INSEGURIDAD EN AMBIENTES MÓVILES

GERSON GEOVANNY DELGADO CABALLERO

PABLO CESAR OSPINA GARCIA

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERÍAS FÍSICO MECÁNICAS
ESCUELA DE INGENIERIAS ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES
ESPECIALIZACIÓN EN TELECOMUNICACIONES
BUCARAMANGA
2010

INSEGURIDAD EN AMBIENTES MÓVILES

GERSON GEOVANNY DELGADO CABALLERO

PABLO CESAR OSPINA GARCIA

Monografía para optar el título de Especialista en Telecomunicaciones

Director
JORGE HERNANDO RAMÓN SUÁREZ
Director Especialización Telecomunicaciones

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERÍAS FÍSICO MECÁNICAS
ESCUELA DE INGENIERIAS ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES
ESPECIALIZACIÓN EN TELECOMUNICACIONES
BUCARAMANGA
2010

AGRADECIMIENTOS

A Dios por darme todas estas capacidades en lo intelectual.

A Mis Padres por esa confianza y apoyo.

Al Ingeniero Jorge Hernándo Ramón Suárez por su colaboración.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE IMÁGENES

Pág.

GLOSARIO

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.

ANCHO DE BANDA – Gama de frecuencias disponibles para las señales. Se mide en Hertzios.

ANTENA – Elemento de un teléfono móvil que aumenta la señal de radio recibida. Puede ser antena fija, antena telescópica o antena interna.

BES – BlackBerry Enterprise Server (BES) es el nombre del paquete de software que es parte de la plataforma inalámbrica BlackBerry de Research In Motion. El software y el servicio se conectan al software de mensajería en las redes empresariales y redirige los correos electrónicos, sincroniza los contactos y calendarios de información entre servidores, estaciones de trabajo de escritorio y dispositivos móviles.

BLUETOOTH – Tecnología de comunicación inalámbrica que permite la conexión entre diferentes equipos en un corto alcance (max 10 mts) vía radio sin necesidad de estar unidos físicamente.

BLUEJACKING – El término bluejacking se refiere a una técnica consistente en enviar mensajes no solicitados entre dispositivos Bluetooth, como por ejemplo teléfonos móviles, PDAs o portátiles.

CLAVE SIMETRICA – La criptografía simétrica es un método criptográfico en el cual se usa una misma clave para cifrar y descifrar mensajes. Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. Una vez ambas tienen acceso a esta clave, el remitente cifra un mensaje usándola, lo envía al destinatario, y éste lo descifra con la misma.

CÁMARA DIGITAL – Es una cámara fotográfica que, en vez de capturar y almacenar fotografías en películas fotográficas como las cámaras fotográficas convencionales, lo hace digitalmente mediante un dispositivo electrónico, o en cinta magnética usando un formato analógico como muchas cámaras de video.

COBERTURA – Área a la que llegan las señales de una red de telefonía móvil.

COMPUTADOR PERSONAL – Ordenador personal o estación de trabajo utilizados exclusivamente en un ambiente de trabajo, en casa o en la oficina, ejecutando un sistema operativo popular, incluyendo Windows, Mac OS y Linux.

EMS – (Enhanced Messaging Services – Servicio de Mensajería Mejorado). Nuevo estándar de mensajería que permite la descarga y el envío/recepción de mensajes de texto acompañados de melodías, imágenes y animaciones. Esta promovido por los fabricantes Alcatel, Motorola, Sony Ericsson y Siemens.

EDGE – Tecnología intermedia entre las generación 2.5 (GPRS) y 3 (UMTS) que permite una rápida transmisión de datos en terminales GSM/EDGE de aproximadamente 240Kpbs, en la actualidad esta tecnología está disponible en Comcel y Movistar, OLA alista su próximo lanzamiento.

EPL – (Eclipse Public License).

ENCRIPTACIÓN – Cualquier procedimiento que se utiliza en criptografía para convertir texto en texto cifrado o para almacenar o transferir información delicada que no debería ser accesible a terceros.

FAT – Tabla de Asignación de Archivos, en inglés, File Allocation Table (FAT) es un sistema de archivos desarrollado para MS-DOS, así como el sistema de archivos principal de las ediciones no empresariales de Microsoft Windows hasta Windows Me.

GPS – Sistema de Posicionamiento Global. Un sistema para determinar la posición mediante la comparación de señales de radio emitidas por varios satélites.

GSM – Sistema global para comunicaciones móviles, (GSM por sus siglas en inglés), Ofrece la integración de servicios como correo de voz, datos de alta velocidad (GPRS/EDGE/UMTS), fax, radio localizador y mensajes cortos, así como comunicación segura. Originalmente fue un estándar Europeo para telefonía móvil digital pero se ha convertido en el sistema móvil más usado a nivel global, en alrededor de 100 países. Las redes de GSM operan en la banda de 900MHz y 1800 MHz en Europa, Asia y Australia, y en la banda de 850MHz, 900Mhz y 1900 MHz en Norte América y en partes de Latinoamérica y África.

GPRS – (General Packet Radio Services - Servicio General de Paquetes Vía Radio) es una técnica de conmutación de paquetes, que es integrable con la estructura actual de las redes GSM. Un paquete de conmutación mejora de las redes GSM y TDMA para aumentar las velocidades de transmisión de datos.

HTTPS – Hypertext Transfer Protocol Secure (en español: Protocolo seguro de transferencia de hipertexto), más conocido por sus siglas HTTPS, es un protocolo de red basado en el protocolo HTTP, destinado a la transferencia segura de datos de hipertexto, es decir, es la versión segura de HTTP.

IEEE Institute of Electrical and Electronics Engineers – Instituto de Ingenieros Eléctricos y Electrónicos, una asociación técnico-profesional mundial dedicada a la estandarización entre otras actividades, su trabajo es promover la creatividad, el desarrollo y la integración, compartir y aplicar los avances en las tecnologías de la información, electrónica y ciencias en general para el beneficio de la humanidad y de los mismos profesionales.

IMEI – El IMEI o Identidad internacional de equipo de estación móvil, identifican a la terminal móvil GSM (aparato telefónico), es individual y debe ser único. Esto quiere decir, entre otras cosas, que la operadora que usemos no solo conoce, quien y desde donde hace la llamada (SIM) sino también desde que terminal telefónico la hizo (y se puede obtener bastante información a partir de él como puedes comprobar con el programa IMEI INFO). Así mismo la red GSM dispone del REGISTRO DE IDENTIFICACIÓN DE EQUIPOS (EIR). Este registro se utiliza para almacenar las identidades de los equipos móviles clasificadas en tres tipos de listas:

1. blanca: contiene todos aquellos identificativos de equipos que han obtenido la homologación;
2. gris: contiene los identificativos de los equipos que es necesario localizar debido a alguna razón técnica;
3. negra: contiene los identificativos de los equipos robados o utilizados de forma ilegal y también la de aquellos equipos que no pueden acceder al sistema porque podrían producir graves problemas técnicos.

El IMEI tiene 15 cifras (en algunos teléfonos 14, se omite el ultimo digito SPARE normalmente un 0). El IMEI subdivide en varios campos TAC, FAC, SNR y SPARE.

IRDA – (Infrared Data Association) Un estándar para la línea de visión infrarroja entre dispositivos en distancias cortas.

JAILBREAK – Jailbreak es un proceso que permite a los usuarios de los dispositivos iPhone, iPod Touch y iPad ejecutar código no oficial en éstos dispositivos traspasando el mecanismo de distribución oficial de Apple. Consiste en modificar el código de software distribuido por apple. Una vez que el dispositivo

es jailbreakeado, los usuarios pueden descargar varias aplicaciones previamente no disponibles a través de la App Store vía instaladores no oficiales como Cydia, Rock App, Icy, e Installer. Cydia es el más popular y su creador Jay Freeman estima que el 8.5% de todos los iPod y los iPhones han sido jailbreakeados.

MECANISMO DE AUTENTICACIÓN – Un mecanismo de hardware o de software que obliga a los usuarios probar su identidad antes de acceder a datos en un dispositivo.

MMS – Servicio de Mensajería Multimedia, que combina imágenes, sonido y texto en un mismo mensaje. Al igual que los mensajes SMS, se puede enviar a cualquier teléfono móvil con capacidad para leer/enviar MMS. Si el teléfono del destinatario no tiene esta funcionalidad, recibe un mensaje de texto con un enlace para ver el mensaje multimedia en Internet.

NAND – Una puerta lógica, o compuerta lógica, es un dispositivo electrónico que es la expresión física de un operador booleano en la lógica de conmutación. Cada puerta lógica consiste en una red de dispositivos interruptores que cumple las condiciones booleanas para el operador particular. Son esencialmente circuitos de conmutación integrados en un chip.

PDA – (Personal Digital Assistant - Asistente Digital Persona). Una computadora de mano que sirve como herramienta para la lectura y transmisión de documentos, correo electrónico y otros medios de comunicación electrónica a través de un enlace de comunicaciones, y para organizar la información personal, como una base de datos el nombre y dirección, un lista de tareas pendientes y un calendario de citas.

PIM – Gestión de información personal. Un conjunto básico de aplicaciones que proporcionan los equivalentes electrónicos de artículos como una agenda, libreta de direcciones, bloc de notas y lista de recordatorios. El conjunto de tipos de datos como contactos, entradas del calendario, entradas de la agenda, notas, notas y recordatorios mantenido en un dispositivo, que puede ser sincronizado con un ordenador de sobremesa.

PIN – Un PIN (Personal Identification Number o Número de Identificación Personal en castellano) es un valor numérico usado para identificarse y poder tener acceso a ciertos sistemas o artefactos, como un teléfono móvil o un cajero automático.

PKI – En criptografía, una infraestructura de clave pública (o, en inglés, PKI, Public Key Infrastructure) es una combinación de hardware y software, políticas y

procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas como el cifrado, la firma digital o el no repudio de transacciones electrónicas.

PROXY – En el contexto de las redes informáticas, el término proxy hace referencia a un programa o dispositivo que realiza una acción en representación de otro. Su finalidad más habitual es la de servidor proxy, que sirve para permitir el acceso a Internet a todos los equipos de una organización cuando sólo se puede disponer de un único equipo conectado, esto es, una única dirección IP.

PUK – El PUK, acrónimo de Personal Unlocking Key (también conocido como Personal Unlocking Code o Personal Unlock Key) o Clave Personal de Desbloqueo en castellano. Es el código normalmente usado en los sistemas de telefonía móvil que se basan en tecnología GSM (Sistema Global para las Comunicaciones Móviles por sus siglas en inglés Global System for Mobile.) Funciona como una clave o password de 8 dígitos de longitud para desbloquear la tarjeta SIM del equipo móvil cuando se ha olvidado el PIN o bien se ha bloqueado totalmente el teléfono.

RAM – La memoria de acceso aleatorio (en inglés: random-access memory cuyo acrónimo es RAM) es la memoria desde donde el procesador recibe las instrucciones y guarda los resultados. Es el área de trabajo para la mayor parte del software de un computador.

ROAMING – Es la forma de definir la conexión de una línea GSM de un país con los operadores de otros países que también tienen el sistema GSM, sin necesidad de cambiar el número de teléfono.

SIM – (Subscriber Identifycation Module - Módulo Simple de Identificación). Tarjeta usada en GSM que contiene los datos de identificación del usuario de un teléfono móvil, como su número de teléfono.

SMART PHONE – (Teléfono inteligente en español). Es un dispositivo electrónico que funciona como un teléfono móvil con características similares a las de un ordenador personal. Casi todos los teléfonos inteligentes son móviles que soportan completamente un cliente de correo electrónico con la funcionalidad completa de un organizador personal.

SMS – (Short Message System – Servicio de Mensajes Cortos). Servicio disponible en la red GSM que permite el intercambio de mensajes escrito de hasta 160 caracteres entre terminales GSM.

SINCRONIZACIÓN DE PROTOCOLOS – Protocolos que permiten a los usuarios ver, modificar y transferir o actualizar datos entre un teléfono celular y una computadora de escritorio.

SISTEMA DE ARCHIVOS – Un mecanismo de software que define la forma en que los archivos se nombran, almacenar, organizar y acceder a los volúmenes lógicos de la memoria con particiones.

SSID – Identificador de red inalámbrica, similar al nombre de la red pero a nivel Wi-Fi.

TSL/SSL – Secure Sockets Layer -Protocolo de Capa de Conexión Segura- (SSL) y Transport Layer Security -Seguridad de la Capa de Transporte- (TLS), su sucesor, son protocolos criptográficos que proporcionan comunicaciones seguras por una red, comúnmente Internet.

TKIP – Protocolo de Integridad de Clave Temporal. Cifra las llaves utilizando un algoritmo hash y, mediante una herramienta de chequeo de integridad, asegura que las llaves no han sido manipuladas.

USB – Universal Serial Bus. Una interfaz de hardware para periféricos de baja velocidad como el teclado, ratón, joystick, escáner, impresora y dispositivos de telefonía.

UMTS – Tecnología de 3G (Tercera Generación) que permite datos de alta velocidad desde 384Kbps hasta 1.4 MB, y aplicaciones innovadoras como Video Llamadas por el móvil, TV en Vivo, monitoreo de Transito en tiempo real y más.

WARCHALKING – Es la práctica de dibujar en paredes o aceras una serie de simbolos para indicar a otros la proximidad de un acceso inalámbrico.

WARDRIVING – Técnica difundida donde individuos equipados con material apropiado (dispositivo inalámbrico, antena, software de rastreo y unidad GPS) tratan de localizar puntos de de acceso inalámbrico.

WEP – Privacidad Equivalente a Cableado. Es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes inalámbricas que permite cifrar la información que se transmite. Proporciona cifrado a nivel 2. Está basado en el algoritmo de cifrado RC4, y utiliza claves de 64 bits (40 bits mas 24 bits del Vector de inicialización IV), de 128 bits (104 bits más 24 bits del vector de inicialización IV).

WI-FI – (Wireless Fidelity) Conjunto de estándares para redes inalámbricas basado en las especificaciones IEEE 802.11 (especialmente la 802.11b), creado para redes locales inalámbricas, pero que también se utiliza para acceso a internet.

WPA – Protocolo Protegido Wi-Fi. Es un sistema para proteger las redes inalámbricas (Wi-Fi); creado para corregir las deficiencias del sistema previo WEP (Wired Equivalent Privacy - Privacidad Equivalente a Cableado).

WPA2 – Protocolo de Aplicación Inalámbrica. Protocolo de seguridad para redes Wi-Fi, definido en el estándar 802.11i. Reemplaza al protocolo temporal WPA. Se basa en el algoritmo AES y se debe incorporar todos los Puntos de Acceso de última generación.

WTLS – Wireless Transport Layer Security o WTLS (seguridad para la capa de transporte en comunicaciones inalámbricas) es un protocolo de seguridad, perteneciente al conjunto de protocolos de Wireless Application Protocol (WAP).

3G – Es la abreviación de tercera-generación en telefonía móvil. Los servicios asociados con la tercera generación proporcionan la posibilidad de transferir tanto voz y datos (una llamada telefónica) y datos no-voz (como la descarga de programas, intercambio de email, y mensajería instantánea).

3DES – En criptografía el Triple DES se llama al algoritmo que hace triple cifrado del DES. También es conocido como TDES o 3DES, fue desarrollado por IBM en 1978.

802.11 – Familia de estándares desarrollador por la IEEE para tecnologías de red inalámbricas

802.11a – Estándar de conexión inalámbrica que suministra una velocidad de transmisión de 54 Mbps en una banda de 5 GHz

802.11b – Estándar de conexión inalámbrica que suministra una velocidad de transmisión de 11 Mbps en un banda de 2.4 GHz Utiliza la tecnología DSSS (Direct Sequencing Spread). La mayoría de los equipos utilizados en la actualidad son de esta tecnología. No es compatible con el 802.11a funciona en otra banda de frecuencia.

802.11g – Estándar de conexión inalámbrica que suministra una velocidad de transmisión de 54 Mbps en una banda de 2.4 GHz Una de sus ventajas es la compatibilidad con el estándar 802.11b.

802.11i – Estándar de seguridad para redes Wi-Fi aprobado a mediados de 2004. En él se define al protocolo de encriptación WPA2 basado en el algoritmo AES.

RESUMEN

TÍTULO: INSEGURIDAD EN AMBIENTES MOVILES*

AUTOR: GERSON GEOVANNY DELGADO CABALLERO**
PABLO CESAR OSPINA GARCIA**

PALABRAS CLAVES:

Telefonía Móvil, Seguridad, Amenazas, Riesgos.

DESCRIPCIÓN:

La telefonía móvil se ha convertido en una herramienta indispensable para la mayoría de las personas y las organizaciones hoy en día. Pequeños, atractivos y relativamente baratos, estos dispositivos además de permitir la comunicación de voz, se pueden utilizar para diferentes funciones. El envió y la recepción de correo electrónico, el almacenamiento de documentos, gestión de la información personal (PIM) (Agenda Telefónica, Calendario, bloc de notas), Cámara fotográfica, el acceso a internet, la reproducción de video e incluso GPS, la reproducción de mp3 y el acceso remoto a datos.

Mientras estos dispositivos proporcionan beneficios y comodidad para la productividad, también representan nuevos riesgos para las organizaciones. Sin embargo, pueden tener cierto riesgo dependiendo de la perspectiva desde la cual se analice, estos dispositivos poseen una serie de características que podrían tornarlos inseguros si no se tienen en cuenta una serie de parámetros a nivel seguridad.

Este documento proporciona una visión general de la telefonía móvil en uso hoy en día, los riesgos que generan la utilización de esta tecnología y las buenas prácticas de seguridad que le evitaran problemas al usuario y/o a la organización. El documento da detalles acerca de los diferentes sistemas operativos utilizados, las amenazas y los riesgos tecnológicos asociados al uso de estos dispositivos y las garantías ofrecidas para mitigarlos.

* Proyecto de Grado
** Facultad de Ingeniería Físico Mecánicas. Escuela de Ingeniería Eléctrica, Electrónica y Telecomunicaciones. Especialización en Telecomunicaciones. RAMON SUAREZ, Jorge.

SUMMARY

TITLE: INSECURITY IN MOBILE ENVIRONMENTS*

AUTHOR: GERSON GEOVANNY DELGADO CABALLERO**
PABLO CESAR OSPINA GARCIA**

KEY WORDS:

Mobile Telephony, Security, Threats, Risks

DESCRIPTION:

Mobile telephony has become an indispensable tool for most people and organizations today. Small, attractive and relatively inexpensive, these devices also allow voice communication; can be used for different functions. The sending and receiving electronic mail, document storage, personal information management (PIM) (Phonebook, Calendar, memo pad), Camera, Internet access, video playback and even GPS, MP3 playback and remote access to data.

While these devices provide benefits for productivity and comfort, they also pose new risks for organizations. However, there may be some risk depending on the perspective from which to analyze, these devices have a number of features that could be unsafe if not taken into account a wide range of security parameters.

This document provides an overview of the mobile phone in use today, the risks incurred by using this technology and security best practices that will avoid problems the user and/or organization. The document gives details about of the different operating systems used; the threats and technology risks associated with the use of these devices and guarantee to mitigate them.

---

* Work Degree

** Faculty the Engineering Physic – Mechanical. School of Electrical, Electronic and Telecommunications. Master of Telecommunications. RAMON SUAREZ, Jorge.

INTRODUCCIÓN

El medio inalámbrico que utilizan las comunicaciones móviles, el crecimiento acelerado y la introducción de nuevos servicios las hace más susceptibles a problemas relacionados con la seguridad en comparación con los medios cableados y genera preocupación en el medio al no saber cómo controlar los riesgos asociados.

En los últimos años las comunicaciones móviles han sorprendido con un sin número de servicios como comercio electrónico en donde se pueden realizar consultas, transacciones, movimientos de cuentas, pagos y demás utilidades, que ofrece una entidad bancaria desde su teléfono celular; compra de artículos en tiendas virtuales, mercadeo sensible con respecto a la ubicación geográfica del usuario, recepción de información desde sitios web, como por ejemplo, resultados de apuestas, acciones de la Bolsa, noticias, todo esto con un modelo de seguridad no del todo fiable.

La tecnología celular está generando expectativas entre los operadores de redes móviles, nuevos proveedores de servicios y usuarios con los avances tecnológicos y la idea de disponer de un equipo móvil con alta capacidad de comunicación, posibilidades de transmisión de datos y una gama de servicios mucho más extensa.

Para certificar la seguridad en la red y el acceso en los dispositivos móviles es necesario garantizar la seguridad en los diferentes componentes del ambiente móvil; dispositivo móvil (teléfonos inteligentes y dispositivos híbridos como BlackBerry), sistema operacional (Symbian OS, Windows CE, Palm OS), aplicación móvil (mensajería instantánea, juegos) y tecnología de comunicación (bluetooth, 802.11b).

Es por esto, que el presente trabajo pretende estudiar un esquema de seguridad para dispositivos móviles, con base en recomendaciones de seguridad de proveedores y algunos entes especializados, como lo es el Instituto Nacional de Normas y Tecnología, NIST (National Institute of Standards and Technology); para documentar dichas recomendaciones y elaborar un informe completo para que sea usado como material de consulta.

1. SISTEMAS OPERATIVOS MÓVILES

1.1 SYMBIAN OS

Figura 1. Logotipo Symbian
Imagen tomada de: http://www.symbian.org/

En junio de 1998 se crea Symbian, una empresa conjunta entre Psion y los principales fabricantes de telefonía móvil: Nokia (47.9%), Panasonic (10.5%), Samsung (4.5%), Siemens (8.4%) y Sony Ericsson (28.7%). Sus orígenes provienen de su antepasado EPOC32, la cual fue rebautizada posteriormente como sistema operativo Symbian.

Symbian es un sistema operativo (OS) diseñado para dispositivos móviles y teléfonos inteligentes (smart phones). Está diseñado para residir en un espacio muy pequeño, hacer un uso dinámico de escasos recursos de memoria, administrar eficientemente la energía y soportar en tiempo real los protocolos de comunicación y telefonía. Actualmente el sistema operativo Symbian acoge al mayor número de terminales móviles en el mundo.

A pesar de su amplio mercado, este tiende a decrecer debido a la llegada de los teléfonos inteligentes (smart phones), especialmente al revolucionario iPhone de Apple y al crecimiento de RIN Blackberry. En junio de 2008, Nokia compró el sistema operativo Symbian y lo ha liberado bajo licencia libre Eclipse Public License EPL. Esta medida fue tomada para competir en el mercado con el sistema operativo de Microsoft Windows Mobile, el cual se debe comprar para así poder ser instalado en un dispositivo móvil.

El objetivo era establecer la Fundación Symbian y convertir este sistema operativo en una plataforma abierta, todo esto para competir con el empuje de otras soluciones como Android de Google. De todos modos, con una cuota del 52% en el mercado mundial, Symbian sigue siendo una fuerza a tener en cuenta.

1.1.1 Detalles de Symbian OS

Tenga en cuenta que esto no será un examen exhaustivo del sistema Operativo Symbian OS, se enfatizará solo en lo que corresponde al ámbito de aplicación del código malicioso y su interacción con el sistema operativo y el usuario.

1.1.2 Sistema de Archivos

El sistema de archivos de los dispositivos Symbian se basa en el formato FAT. Siendo este un factor muy significativo en lo que respecta al sistema de archivos, ya que se cuenta con un alto nivel de soporte. Se utiliza para el almacenamiento de datos del usuario en la NAND Flash, unidades de memoria RAM interna, y medios extraíbles. El malware no infecta un dispositivo Symbian, se encuentra inactivo hasta que se copia en una máquina Windows. Una vez allí, y suponiendo que la víctima lo ejecuta, el archivo se infecta en el escritorio de la víctima.

1.1.3 Sistema Operativo

El actual sistema operativo Symbian se basa en el núcleo EKA2, diseñado para el procesador ARM. Una de las mejoras clave del núcleo EKA2 es su capacidad para manejar el teléfono. Algunos de los conceptos avanzados construidos en el núcleo son el Wi-Fi, sincronización de Exchange, la desfragmentación de la RAM (se incrementa la eficiencia de RAM), la gestión de memoria para reducir el consumo de energía (almacenamiento de datos en la memoria RAM requiere energía), gestión de archivos, servicios multimedia, ente otros.

El núcleo de Symbian subcontrata las extensiones, servicios y controladores de capas en la parte superior del nanokernel "para maximizar la estabilidad del dispositivo. También a diferencia de otros sistemas operativos, existen diferentes versiones del sistema operativo Symbian, por lo que una aplicación que se ejecuta en un tipo de dispositivo no puede funcionar en otro.

