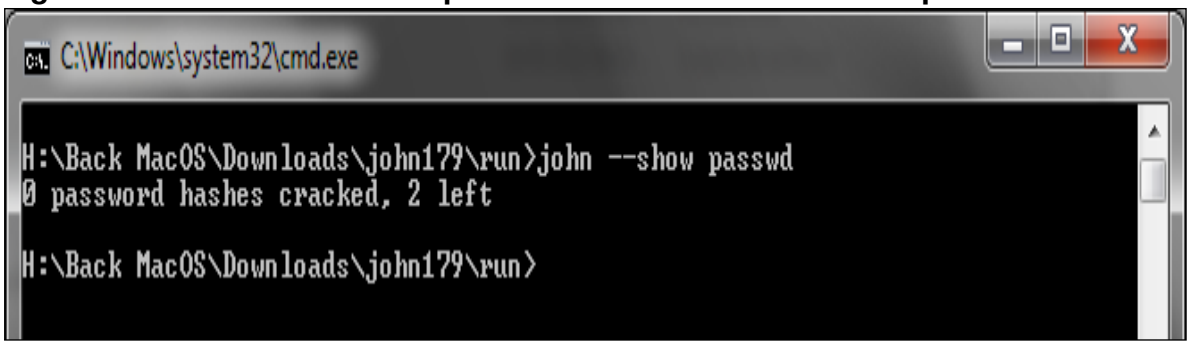


Fuente: los autores

6.3.4.2 Cracking mediante diccionario. La aplicación John the Ripper por defecto viene con un diccionario de contraseñas “password.lst”, que aunque es pequeño maneja las contraseñas más comunes conocidas.

Se verifica la existencia de hash mediante “John --show passwd”.

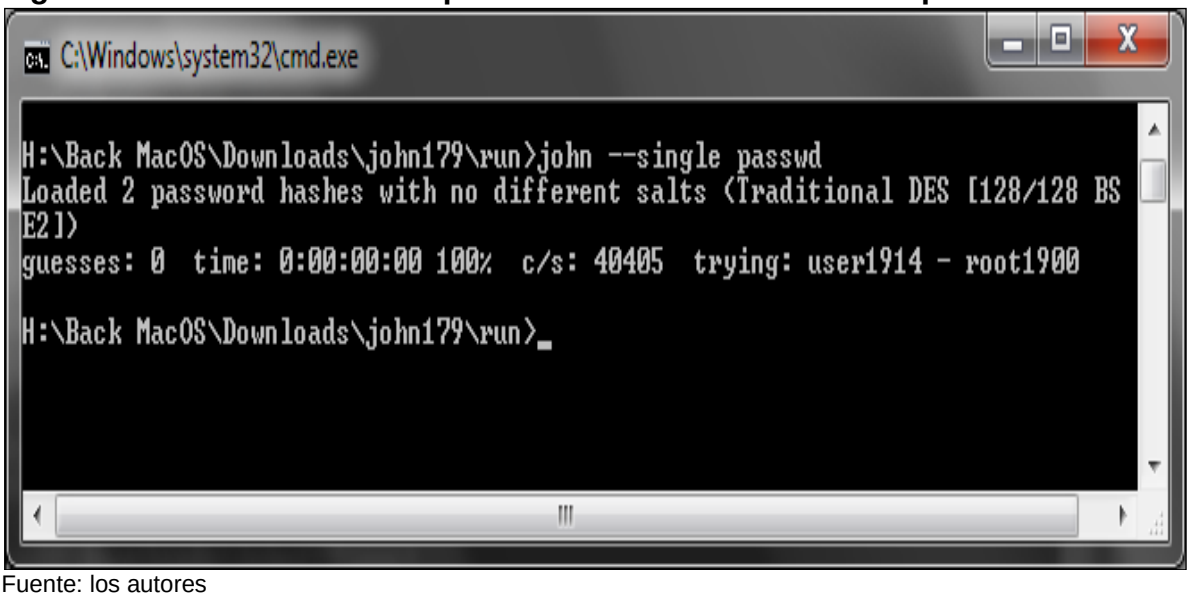
Figura 16. Verificando Hash que contiene la información del password



Fuente: los autores

Se intenta realizar cracking con los algoritmos propios de Jhon the Ripper (cracking simple), mediante el comando “john –single passwd”.

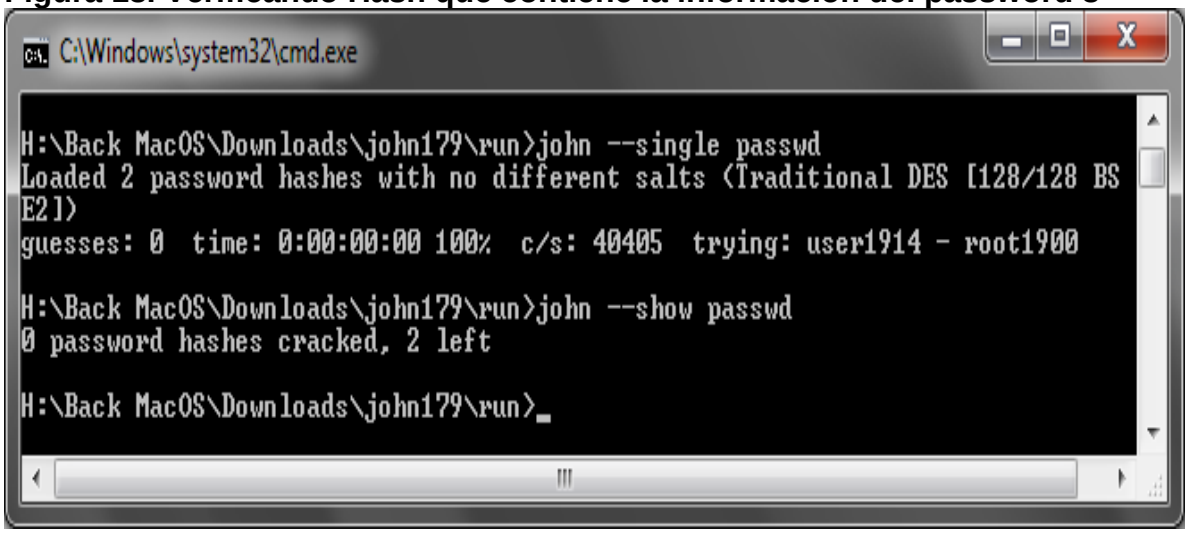
Figura 17. Verificando Hash que contiene la información del password 2



Fuente: los autores

Se verifica el estado de los hash para saber si el cracking simple fue exitoso:

Figura 18. Verificando Hash que contiene la información del password 3

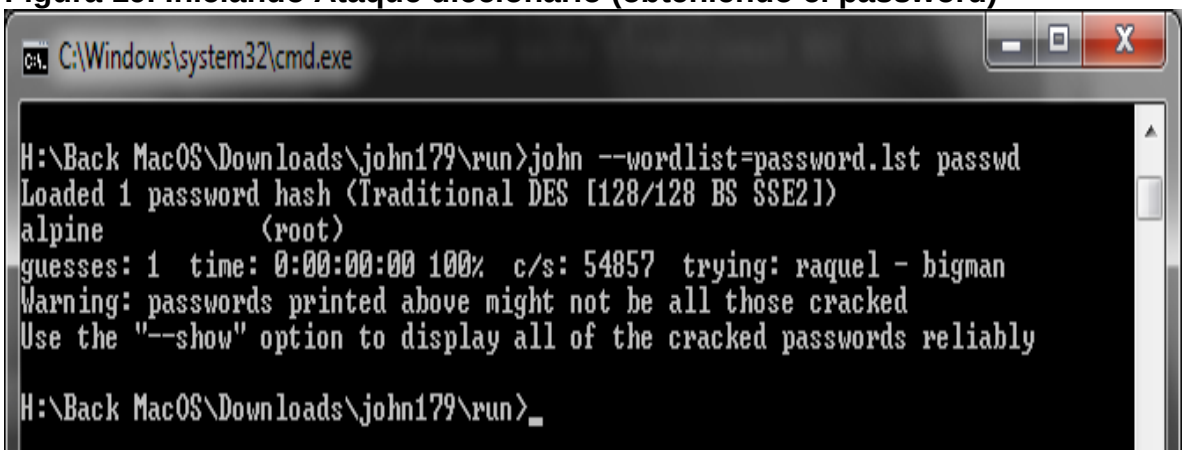


Fuente: los autores

Como se ve en la imagen anterior, el cracking simple no fue exitoso, es necesario realizar uno mediante diccionario.

Se intenta realizar cracking mediante el diccionario por defecto de Jhon the Ripper (password.lst) como se muestra en la imagen siguiente:

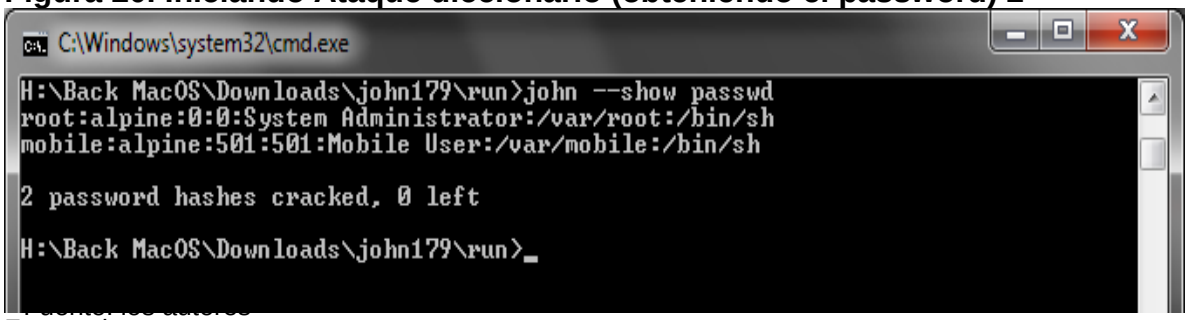
Figura 19. Iniciando Ataque diccionario (obteniendo el password)



Fuente: los autores

Jhon the Ripper informa haber cargado el hash de una contraseña, se verifica si se encuentran descifrados, imagen a continuación:

Figura 20. Iniciando Ataque diccionario (obteniendo el password) 2



Fuente: los autores

6.3.4.3 Resultados del password cracking. iOS tiene dos usuarios protegidos mediante contraseña:

Tabla 7 Listando los Usuarios iPhone

Usuario	Tipo	Contraseña
Súper-Usuario	root	alpine
Usuario	mobile	alpine

Fuente: los autores

Cabe resaltar que las contraseñas son las de los usuarios del Sistema Operativo como tal, y que no se han modificado desde la primera generación de iPhone.[100]

[100] IOS FORENSIC ANALYSIS FOR IPHONE, iPad, and iPod touch,: iOS Operating and File System Analysis. Boston. 2002.p.43.

6.4 ANÁLISIS GENERAL DE LAS VULNERABILIDADES

Tomando como base los testeos realizados y teniendo en cuenta que se realizó el procedimiento de Jailbreak y que se tiene la contraseña del súper usuario del sistema operativo, podemos crear un escenario donde saltan a la vista las vulnerabilidades que pueden presentarse.

Para argumentar la afirmación, se desarrolla un caso común e hipotético del uso del Jailbreak.

La aplicación Cydia se instala al realizar el procedimiento de Jailbreak, si bien es cierto que es opcional, también lo es, que es mediante ella que se pueden instalar aplicaciones sin pagar, entonces su instalación se da en la mayoría de los casos; Cydia permite la gestión de paquetes dpkg mediante una interfaz gráfica similar a los administradores de paquetes de distribuciones Linux. Fue desarrollado por Jay Freeman (también conocido como "saurik")[101], esta permite habilitar la transferencia de archivos de forma remota. Instalando el servicio de SSH abriendo el puerto 21, de hecho, en la página inicial de Cydia hay un manual que indica cómo hacerlo.

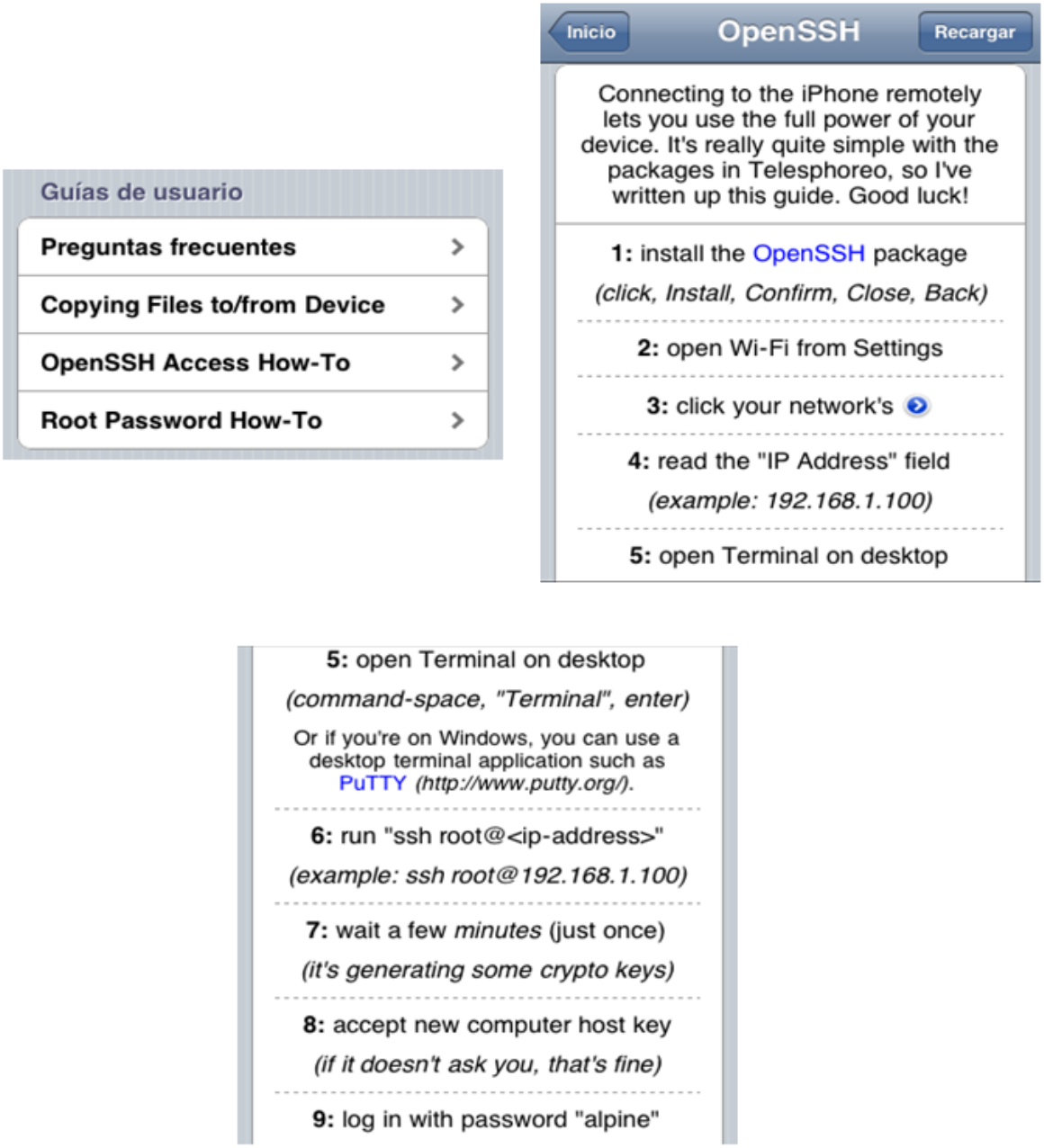
Figura 21. iPhone modificado a través de la aplicación CYDIA

Fuente: los autores

6.4.1 Instalación de SSH en iOS mediante Cydia. Se realiza la instalación del servicio SSH y con la contraseña del root, se accede remotamente al dispositivo suponiendo que se encuentre en una red inalámbrica pública para ver qué información sensible se puede obtener

[101] SAURIK. Linux. Bogotá: [citado 2 agosto, 2013]. Disponible en Internet < URL : http://www.saurik.com/id/1>

Figura 22. Instalando y configuración de acceso mediante SSH



Fuente: los autores

Se ingresa en la aplicación Cydia desde el iPhone con Jailbreak, en la página inicial, aparece un manual donde dice cómo realizar la instalación de SSH. Siguiendo las indicaciones, se instala el paquete SSH:

Figura 23. Instalando y configuración de acceso mediante SSH 2

Fuente: los autores

Al finalizar, podremos ingresar al dispositivo remotamente mediante un cliente SSH.

Figura 24. Confirmación de la instalación de SSH.

Fuente: los autores

Si bien es cierto que el manual de Cydia recomienda e indica como modificar la contraseña del root, también lo es que mundialmente según Symantec, solamente el 63% de las personas cambian sus contraseñas; [102]más aún si solamente se indica que Cydia funciona para instalar aplicaciones sin pagar sin advertir que esto trae consigo que se desbloquee el ingreso al dispositivo a cualquier atacante.

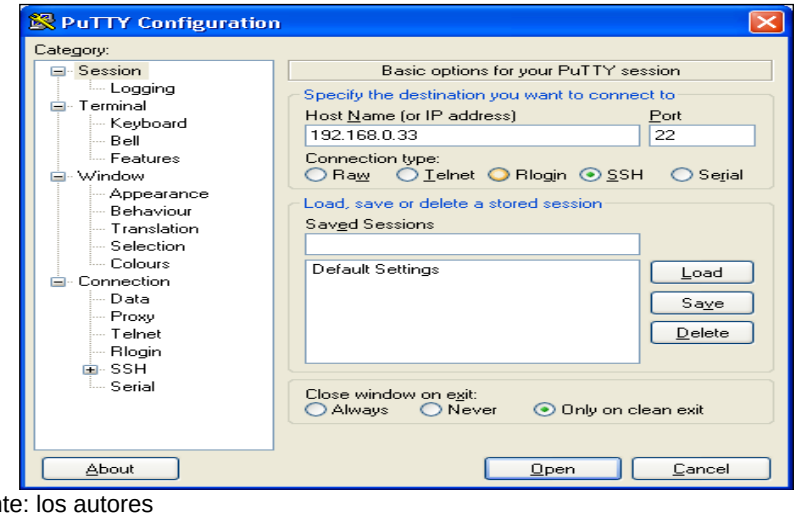
Teniendo en cuenta el caso de tener un iPhone con Jailbreak y con SSH instalado y estar conectado en una red inalámbrica pública, es posible identificar el teléfono con el IP Scanner y buscar el puerto 21 abierto mediante Nmap.

