Taller Seguridad Informática - MSI 2010. Cátedra de Seguridad Informática, Ciudad Autónoma de Buenos Aires, 2010.

Mecanismos de Seguridad en la Transferencia de infomación con dispositivos Bluetooth.

Diego Sebastian Escobar, Diana Patricia Sarmiento Arango, Germán Villota Narváez y Jacobo Zambrano Barón.

MECANISMOS DE SEGURIDAD EN LA TRANSFERENCIA DE INFORMACIÓN CON DISPOSITIVOS BLUETOOTH

Seguridad en Redes I

Integrantes:

Diego Sebastián Escobar

Diana Patricia Sarmiento Arango

Germán Villota Narváez

Jacobo Zambrano Barón

Presentado a:

Ing. Hugo Pagola

Ing. Juan Manuel Caracoche

Maestría en Seguridad Informática

Universidad de Buenos Aires - UBA

Mayo de 2010

Buenos Aires, Argentina

TABLA DE CONTENIDO

1. INTRODUCCIÓN

Bluetooth es una tecnología de interconexión para la transmisión de datos que usa enlaces por radiofrecuencia y está orientado a cubrir distancias cortas, tiene como principal objetivo suprimir los cables de interconexión entre los dispositivos que la incorporan, a la hora de interactuar entre modelos y fabricantes diferentes, así como también difundir una tecnología de bajo costo que se pueda incluir en los aparatos sin influir significativamente en su costo.

En la actualidad, con más frecuencia se encuentran dispositivos que integran dicha tecnología por la facilidad y comodidad que implica una comunicación sin cables y de un costo relativamente bajo, es por esto que se puede considerar un hecho natural que la masificación de Bluetooth atraiga la atención para ser vulnerado y que sea necesario que la información transmitida entre los diferentes dispositivos posean un mínimo nivel de seguridad.

En el presente documento se muestra un bosquejo general de la tecnología Bluetooth, pasando brevemente por las etapas que ha ido superando este estándar en su proceso de desarrollo, hasta llegar al modo de operación que se tomará como punto de partida para el análisis, buscando responder a las preguntas ¿Qué tan seguro es el uso de esta tecnología? ¿Qué mecanismos de seguridad implementa actualmente? ¿Se puede mejorar el nivel de la seguridad? ¿A qué vulnerabilidades está expuesto y qué tan crítico puede llegar a ser un punto débil en la seguridad?

2. BLUETOOTH

2.1 Conceptos básicos

El nombre viene de Harald Bluetooth, un Vikingo y rey de Dinamarca del 940 al 981 que fue reconocido por su capacidad de ayudar a la gente a comunicarse, y que durante su reinado unió Dinamarca y Noruega. La idea de utilizar su nombre nació en 1994 cuando la compañía Ericsson se propuso crear una interface de bajo poder y bajo costo que permitiera la comunicación entre un teléfono móvil y sus accesorios (audífonos), esta idea creció y en 1998 se creó el SIG (Special Interest Group), conformado por compañías como 3Com, Ericsson, IBM, Intel, Microsoft, Motorola, Nokia, Toshiba y cientos de compañías asociadas.

Fue diseñado para ser seguro, económico y fácil de usar desde el primer uso, fue introducido en el año 1999 y desde entonces se ha hecho día a día más popular, elimina cables de comunicación entre equipos móviles y fijos, facilita las transmisiones de Voz y Datos, permite crear redes "ad-hoc"[1] y ofrece lo último en sincronismo entre todos los accesorios personales.

Dado que la tecnología inalámbrica es una plataforma abierta, todos los miembros del SIG tienen permiso para utilizar la tecnología Bluetooth en sus productos y servicios, existen tres niveles de membrecía: Promotor, Asociado e Incorporador.

- **Promotor:** Los miembros promotores son aquellas compañías que hacen parte del SIG, que fueron mencionadas anteriormente. Adicionalmente a tener asiento en la Mesa Directiva, los miembros Promotores también tienen asiento en BQRB (Bluetooth

1 Una red ad hoc es aquella (especialmente inalámbrica) en la que no hay un nodo central, sino que todos los dispositivos están en igualdad de condiciones. (http://es.wikipedia.org/wiki/Ad_hoc)

Qualification Review Board) y dedican personal a los comités y grupos de trabajo que guían el desarrollo y promoción de la tecnología.

- **Asociado:** No obstante que todos los miembros pueden utilizar las especificaciones publicadas y los registros de licencias de Bluetooth, los miembros asociados tiene la posibilidad de trabajar con otros miembros asociados y/o compañías Promotoras para la revisión de las especificaciones antes de su publicación. Los Miembros Asociados deben pagar una matrícula anual.

- **Incorporador:** Los miembros Incorporadores de Bluetooth SIG pueden utilizar las especificaciones publicadas de la tecnología Inalámbrica Bluetooth y utilizar las patentes de Bluetooth SIG, pero no tienen la oportunidad de influenciar o tener acceso temprano a la tecnología sin publicar. La participación como miembro incorporador es libre de costo.

2.2 Características de la tecnología

El estándar se divide en las siguientes normas:

- **IEEE 802.15.1** define Bluetooth 1.x, que puede alcanzar velocidades de 1 Mbps.

- **IEEE 802.15.2** recomienda prácticas para utilizar la banda de frecuencia de 2.4 GHz (la frecuencia también utilizada por WiFi).

- **IEEE 802.15.3** es un estándar que actualmente se está desarrollando, que ofrecerá velocidad de banda ancha (20 Mbps) con Bluetooth.

- **IEEE 802.15.4** es un estándar que actualmente se está desarrollando para el uso con aplicaciones Bluetooth de baja velocidad.

Los dispositivos se clasifican como Clase I, Clase II o Clase III en referencia a su potencia de transmisión, la cual define el alcance que pueden llegar a tener las transmisiones, siendo totalmente compatibles los dispositivos de una clase con los de las otras.

CLASE	POTENCIA (Perdida de señal)	ALCANCE
I	100 mW (20 dBm)	100 metros
II	2,5 mW (4 dBm)	15-20 metros
III	1 mW (0 dBm)	10 metros

Tabla 1. Potencia vs Alcance

En la mayoría de los casos, la cobertura efectiva de un dispositivo de Clase II se extiende cuando se conecta a un transceptor de Clase I, esto es así gracias a la mayor sensibilidad y potencia de transmisión del dispositivo de Clase I, es decir, la mayor potencia de transmisión del dispositivo de Clase I permite que la señal llegue con energía suficiente hasta el de Clase II, y por otra parte la mayor sensibilidad del dispositivo de Clase I permite recibir la señal del otro pese a ser más débil.