Kernel Architecture (EKA2) es el hardware y el núcleo principal. Gestiona los recursos de la CPU y la memoria del teléfono, y proporciona una arquitectura de controladores al dispositivo para administrar los recursos de hardware. El núcleo tiene una arquitectura de capas para que puedan ser transportados a un hardware diferente.

1.1.4 Seguridad

Una de las principales prioridades para los dispositivos Symbian es la seguridad. La cuestión es tan importante que Symbian realiza un gran esfuerzo para asegurar

que sea muy difícil para alguien atacar el sistema de forma remota y toman las medidas necesarias para cerrar los agujeros presentes. Además, cada nueva versión incluye algunas características significas en la protección. Pero a pesar de todas las protecciones los usuarios siguen siendo el eslabón más débil ya que son ellos los que instalan aplicaciones que en su mayoría son realmente dañinas.

1.1.5 Plataforma de Seguridad

El propósito de la arquitectura de la plataforma de seguridad Symbian es permitir a los usuarios utilizar sus dispositivos móviles de una manera fácil y confiable y a su vez, brindarle la capacidad de defenderse contra los programas maliciosos. La plataforma Symbian permite que las aplicaciones utilicen la arquitectura de la Plataforma de Seguridad a fin de obtener acceso a las funciones sensibles dentro de la plataforma. La plataforma de seguridad Symbian aborda tres conceptos: Capabilities, Application signing, Data caging.

- **Capabilities (Capacidades)**
  Permite a la plataforma Symbian controlar los permisos que poseen las aplicaciones para ejecutarse. El acceso a las capacidades está determinado por la configuración del dispositivo y la forma en que la solicitud haya sido firmada. Las API que dan acceso a esta funcionalidad se encuentran protegidas por una serie de capacidades. Hay veinte posibilidades, y se dividen en cuatro grupos:
  - *User capabilities (Capacidades del usuario)*
  - *System capabilities (Capacidades del sistema)*
  - *Restricted capabilities (Capacidades restringidas)*
  - *Device manufacturer capabilities (Capacidades del Fabricante)*

- **Application Signing (Aplicación de Firma)**
  Todas las aplicaciones Symbian deben ser firmadas antes de que puedan ser instaladas. La firma es una forma de codificación de un certificado digital en el archivo de instalación de la aplicación. El certificado identifica a los proveedores de la aplicación, y se otorga acceso a las capacidades (Capabilities) definidas durante el proceso de construcción.

- **Data Caging**

Significa que cada aplicación corre en sus propios procesos y tiene acceso solo a su propio espacio de memoria. Las aplicaciones y los usuarios sólo tienen acceso a ciertas áreas del sistema de archivos. En la práctica, las aplicaciones pueden

acceder a sus propias carpetas y carpetas privadas que están marcadas como abiertas. Esto significa, por ejemplo, que una aplicación no puede acceder a la carpeta privada y los datos de otra aplicación.

1.1.6 Firma de Código

Además de las características antes mencionadas de la Plataforma de Seguridad que contribuyen a que el dispositivo Symbian sea más seguro, un componente principal es el de “code-signing”. Que consiste en firmar digitalmente los ejecutables y scripts para confirmar el autor del software y garantizar que el código no ha sido alterado o dañado desde que fue firmado por el uso de un hash criptográfico.

1.2 RIM (BlackBerry)

Figura 2. Logotipo BlackBerry
Imagen tomada de: http://www.blackberry.com/

Este sistema operativo desarrollado por la empresa RIM (Research In Motion), incluye aplicaciones típicas de Smartphone (libreta de direcciones, calendario, listas de tareas, etc.), es fundamentalmente conocido por su capacidad para enviar y recibir correo electrónico de internet.

Este sistema operativo ha sido diseñado principalmente para entornos empresariales, permitiendo extender los servicios de información de la empresa como acceso al correo e información corporativa a los empleados móviles.

Uno de los aspectos importantes al tratarse de un entorno empresarial, es que se pueda realizar una gestión centralizada de los dispositivos distribuidos a los empleados. Esta característica proporcionada por BlackBerry permite a los administradores poder establecer los parámetros de seguridad de forma centralizada para todos los usuarios (o grupos de usuarios), utilizando el servidor BES (BlackBerry Enterprise Server). Además un administrador puede decidir

eliminar todos los datos de un terminal BlackBerry si se determina que éste ha sido robado o perdido, controlar y definir cuáles smart phones tienen permiso para realizar determinadas actividades, tales como envío de correos electrónicos, acceso a Internet o a determinadas aplicaciones corporativas; controlar el acceso a Internet y a la Intranet, según la política de acceso de la empresa y bloquear recursos de los smart phones, como cámara fotográfica, red Wi-Fi o bluetooth.

1.2.1 Detalles BlacBerry

Una de las cualidades positivas de la BlackBerry es que el sistema operativo fue diseñado exclusivamente para el hardware. Como resultado, los usuarios suelen encontrar una sincronía que no existe en los dispositivos de Windows Mobile. Como el dispositivo está diseñado por BlackBerry, controla cómo funciona el software y a su vez provee un enorme impacto en la seguridad.

Al igual que la mayoría de los dispositivos móviles, la mayoría de los BlackBerries utilizan el procesador ARM o Xscale por sus características de bajo consumo de energía. Además de esto, RIM ha diseñado un sistema operativo propietario donde posee totalmente el control.

La interfaz y todas las aplicaciones de BlackBerry están diseñadas bajo Java Micro Edition, que a su vez añade una capa de protección al dispositivo. Los desarrolladores de Blackberry pueden descargar un kit de desarrollo de software para el JDE (Java Development Environment), pero tendrá que pagar una cuota de certificación de $100 para el acceso a las API que son necesarias. Este es un obstáculo financiero para los desarrolladores, pero también es un obstáculo financiero para los potenciales creadores de malware que tienen que obtener su código firmado para que sea eficaz.

1.2.2 Plataforma BlackBerry

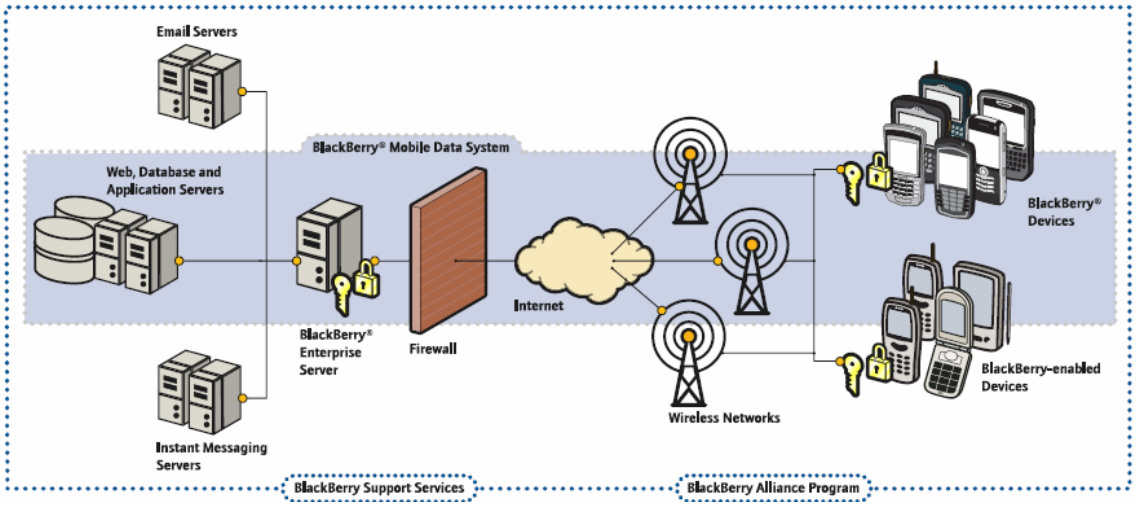

Figura 3. Arquitectura de Blackberry
Imagen tomada de: http://www.cybsec.com/upload/CYBSEC_Seguridad_Blackberry_Sobrero.pdf

Los elementos que forman una plataforma basada en BlackBerry son los dispositivos móviles y teléfonos inteligentes (smart phones); la infraestructura BlackBerry Mobile Data System (BlackBerry MDS) optimizada para crear, implementar y administrar aplicaciones para BlackBerry Enterprise Solution; los dispositivos BlackBerry Enabled que son los dispositivos BlackBerry Connect (incluyen la tecnología de transmisión de BlackBerry, pero corresponden a otros fabricantes, y permiten la conexión con BlackBerry Enterprise Server) y los dispositivos BlackBerry Built-In (integran todas las funcionalidades de BlackBerry, como el correo electrónico, calendario, contactos, explorador, tareas y bloc de notas); la BlackBerry Alliance Program que agrupa una gran comunidad de proveedores de software, integradores de sistemas y proveedores de soluciones independientes que ofrecen aplicaciones, servicios y soluciones para BlackBerry Enterprise Solution; los Servicios de asistencia técnica de BlackBerry y el servidor BlackBerry Enterprise Server (BES) que es el nodo central de la plataforma.

El BES ofrece herramientas para administrar todos los smart phones de la compañía, lo que se conoce también como Mobile Device Management. Esa solución permite asegurar que todos los smart phones siguen rigurosamente las políticas de seguridad de la empresa maximizando la protección de la información. Estas políticas de seguridad se pueden alterar y replicar inmediatamente a todos los smart phones de la empresa.

Se destaca por ofrecer gestión de infraestructura, utiliza una tecnología propia de transmisión de datos que compacta toda la información que se envía a los smart phones, reduciendo el tiempo de descarga ya que el volumen de datos en circulación es menor. La alta compactación de los datos también es un aspecto relevante de BlackBerry, eso explica el hecho de que sea la plataforma típicamente elegida por usuarios que viajan con frecuencia y, por lo tanto, utilizan datos bajo la modalidad de roaming por encontrase fuera de su área de cobertura. Los correos electrónicos se entregan en forma push, es decir, todo correo electrónico que se recibe es activamente entregado en su smart phone, sin que se necesite tener una transmisión de datos constante para verificar si hay un correo electrónico por llegar.

1.2.3 Seguridad

Comparte muchas de las características de seguridad incorporadas en Symbian OS y Windows Mobile como criptografía, PKI, comunicaciones TLS/SSL y WTLS.
Es necesario proteger la información de mensajería y los datos corporativos ya que el canal de transmisión es inseguro. Para conseguir esto, el dispositivo BlackBerry y el servidor BES (BlackBerry Enterprise Server) cifran la comunicación utilizando un sistema de clave simétrica 3DES o AES. Estas claves son establecidas durante el proceso de activación del dispositivo (enrollment).

En el caso de comunicaciones con servidores de Aplicaciones o con Internet, es posible que éstas vayan protegidas con HTTPS entre el servidor BES (BlackBerry Enterprise Server) y Servidor de aplicaciones (modo proxy), e incluso utilizar HTTPS de extremo a extremo, obteniendo una mayor seguridad, ya que el BES (BlackBerry Enterprise Server) no actúa como punto débil en los datos transmitidos.

BlackBerry ofrecen seguridad no sólo para los mensajes, sino también para acceder a Internet y ejecutar con rapidez las aplicaciones de misión crítica de su empresa. En el smart phone, la misma plataforma impide que programas maliciosos ejecuten acciones que pondrían en riesgo la seguridad de la información del dispositivo. En la red, la plataforma BlackBerry cuenta con los NOCs (Network Operation Centers), que son los centros de seguridad para la solución. Todos los datos que circulan por los terminales BlackBerry pasan por uno de los NOCs (Network Operation Centers) BlackBerry, que detectan y filtran cualquier ataque o amenaza que puedan poner en riesgo la seguridad de la información de su empresa. Los NOCs (Network Operation Centers) aseguran la

integridad de los datos, pero no acceden en éstos, es decir, no conocen el contenido de los mensajes.

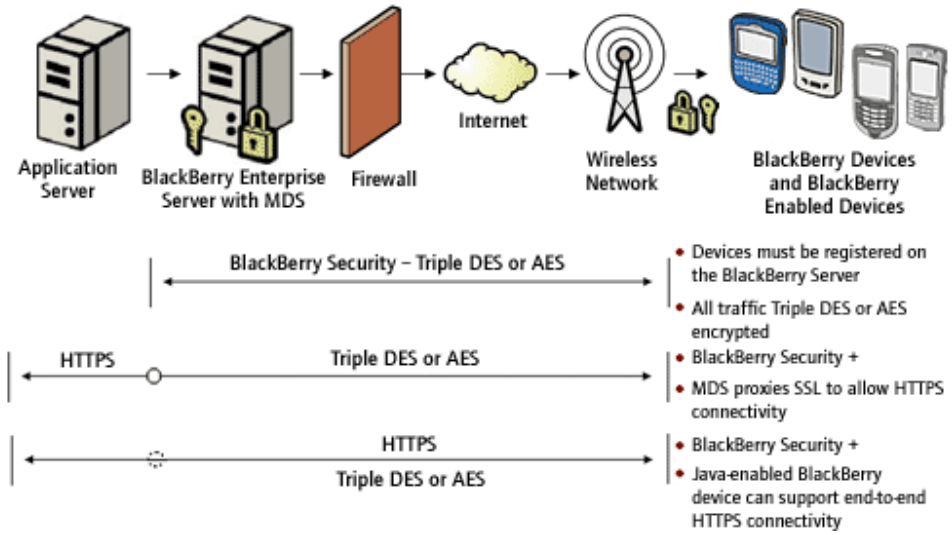

Figura 4. Arquitectura de seguridad de Blackberry
Imagen tomada de: http://www.isecauditors.com/downloads/present/igc2005-seguridad-dispositivos-moviles.pdf

1.3 WINDOWS MOBILE

Figura 5. Logotipo Windows Mobile
Imagen tomada de: http://www.microsoft.com/windowsmobile/en-us/default.mspx

Windows Mobile (WM) es el esfuerzo e intento de Microsoft de implementar su experiencia de escritorio en un dispositivo móvil. Esta plataforma ofrece todos los componentes necesarios que se puede esperar en un dispositivo móvil, y además, se extiende mucho más allá del sistema operativo central debido a la existencia de decenas de miles de programas de terceros que los usuarios pueden descargar e instalar en este dispositivo. Si bien tuvo un gran comienzo, en los últimos años ha

visto Windows Mobile una tasa de crecimiento bastante alta y ha madurado como sistema operativo.

En la actualidad, hay tres versiones de Windows Mobile (WM): WM Standard (smart phone tradicional), WM Profesional (smart phone con pantalla táctil), y WM Classic (PDA sin teléfono).

Una de las claves del éxito de Windows Mobile (WM) es su asociación con HTC, un proveedor de dispositivos móviles, con el que llevan trabajando desde 2001. Gracias a esta relación a largo plazo, con el tiempo se ha desarrollado una comunidad que ha ayudado a impulsar “el factor geek" y ha hecho que los dispositivos HTC estén corriendo Windows Mobile haciéndolo mucho más popular.

Las aplicaciones de Windows Mobile (WM) son muy fáciles de elaborar debido a que la firma de código “code-signing” no es un requisito para que una aplicación pueda ser instalada, cualquiera puede pasar un par de horas desarrollando una aplicación y esperar que funcione en cualquiera de los millones de dispositivos que hay.

1.3.1 Detalles de Windows Mobile

Tenga en cuenta que esto no será un examen exhaustivo del sistema Operativo Windows Mobile (WM), se enfatizará solo en lo que corresponde al ámbito de aplicación del código malicioso y su interacción con el sistema operativo y el usuario.

1.3.2 Sistema de Archivos

El sistema de archivos de los dispositivos de Windows Mobile es algo similar a lo que maneja Microsoft en sus demás productos. Los archivos de los programas normalmente se almacenan en \Archivos de programas, los archivos del sistema se encuentran en \Windows y los archivos personales se almacenan en \Mis documentos. Si bien el sistema de archivos de almacenamiento superficial es bastante estándar, ciertas características deben ser comprendidas.

1.3.3 Xip (eXecution In Place)

Normalmente, cuando un archivo es ejecutado, primero se copia en la memoria RAM. Sin embargo, debido a las limitaciones de recursos (tanto para poder mantener el estado y el tamaño de la memoria RAM), muchos de los ejecutables de Windows Mobile (WM) /DLL son capaces de ser ejecutadas en su lugar (XIP).

El resultado final, en cuanto a malware, es que estos archivos no pueden ser alterados o borrados.

1.3.4 Cifrado

La pérdida o robo de los dispositivos móviles ha sido un gran problema para los usuarios, debido a que en él se almacenan y se encuentran todos los datos sensibles, ya sean de tipo personal o empresarial. Mientras el dispositivo móvil y el sistema de archivos se pueden proteger con una contraseña, cualquier tarjeta de memoria externa puede ser removida. Para ayudar a mitigar este riesgo, Microsoft incluyó con el sistema operativo un sistema de cifrado que puede cifrar tarjetas de memoria. Por desgracia, si el dispositivo sufre un fallo electrónico o un “hard reset” restablecimiento completo del sistema operativo, todos los datos de la tarjeta quedan para siempre cifrados. Esto es porque es creado un ID (Identificación) único cuando ocurre un “hard reset” el cual amarra al proceso de cifrado. Por esta razón, al realizar un “hard reset” a un dispositivo con malware este puede también afectar a los datos en la memoria externa.

Un restablecimiento completo (hard-reset) o un fallo electrónico pueden dejar archivos cifrados en una tarjeta de memoria externa de manera permanente, por el hecho de que parte de la rutina de cifrado incluye un valor único de identificación (ID) que es creado cuando un dispositivo se restablece o vuelve a su estado original.

1.3.5 Firma de Código

Una de las mayores amenazas que enfrentaron las primeras versiones de Windows Mobile (WM) fue el hecho de que cualquier ejecutable (por ejemplo, EXE, DLL, etc.) podría tener acceso completo a todos los recursos en el dispositivo. Para ayudar a mitigar esta amenaza, Microsoft implementó la firma de código en Windows Mobile 5. En resumen, cuando cualquier módulo ejecutable (por ejemplo, EXE, DLL, CPL) se va ejecutar, la firma de código se extrae y se analiza una serie de certificados y la política de dicho dispositivo para saber en que 'modo' o grupo de código del módulo se ejecutará, para el Smartphone hay dos grupos de código: Normal; Ejecutar con restricciones de acceso a ciertas API's y otros activos, y de confianza; se ejecutan con pleno acceso a todos activos en el dispositivo. Windows Mobile 5.0 Pocket PC tiene un grupo de código: de confianza.

Los grupos de código se mantienen en proceso de granularidad que significa que se carga la DLL en un espacio del proceso donde se debe ejecutar en el mismo

grupo de código que el exe. Por lo tanto hay algunas restricciones que impone el cargador durante la carga del archivo DLL, por ejemplo un exe que se ejecuta en el grupo de código de confianza no puede cargar un archivo DLL que se resuelve en el grupo de código normal, de lo contrario el archivo DLL automáticamente recibirá una elevación de privilegios. Por el contrario un grupo de código de confianza de DLL cargadas por un exe que se ejecuta en el grupo de código normal, obligará a la DLL en el grupo de código normal coincidir con el proceso que contiene.

Irónicamente, la firma de código no ha sido muy eficaz para detener el malware. Debido a que la firma tiene costos, la mayoría de los desarrolladores simplemente no firman su código, solicitan al usuario el permiso de instalación. Como resultado, el usuario típico siempre permitirá que un archivo se ejecute, ya que es un procedimiento operativo estándar al utilizar un dispositivo Windows Mobile (WM).

1.3.6 Sistema Operativo

Es técnicamente una versión de Windows CE. En el transcurso de los años, Microsoft ha realizado cambios muy significativos en el sistema operativo que ha impactado en su usabilidad, seguridad, gestión de procesos, gestión de memoria, almacenamiento de archivos, entre otros. En esta sección, vamos a ver algunas de las mejoras más significativas del sistema operativo y por qué son importantes en cuanto a malware.

1.3.7 Modo Núcleo Vs Modo Usuario

Como la mayoría de los sistemas operativos, Windows CE tiene un Modo Núcleo y un Modo Usuario. El termino modo se utiliza para describir el nivel de acceso de un hilo del proceso que se ejecuta en un dispositivo.

En Windows Mobile (una versión de Windows CE), el modo núcleo es un nivel de de acceso de privilegios que da a los hilos del proceso control directo sobre los recursos de hardware (por ejemplo, la capacidad de leer y escribir directamente hacia y desde la RAM). Los hilos en modo usuario, en cambio, no tienen acceso directo a los recursos del modo núcleo. En su lugar, tiene que pasar por el núcleo y dejar que el núcleo maneje el acceso. Esto esencialmente evita que el código malicioso haga cosas que no debería.

En versiones de Windows CE antes de la versión 6, era posible poner un hilo dentro y fuera del modo núcleo a través de código en modo usuario a través de la API SetKMode. Esto, en esencia era una laguna enorme a través del cual un

atacante podría obtener acceso de bajo nivel a los recursos a nivel del núcleo. Desde la versión 6, todavía queda un camino en el que un atacante podría dar al código de usuario el acceso directo al modo núcleo. En concreto, si un hilo de modo usuario pasa una llamada a la función de modo núcleo la función a su vez ejecuta una función que está en el espacio de modo usuario, el código dará acceso con permiso a nivel de kernel.

A partir de Windows CE 6, todos los componentes críticos del sistema operativo que antes estaban en el modo usuario se mueven al núcleo. Esto ayudó a aumentar el rendimiento porque los servicios se encuentran ahora dentro del núcleo y pueden regresar los resultados directamente a través de la aplicación en lugar del núcleo, como ocurre con las versiones anteriores. En esencia, esta medida elimina pasos adicionales sin tener que preocuparse acerca de la compatibilidad con las versiones anteriores.

1.3.8 Drivers

El sistema operativo central es casi lo mismo en todos los dispositivos de Windows Mobile (WM), es increíble la cantidad de variaciones que hay en el producto final. Cada dispositivo tiene su propio hardware, el cual debe trabajar con Windows Mobile, por esta razón el fabricante de equipos originales (OEM - Original Equipment Manufacturer) debe agregar los drivers propios de terceros para la imagen final que se coloca en el dispositivo móvil. En Windows Mobile 6, existen dos cargadores de drivers: device.dll y udevice.exe. El primero forma parte del núcleo y maneja los drivers en modo kernel. El segundo, realmente controla los driver en modo usuario y puede ser cargado múltiples veces. Los drivers en udevice.exe, van a estar estables pero altamente regulados por el núcleo a través de un reflector que verifica y apodera las solicitudes realizadas por el espacio del kernel. La estabilidad se logra debido a que cada driver puede estar en su propio espacio de memoria y un accidente en uno de ellos no afecta al otro. Los drivers del núcleo de terceros deben ser hechos, y realmente sólo se limitan a los dispositivos que son de alto rendimiento, como los dispositivos de red. Esto se debe a que la instalación de un driver a nivel del kernel de terceros abre agujeros de seguridad potenciales. La realidad es que los drivers de otros fabricantes no suelen ser tan seguros o tan estables como los componentes del núcleo central, lo cual podría conducir a que un exploit tenga acceso a nivel del kernel.

1.3.9 Memoria / Proceso de Limitación

Antes de Windows Mobile 6, hubo algunas limitaciones significativas en el proceso y las asignaciones de memoria. En concreto, un dispositivo Windows Mobile sólo

podía aguantar 32 procesos, cada uno con un máximo de 32 MB de memoria. En Windows Mobile 5, el resultado fue un mapa de memoria virtual total de 4GB. Los dos primeros fueron asignados al núcleo, el tercero fue asignado para un espacio de memoria compartida, y el tercero estaba compuesto por pedazos de 32*32 MB, como se ilustra en la Figura 6 (uno por cada proceso).

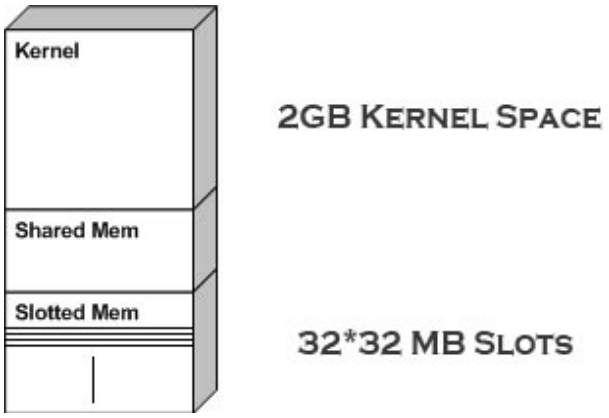

Figura 6. Memoria Windows Mobile 5
Imagen tomada de: http://www.microsoft.com/Windowsmobile/en-us/default.mspx

Con Windows CE 6, la memoria de núcleo unificada sigue siendo del mismo tamaño, pero ahora cada proceso tiene su propio proceso de 2 GB de espacio dedicado (ver Figura 7). Además, el número de procesos se incrementó a un teórico de 32.000. Además del aumento de tamaño, un pedazo de memoria virtual no está compartiendo espacio con cualquier otro proceso. Esto ayuda a mantener el sistema más estable para reducir el impacto de choque y la corrupción de espacio compartido, y también ayuda a mitigar las amenazas a la seguridad a través de los problemas de memoria compartida.