Se utiliza PuTTY [103] para iniciar una sesión remota en el dispositivo:

[102] SYMATEC. Op.cit.,p. 4

[103] CHIARK. Putty. . Bogotá: [citado 2 agosto, 2013]. Disponible en Internet < URL : http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>

Figura 25. Inicio de sesión utilizando el usuario root mediante PuTTY



Fuente: los autores

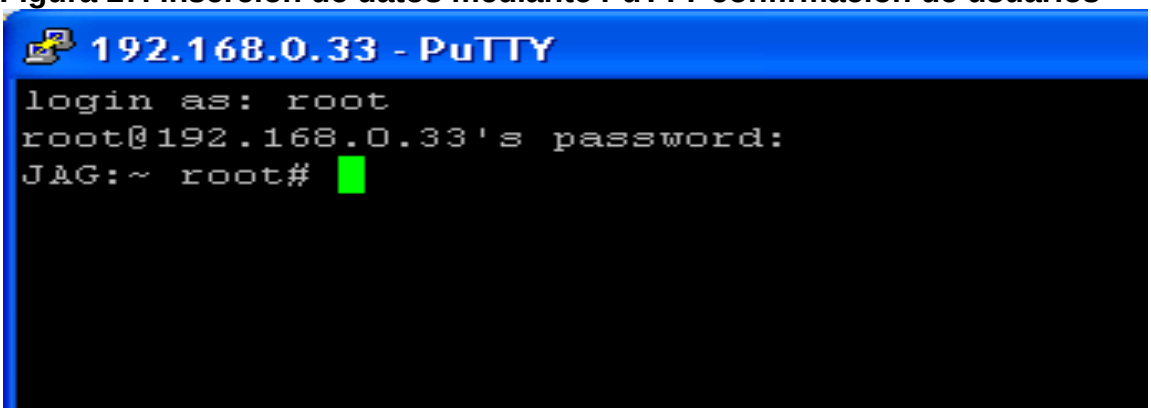
- Verificación de la identidad del host a través del fingerprint de su llave RSA.

Figura 26. Confirmación de seguridad utilizando el usuario root mediante PuTTY

Fuente: los autores

- Se inicia sesión con el usuario root.

Figura 27. Inserción de datos mediante PuTTY confirmación de usuarios

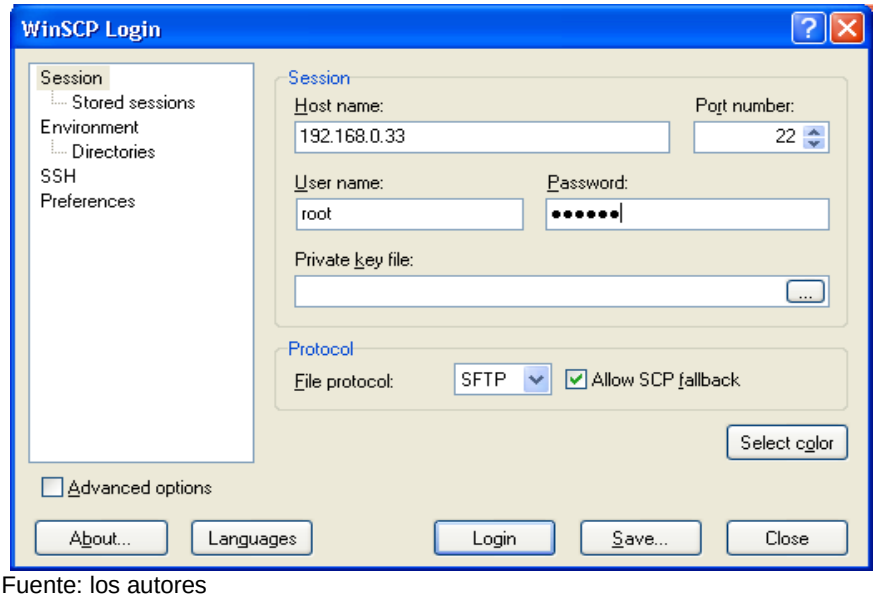


Fuente: los autores

Desde aquí podemos sencillamente ejecutar el comando reboot, logrando que el dispositivo se reinicie sin solicitar ninguna autorización del usuario, considerando esto como un sencillo ataque de denegación de servicio, más aun si se realizara de manera repetitiva.

6.4.2 Extracción de información. También es posible robar información del dispositivo, ingresando mediante el mismo protocolo con la aplicación libre para Windows WinSCP [104]

Figura 28. Conexión WinSCP

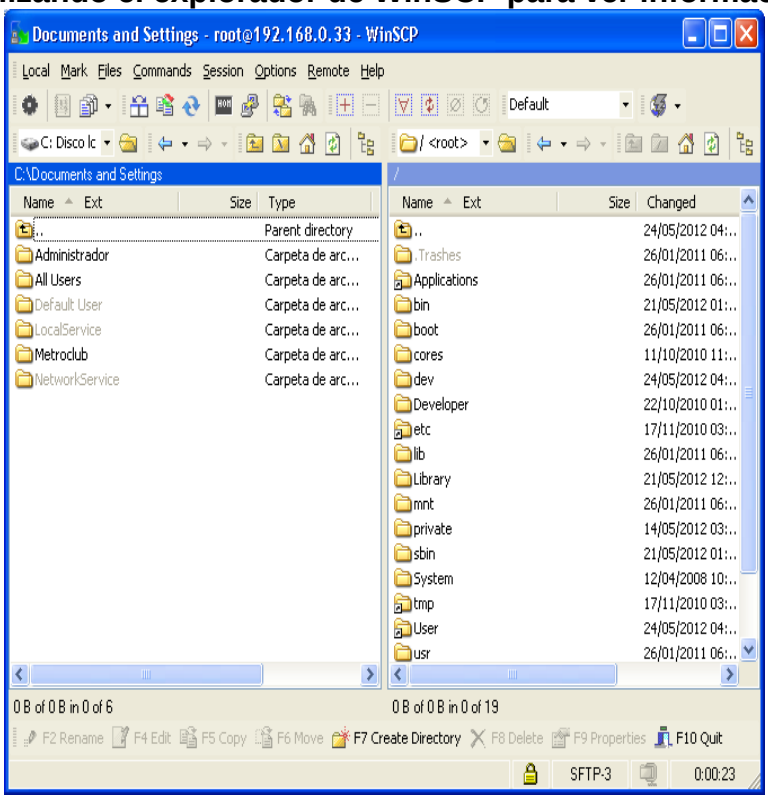


Fuente: los autores

[104] SOURCEFORCE. extracción de información. . Bogotá: [citado 2 agosto, 2013]. Disponible en Internet < URL : http://sourceforge.net/projects/winscp/files/WinSCP/4.3.7/winscp437.zip/download>

Como se ve en la imagen siguiente, se tiene acceso a todos los archivos del iPhone tal y como sucedía con iExplorer, solo que esta vez sin utilizar el cable y todo mediante WiFi.

Figura 29. Utilizando el explorador de WinSCP para ver información



Fuente: los autores

Es posible extraer información importante como mensajes de texto, libreta de direcciones, calendario, entre otros. Esta información se encuentra almacenada en archivos de SQLite, (*.db) en las siguientes ubicaciones:

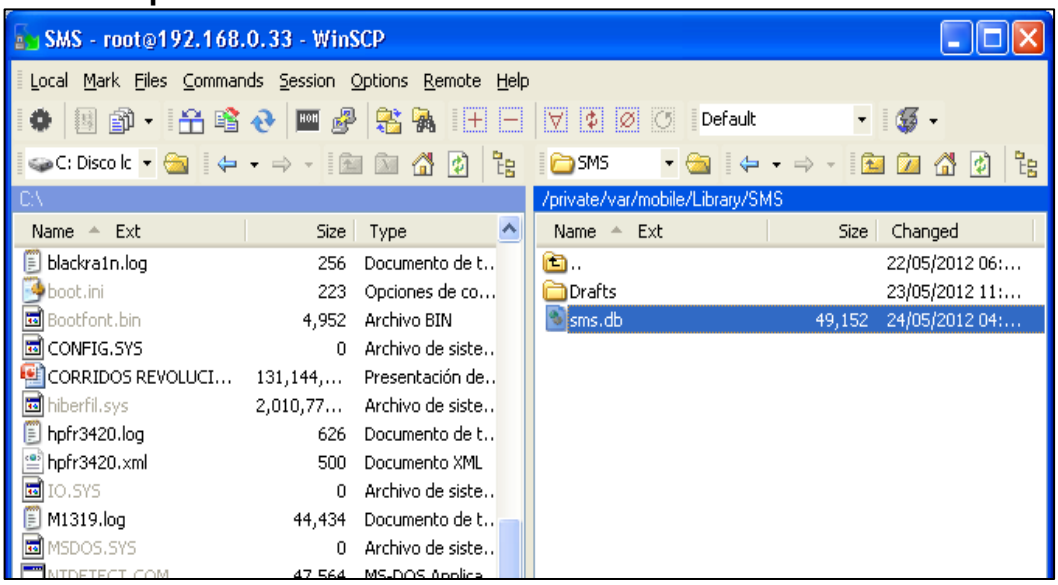
Tabla 8 Listado de rutas para el acceso a la información

Accesos a	Ruta de almacenamiento
Mensajes de Texto	/Var/Mobile/Library/SMS
Contactos	/User/Library/AddressBook
Correos	/Var/Mobile/Library/Mail
Calendario	/Var/Mobile/Library/Calendar
Historial de llamadas	/Var/Mobile/Library/CallHistory
Notas	/Var/Mobile/Library/Notes
Safari	/Var/Mobile/Library/Safari

Fuente: los autores

Se realiza la prueba extrayendo el archivo de los mensajes de texto usando la ruta: (/Var/Mobile/Library/SMS/sms.db), para abrirlo se utiliza la aplicación SQLite Database Browser.

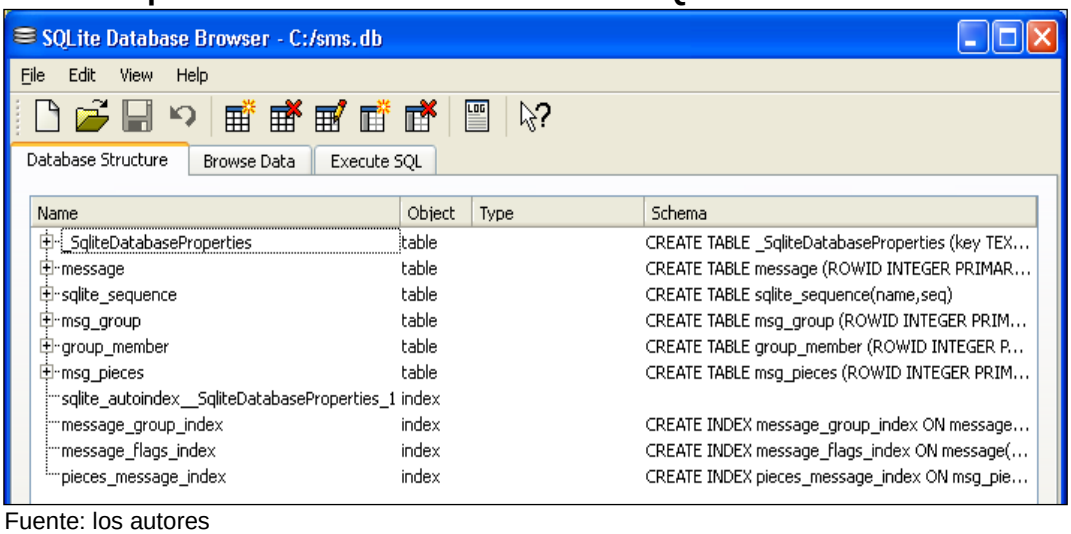
Figura 30. Explorando información confidencial con WinSCP



Fuente: los autores

Se abre el archivo sms.db con el SQLite Database Browser.

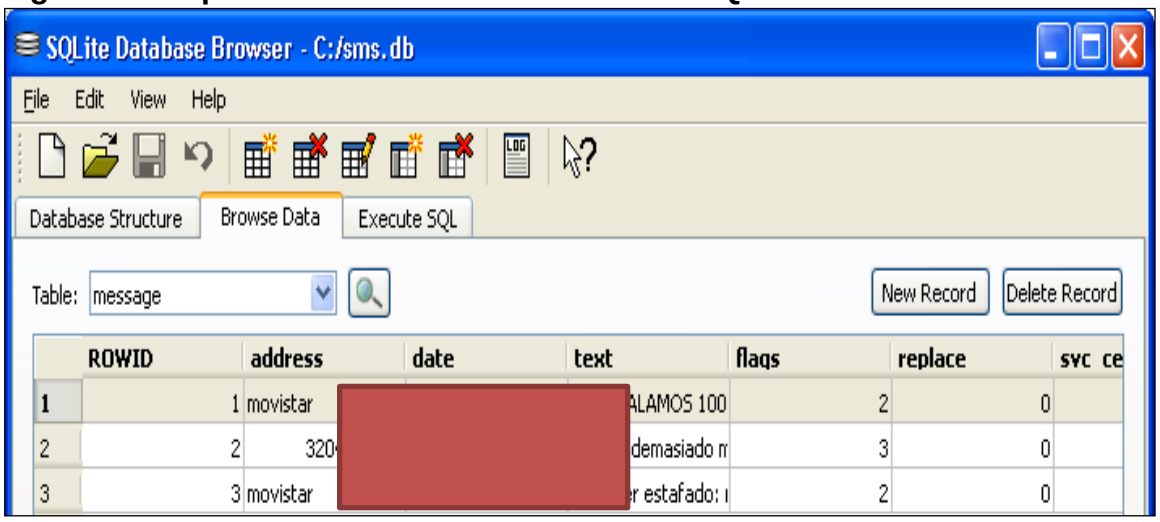
Figura 31. Explorando información utilizando SQLite



Fuente: los autores

En la pestaña Browse Data, es posible explorar las tablas de la base de datos. La tabla message contiene los mensajes de texto enviados y recibidos incluyendo información de remitente, destinatario y contenido del mensaje:

Figura 32. Explorando información utilizando SQLite 2



Fuente: los autores

7. CONCLUSIONES

- Las restricciones propias de iOS para muchos usuarios supone un desaprovechamiento del Hardware, aunque esto vaya en contra del criterio de los ingenieros diseñadores del iPhone, razón por la cual, este tipo de usuarios encuentran la necesidad de realizar procedimientos como el “jailbreak” con el fin de habilitar dichas restricciones, algunas de ellas como la imposibilidad de grabar video, realizar transferencia de archivos por Bluetooth, utilizar el dispositivo como medio de almacenamiento y ejecutar varias aplicaciones a la vez (multitarea).

- Tanto los usuarios como las organizaciones (sin importar el nivel de conocimiento), son cada vez más dependientes de Internet y sus servicios asociados, lo que también los expone constantemente a diferentes amenazas, en las que se utilizan estas condiciones para cometer acciones delictivas con fines económicos y comerciales entre otros (Ingeniería social, Phishing, entre otros), en consecuencia, es sumamente importante incorporar, como hábito cotidiano, las medidas de seguridad recomendadas la guía de mejores prácticas anexa a este documento. Al bloquear las amenazas de forma temprana se reduce considerablemente la posibilidad de ser potenciales víctimas de las actividades delictivas, que se llevan a cabo atentando contra la seguridad de los entornos de información independientemente de si es un Smartphone corporativo o personal.

- Adicionalmente se debe tener presente que también es necesario mantenerse informados en lo que respecta a los problemas de seguridad que suponen el uso de determinados medios de comunicación e interacción, es indispensable mantener las aplicaciones actualizadas y estar pendiente de las alertas que pueden generar las herramientas de seguridad que se instalan en los dispositivos con iOS.

- No es necesario disponer de gran conocimiento a nivel técnico para realizar los procedimientos de Jailbreak, las herramientas disponibles para ello son libres y de fácil acceso en Internet, además no se requiere un equipo de características particulares para lograr la ejecución de estos procedimientos.

- El hecho de que el iPhone no permita utilizarse como medio de almacenamiento disminuye el riesgo de que algún código malicioso intente escribir sobre los archivos del Sistema Operativo, esto, en comparación con equipos Android que permiten la lectura de medios extraíbles como memorias MicroSD y conexión como medio de almacenamiento en los cuales pueden filtrarse archivos riesgosos que representan un riesgo latente para el sistema y la información contenida en él.

- Los dispositivos iOS instalan sus aplicaciones en entornos controlados, siempre y cuando no se modifique el sistema operativo original (Jailbreak). Esta situación se presenta gracias a la tienda oficial de aplicaciones propia del fabricante AppStore de Apple. Toda aplicación que se carga en estas tiendas esta

previamente validada y verificada con el fin de garantizar la estabilidad al momento de ejecutarlas en cada Sistema Operativo, previniendo algunos problemas como sobrecargas de memoria, bugs en los programas o deterioro del hardware.

- Es importante ser conscientes de la necesidad de proteger la información almacenada en los Smartphone, cada día es mayor el número de usuarios que los utilizan y guardan datos sensibles en ellos. Este documento permitió comprobar que un Sistema Operativo Móvil puede llegar a ser vulnerable si se realizan modificaciones diferentes a las establecidas de fábrica y que la información almacenada en ellos puede ser extraída mediante prácticas sencillas colocando en riesgo la privacidad del usuario.

- Resulta imposible considerar que exista un sistema cien por ciento seguro, sin embargo, hay medidas preventivas que se pueden implementar para procurar evitar ataques sobre teléfonos celulares inteligentes bajo cualquier ambiente, sea corporativo o personal. Luego de la investigación realizada y las pruebas ejecutadas sobre los dispositivos de muestra, fue posible desarrollar un manual de mejores prácticas para la protección de la información en Smartphone anexo a éste documento, que pretende ayudar a los propietarios de este tipo de dispositivos a tomar conciencia y proteger la información que contengan en ellos.

BIBLIOGRAFIA

ACIS. Ingeniería social. Bogotá: [citado 12 junio, 2013]. Disponible en Internet < URL: http://www.acis.org.co/fileadmin/Base_de_Conocimiento/V_Jornada_de_Seguridad/IngenieraSocial_CarlosBiscione.pdf>

ACISSI. Seguridad Informática Ethical Hacking, Conocer el ataque para una mejor defensa. Bogotá: Mc Graw Hill, 2008.p. 17.

ALEGSA. Vulnerabilidad. Bogotá: [citado 13 agosto, 2013]. Disponible en Internet < URL : http://www.alegsa.com.ar/Dic/vulnerabilidad.php>

ALEQSA. Los RSA. Bogotá: [citado 1 junio, 2013]. Disponible en Internet < URL http://www.alegsa.com.ar/Dic/rsa.php>

ALEQSA. MicroSD. Bogotá: [citado 12 junio, 2013]. Disponible en Internet < URL: http://www.alegsa.com.ar/Dic/microsd.php>

ALVAREZ, Josué. Integridad. Bogotá: [citado 12 junio, 2013]. Disponible en Internet < URL: http://neo.lcc.uma.es/evirtual/cdd/tutorial/red/icmp.html>

ANDROID. Evolución histórica de los Smartphone. Bogotá: [citado 12 agosto, 2013]. Disponible en Internet < URL : http://www.android.es/historia-del-smartphone.html#axzz1dGLIi1ec>

APPLDNLD. Procedimiento de Jailbreaking. Bogotá: [citado 7 agosto, 2013]. Disponible en Internet < URL : http://appldnld.apple.com/iPhone4/061-9853.20101122.Vfgt5/iPhone1,2_4.2.1_8C148_Restore.ipsw>

APPLE. ¿Qué es una AppStore? [en línea]. Bogotá: [citado 26 junio, 2013]. Disponible en Internet : < URL: Tomado de: http://www.apple.com/osx/apps/app-store.html>

APPLE. ¿Qué son los iOS? Bogotá: [citado 12 junio, 2013]. Disponible en Internet < URL: http://www.apple.com/es/ios/what-is/>

ARRIETA. Marlen. Emparejamiento. [en línea]. Bogotá: [citado11 julio, 2013]. Disponible en Internet < URL: http://www.seguridadmobile.com/bluetooth/seguridad-bluetooth/sniffar-emparejamiento-Bluetooth.html>

ARTEMISA. Análisis forense en dispositivos móviles. Bogotá: [citado 12 agosto, 2013]. Disponible en Internet < URL:http://artemisa.unicauca.edu.co/~rhernandez/articulos/Articulo_UPM-Criptored_Symbian_OS_Forensics_UJaveriana.pdf>

BANCOVIMIENDA. Fraudes informáticos. Bogotá: [citado 28 julio, 2013]. Disponible en Internet < URL: http://www.bancovimenca.com/html/fraude_electronico.html>

BECERRA, Luis. Logs. Bogotá: [citado 12 junio, 2013]. Disponible en Internet < URL: http://www.desarrolloweb.com/faq/408.php>

BERTOLINI, Javier. Seguridad de la información redes informática y sistemas de información. Bogotá: Mc Graw Hill, 2001.p. 15.