2.3 Modo general de operación para Transmisión y Recepción

Bluetooth define un canal de comunicación de máximo 720 Kb/segundo (1 Mbps de capacidad bruta) con rango óptimo de 10mts (opcionalmente 100mts con repetidores), todos aquellos accesorios que se comunican mediante la Tecnología Bluetooth corren el riesgo de encontrar interferencia en la banda que están transmitiendo, las redes inalámbricas y otras aplicaciones basadas en la IEEE 802.11 (WLAN) pueden tener conflicto con Bluetooth, los accesorios que operan en la banda libre de 2.4 Ghz ISM (Industrial, Científico y Medico) pueden tener conflicto también.

La frecuencia de radio con la que trabaja está en el rango de 2,4 a 2,48 GHz con amplio espectro y saltos de frecuencia con posibilidad de transmitir en Full Dúplex con un máximo de 1600 saltos/segundo. Los saltos de frecuencia se dan entre un total de 79 frecuencias con intervalos de 1Mhz; esto permite dar seguridad y robustez.

Cuando otro dispositivo Bluetooth o una red inalámbrica (WLAN) entran en el ambiente de

trabajo, se presentan interferencias, pues las WLAN trabajan dentro de este rango en unas frecuencias más bajas.

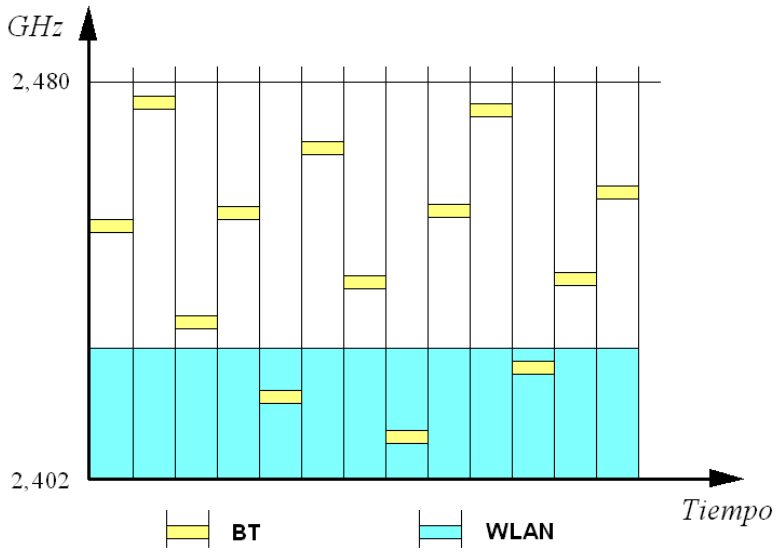


Figura 1. Interferencia de Bluetooth con WLAN

Por lo tanto se creó AFH (Adaptative, Frecuency, Hopping) que permite a Bluetooth adaptarse al ambiente, identificando aquellas fuentes fijas de interferencia y excluyéndolas de su lista de canales disponibles. A continuación se muestra como se seleccionan los canales utilizados por otras fuentes y no los utiliza para su transmisión.

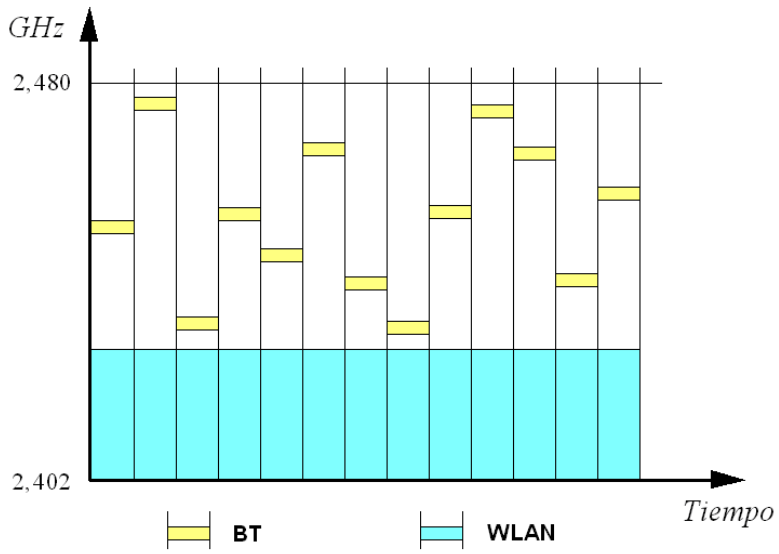


Figura 2. Operación de Bluetooth con AFH

La potencia de salida para transmitir a una distancia máxima de 10 metros es de 0 dBm (1 mW), mientras que la versión de largo alcance transmite entre 20 y 30 dBm (entre 100 mW y 1 W). Para lograr alcanzar el objetivo se ideó entonces una solución de bajo consumo y bajo costo que se puede implementar en un solo chip utilizando circuitos CMOS. De esta manera, se logró crear una solución de 9×9mm y que consume aproximadamente 97% menos energía que un teléfono celular común.

Figura 3. Topología punto a punto

El protocolo de banda base combina conmutación de circuitos y paquetes lo cual asegura que los paquetes no lleguen fuera de orden, los slots pueden ser reservados por paquetes síncronos, un salto diferente de señal es usado para cada paquete. La conmutación de circuitos puede ser asíncrona o síncrona, tres canales de datos síncronos (voz), o un canal de datos síncrono y uno asíncrono, pueden ser soportados en un solo canal, cada canal de voz puede soportar una tasa de transferencia de 64 Kb/segundo en cada sentido, la cual es suficientemente adecuada para la transmisión de voz. Un canal asíncrono puede transmitir como máximo 721 Kb/segundo en una dirección y 56 Kb/segundo en la dirección opuesta y para una conexión síncrona es posible soportar 432,6 Kb/segundo en ambas direcciones si el enlace es simétrico.