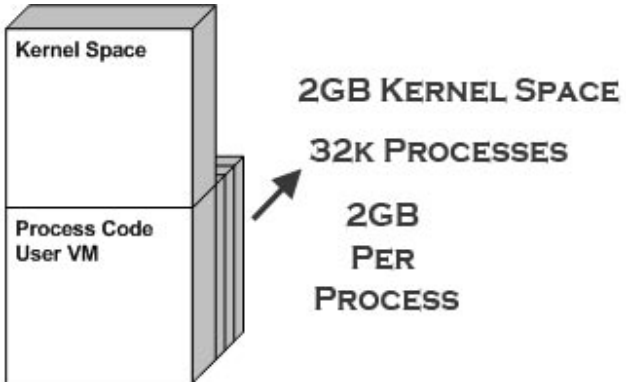

Figura 7. Memoria Windows Mobile 6
Imagen tomada de: http://www.microsoft.com/Windowsmobile/en-us/default.mspx

1.4 iPhone OS X

Figura 8. Logotipo iPhone OS X
Imagen tomada de: http://www.apple.com/es/

En el 2002 después de sacado el primer iPod a la venta, Steve Jobs empezó a tener la idea de crear un teléfono como un solo instrumento, debido a que observaba en la gran mayoría de las personas como cargaban teléfonos, blackberries y reproductores MP3. Esto le dio una visión para proteger su nueva línea de productos, que era la de aventurarse en el mundo de los inalámbricos. A mediados del 2005, el presidente de Apple Steve Jobs ya había encargado el desarrollo del iPhone a unos 200 ingenieros de los mejores de su compañía. El prototipo presentaba muchas fallas, las llamadas se perdían constantemente, la batería no se cargaba eficientemente, la información y las aplicaciones no funcionaban correctamente volviéndose inutilizables. Tanto así, que al final de la demostración Steve Jobs llego a la conclusión que todavía no tenía un producto.

El iPhone iba a ser uno de los productos expuestos en la convención anual Macworld de Apple que se llevaría a cabo el 9 de enero de 2007, siendo este la pieza central del evento, por lo tanto si el iPhone no estaba listo a tiempo la convención sería un fracaso y el precio de las acciones de la compañía se vería afectado en gran manera.

Para la creación del iPhone Steve Jobs logro obtener la colaboración exclusiva de AT&T Mobility (llamada Cingular en ese tiempo) convirtiéndose en la única empresa telefónica de iPhone. Los términos de negociación con una de las más grandes industrias de los celulares fueron de muy buena rentabilidad para Steve Jobs y retuvo el control total sobre el diseño, manufactura, y mercado del iPhone, quitándoles el poder a las empresas telefónicas y otorgándoselo a los fabricantes, desarrolladores, y consumidores generando un cambio sustancial en el negocio de los teléfonos celulares.

Después de un duro y estresante trabajo por parte del grupo de ingenieros, Steve Jobs a solo unas semanas antes de la convención Macworld ya tenía un prototipo para mostrar a los asistentes, medios de comunicación y a su gran socio AT&T Mobility. Seis meses después, el 29 de Junio de 2007 el primer iPhone salió a la venta en E.E.U.U, al mismo tiempo Apple saco la versión 7.3 de iTunes, la cual contiene el soporte para los servicios de activación y sincronización del iPhone. Ese fin de semana Apple vendió 270.000 iPhones en las 30 primeras horas. Poco después estuvo disponible en otros 5 países: Irlanda, Reino Unido, Francia, Alemania y Austria. El 11 de julio de 2008, Apple lanzó el iPhone 3G en 22 países, incluyendo los 6 originales, esperando lanzar el producto en más de 48 países durante los meses siguientes.

1.4.1 Sistema Operativo

El sistema operativo del iPhone es una versión minimizada del Mach kernel que se encuentra en Mac OS X, el mismo sistema operativo de Apple que se instala en una PC Mac o Laptop Mac, denominado iPhone OS. La diferencia entre el iPhone y el Mac es que este incluye la mayoría de las extensiones, o controladores de hardware, en el kernel. Además adiciona al kernel las extensiones del puerto USB, la pantalla táctil y demás componentes necesarios para garantizar comunicaciones y la transferencia de datos.

IPhone OS tiene 4 capas de abstracción: la capa del núcleo del sistema operativo, la capa de servicios principales, la capa de medios de comunicación y la capa de Cocoa Touch. El sistema operativo ocupa bastante menos de medio gigabyte del total del dispositivo, de 8 GB o de 16 GB.

Dado que se trata esencialmente de OS X, el sistema de archivos es bastante previsible. Todos los archivos personales se almacenan en el directorio de la carpeta /var/root, que tiene una subcarpeta denominada Biblioteca que almacena la información generada por el uso normal (es decir, los mensajes de correo, historial del Safari, el contenido de YouTube, etc.) Todos los archivos multimedia, como imágenes, vídeos y archivos de música se almacenan en la carpeta /Media.

Cuando una aplicación se instala, se coloca en el directorio /Applications fuera el directorio raíz (root). Más allá de esto, el sistema de archivos es despojado hasta el punto en el que los principales archivos que usted esperaba encontrar en un sistema BSD (Berkeley Software Distribution - Distribución de Software Berkeley) no existen (por ejemplo, ls, sh, cat).

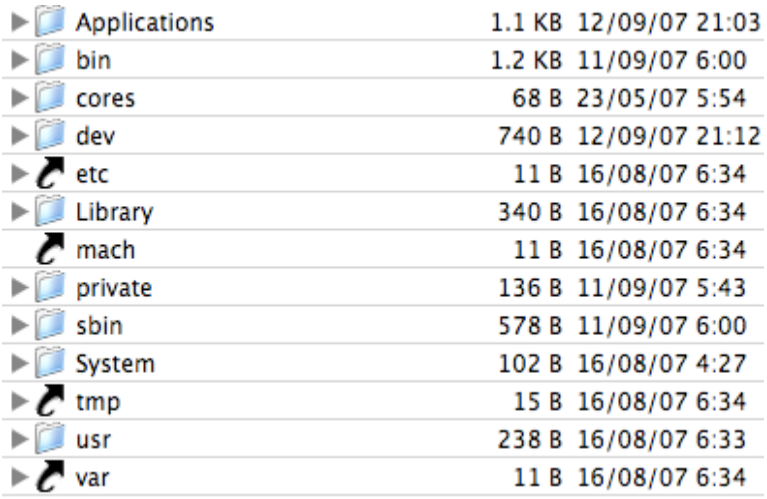

Figura 9. Sistema de Archivos iPhone
Imagen tomada de: Autor Proyecto

1.4.2 Aplicaciones

Apple diseñó el iPhone para tener una interfaz bien controlada y permitir el soporte aplicaciones. Las aplicaciones para iPhone tendrán que obtenerse a través de iTunes, donde solo se puede acceder a lo que Apple permite acceder. El soporte a las aplicaciones de otros fabricantes de Apple no estuvo disponible para el iPhone desde hace casi un año después de su lanzamiento.

Debido a esto la comunidad de hackers a menos de un mes después de su lanzamiento estaban muy ocupados en la creación e instalación de aplicaciones

en sus iPhones. De hecho, la comunidad iPhone hacking ha desarrollado una cadena de herramientas de código abierto que se considera más potente que lo que Apple ha proporcionado con su kit de desarrollo de software.

Para el usuario medio, que nunca ha escuchado el término Jailbreak, todas las aplicaciones adicionales tendrán que obtenerse a través de iTunes. Esto, sin embargo, viene con los costos y los peajes. Cabe señalar que la instalación de aplicaciones de terceros fuera del entorno de iTunes puede ser arriesgada, porque no hay garantía de que el código no contiene algo dañino.

Sin embargo, el acceso a las aplicaciones de terceros que requieren que un usuario realice "jailbreak" a su teléfono y el tomar esos riesgos, trae beneficios que bien valen la pena, ya que hay numerosos programas que pueden ser libremente añadidos a la interfaz del iPhone.

Los desarrolladores que deseen crear aplicaciones para el iPhone tienen dos caminos. El primero es utilizar el kit de desarrollo de software de Apple y, posteriormente, ofrecer la aplicación a través de iTunes. El segundo es utilizar la serie de herramientas de código abierto, que le permitirá ofrecer su aplicación a cualquier persona que haya pasado por el proceso de Jailbreak.

1.5 ANDROID

Figura 10. Logotipo Android
Imagen tomada de: http://www.android.com/

Android es un sistema operativo para dispositivos móviles, basado en el núcleo de Linux, basado en el software libre, es actualmente es el motor de los dispositivos comercializados por Google. Creado por la *Open Handset Alliance,* alianza tecnológica encabezada por Google, acompañada de compañías del nivel de T-Mobile, HTC, Motorola, Telefónica, Samsung, Intel o Nvidia.

La primera versión de un teléfono móvil Android fue el G1 T-Mobile G1/HTC Dream anunciado el 23 de septiembre de 2008, lanzado de forma exclusiva para Estados Unidos.

Figura 11. G1 T-Mobile G1/HTC Dream
Imagen tomada de: http://www.t-mobileg1.com/#/g1-demo-one-touch-google-search/

La característica más importante es que se trata de una plataforma totalmente abierta tanto para fabricantes de dispositivos móviles como para desarrolladores de aplicaciones. En su núcleo, Linux, están escritas las librerías que se encargan de las funcionalidades básicas. Estas librerías están escritas en C/C++ y pueden ser accedidas directamente desde los programas de la plataforma. Algunas de ellas son; librerías en C del sistema, librerías multimedia, gestor de superficies, librería del núcleo web, SGL (motor gráfico 2D), librerías para 3D, freetype y SQLite.

Android también proporciona al desarrollador un completo Framework Java, un intento de normalización de la cantidad de especificaciones en que se ha convertido J2ME, es totalmente compatible con cualquier tipo de transmisión por lo que funcionará igual sobre dispositivos que usen GPRS con otros que usen 3G. Las interfases gráficas de usuario están diseñadas usando archivos XML que además de fáciles de diseñar permiten al equipo representar las interfases en la mayor parte de los casos independientemente de las dimensiones de la pantalla, las aplicaciones están escritas en Java pero tienen acceso directo a bajo nivel a través de la API.

1.5.1 Arquitectura Android

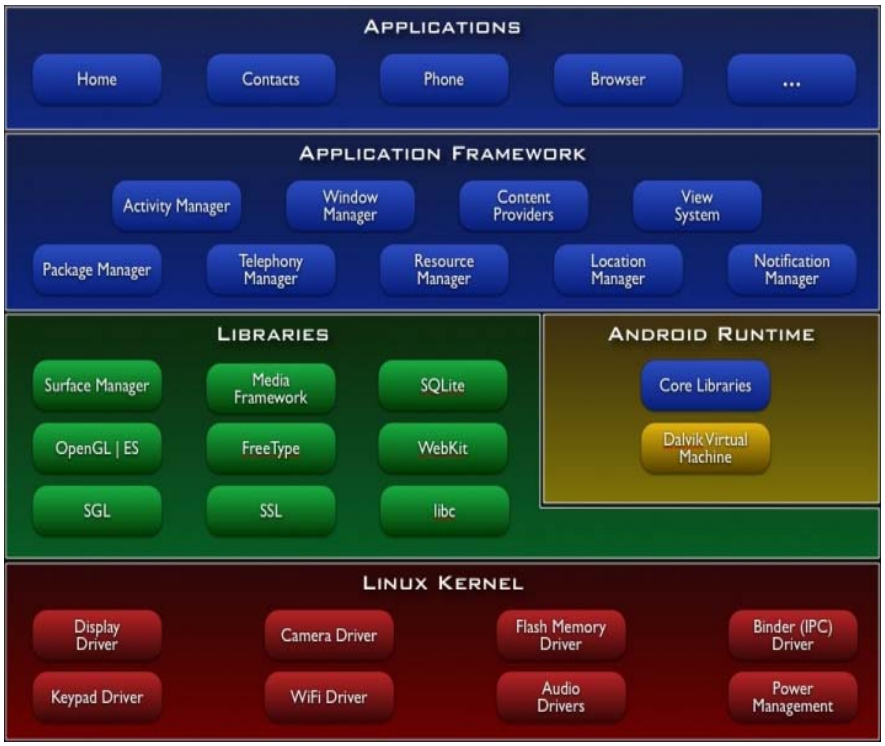

Figura 12. Arquitectura Android
Imagen tomada de: http://developer.android.com/guide/basics/what-is-android.html

La arquitectura está compuesta por librerías que proporcionan un conjunto de funciones básicas compartibles y reusables, a continuación se describen sus capas:

- **Aplicaciones:** incluyen como base un cliente de email (correo electrónico), calendario, programa de SMS, mapas, navegador, contactos, y algunos otros servicios mínimos; todas ellas escritas en el lenguaje de programación Java.

- **Framework de aplicaciones:** está diseñado para simplificar la reutilización de componentes; cualquier aplicación puede publicar sus capacidades y cualquier otra aplicación puede luego hacer uso de esas capacidades, este mismo mecanismo permite que los componentes sean reemplazados por el usuario.

- **Librerías:** incluyen en su base de datos un set de librerías C/C++, que son expuestas a todos los desarrolladores a través del framework de las aplicaciones.

- **Runtime de Android** incorpora un set de librerías que aportan la mayor parte de las funcionalidades disponibles en las librerías base del lenguaje de programación Java.

- **Núcleo Linux**: depende de Linux para los servicios base del sistema como seguridad, gestión de memoria, gestión de procesos, stack de red, y modelo de controladores.

1.5.2 Seguridad

La seguridad es uno de los aspectos más cuidados de Android. Está dividido en niveles Primero está el bajo nivel, manejado por las facilidades estándar de Linux teniendo en cuenta permisos de acceso para archivos, usuarios, servicios, etc. El nivel alto, está manejado en Java, que se encarga de la integridad del código, del sistema de acceso, y de aislar una aplicación de otra. Además en niveles intermedios Android hace uso de la Memoria Protegida, gestión de procesos, así como un sistema de permisos explícitos de cara a los servicios a los que un programa desea acceder en un momento dado.

2. VULNERABILIDADES EN SISTEMAS OPERATIVOS MÓVILES

En la actualidad la Seguridad de la información se enfrenta a diversos retos, tales como, Gusanos de internet, ataques de negación de servicios, virus, diversos tipos de intrusiones y nuevos y más sofisticados ataques que se generan cada día. Además, el drástico aumento de las vulnerabilidades descubiertas, junto con la velocidad a la que se crean nuevas amenazas hace de este reto aún mayor. La medición y gestión de riesgos de la red es un desafío importante para los usuarios y las empresas de todos los tamaños.

2.1. VULNERABILIDADES EN SYMBIAN OS

Los dispositivos Symbian son los más atacados en el mercado. En los últimos años, han sido el blanco de algunos ataques de malware, uno de cada 63 teléfonos inteligentes que funcionan con el Sistema operativo Symbian está infectado con algún tipo de malware. Sin embargo, el ambiente de vulnerabilidades para Symbian es mucho menor de lo que es para el iPhone y los dispositivos de Windows Mobile.

2.1.1 Acceso AllFiles

En el sistema operativo Symbian, existe una API AllFiles que brinda al usuario acceso completo a todos los archivos en el dispositivo, convirtiéndose en una funcionalidad muy peligrosa. El acceso a esta cantidad de datos es inseguro porque puede conceder acceso a la información personal y sensible como nombres de usuario y contraseñas.

La capacidad AllFiles da acceso de lectura al sistema de ficheros. También da acceso a escritura pública a la mayor parte del sistema de archivos (excepto */sys* y partes del */resource*, que requieren TCB). En particular, un programa con capacidad de AllFiles puede leer y escribir en cualquier programa en el directorio */private*.

2.1.2 Instaladores Warezed

La mayor fuente de vulnerabilidades de Symbian OS se encuentra en copias ilegales de programas válidos. Aunque la mayoría de los usuarios que descargan juegos y aplicaciones online ilegítimamente son consientes que están corriendo el riesgo de infectarse a sí mismos. Pero con el beneficio que representa aparentemente vale la pena tomar el riesgo de la instalación de forma inesperada de algo peligroso. Irónicamente, algunos proveedores de software empeoran el

problema mediante la liberación de versiones de su software con capacidades de carga intencional.

Es así como fue encontrado en el 2004 un juego “Mosquitos” con la funcionalidad de enviar mensajes de texto SMS costosos a líneas de tarificación adicional, donde los medios supusieron que era un virus o un troyano por que presentaba todos los síntomas de acuerdo a su funcionalidad. El programa no tenía ninguna protección de derechos de autor y realizaba una actividad maliciosa sin que el usuario lo supiera. Más tarde, se pudo comprobar que la funcionalidad del envió de SMS fue puesto en el juego desde el principio por el fabricante original. La función original se incluyo cuando el juego se puso en marcha a finales del año 2004 con la intención de evitar que los usuarios compraran versiones más baratas en los distintos países, lo cual se convirtió más bien en una función de protección de copia fallida del juego original. Independientemente de la intención o la motivación o la verdad del asunto, la versión terminó en un sitio de warez y comenzó a extenderse, lo que causó que una gran cantidad de dispositivos enviaran mensajes premium. El punto está: Si la solicitud no procede de una fuente válida, no se puede confiar en ella.

2.1.3 Ingeniería Social

Como si el factor warez no fuese suficiente, se descubrió rápidamente que los dispositivos Bluetooth en el Symbian OS eran "vulnerables" a todo tipo de abusos. La mayoría de ellos sólo dio lugar a molestos mensajes en el teléfono donde algunos de los ataques vía Bluetooth eran capaces de robar la información de las agendas y mucho más. Sin embargo, el factor humano es el que ha ayudado a convertir a los dispositivos habilitados para utilizar la tecnología Bluetooth en una amenaza. En concreto, en muchos de los dispositivos Symbian se habilita el Bluetooth y este queda en modo de detección, lo cual es algo trivial para que otro dispositivo Bluetooth pueda detectarlo. Una vez que los creadores de virus se dieron cuenta de esto, fueron capaces de aprovechar un poco la ingeniería social contra el propietario del teléfono para engañarlo de que acepte una transferencia de archivos vía Bluetooth, y luego ejecutar ese archivo.

2.2 VULNERABILIDADES EN RIM (BLACKBERRY)

Los dispositivos BlackBerry son relativamente seguros. Se construyen desde la base para mantener un entorno restrictivo. Sin embargo, existen algunas lagunas que pueden dar a un atacante la razón para llegar a vulnerar un BlackBerry.

Al igual que otros entornos móviles, la BlackBerry ejecuta código sin firmar si el usuario lo instala. Sin embargo, el acceso a ciertas funciones, tales como el acceso a la red, no se permitirá solo hasta que el usuario acepta el riesgo mediante la confirmación de un sistema. Esto podría resultar en actividad no autorizada en las cuentas de SMS premium.

En segundo lugar, es posible conseguir un pedazo de código malicioso firmado por $100 con tarjetas anónimas de crédito pre-pagado. Una vez que la solicitud de instalación está firmada, tendrá acceso a los datos, lo que puede dar al malware la posibilidad de acceder a la funcionalidad de correo electrónico del dispositivo, incluyendo la lectura y el envío de mensajes de correo electrónico.

2.2.1 Vulnerabilidades en el PDF Distiller del Servicio de archivos adjuntos de BlackBerry para el BlackBerry Enterprise Server

Múltiples vulnerabilidades de seguridad existen en el PDF Distiller de algunas versiones publicadas del componente BlackBerry Attachment Service de BlackBerry Enterprise Server. Estas vulnerabilidades podrían permitir que un individuo envié un mensaje de correo electrónico con un archivo PDF especialmente diseñado, que cuando se abra el archivo en un smartphone BlackBerry asociado con la cuenta de usuario en un servidor BlackBerry Enterprise, podría causar daños en la memoria y posiblemente conducir a una Denegación de Servicio (DoS) o la ejecución de código arbitrario en el equipo que se aloja el componente BlackBerry Attachment Service del BlackBerry Enterprise Server .

2.2.2 Vulnerabilidad en BlackBerry Desktop Manager permite la ejecución de códigos de forma remota

En esta vulnerabilidad el atacante engaña al usuario llevándolo a hacer clic en un enlace de un sitio web que parece proceder de una fuente de confianza, y el usuario elige acceder a ese sitio desde el equipo que está ejecutando el BlackBerry Desktop Manager, el usuario puede ser engañado en la navegación a una página web que el atacante malintencionado ha diseñado para llevar a cabo la ejecución de código remoto usando los privilegios del usuario en el equipo. El

BlackBerry Desktop Manager no necesita estar en ejecución para que un atacante pueda aprovechar esta vulnerabilidad .

2.2.3 Vulnerabilidad XSS (cross site scripting) en el MDS Connection Service del BlackBerry Enterprise Server

Vulnerabilidad en MDS Connection Service en el BlackBerry Enterprise Server versión 4.1.6 y anteriores MR4. BlackBerry Enterprise Server es vulnerable a secuencias de comandos entre sitios, causada por la validación incorrecta de la entrada del usuario, suministrado por el /admin/statistics/ConfigureStatistics secuencia de comandos dentro de la conexión del servicio MDS. Un atacante remoto podría explotar esta vulnerabilidad utilizando varios parámetros en una dirección URL especialmente diseñados para ejecutar un script en el navegador web de una víctima en el contexto de seguridad del sitio de alojamiento Web, una vez que se hace clic en la URL. Un atacante podría utilizar esta vulnerabilidad para robar las credenciales de autenticación de la víctima basada en cookies .

2.2.4 Vulnerabilidad en el control ActiveX de BlackBerry Application Web Loader

Existe un desbordamiento de búfer explotable en el control ActiveX de BlackBerry Application Web Loader que utiliza Internet Explorer para instalar aplicaciones en dispositivos BlackBerry.
Cuando se navega en el dispositivo BlackBerry en un sitio web que está diseñado para instalar el control ActiveX de BlackBerry Application Web Loader en los dispositivos BlackBerry mediante una conexión USB, y se hace clic en Sí para instalar y ejecutar el control ActiveX, el control ActiveX introduce la vulnerabilidad a la computadora .

2.2.5 Programa TXSBBSpy

No es necesario aprovecharse de las vulnerabilidades para burlar los protocolos de seguridad de la Blackberry, simplemente utilizando un programa llamado TXSBBSPY, creado por el señor Tyler Shields, investigador de seguridad senior de VeraCode, que es simplemente una aplicación legítima escrita para la BlackBerry el cual tiene la capacidad de acceder y volcar a los contactos del dispositivo, los mensajes de correo electrónico, los registros del teléfono, la ubicación actual y las grabaciones realizadas por el micrófono de la BlackBerry.

≈ BlackBerry Security. Boletines e información. http://es.blackberry.com/ataglance/security/news.jsp.

También monitorea continuamente los mensajes SMS entrantes y salientes, las llamadas realizadas y registra las coordenadas GPS del dispositivo en tiempo real. La aplicación es compatible con varios protocolos de comunicación, incluyendo HTTP, UDP, SMS y correo electrónico, y puede ser controlado remotamente a través de comandos simples.

2.3 VULNERABILIDADES EN WINDOWS MOBILE

Los dispositivos Windows Mobile son una combinación de hardware y software. Como resultado de ello, no nos debería sorprender que haya errores de software que puedan ser explotados a través de código malicioso. Las principales causas que justifican el aumento del riesgo en los dispositivos de Windows Mobile pueden ser:

- Con la idea de código fuente compartida de Windows Mobile, los atacantes pueden conocer en profundidad el sistema operativo de forma sencilla.
- Los usuarios de los teléfonos móviles tienden a guardar una gran cantidad de datos privados en sus dispositivos. Esto puede en algún momento resultar atractivo para los atacantes, ya que pueden obtener importantes ganancias económicas a través del robo de identidad o la apropiación de información de tarjetas de crédito.
- Debido a que Windows Mobile se basa en Win32, y éste es muy similar al utilizado por Windows en un computador normal, un atacante que siempre ha realizado sus ataques contra PCs, le puede resultar más fácil hacer el mismo ataque a un dispositivo móvil.