CASTRO. Julián. Bogotá: [citado 2 julio, 2013]. Disponible en Internet < URL: http://www.desarrolloweb.com/articulos/513.php>

CONTRERAS, Fabio. PDA. Bogotá: [citado 8 junio, 2013]. Disponible en Internet < URL http://www.masadelante.com/faqs/que-es-un-pda>

CORDERO, Luis. Seguridad informática. Bogotá: [citado 11 junio, 2013]. Disponible en Internet < URL : http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf>

CORREDOR. Malvare. Bogotá: [citado 12 junio, 2013]. Disponible en Internet < URL: http://aprenderinternet.about.com/od/SeguridadPrivacidad/a/Que-Es-Malware.htm>

DEFINICION ABC. Confidencialidad. [en línea]. Bogotá: [citado17 julio, 2013]. Disponible en Internet < URL:http://www.definicionabc.com/comunicacion/confidencialidad.php>

DIARIO EL PAÍS. Froyo. Bogotá: [citado 2 julio, 2013]. Disponible en Internet < URL:http://tecnologia.elpais.com/tecnologia/2010/05/21/actualidad/1274432462_850215.html>

DIARIO EL TIEMPO. Protección de la Información. Bogotá: [citado 11 junio, 2013]. Disponible en Internet < http://m.eltiempo.com/tecnologia/telecomunicaciones/smartphones-en-colombia/10117907>

DIAZ, Gabriel. Los RIM. Bogotá: [citado 5 junio, 2013]. Disponible en Internet < URL http://www.venio.info/pregunta/que-es-rim-548.html>

DIAZ, J. Sistema Androide. [en línea]. Bogotá: [citado 26 junio, 2013]. Disponible en Internet : < URL: Tomado de: https://sites.google.com/site/androtechrd/ >

DURAN, Camilo. Simetría. Bogotá: [citado 1 junio, 2013]. Disponible en Internet < URL : http://www.virusprot.com/art1.html>

DURAN, Diana. Root. Bogotá: [citado 6 agosto, 2013]. Disponible en Internet < URL http://www.poderpda.com/plataformas/android/android-root/>

ENCICLOPEDIA EN LINEA. Encripción. [en línea]. Bogotá: [citado11 julio, 2013]. Disponible en Internet < URL: http://enciclopedia.us.es/index.php/Heur%C3%ADstica>

ESET. Pérdida o robo de datos. . Bogotá: [citado 12 agosto, 2013]. Disponible en Internet < URL : http://www.eset-la.com/pdf/documento_guia_de_seguridad_para_usuarios_de_smartphone_baj.pdf>

ESET.LA. Drive-By-Download. [en línea]. Bogotá: [citado11 julio, 2013]. Disponible en Internet < URL: http://www.eset-la.com/centro-amenazas/articulo/drive-by-download-infeccion-web/1792>

EURAM. Os. Bogotá: [citado 12 junio, 2013]. Disponible en Internet < URL http://www.euram.com.ni/pverdes/verdes_informatica/informatica_al_dia/que_es_un_so_144.htm >

FIGUEREDO. Hugo. Glosario. Bogotá: [citado 20 junio, 2013]. Disponible en Internet < URL : http://www.internetglosario.com/560/Spam.html>

FONTALVO; Gilma. Los DFU. [en línea]. Bogotá: [citado11 julio, 2013]. Disponible en Internet < URL: http://theiphonewiki.com/wiki/DFU_Mode>

FORERO, Julio. Que es el BIT. [en línea]. Bogotá: [citado11 julio, 2013]. Disponible en Internet < URL: http://www.masadelante.com/faqs/bit>

GARCIA, Josefina. SSH. Bogotá: [citado 16 agosto, 2013]. Disponible en Internet < URL : http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/ch-ssh.html>

GOMEZ, Héctor. Cracker. [en línea]. Bogotá: [citado2 agosto, 2013]. Disponible en Internet < URL:http://www.informatica-hoy.com.ar/aprender-informatica/Que-es-un-Cracker.php>

GOOGLE. Google play. Bogotá: [citado 2 agosto, 2013]. Disponible en Internet < URL: http://play.google.com/intl/es/about/index.html#utm_source=HA_Desktop_CO&utm_medium=GDN&utm_campaign=gplaunch>

GUARZIZO. Sonia. Procedimiento de Jailbreaking. Bogotá: [citado 2 agosto, 2013]. Disponible en Internet < URL : http://theiphonewiki.com/wiki/index.php?title=Redsn0w>

GUPEA. Penetration Testing of Android-based Smartphones. Bogotá: [citado 12 agosto, 2013]. Disponible en Internet < URL : http://gupea.ub.gu.se/bitstream/2077/27864/1/gupea_2077_27864_1.pdf/

HIGUERA, Fanny. Tethering. Bogotá: [citado 1 junio, 2013]. Disponible en Internet < URL : http://www.idamovil.com/que-es-tethering-como-compartir-tu-conexion-de-internet-del-iphone/ >

HUGHES. Los TDD. Bogotá: [citado 17 julio, 2013]. Disponible en Internet < URL : http://www.hughes.com/HNS%20Library%20For%20Products%20%20Technology/Administracion_Airlink.pdf>

IETF. Definición de Handovers. Bogotá: [citado 12 junio, 2013]. Disponible en Internet < URL: http://www.ietf.org/rfc/rfc4068.txt>

INEGI. Metadata. Bogotá: [citado 12 junio, 2013]. Disponible en Internet < URL: http://antares.inegi.gob.mx/metadatos/metadat1.htm>

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Trabajos escritos: presentación y referencias bibliográficas. Sexta actualización. Bogotá: ICONTEC, 2008. 110 p.

IPHONEOSX. Cydia. . [en línea]. Bogotá: [citado11 julio, 2013]. Disponible en Internet < URL: http://iphoneosx.com/cydia/>

JIMENEZ. Gabriel. Wireless. Bogotá: [citado 17 junio, 2013]. Disponible en Internet < URL : http://www.masadelante.com/faqs/wireless>

KIOSKEA. Los SD. Bogotá: [citado 17 junio, 2013]. Disponible en Internet < URL http://es.kioskea.net/contents/pc/sd-secure-digital.php3>

LOPEZ, Gregorio. Wifi. Bogotá: [citado 1 junio, 2013]. Disponible en Internet < URL : http://www.aulaclic.es/articulos/wifi.html>

LUGO, G. ¿Qué es PuTTY? Bogotá: [citado 22 agosto, 2013]. Disponible en Internet < URL http://www.desarrolloweb.com/articulos/putty.html>

LUGO. Julio. Los wraper. Bogotá: [citado 1 junio, 2013]. Disponible en Internet < URL : http://joomla.org.ar/tutoriales/uso-de-wrapper-contenido-externo.html >

MACROPLANT. Cracking de Password. Bogotá: [citado 2 agosto, 2013]. Disponible en Internet < URL : http://www.macroplant.com/iexplorer/download-pc.php>

MEZA, Jorge Iván. Definiciones. [en línea]. Bogotá: [citado 23 junio, 2013]. Disponible en Internet : < URL: <http://blog.jorgeivanmeza.com/2010/10/cifrado-y-descifrado-simetrico-con-rijndael-aes-utilizando-cmono/>

MICROSOFT. Definiciones y conceptos. [en línea]. Bogotá: [citado 26 junio, 2013]. Disponible en Internet : < URL: http://msdn.microsoft.com/en-us/library/windows/desktop/aa374872(v=vs.85).aspx>

MIGRACIONES. Exchange. Bogotá: [citado 21 agosto, 2013]. Disponible en Internet < URL: http://www.migraciones.gob.pe/Informacion/INF%20TEC%20SOFTWARE.pdf{En Línea} {Visitado>

MISSRESPUESTAS. Mp3. Bogotá: [citado 1 junio, 2013]. Disponible en Internet < URL http://www.misrespuestas.com/que-es-mp3.html>

MOLINA, Alberto. MDNS. Bogotá: [citado 12 junio, 2013]. Disponible en Internet < URL: http://albertomolina.wordpress.com/2008/07/07/utilizando-mdns-en-una-red-local/>

MONTOYA, José. Definiciones. [en línea]. Bogotá: [citado11 julio, 2013]. Disponible en Internet < URL: http://www-03.ibm.com/systems/es/information_infrastructure/solutions/information_availability/>

MORA, Rogelio. Disponibilidad. . Bogotá: [citado 1 agosto, 2013]. Disponible en Internet < URL:http://www.iso27000.es/glosario.html#section10c>

MORENO, Gisell. Zeroconf. Bogotá: [citado 1 junio, 2013]. Disponible en Internet < URL : http://computer.yourdictionary.com/zeroconf>

MOSQUERA, Henry. Confidencialidad. Bogotá: [citado 11 junio, 2013]. Disponible en Internet < URL : http://www.iso27000.es/glosario.html#section10c>

NMAP. Escaneo. Bogotá: [citado 22 agosto, 2013]. Disponible en Internet < URL : http://nmap.org/:es>

QPS. Que es una GPS. Bogotá: [citado 12 junio, 2013]. Disponible en Internet < URL: http://www.gps.gov/spanish.php >

REVISTA ENTER. Los ataques móviles. Bogotá: [citado 12 agosto, 2013]. Disponible en Internet < URL : http://www.enter.co/seguridad-y-privacidad/los-ataques-moviles-estan-cerca-de- duplicarse-ibm/ >

REVISTA ITNOW. Compañía Ericsson. Bogotá: [citado 1 junio, 2013]. Disponible en Internet < URL : http://revistaitnow.com/noticias-itu/on-los-datos-moviles-el-futuro-negocio-de-las-telecomunicaciones-2/>

RINCON, Lisbeth. Home Banking. Bogotá: [citado 12 junio, 2013]. Disponible en Internet < URL: http://www.bcra.gov.ar/pdfs/snp/SNP0165.pdf>

ROJAS, MANUEL Criptografía. Bogotá: [citado 12 agosto, 2013]. Disponible en Internet < URL : http://bvs.sld.cu/revistas/aci/vol11_6_03/aci11603.htm>

ROMERO, Giovanni. Historia de la Seguridad digital. Bogotá: [citado 12 agosto, 2013]. Disponible en Internet < URL : http://www.seguridaddigital.info/index.php?option=com_content&task=view&id=23&Itemid=26>

ROMERO, Luis. Boot. [en línea]. Bogotá: [citado 26 junio, 2013]. Disponible en Internet : < URL : http://www.alegsa.com.ar/Dic/boot.php>

RONCANCIO, Luis. Cifrado. [en línea]. Bogotá: [citado 11 julio, 2013]. Disponible en Internet < URL: http://www.mitecnologico.com/Main/Cifrado>

RUIZ, Martha. Arquitectura del sistema operativo. Bogotá: [citado 12 agosto, 2013]. Disponible en Internet < URL : http://images.apple.com/iphone/business/docs/iOS_Security_Oct12.pdf>

SALAZAR. Diana. Modelo para medir madurez. Bogotá: [citado 2 agosto, 2013]. Disponible en Internet < URL : http://ufh.netd.ac.za/jspui/bitstream/10353/281/1/SA%20%28200481118%29%20Dissertation.pdf >

SANCHEZ, José. Ingeniería de Proyectos Informáticos: Actividades y Procedimientos. México: Paidos, 2000.p. 170.

SOFTWARE LIBRE. Los Hacker. Bogotá: [citado 12 junio, 2013]. Disponible en Internet < URL: http://www.softwarelibrecr.org/faq/hacker>

SOLANO, Gregorio. Procedimiento de Jailbreaking. Bogotá: [citado 2 agosto, 2013]. Disponible en Internet < URL : http://blog.iphone-dev.org/>

SOTELO, Juan. Procedimiento de Jailbreaking. Bogotá: [citado 8 agosto, 2013]. Disponible en Internet < URL : http://theiphonewiki.com/wiki/index.php?title=DFU_Mode>

SOTELO, Luis. Los DES. [en línea]. Bogotá: [citado11 julio, 2013]. Disponible en Internet < URL: http://www.tierradelazaro.com/public/libros/des.pdf>

SUAREZ, Hugo. ICPM. : [citado 12 junio, 2013]. Disponible en Internet < URL: http://neo.lcc.uma.es/evirtual/cdd/tutorial/red/icmp.html >

SUPPOR APPLE. Preparación de dispositivos. Bogotá: [citado 12 agosto, 2013]. Disponible en Internet < URL : http://support.apple.com/kb/HT3743?viewlocale=es_ES#>

SYMANTEC. Los Smartphone. Bogotá: [citado 1 junio, 2013]. Disponible en Internet <http://www.symantec.com/content/es/mx/enterprise/images/theme/mobility/America-Latina-2012-State-of-Mobility-Survey-Report-SPA.pdf>

SYMANTEC. Aplicaciones. Bogotá: [citado 11 junio, 2013]. Disponible en Internet < URL : http://www.symantec.com/content/es/mx/enterprise/images/theme/mobility/America-Latina-2012-State-of-Mobility-Survey-Report-SPA.pdf>

SYMATEC. Seguridad digital. Bogotá: [citado 12 agosto, 2013]. Disponible en Internet < URL : http://www.symantec.com/content/en/us/about/media/pdfs/symc_mobile_device_security_june2011.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011Jun_worldwide_mobilesecuritywp>

TENABLE. Escaneo. Bogotá: [citado 2 agosto, 2013]. Disponible en Internet < URL : http://www.tenable.com/products/nessus>

UTPL. IEEE. Bogotá: [citado 12 junio, 2013]. Disponible en Internet < URL: http://www.utpl.edu.ec/ieee/?p=4

VIAFORENSICS. Advancements in Android Forensics. Bogotá: [citado 2 agosto, 2013]. Disponible en Internet < URL : http://viaforensics.com/services/mobile-forensics/android-forensics/ >

WIKITE. FDD. Bogotá: [citado 12 agosto, 2013]. Disponible en Internet < URL: http://es.wikitel.info/wiki/FDD>

ANEXOS

Anexo A. Mejores Prácticas y Recomendaciones Para Salvaguardar la Información en Smartphone con Sistema Operativos iOS.

INTRODUCCIÓN

Al igual que las amenazas informáticas en general, los códigos maliciosos han ido evolucionando a la par de las tecnologías de información y comunicación, aumentando considerablemente el nivel de complejidad y agresión.

Es necesario que los usuarios inicien con la implementación de buenas prácticas para proteger el entorno de información, y disminuir aún más la posibilidad de formar parte de potenciales y eventuales víctimas de cualquiera de las amenazas, que constantemente buscan sacar provecho de las debilidades de cada uno de los usuarios de dispositivos inteligentes. Para ello, inevitablemente se deben conocer los peligros latentes y cómo detenerlos a través de mecanismos de prevención.

El presente documento expone medidas preventivas de seguridad tendientes a minimizar el volumen de “Riesgos y Vulnerabilidades”; brinda herramientas preventivas para las tecnologías y servicios más populares y más utilizados por los usuarios y aborda en cada punto los mecanismos de prevención que permiten detectar, de manera temprana y sin acciones complejas, las operaciones maliciosas más comunes.

Cuando se tiene control físico sobre los Smartphone se puede llegar a pensar que estos dispositivos son menos accesibles a intrusos, claro está que los usuarios en muchas ocasiones desconocen que las conexiones por medio de bluetooth y red inalámbrica, se pueden realizar sin tener contacto físico con el dispositivo. Esta falsa sensación de seguridad junto con el uso de aplicaciones del estilo del correo electrónico, redes sociales y contenido multimedia privado, conlleva al almacenamiento de datos personales y confidenciales en el dispositivo móvil, muchas veces de forma inadvertida para el usuario. Esto conduce a que los usuarios descuiden las precauciones básicas tales como cambiar la configuración de seguridad por defecto.

1. MANTENER ACTUALIZADO EL SISTEMA

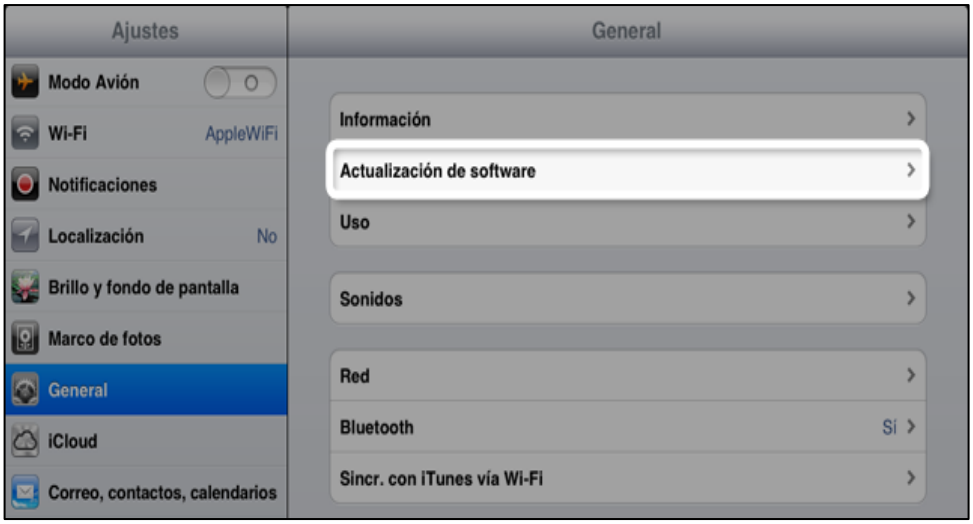
No descargar actualizaciones desde sitios de dudosa reputación y hacerlo sólo desde sitios de confianza (Fabricantes de aplicaciones y AppStore de Apple) pues cuentan con protocolos de cifrado (HTTPS) y certificados de seguridad, descargar las actualizaciones desde sitios no oficiales implica un potencial riesgo de infección. Descargar las actualizaciones a través de los mecanismos ofrecidos por el fabricante. En el caso de las actualizaciones de productos de Apple, la disponibilidad de los mismos es informada cada mes, aunque puede haber excepciones en casos de vulnerabilidades críticas.

Para las plataformas de Apple se puede:

Acceder al sitio web de Apple[105]para obtener los últimos parches de seguridad y configurar el centro de seguridad de cada dispositivo para presentar una alternativa de mayor confianza, es necesario recordar que las compañías desarrolladores encuentran nuevas amenazas día a día y los parche de seguridad que se ofrecen para mejor la protección del dispositivo.

Utilizar herramientas para verificar la falta de actualizaciones en el sistema operativo, en iOS de Apple a través de iTunes se comprueba automáticamente si hay actualizaciones disponibles.