Topologías de Red

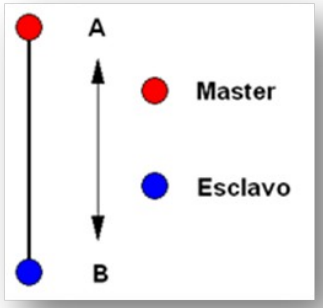
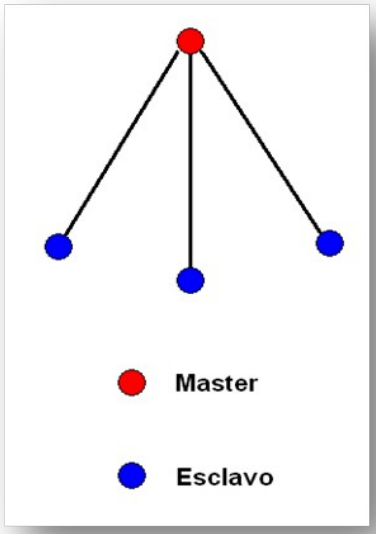


Figura 4. Topología punto a

- ***Punto a Punto:***

  El Maestro (A), envía una consulta y otro usuario, el Esclavo (B), contesta.

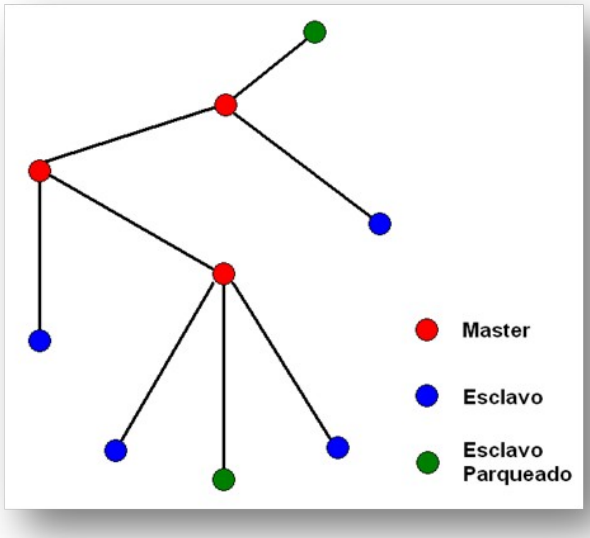
  El Maestro puede cambiar de lado. Siempre quien hace la consulta es el maestro.



- ***Punto a Multipunto:***

  Un Maestro (A) puede llegar a tener hasta
  7 Esclavos activos.

  Un Maestro (A) puede llegar a tener hasta 255 esclavos conectados, pero poniendo en espera aquellos que no generan consultas.



Scatternet

El Maestro (A) de una Red de área personal (PAN) puede ser esclavo en otra PAN.

Los Esclavos (B) pueden participar en diferentes PAN.

2.4 Protocolos utilizados

La pila de protocolos Bluetooth está constituida de varias capas entre las cuales, a excepción de las capas más bajas, existen protocolos que permiten su interacción.

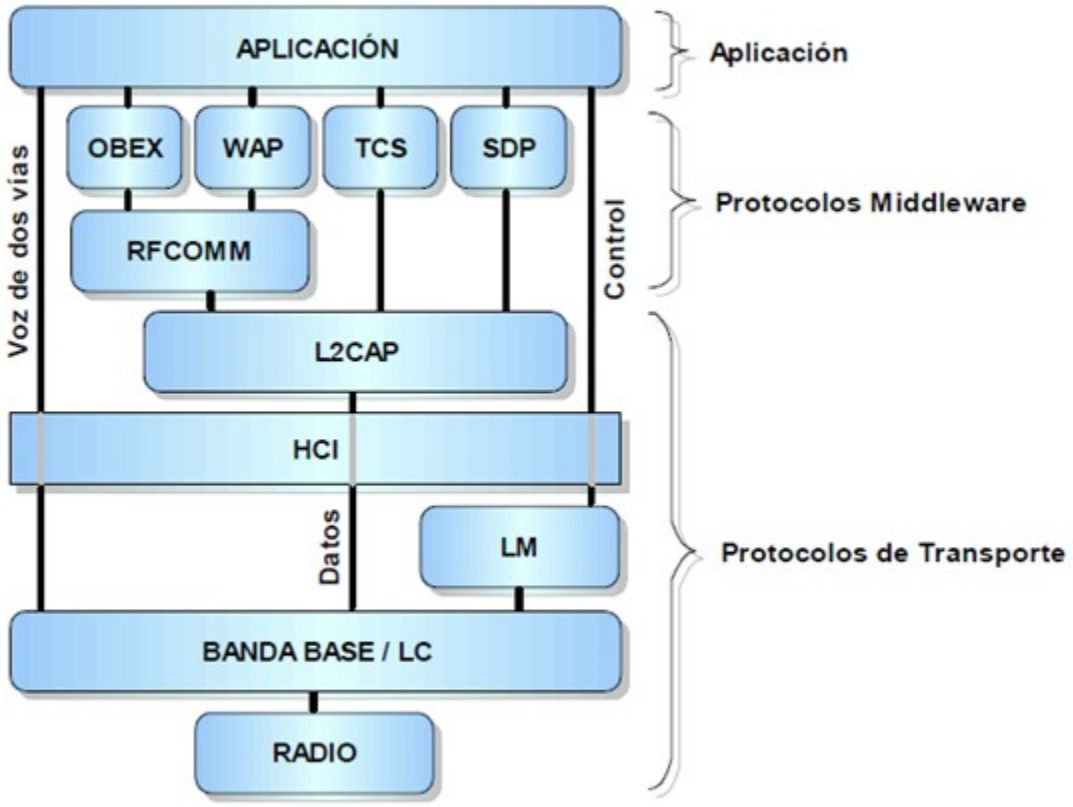


Figura 6. Capa de protocolos Bluetooth

- **Protocolos de Transporte**

  Permiten la búsqueda de dispositivos Bluetooth, el manejo y la configuración de enlaces lógicos y físicos que conforman un “canal virtual” por la cual fluyen los datos desde y hacia las capas más altas. En la pila Bluetooth, los protocolos de transporte son indispensables para cualquier aplicación y en su mayoría pueden ser implementados tanto en hardware como firmware. Las capas que conforman este grupo son: radio, banda base y controlador de enlace (LC), manejador de enlace (LM), interfaz controlador de host (HCI) y protocolo de adaptación y control de enlace lógico (L2CAP).

