

Bluetooth-La Amenaza Azul

Introducción

El Estándar Bluetooth, nacido en 1994 y formalizado en 1998 por el Bluetooth-SIG (Special Interest Group), es una tecnología inalámbrica de bajo costo, que opera en la banda no licenciada de 2.4Ghz de frecuencia (misma banda que utilizan algunos estándares de la tecnología 802.11). Básicamente posee cuatro canales, tres canales sincrónicos de voz (64 Kbps por canal) y un canal de datos asincrónicos. La velocidad de transmisión de los canales asincrónicos es de 723,2 Kbps mientras que la del canal asincrónico es de 433,9 Kbps.

Existen hoy en día tres versiones de Bluetooth

- **Bluetooth Protocolo V1.1** No provee compatibilidad para coexistir con 802.11
- **Bluetooth Protocolo V1.2** (2003) Data Rate 1Mbps
- **Bluetooth Protocolo V2.0 +EDR** (Enhanced Data Rate) (2004) Data Rate 3Mbps

Uno de los hechos que hacen que esta tecnología sea de bajo costo, es la potencia necesaria para funcionar, tan sólo 0,1 Watts que sin duda alguna reduce considerablemente el consumo de los equipos y que además permite ser incorporada en los teléfonos celulares y las PDA sin que afecte en exceso el consumo de sus baterías.

La tecnología Bluetooth permite la comunicación inalámbrica, entre diferentes dispositivos que la incorporen sin necesidad de línea de vista y son el reemplazo esperado de la tecnología infrarroja. Sin embargo, la frecuencia que opera (2.4Ghz banda no licenciada), debió enfrentarse al temor elemental de cualquier comunicación inalámbrica, la interferencia, y a fin de superarla se implementaron las siguientes características:

- Frequency Hopping: Patrón de saltos predefinido
- Saltos de 1Mhz sobre 79 frecuencias diferentes entre 2.402 GHz y 2.480 GHz
- Saltos entre frecuencias más rápidos que en otras tecnologías inalámbricas (1600 Saltos por segundo)

Este punto a su vez incorpora, una medida importante desde el punto de vista de la seguridad, ya que para poder monitorear el tráfico de una comunicación debemos formar necesariamente parte de la misma, de lo contrario la única alternativa viable es la de adquirir costosos equipos que puedan monitorear tráfico, sin la necesidad de ser parte de la conexión, algo viable solo para unos pocos adinerados.

Bluetooth STACK

La pila del protocolo Bluetooth esta conformada de la siguiente manera:

Radio Layer	Es la capa mas baja, define las características de la transmisión, cada dispositivo esta clasificado en tres clases diferentes: <ul style="list-style-type: none">• Clase 1 100 Metros Aproximadamente• Clase 2 10 Metros Aproximadamente• Clase 3 1 Metro Aproximadamente
Baseband Layer	Es la capa física, provee corrección de errores y características de seguridad, a través de la encriptación de datos, también administra los saltos de frecuencia y los datos contenidos en el header del paquete
Link Manager Protocol (LMP)	Es el contenedor de aproximadamente 20 PDU Protocol Data Units, estas unidades son enviadas desde un dispositivo al otro, algunas de las mas utilizadas son: <ul style="list-style-type: none">• Power Control• Autenticacion• Calidad de Servicio (QOS)
Host Controller Interface	Envía comandos a las capas dos capas inferiores, permitiendo una vía para la utilización, de las bondades de Bluetooth
The Logical Link Control and Adaptation Protocol (L2CAP)	Controla el link entre dos dispositivos, y además es la encargada de proveer los servicios a los mismos
Cable Replacement Protocol (RFCOMM)	Es el protocolo de transporte, envía la señal montada sobre L2CAP
Service Discovery Protocol (SDP)	Busca otros dispositivos Bluetooth disponibles y tiene la provee la capacidad de establecer una conexión con los mismos, se comunica directamente con la capa de L2CAP

Redes

Cuando se conectan más de un dispositivo BT compartiendo un mismo canal,

de comunicación forman una red denominada Piconet. Dichas redes están compuestas por un dispositivo Master quien impone la frecuencia de saltos para la Piconet, y todos los demás dispositivos son los denominados Slaves (esclavos). Las Piconet solo pueden aceptar hasta 7 dispositivos Slaves

conectados al mismo tiempo, sin embargo, son soportados hasta 200 dispositivos pasivos.