Figura 1. Actualización iOS



Fuente: Los autores

[105]SUPPORT APPLE. Preparación de dispositivos. Bogotá: [citado 12 agosto, 2013]. Disponible en Internet < URL : http://support.apple.com/kb/HT3743?viewlocale=es_ES#>

2. ASEGURAMIENTO DEL SISTEMA OPERATIVO

Otro de los aspectos importantes en materia de prevención, radica en configurar el sistema operativo para hacerlo más seguro. Entre las buenas prácticas que se pueden tener en cuenta se encuentran:

Deshabilitar conexiones Bluetooth y Wi-Fi si no se están utilizando. Esto evita la propagación de gusanos informáticos (virus que invaden el sistema operativo del dispositivo y generar huecos de seguridad) que aprovechen ese servicio como método de infección. El Bluetooth, una tecnología bastante potente y útil para la transmisión de datos y voz como lo es por ejemplo el (manos libres que se usa en para contestar las llamadas telefónicas dentro de un vehículo), pero su nivel de seguridad no lo es tanto cuando deja de usarse, ya que la conexión sigue abierta y la espera de recibir o enviar datos (genera un canal de comunicación por medio del cual es posible la extracción de información).

Figura 2. Configuración de Wi-Fi y Bluetooth

Fuente: Los autores

En el aseguramiento del sistema operativo es recomendable contar con el apoyo de un antivirus actualizado, en lo posible con algunas funciones específicas tales como: cortafuegos (Firewall), el cual evita ataques no autorizados por personas o software malicioso, anti spam para evitar correo basura, anti espías para evitar accesos no autorizados, etc. A partir de agosto del 2010 la firma de antivirus ESET lanzó una aplicación para la protección del iOS de Apple[106]. No obstante existen otras soluciones de antivirus de otros fabricantes como Norton Symantec el cual está disponible para iPhone en el AppStore[107]. De esta misma forma hay otras

[106] ARTEAGA. Cortafuegos. Bogotá: [citado 12 agosto, 2013]. Disponible en Internet < URL : :http://blogs.eset-la.com/corporativo/2010/08/27/nueva-aplicacion-eset-ipad-iphone-ipod-touch/>

[107] ITUNES. iPhone en el AppStore. . [en línea]. Bogotá: [citado 23 junio, 2013]. Disponible en Internet : < URL: http://itunes.apple.com/us/app/symantec-mobile-management/id459307928?mt=8>

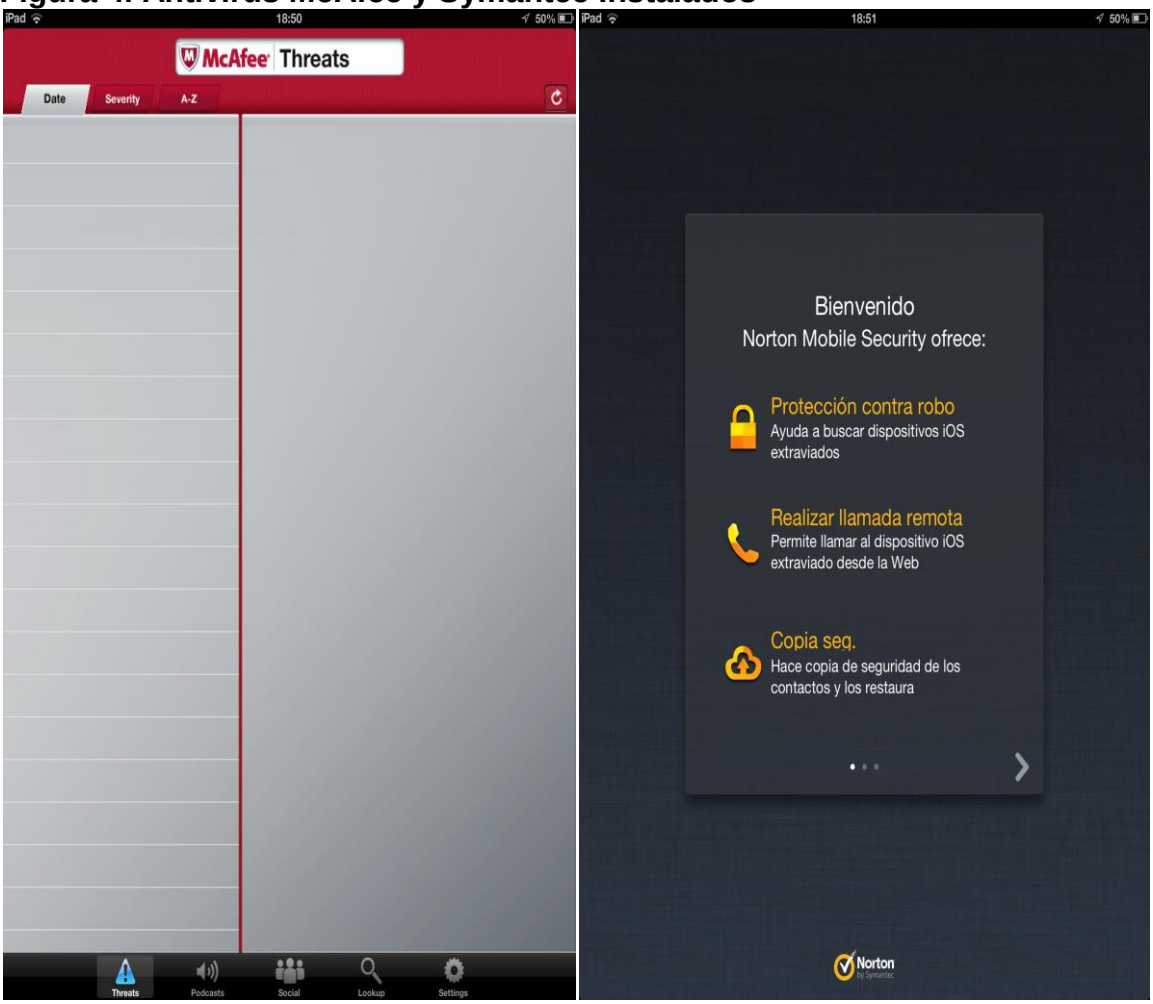
corporaciones desarrolladoras de antivirus que pueden contribuir con la seguridad de los Smartphone. Lo importante es contar con uno instalado y actualizado. Cabe reiterar que se aconseja descargar estas aplicaciones directamente desde el AppStore.

Figura 3. Antivirus para iPhone

Fuente: Los autores

En la siguiente imagen se evidencian dos soluciones de antivirus instaladas, se recomienda que se instale un solo antivirus para que no se genere ningún conflicto que llegue a afectar la estabilidad y rendimiento del dispositivo.

Figura 4. Antivirus McAfee y Symantec Instalados



Fuente: Los autores

Utilizar contraseñas fuertes[108]. El empleo de contraseñas simples (De corta longitud, con ausencia de caracteres especiales, números y variaciones entre mayúsculas y minúsculas) es otra de las debilidades que los códigos maliciosos suelen aprovechar para propagarse por los recursos de información. Es decir, una contraseña fuerte puede ser: E@n2013!, una clave de varios caracteres alfanuméricos, y caracteres especiales. La cual se puede configurar en ajustes/ Ubicación y seguridad. Para esta generación de claves seguras se puede apoyar con páginas web como la siguiente: http://password.es/comprobador/

[108] Fonseca, Juian. Contraseñas consistentes. . [en línea]. Bogotá: [citado 23 junio, 2013]. Disponible en Internet : < URL: :http://www.eset-la.com/threat-center/2037-seguridad-contrasenas>

Figura 5. Comprobador de contraseñas

Fuente: Los autores

3. ASEGURAMIENTO A NIVEL CORPORATIVO

En ambientes corporativos, la información contenida en Smartphone puede ser sensible para la organización y muchas organizaciones entregan dispositivos iOS para que sus empleados aumenten su productividad y su disponibilidad en el trabajo.

Dado que el dispositivo móvil empieza a ejecutar un rol de herramienta de trabajo, los datos contenidos en él son de gran importancia para las empresas y en muchos casos puede llegar a ser confidencial.

MDM (Administración Remota de Dispositivo, del inglés, Mobile Device Management) es un software que permite administrar remotamente dispositivos móviles de forma centralizada a nivel organizacional.[109]

El marco MDM integrado en iOS ofrece la capacidad de interactuar inalámbricamente con los dispositivos iOS que son administrados por organizaciones. Otros fabricantes, utilizan este marco para construir servicios MDM que se comunican con los dispositivos iOS.

MDM ofrece a los departamentos de TI la posibilidad de:

- Registrar con seguridad los dispositivos en un entorno empresarial
- Configurar y actualizar la configuración del dispositivo
- Monitorear el cumplimiento de las políticas corporativas
- Limpiar o bloquear los dispositivos gestionados de forma remota.

El uso de un servidor MDM ofrece a las organizaciones una gestión sencilla a los usuarios que acceden a los servicios de la empresa, independientemente de quién es el propietario del dispositivo adicionándolos a través de perfiles:

[109] TORRES, Gereardo. Administración remota de dispositivos en inglés. . [en línea]. Bogotá: [citado 23 junio, 2013]. Disponible en Internet : < URL: http://www.gartner.com/it-glossary/mobile-device-management-mdm/

Figura 6. Perfiles de MDM en iOS

Fuente. TARMAC. Cuentas de usuarios. . [en línea]. Bogotá: [citado 23 junio, 2013]. Disponible en Internet : < URL: http://www.tarmac-mdm.com/us/mdm.html>

Para iOS el framework de MDM tiene las siguientes características:

Gestión de cuentas de usuario. Gestión de cuentas de usuario corporativas que pueden originarse desde sistemas comunes de autenticación en organizaciones como:[110]

- Microsoft Active Directory Domain Services.
- Open Directory
- Open LDAP
- MySQL
- SAP[111]

Gestión de configuraciones. Configuración de características incluyendo contraseñas, restricciones del dispositivo y políticas de voz y roaming de datos.

- Estas pueden ser utilizadas para estandarizar el uso de códigos de bloqueo complejos en el iOS y no utilizar el código simple de cuatro dígitos numéricos.

[110] TARMAC. Cuentas de usuarios. . [en línea]. Bogotá: [citado 23 junio, 2013]. Disponible en Internet : < URL: http://www.tarmac-mdm.com/us/mdm.html>
[111] Ibid.,p. 2.

- Es posible prevenir la instalación de software, roaming de datos internacional, entre otras características de iOS, de modo que el dispositivo sea utilizado únicamente para fines laborales.

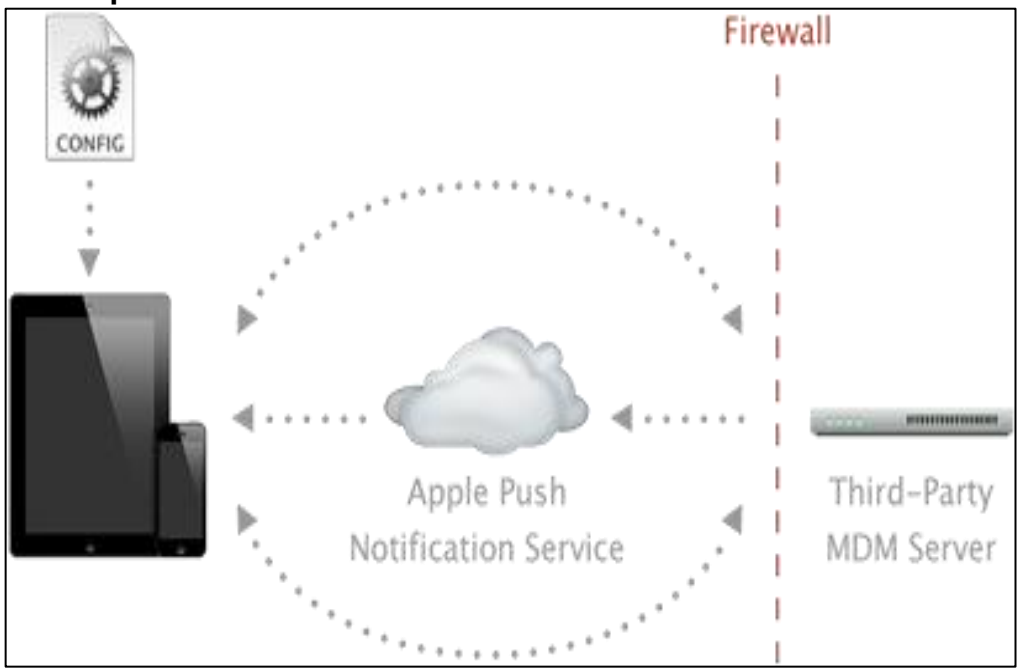
Gestión de aplicaciones. Despliegue, administración, y desinstalación de aplicaciones desde la AppStore o aplicaciones in-house.

Consultas al dispositivo. Programación de consultas del dispositivo como configuraciones, acceso a redes, aplicaciones e información del estado de seguridad.

Comandos de seguridad. Posibilidad de borrar la contraseña del usuario y bloquear o borrar de forma remota un dispositivo perdido o robado.

Arquitectura de MDM. Para establecer la primera conexión con un dispositivo iOS, los servidores de MDM utilizan el servicio Apple Push Notification. Una vez que el servidor se ha establecido una conexión, todas las tareas se llevan a cabo en el dispositivo por el marco integrado MDM en iOS. Este marco permite a los servidores de MDM mantenerse en contacto con el dispositivo sin afectar el rendimiento o la vida de la batería. También significa que no hay necesidad de que cada proveedor de soluciones MDM deba crear un agente suyo.

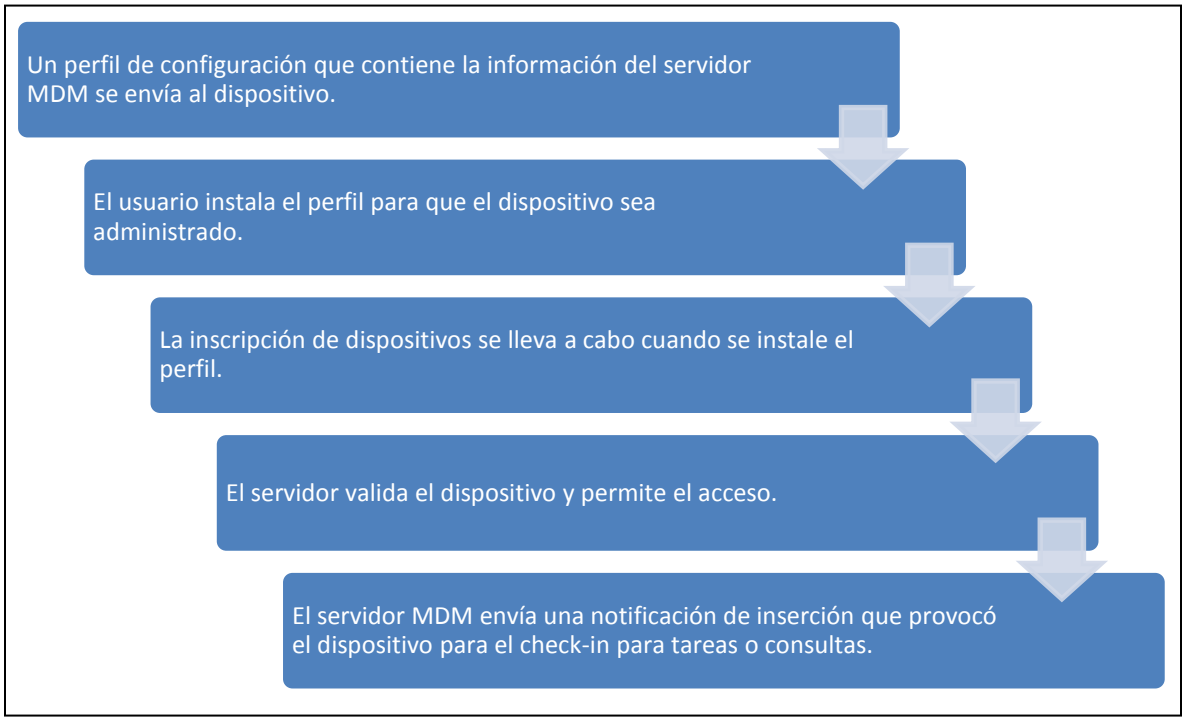
Figura 7. Arquitectura MDM



Fuente. TARMAC. Cuentas de usuarios. . [en línea]. Bogotá: [citado 23 junio, 2013]. Disponible en Internet : < URL: http://www.tarmac-mdm.com/us/mdm.html

Configuración de MDM. El proceso de configuración de MDM en dispositivos iOS es sencillo, independientemente del servidor MDM que se utilice el despliegue es el mismo:

Figura 8. Configuración de MDM en iOS



Fuente: Los autores

4. PROTECCIÓN EN EL CORREO ELECTRÓNICO

El correo electrónico constituye uno de los canales de propagación/infección de malware más utilizados por atacantes; por lo tanto es importante que los usuarios incorporen como hábito determinadas prácticas que permitan prevenir los ataques realizados a través de códigos maliciosos. A continuación se presenta una serie de medidas preventivas orientadas a aumentar la seguridad durante el uso del correo electrónico.

4.1 SPAM

El spam[112] es el correo electrónico que promociona diferentes productos y servicios a través de publicidad no solicitada y enviada masivamente a las direcciones de correo de los usuarios. Constituye uno de los principales medios de propagación de una importante cantidad de códigos maliciosos y por lo tanto se recomienda:

No confiar en correos de remitentes desconocidos, en el caso de contener archivos adjuntos, no abrirlos para prevenir la ejecución de algún malware.

Cuando se reciben adjuntos, prestar especial atención a las extensiones de los mismos, dado que suelen utilizar técnicas de engaño como la doble extensión o espacios entre el nombre del archivo y la extensión del mismo.

Evitar publicar las direcciones de correo en sitios web de dudosa reputación como sitios pornográficos, foros, chats, comercio electrónico y donaciones. Esto minimiza la posibilidad de que la dirección se guarde en la base de datos de los spammers.

No responder jamás el correo spam. Es preferible ignorarlos y/o borrarlos, ya que si se responde se confirma que la dirección de correo se encuentra activa.

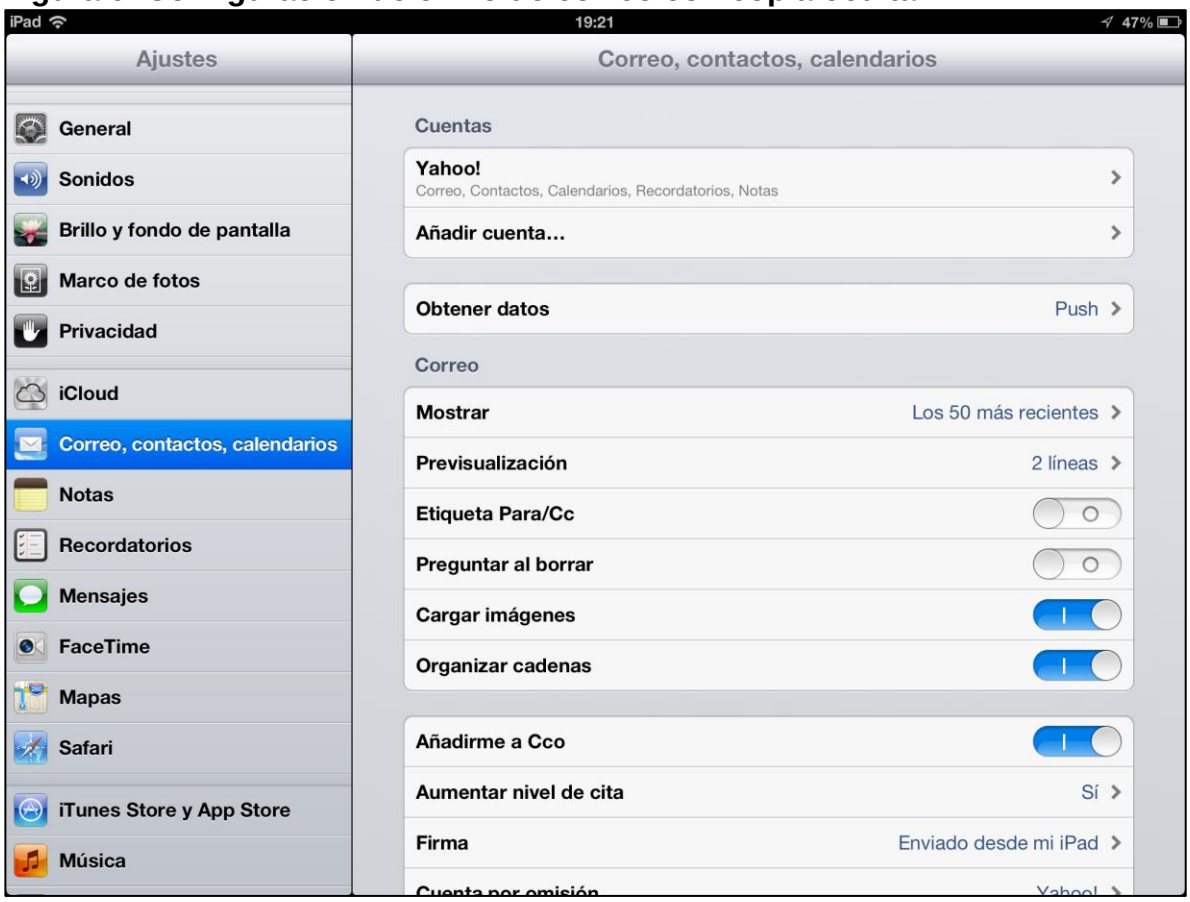
En lo posible, evitar el re-envío de mensajes en cadena[113], toda vez que suelen ser utilizados para recolectar direcciones de correo activas y hacer uso de técnicas de ataque como spam y phishing.