- **Protocolos de Middleware**

  Los protocolos de capa media (middleware), presentan interfaces estándar para el flujo de datos desde el grupo de transporte hacia la capa de aplicación. En términos sencillos, funcionan como protocolos intermediarios. Estos incluyen: RFCOMM, OBEX, WAP (al igual que TCP, IP y PPP), TCS y SDP.

- **Aplicación**

  El grupo de aplicación se refiere a software tal como lo define la SIG y es suministrado por el fabricante del aparato o vendido por desarrolladores independientes, son programas que se acompañan con la pila del protocolo Bluetooth para obtener beneficios del aparato. En caso de aplicaciones existentes, o legado, que no traen soporte Bluetooth, posiblemente requieran de software adicional de adaptación.

  Para una aplicación determinada, no es necesario utilizar todas las capas de la pila, la especificación de perfiles indica que capas en particular se deben implementar y de qué manera según la aplicación.

Los datos en la pila fluyen a través de todas las capas a excepción de la información de audio, que va directamente desde la banda base hacia la aplicación con alto grado de prioridad para garantizar la calidad de servicio en tiempo real esperado por aplicaciones de audio.

3. SEGURIDAD EN BLUETOOTH

3.1 Modos de seguridad

Los dispositivos con Bluetooth tienen básicamente dos estados posibles:

- Estado Descubrimiento
- Estado Descubrimiento

Cabe mencionar que si algún dispositivo se encuentra en estado No Descubrimiento, igualmente puede ser mapeado siempre y cuando el atacante conozca la dirección Mac (BD_ADDR) del mismo.

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/ Encripción**

  Ocurre a nivel de enlace 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[3.2] cuando los dos dispositivos se comunican por primera vez.

La nueva versión de Bluetooth v2.1+EDR aumenta los niveles de seguridad en escenarios de emparejamiento en los cuales interviene el usuario, la protección contra intrusos hace que una simple clave de acceso de 6 dígitos, sea más fuerte que una clave de 16 caracteres alfanuméricos. También ofrece protección contra el ataque conocido como “Man in the middle” reduciendo la posibilidad de que un intruso intercepto información son ser detectado.

3.2 Generación de claves

Como se mencionó anteriormente, la generación de la clave de enlace utilizada en el Modo3, se realiza mediante un proceso de Paring o Emparejamiento, para comprender este proceso, debemos aclarar que por defecto, 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 solo si requiere utilizar un determinado servicio (por ejemplo para el servicio de marcación por modem), y la forma de hacerlo es mediante códigos PIN[2]. Tanto el usuario del dispositivo cliente como así también el proveedor del servicio, debe introducir el código PIN, 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

2 Cadena ASCII de hasta 16 caracteres de longitud

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.

3.3. Vulnerabilidades

En Noviembre de 2003 Adam Laurie, descubrió que había serios defectos en los mecanismos de autenticación y transferencia de datos en algunos dispositivos con Bluetooth habilitado. Entre otras cuestiones, las tres vulnerabilidades más importantes encontradas fueron:

- Posibilidad de acceso al contenido completo de la memoria de algunos teléfonos desde un dispositivo “de confianza”, aunque este hubiese sido borrado ya de la lista de teléfonos “de confianza”. Estos datos no solo incluían la agenda y el calendario, sino también archivos multimedia como imágenes y sms.
- Se podían obtener datos confidenciales de algunos teléfonos con Bluetooth habilitado de forma anónima y sin el conocimiento ni consentimiento del propietario. Estos datos incluían, al menos, toda la agenda e IMEI del celular.
- Se podría conseguir acceso al conjunto de comandos AT del dispositivo, consiguiendo llegar a los comandos y canales de más alto nivel, como datos, voz y mensajería.

A continuación se detallarán algunos de los ataques demostrados atacando las vulnerabilidades enunciadas:

- **Blueprinting**

  Blueprinting es un método para descubrir remotamente detalles acerca de dispositivos con Bluetooth habilitado; puede ser usado para generar estadísticas acerca de

fabricantes y modelos, y para descubrir si hay o no dispositivos en un rango que tengan problemas de seguridad con Bluetooth.

Como se indicó anteriormente, la dirección MAC tiene algunas características que la hacen única, especifican el fabricante y el modelo. Esta dirección puede ser también interpretada como la dirección hardware que es codificada en el chipset del dispositivo. Blueprinting combina la información que revela un dispositivo Bluetooth para determinar el modelo y el fabricante.

- **Bluesnarfing**

Es posible, en dispositivos de ciertas marcas, conectar con dicho dispositivo sin alertar al propietario, consiguiendo acceso a partes restringidas de los datos almacenados, incluyendo la agenda en su totalidad (y cualquier imagen u otros datos que vayan asociados con las entradas de la misma), calendario, reloj, propiedades, registro de cambio, IMEI...

Algunos modelos de teléfonos móviles en los que ha sido encontrada esta vulnerabilidad son los siguientes[3]:

- Nokia 6310i
- Nokia 8910i
- Ericsson T39
- Ericsson R520
- Ericcson T68
- Sony Ericsson T68i
- Sony Ericsson T610
- Sony Ericsson T630
- Sony Ericsson Z600

3 Fuente: Facultad de Informática - Universidad Complutense de Madrid

- **Bluesmack**

  BlueSmack es un ataque por el puerto Bluetooth que deja inoperativos de forma inmediata algunos dispositivos que disponen de dicho puerto. Este ataque de denegación de servicios puede ser realizado usando herramientas estándar del paquete de utilidades de BlueZ para Linux.

  El “Ping de la muerte” es básicamente un mensaje de ping que afectaba a las primeras versiones de Microsoft Windows 95. El BlueSmack es el mismo tipo de ataque, pero trasladado a Bluetooth. En la capa L2CAP existe la posibilidad de solicitar un eco desde otro terminal con Bluetooth. Al igual que con el ping ICMP, la idea del ping L2CAP (solicitud de eco) es también comprobar la conectividad y tantear el tiempo de vuelta en el enlace establecido.