Desde esta perspectiva vamos a discutir el panorama de las vulnerabilidades en las que se aplica a este sistema operativo y el programa del tercero que se ejecuta en ella.

2.3.1 KDataStruct

Si bien esta vulnerabilidad sólo existe en Windows Mobile 2003SE y en los dispositivos anteriores, dejó una gran impresión en la comunidad de seguridad de Windows Mobile.

Windows Mobile somete todas sus funciones al sistema principal en el archivo coredll.dll, que es muy parecido al archivo kernel32.dll de Windows XP. De esta manera, los desarrolladores no tienen que incluir en el código las funciones

básicas en sus propios programas, sino que llaman a la función desde su aplicación. Cuando la aplicación es compilada en el dispositivo destino, importa las direcciones de las API coredll y utiliza el espacio de memoria que es asignado. El Shellcode se ejecuta dentro del hilo del programa vulnerable, lo que puede o no tener un enlace a la dirección de la API en coredll.

En WM, la dirección podría estar en cualquier lugar, ya que cada dispositivo tiene su propio archivo coredll.dll con direcciones diferentes. En resumen, KDataStruct proporciona una dirección a la lista de todos los módulos, de los que puede determinar si en el módulo se encuentra coredll.dll. Una vez que se obtiene, puede buscar a través de la memoria por un nombre específico y obtener la dirección virtual que coincide con el API al que desea llamar. Esto resume cómo la vulnerabilidad puede ser explotada.

2.3.2 Pocket IE

Pocket Internet Explorer (PIE) es el navegador web por defecto incluido en Windows Mobile, es vulnerable a varios ataques. A continuación se presenta un breve resumen de las vulnerabilidades encontradas hasta la fecha:

- Denegación de Servicio DoS. Uno que impacto al PIE de WM4.2 fue a través de las etiquetas <DIV> anidadas, y otro fue originado por el uso excesivo de caracteres Wireless Markup Language (WML). En una nota relacionada, varias compañías de seguridad han encontrado problemas de denegación de varios otros componentes básicos de WM, incluyendo fotografías y vídeos, paquetes IGMP, y controladores de SMS.

- Vulnerabilidad entre dominios en WM 4.2 y anteriores. Fallo en PIE para restringir los objetos JavaScript que se ejecuta en un dominio de acceso al contenido de otro dominio (DOM). Esto podría permitir a alguien leer/escribir desde una página que debería estar fuera del control del navegador, incluyendo los archivos locales. Cuando se combina con técnicas de ofuscación de URL, es posible engañar a alguien para hacerle creer que estaban en una página real y robar sus credenciales.

- Pocket IE Local File Disclosure. En WM6 y posteriores, es posible detectar si existe un archivo en el dispositivo. Esto puede ser aprovechado para realizar una estafa a través de ingeniería social para convencer a un usuario en la Web de descargar e instalar archivos.

2.3.3 Active Sync

A fin de mantener un dispositivo WM sincronizado a un PC, el software Active Sync debe estar instalado. Se ha descubierto que este programa tiene algunos errores en lo que puede ser explotado para extraer información de un usuario.

En concreto, ActiveSync 3.8.1 y anteriores no cifra las sesiones establecidas, lo que hace posible capturar la contraseña en texto plano y también permite la suplantación de la inicialización del proceso de sincronización.

En las versiones más recientes, el protocolo ActiveSync es fácilmente descifrable a su paso por la conexión USB con el dispositivo. Esto sólo requiere la contraseña XOR con un valor que también se incluye en la sesión de datos.

2.3.4 PocketPC MMS

El servicio de mensajería multimedia (MMS) es de uso común para la difusión de malware para móviles, smartphone y muchos gusanos lo utilizan para el envío de copias de sí mismos a sus futuros anfitriones. Además, todos los conocidos gusanos MMS sólo utilizan este servicio como un medio de transporte, no como un vector de infección. El vector de infección todavía es la ingeniería social.

2.3.5 Denegación de Servicio a través de WAP Push y Wi-Fi

Los teléfonos con Windows Mobile aceptan mensajes WAP Push en todas las interfaces de red por el puerto UDP 2948. Este hecho, junto con las vulnerabilidades descubiertas en el cliente MMS, crea una interesante denegación de servicio contra estos teléfonos, sobre todo desde MMS Composer que no solamente se encarga de MMS y SMS, sino también del e-mail. El ataque obvio es inundar simplemente un teléfono con notificaciones de mensajes nuevos. Este ataque no sólo se traducirá en una bandeja de entrada ya que el teléfono también tratará de recibir cada mensaje, y por lo tanto crear una conexión GPRS.

Después de un par de cientos de notificaciones de mensajes, el teléfono será notablemente lento debido a la amplia utilización de la memoria. La eliminación de estos mensajes falsos también llevará algún tiempo y paciencia, ya que algunas versiones de MMS Composer no admiten borrar varios mensajes a la vez. Así el usuario tiene que borrar un mensaje a la vez.

2.3.6 Funciones de mayor riesgo

Mensajes de texto

Windows Mobile permite el envío y bloqueo de mensajes a través de las funciones de la interfaz API. Existen malware que utilizan ésta interfaz para enviar mensajes falsos a cualquier persona que se encuentra en la lista de contactos del usuario del dispositivo. Cuando el mensaje llega a su destino, el usuario final observa que el mensaje viene de un número telefónico conocido, por lo cual, lo acepta y recibe el mensaje, sin saber que de manera trasparente aceptó el ingreso del malware a su dispositivo.

El malware también puede utilizar la interfaz API para enviar mensajes de texto especiales a un proveedor de servicios con cargo a la tarjeta prepago del dispositivo móvil del usuario. El usuario sin saberlo le aparece su cuenta con menor dinero debido al ataque que ha recibido.

Contactos

La lista de contactos se puede decir que es el activo de información de una persona que tiene un dispositivo móvil. Si ésta persona trabaja en una organización y le roban los datos de los contactos, puede tener consecuencias nefastas tanto para los empleados como para la propia empresa. Un malware para móviles puede robar los datos y enviarlos en un mensaje de texto a personas desconocidas o a un grupo delincuencial con fines de delictivos.

Fotos y Vídeo

La gran mayoría de usuarios guardan en sus dispositivos móviles las fotos o vídeos personales, esto puede llegar a ser un blanco perfecto de un malware. Éste código malicioso podría buscar todos los archivos jpg, mpeg utilizando la API de archivos y enviárselos a una persona malintencionada a través de la red inalámbrica.

Documentación

Gran cantidad de usuarios guardan sus documentos personales en su móvil, ya que les permite tenerlos disponibles en cualquier momento que los requieran. Los archivos pueden ser de Word, Excel, o pdf, el riesgo está, en que estos archivos pueden ser utilizados por algún malware, afectando así al usuario del dispositivo.

2.4 VULNERABILIDADES IPHONE OS X

Apple dentro de sus ideas de propiedad intento la posibilidad de mantener alejados a los atacantes y a los hacker de su dispositivo. Sin embargo, cometió varios errores grandes que han dado lugar a que el dispositivo no sólo este totalmente introducido en la comunidad hacker, que quiere el dispositivo abierto y libre, sino también por la comunidad de seguridad que inmediatamente sondeó el iPhone con la esperanza de encontrar vulnerabilidades en el sistema operativo y sus aplicaciones. A continuación se tendrán en cuenta el proceso detrás de cómo el iPhone fue desbloqueado, así como examinar algunas vulnerabilidades que puede conducir al acceso no autorizado al iPhone.

2.4.1 iPhone Hacking

Como se mencionó anteriormente, el iPhone se vende como un dispositivo de propiedad de Apple, lo que significa que sólo se puede instalar el software de la tienda de Apple y que éste debe estar en la red de su elección. Sin embargo, eso no significa que vaya a permanecer así por mucho tiempo.

Proceso Jailbreaking iPhone

1. Recomendaciones a tener en cuenta
   Debes tener instalada la versión del Firmware 3.1.2.
   Realizar una copia de seguridad de las configuraciones, contactos y aplicaciones.

2. Descargar el blackra1n
   Blackra1n es un software que elimina cualquier interacción que tenga que hacer el usuario con el dispositivo y se encarga totalmente de todo el proceso automáticamente.

3. Desbloquear iPhone (2g, 3G, 3GS)

- Cerrar iTunes y conectar el dispositivo, después ejecutar blackra1n. Clic en el botón “make it ra1n”

 Comunidad Dragonjar. Desbloquea (Jailbreak) o Actualiza el iPhone OS 3.1.2 para iPhone y iPod Touch.
http://www.dragonjar.org/desbloquea-jailbreak-firmware-3-1-2-iphone-y-ipod-touch.xhtml

Figura 13. Ejecución blackra1n
Imagen tomada de: http://www.dragonjar.org

- Aceptar y esperar que blackra1n realice todo el procedimiento.

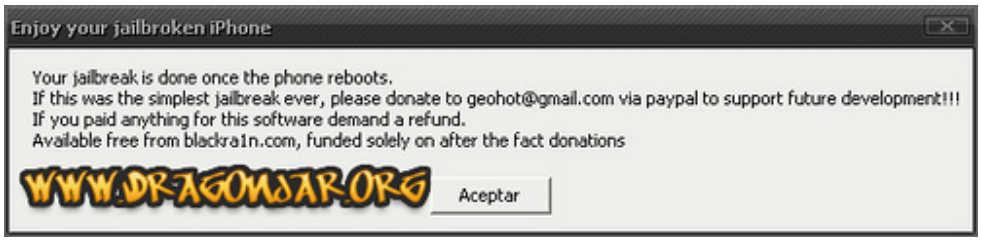

Figura 14. Proceso Jailbreak
Imagen tomada de: http://www.dragonjar.org

- Instalar algún administrador de paquetes desde la aplicación blackra1n que quedo instalada en tu iPhone.

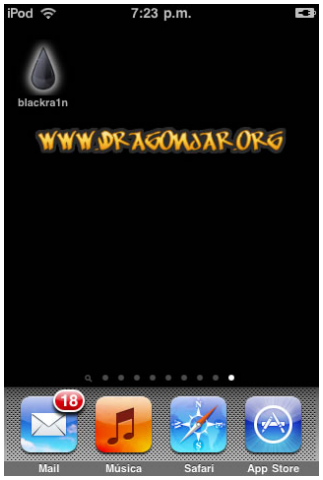

Figura 15. Aplicación blackra1n instalada
Imagen tomada de: http://www.dragonjar.org

- Abrir blackra1n el cual te permite escoger entre 3 administradores de paquetes para tu dispositivo:

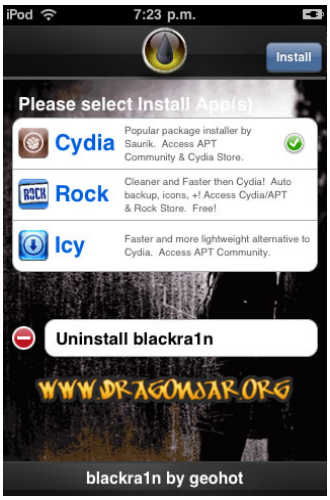

Figura 16. Administrador de Paquetes
Imagen tomada de: http://www.dragonjar.org

- Cydia es el más popular de los 3 y casi todos los tutoriales utilizan este administrador de paquetes, aunque los otros 2 son mucho más rápidos y livianos. Se recomienda hacer pruebas y de acuerdo a ellas escojas el que más se adapte a tus necesidades

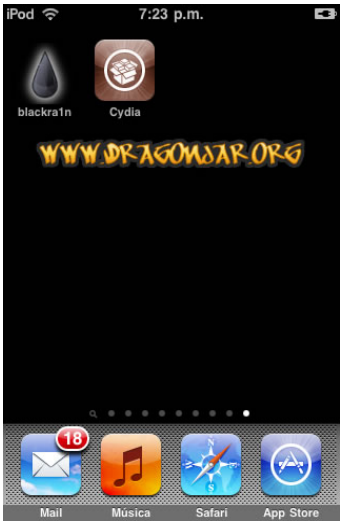

Figura 17. Administrador Cydia Instalada
Imagen tomada de: http://www.dragonjar.org

Una vez realizado el proceso de jailbreak el smartphone en manos de un atacante experto puede ser utilizado para penetrar en las redes de una organización. Ya no tienen que caminar por ahí con un ordenador portátil voluminoso para realizar el trabajo. Al tomar un IPHONE y haciendo una serie de ajustes de software y la instalación de algunas de las herramientas adecuadas puede encontrar vulnerabilidades en su red.

2.4.2 Vulnerabilidades

CoreAudio

Se produce un desbordamiento del búfer en el manejo de archivos de audio mp4. La reproducción de un archivo de audio mp4 creado con fines malintencionados puede provocar la finalización inesperada de la aplicación o la ejecución de código arbitrario.

ImageIO

Existe un desbordamiento del búfer de pila en el manejo de imágenes TIFF por parte de ImageIO. La visualización de una imagen TIFF creada con fines malintencionados puede provocar la finalización inesperada de una aplicación o la ejecución de código arbitrario.

Modo de recuperación Existe un problema de corrupción de memoria causado por la gestión de un determinado mensaje de control de USB. Una persona con acceso físico al dispositivo podría aprovecharse de esta situación para eludir la contraseña y acceder a la información del usuario.

WebKit

Existen varios problemas de validación de entrada en el manejo de listados de directorios FTP por parte de WebKit. El acceso a un servidor FTP creado con fines malintencionados podría conducir a la finalización inesperada de una aplicación, a la divulgación de información o a la ejecución de código arbitrario.

 Soporte Técnico de Apple. Acerca del contenido de seguridad de iPhone OS 3.1.3 y iPhone OS 3.1.3 para iPod touch. http://support.apple.com/kb/HT4013?viewlocale=es_ES&locale=es_ES.

WebKit

Cuando WebKit se encuentra con un Media Element HTML 5 que apunta a un recurso externo, no emite una devolución de llamada de carga de recursos para determinar si dicho recurso debería cargarse. Esto podría conducir a peticiones no deseadas a servidores remotos. Por ejemplo, el remitente de un mensaje de correo electrónico con formato HTML podría aprovecharse de esto para averiguar si el mensaje se leyó.

2.5 VULNERABILIDADES EN ANDROID

Los ataques de denegación de servicio se convierten en la mayor amenaza para este sistema operativo.

Con el transcurrir del tiempo y a medida que avanza aceleradamente el uso de este sistema operativo se han descubierto numerosas vulnerabilidades que aunque como en los demás sistemas operativos se corrigen a tiempo no dejan de ser un problema para aquellos que la seguridad no es una prioridad.

2.5.1 Vulnerabilidad en el sistema de mensajes (SMS)

Según una nota publicada por oCERT; este fallo permite a los atacantes utilizar mensajes WAP Push manipulados para desconectar un teléfono móvil de una red. Este tipo de mensajes suele utilizarse para enviar tonos a los usuarios de teléfonos móviles. Un mensaje WAP malicioso puede causar que el teléfono se reinicie sin conocimiento del usuario, lo que podría llevarle a una pérdida temporal de conectividad y a la caída de llamadas. En los casos en los que la tarjeta SIM del teléfono esté protegida por un PIN, los usuarios necesitarán volver a introducir el código para restablecer la conectividad, lo que causaría mayores retrasos. Cuando el fallo ocurre repetidamente, podría acabar resultando en una denegación de servicio.

2.5.2 Vulnerabilidad Maquina Virtual Dalvik

La interfaz de programación para Android, (máquina virtual Dalvik), permite a los atacantes crear una condición de denegación de servicio que provoca que los dispositivos se reinicien repetidamente sin que el usuario perciba el fallo.

 Soporte Técnico de Apple. Acerca del contenido de seguridad de iPhone OS 3.1.3 y iPhone OS 3.1.3 para iPod touch. http://support.apple.com/kb/HT4013?viewlocale=es_ES&locale=es_ES.

Figura 18. Ataque de denegación de servicio; reinicio, desconexión, y bloqueo de dispositivo

Imagen tomada de: http://www.blackhat.com/presentations/bh-usa-09/MILLER/BHUSA09-Miller-FuzzingPhone-PAPER.pdf

2.5.3 Vulnerabilidad en Manifest.permission.CAMERA y Manifest.permission.AUDIO_RECORD.

Errores de validación a la hora de manejar los permisos encargados de verificar el acceso a la cámara y al audio (Manifest.permission.CAMERA y Manifest.permission.AUDIO_RECORD respectivamente). Esto podría ser aprovechado por un atacante para obtener grabaciones de audio y video sin el consentimiento del usuario. Cualquier aplicación en este sistema operativo necesita la confirmación explícita del usuario para acceder a los recursos de audio y vídeo. Pero si se crea (y el usuario instala) una aplicación que no pida el uso de esos permisos, por error, los tendrá implícitamente (podrá usar el micrófono y la cámara) sin necesidad de que el usuario lo sepa. Esta vulnerabilidad evade este control y permite que no se pida autorización al usuario para acceder a la cámara y el audio.

2.5.4 Vulnerabilidad en el navegador Web

Permite que un atacante acceda y controle el navegador del teléfono y otros procesos desde una locación remota. Una vez que el teléfono de un individuo está infectado, los atacantes son capaces de acceder a datos guardados en el navegador y su historial.

La vulnerabilidad está dentro del código escrito por PacketVideo, la compañía de software que contribuyó con una versión Open Source de su aplicación multimedia para Android, convirtiéndola en el subsistema de reproducción de archivos multimedia del navegador de Android.

2.5.5 Aplicaciones Fraudulentas en Android Market

Algunas aplicaciones fraudulentas han aparecido en Android Market, la tienda de aplicaciones para el sistema operativo para móviles de Google. Cerca del 20% de las 48.000 aplicaciones en la tienda de Android permiten que aplicaciones de terceros accedan a información sensible o privada. El 5% de las aplicaciones pueden hacer llamadas a cualquier número y el 2% permiten que una aplicación envíe mensajes SMS desconocidos a números premium que provocan cargos costosos.

Estas aplicaciones tienen el mismo tipo de acceso a la información sensible, correos electrónicos y mensajes de texto, información de llamadas, y ubicación del dispositivo. Esto ya ocurrió con el caso de una aplicación que fue publicada por un autor con el nombre de Droid09, la cual permitía al usuario llevar a cabo actividades bancarias desde el teléfono, con finalidad de robar la identidad digital del usuario, los datos de acceso a la cuenta bancaria. Los atacantes utilizaron una técnica conocida como phishing; la aplicación maliciosa se camuflaba como una aplicación de banca online para móviles con Android.

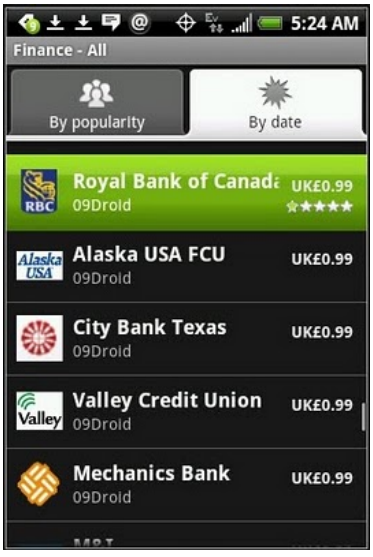

Figura 19. Ataque Acceso a aplicación creada por atacante
Imagen tomada de: http://spamloco.net/2010/01/phishing-bancario-android-marketplace.html

2.5.6 Vulnerabilidad Bloqueo de Pantalla

El mecanismo de seguridad empleado requiere que los usuarios de entrada de un patrón utilizando puntos que aparecen en pantalla antes de que puedan acceder a la mayoría de las funciones del teléfono. Explotar el error es bastante simple, mientras se recibe una llamada entrante en un smart phone que tiene su pantalla de bloqueo activado, puede simplemente pulsar el botón 'Atrás' para evitar el bloqueo y saltar a la pantalla de inicio. Esto, por supuesto, da acceso a la cuenta del dueño del correo electrónico, páginas web, cookies, directorio telefónico, y todo lo almacenado en el teléfono.

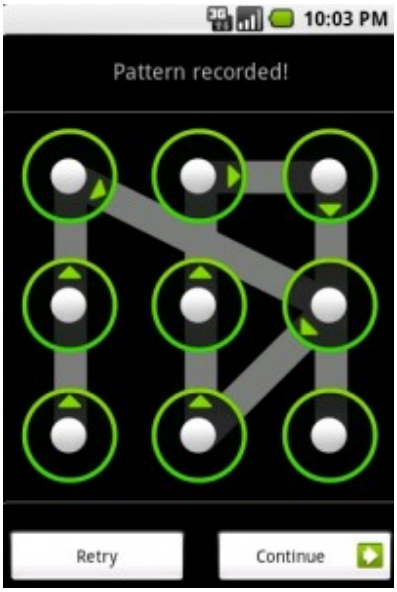

Figura 20. Pantalla de Bloque Activada
Imagen tomada de: http://techcrunch.com/2010/01/11/verizon-droid-security-bug/

3 ATAQUES EN LAS TECNOLOGÍAS EMPLEADAS EN LOS DISPOSITIVOS MÓVILES

3.1 REDES INALÁMBRICAS WI-FI

3.1.1. Avances en la seguridad inalámbrica

Al hacerse evidentes las vulnerabilidades de las soluciones inalámbricas se comenzaron a popularizar los mecanismos de ataque tornándose cada vez mas fácil el acceso a recursos y aplicativos la mayoría de libre distribución. Este hecho llevo al desarrollo fuerte de soluciones enfocadas a mejorar la seguridad en las redes inalámbricas fue así como se llegó al desarrollo de mecanismos de cifrado; inicialmente el WEP, mejorado posteriormente por el WAP y WAP2.

3.1.2. WEP (Wired Equivalent Privacy)

Este fue el primer método de cifrado usado para la norma 802.11. Este tipo de cifrado requiere de una clave estática de 40 bits introducido por los usuarios de cada extremo con esta clave sumada con un vector de inicialización estático de 24 bits se obtiene una nueva clave de 64 bits a través de un algoritmo llamado RC4. Si este tipo de cifrado se le hace una operación lógica XOR esto obtendría una nueva información cifrada como lo muestra la figura XX.

3.1.3. Vulnerabilidades WEP (Wired Equivalent Privacy)

La falla comúnmente aprovechada de este primer método de cifrado es su vector de inicialización el cual está compuesto por 24 bits, ya que éste se transmite en texto claro y cada vez que se está transmitiendo se genera el mismo vector de inicialización, por lo que al escuchar una red se podría obtener este vector, al tener este vector, el atacante sabe que seguido de él, se encuentra la clave hexadecimal escogida por el usuario, así que solo es cuestión de recoger suficiente información y comenzar a probar las tramas para encontrar dicha clave y romper este método.

Figura 21. Proceso de Encriptación
Imagen tomada de: Revista NEX IT Specialist #13, Diciembre 2004, vol 1, pag 58, ISSN 1668-5423

3.1.4. WPA (Wi-fi protected Access)

Después del fracaso del primer método de cifrado en redes inalámbricas se creó otro método mejorado que parece mitigar enormemente la efectividad de los ataques, basándose en cierta medida en el WEP el cual incluiría métodos de autenticación y utilización de un vector de inicialización más largo.

Aunque el algoritmo de cifrado no cambio, continuando con RC4, pero con la gran diferencia que WPA usa un protocolo de Integridad de Clave no estática TKIP (Temporal Key Integrity Protocol), este protocolo cambia la clave de 128 bits usada en la transmisión de los datos cada 10.000 paquetes. Así mismo se tiene una segunda opción por medio del AES (Advanced Encryption Standard) basado en el algoritmo Rijndael, inventado por Joan Daemen y Vincent Rijmen. AES emplea tres longitudes de clave: 128-bits, 192 bits y 256 bits.

La seguridad de este nuevo método, recae totalmente en la complejidad de la contraseña utilizada por el usuario, entre más compleja sea, más difícil para un atacante descubrirla.

3.1.5. Métodos de Autenticación más comunes

- **PSK (Pre-share Key)**

  La clave previamente compartida es una serie hexadecimal o una frase que debe coincidir con el punto de acceso y todos los clientes.
  La seguridad 802.1x no está disponible cuando se utiliza WPA - Personal o WPA2 Personal métodos.