Si de todos modos se desea enviar mensajes en cadena, es recomendable hacerlo siempre con copia oculta (CCO) para que quien lo recibe lea solo la dirección del emisor.

[112]ESET. Spam. . [en línea]. Bogotá: [citado 23 junio, 2013]. Disponible en Internet : < URL: http://www.eset-la.com/threat-center/1639-spam-hoy-ahora-y-siempre>

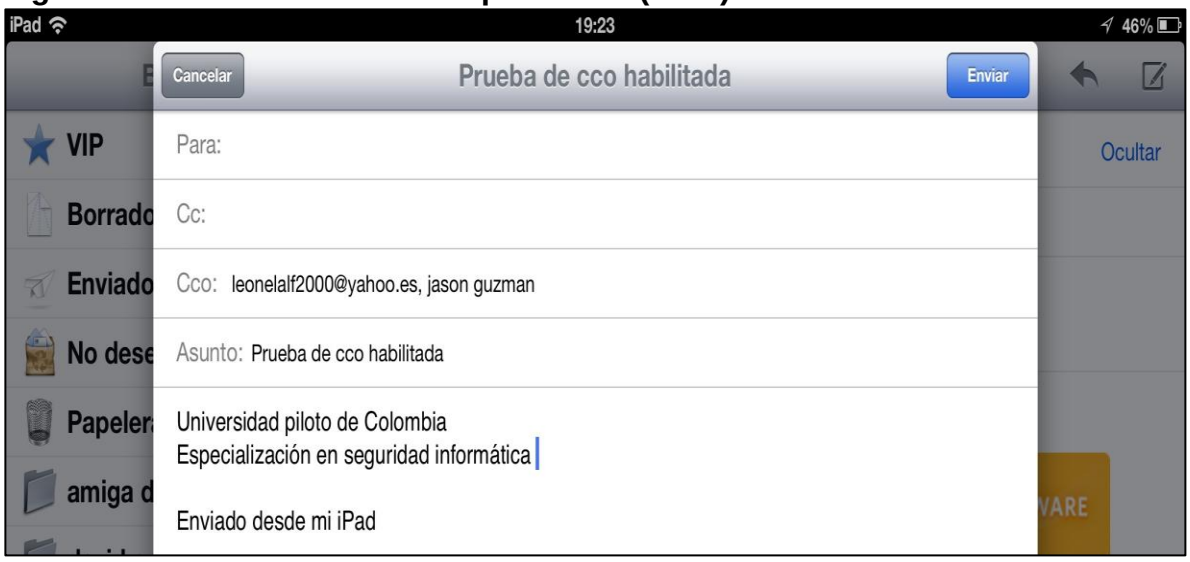
[113] PINEIRO. Oliva. Mensajes de cadena. . [en línea]. Bogotá: [citado 23 junio, 2013]. Disponible en Internet : < URL: http://www.segu-info.com.ar/malware/hoax.htm>

Figura 9. Configuración de envió de correo con copia oculta



Fuente: Los autores

Figura 10. Enviar correo con copia oculta (CCO)



Fuente: Los autores

Utilizar claves seguras y cambiar la contraseña con periodicidad si se utiliza el servicio de correo electrónico por medio de una página web. Esto favorece la seguridad de la información, puesto que hace más difícil el hallazgo mediante algunas técnicas.

Configurar la pregunta secreta (siendo este uno de los mecanismos de seguridad ofrecidos por los proveedores de correo electrónico) con palabras que no sean de fácil deducción para fortalecer aún más la seguridad de la información.

Como medida de seguridad extra, se sugiere evitar ir a enlaces externos de procedencia desconocida y descargar información de los mismos, teniendo en cuenta que estos sitios puede afectar la seguridad de la información

También es preferible que se evite ingresar el nombre de usuario y su respectiva contraseña en sitios de los cuales no se tenga referencia. De esta manera se preserva la privacidad de la cuenta de correo y, por ende, la información que se intercambia a través de la misma.

4.2 PHISHING

El phishing[114] es una modalidad delictiva encuadrada en la figura de estafa realizada a través de Internet, y constituye otra de las amenazas de seguridad más propagadas a través del correo electrónico. Entre las buenas prácticas de seguridad que se recomiendan a los usuarios, para que éstos eviten ser víctimas del phishing, están las siguientes:

Tener en cuenta que las entidades bancarias y financieras no solicitan datos confidenciales a través de este medio, de esta manera se minimiza la posibilidad de ser víctima de esta acción delictiva.

Desconfiar de los correos que dicen ser emitidos por entidades que brindan servicios y solicitan cambios de datos sensibles como nombres, número de cedula, contraseñas, números de cuentas, ya que suelen ser métodos de Ingeniería Social (obtener información por medio de engaños o datos que aparentan ser verídicos).

No ingresar a enlaces que aparecen en el cuerpo de los correos electrónicos, ya que pueden re-direccionar hacia sitios web clonados (sitios que aparentan ser legítimos a los originales, suele ser usado en páginas bancarias, redes sociales y proveedores de correo).

Asegurarse de que la dirección del sitio web de entidades financieras o comercio electrónico (o sitios que manipulen información confidencial) al cual se accede

[114]BANCO CAJA SOCIAL. Phishing. . [en línea]. Bogotá: [citado 23 junio, 2013]. Disponible en Internet : < URL: :https://www.bancocajasocial.com/tips-de-seguridad>

comience con el protocolo HTTPS. La "**s**" final, significa que la página web es segura[115] y que toda la información depositada en la misma viajará de manera cifrada.

Comunicarse telefónicamente con la compañía para descartar la posibilidad de ser víctima de un engaño, si se tiene dudas sobre la legitimidad de un correo.

Jamás se deben enviar contraseñas, números de tarjetas de crédito u otro tipo de información confidencial a través del correo electrónico, ya que la comunicación podría ser interceptada y robada.

Habituarse a examinar periódicamente la cuenta bancaria, a fin de detectar a tiempo alguna actividad extraña relacionada con la manipulación de la cuenta o transacciones no autorizadas.

Denunciar casos de phishing (dentro de lo posible) en la entidad de confianza, ya que además de cortar la actividad del sitio malicioso, se colabora con la seguridad general de la navegación en Internet.

[115]MICROSOFT. Definiciones y conceptos. [en línea]. Bogotá: [citado 26 junio, 2013]. Disponible en Internet : < URL: http://msdn.microsoft.com/en-us/library/windows/desktop/aa374872(v=vs.85).aspx>

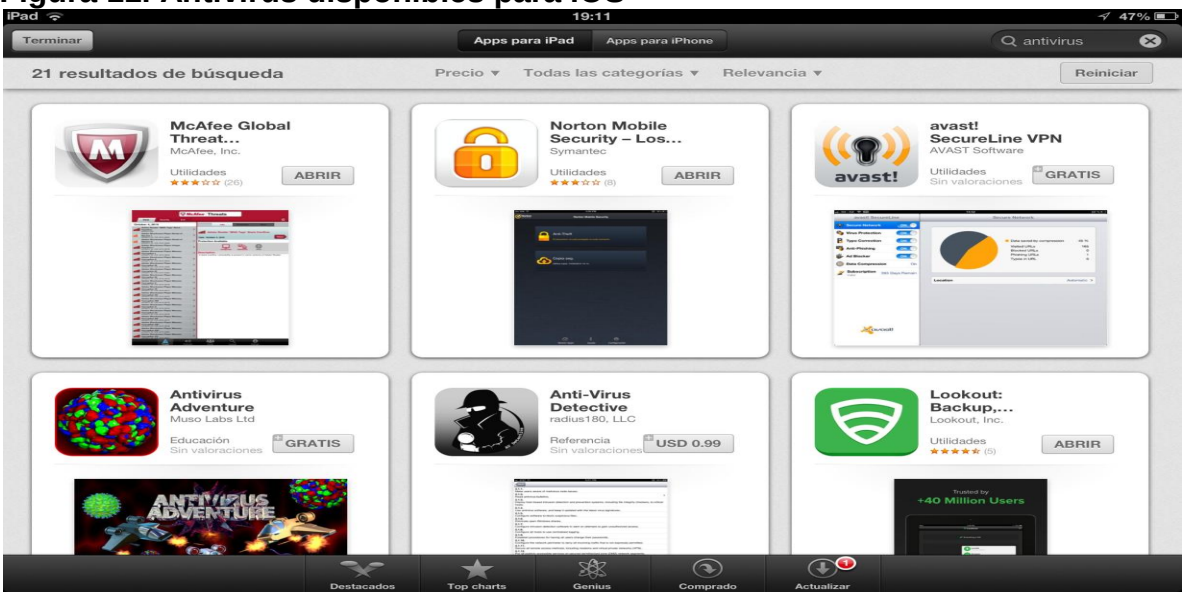
5. SEGURIDAD EN LA NAVEGACIÓN

En los últimos años, Internet se ha transformado en una plataforma de ataque[116]donde acciones delictivas se llevan a cabo a través de diferentes técnicas como por ejemplo el Drive-by-Download el cual permite infectar masivamente los dispositivos por medio de accesos web[117].En consecuencia, es fundamental navegar con cautela y tener presente las recomendaciones más importantes, entre ellas:

Descargar programas de seguridad solamente desde el sitio oficial del fabricante, es decir desde la AppStore, para evitar la descarga de archivos que pudieran ser previamente manipulados con fines delictivos.

Instalar, en lo posible, un programa antivirus con capacidades proactivas (es decir que analizan sin solicitud del usuario descargas y programas instalados), como ESET NOD32[118], Kaspersky[119] y Norton[120] entre otros, que permita detectar códigos maliciosos incluso desconocidos (aplicación que altera el funcionamiento correcto de las aplicaciones) y explorar con el mismo cada archivo descargado.

Figura 11. Antivirus disponibles para iOS



Fuente: Los autores

[116] ESET.,op.cit.,p. 3

[117] Ibid.,p. 3.

[118]Ibid.,p.6.

[119] KARPESKY. Antivirus. . [en línea]. Bogotá: [citado 26 junio, 2013]. Disponible en Internet : < URL:http://www.kaspersky.com/sp/kaspersky_mobile_security>

[120] NORTON. Antivirus. . [en línea]. Bogotá: [citado 26 junio, 2013]. Disponible en Internet : < URL: de :http://norton.symantec.com/norton/ps/3up_co_es_navnis360.html?om_sem_cid=hho_sem_ic:co:ggl:es:b|kw0000004480|10672096712&country=CO

Figura 12. Comparación de antivirus y los sistemas operativos soportados

Antivirus	Sistema Operativo	Características	Precio
AVG Antivirus	Android	Escáner de malware. Protección contra robo. Escudo de navegación Web. Filtro de mensajes SMS. Gestor de procesos.	Gratuito
Avast! Mobile Security	Android, BlackBerry, Symbian OS, Nokia	Escáner de aplicaciones y tarjeta SD. Asesor de privacidad. Administrador de apps. Escudo de navegación Web. Filtro de llamadas y SMS. Cortafuegos (requiere root). Antirrobo.	Gratuito y pago
Kaspersky Mobile Security 9	Android, BlackBerry, Symbian OS, Nokia	Antivirus en la Nube. Antirrobo. Filtro de llamadas y SMS. Opciones de privacidad.	Gratuito y pago
McAfee: WaveSecure	BlackBerry, Android, Symbian OS, Windows Mobile y Java	Envía mensaje SMS de manera oculta con el número de teléfono de la nueva SIM. Permite localizar el terminal desde la web del autor. Realiza copias de seguridad de los contactos. Bloquea el terminal.	Gratuito y pago
Lookout Mobile Security	Android, BlackBerry, Windows Mobile	Escáner antivirus. Programador de tareas. Localizador por GPS. Sistema antirrobo. Copias de seguridad. Navegación segura. Asesor de privacidad.	Gratuito y pago

Fuente: Los autores

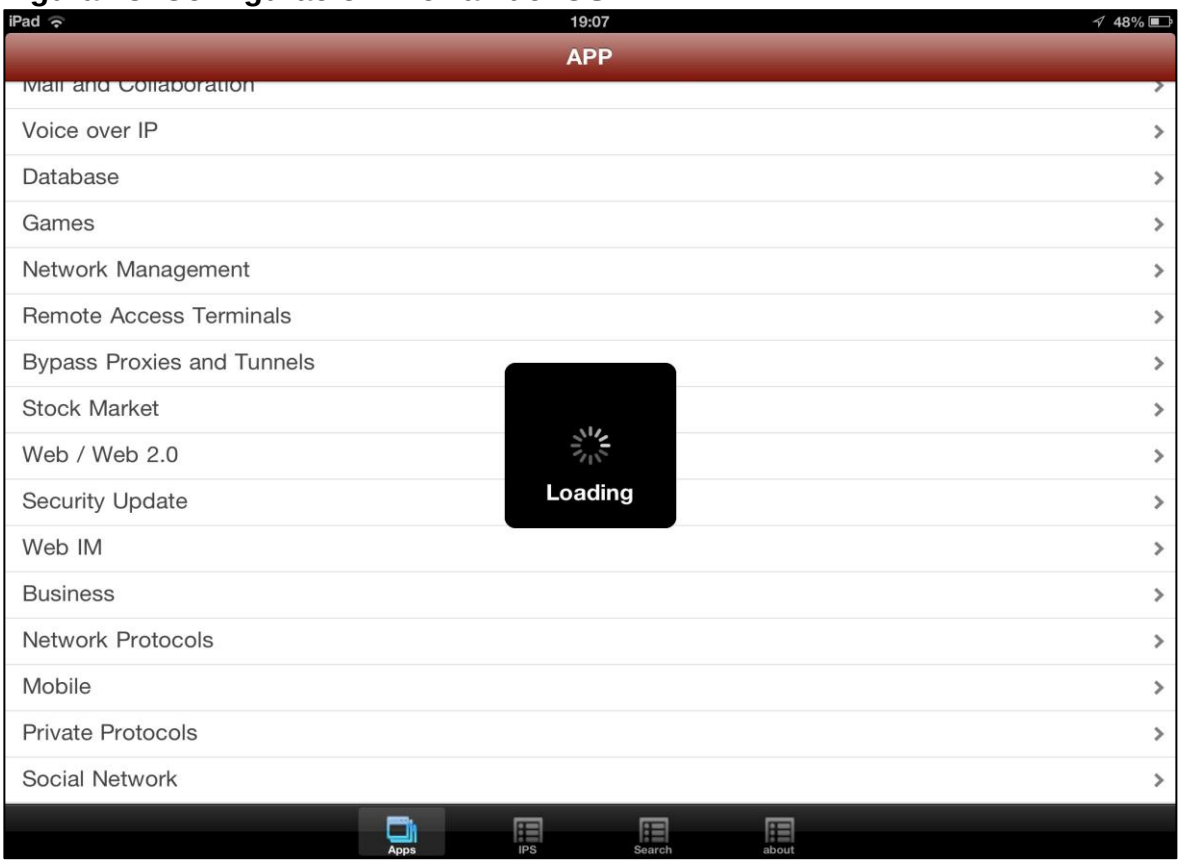
Tratar de no acceder a servicios como Home-Banking (transacciones financieras que se realizan generalmente desde un cajero electrónico) desde lugares públicos (bibliotecas, cafés, hoteles y centros comerciales.

Si se navega desde sitios públicos, es recomendable eliminar los archivos temporales, caché, cookies, direcciones URL, contraseñas y formularios donde se hayan ingresado datos.

El bloqueo de determinados sitios considerados maliciosos, ya sea porque descargan malware o porque contienen material de dudosa reputación, es también otra de las mejores prácticas que ayudan a la prevención y refuerzan la seguridad del equipo, por medio de la configuración de seguridad de cada navegador en los dispositivos.

Disponer, además, de un Firewall personal que permita bloquear comunicaciones entrantes y salientes.

Figura 13. Configuración firewall de iOS



Fuente: Los autores

ESET Smart Security, por ejemplo, incorpora un Firewall personal (WatchGuard security portal, ofrece una solución en dispositivos con iOS de Apple).

Evitar el ingreso a sitios web con contenidos ilegales, como aquellos que ofrecen crack; ya que constituyen canales propensos a la propagación de malware.

Impedir la ejecución de archivos desde sitios web sin verificar previamente que es lo que dice ser. Es importante no hacer clic sobre el botón **Instalar** ya que esto provoca que el archivo se ejecute automáticamente luego de descargado, dejando al margen la posibilidad de verificar su integridad.

En lo posible se recomienda, leer atentamente las políticas de privacidad de las aplicaciones descargadas desde sitios web no oficiales o de dudosa reputación, antes de instalarlas.

No realizar la instalación de complementos extras como aplicaciones recomendadas o protectores de pantallas sin verificar previamente su autenticidad.

6. SEGURIDAD EN REDES SOCIALES

En la actualidad, las redes sociales son muy populares[121] y los usuarios las utilizan masivamente; estas características las transforman en importantes focos de propagación de malware. Por tal motivo, se torna necesario tener en cuenta y aplicar las siguientes medidas preventivas:

No publicar información privada y confidencial, debido a que personas extrañas pueden aprovechar esta información con fines maliciosos.

También es recomendable evitar la publicación de fotografías propias y de familiares. Las fotografías pueden ser utilizadas para complementar actos delictivos, incluso fuera del ámbito informático (extorciones a familiares y amigos).

Mantener la privacidad del perfil; es decir, configurar el perfil para que no sea público por medio de las opciones de seguridad que ofrecen los sitios de redes sociales.

Figura 14. Herramientas de Privacidad

Fuente: Los autores

[121] SEMANA. Seguridad en redes sociales. . [en línea]. Bogotá: [citado 26 junio, 2013]. Disponible en Internet : < URL: http://www.semana.com/vida-moderna/redes-sociales-populares/140949-3.aspx>

No responder las solicitudes de desconocidos, ya que pueden contener códigos maliciosos o pueden formar parte de actividades delictivas en el dispositivo móvil.