- **Backdoor**

  El ataque por Backdoor implica establecer una relación de confianza entre dos dispositivos, pero asegurando que ésta no continuará apareciendo en el registro del dispositivo objetivo una vez finalice al ataque. De esta forma, a menos que el propietario del terminal objetivo lo esté observando en el momento justo en que se establezca la conexión, éste no apreciara ningún cambio y el atacante estará capacitado para continuar usando cualquier recurso del dispositivo con el que se ha establecido la relación de confianza. Esto significa no solo la posibilidad de obtención de datos, sino de otros servicios como empleo del terminal como modem, Internet, WAP y GPRS, los cuales pueden ser conseguidos sin el consentimiento del propietario.

Análisis de los lugares riesgosos con el uso del Bluetooth [4]

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.

4 Fuente: Pointsec Mobile Technologies

- En una biblioteca
- En un Shopping o en un bar
- En un campo de fútbol.
- En alguna tienda de telefonía.
- En el subte.

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

Analizando los datos existentes sobre el uso de celulares, hay que tener precaución con la habilitación y disponibilidad del mismo.

3.4. Consejos prácticos para mejorar la seguridad en sus equipos Bluetooth

Si bien Bluetooth se ha diseñado como una tecnología que provee seguridad mediante mecanismos de autenticación y encriptación, también tiene múltiples vulnerabilidades que pueden ser reducidas siguiendo ciertas recomendaciones básicas.

Un dispositivo Bluetooth puede ser configurado en modo “Visible (Discoverable)” o “No

visible (Non discoverable)", de los cuales el segundo modo es más inseguro ya que está abierto y puede ser encontrado por cualquier dispositivo Bluetooth que haga una búsqueda de dispositivos dentro de su radio de acción. El primer modo, si bien es más seguro, sigue estando visible por dispositivos con los que se ha emparejado previamente o que de alguna manera reconozcan la MAC del dispositivo Bluetooth; por este motivo, no es recomendable emparejarse ni aceptar contenido de dispositivos desconocidos.

El código PIN predeterminado de cada dispositivo es siempre conocido por todos, por lo tanto es recomendable que sea cambiado por otro

4. PROYECCIÓN A FUTURO DE LA TECNOLOGÍA BLUETOOTH

- **Ultra Wide Band Bluetooth**

  El 28 de marzo de 2006, la asociación Bluetooth SIG anunció su intención de utilizar Ultra-Wideband/MB-OFDM como capa física para futuras versiones de Bluetooth. La integración de UWB creará una versión de la tecnología Bluetooth con opción a grandes anchos de banda. Esta nueva versión permitirá alcanzar los requisitos de sincronización y transferencia de grandes cantidades de datos así como de contenidos de alta definición para dispositivos portátiles, proyectores multimedia, televisores y teléfonos VOIP.

  Al mismo tiempo, la tecnología Bluetooth continuará satisfaciendo las necesidades de aplicaciones de muy bajo consumo como ratones, teclados o auriculares mono permitiendo a los dispositivos seleccionar la capa física más apropiada para sus requisitos.

- **Ultra Low Power Bluetooth** [5]

  En el año 2007, Nokia y la asociación Bluetooth SIG anunciaron que la tecnología Wibree formará parte de la especificación de Bluetooth como versión de muy bajo consumo. Sus aplicaciones son principalmente dispositivos sensores o mandos a distancia. Una de ellas y la que parece que más pronto estará disponible en el mercado es Wibree, una tecnología desarrollada por Nokia y que según la empresa finlandesa es hasta 10 veces más eficaz en energía que Bluetooth. Lo destacable es que Wibree se convertirá en parte de la especificación de Bluetooth para los dispositivos inalámbricos de baja potencia.

- **Mejoras en la Gestión**

  Permite la configuración automática de las topologías "piconet" produciendo una

---

5 Fuente: http://tecnochica.com/2007/06/wibree/ - http://www.nokia.com/A4136001?newsid=1132534

mejora en la disponibilidad de los datos de audio y video para ser transmitida en una mayor calidad, especialmente cuando el mejor esfuerzo de tráfico se está transmitiendo en la misma piconet.

- **El Bluetooth como nuevo canal de difusión**

  Al ser un dinámico transmisor de información, impulsará al Bluetooth como un nuevo modelo de publicidad llamado “Proximity Marketing”. Al ser un dispositivo de comunicación masivo, se pronostica su uso en:

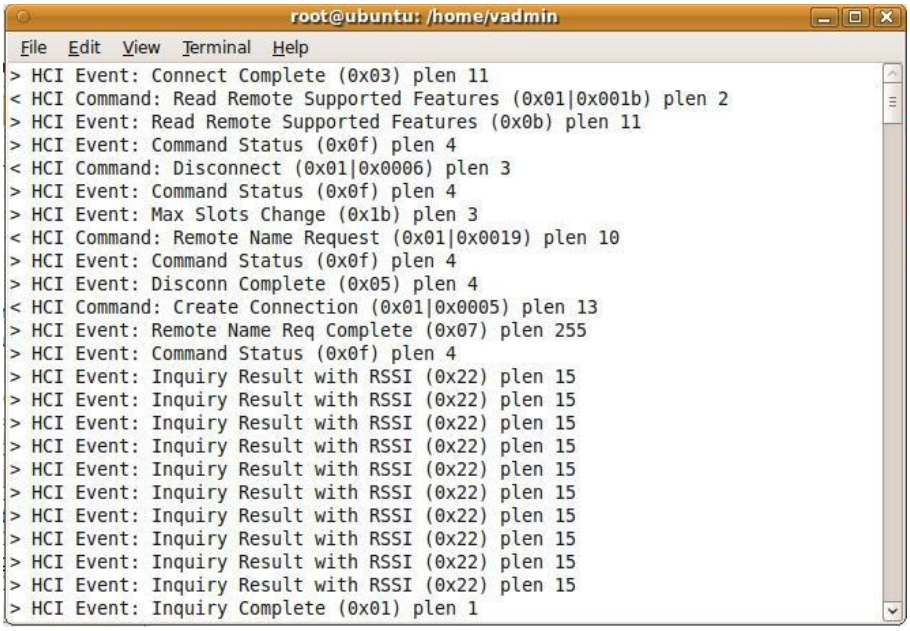
  - Ferias y congresos: Para el envío de publicidad a todas las personas que pasen por delante del Stand.
  - Grandes superficies y Locales comerciales: Informar a clientes de nuevas ofertas y promociones. Descarga gratuita de anuncios y contenidos.
  - Bares y discotecas: Para enviar promociones a sus clientes, contenidos divertidos como música, vídeos, etc.