- **EAP-TLS (Extensible Authentication Protocol - Transport Layer Security)**

  EAP-TLS fue la primera técnica de autenticación EAP necesarios para la compatibilidad WPA/WPA2. EAP-TLS, actualmente se puede calificar como bastante seguro. Utiliza certificados para autenticar a todos los usuarios en una red esto es también su mayor caída. La gestión de los certificados para todos los usuarios en una organización de cualquier tamaño puede ser un desafío enorme, lo cual lo hace bastante impráctico para aplicar a la realidad.
  Conceptualmente EAP-TLS no es tan complicado, funciona de la siguiente manera: El servidor manda al cliente su certificado, el cual es usado para el cifrado de mensajes, luego el cliente envía al servidor de autenticación su certificado, el cual el servidor tiene que verificar. Al hacer esta revisión el servidor y el cliente proceden a generar una llave aleatoria. Esta llave es usada para inicializar un cifrado simétrico para cifrar los datos la sesión TLS.

3.1.6. Estándares para Wireless

Wireless LAN están referidas a un número de estándar en el IEEE. Todas las especificaciones Wireless LAN están incluidas dentro de las normas IEEE 802,11. La mayoría de éstas son en realidad ratificaciones o adiciones a la norma original y aunque existen numerosos tipos de ellas las de mayor prevalencia son 802.11a, 802.11b, 802.11g, 802.11n y sus ratificaciones. Cada una de estas normas tiene características particulares que las hacen únicas. La siguiente tabla muestra un resumen de las cuatro normas principales.

Table 1: The Common 802.11X Standards			
Protocol	**Frequency Band**	**Typical Data Rate**	**Maximum Data Rate**
Legacy	2.4 GHz	1 Mbit/s	2 Mbit/s
802.11a	5 GHz	25 Mbit/s	54 Mbit/s
802.11b	2.4 GHz	6.5 Mbit/s	11 Mbit/s
802.11g	2.4 GHz	11 Mbit/s	54 Mbit/s
802.11n	2.4 and 5 GHz	200 Mbit/s	540 Mbit/s

Tabla 1. Normas IEEE Wireless LAN
Imagen tomada de: Hacking Exposed Wireless, McGraw Hill, 2007, pag. 45, ISBN:9780072262582

3.1.7. Métodos de interceptación de redes inalámbricas (Wireless Hacking)

Hoy por hoy asegurar las redes inalámbricas se ha convertido en una tarea importante por hacer, ya que se puede dejar expuesta todo tipo de información incluyendo la más sensible para una organización o personal. Hay que tener en cuenta lo débil que pueden llegar a ser estas contraseñas antes que nada si son fáciles de descubrir por un atacante, es decir, si no son lo suficientemente complejas y si no se usa un método de cifrado y autenticación fuerte, siempre estaremos dispuestos a tener ataques ya sea por venganza, diversión o robo de información para fines comerciales, entre otros, ya que existen métodos al alcance de todos con gran facilidad de uso para medir el nivel de seguridad. No es ilegal llevar a la práctica estos métodos si lo que se desea es reforzar el nivel de seguridad de su red.

3.1.8. War Walking

La palabra war o guerra, hace referencia a un método, táctica o estrategia para atacar a su objetivo; se tomo de la película “War Games” se usaba un método para escanear líneas telefónicas para poder atacar, si lograba poder conectarlos, aunque el significado literal sea ataque, esta técnica se usa solo para evaluar.

La técnica war walking es un evaluó de las redes caminando, esto se logra utilizando una PDA (Personal Digital Assistant - Asistente Digital Personal) con un software de escaneo y una antena por lo general de creación casera parecidas a

las antenas con una lata de papas pringles, en búsqueda de una red inalámbrica sin protección.

Esta técnica puede ser bastante dañina, ya que muchos de estos dispositivos poseen GPS incluidos lo que puede dejar al descubierto la ubicación de las redes a otros atacantes.

Figura 22. Herramienta para War Walking
Imagen tomada de: Revista NEX IT Specialist #13, Diciembre 2004, vol 1, pag 58 ISSN 1668-5423

3.1.9. War Driving

Figura 23. War Driving
Imagen tomada de: Revista NEX IT Specialist #13, Diciembre 2004, vol 1, pag 58 ISSN 1668-5423

Esta es una técnica un poco más sofisticada ya que se hace un escaneo de las redes inalámbricas mientras se va en un automóvil, en Bucaramanga se realizo una serie de pruebas de esta técnica dando como resultados las siguientes imágenes. Estas pruebas llevadas a cabo en la ciudad de Bucaramanga, sé

sectorizo de tal manera que se expresa por los barrios de la ciudad en los cuales más actividad inalámbrica existe actualmente.

Se identificó la cantidad de redes encontradas en las zonas, con seguridad WEP, WPA u OPN (sin seguridad).

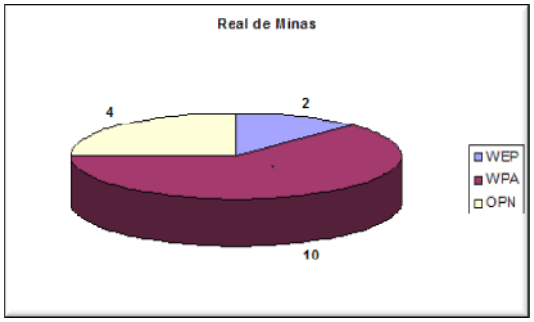

Figura 24. War Driving Real de Minas
Imagen tomada de: Autor Proyecto

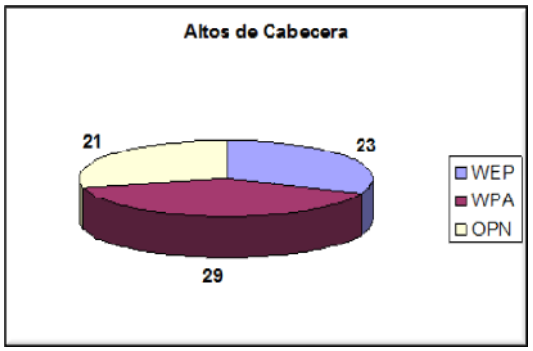

Figura 25. War Driving Altos de Cabecera
Imagen tomada de: Autor Proyecto

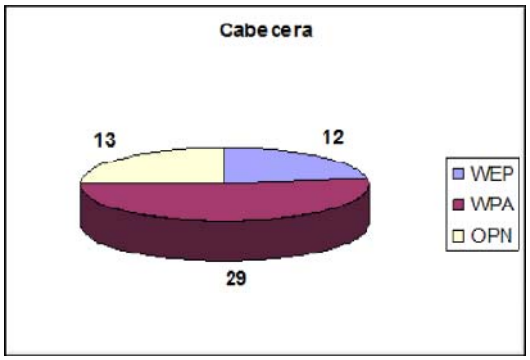

Figura 26. War Driving Cabecera
Imagen tomada de: Autor Proyecto

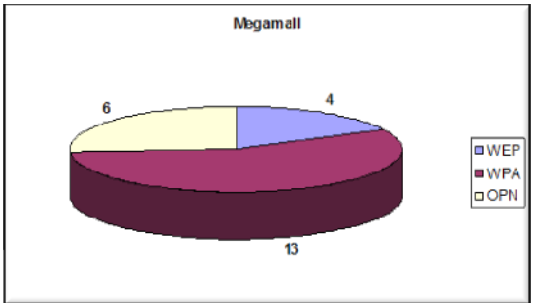

Figura 27. War Driving Centro Comercial Megamall
Imagen tomada de: Autor Proyecto

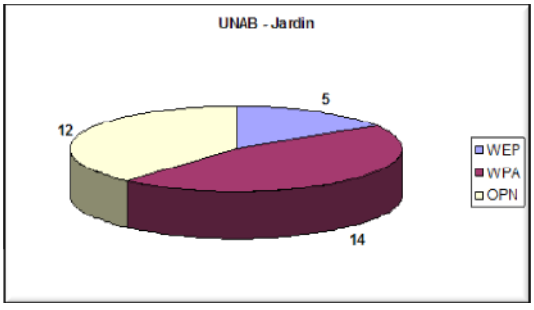

Figura 28. War Driving Barrio El Jardin – Universidad Autónoma de Bucarmanga
Imagen tomada de: Autor Proyecto

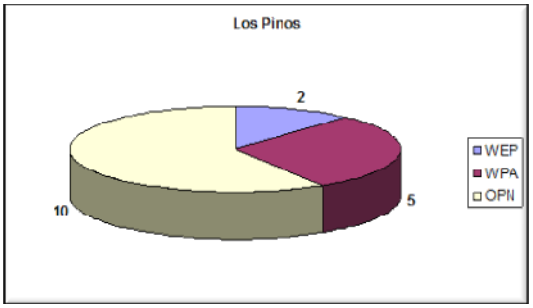

Figura 29. War Driving Barrio Los Pinos
Imagen tomada de: Autor Proyecto

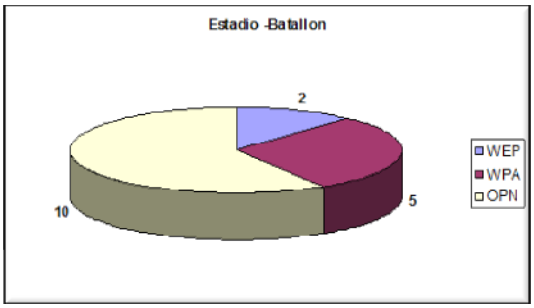

Figura 30. War Driving Estadio - Batallón
Imagen tomada de: Autor Proyecto

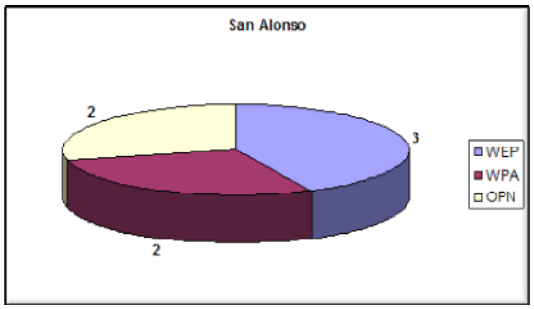

Figura 31. War Driving Barrio San Alonso
Imagen tomada de: Autor Proyecto

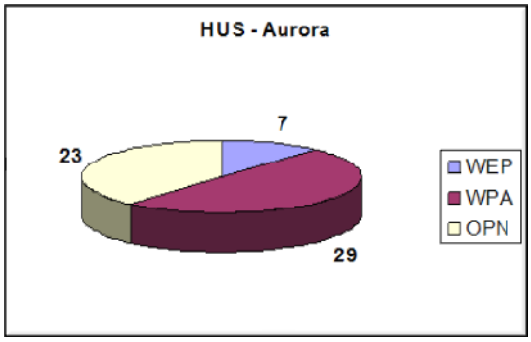

Figura 32. War Driving Barrio Aurora – Hospital Universitario de Santander
Imagen tomada de: Autor Proyecto

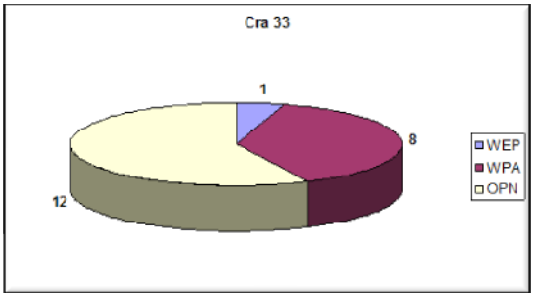

Figura 33. War Driving Zona Comercial Carrera 33
Imagen tomada de: Autor Proyecto

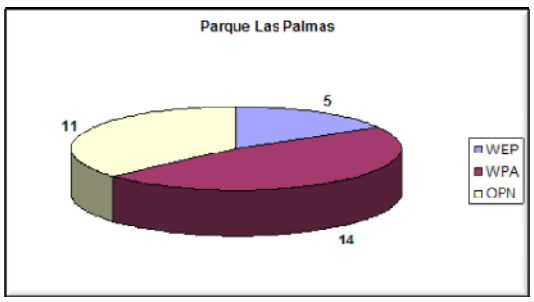

Figura 34. War Driving Parque las Palmas
Imagen tomada de: Autor Proyecto

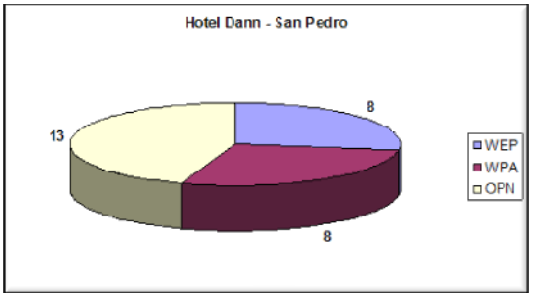

Figura 35. War Driving Barrio Sotomayor
Imagen tomada de: Autor Proyecto

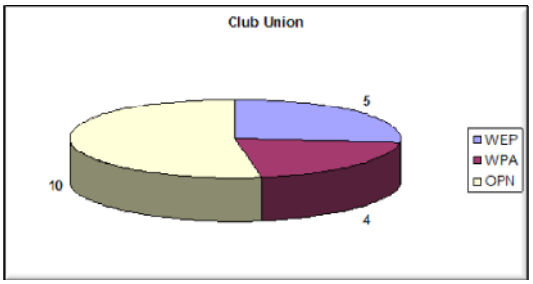

Figura 36. War Driving Alrededores Club Unión
Imagen tomada de: Autor Proyecto

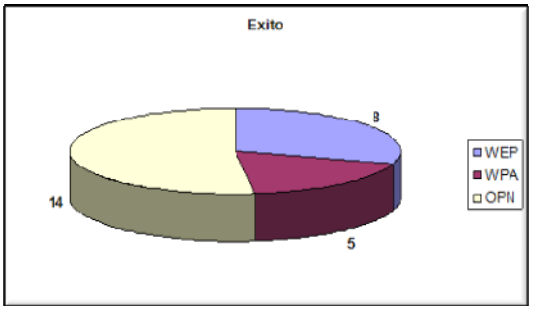

Figura 37. War Driving Éxito Cabecera
Imagen tomada de: Autor Proyecto

Después de considerar la información recopilada en el War Driving, y analizarla debidamente mostrándola en graficas para fácil comprensión, se puede resaltar que aunque se cuenta con mejores métodos de cifrado como el WPA aun existen redes inalámbricas en la ciudad de Bucaramanga que usan WEP, más alertador resulta confirmar que predominan las redes abiertas, aunque algunas de estas son

de acceso público pertenecientes a restaurantes, cafés, bares y otros la gran mayoría son de oficinas y de familias, otro aspecto a resaltar es la poca prevención al elegir nombre a las redes, como el nombre por defecto de un router, mal configurado sería mucho más sencilla su intrusión o también, nombres como Familia Pepito, señalando al atacante un “aquí estamos nosotros” lo cual no es buena idea.

3.1.10. War Chalking

Esta técnica consiste en detectar redes y avisar a otros atacantes marcando la zona de detección con una tiza (como su nombre lo indica). Este aviso se escribe con este elemento ya que es más fácil poder corregir en caso de que la red inalámbrica o sus parámetros sean modificados. Está técnica cuenta símbolos establecidos, para mayor facilidad de comprensión, además generalmente estas marcas se encuentran en zonas menos transitadas, contienen además el SSID si es una red abierta o cerrada y el ancho de banda, en las figuras 18 y 19 se explican dichas simbologías.

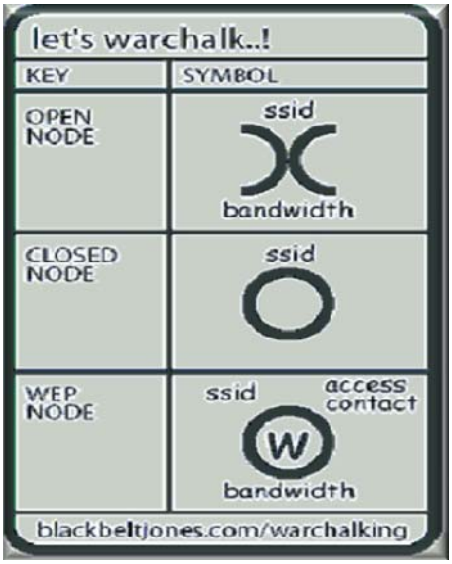

Figura 38. Símbolos Warchalk
Imagen tomada de: Revista NEX IT Specialist #13, Diciembre 2004, vol 1, pag 59, ISSN 1668-5423

Figura 39. War Chalking
Imagen tomada de: Revista NEX IT Specialist #13, Diciembre 2004, vol 1, pag 60 ISSN 1668-5423

3.1.11 Software

Hoy en día se encuentran a disposición una gran cantidad de aplicaciones que hacen monitorización de redes inalámbricas, en esta sección solo se contemplan herramientas usadas para intrusiones con licenciamiento OpenSource tanto como para Linux como para Windows.

La figura 20. Muestra una captura de tráfico, esto se logra colocando una tarjeta de red inalámbrica la cual pueda configurarse en modo promiscuo. La mayoría de las tarjetas inalámbricas vienen sin estos controladores, por lo general toca descargarlos de Internet y proceder con su respectiva instalación o compilación. Esta figura muestra los extremos de cada conexión con direcciones MAC tipo de cifrado y tipo autenticación, además de los usuarios que ya están autenticados dentro de este AP (Access Point). La figura 21 muestra el resultado después de un ataque de diccionario y fuerza bruta el cual obtuvo una llave después de un análisis de tráfico.

3.1.12 Airodump-ng

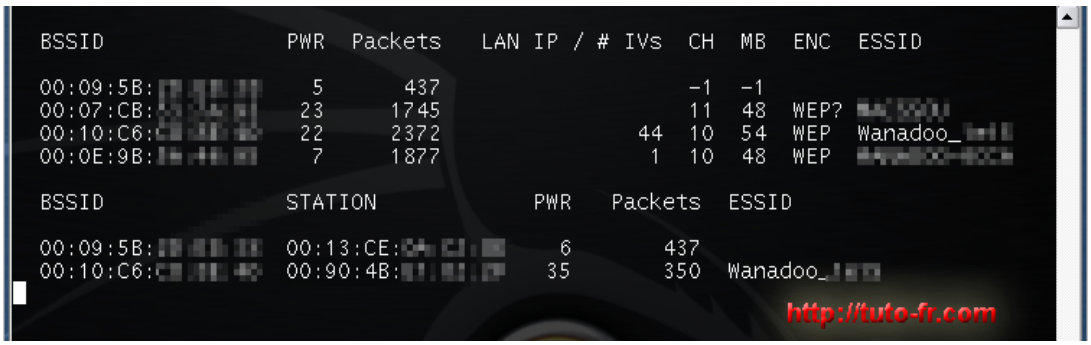

Figura 40. Captura de Tráfico con airodump-ng
Imagen tomada de: http://www.aircrack-ng.org/doku.php?id=spanish_tuto-fr.com_en_tutorial_tutorial-crack-wep-aircrack.php

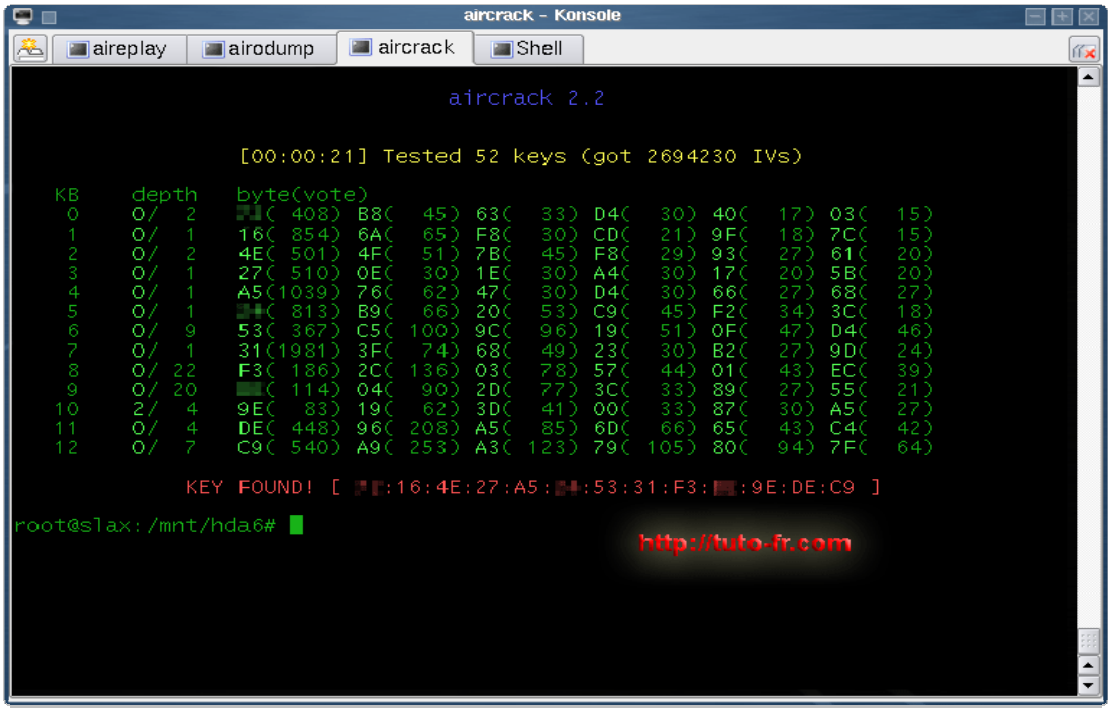

Figura 41. Ataque Diccionario y Fuerza Bruta
Imagen tomada de: http://www.aircrack-ng.org/doku.php?id=spanish_tuto-fr.com_en_tutorial_tutorial-crack-wep-aircrack.php

3.1.13 Aircrack-ng

Aircrack-ng es actualmente el programa por excelencia para hacer este tipo de ataques de crack de contraseñas 802.11 WEP y WPA/WPA2-PSK. Aircrack-ng puede recuperar la clave WEP una vez que se han capturado suficientes paquetes de la red atacada con el comando airodump-ng. Este programa de la suite aircrack-ng lleva a cabo varios tipos de ataques para descubrir la clave WEP con pequeñas cantidades de paquetes capturados, combinando ataques estadísticos con ataques de fuerza bruta. Para crack de claves WPA/WPA2-PSK, es necesario usar un diccionario, dada la mayor complejidad de este tipo de seguridad.

3.1.14 Pruebas en laboratorio

En laboratorio se llevó a cabo pruebas con el Aircrack-ng que está incluido en el live CD Linux BackTrack 3.

Para este fin se uso un computador de escritorio corriendo BackTrack 3 con una tarjeta inalámbrica externa USB la cual puede configurarse en modo promiscuo y un computador portátil quien se conecta a la red inalámbrica, para WEP, se llevaron a cabo los siguientes pasos:

1. Se configuro un Access Point con cifrado WEP y con acceso a Internet.

2. Se conecta un PC a la red inalámbrica configurada.

3. Preparar el equipo atacante:

- Instalarle una tarjeta inalámbrica.
- Iniciar este equipo con Back Track 3.
- Con el comando iwconfig, configurar la tarjeta inalámbrica (rausb0) en modo promiscuo. (iwconfig rausb0 mode monitor)
- Verificar que la red a vulnerar se encuentre al alcance.
- Detectar las redes inalámbricas disponibles
- (airodump-ng rausb0)

4. Realizar el ataque:

Conectar otro equipo en la red cifrada y colocarlo a descargar información (Equipo Victima)

En un terminal el siguiente comando captura el tráfico que se esté enviando para poder realizar el ataque, todo el tráfico capturado lo envía al archivo “prueba”

airodump-ng --channel 1 --bssid 00:14:7C:2F:65:38 rausb0 -w prueba

Donde:

- channel es el canal de transmisión del A.P.
- bssid es la MAC del Access Point
- rausb0 es la interfaz wireless
- -w prueba envía la salida al archivo de nombre “prueba”

En otra terminal el siguiente comando envía peticiones arp a fin de generar el tráfico suficiente para poder descifrar la clave

aireplay-ng -3 -b 00:14:7C:2F:65:38 -h 00:18:DE:96:5C:09 rausb0

Donde la primera MAC corresponde a la del Access Point y la segunda a la del equipo “Equipo Victima”

Finalmente en una tercera ventana de terminal el siguiente comando descifra la clave

aircrack-ng prueba.cap

Donde prueba.cap es el archivo del tráfico capturado en la primera ventana terminal.

El sistema automáticamente se detiene cuando este último proceso encuentra la clave y la muestra en hexadecimal y ASCII.

3.2 BLUETOOTH HACKING

Según la historia el origen del nombre ‘bluetooth’ proviene de un Rey vikingo y Danés que gobernó Dinamarca entre los años 940 a 981 se llamaba Harald Blåtand (Blâtand en danés significa: "blâ": piel oscura, y "tan": buena persona, que en inglés se traduce a Harald Bluetooth). Convirtió las tribus en guerra de Noruega, Suecia y Dinamarca al cristianismo y consecuentemente la cristianización de la sociedad y el pueblo vikingo. Por esta razón fue reconocido por su capacidad de ayudar a la gente a comunicarse.