Ignorar los mensajes que ofrecen material pornográfico, pues usualmente a través de ellos suele canalizarse la propagación de malware, además de otras acciones ofensivas en el dispositivo móvil.

No abrir contenidos con spam a través de este medio. De esta manera se evita formar parte del ciclo de vida del spam a través de este canal.
Cambiar periódicamente la contraseña para evitar que la misma sea descubierta fácilmente y evitar el almacenamiento de está en el dispositivo móvil.

Antes de aceptar contactos espontáneos, es recomendable verificar su existencia y que realmente provienen de quien dice ser. Esto se puede validar con la configuración de la cuenta personal en el Smartphone con iOS 4.2.1 o posteriores.

Figura 15. Configuración de seguridad

Fuente: Los autores

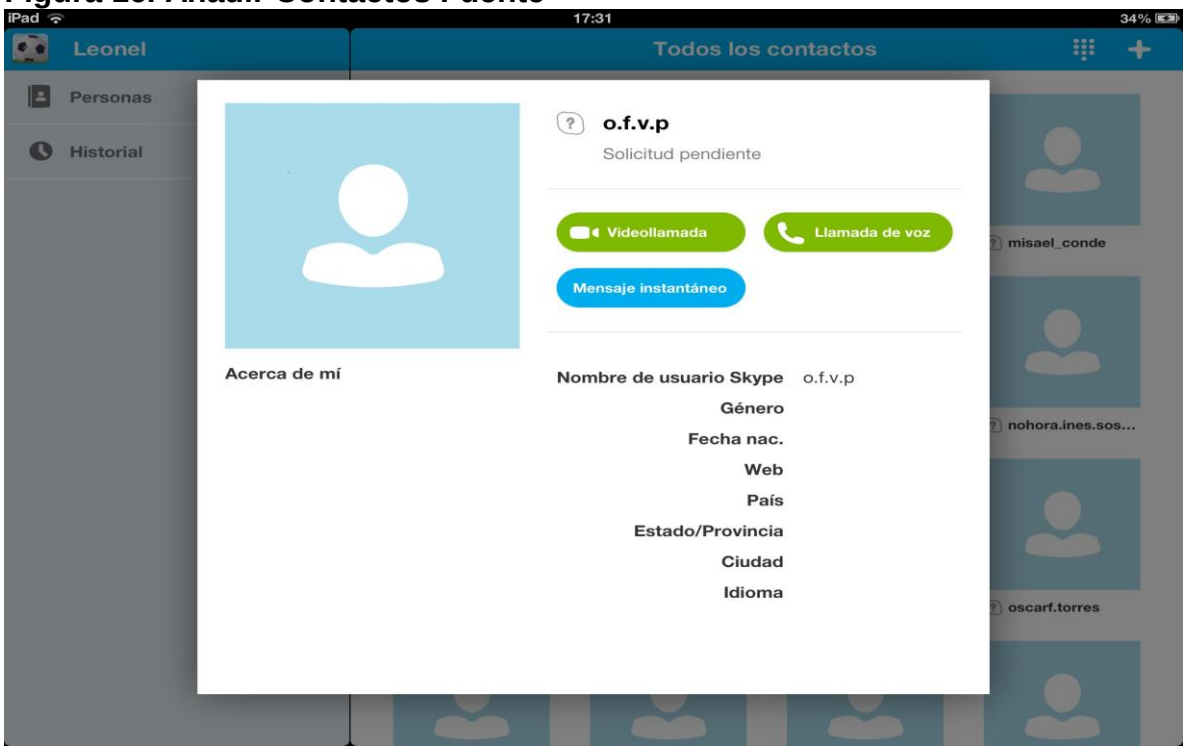
7. SEGURIDAD EN MENSAJERÍA INSTANTÁNEA

Otro medio de comunicación popular, y que se emplea masivamente, son los clientes de mensajería instantánea, que, en consecuencia, constituyen uno de los servicios más explotados por diferentes amenazas, dentro de las cuales una de las más activas es el malware.

Por tal motivo poner en ejecución medidas tendientes a volver más seguro el cliente de mensajería instantánea se transforma en una tarea casi obligada. Para prevenir ser víctimas de acciones maliciosas llevadas a cabo a través de esta tecnología, se recomienda aplicar alguna de las medidas de seguridad que a continuación se describen:

Evitar aceptar como contacto cuentas desconocidas sin verificar a quién pertenece, ya que en la mayoría de los casos se trata de intentos de engaños con fines maliciosos. Como se evidencia en la siguiente imagen, generalmente son dominios desconocidos y no de HOTMAIL por ejemplo (o.f.v.p@mobiuswoman.info), como se observa en la imagen número 12

Figura 16. Añadir Contactos Fuente

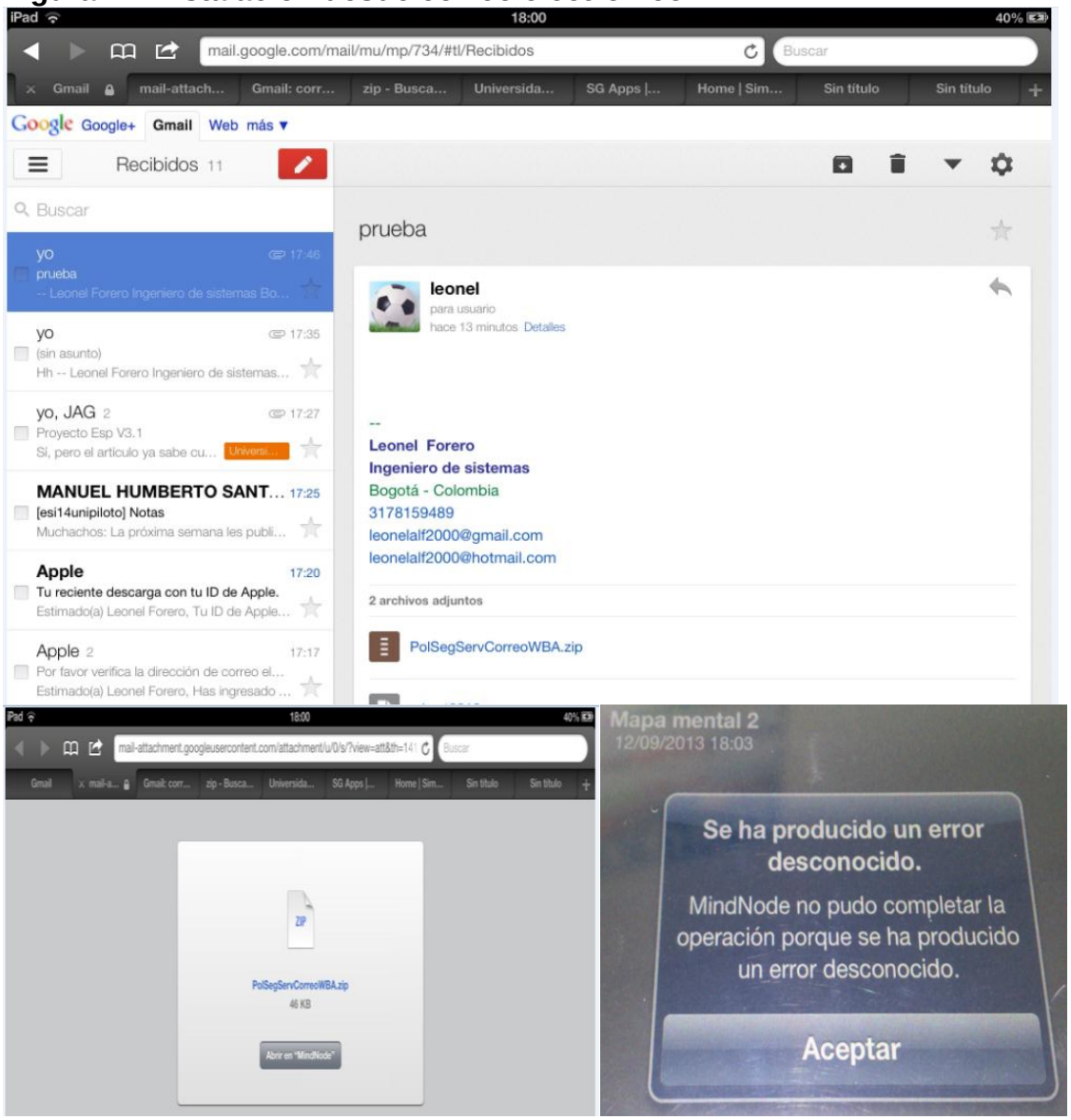


Fuente: Los autores

No descargar archivos sospechosos, sobre todo cuando vienen acompañados de mensajes genéricos o en otro idioma. Esto constituye una de las características principales de los códigos maliciosos que se propagan a través de este canal de

comunicación, en especial archivos con extensiones que pueden ser instaladores en los Smartphone, por ejemplo aplicaciones (*.ipa y algunos *.zip).

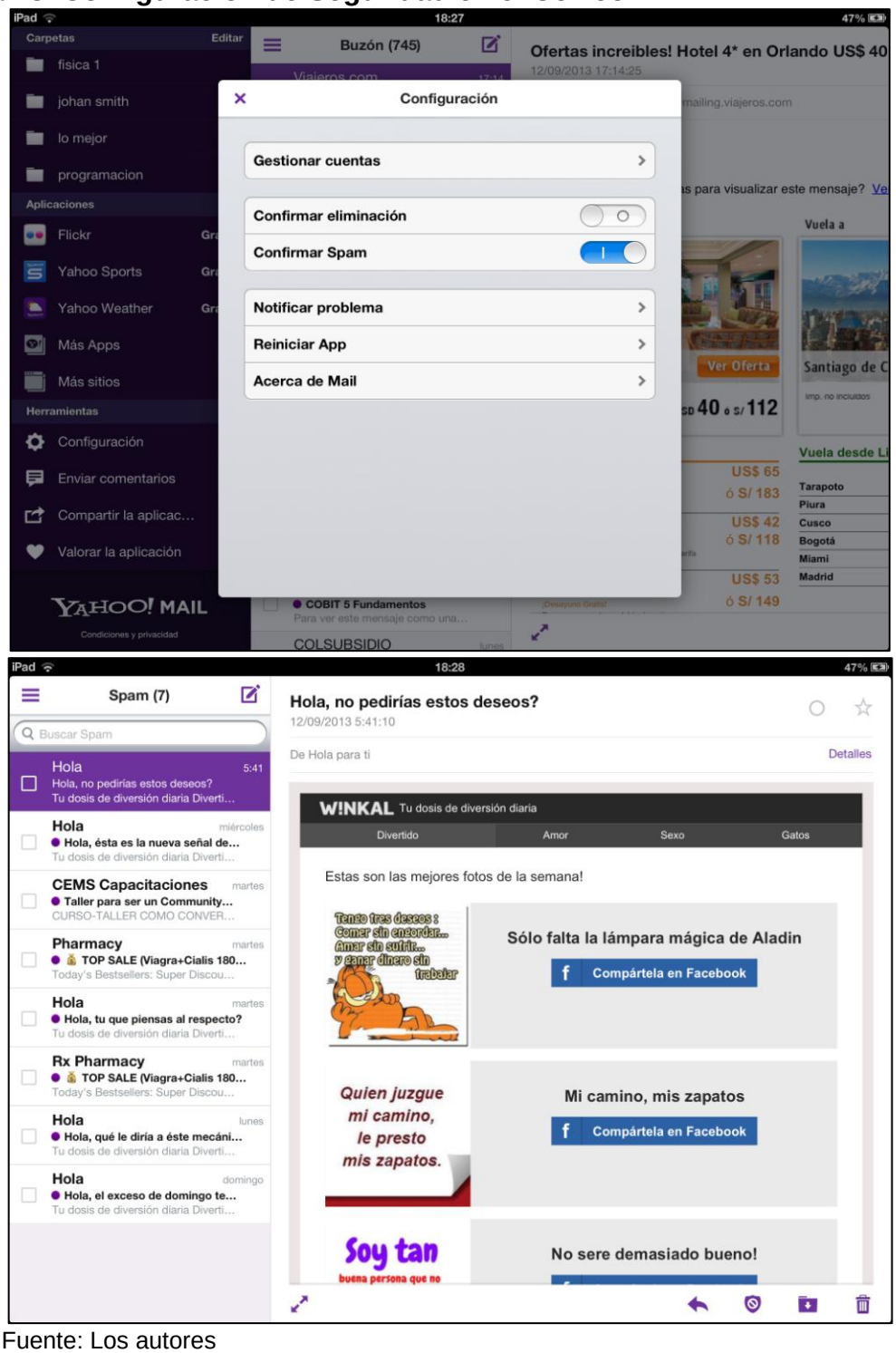
Figura 17. Instalación desde correo electrónico



Fuente: Los autores

Adicional se pueden evaluar algunas alternativas en otros clientes de correo como yahoo:

Figura 18. Configuración de Seguridad en el Correo

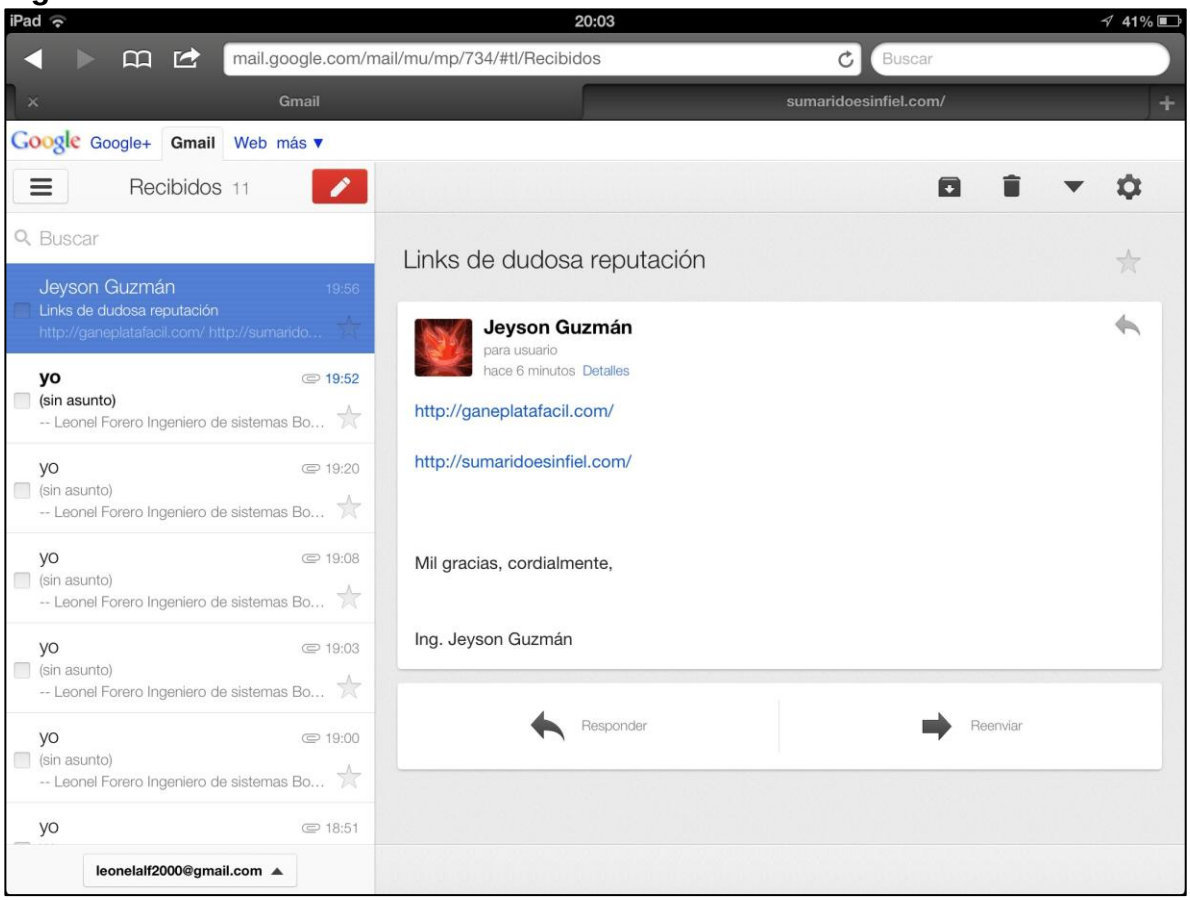


Fuente: Los autores

Configurar en el cliente de mensajería la exploración automática de archivos en el momento de su recepción. La mayoría de estos clientes contemplan la posibilidad de configurarlos con un antivirus.

Es recomendable, al igual que con el correo electrónico, no hacer clic sobre los enlaces incrustados en el cuerpo del mensaje, ya que pueden direccionar a páginas con contenido malicioso o hacia la descarga de malware.

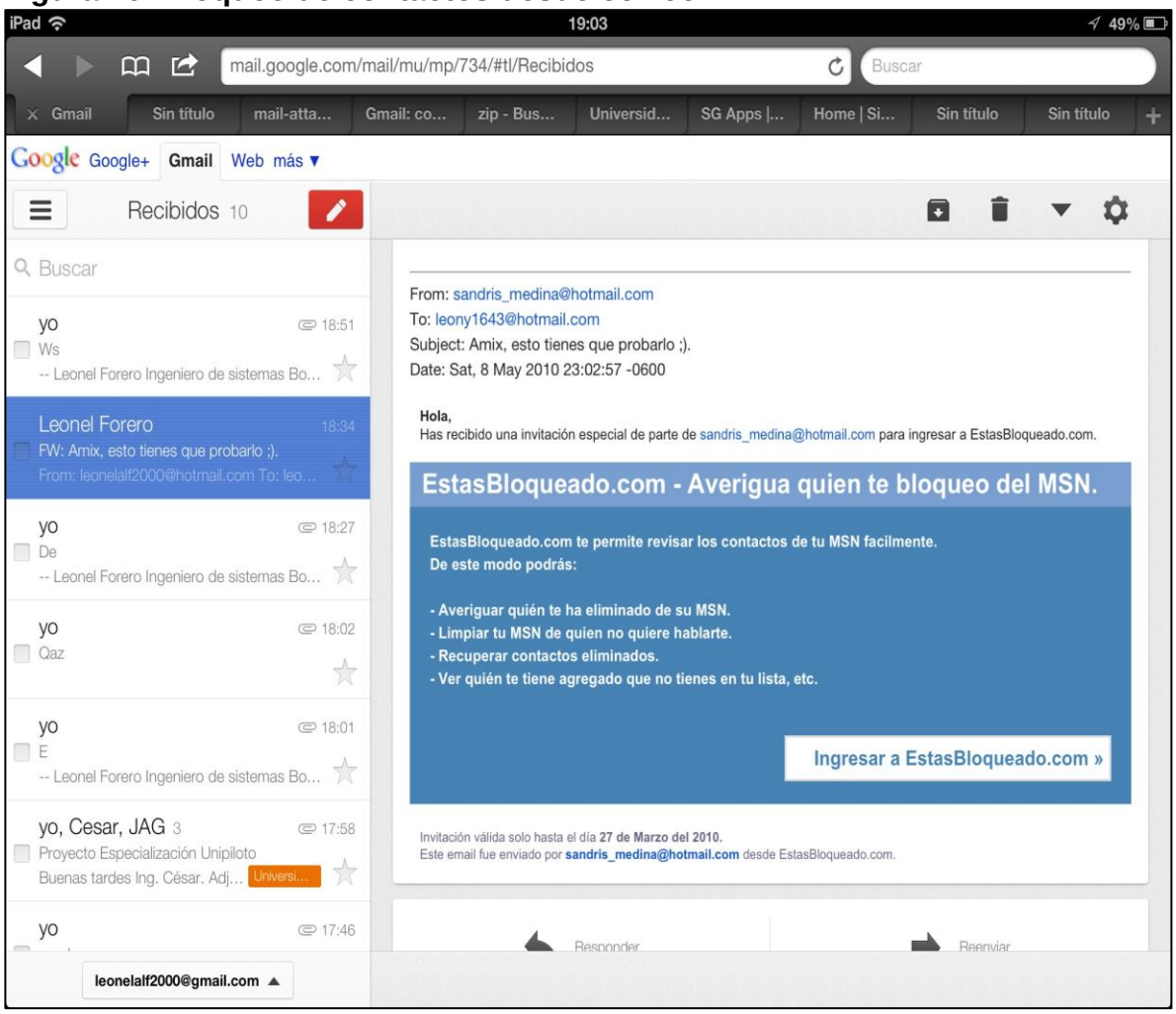
Figura 19. Vista de enlaces desde el correo



Fuente: Los autores

No escribir los datos de autenticación en páginas que prometen ofrecer información de contactos bloqueados y similares. Estos sitios suelen comprometer la privacidad de la información que se aloja en los correos, además de utilizar la cuenta con otros fines delictivos.