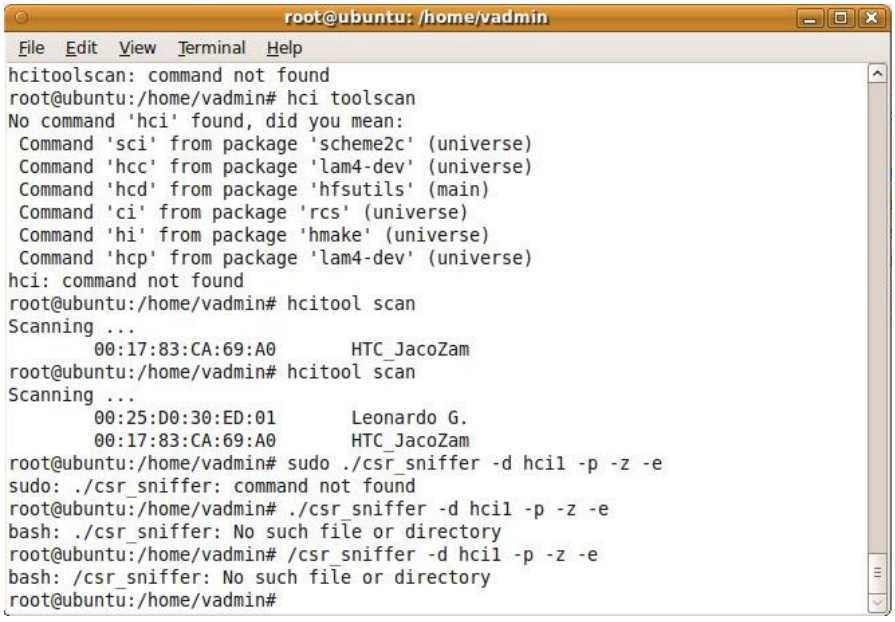
5. EJERCICIO PRÁCTICO

El ejercicio práctico se oriento en dos pasos, primero a conseguir la MAC de los dispositivos Bluetooth que se encuentren en el entorno, y posteriormente se apunto a activar un sniffer en el canal para captar tráfico.

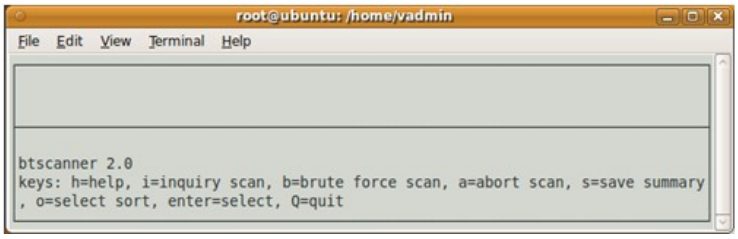
La averiguación de MAC se logro con un teléfono HTC y el programa Bluezard:

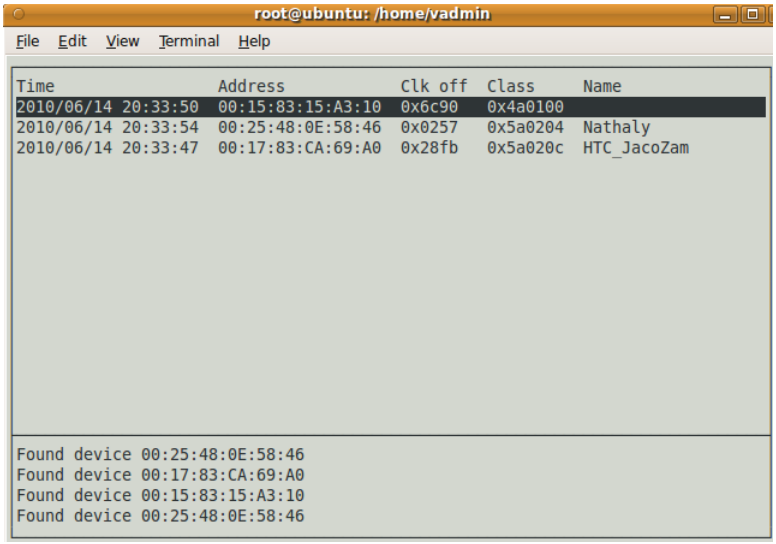
Para realizar el Sniffer se utilizaron dos programas diferentes, el primero es el **hcidump** el cual permite capturar los mensajes en una señal Bluetooth de un quipo que se ha emparejado con él. A continuaciones algunas gráficas de la prueba:


root@ubuntu: /home/vadmin
File Edit View Terminal Help
> HCI Event: Connect Complete (0x03) plen 11
< HCI Command: Read Remote Supported Features (0x01|0x001b) plen 2
> HCI Event: Read Remote Supported Features (0x0b) plen 11
> HCI Event: Command Status (0x0f) plen 4
< HCI Command: Disconnect (0x01|0x0006) plen 3
> HCI Event: Command Status (0x0f) plen 4
> HCI Event: Max Slots Change (0x1b) plen 3
< HCI Command: Remote Name Request (0x01|0x0019) plen 10
> HCI Event: Command Status (0x0f) plen 4
> HCI Event: Disconn Complete (0x05) plen 4
< HCI Command: Create Connection (0x01|0x0005) plen 13
> HCI Event: Remote Name Req Complete (0x07) plen 255
> HCI Event: Command Status (0x0f) plen 4
> HCI Event: Inquiry Result with RSSI (0x22) plen 15
> HCI Event: Inquiry Result with RSSI (0x22) plen 15
> HCI Event: Inquiry Result with RSSI (0x22) plen 15
> HCI Event: Inquiry Result with RSSI (0x22) plen 15
> HCI Event: Inquiry Result with RSSI (0x22) plen 15
> HCI Event: Inquiry Result with RSSI (0x22) plen 15
> HCI Event: Inquiry Result with RSSI (0x22) plen 15
> HCI Event: Inquiry Result with RSSI (0x22) plen 15
> HCI Event: Inquiry Result with RSSI (0x22) plen 15
> HCI Event: Inquiry Result with RSSI (0x22) plen 15
> HCI Event: Inquiry Complete (0x01) plen 1



