Bluetooth-La Amenaza Azul

Ezequiel M Sallis CISSP/CCNA/NSP
Senior Security Specialist
Root-Secure
http://www.root-secure.com.ar/

Introducción

El Estándar Bluetooth, nacido en 1994 y formalizado en 1998, es una tecnología inalámbrica de bajo costo, que opera en la banda no licenciada de 2.4Ghz de frecuencia (misma banda que utiliza la tecnología 802.11). Básicamente posee cuatro canales, 3 canales sincrónicos de voz (64 Kbps por canal) y 1 canal de datos asincrónico. La velocidad de transmisión de los canales asincrónicos es de 723,2 Kbps mientras que la del canal asincrónico es de 433,9 Kbps.
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 sin duda alguna permitió incorporarla a los teléfonos celulares y las PDA sin que afecte en exceso el consumo de sus baterías.
El Bluetooth permite la comunicación inalámbrica, entre diferentes dispositivos pero que posean la misma tecnología. Sin embargo, en la frecuencia que opera (en la 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 Hoping: 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)

El protocolo BT esta basado en el siguiente Stack:

Radio Layer	Es la capa mas baja, define las características de la transmisión, cada dispositivo esta clasificado en tres clases diferentes: • Clase 1 (hasta 10 centimetros) •Clase 2 (hasta 10 metros) •Clase 3 (hasta 100 metros)
Baseband Layer	Es la capa física, provee corrección de errores y características de seguridad, a través de la encripción 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: •Power Control •Autenticacion •Calidad de Sevicio (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

Hasta 7 dispositivos esclavos activos son admitidos en una Piconet pero 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 deshabilidatos

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/ Encripción

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.

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 autentificarse 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.

Información Comprometida y Lugares de Uso Riesgoso

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

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, que permite

detectar básicamente

Fabricante del dispositivo

Modelo del dispositivo

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

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

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 victima 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

Tal cual sucede, en 802.11, la implementación de los algoritmos de encripción y seguridad, poseen importantes debilidades. En el caso de Bluetooth, este contiene varios elementos, como el management de llaves de encripción 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 encripción por bloque, que permite la utilización de llaves de 128, 192 y 256, para el caso el algoritmo utilizado es Safer+ de 128bits.
Entonces, un atacante podría, interceptar el PIN durante el proceso de paring de dos dispositivos, para luego poder monitorear toda la conversación
El proceso de Cracking de PIN demora 0,06 Milésimas de segundo en un Pentiun IV 3Ghz (PIN 4 Dígitos)

Conclusión:

Las nuevas tecnologías, traen asociadas cientos de riesgos y amenazas para las que muchas veces las empresas, no esta 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

Ezequiel M Sallis CISSP/CCNA/NSP
Senior Security Specialist
Root-Secure
http://www.root-secure.com.ar/