Figura 20. Bloqueo de contactos desde correo



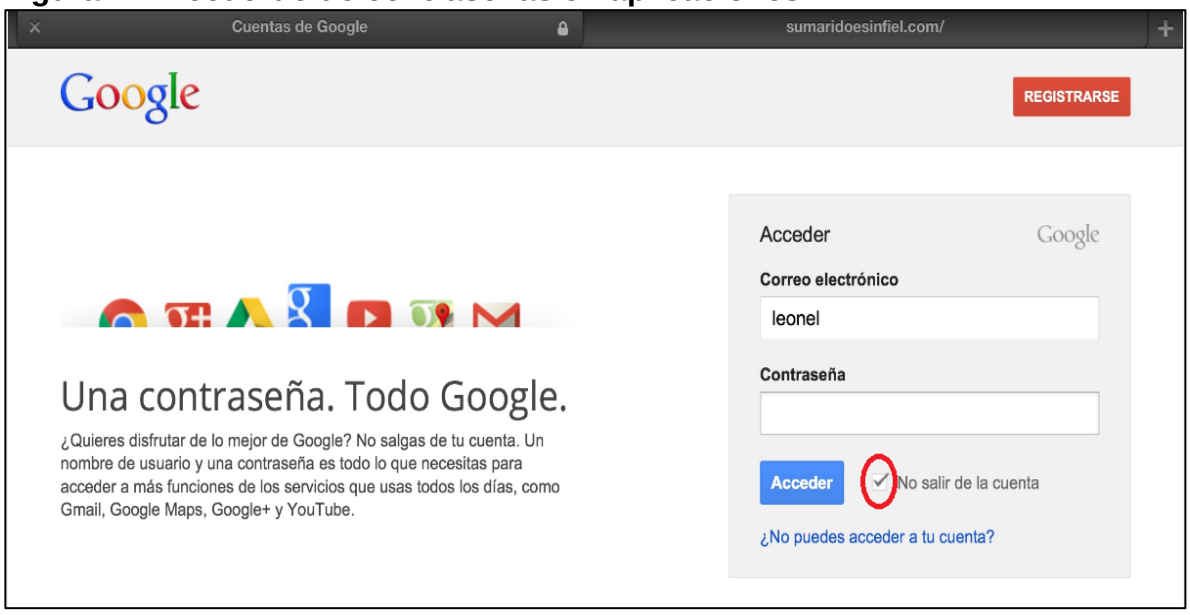
Fuente: Los autores

Cambiar la contraseña de manera periódica. Ayuda a maximizar el nivel de seguridad.

No compartir la contraseña con nadie. El carácter de ésta es privado, con lo cual lo recomendable es que sólo la conozca el usuario que la ha creado.

Cuando se accede a los servicios de mensajería instantánea o de correo electrónico desde dispositivos que no son propios, es recomendable deshabilitar la opción de inicio automático para que no quede la dirección (ni la contraseña) grabada. Esto evita que terceros inicien sesión de manera automática.

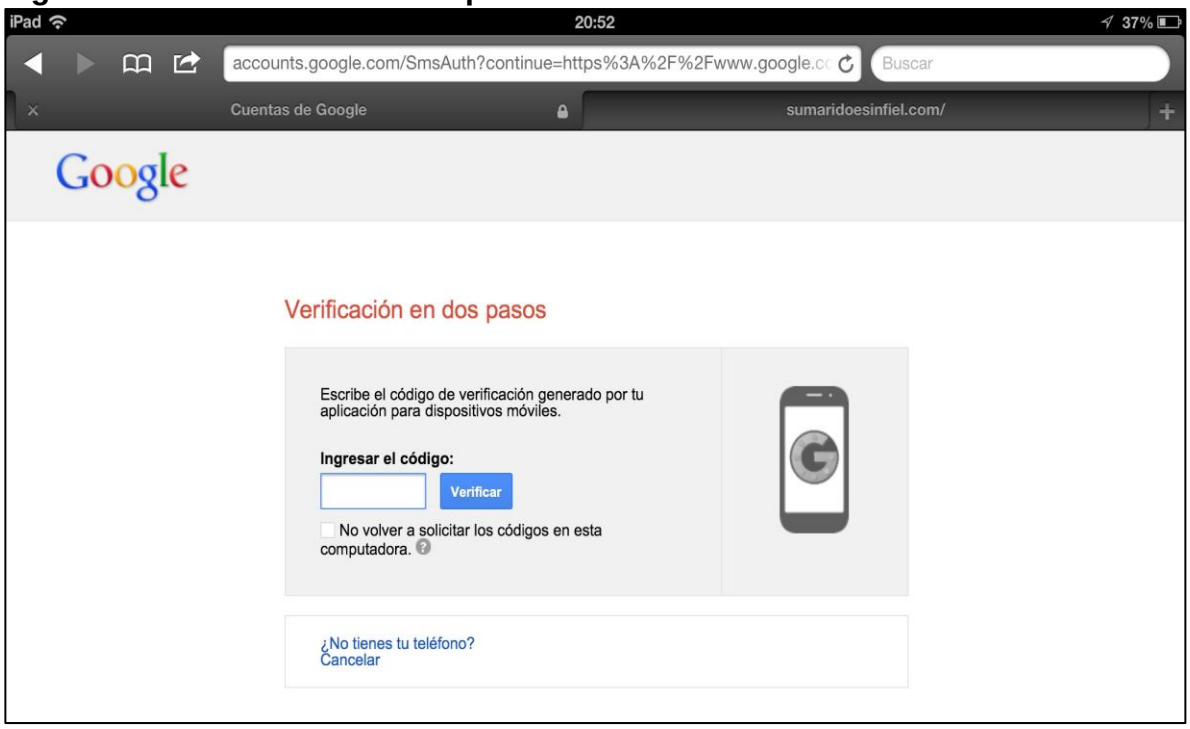
Figura 21. Recuerdo de contraseñas en aplicaciones



Fuente: Los autores

Una buena práctica es habilitar la verificación de acceso en dos pasos:

Figura 22. Verificación en dos pasos

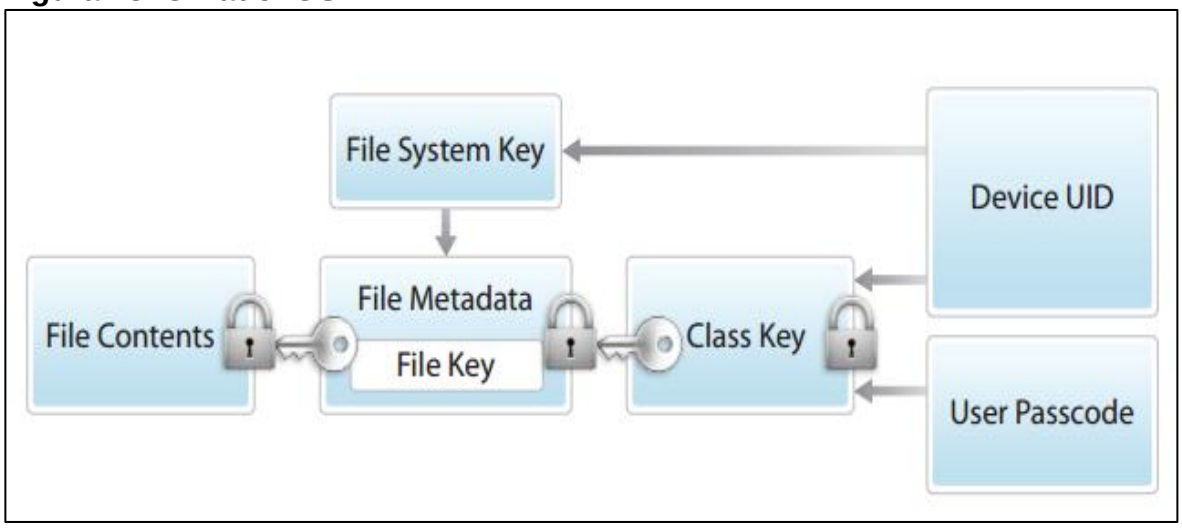


Fuente: Los autores

8. CRIFRADO DE LA INFORMACIÒN

El contenido de un archivo se cifra con una clave por archivo, que se envuelve con una clave de clase y se almacena en los metadatos de un archivo, que es a su vez cifrada con la clave de sistema de archivos (mediante el algoritmo AES). La clave de clase está protegida con el UID hardware y, para algunas clases, con códigos de acceso del usuario. Esta jerarquía proporciona flexibilidad y rendimiento. Por ejemplo, cambiar la clase de un archivo sólo requiere reemplazar su clave por archivo, y un cambio de código de acceso sólo requiere rearmar la clave de clase.

Figura 23. Cifrado iOS



Fuente. SYMATEC. Cifrado iOS. . [en línea]. Bogotá: [citado 26 junio, 2013]. Disponible en Internet : < URL:http://www.symantec.com/content/es/mx/enterprise/images/theme/mobility/America-Latina-2012-State-of-Mobility-Survey-Report-SPA.pdf>

La protección depende de la calidad del código de acceso, iOS permite claves sencillas de 4 cifras numéricas o las más seguras que son alfanuméricas. Cabe resaltar que la Protección de Datos descrita arriba no se activa si no se habilita el código de acceso.

El código descrito anteriormente se puede habilitar en la opción de ajustes, general, bloqueo con código, activar código:

Figura 24. General, Activación de código

Fuente: Los autores

Figura 25. Activación de código

Fuente: Los autores

9. CONCLUSIONES

Tanto los usuarios como las organizaciones (sin importar el nivel de conocimiento), son cada vez más dependientes de Internet y sus servicios asociados, lo que también los expone constantemente a diferentes amenazas, en las que se utilizan estas condiciones para cometer acciones delictivas con fines económicos y comerciales entre otros (Ingeniería social y Phishing), en consecuencia, es sumamente importante incorporar, como hábito cotidiano, las medidas de seguridad recomendadas en esta guía de mejores prácticas.

Al bloquear las amenazas de forma temprana se reduce considerablemente la posibilidad de ser potenciales víctimas de las actividades delictivas, que se llevan a cabo atentando contra la seguridad de los entornos de información independientemente de si es un Smartphone corporativo o personal. Es allí donde se vislumbra la ventaja de tener una guía que muestre algunas estrategias de seguridad a nivel de: actualización de sistema operativo, aseguramiento o hardening del sistema operativo, protección en el correo electrónico, seguridad en la navegación, seguridad en redes sociales, seguridad en mensajería instantánea y cifrado de la información.

Recomendaciones de seguridad para Smartphone

Jasón Andrés Guzmán
Universidad Piloto de Colombia
Bogotá, Colombia
Jeyson903@gmail.com

Leonel Alberto Forero
Universidad Piloto de Colombia
Bogotá, Colombia
Leonelalf2000@gmail.com

Resumen:

El siguiente documento presenta una relación de las mejores prácticas y recomendaciones para el uso seguro de dispositivos móviles tipo Smartphone; por esta razón se toma como base inicial la seguridad en el sistema operativo, donde se incluyen: consejos para mantener actualizado el sistema, prácticas para establecer conexiones seguras y seguidamente se relacionan una serie de tips para proteger nuestro dispositivo mediante el uso de aplicaciones. Sin restar importancia a la implementación de contraseñas seguras, adicionalmente se tratan temas como la protección en el uso del correo electrónico, navegación web y la seguridad en las redes sociales; ya que estos servicios son de uso cotidiano y seguido a esto se aconseja sobre el almacenamiento de la información trayendo a contexto la seguridad que se debe tener con los medio extraíbles compatibles con estos dispositivos; para finalizar se relaciona una serie de conclusiones donde se resalta la optimización que debemos dar a la protección de la información, ya sea personal o corporativa.

Abstract:

The following document presents a list of best practices and recommendations for safe use of mobile devices Smartphone type, for it is taken as the initial base operating system security, which includes: tips to keep your system, to establish practices secure connections and then relate a series of tips to protect our device using applications without leaving the implementation of secure passwords and additionally covers topics such as protection in the use of email, web browsing and security social networks, as these services are used daily, following this advice on the storage of information bringing the security context should be to removable media (flash Memory and sD type) is related to complete a number of conclusions which highlights the importance given to the protection of information, whether personal or corporate.

Palabras Clave: Smartphone, Seguridad, Riesgo, Información.

INTRODUCCIÓN

En la actualidad, es evidente el uso frecuente de los Smartphone, se pueden observar en distintas partes como centros comerciales, oficinas, reuniones e instituciones educativas entre otros; estos son utilizados por usuarios de diversas edades, niveles y clases sociales, razón por la cual la seguridad de la información juega un factor importante a nivel personal y corporativo, debido a esto, es de vital importancia conocer algunas bondades y desventajas de los Smartphone, de la misma manera, reconocer las vulnerabilidades a nivel de seguridad en la información que afectan aspectos como lo la disponibilidad, integridad confidencialidad y control de acceso en estos.

Es necesario evidenciar algunas vulnerabilidades, educar e informar a los usuarios de los dispositivos, sobre el riesgo latente que existe si no se toman medidas de prevención para la protección de la información que un Smartphone puede almacenar; la suplantación de identidad, la ingeniería social, el fraude y la pérdida o el robo del dispositivo, son factores que se pueden mitigar con la adopción de buenas prácticas como las que se relacionan en este documento, estas buscan proteger la información y disminuir la posibilidad de que su usuario forme parte de las víctimas potenciales y se enfrente a las amenazas, peligros y riesgos de manera innecesaria.

Cuando se tiene posesión de un Smartphone se puede llegar a pensar que estos dispositivos son menos accesibles a intrusos, pues los usuarios en muchas ocasiones desconocen que las conexiones por medio de bluetooth o redes inalámbricas se pueden realizar sin tener contacto físico con el dispositivo. Esta falsa sensación de seguridad, junto con el uso de aplicaciones del estilo del correos electrónicos, redes sociales y contenido multimedia como lo son: mensajes, fotos, música y videos, conlleva al almacenamiento de datos personales o corporativos que en su mayoría son de carácter privado o confidencial, muchas veces de forma inadvertida para el usuario.

A continuación se describen una serie de recomendaciones básicas para mejorar la seguridad del Smartphone y proteger la información almacenada en el mismo.

1. Seguridad del sistema operativo

El Aspecto más importante en materia de prevención, radica en configurar el sistema operativo de una forma adecuada, ya que es este el que permite la ejecución de aplicación, organización y administración de la información, de igual forma, puede ser configurado para fortalecer su seguridad; entre las buenas prácticas que se pueden tener en cuenta se encuentran:

1.1. Mantener actualizado el sistema

Siempre es recomendable usar las páginas de los fabricantes como es el caso del AppStore para sistemas Apple, pues son estos quienes generan las diferentes recomendaciones, parches y métodos de protección que son compatibles con cada dispositivo; de este modo, descargar actualizaciones desde sitios de dudosa reputación (no recomendados por el fabricante) aumenta los riesgo de conseguir vulnerabilidades, lo que comúnmente se conoce como huecos de seguridad.

1.2. Conexiones seguras.

Deshabilitar conexiones inalámbricas como Bluetooth y Wi-Fi si no se están utilizando evita la propagación de gusanos informáticos (virus que invaden el sistema operativo del dispositivo y generar huecos de seguridad [1]), los cuales, aprovechan ese servicio como método de infección.

El Bluetooth es una tecnología bastante útil para la transmisión de datos y voz como lo es por ejemplo: el manos libres que se usa para contestar las llamadas telefónicas dentro de un vehículo; pero su nivel de seguridad es vulnerable en tanto cuando deja de usarse, debido a que la conexión sigue abierta y en la espera de recibir o enviar datos (esto genera un canal de comunicación por medio del cual es posible visualizar la información de los dispositivos), este tipo conexión puede ser usada de forma mal intencionada para la sustracción de datos e información sin autorización.

A continuación se muestran un ejemplo de esta configuración:

Imagen 1- Configuración de Wi-FiWi-Fi y Bluetooth

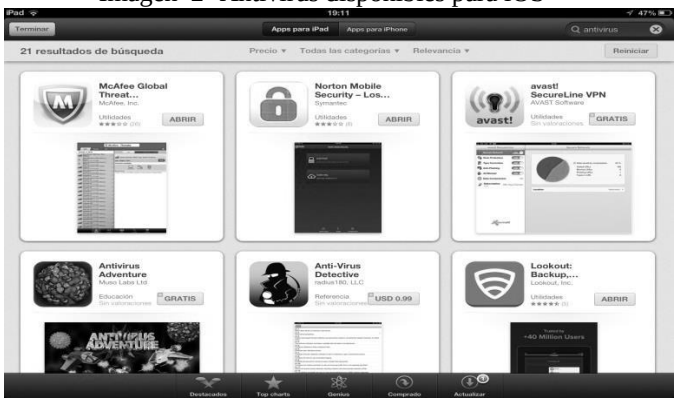
Fuente: Los autores

En la actualidad existen infinidad de puntos de acceso Wi-Fi sin ningún tipo de seguridad implementada o simplemente de sitios públicos como aeropuertos, centros comerciales o restaurantes que dejan estos canales de comunicación abiertos para que el público en general pueda acceder a ellos fácilmente; el peligro aparece cuando el punto de acceso está abierto intencionadamente con un propósito malicioso (es decir, existen puntos de acceso libres y abiertos de manera intencional para que los usuarios los utilicen mientras su información puede ser vulnerada), o cuando en la red pública está conectado algún equipo con el mismo fin. De esta manera, un usuario pensará que está usando "Internet gratis", pero lo que realmente sucede es que al conectarse a esa red una persona no autorizada puede acceder a su dispositivo móvil.

2. Software de protección.

Instalar, en lo posible, un programa antivirus con capacidades proactivas, (es decir, que analizan sin solicitud del usuario en tiempo real descargas y programas instalados), que incluya cortafuegos (Firewall), el cual evita ataques no autorizados por personas o software malicioso, antispam para evitar correo basura, anti espías, accesos no autorizados, entre otras aplicaciones.

Imagen 2- Antivirus disponibles para iOS



Fuente: Los autores

A partir de agosto del 2010 la firma de antivirus ESET [2] lanzó una aplicación para la protección de Smartphone; no obstante existen otras soluciones de antivirus disponibles en el mercado para su evaluación y/o compra como Kaspersky [3] y Norton [4] entre otras.