El segundo Sniffer utilizado es el **BTScanner** el cual captura paquetes Bluetooth de dispositivos activos que se encuentren en su rango de acción, incluso si no se encuentran emparejados con él; y también entrega la información de los dispositivos como la dirección MAC y el nombre de usuario. A continuaciones algunas gráficas:



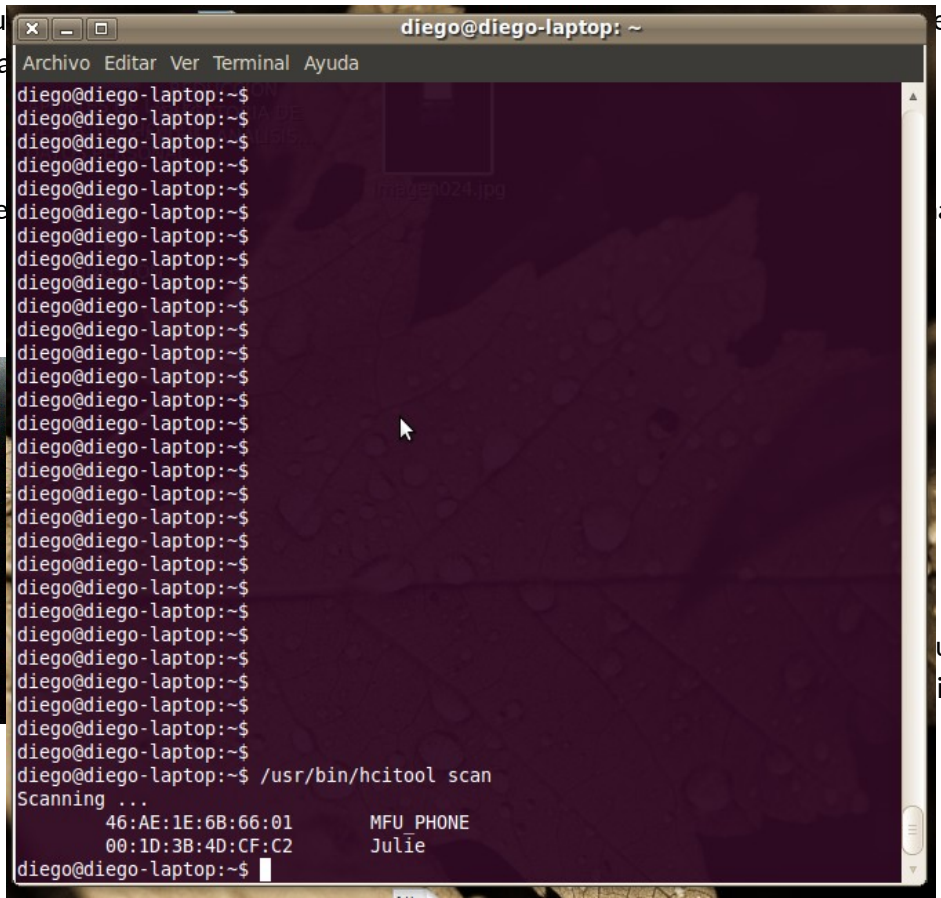


Ejemplo Ataque Bluesnarfing

Equipo utilizado: Acer 5315-2844
SO: Ubuntu 10.4
USB Bluetooth genérico.
2 Celulares, Nokia 6555, Black Phone Bla

El objetivo de este ataque es suplantar la identidad de uno de los celulares, cuando existe una conexión establecida entre ambos. Se explota la vulnerabilidad de algunos dispositivos que requiere au e acceder a la