Los dispositivos esclavos pueden a su vez estar interconectados a diferentes Piconet, formando lo que se denomina una Scatternet, pero esta característica no se aplica al dispositivo Master ya que el mismo solo puede estar en una Piconet.

Seguridad

Los dispositivos con Bluetooth tienen básicamente dos estados o modos posibles:

- **Modo Descubrimiento**
- **Modo No Descubrimiento**

Cabe mencionar que si algún dispositivo se encuentra en modo No Descubrimiento, igualmente puede ser mapeado siempre y cuando el atacante conozca la Mac Address (BD_ADDR)

Básicamente los modelos de Seguridad de los dispositivos Bluetooth se clasifican en tres modos primarios:

Modo 1: Sin seguridad (Modo Default)

Esencialmente, los mecanismos de autenticación y cifrado están deshabilitados

Modo 2: Aplicación/ Nivel Servicio

Ocurre en la capa L2CAP, nivel de servicios. Primero se establece un canal entre el nivel LM y el de L2CAP y recién entonces se inicializan los parámetros de seguridad. Como característica, el acceso a servicios y dispositivos es controlado por un Gestor de Seguridad por lo cual variando las políticas de seguridad y los niveles de confianza se pueden gestionar los accesos de aplicaciones con diferentes requerimientos de seguridad que operen en paralelo. Otra característica importante de este modo es que no hay ninguna codificación adicional de PIN o claves.

Modo 3: Autenticación vía PIN/ Seguridad a nivel MAC/ Encriptación








Ocurre a nivel de Link y todas las rutinas se corren internamente en el chip BlueTooth por lo que nada se transmite en texto plano. A diferencia del Modo 2, los procedimientos de seguridad se inician antes de establecer algún canal y el cifrado se basa en la autenticación PIN y seguridad MAC. Básicamente, comparte una clave de enlace (clave de link) secreta entre dos dispositivos. Para generar esta clave, se usa un procedimiento de “paring” cuando los dos dispositivos se comunican por primera vez

Proceso de Paring

Para comprender el proceso de Paring o Emparejamiento, debemos aclarar que por default, la comunicación Bluetooth no se valida, de manera tal que cualquier dispositivo puede o podría hablar con cualquier otro. Un dispositivo Bluetooth se autentifica con otro si por requiere utilizar un determinado servicio (por ejemplo para el servicio de marcación por modem). Como ya mencionamos, la forma de autenticarse es mediante códigos PIN (cadena ASCII de hasta 16 caracteres de longitud). Tanto el usuario del dispositivo cliente como así también el proveedor del servicio, debe introducir el código PIN, obviamente, en ambos dispositivos el código ingresado debe ser exactamente el mismo. Al finalizar este proceso correctamente, ambos dispositivos generan una clave de enlace la cual se puede almacenar en el propio dispositivo o en un dispositivo de almacenamiento externo. Dicha clave será utilizada la siguiente vez que se comuniquen ambos dispositivos sin la necesidad de la intervención de los usuarios para que coloquen nuevamente sus contraseñas. Si alguno de los dos dispositivos pierde la clave, se debe a realizar todo el proceso nuevamente. Todo este proceso es conocido como emparejamiento o Paring.