El nombre por el cual se le conoce a esta tecnología “Bluetooth” se debe a que al igual que el rey danés logro unir diferentes tribus con sus diferentes ideologías, el estándar Bluetooth pretende unir diferentes dispositivos.

El logo de Bluetooth mezcla la representación de las Runas Nórdicas Agalas (H) y Berkana (B) en un mismo símbolo.

Figura 42. Logotipo Bluetooth
Imagen tomada de: http://www.seguridadmobile.com/bluetooth/especificacion-bluetooth/estandar-bluetooth/index.html

En el año 1994, la empresa Ericsson inició diversas investigaciones con el fin de estudiar la viabilidad de la existencia de una nueva interfaz entre diversos aparatos, entre ellos, teléfonos móviles u otros dispositivos, que ofreciera bajo consumo y costo.

En 1998 se creó el SIG de Bluetooth (Special Interest Group), que consistía en la unión de diversas empresas de informática y telecomunicaciones entre las cuales se encontraban Intel, Toshiba, Nokia, Ericsson e IBM, y poco tiempo después se incorporaron otras tantas como Microsoft, Motorola, 3COM, y Lucent. Gracias a esta unión y sus esfuerzos de investigación, se consiguió el avance de los estudios, y que los proyectos fueran de por sí una verdadera realidad.

3.2.1 Estándar Bluetooth

Bluetooth es una tecnología que define un estándar global de comunicaciones inalámbricas, especialmente diseñado para redes de área personal WPAN (Wireless Personal Area Network), permitiendo la transmisión de voz y datos mediante la conexión de dispositivos electrónicos entre sí de manera inalámbrica (wireless) en entornos de comunicación móvil y estática.

La norma industrial IEEE 802.15.1 define el estándar global de comunicación inalámbrica entre diferentes dispositivos a través de un enlace por radiofrecuencia, globalmente y sin licencia de corto rango.

Bluetooth es capaz de transmitir a velocidades de 1 Mbps y está apoyado por un gran número de empresas de tecnología, ha surgido últimamente como un posible sustituto a todo tipo de cable anexado a un computador, debido a su bajo costo y el apoyo empresarial con que cuenta. Con la velocidad de transmisión de un 1 Mbps podrá substituir las conexiones de cables paralelos y seriales utilizados en impresoras, conexiones de portátiles, mouses, teclados y otros dispositivos, debido a que es 3 y 6 veces más rápido. La tecnología Bluetooth puede transmitir información de forma efectiva a una distancia de 10 metros entre aparatos que utilicen transmisores "Bluetooth". El FHSS (Frequency Hopping Spread Spectrum) el "Hopping Pattern" de Bluetooth es de 1600 veces por segundo, lo cual garantiza que la transmisión de datos sea altamente segura.

Esta tecnología opera en la banda 2.4 a 2.48 GHZ libre para ISM (Industrial, Scientific and Medical), es decir no requiere licencia de operador, se evitan interferencias con otros protocolos que operen en la misma banda de frecuencias y se logra una compatibilidad universal entre dispositivos Bluetooth. Utiliza un transmisor de salto de frecuencia que sirve para reducir las interferencias y disminuir la intensidad de la señal. El FHSS (Frequency Hopping Spread Spectrum), divide la banda en 79 canales (23 en España, Francia y Japón) de longitud 1 MHZ y realiza 1600 saltos por segundo. La capacidad de transmisión varía según las versiones del núcleo; a una velocidad de transmisión de 1 Mbps en el modo de velocidad básica y una velocidad de transmisión aérea total de 2 a 3 Mbps en el modo de trasferencia mejorada (EDR). Actualmente se encuentra en la versión 2.0, ha pasado por las versiones 1.1, 1.2 mejorando la velocidad de transmisión, la eficiencia y seguridad en los procesos de cifrado y el incremento en las velocidades de configuración en la comunicación con otros dispositivos.

“Piconet” o “Picored” es el nombre dado a una red Bluetooth. Está compuesta por una única unidad maestro y varias unidades denominadas esclavos. Dentro de la “Piconet” cualquier dispositivo puede actuar como Maestro o Esclavo siempre y cuando un único dispositivo debe realizar las funciones de Maestro.

En una “Piconet” pueden comunicarse entre sí hasta (8) unidades Bluetooth. El Maestro utiliza un reloj y un patrón de saltos para sincronizar a los demás dispositivos esclavos. Todas las unidades comparten el canal físico y están sincronizadas desde el punto de vista del tiempo y la secuencia de saltos entre canales. La tecnología Bluetooth permite las conexiones punto a punto como punto a multipunto, donde se establece y enlazan varias piconets en forma de scatternet. Utiliza la técnica de acceso múltiple por división de tiempo (TTD). Esto

permite a un dispositivo participar de forma secuencial en diferentes piconets, estando activo en sólo una piconet cada vez.

La pila de protocolos Bluetooth se basa en el modelo de referencia OSI (Open System Interconnect) de ISO (Internacional Standard Organization) para interconexión de sistemas abiertos. Utiliza una arquitectura de protocolos que divide las diversas funciones de red en un sistema de niveles. De esta manera permite el intercambio transparente de información y fomentan la interoperabilidad entre los productos de diferentes fabricantes.

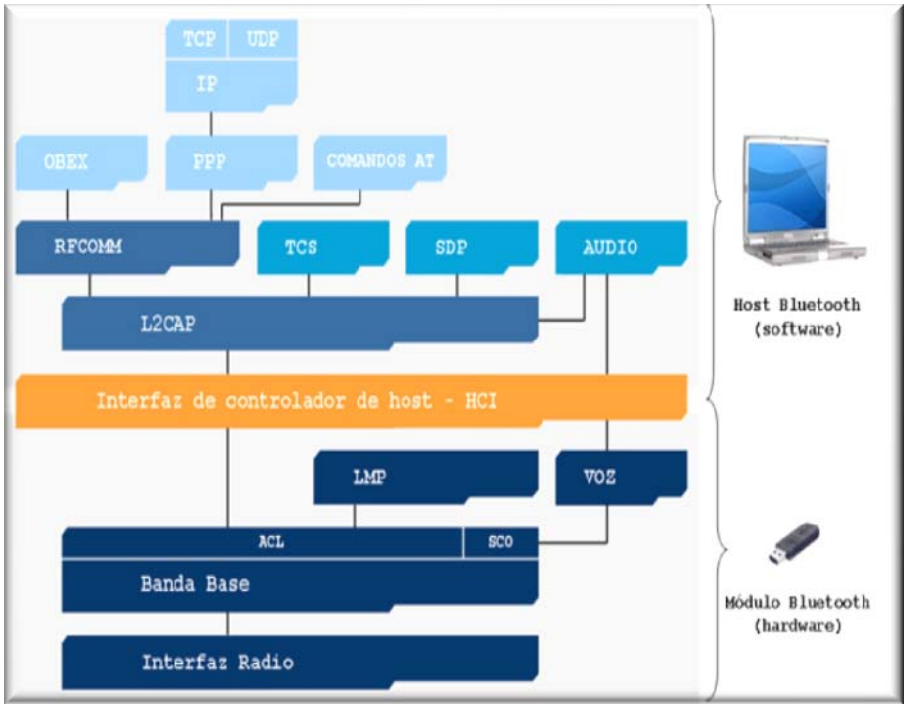

Figura 43. Pila de Protocolos
Imagen tomada de: http://www.seguridadmobile.com/bluetooth/especificacion-bluetooth/arquitectura-de-protocolo/index.html

Se divide en dos zonas, donde cada una se implementa en distintos procesadores:

- El **módulo Bluetooth** (hardware), Es el encargado del envío de información a través de la interfaz de radiofrecuencia.
- El **host Bluetooth** (software), Es el encargado de las capas superiores de enlace y aplicación.

Funciones de las Capas:

- **Capa de banda base e interfaz de radio.** Permite el enlace físico por radiofrecuencia (RF) entre unidades Bluetooth dentro de una picorred, realiza las tareas de modulación y demodulación de los datos en señales RF que se transmiten por el aire.

- **Capa de Protocolo de Gestión de Enlace (LMP) Link Manager Protocol.** Controla y Configura el enlace entre los dispositivos Bluetooth y negociación del tamaño de los paquetes de banda base. Controlar el funcionamiento de los dispositivos en la piconet y proporciona servicios de gestión en las capas inferiores de la arquitectura: capa de radio y de banda base.

- **Capa de Interfaz de Controlador de Host (HCI) Host Controller Interface.** Lleva las comunicaciones entre un módulo Bluetooth y un host separados, permitiéndole a este último acceder a las capacidades de hardware del módulo.

- **Capa de Protocolo de Adaptación y Control del Enlace Lógico (L2CAP) Logical Link Control and Adaptation Protocol.** Se encuentra por encima de la banda base y su función es ofrecer una abstracción de los canales de comunicación a los servicios y las aplicaciones. También es la encargada de la unificación y la segmentación de los datos mediante la multiplexación y demultiplexación de varios canales.

- **Capa de Protocolo de Descubrimiento de Servicios (SDP) Service Discovery Protocol.** Se encargar de buscar y encontrar servicios disponibles en dispositivos Bluetooth.

- **Capa RFCOMM (Radio Frequency Communication).** Suministra una emulación de los puertos serie RS-232 sobre el protocolo L2CAP.

- **Comandos AT.** Instrucciones codificadas que conforman un lenguaje de comunicación entre el hombre y un terminal módem.

3.2.2 Elementos de Seguridad en Bluetooth

La tecnología Bluetooth define tres mecanismos de seguridad a nivel de enlace:

Autorización. Es el proceso por el cual un dispositivo Bluetooth verifica su identidad en otro dispositivo para poder acceder a los servicios que ofrece.

Autenticación. Es el procedimiento que determina los derechos que tiene un dispositivo Bluetooth para acceder a los servicios que ofrece un sistema.

Cifrado de datos. Protege la información que se transmite en un enlace entre dispositivos Bluetooth y garantiza la confidencialidad del mensaje transmitido.

Existen 3 modos de seguridad a nivel de enlace en función de la implementación de los mismos:

Modo 1.

- Ausencia de seguridad.
- La Autenticación y el Cifrado de Datos están deshabilitados.
- Modo promiscuo, todos los dispositivos Bluetooth se puedan conectar a él.
- Ninguna parte del tráfico de datos es cifrada.

Modo 2.

- Seguridad en los servicios a nivel de L2CAP.
- Utiliza la Autorización como mecanismos de seguridad al establecerse el canal de comunicación.
- Un gestor de seguridad controla el acceso de los dispositivos a los diferentes servicios, en función de su nivel de confianza.
- Parte de la información es cifrada con claves individuales generadas durante la conexión (Punto a Punto). El tráfico de difusión no está cifrado.

Modo 3.

- Seguridad en el dispositivo a nivel de LMP.
- Utiliza la Autenticación como mecanismos de seguridad antes de establecerse el canal de comunicación.
- Requiere emparejamiento de dispositivos y existencia de clave de enlace compartida para validar la conexión entre dispositivos.

- La interacción con el usuario requiere la introducción de un código PIN para llevar a cabo el emparejamiento de dispositivos.
- Todo el tráfico se cifra con la clave de cifrado generada.

Los primeros teléfonos celulares fábricos tenían el modo de seguridad de enlace 1, trayendo como consecuencia la aparición de los primeros ataques a teléfonos móviles. Las nuevas versiones de teléfonos celulares incorporaron el Modo de seguridad de enlace 2 y, más tarde, el Modo 3, debido a que los fabricantes se dieron cuenta del riesgo que se tenía al no proteger los teléfonos celulares.

3.2.3 Ventajas y Desventajas de la Tecnología Bluetooth

Debido al crecimiento desmesurado que ha tenido en los últimos años la tecnología Bluetooth es importante exponer las diferentes ventajas y desventajas que ofrece esta tecnología.

Ventajas

A. **Ampliamente Utilizada.** Hoy en día la tecnología Bluetooth es muy popular y se mantiene más popular con el paso del tiempo. Muchas empresas la están utilizando en la mayoría de sus productos: computadoras portátiles, teléfonos celulares, auriculares, impresoras, etc.
B. **Simplicidad o Sencillez.** No se necesita saber ni realizar una especialización para el manejo de la tecnología. Cualquier persona que no tenga ningún conocimiento acerca de la tecnología será capaz de utilizar la función Bluetooth debido a su simplicidad y la facilidad de uso.
C. **Libre de Costo.** No tiene ningún costo por lo tanto usted no tendrá que pagar un centavo por el uso de la Tecnología Bluetooth.
D. **Funciona Inalámbricamente.** No es necesaria la utilización de cables y no tiene de que preocuparse por encontrar el lugar correcto para conectarse.
E. **Variedad de dispositivos.** Se encuentra disponible en una gran variedad de tipos de dispositivos. Celulares, GPS, Impresoras, PDA, Laptops etc. Debido a su bajo costo y su reducido tamaño, esta tecnología se puede implementar en dispositivos de tamaño muy reducido lo cual lo hace muy atractivo para las compañías fabricantes de dispositivos móviles.
F. **Dispositivos de Bajo Costo.** El bajo costo en los dispositivos Bluetooth se convierte en una alternativa viable para que las compañías la implementen.

G. **Protocolo Estándar.** Garantiza un alto nivel de compatibilidad entre los dispositivos. Permite la conexión entre dispositivos aunque no sean de la misma marca o modelo.
H. **Baja Interferencia.** Evita casi siempre las interferencias de otros dispositivos inalámbricos debido al salto de frecuencias.
I. **Consumo de Poca Energía.** Como resultado de las señales de baja potencia que Bluetooth usa, la tecnología requiere poca energía y utilizará menos batería o corriente eléctrica.
J. **Transferencia de Voz y Datos.** Permite que los dispositivos compatibles compartan comunicaciones de datos y de voz.
K. **PAN (Personal Area Network).** Permite conectar hasta siete dispositivos de Bluetooth entre ellos dentro de un área de hasta 30 pies, formando una "piconet" o PAN. Para un solo cuarto, usted puede también instalar piconets múltiples.
L. **Mejoramiento Continuo.** Las nuevas versiones de Bluetooth que se están fabricando, ofrecen muchas nuevas ventajas y serán compatibles con aquellas versiones más viejas.
M. **La tecnología Bluetooth se mantendrá vigente.** La tecnología de Bluetooth es una tecnología mundial, con estándar universal. Puede contar con este tipo de tecnología por muchos años.

Desventajas

A. **Velocidad de transmisión lenta.** Se presenta en el momento de transferir archivos de más de un (*1 MB/seg.*), sin embargo ya están encaminados los esfuerzos para tratar de aumentar su velocidad a 100 MB/seg.

B. **Conexiones Poco Seguras.** Es vulnerada por el ataque Blue MAC Spoofing. Existe un software que puede crear Sniffers Bluetooth caseros a bajo costo. Se puede enviar y recibir mensajes y archivos indeseados (B*luejacking*).

C. **Distancia Limitada.** Radio de acción entre los periféricos (*30 pies entre ellos*). Luego de esa distancia no se puede garantizar la transmisión adecuada de los datos.

D. **Limitación entre la cantidad de periféricos que se pueden utilizar.** Los adaptadores Bluetooth solo permiten la conexión hasta 7 equipos.

3.2.4 Dispositivos Bluetooth

La tecnología Bluetooth posee una gran variedad de dispositivos de uso cotidiano que incorporan tecnología Bluetooth, por esa razón es importante mencionar algunos de ellos.

Los productos mencionados aquí representan la diversidad de productos Bluetooth en el mercado.

Audio: Auriculares estéreo, manos libres auriculares.

Automóvil: Sistemas integrados, manos libres, módulos GPS.

Ordenadores Personales: Ordenadores portátiles con Bluetooth integrado, adaptadores USB Bluetooth, gateways de acceso a otras redes.

Periféricos: Teclados y ratones inalámbricos, impresoras.

 MORENO, Alberto. Dispositivos Bluetooth. http://www.seguridadmobile.com/bluetooth/especificacion-bluetooth/dispositivos-bluetooth/index.html.

Telefonía y Ordenadores de bolsillo: Teléfonos móviles, smart phones, PDAs.

Video e Imagen: Cámaras de fotos, cámaras de video, proyectores.

En total existen 5407 productos con tecnología Bluetooth en el mercado.

3.2.5 Bluetooth Hacking

Existen varios tipos de Ataques desarrollados para teléfonos celulares, a continuación mencionaremos los ataques a teléfonos móviles antiguos y actuales.

3.2.6 Ataques a teléfonos móviles antiguos.

- **Bluesnarf.** Extrae los archivos de un teléfono móvil a través del Perfil de Carga de Objetos (OBEX Object Push) sin la autorización del usuario. El perfil tiene como propósitos la carga y descarga de objetos como las citas y el intercambio de tarjetas de visita. Esta vulnerabilidad estaba presente en los primeros teléfonos móviles que carecían de autorización y autenticación permitiendo la descarga mediante la operación OBEX GET de los archivos conocidos como la agenda de contactos o el calendario de citas. En la actualidad los teléfonos móviles incorporan mecanismos de Autorización en el acceso a este perfil, lo que hace que se requiere que el teléfono celular deba estar incluido en la lista de dispositivos de confianza, de lo contrario requerirá de la confirmación por parte del usuario del teléfono celular.

- **BlueBug.** Establece una conexión RFCOMM a un determinado canal sin necesidad de autenticación, el atacante puede ejecutar comandos AT en el teléfono celular permitiéndole llevar a cabo acciones como obtener información básica: Marca, modelo, IMEI, Realizar llamadas de voz, desvío de llamadas, Gestión de la agenda de contactos y mensaje SMS: Leer, escribir, borrar y enviar, Acceso a la agenda de llamadas: Últimas llamadas perdidas, recibidas o realizadas. Convirtiéndose en una de las vulnerabilidades más peligrosas y con mayor impacto en los usuarios de teléfonos móviles, no sólo por la violación de privacidad (Contactos,

Mensajes SMS), sino por las consecuencias económicas al momento de permitir realizar llamadas telefónicas. La solución adoptada para esta vulnerabilidad en los teléfonos móviles consiste en añadir mecanismos de autenticación y autorización antes de permitir el establecimiento de una conexión RFCOMM.

- **HeloMoto.** Afecta solo a teléfonos móviles Motorola en los siguientes modelos: V80, v500 y v600. Se basa en una implementación incorrecta de la gestión de la lista de dispositivos de confianza. El atacante inicia una conexión al Perfil de Carga de Objetos (OBEX Push Object) con la intención de enviar una tarjeta de visita. De forma automática el dispositivo atacante es añadido a la lista de dispositivos de confianza, si el proceso de envío fue interrumpido por el atacante antes de llegar a su fin. Con el dispositivo incluido en la lista de dispositivos de confianza, el atacante puede acceder a perfiles que requieran autorización pero no autenticación.

3.2.7 Ataques a teléfonos móviles actuales.

- **Blueline.** Es una falsificación o spoofing de la interfaz del usuario sustituyen el mensaje original de la ventana del celular de una conexión que entra por cualquier otro texto para persuadir a la victima para que se acepte la conexión.

- **Blue MAC Spoofing.** Similar por su analogía con el clásico ataque MAC Spoofing en redes Ethernet. Permite suplantar la identidad de un dispositivo de confianza para atacar un teléfono móvil y utilizar sus credenciales para acceder a perfiles que requieren autorización y/o autenticación.

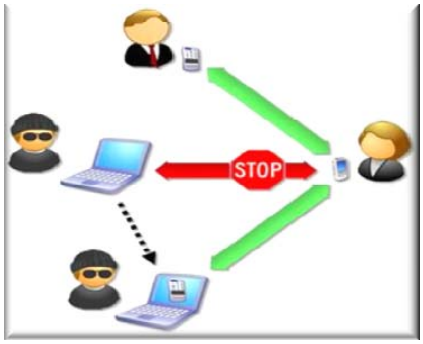

Figura 44. Ataque Blue MAC Spoofing

Imagen tomada de: http://www.seguridadmobile.com/bluetooth/seguridad-bluetooth/blue-mac-spoofing.html

3.2.8 Demostración paso a paso ataque Bluetooth Hacking

Pasos a seguir:

I. Descargar la herramienta Super Bluetooth Hack de la siguiente dirección http://java.xor.sk/?en=1&x=discover. Cabe aclarar que para algunas versiones de teléfonos celulares la aplicación muestra error, así que debemos indagar en la página del creador para mirar la compatibilidad con los demás dispositivos.

II. Descargada la aplicación se procede a instalarla en el teléfono celular, para este caso se utiliza un Nokia N95 y el software de Nokia PC Suite. Una vez conectado el teléfono celular ya sea vía cable, infrarrojo o Bluetooth, se selecciona la opción *Instalar Aplicaciones.*

Figura 45. Software Nokia PC Suite
Imagen tomada de: Autor Proyecto

III. Se selecciona la ubicación de la aplicación para proceder a la instalación en el teléfono celular ya sea en la memoria del teléfono o en la tarjeta de memoria del mismo.

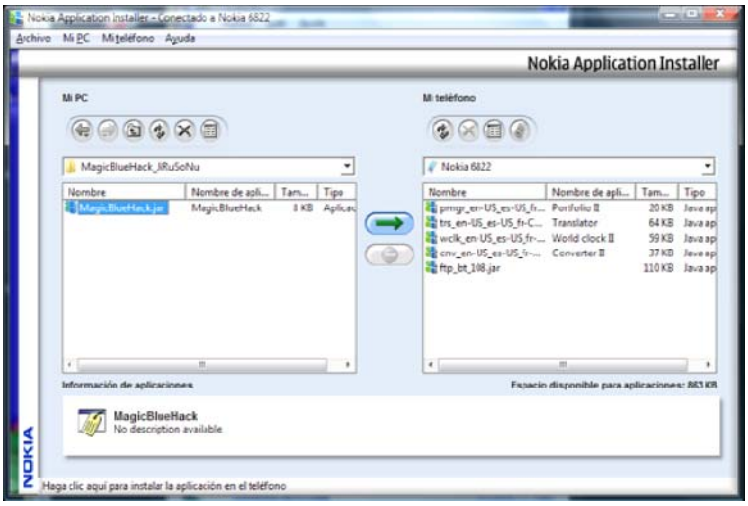

Figura 46. Nokia Application Installer
Imagen tomada de: Autor Proyecto

IV. Ubicada la aplicación se procede a la instalación.

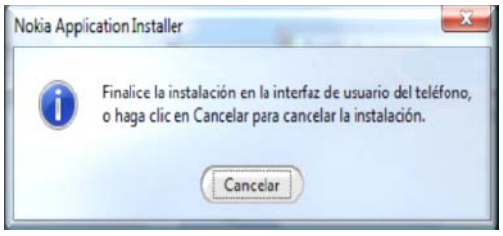

Figura 47. Nokia Application Installer
Imagen tomada de: Autor Proyecto

V. Ahora se procede a ejecutar la aplicación en el teléfono.

Figura 48. Aplicaciones Nokia N95
Imagen tomada de: Autor Proyecto

VI. Cargado de la aplicación

Figura 49. Ejecución Super Bluetooth Hack
Imagen tomada de: Autor Proyecto

VII. Terminado el proceso de cargado de la aplicación se procede a efectuar el ataque, se selecciona la opción conectar.

Figura 50. Conexión a Dispositivos
Imagen tomada de: Autor Proyecto

VIII. Buscar Dispositivos

Figura 51. Escaneo de Dispositivos
Imagen tomada de: Autor Proyecto

IX. Seleccionar nuestra victima

Figura 52. Selección de la Victima
Imagen tomada de: Autor Proyecto

X. Seleccionada la víctima, se procede a efectuar el ataque haciendo uso de las opciones que nos ofrece la herramienta.

Figura 53. Opciones Super Bluetooth Hack
Imagen tomada de: Autor Proyecto

XI. Realizar llamadas

Figura 54. Realizar Llamadas
Imagen tomada de: Autor Proyecto

XII. Ver la lista de contactos, llamadas perdidas, contestadas, etc.

Figura 55. Seleccionar Lista de Contactos
Imagen tomada de: Autor Proyecto

XIII. Lista de Contactos Tarjeta SIM

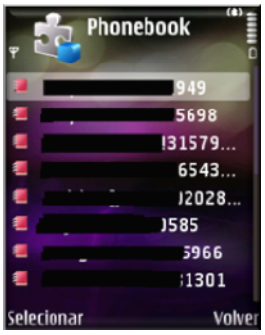

Figura 56. Lista de Contactos
Imagen tomada de: Autor Proyecto

En esta pequeña demostración se omitieron algunos pasos importantes para la realización exitosa del ataque, como lo es la estrategia utilizada o ingeniería social implementada para que la víctima acepte nuestra conexión y nuestra clave de autenticación para poder tener acceso libre al teléfono celular. Eso depende de la imaginación que cada uno de ustedes tenga para lograr engañar a su víctima.