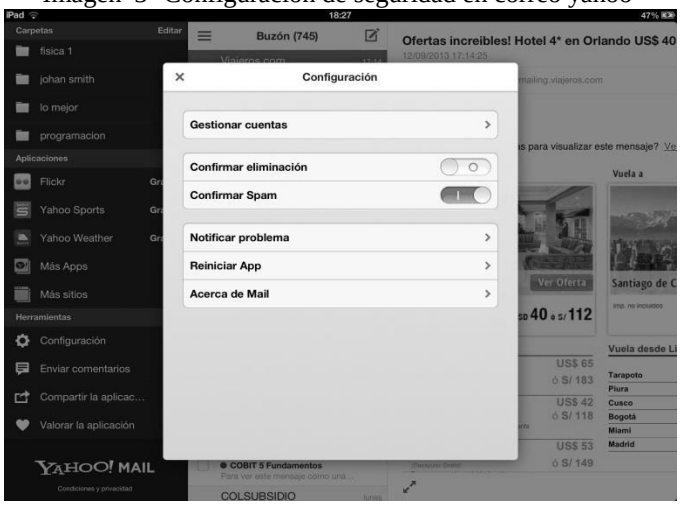
2.1. Fortalecer contraseñas

Utilizar contraseñas fuertes[5]; el empleo de contraseñas simples (de corta longitud, con ausencia de caracteres especiales, números y variaciones entre mayúsculas y minúsculas), es otra de las debilidades que los códigos maliciosos con capacidad de descifrado de contraseñas suelen aprovechar para propagarse por los recursos de información, es decir, una contraseña fuerte puede ser: (E@n2013!), una clave de varios caracteres alfanuméricos que incluya además caracteres especiales, ayudará a mejorar el nivel se seguridad en el dispositivo, haciendo que los accesos no autorizados sean de mayor dificultad.

2.2. Protección en el correo electrónico.

El correo electrónico constituye uno de los canales de propagación/infección de malware más utilizados por atacantes; por lo tanto es importante que los usuarios incorporen como hábito determinadas prácticas que permitan prevenir los ataques realizados a través de códigos maliciosos. A continuación, se presenta una serie de medidas preventivas orientadas a aumentar la seguridad durante el uso del correo electrónico.

Imagen 3- Configuración de seguridad en correo yahoo



Fuente: Los autores

No confiar en correos de remitentes desconocidos, y en el caso de contener archivos adjuntos no abrirlos, esto evita la ejecución de algún tipo de malware incluido en el mismo; cuando se reciben adjuntos, prestar especial atención a las extensiones de los mismos, dado que suelen utilizar técnicas de engaño como la doble extensión o espacios entre el nombre del archivo y la extensión del mismo.

Evitar publicar las direcciones de correo en sitios web de dudosa reputación como sitios pornográficos, foros, chats, comercio electrónico y donaciones; esto minimiza la posibilidad de que la dirección se guarde en la base de datos de los spammers (persona o entidad que capturan listados de correos electrónicos) y posteriormente las utilizan con la finalidad de enviar correo de tipo Spam (el spam[6] es el correo electrónico que promociona diferentes productos y servicios a través de publicidad no solicitada y enviada masivamente a las direcciones de correo de los usuarios), el cual constituye uno de los principales medios de propagación de una importante cantidad de códigos maliciosos.

No responder jamás el correo spam, por ello se recomienda ignorarlos y/o borrarlos, ya que si se responde se confirma que la dirección de correo se encuentra activa.

En lo posible, evitar el re-envío de mensajes en cadena[7], toda vez que suelen ser utilizados para recolectar direcciones de correo activas y hacer uso de técnicas de ataque como spam y phishing; el phishing [8] es una modalidad delictiva enmarcada en la figura de estafa realizada a través de Internet, y constituye otra de las amenazas de seguridad más propagadas a través del correo electrónico; si de todos modos se desea enviar mensajes en cadena, es recomendable hacerlo siempre con copia oculta (CCO) para que quien lo recibe lea solo la dirección del emisor.

Utilizar claves seguras (fortalecidas según las recomendaciones anteriormente dadas) y cambiar la contraseña con periodicidad si se utiliza el servicio de correo electrónico por medio de una página web. Esto favorece la seguridad de la información, puesto que hace más difícil el hallazgo mediante algunas técnicas de explotación de información.

Configurar la pregunta secreta como opción de seguridad siendo este uno de los mecanismos ofrecidos por los proveedores de correo electrónico, con palabras que no sean de fácil deducción para fortalecer aún más la seguridad de la información contenida en el correo electrónico.

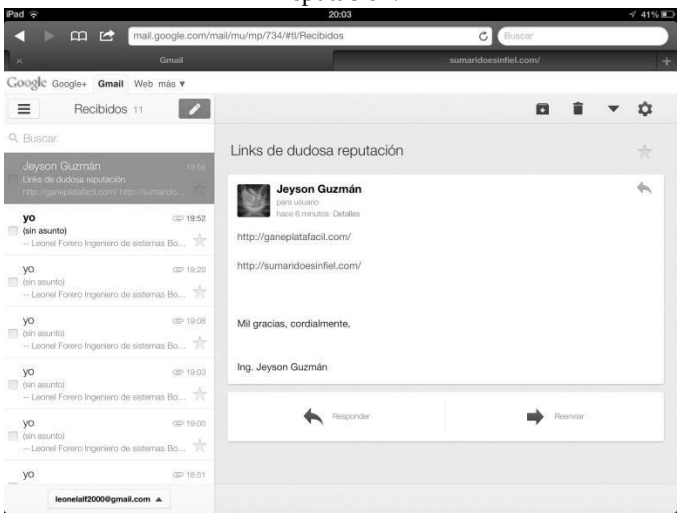
Como medida de seguridad extra, se sugiere evitar ir a enlaces externos de procedencia desconocida y descargar información de los mismos, teniendo en cuenta que estos sitios puede afectar la seguridad de la información

Del mismo modo, es preferible que se evite ingresar el nombre de usuario y su respectiva contraseña en sitios de los cuales no se tenga referencia, de esta manera se preserva la privacidad de la cuenta de correo y por ende, la información que se intercambia a través de la misma.

Se debe desconfiar de los correos que dicen ser emitidos por entidades que brindan servicios y solicitan cambios de datos sensibles como nombres, número de cedula, contraseñas, números de cuentas, ya que suelen ser métodos de Ingeniería Social[9] para obtener información por medio de engaños o datos que aparentan ser verídicos); se debe tener en cuenta que las entidades bancarias y financieras no solicitan datos confidenciales a través de este medio, de esta manera se minimiza la posibilidad de ser víctima de una acción delictiva.

No ingresar a enlaces que aparecen en el cuerpo de los correos electrónicos, ya que pueden re-direccionar hacia sitios web clonados (sitios que aparentan ser legítimos a los originales, suele ser usado en páginas bancarias, redes sociales y proveedores de correo).

Imagen 4- Mensaje de correo con enlaces de dudosa reputación.



Fuente: Los autores

Jamás se deben enviar contraseñas, números de tarjetas de crédito u otro tipo de información confidencial a través del correo electrónico, ya que la comunicación podría ser interceptada y robada.

Denunciar casos de phishing[8] (técnica de robo de información, mediante la suplantación de identidad a través de plataformas web) en entes de orden público como el Colcert de la policía Nacional de Colombia, ya que además de cortar la actividad del sitio malicioso, se colabora con la seguridad general de la navegación en Internet.

Imagen 52- Imagen Lockout Informe de Análisis

Fuente: Los autores

3. Seguridad en la navegación

En los últimos años, Internet se ha transformado en una plataforma de ataque[9] donde acciones delictivas se llevan a cabo a través de diferentes técnicas como por ejemplo el Drive-by-Download, el cual permite infectar masivamente los dispositivos por medio de accesos web[10]. En consecuencia, es fundamental navegar con cautela y tener presente las recomendaciones más importantes, entre ellas:

En lo posible no acceder a servicios como Home-Banking (transacciones financieras que se realizan generalmente desde un cajero electrónico) desde lugares públicos bibliotecas, cafés, hoteles y centros comerciales.

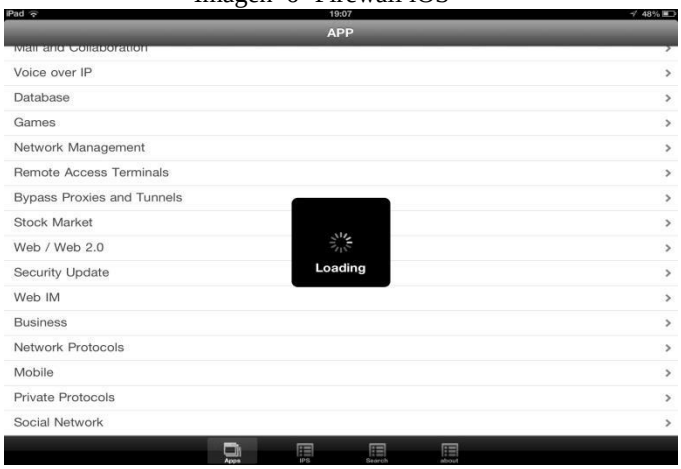
Asegurarse de que la dirección del sitio web de entidades financieras o comercio electrónico (sitios que permiten la manipulación de información confidencial), al cual se accede, comience con el protocolo HTTPS; la "s" final, significa que la página web es segura [11] y que toda la información depositada en la misma viajará de manera cifrada.

Si se navega desde sitios públicos, es recomendable eliminar los archivos temporales, caché, cookies, direcciones URL, contraseñas y formularios donde se hayan ingresado datos.

El bloqueo de determinados sitios considerados maliciosos, ya sea porque descargan malware o porque contienen material de dudosa reputación, es también otra de las mejores prácticas que ayudan a la prevención y refuerzan la seguridad del equipo, por medio de la configuración de seguridad de cada navegador en los dispositivos.

Disponer, además, de un Firewall personal que permita bloquear comunicaciones entrantes y salientes. ESET Smart Security, por ejemplo, incorpora un Firewall personal.

Imagen 6- Firewall iOS



Fuente: Los autores

Evitar el ingreso a sitios web con contenidos ilegales, como aquellos que ofrecen cracks; ya que constituyen canales propensos a la propagación de malware.

Impedir la ejecución de archivos desde sitios web sin verificar previamente que es lo que dice ser. Es importante no hacer clic sobre el botón Instalar ya que esto provoca que el

archivo se ejecute automáticamente luego de descargado, dejando al margen la posibilidad de verificar su integridad.

En lo posible se recomienda, leer atentamente las políticas de privacidad de las aplicaciones descargadas desde sitios web no oficiales o de dudosa reputación, antes de instalarlas.

No realizar la instalación de complementos extras como aplicaciones recomendadas o protectores de pantallas sin verificar previamente su autenticidad.

3.1. Seguridad en redes sociales

En la actualidad, las redes sociales son muy populares [12] y los usuarios las utilizan masivamente; estas características las transforman en importantes focos de propagación de malware, por tal motivo, se torna necesario tener en cuenta y aplicar las siguientes medidas preventivas:

No publicar información privada y confidencial, debido a que personas extrañas pueden aprovechar esta información con fines maliciosos.

También es recomendable evitar la publicación de fotografías propias y de familiares. Las fotografías pueden ser utilizadas para complementar actos delictivos, incluso fuera del ámbito informático (extorciones a familiares y amigos).

Mantener la privacidad del perfil; es decir, configurar el perfil para que no sea público por medio de las opciones de seguridad que ofrecen los sitios de redes sociales.

No responder las solicitudes de desconocidos, ya que pueden contener códigos maliciosos o pueden formar parte de actividades delictivas en el dispositivo móvil.

Ignorar los mensajes que ofrecen material pornográfico, pues usualmente a través de ellos suele canalizarse la propagación de malware, además de otras acciones ofensivas en el dispositivo móvil.

Cambiar periódicamente la contraseña para evitar que la misma sea descubierta fácilmente y evitar el almacenamiento de está en el dispositivo móvil.

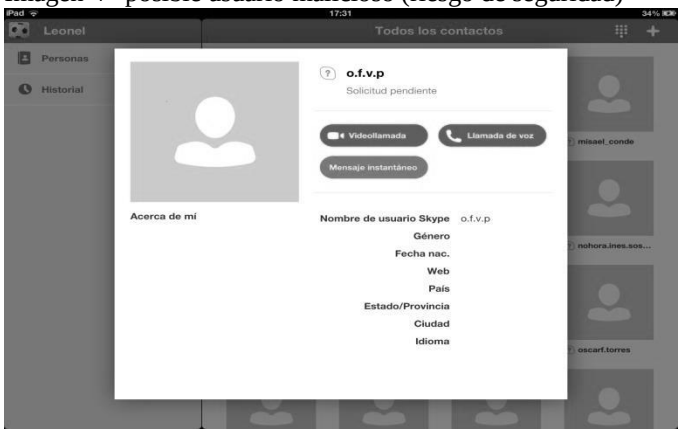
3.2. Seguridad en mensajería instantánea

Otro medio de comunicación popular y que se emplea masivamente, son los clientes de mensajería instantánea, que constituyen uno de los servicios más explotados por diferentes amenazas informáticas dentro de las cuales una de las más activas es el malware.

Por tal motivo, poner en ejecución medidas tendientes a volver más seguro el cliente de mensajería instantánea se transforma en una tarea casi obligada. Para evitar ser víctima de acciones maliciosas llevadas a cabo mediante esta tecnología, se recomienda aplicar alguna de las medidas de seguridad que a continuación se recomiendan:

Evitar aceptar como contacto cuentas desconocidas sin verificar a quién pertenece, ya que en la mayoría de los casos se trata de intentos de engaños con fines maliciosos. Generalmente son dominios desconocidos y no de HOTMAIL por ejemplo bayne918g5t2@mobiuswoman.info, como se observa en la siguiente imagen.

Imagen 7- posible usuario malicioso (riesgo de seguridad)



Fuente: Los autores

No descargar archivos sospechosos, sobre todo cuando vienen acompañados de mensajes genéricos o en otro idioma; esto constituye una de las características principales de los códigos maliciosos que se propagan a través de este canal de comunicación, en especial archivos con extensiones que pueden ser instaladores en los Smartphones, por ejemplo aplicaciones (*.ipa y algunos *.zip).

Imagen 83 –Mensaje con posible adjunto malicioso

Fuente: Los autores

Configurar en el cliente de mensajería la exploración automática de archivos en el momento de su recepción; la mayoría de estos clientes contemplan la posibilidad de configurarlos con un antivirus.

Es recomendable, al igual que con el correo electrónico, no hacer clic sobre los enlaces incrustados en el cuerpo del mensaje, ya que pueden direccionar a páginas con contenido malicioso o hacia la descarga de malware.

No compartir la contraseña con nadie; el carácter de ésta es privado, con lo cual lo recomendable es que sólo la conozca el usuario que la ha creado.

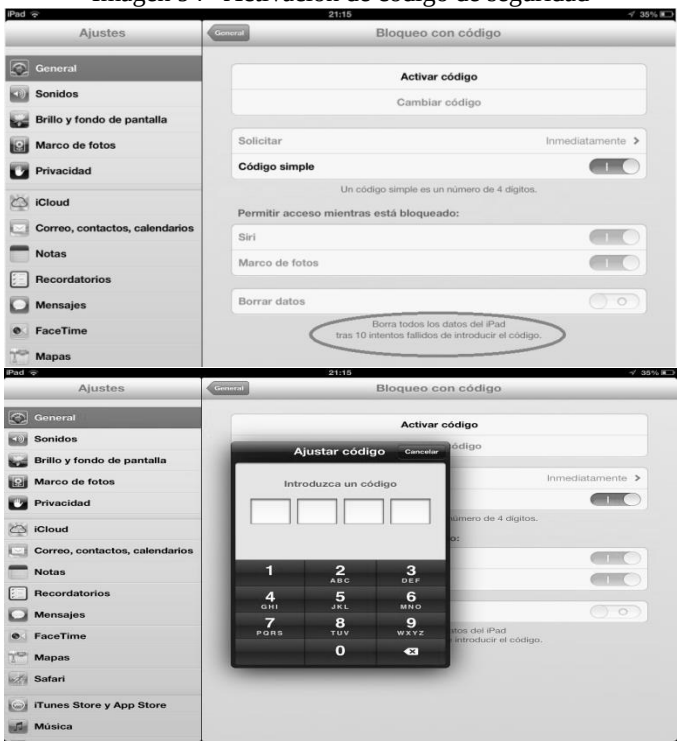
Cuando se accede a los servicios de mensajería instantánea o de correo electrónico desde Smartphones que no son propios, es recomendable deshabilitar la opción de inicio automático para que ni la dirección ni la contraseña sea grabada, esto evita que terceros inicien sesión de manera automática.

No compartir información confidencial a través de este medio ya que la misma puede ser interceptada y robada con fines delictivos.

4. Encripción de la información

La protección depende de la calidad del código de acceso, iOS permite claves sencillas de 4 cifras numéricas o las más seguras que son alfanuméricas. Cabe resaltar que la Protección de Datos no se activa si no se habilita el código de acceso, este se puede habilitar en la opción de ajustes, general, bloqueo con código, activar código:

Imagen 94 –Activación de código de seguridad



Fuente: Los autores.

Referencias

[1] Tomado de : http://www.revistalideres.ec/tecnologia/smartphone-blanco-VIRUS-informaticos_0_715128511.html [Visitado el 11 de Junio de 2013]J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[2] Tomado de :http://www.eset-la.com/hogar/mobile-security-antivirus [Visitado el 5 de Julio de 2013]

[3] [1]Tomado de :http://www.kaspersky.com/sp/kaspersky_mobile_security [Visitado el 5 de Julio de 2013]

[4] [1]Tomado de :http://norton.symantec.com/norton/ps/3up_co_es_navnis360.html?om_sem_cid=hho_sem_ic:co:ggl:es:b|kw0000004480|10672096712&country=CO [Visitado el 23 de Julio de 2013]

[5] [1]Tomado de: http://www.eset-la.com/threat-center/2037-seguridad-contraseñas [Visitado el 23 de Julio de 2013]

[6] Tomado de: http://www.eset-la.com/threat-center/1639-spam-hoy-ahora-y-siempre [Visitado el 23 de Julio de 2013]

Tomado de: http://www.segu-info.com.ar/malware/hoax.htm [Visitado el 15 de Julio de 2013]

[7] Tomado de: https://www.bancocajasocial.com/tips-de-seguridad [Visitado el 23 de Julio de 2013]

[8] Tomado de: http://www.acis.org.co/fileadmin/Base_de_Conocimiento/V_Jornada_de_Seguridad/IngenieraSocial_CarlosBiscione.pdf [Visitado el 28 de Julio de 2013]

[9] Tomado de: http://www.pandasecurity.com/spain/homeusers/security-info/cybercrime/phishing/ [Visitado el 15 de Julio de 2013]

[10] Tomado de: http://www.eset-la.com/threat-center/2001-tendencias-eset-malware-2009 [Visitado el 28 de Julio de 2012]

[11] Tomado de: http://www.enhacke.com/tag/smartphone/ [Visitado el 15 de Julio de 2013]

[12] Tomado de: http://www.microsoft.com/multicountryamericas/seguridadhogar/Usted-Phishing-Default.aspx [Visitado el 3 de Agosto de 2013]

[13] Tomado de: http://www.semana.com/vida-moderna/redes-sociales-populares/140949-3.aspx [Visitado el 20 de Agosto de 2013]

[14] Tomado de http://www.culturiarte.com/2013/01/las-redes-sociales-mas-populares.html [visitado el 24 de septiembre de 2013]