Riesgos y Ataques en la tecnología Bluetooth

Es muy común encontrarse en los archivos almacenados en las PDA y en los Celulares, los usuarios y las contraseñas de las PC y hasta de los servidores que para no dejarlos anotados en un papel lo anotan en sus dispositivos móviles. Los lugares de mayor riesgo o donde es fácilmente posible obtener información como la mencionada anteriormente es en lugares públicos como por ejemplo:

-  En el cine
-  En una plaza con mucha gente
-  En una biblioteca
-  En un centro comercial o en un bar
-  En un campo de fútbol
-  En alguna tienda de telefonía
-  En el tren - autobús

Según estadísticas los usuarios suelen utilizar los dispositivos como pda o celulares para lo siguiente:

- 85% utiliza estos dispositivos para almacenar el día a día del negocio
- 85% Las utiliza para almacenar contactos y direcciones relacionadas con el negocio
- 33% Las utiliza para almacenar PINs y Passwords
- 32% Para recibir y enviar correo
- 25% Para llevar el detalle de sus cuentas bancarias
- 25% Para almacenar información corporativa

- **Fuente: Pointsec Mobile Technologies**

Como podemos ver la información comprometida, puede o no ser de carácter corporativo, pero puede brindar al atacante de obtener datos que permitan desarrollar luego una estrategia de ataque mas efectiva.

Desde principios de 2003, comenzaron a hacerse publicas, algunas debilidades y vulnerabilidades que afectaban directamente a esta tecnología.

La primera de ellas, fue descubierta por la gente de Atstake, y fue denominada War Nibling, y permite descubrir en a todos los dispositivos que esten en el alcance del atacante esten estos en modo descubrimiento o no.

Después y de la mano de Adam Laurie y la gente del grupo Trifinite, fueron descubiertas las siguientes técnicas:

BluePrinting



Es una técnica de Fingerprinting pero de dispositivos Bluetooth, permite saber

Fabricante del dispositivo

Modelo del dispositivo (Solo algunas veces)

Se basa en la dirección Mac Address del dispositivo, esta compuesta por 6 bytes, los primeros 3 indican el fabricante y los restantes el modelo

Las herramientas para estos ataques buscan dispositivos que se encuentren en Modo Descubrimiento, toma las direcciones Mac, y la compara contra la base de firmas que posee determinando así el Fabricante del dispositivo y su modelo (ver tabla ejemplo en el Anexo 1 "BluePrint Device Hashes"). Para el caso de los dispositivos que no se encuentren en Modo Descubrimiento, existen herramientas que se basan en ataques de Brute Force.

BlueBug



Es una vulnerabilidad que fue encontrada en varios teléfonos celulares con interfaz Bluetooth

Permite enviar comandos AT al celular, a través de un canal encubierto de la tecnología Bluetooth, permitiendo al atacante:

- Extraer del celular la agenda telefónica y calendario entre otros
- Modificar o Borrar entradas en el calendario, o en los contactos telefónicos
- Enviar un mensaje SMS desde el celular comprometido

- Provocar que el celular comprometido, realice llamadas telefónicas a los números que el atacante desee

BlueSnarfing y Long Distance Snarf



Este es el ataque que se aprovecha del bluebug, y básicamente permite, extraer información de un celular, en vez de colocarla, varios equipos son vulnerables a este ataque (Nokia 6310,6310i y varios otros).

En agosto de 2004, lograron llevar mas allá los limites de alcance de un dispositivo clase uno, logrando extraer y modificar la agenda telefónica y el calendario de un teléfono celular a una distancia de 1,78 Km. Utilizando una Laptop bajo Linux (Con todas las librerías de Bluetooth), con un adaptador USB Bluetooth modificado (Clase 1) y una antena direccional cuyo objetivo era un Celular Nokia 6310 Dispositivo (Clase 2)

BlueSmack



Es un ataque de Denegación de servicio que aprovecha las debilidades en la implementación de Bluetooth, mas puntualmente en L2CAP. Permite mal formar un requerimiento causando que el dispositivo se cuelgue o se reinicie sin necesidad de establecer un conexión previa.