Existe otra herramienta denominada Magic Blue Hack, no es muy completa comparada con la usada en esta demostración pero ofrece la opción de enviar mensajes de texto, opción que no trae la herramienta aquí usada.

4. VIRUS Y CÓDIGO MALICIOSO PARA SISTEMAS OPERACIONALES MÓVILES

4.1. ¿Qué es un virus informático?

En el estricto sentido de la palabra un virus informático es un programa diseñado expresamente para causar un mal funcionamiento de una computadora, realizando acciones en el sistema operativo de la máquina para eliminar, modificar o dañar la información contenida en esta y generalmente provocando una baja en el rendimiento de la misma, causado por estas modificaciones o por procesos ejecutados por el virus para propagarse e infectar otras máquinas, generalmente sin que el usuario afectado se percate de lo que ocurre.

El origen de los virus se remonta a mediados de los 80’ cuando dos programadores en Pakistan Basit y Amjad Alvi de Lahore, descubrieron que sus clientes copiaban y distribuían sus programas sin autorización; buscando una manera de contrarrestar esto, ingeniaron un programa que se copiaba a sí mismo y creaba un mensaje de copyright en cada copia de un disquete que sus clientes hicieran sin autorización, creando de esta manera el primer virus informático y generando a partir de esta idea toda una cultura alrededor de lo virus informáticos.

4.2. ¿Tipos de virus?

Al igual que en los virus orgánicos que atacan al cuerpo humano, dentro del reino de los virus informáticos, podemos encontrar diferentes tipos de virus que pueden ser clasificados no solo por la gravedad de sus efectos, sino principalmente por su modo de actuar y propagarse; de esta manera podemos clasificar los virus informáticos en los siguientes grupos, que no entraremos a detallar ya que no es el tema principal de esta sección.

- ✓ Virus Troyanos
- ✓ Gusanos
- ✓ Macro virus
- ✓ Polimórficos o mutantes
- ✓ Hoax o falsos virus
- ✓ Jokers o bromistas
- ✓ Virus de sector de arranque

Dentro de esta clasificación incluiremos adicionalmente los Virus de dispositivos móviles, los cuales son el tema principal a tratar.

Aunque en términos generales, como ya se ha dicho en la definición general de virus informático, un virus esta creado con el fin específico de causar el mal funcionamiento de una computadora, no podemos sesgar esta definición al concepto clásico de computadora, ya que los dispositivos móviles modernos bien pueden ser considerados como computadoras, ya que cuentan con capacidades cada vez más amplias de almacenamiento y procesamiento, además en su interior funcionan con sistemas operativos específicos para esta clase de plataformas que cada vez son más complejos y si a esto le sumamos que estos pequeños aparatos cada día se hacen más indispensables para nuestras labores cotidianas, creo que es posible visualizar un objetivo muy interesante para los creadores de virus, con un ingrediente adicional que es la alta interconectividad que cada vez incorporan los proveedores en estos dispositivos

4.3. Métodos de contagio

Debido a que un virus informático en el fondo es un programa como cualquier otro, es necesario que sea ejecutado para conseguir sus objetivos, desde la perpetuación de la infección hasta lograr su posible propagación.

Es decir, El virus tiene que ser ejecutado para conseguir infectar un ordenador. Con este propósito, los virus pueden adosarse a otros programas u ocultar su código de manera que se ejecuten al intentar abrir ciertos tipos de archivos. Un archivo infectado te puede llegar en un disco, adjunto en un email o al descargarlo de Internet. En cuanto ejecutes el archivo, se ejecutará el código del virus. El virus intentará entonces infectar otros archivos o discos y realizar cambios en su ordenador.

En la actualidad debido a la proliferación de las memorias USB o penDrive, estos se han convertido en el medio ideal para propagar los virus informáticos y los creadores de virus se han esforzado en crear virus específicamente para explotar esta nueva situación, con virus que se replican de manera automática del computador a las memorias USB y viceversa; incrementando de manera exponencial la posibilidad de propagación.

4.4. Virus en dispositivos móviles

La preocupación por los virus en los dispositivos móviles ha existido desde hace varios años atrás y se incrementó a mediados del 2004 cuando se informó de la aparición del primer virus para esta clase de dispositivos, este virus, denominado Cabir, afectaba a dispositivos funcionando con el sistema operativo Symbian OS y se propagaba por medio de conexiones Bluetooth.

Luego de esto quedó demostrado que es completamente viable la creación de virus para dispositivos móviles, pero muy a pesar de lo que se podría pensar, este virus no causó estragos a niveles exorbitantes ni caos en la innumerable cantidad de teléfonos celulares que emplean Symbian y que disponen de una conexión vía Bluetooth, esto solo gracias a que el Cabir, fue tan solo una prueba de concepto creada por un grupo de ingenieros denominados grupo internacional 29a y a que lo único que causaba era que apareciera un mensaje con la palabra Caribe en la pantalla del celular cada vez que este se encendiera y que de inmediato intentara rastrear otras terminales cercanas a quienes intentaría infectar con el virus.

Luego del Cabir apareció el Duts, que estaba dirigido a dispositivos que emplearan el sistema operativo Windows Pocket PC y aunque también se trataba solo de una prueba de concepto, causó tanto revuelo como el mismo Cabir.

Luego de estas dos pruebas de concepto, apareció lo que podemos considerar como el primer virus real para dispositivos móviles, se trataba del virus Mosquito, que se empezó a distribuir en las copias piratas de un juego para Symbian que llevaba el mismo nombre, originalmente no se trataba de un virus, pero finalmente las cosas no salieron como los desarrolladores lo esperaban y es considerado un virus. Mosquito enviaba un mensaje de texto cada vez que detectaba que se instalaba una copia ilegal del juego, pero no funcionó correctamente y empezó a propagarse, distribuido por las redes P2P.

El virus Mosquito más allá de enviar mensajes de texto no significaba peligro alguno ya que no modificaba ni eliminaba ficheros del dispositivo o alteraba su funcionamiento, de manera que no se puede considerar como una amenaza.

Posterior a estos virus, surgieron algunos otros como Skulls y Comwar, que se propagan a través de conexiones Bluetooth, páginas Web o por los mensajes multimedia (MMS).

Estos virus estaban dirigidos a versiones de Symbian y a modelos de dispositivos específicos ya que deshabilitaban funcionalidades o acceso a aplicaciones propias de esos modelos.

Hasta ahora nos hemos remitido solo a nombrar viejos virus aparentemente inofensivos, pero ¿a que nos enfrentamos en la actualidad? ¿Existe riesgo real de virus en dispositivos móviles hoy en día?

Pues la respuesta es sí, y de nuevo el más atacado resulta ser Symbian, sin que esto quiera decir que sea malo o que sea inseguro.

Teniendo en cuenta las tres premisas de la seguridad informática, es necesario proteger: la Confidencialidad, la Integridad y la Disponibilidad de la información; podríamos determinar si un virus es o no un verdadero riesgo, es decir, si existe un virus que nos impacte directa o indirectamente uno de estos tres pilares, debemos considerarnos en riesgo.

Con esto en mente, es interesante mencionar un virus más reciente que aunque no adquirió magnitudes mundiales, ya que solo afectó a usuarios en China y de un mismo operador celular, nos da un claro ejemplo del alcance de esta clase de virus, en este caso que compromete seriamente la confidencialidad de la información; se trata del virus SymbOS/Beselo.A!worm que puede ser ejecutado en algunos dispositivos corriendo Symbian S60, los especialistas de “Fortinet lo han detectado en dispositivos de mano como los Nokia 6600, 6630, 6680, 7610, N70 y N72. Este software malicioso se instala en los terminales oculto como un archivo multimedia (MMS) con un nombre sugerente como Beauty.jpg o Sex.mp3.”

Lo interesante de este virus es que posterior a la infección, el virus recolecta todos los número telefónicos almacenados en el teléfono, los empaqueta en un fichero .SIS (Symbian Installation Source), y los envía por medio de un MMS.

Ya se ha hablado un poco sobre los virus en dispositivos móviles basados en Symbian OS, pero y ¿qué pasa con Windows Mobile?, pues como es de esperarse también existen virus desarrollados específicamente para esta plataforma y al igual que los del Symbian, no son para nada nuevos.

Kaspersky Labs reportó a mediados del 2004 la aparición del que es considerado el primer virus para Windows Mobile, el Duts, como se denominaba el virus, al igual que el Cabir en Symbian, era tan solo una prueba de concepto, para demostrar que esta plataforma era vulnerable y que era posible perpetrar un ataque contra la misma.

Duts se trataba de un virus tipo gusano de 1520 bytes de tamaño y su forma de propagación en los dispositivos móviles era vía correo electrónico, por Internet a través de su memoria RAM o al conectarlo a un PC utilizando la tecnología Bluetooth y aunque no significaba ningún peligro real, abrió la puertas para el mundo de los virus en esta plataforma.

Posterior al Duts surgieron algunos otros virus para Windows Mobile que empezaron a tornarse un tanto más agresivos, aunque sin representar aún un riesgo alto, como el virus Worm.MSIL.Cxover, que luego de infernar el dispositivo, busca los ficheros que habían sido eliminados del dispositivo para intentar enviarlos a otros dispositivos, o como el Email-Worm.MSIL.Letum, que intentaba enviar correos electrónicos desde el dispositivo que infectaba. Algunos datos adicionales que nos pueden dar una mejor visión acerca de los virus en dispositivos móviles los podemos encontrar el Kaspersky Security Bulletin 2006: Mobile malware, en donde muestra un análisis detallado de la evolución de los mismos hasta ese año. De este informe es importante destacar la clasificación hecha por Kaspersky sobre las finalidades de los virus en los dispositivos móviles en donde no es de extrañar la especial orientación comercial que suelen tener estos virus, teniendo dentro de sus principales objetivos el hurto del dinero de los usuarios de estos dispositivos. Según el mismo informe, a lo largo del 2006 aparecieron:

- ✓ 22 familias de virus conocidas
- ✓ 10 variantes o modificaciones de esas familias originales
- ✓ plataformas o sistemas operativos claramente vulnerados (Symbian y Windows Mobile)

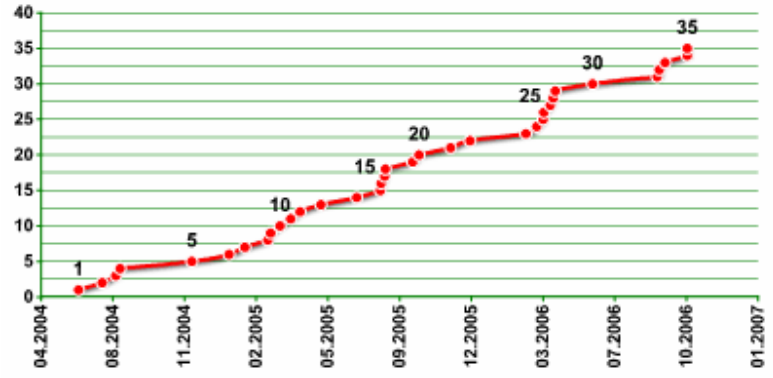

Figura 57. Aumento del número de familias de virus móviles en 2006
Imagen tomada de: http://www.viruslist.com/en/analysis?pubid=204791922

Innovation	Family	Month	OS	Functionality
+	Trojan-SMS.J2ME.RedBrowser	February 2006	J2ME	Sends SMS
+	Worm.MSIL.Cxover	March 2006	Windows Mobile / .NET	Deletes files, copies its body to other devices
-	Worm.SymbOS.StealWar	March 2006	Symbian	Data theft, spreads via Bluetooth and MMS
+	Email-Worm.MSIL.Letum	March 2006	Windows Mobile / .NET	Spreads via email
+	Trojan-Spy.SymbOS.Flexispy	April 2006	Symbian	Data theft
-	Trojan.SymbOS.Rommwar	April 2006	Symbian	Replaces system applications
-	Trojan.SymbOS.Arifat	April 2006	Symbian	—
-	Trojan.SymbOS.Romride	June 2006	Symbian	Replaces system applications
+	Worm.SymbOS.Mobler.a	August 2006	Symbian	Deletes antivirus files, replaces system applications, replicates via memory cards
+	Trojan-SMS.J2ME.Wesber	September 2006	J2ME	Sends SMS
+	Trojan-Spy.SymbOS.Acallno	September 2006	Symbian	Data theft
-	Trojan.SymboS.Flerprox	October 2006	Symbian	Replaces system boot files
-	not-a-virus:Tool.SymbOS.Hidmenu	October 2006	Symbian	Application

New mobile virus families in 2006

Tabla 2. Nuevas familias de virus móviles en 2006
Imagen tomada de: http://www.viruslist.com/en/analysis?pubid=204791922

5. CONLUSIONES: RECOMENDACIONES DE SEGURIDAD – BUENAS PRACTICAS

Hoy en día la gran mayoría de las personas utilizan dispositivos móviles y las empresas proveen a sus gerentes, ejecutivos y demás personal de la empresa dispositivos móviles sin tener en cuenta los riesgos asociados a la extracción y/o modificación de la información.

Por lo tanto se hace necesario contar con recomendaciones de seguridad básicas y con políticas de seguridad alineadas a los avances de la tecnología de información y las telecomunicaciones. Por esta razón es muy importante tener en cuenta y poner en práctica las siguientes medidas básicas de seguridad con el fin de proteger a los dispositivos móviles que utilizamos a diario.

Las medidas indicadas son simples y de fácil aplicación, por lo tanto tendrán que convertirse en la conducta habitual de un usuario que maneje cualquier tipo de dispositivo móvil. Todas estas recomendaciones de seguridad podrán ser implantadas en mayor o menor medida en función de la capacidad de procesamiento del terminal o dispositivo utilizado.

Como guía de buenas prácticas, y a modo de resumen, se propone el siguiente decálogo de medidas de seguridad:

- ✓ Actualizar la política de seguridad, para considerar el entorno móvil .
- ✓ Elaborar una Guía de Buenas Prácticas para usuarios, prestando especial atención a la formación y concienciación .
- ✓ Implantar mecanismos de copias de seguridad .
- ✓ Implantar mecanismos de reinicialización y borrado remoto .
- ✓ Aplicar control de acceso al dispositivo .
- ✓ Disponer de gestión centralizada de dispositivos .
- ✓ Implantar cifrado de datos sensibles .

 REBOLLAL, Eduardo López. JARAUTA SÁNCHEZ, Javier. Seguridad en Entornos Móviles Corporativos. http://www.sia.es/noticias/SIC79_082-088.pdf.

- ✓ Disponer de protección anti-malware .
- ✓ Habilitar el control de políticas en puntos de acceso .
- ✓ Prevenir las fugas de información .
- ✓ Nunca pierda de vista el dispositivo, ya que éste resulta atractivo para su sustracción o robo .
- ✓ Active el código PIN y guarde en lugar seguro el PUK .
- ✓ En dispositivos avanzados, active la opción de bloqueo de terminal cada cierto tiempo (ej. 10 minutos), y la solicitud de una contraseña para desbloquear el terminal .
- ✓ Active el bloqueo automático de su teléfono móvil para evitar que personas no autorizadas puedan acceder a sus datos .
- ✓ Utilice contraseñas robustas y sencillas para proteger el dispositivo y las conexiones .
- ✓ Vigile el consumo e infórmese de cualquier anomalía en su factura .
- ✓ Esté prevenido ante fraudes mediante mecanismos de “ingeniería social”, que intentan embaucarle para llamar y/o enviar mensajes a determinados números .
- ✓ No libere ni manipule los componentes del terminal en lugares que no le ofrezcan las garantías suficientes .
- ✓ Mantenga un sistema periódico de copias de seguridad (backup) .
- ✓ No abra correos electrónicos ni acepte archivos de los cuáles desconozca el remitente .

 REBOLLAL, Eduardo López. JARAUTA SÁNCHEZ, Javier. Seguridad en Entornos Móviles Corporativos. http://www.sia.es/noticias/SIC79_082-088.pdf.

 Guía para proteger y usar de forma segura su móvil. http://www.inteco.es/Seguridad/Observatorio/manuales_es/GuiaManual_movil

- ✓ Utilice programas de cifrado para proteger la información de los dispositivos .
- ✓ Instale software original para poder solicitar soporte al fabricante .
- ✓ No deje las tarjetas de memoria dentro del dispositivo si no las necesita, en caso de robo o extravío limitará en gran medida las pérdidas .
- ✓ En caso de pérdida o robo haga una denuncia y llame al operador para bloquear la tarjeta SIM y el dispositivo .
- ✓ Solicite el borrado remoto de la información si dispone de este servicio .
- ✓ En los equipos basados en Windows Mobile, puede pasar con contraseña desde el PC los documentos de Word o Excel que tengan datos confidenciales. No tendrá problemas para abrirlos en el celular .
- ✓ Cuando vaya a ceder o entregar un teléfono inteligente, asegúrese de borrar (después de copiar) toda su información y sus archivos. Es común que la gente reciba dispositivos móviles que tienen datos confidenciales del dueño anterior .
- ✓ No se conecte a puntos de acceso no conocidos .
- ✓ Tenga un antivirus actualizado: con cortafuegos, antispam, anti-espías, etc .
- ✓ No instale aplicaciones de procedencia desconocida o no fiable .
- ✓ Configure el dispositivo para que no se puedan instalar programas que no estén certificados y/o de fuente desconocida .
- ✓ Evite realizar emparejamientos en lugares públicos .

 Guía para proteger y usar de forma segura su móvil. http://www.inteco.es/Seguridad/Observatorio/manuales_es/GuiaManual_movil

 Recomendaciones de seguridad para proteger el teléfono celular. http://www.pac.com.ve/index.php?option=com_content&view=article&catid=67&Itemid=76&id=4813

- ✓ Activar el Bluetooth en el dispositivo sólo cuando sea necesario y desactivarlo cuando no se vaya a utilizar más .

- ✓ Configurar el dispositivo en modo oculto para disminuir las probabilidades de que un atacante detecte la presencia del dispositivo al escanear en búsqueda de equipos Bluetooth .

- ✓ Configurar el dispositivo para que utilice la función de cifrado en todas las comunicaciones. Garantizando la confidencialidad del intercambio de mensajes .

- ✓ Cambiar el nombre del dispositivo asignado por el fabricante. No dejar o utilizar el mismo nombre de la marca y modelo, por ejemplo: W600, N95. Utilizar otra clase de nombres .

- ✓ No aceptar conexiones entrantes de dispositivos desconocidos. Esto implica también intentos de conexión de personas en las que no se confía aunque el pretexto pueda parecer inofensivo, por ejemplo: Emparejar dos dispositivos para transferir una fotografía .

- ✓ Configurar todos los perfiles soportados por el dispositivo para que requieran autenticación ante cualquier intento de acceso .

- ✓ Verificar periódicamente la lista de dispositivos de confianza y eliminar aquellas entradas de dispositivos con los que habitualmente no se establece conexión .

- ✓ Aunque actualmente todavía no se ha descubierto una forma de romper la seguridad del emparejamiento realizando fuerza bruta sobre un código de seguridad Bluetooth (clave PIN) que hayan empleado dos dispositivos emparejados, utilizar en la medida de lo posible claves PIN de longitud extensa, hasta 16 bytes .

 MORENO, Alberto. Recomendaciones de Seguridad. http://www.seguridadmobile.com/bluetooth/seguridad-bluetooth/recomendaciones.html.

En cada organización se han de decidir las prioridades, las medidas que mejor se ajusten a las necesidades identificadas y la extensión con que se tienen que aplicar. Lo más inmediato suele ser empezar por la actualización de políticas y la revisión y extensión de los procedimientos de gestión y control. Por otra parte, la industria viene trabajando desde hace muchos años en este campo, y ya se dispone de herramientas y familias de soluciones que ayudan a establecer algunas de las funciones expresadas.

BIBLIOGRAFÍA

SYMBIAN OS

Important dates in Symbian History. The History of Symbian.
Disponible en Internet:
<http://www.symbian.org/about-us/history-symbian>
Descripción: La historia de Symbian OS.

Wikipedia: La Enciclopedia Libre, Symbian OS.
Disponible en Internet:
<http://en.wikipedia.org/wiki/Symbian_OS>
Descripción: Información general de Symbian OS.

Gartner. Worldwide Smartphone Sales Reached Its Lowest Growth Rate With 3.7 Per Cent Increase in Fourth Quarter of 2008.
Disponible en Internet:
<http://www.gartner.com/it/page.jsp?id=910112>
Descripción: Estudio de ventas sistemas operativos móviles.

Symbian Developer. Symbian^3 Product Developer Library.
Disponible en Internet:
<http://developer.symbian.org/main/documentation/reference/s3/pdk/ >
Descripción: Biblioteca completa de documentación Symbian OS.

VILLEGAS MARTÍNEZ, Aidee Grissel. AGUILAR JUÁREZ, Irene. Análisis Técnico de los Sistemas Operativos Symbian y Windows Mobile.
Disponibe en Internet:
< http://www.scribd.com/doc/18308200/ANALISIS-TECNICO-DE-LOS-SISTEMAS-OPERATIVOS-SYMBIAN-Y-WINDOWS-MOBILE>
Descripción: Articulo sobre el análisis técnico de los sistemas operativos Symbian y Windows Mobile.

Belatrix Software Factory BSF S.A. Documento de Investigación sobre el Análisis de las Características de los Dispositivos Móviles Inteligentes (Smart Phones).
Disponible en Internet:
<http://www.belatrixsf.com/index.php/spdesarrollosmoviles>
Descripción: Breve análisis de las características de los dispositivos móviles.

MCCUE, Andy. Mobile Mosquito premium rate SMS "Trojan" not a virus.
Disponible en Internet:
<http://www.silicon.com/technology/security/2004/08/12/mobile-mosquito-premium-rate-sms-trojan-not-a-virus-39123118/>
Descripción: Noticia sobre el troyano “Mosquito” en Symbian OS.

Wiki Symbian Developer. Capabilities (Symbian Signed)/AllFiles Capability.
Disponible en Internet:
<http://developer.symbian.org/wiki/index.php/Capabilities_(Symbian_Signed)/AllFiles_Capability>
Descripción: Capacidades de la plataforma de seguridad de Symbian OS.

Vulnerabilidad en teléfonos Nokia con un simple SMS.
Disponible en Internet:
<http://climbo.wordpress.com/2009/01/15/vulnerabilidad-en-telefonos-nokia-con-un-simple-sms/>
Descripción: Tutorial vulnerabilidad SMS (Mensajes de Texto) en Symbian OS.

S60 Curse of Silence Demo.
Disponible en Internet:
<http://www.youtube.com/watch?v=GuOGn8ATa9U>
Descripción: Video de demostración vulnerabilidad SMS en Symbian OS.

RIM (BlackBerry)

Introduction to BlackBerry Development.
Disponible en Internet:
<http://www.blackberry.com/DevMediaLibrary/view.do?name=introblackberrydev>
Descripción: Introducción BlackBerry para desarrolladores.

Wikipedia: La Enciclopedia Libre, *BlackBerry*.
Disponible en Internet:
<http://es.wikipedia.org/wiki/BlackBerry>
Descripción: Información general BalckBerry.

KAO, Robert. SARIGUMBA, Dante. BlackBerry For Dummies. Wiley Publishing, Inc.

HOFFMAN, Daniel V. Blackjacking: Security Threats to BlackBerry, PDAs, and Cell Phones in the Enterprise. Wiley Publishing, Inc.

BACHMANN, Glenn. Hacking BlackBerry. Wiley Publishing, Inc.

FISHER, Dennis. Spyware en BlackBerry puede interceptar textos, correo y localizar la posición del usuario.

Disponible en Internet:
<http://threatpost.com/es_la/blogs/spyware-en-blackberry-puede-interceptar-textos-correo-y-localizar-la-posicion-del-usuario-0208>
Descripción: Breve reseña programa espía en BlackBerry.

NYSTEDT, Dan. BlackBerry, Other Smartphone Users Easy Spy Targets.
Disponible en Internet:
<http://www.pcworld.com/article/173265/blackberry_other_smartphone_users_easy_spy_targets.html>
Descripción: Breve reseña programa espía en BlackBerry.

BlackBerry Spy Software Video.
Disponible en Internet:
<http://www.spyblackberry.com/52/blackberry-spy-software-video/>
Descripción: Comentarios en video sobre el programa espía en BlackBerry.