Es similar al conocido ping de la muerte, l2ping es una funcionalidad que esta presente en las librerías Bluez, de Linux, y permiten a una atacante a especificar el tamaño del paquete a enviar

BlueBump



Su fin es robar la link-key del teléfono de la victima, para establecer posteriores conexiones, sin que esta lo note y aparentando ser un dispositivo confiable. Este tipo de ataque incorpora técnicas de Ingeniería social pero fundamentalmente se basa en el beneficio de poder regenerar la link-key mientras la conexión esta establecida (Ver mas en **Cracking BT PIN y la reciente herramienta BTCrack**)

Hello Moto



Es una debilidad en exclusiva de algunos dispositivos Motorola.

La debilidad radica en una mala implementacion de la relacion de confianza que se establece en el proceso de paring.

Permite establecer la relacion de confianza, entre el dispositivo del atacante y la victima, si este primero intenta establecer una conexion al OPP (Obex Push Profile) y luego la cancela, el dispositivo del atacante sera agregado a la lista de dispositivos confiable de la victima.

Todo esto sucede sin que medie ninguna interaccion por parte de la victima

BlueSpam



Es un ataque basado en la búsqueda de dispositivos en Modo Descubrimiento, a los cuales luego les enviará mensajes arbitrarios creados por el atacante. Este tipo de ataques no requiere la interacción por parte de la víctima para recibir el spam

BlueJacking



Es el ataque quizás más inofensivo pero desde el cual se han sentado muchas bases para nuevos ataques. Consiste en conectarse a un dispositivo Bluetooth y colocarle imágenes, mensajes o contactos al dueño del dispositivo. También es utilizado para realizar ingeniería social y utilizarla en complemento con otro tipo de ataques que requieran que los equipos estén aparejados.

Cracking BT PIN y la reciente herramienta BTCrack (www.enruns.com)



Tal cual sucedió, con WEP en 802.11, la implementación de los algoritmos de encriptación y seguridad sobre bluetooth, poseen importantes debilidades.

En el caso de Bluetooth, este contiene varios elementos, como el management de llaves de encriptación y autenticación basada en un PIN los cuales son utilizados en el proceso de Paring y la utilización de estos reside en la decisión del usuario. El algoritmo que brinda seguridad a estas tecnologías es SAFER+, este es un algoritmo simétrico de encriptación por bloque, que permite la utilización de llaves de 128, 192 y 256, para el caso el algoritmo utilizado es Safer+ de 128bits.

Haciendo un poco de historia acerca de las investigaciones llevadas a cabo sobre este aspecto, en el 2003 Ollie Whitehouse comenzó a hablar de algunas debilidades en el proceso de paring que podrían permitir romper el PIN, mas adelante algunos investigadores, hicieron mejoras sobre esta técnica y encontraron la manera de forzar a un dispositivo a que reinicie el proceso de paring, por ultimo en el 2006 Thierry Zoller llevo a cabo la implementación de una herramienta para Win32 que llevaria todo lo anterior a la practica (BTCrack) y además realizo otra propuesta diferente a la de Shaked y Wool, para forzar el proceso de re-emparejamiento.

Para poner esto en palabras simples, alguna de las cosas que podrían suceder seria la siguiente:

Escenario:

Dos dispositivos, Un Master y un Slave, realizar exitosamente el proceso de emparejamiento, autenticando esto mediante un PIN.

Primer Paso:

El atacante debería en primer lugar conocer las direcciones MAC de ambos dispositivos, esto no sería un problema para el atacante ya que como se menciono mas arriba existen técnicas y herramientas disponibles.

Segundo Paso:

El atacante debería modificar la dirección MAC de su dispositivo por la del dispositivo Slave

Tercer Paso:

El atacante ahora debería intentar iniciar con el Master el proceso de paring, al mismo tiempo este debería estar monitoreando y capturando la información transmitida.

Cuarto Paso:

Tomar el output de la información capturada, durante el proceso de emparejamiento y dárselo como input al BTcrack, debido a las debilidades arriba mencionadas, la herramienta se encargara rápidamente de informarle al atacante cual es el PIN

En base a los estudio realizados por Thierry Zoller en un equipo Dual-Core P4 de 2Ghz, el tiempo que le llevaria a la herramienta romper el PIN es:

PIN de 4 Digtos: 0.035 Segundos

PIN de 5 Digtos: 0.108 Segundos

PIN de 6 Digtos 4.321 Segundos

PIN de 9 Digtos 1318 Segundos

Es por esto que entre otras recomendaciones el SIG recomienda realizar el proceso de emparejamiento en un lugar "seguro"

Algunas Herramientas

Btbrowser:

<http://www.benhui.net/bluetooth/btbrowser.html>

- Permite descubrir dispositivos BT
- Permite conocer las especificaciones tecnicas de los mismos
- Permite Ver los servicios disponibles por esta
- Aplicacion en Java soportada por varios telefonos celulares

Bthdisc:

www.trifinite.org

- Permite descubrir dispositivos BT
- Informa Clase y Direccion Mac Address

Bt_Audit: Scanner con dos funcionalidades

<http://www.betaversion.net/btdsd/>

- Scanner para la L2CAP
- Scanner RFCOMM

Plataforma Operativa : Linux

Sniffing Local

- Hcidump

Piconet Sniffing

- Hardware o firmware especial

Air Sniffing

- Frontline (<http://www.fte.com/>)
- LeCroy/CatC (<http://www.lecroy>)

Herramienta de auditoria para telefonos celulares - BLOOVER

Actualmente por la version 2, es un aplicacion realizada en java, que permite realizar, el ataque de Bluesnarf, directamente desde un celular, con tecnologia Bluetooth y soporte para aplicaciones Java J2ME MIDP 2.0 VM y JSR-Bluetooth API (Download:http://trifinite.org/trifinite_downloads.html)

Funcionalidades:

Permite modificar y leer entradas en la agenda telefonica

Permite leer los mensajes de texto, almacenados en el telefono

Permite setear en el celular comprometido, un numero telefonico para el redireccionamiento de llamadas!!!!!!

Ejecutar el Hello Moto Attack

Ejecutar Bluejacking

Enviar Objetos malformados a traves de OBEX

BTCrack www.enruns.com

Herramienta recientemente presentada el Hack.Lu 2006

Permite romper Claves y Llaves de enlace (PIN y Link Key)

Previamente requiere como entrada, los datos sniffeados durante el proceso de paring

Algunas Debilidades Generales

- El usuario suele relacionar el concepto de PIN con una cadena de caracteres corta (4), la tecnología lo permite
- Los ataques de ingeniería social, pueden preceder a los ataques antes decriptos y facilitar aun mas la tarea del atacante

Ej: Nombre del Dispositivo "Para continuar ingrese 1234"

- El algoritmo utilizado para brindar seguridad es Simétrico (misma clave para encriptar que para desencriptar) y no existe un canal seguro de transmisión,, el problema se potenciaría en implementaciones grandes de BT.
- NO existe autenticación de Usuarios
- NO existen límites para el reintento de ingreso de claves
- SIN paring previo algunos servicios e información son visibles
- Covert Channels
- Errores de Programación e Implementación

Conclusión:

Las nuevas tecnologías, traen asociadas cientos de riesgos y amenazas para las que muchas veces las empresas, no están preparadas, y lo que es peor, a veces ni siquiera están preparadas

Muchas corporaciones, dan a sus directivos estos dispositivos, sin tener en cuenta los riesgos asociados a los que se expone la información contenida en ellos, es por esto que hay que crear la conciencia necesaria y tomar medidas que permitan mitigar los riesgos asociados.

La creatividad, es una de las herramientas de ataque, contra la que muy pocos desarrollan contramedidas

Referencias:

- www.bluetooth.org
- www.trifinite.org
- www.nruns.com
- <http://gospel.endorasoft.es>
- <http://student.vub.ac.be/~sijansse/2e%20lic/BT/Tools/Tools.pdf>

**Ezequiel M Sallis CISSP/CEH/CCNA/NSP
Senior Security Specialist
Root-Secure Director**