NARAINE, Ryan. BlackBerry advierte sobre falla que genera robo de identidad.
Disponible en Internet:
<http://threatpost.com/es_la/blogs/blackberry-advierte-sofre-falla-que-genera-robo-de-identidad-100509>
Descripción: Vulnerabilidad “phishing” en BlackBerry.

AGGARWAL, Mayank. VENNON, Troy. SMobile Global Threat Center. Study of BlackBerry Proof-of-Concept Malicious Applications.
Disponible en Internet:
<http://threatcenter.smobilesystems.com/?p=1752>
Descripción: Artículo relacionado con el estudio de aplicaciones maliciosas en BlackBerry.

BlackBerry Security. Boletines e información.
Disponible en Internet:
<http://es.blackberry.com/ataglance/security/news.jsp>
Descripción: Boletines e información de vulnerabilidades en BlackBerry.

VERACODE. TXSBBSpy Demo.
Disponible en Internet:
<http://vimeo.com/9192358>
Descripción: Video tutorial del programa espía en BlackBerry.

WINDOWS MOBILE

Una historia sencillamente brillante. Enfoque compartido a la innovación.
Disponible en Internet:
<http://www.htc.com/es/quietlybrilliant/index.html>
Descripción: La historia de HTC donde encontramos la alianza con Microsoft.

USIGLIO KOVACS, Bruno Paulo. MONTEIRO, Vanesa de Freitas. Un estudio Práctico de las Amenazas de Seguridad a los Dispositivos Portátiles con Windows Mobile.
Disponible en Internet:
<http://www-di.inf.puc-rio.br/~endler/projects/Anubis/Ameacas.pdf>
Descripción: Monografía “Un estudio Práctico de las Amenazas de Seguridad a los Dispositivos Portátiles con Windows Mobile.”

Windows Mobile.
Disponible en Internet:
<http://www.microsoft.com/windowsmobile/en-us/default.mspx>
Descripción: Pagina Oficial Windows Mobile - Información general.

McAfee. WinCE/Infojack.
Disponible en Internet:
<http://vil.nai.com/vil/content/v_144191.htm >
Descripción: Boletín e información de vulnerabilidad en Windows Mobile por parte de McAfee.

MORENO TABLADO, Alberto. Vectores de ataque Bluetooth a teléfonos Windows Mobile.
Disponible en Internet:
<http://www.seguridadmobile.com/windows-mobile/seguridad-windows-mobile/ataques-bluetooth.html>
Descripción: Vectores de ataque Bluetooth a teléfonos Windows Mobile.

WinCE / InfoJack Trojan. El troyano que está atacando a los Windows CE.
Disponible en Internet:
<http://www.tecnoseguridad.net/wince-infojack-trojan-el-troyano-que-est-atacando-a-los-windows-ce/>
Descripción: Noticia sobre vulnerabilidad en Windows Mobile – Troyano WinCE/InfoJack

Seguridad en Windows Mobile.
Disponible en Internet:
<http://www.tecnoseguridad.net/seguridad-en-windows-mobile/>
Descripción: Breve reseña sobre seguridad en Windows Mobile.

MULLINER, Collin. Advanced Attacks Against PocketPC Phones.
Disponible en Internet:
<http://mulliner.org/pocketpc/feed/CollinMulliner_syscan07_pocketpcmms.pdf >
Descripción: Diapositivas sobre ataques avanzados contra teléfonos PocketPC.

MORENO TABLADO, Alberto. HTC / Windows Mobile OBEX FTP Service Directory Traversal.
Disponible en Internet:
<http://seguridadmobile.blogspot.com/2009/07/htc-windows-mobile-obex-ftp-service.html>
Descripción: Boletín e información de vulnerabilidad en Windows Mobile - HTC / Windows Mobile OBEX FTP Service Directory Traversal.

Hacking Windows Mobile 6.1 to Enable Tethering.
Disponible en Internet:
<http://stevenharman.net/blog/archive/2008/10/03/windows-mobile-internet-connection-sharing-hack.aspx>
Descripción: Breve reseña de hacking en Windows Mobile 6.1 para obtener una conexión compartida a Internet.

Kaspersky. Introducción a la virología móvil, parte II.
Disponible en Internet:
<http://www.kaspersky.com/sp/news?id=199601936>
Descripción: Articulo sobre el análisis general del problema de los virus para teléfono móviles.

BECHER, Michael. FREILING, Felix C. LEIDER, Boris. On the Effort to Create Smartphone Worms in Windows Mobile.
Disponible en Internet:
<http://pi1.informatik.uni-mannheim.de/filepool/publications/on-the-effort-to-create-smartphone-worms-in-windows-mobile.pdf>
Descripción: Artículo donde cuenta el esfuerzo que se necesita para crear gusanos en los Smartphone de Windows Mobile.

AKPODIETE, Tari. What is the InfoJack Trojan and How Does it Affect Windows CE machines.
Disponible en Internet:
<http://www.smartphonemag.com/cms/blogs/18/what_is_the_infojack_trojan_and_how_does>
Descripción: Breve reseña sobre el Troyano WinCE/InfoJack.

Windows Mobile Device Security Model.
Disponible en Internet:
<http://msdn.microsoft.com/en-us/library/bb416353(v=MSDN.10).aspx>
Descripción: Biblioteca completa de documentación Windows Mobile.

iPhone OS X

VOGELSTEIN, Fred. The Untold Story: How the iPhone Blew Up the Wireless Industry.
Disponible en Internet:
<http://www.wired.com/gadgets/wireless/magazine/16-02/ff_iphone?currentPage=1>
Descripción: La historia no contada del iPhone.

Wikipedia: La Enciclopedia Libre, Historia del iPhone.
Disponible en Internet:
<http://es.wikipedia.org/wiki/Historia_del_iPhone>
Descripción: Historia del iPhone.

La verdadera historia del iPhone. Publicado por: Wired.
Disponible en Internet:
<http://www.vanguardia.com.mx/diario/noticia/tech/tecnologia/la_verdadera_historia_del_iphone/128957>
Descripción: La verdadera historia del iPhone.

Wikipedia: La Enciclopedia Libre, iPhone.
Disponible en Internet:
<http://es.wikipedia.org/wiki/I-Phone>
Descripción: Información general de iPhone.

iPhone 4.
Disponible en Internet:
<http://www.apple.com/la/iphone/features/>
Descripción: Pagina Oficial de Apple – Información general iPhone.

Descubierta nueva vulnerabilidad en el iPhone.
Disponible en Internet:
<http://www.actualidadiphone.com/2010/05/28/descubierta-nueva-vulnerabilidad-en-el-iphone/>
Descripción: Breve reseña sobre vulnerabilidad en el iPhone.

BETANCOURT, Christian. iPhone OS 3.1.3 corrige numerosas vulnerabilidades de seguridad.
Disponible en Internet:
<http://www.opensecurity.es/iphone-os-3-1-3-corrige-numerosas-vulnerabilidades-de-seguridad/>
Descripción: Informe sobre corrección de vulnerabilidades de seguridad en el iPhone.

Vulnerabilidad SMS iPhone.
Disponible en Internet:
<http://www.blueplastic.net/vulnerabilidad-sms-iphone/>
Descripción: informe sobre vulnerabilidad SMS en el iPhone

Vulnerabilidad en el iPhone OS pondrá en peligro nuestros datos.
Disponible en Internet:
<http://iphonefanatico.com/2010/05/29/una-nueva-vulnerabilidad-en-el-iphone-os-pondra-en-peligro-nuestros-datos/>
Descripción: Breve reseña sobre vulnerabilidad en el iPhone

GOMEZ, Rafael. Apple arregla una vulnerabilidad en la mensajería SMS del iPhone.
Disponible en Internet:
<http://atpixeles.com/apple-arregla-una-vulnerabilidad-en-la-mensajeria-sms-del-iphone>
Descripción: Informe corrección vulnerabilidad SMS en el iPhone.

Soporte Técnico de Apple. Acerca del contenido de seguridad de iPhone OS 3.1.3 y iPhone OS 3.1.3 para iPod touch.
Disponible en Internet:
<http://support.apple.com/kb/HT4013?viewlocale=es_ES>
Descripción: Boletines e información de vulnerabilidades en el iPhone.

iPhone OS 3.1.3 fixes vulnerabilities.
Disponible en Internet:
<http://www.h-online.com/security/news/item/iPhone-OS-3-1-3-fixes-vulnerabilities-920756.html>
Descripción: Breve reseña sobre vulnerabilidad en el iPhone.

PRINCE, Brian. Apple iPhone SMS Used as Bait in Rogue Antivirus Scam.
Disponible en Internet:
<http://www.eweek.com/c/a/Security/Apple-iPhone-MMS-Used-as-Bait-in-Rogue-Antivirus-Scam-180249/?kc=rss>
Descripción: Breve reseña sobre el uso de SMS o MMS para engañar a los usuarios a la descarga de software antivirus falso en el iPhone.

ANDROID

Android Developer. What is Android?
Disponible en Internet:
http://developer.android.com/guide/basics/what-is-android.html
Descripción: Biblioteca completa de documentación de Android.

MULLINER, Collin. MILLER, Charlie. Fuzzing the Phone in your Phone.
Disponible en Internet:
<http://www.blackhat.com/presentations/bh-usa-09/MILLER/BHUSA09-Miller-FuzzingPhone-PAPER.pdf>
Descripción: Articulo vulnerabilidad maquina Virtual Dalvik.

KINCAID, Jason. Security Flaw Makes It Easy To Bypass Verizon Droid Screen Lock.
Disponible en Internet:
<http://techcrunch.com/2010/01/11/verizon-droid-security-bug/>
Descripción: Breve reseña vulnerabilidad bloque de pantalla en Android.

VENNON, Troy. STROOP, David. Android Market. Threat Analysis of the Android Market.
Disponible en Internet:
<http://threatcenter.smobilesystems.com/wp-content/uploads/2010/06/Android-Market-Threat-Analysis-6-22-10-v1.pdf>
Descripción: Articulo análisis de amenazas en el mercado Android.

TORRE, Víctor Antonio. Varias vulnerabilidades de denegación de servicio en Android.
Disponible en Internet:
<http://www.hispasec.com/unaaldia/4004>
Descripción: Breve reseña de vulnerabilidades de denegación de servicio en Android.

TORRE, Víctor Antonio. Problema de seguridad en Android.
Disponible en Internet:
<http://www.hispasec.com/unaaldia/3921>
Descripción: Breve reseña con problema de seguridad en Android.

ROPERO, Antonio. Una vez más, malware en aplicaciones legítimas.
Disponible en Internet:
<http://www.hispasec.com/unaaldia/4152>
Descripción: Breve reseña de malware en aplicaciones legítimas de Android.

Problema de seguridad en Android : Pueden activar remotamente Cámara y Micrófono.
Disponible en Internet:
<http://www.zonavirus.com/noticias/2009/problema-de-seguridad-en-android-pueden-activar-remotamente-camara-y-microfono.asp>
Descripción: Breve reseña de vulnerabilidad de activación remota de cámara y micrófono en Android.

Android denial-of-service issues
Disponible enInternet:
<http://www.ocert.org/advisories/ocert-2009-014.html>
Descripción: Boletín informe de vulnerabilidad denegación de servicios en Android.

ESPINOZA, Francisco. Se descubren graves vulnerabilidades en Android.
Disponible en Internet:
<http://tekcrispy.com/2008/11/se-descubren-graves-vulnerabilidades-en-android/>
Descripción: Informe sobre grave vulnerabilidad en Android.

Android tiene vulnerabilidades en su navegador web.
Disponible en Internet:
<http://www.incubaweb.com/android-tiene-vulnerabilidades-en-su-navegador-web/>
Descripción: Noticia vulnerabilidad en navegador web de Android.

Google resuelve vulnerabilidades de denegación de servicio en Android.
Disponible en Internet:
<http://www.idg.es/pcworldtech/Google-resuelve-vulnerabilidades-de-denegacion-de-/doc85886-Actualidad.htm>
Descripción: Informe corrección de vulnerabilidades denegación de servicios en Android.

Problema de seguridad en Android.
Disponible en Internet:
<http://www.infosecurityvip.com/newsletter/vulnerabilities_ago09.html>
Descripción: Boletines e informes de vulnerabilidades en Android.

Android tiene un tremendo agujero (negro) de seguridad en su navegador.
Disponible en Internet:
<http://www.faq-mac.com/noticias/34519/android-tiene-tremendo-agujero-negro-seguridad-navegador#>
Descripción: Informe de vulnerabilidad en el navegador de Android.

HERRANZ, Arantxa. Aparecen aplicaciones phishing en Android.
Disponible en Internet:
<http://www.idg.es/pcworldtech/mostrarNoticia.asp?id=88867&seccion=actualidad>
Descripción: Breve reseña de la aparición de programas fraudulentos en Android Marquet.

El phishing bancario llega a la Android Marketplace de Google.
Disponible en Internet:
<http://spamloco.net/2010/01/phishing-bancario-android-marketplace.html>
Descripción: Breve reseña de aplicaciones bancarias fraudulenta en la tienda online de Android.

REDES INALÁMBRICAS WI-FI

Revista NEX IT, Specialist. Ethical Hacking #13 vol1. Pag. 52-62.

BEAVER, Kevin. DAVIS, Peter T. Hacking wireless Networks for Dummies.

CACHE, Johnny. LIU, Vincent. Hacking Exposed Wireless, McGraw Hill.

aircrack-ng.
Disponible en Internet:
<http://www.aircrack-ng.org/doku.php>
Descripción: Página oficial de la herramienta aircrack-ng.

BLUETOOTH HACKING

Wikipedia: La Enciclopedia Libre, *Bluetooth*.
Disponible en Internet:
<http://es.wikipedia.org/wiki/Bluetooth>
Descripción: Información general tecnología Bluetooth.

Historia del Bluetooth.
Disponible en Internet:
<http://motos.autocity.com/reportajes/Cascos-Bluetooth/01-2006/index_historiabluetooth.html?cod=4730>
Descripción: Historia del Bluetooth.

Historia del Bluetooth.
Disponible en Internet:
<http://www.mobilecloseup.com/foros/showthread.php?t=1138>
Descripción: Historia del Bluetooth

Historia del Bluetooth.
Disponible en Internet:
<http://www.perspectivaciudadana.com/contenido.php?itemid=17917>
Descripción: Historia del Bluetooth.

Historia de la Tecnología Bluetooth.
Disponible en Internet:
<http://spanish.bluetooth.com/Bluetooth/SIG/History_of_the_SIG.htm>
Descripción: Historia del Bluetooth.

Christian. ¿Qué es Bluetooth?
Disponible en Internet:
<http://tecnyo.com/%C2%BFque-es-bluetooth/>
Descripción: Definición de la tecnología Bluetooth.

¿Qué es Bluetooth?
Disponible en Internet:
<http://www.alegsa.com.ar/Notas/86.php>
Descripción: Definición de la tecnología Bluetooth.

VELASCO, Alejandro. Métodos de Modulación de Frecuencia.
Disponible en Internet:
<http://www.monografias.com/trabajos14/modulac-frecuencia/modulac-frecuencia.shtml>
Descripción: Frecuencias para sistemas spread spectrum, wi-fi, bluetooth y wlan.

Aspectos Técnicos.
Disponible en Internet:
<http://www.bluetooth.com/Spanish/Technology/Pages/default.aspx>
Descripción: Página oficial tecnología Bluetooth – Aspectos Técnicos

MORENO, Alberto. Estándar Bluetooth.
Disponible en Internet:
<http://www.seguridadmobile.com/bluetooth/especificacion-bluetooth/estandar-bluetooth/index.html>
Descripción: Reseña del estándar Bluetooth.

MORENO, Alberto. La Pila de Protocolos Bluetooth.
Disponible en Internet:
<http://www.seguridadmobile.com/bluetooth/especificacion-bluetooth/arquitectura-de-protocolo/index.html>
Descripción: Articulo arquitectura de protocolos Bluetooth.

Descripción General del Funcionamiento.
Disponible en Internet:
<http://www.bluetooth.com/English/Technology/Works/Pages/Overview_of_Operation.aspx>
Descripción: Panorámica de las operaciones.

MORENO, Alberto. Elementos de Seguridad en Bluetooth.
Disponible en Internet:
<http://www.seguridadmobile.com/bluetooth/seguridad-bluetooth/elementos-de-seguridad.html>
Descripción: Articulo elementos de seguridad en Bluetooth.

TORRES, Roberto. 10 Ventajas de Bluetooth.
Disponible en Internet:
<http://www.articulos-espanoles.com/Article/10-Ventajas-de-Bluetooth/17>
Descripción: Ventajas tecnología Bluetooth.

Ventajas y desventajas de Bluetooth.
Disponible en Internet:
<http://junihh.wordpress.com/2007/06/02/ventajas-y-desventajas-de-bluetooth/>
Descripción: Ventajas y Desventajas tecnología Bluetooth.

MORENO, Alberto. Dispositivos Bluetooth.
Disponible en Internet:
<http://www.seguridadmobile.com/bluetooth/especificacion-bluetooth/dispositivos-bluetooth/index.html>
Descripción: Dispositivos de uso cotidiano que incorporan tecnología Bluetooth.

Product Directory.
Disponible en Internet:
<http://www.bluetooth.com/English/Products/Pages/Products.aspx>
Descripción: Directorio de Productos con tecnología Bluetooth.

Pancake. Bluetooth Hacking.
Disponible en Internet:
<http://www.kaslab.net/downloads/Telematicas_2006/Telematicas_2006-Bluetooth_Hacking-pancake.pdf>
Descripción: Presentación en diapositivas Bluetooth hacking.

MORENO, Alberto. Bluesnarf.
Disponible en Internet:
<http://www.seguridadmobile.com/bluetooth/seguridad-bluetooth/bluesnarf.html>
Descripción: Articulo ataque Bluesnarf.

MORENO, Alberto. Bluebug
Disponible en Internet:
<http://www.seguridadmobile.com/bluetooth/seguridad-bluetooth/bluebug.html>
Descripción: Articulo ataque Bluebug

MORENO, Alberto. HeloMoto.
Disponible en Internet:
<http://www.seguridadmobile.com/bluetooth/seguridad-bluetooth/helomoto.html>
Descripción: Articulo ataque HeloMoto.

MORENO, Alberto. Blueline.
Disponible en Internet:
<http://www.seguridadmobile.com/bluetooth/seguridad-bluetooth/blueline.html>
Descripción: Articulo ataque Blueline

MORENO, Alberto. BD_ADDR Spoofing.
Disponible en Internet:
<http://www.seguridadmobile.com/bluetooth/seguridad-bluetooth/blue-mac-spoofing.html>
Descripción: Articulo ataque BD_ADDR Spoofing.

La comunidad Dragónjar. Super Bluetooth Hack, Controla Teléfonos con Bluetooth Activado.
Disponible en Internet:
<http://www.dragonjar.us/super-bluetooth-hack-controla-telefonos-con-bluetooth-activado.xhtml>
Descripción: Breve reseña del software Super Bluetooth Hack.

Pocket Car Whisperer Attack.
Disponible enInternet:
<http://www.trucoswindows.net/conteni5id-57-SEGURIDAD-El-ataque-Pocket-Car-Whisperer.html>
Descripción: Articulo introducing new pocket car whisperer attack.

VIRUS Y CÓDIGO MALICIOSO

Microsoft Corporation, ¿Qué es un virus informático?
Disponible en Internet:
<http://www.microsoft.com/latam/protect/computer/basics/virus.mspx>
Descripción: Definición de virus informático.

OLDFIELD, Paul. Virus informáticos al descubierto, 2001, Sophos Plc

Michael F. Rogers, IDIA 612 Research Paper: Mobile Device Technology and Ergonomic Considerations Relevant to Wide Area Gaming, 2006

VARAS, Sofía, Virus para dispositivos móviles: ¿La próxima amenaza?
Disponible en Internet:
<http://www.mouse.cl/2004/rep/08/24/index.asp>
Descripción: Breve reseña virus cabir y mosquito.

GONZÁLEZ, Encarna. Detectado un nuevo virus en dispositivos con Symbian, Pc. World.
Disponible en Internet:
<http://www.idg.es/pcworldtech/Detectado_un_nuevo_virus_en_dispositivos_con_Symbi/doc64066-seguridad.htm>
Descripción: Informe virus denominado SymbOS/Beselo.A!worm.

GOSTEV, Alexander. 2007, Kaspersky Security Bulletin 2006: Mobile malware,
Disponible en Internet:
<http://www.viruslist.com/en/analysis?pubid=204791922#sit>
Descripción: Informe Kaspersky Security Bulletin 2006: Mobile malware.

GOSTEV, Alexander. Monthly Malware Statistics: october 2008,
Disponible en Internet:
<http://www.viruslist.com/en/analysis?pubid=204792039>
Descripción: Estadísticas mensuales de Malware: Octubre 2008.

ZHU, Cheng. Malware para móviles: amenazas y prevención.
Disponible en Internet:
<http://www.mcafee.com/us/local_content/white_papers/threat_center/wp_malware_r2_es.pdf>
Descripción: Artículo de McAfee. Malware para móviles: Amenazas y prevención

HYPPONEN, Mikko. Mobile Malware.
Disponible en Internet:
<http://www.cs.virginia.edu/~robins/Malware_Goes_Mobile.pdf>
Descripción: Artículo mobile malware.

Mobile Systems. Global Threat Center.
Disponible en Internet:
<http://threatcenter.smobilesystems.com/>
Descripción: Pagina con información referente a amenazas globales móviles.

RECOMENDACIONES DE SEGURIDAD – BUENAS PRACTICAS

Los diez mandamientos de la seguridad para los usuarios de teléfonos móvil.
Disponible en Internet:
<http://www.techweek.es/seguridad/informes/1006691004801/diez-mandamientos-seguridad-usuarios.1.html>
Descripción: Breve reseña de recomendaciones de seguridad para dispositivos móviles.

Recomendaciones de seguridad para proteger el teléfono celular.
Disponible en Internet:
<http://www.pac.com.ve/index.php?option=com_content&view=article&catid=67&Itemid=76&id=4813>
Descripción: Breve reseña de recomendaciones de seguridad para dispositivos móviles.

REBOLLAL, Eduardo López. JARAUTA SÁNCHEZ, Javier. Seguridad en Entornos Móviles Corporativos.
Disponible en Internet:
<http://www.sia.es/noticias/SIC79_082-088.pdf>
Descripción: Articulo de seguridad en entornos móviles corporativos y buenas prácticas.

Estudio sobre la situación de seguridad y buenas prácticas en dispositivos móviles y redes inalámbricas.
Disponible en Internet:
<http://www.inteco.es/Seguridad/Observatorio/Estudios_e_Informes/Estudios_e_Informes_1/estudio_redes>
Descripción: Estudio sobre la situación de seguridad y buenas prácticas en dispositivos móviles y redes inalámbricas.

Guía para proteger y usar de forma segura su móvil.
Disponible en Internet:
<http://www.inteco.es/Seguridad/Observatorio/manuales_es/GuiaManual_movil>
Descripción: Guía para proteger y usar de forma segura su móvil.

CARACCIOLO, Claudio. SALLIS, Ezequiel. Seguridad en Dispositivos Móviles; Smartphone- Pocket PC.
Disponible en Internet:
<http://www.root-secure.com/site/descargas.php>
Descripción: Ataques que se realizan sobre equipos como el BlackBerry, el iPhone y los PDA, y cómo se debe proteger a estos dispositivos.

Teléfonos inteligentes: ¿productivos pero riesgosos?
Disponible en Internet:
<http://www.kinkaya.com.ar/noticias/telefonos-inteligentes>
Descripción: Ataques que se realizan sobre equipos como el BlackBerry, el iPhone y los PDA, y cómo se debe proteger a estos dispositivos.

MORENO, Alberto. Recomendaciones de Seguridad.
Disponible en Internet:
<http://www.seguridadmobile.com/bluetooth/seguridad-bluetooth/recomendaciones.html>
Descripción: Recomendaciones de seguridad tecnología Bluetooth.

GENERAL

MILLS, Elinor. Using your smartphone safely (FAQ).
Disponible enInternet:
<http://news.cnet.com/8301-27080_3-10424759-245.html>
Descripción: Preguntas más frecuentes con relación a la seguridad en dispositivos móviles.

MOLINA, Fabián Alejandro. Seguridad en Aplicaciones Móviles.
Disponible en Internet:
<http://www.acis.org.co/fileadmin/Base_de_Conocimiento/VI_JornadaSeguridad/Fabian_Molina_VIJNSI.pdf>
Descripción: Presentación en diapositivas acerca de la Seguridad en Aplicaciones Móviles.