1. Se e ación.
2.

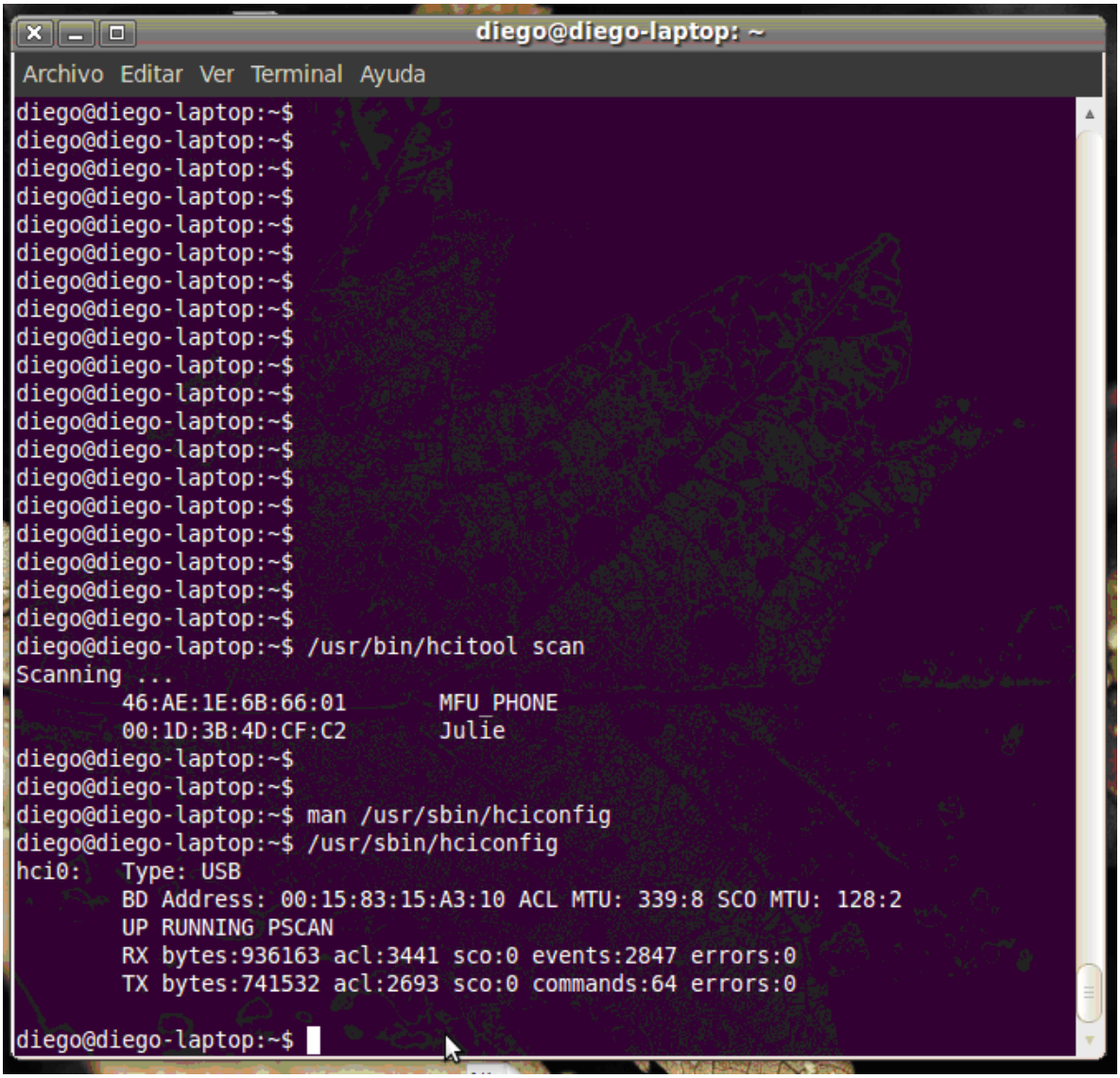


2. En la La ueZ), y se conect itivos

bluetooth a nuestro alcance.

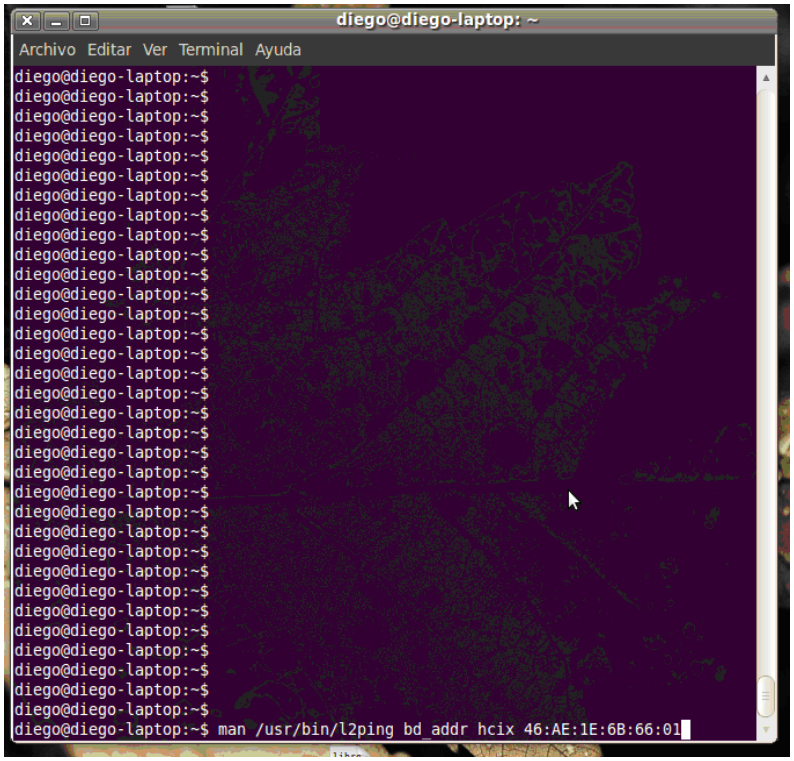
En es caso, el Celular Nokia 6555 tiene la MAC 00:1d:3B:4D:CF:C2, Black Phone Bla tiene la MAC 46:AE:1E:6B:66:01.

Inicialmente, si intentamos conectarnos al con nuestro perfil y enviar un archivo, al tratarse de un equipo no incluido en la lista de dispositivos de confianza, el usuario del primer teléfono deberá autorizar explícitamente la conexión…

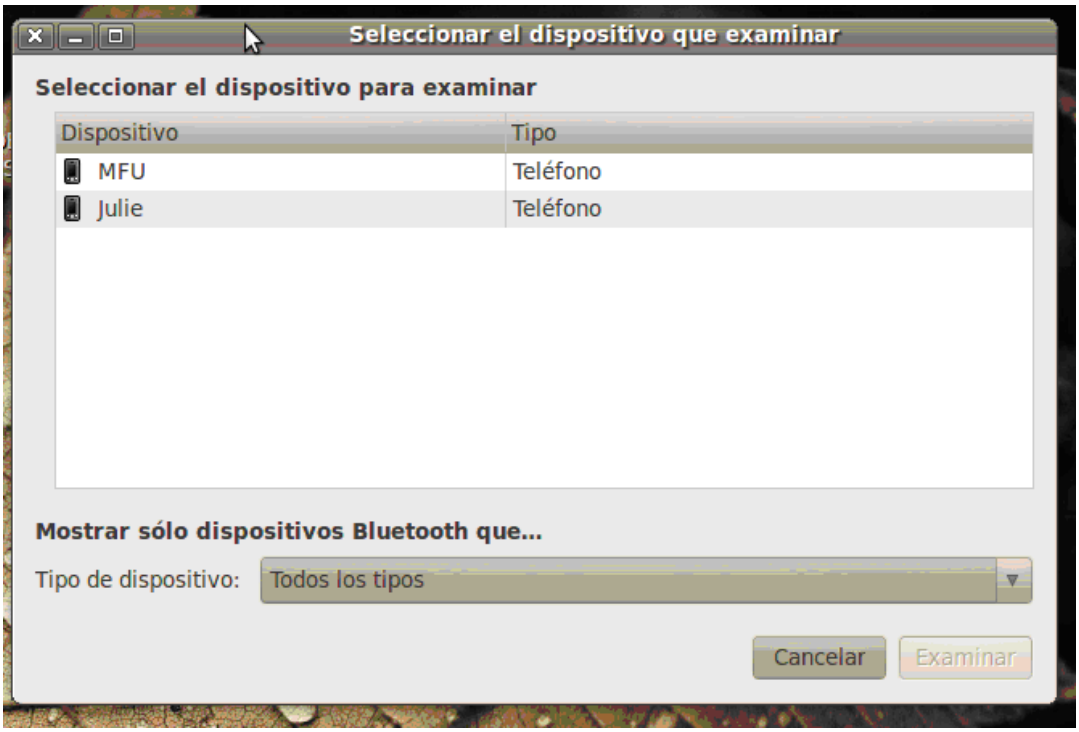


La MAC del Bluetooth el equipo es 00:15:83:15:A3:10. Para evitar el mecanismo de autorización, podemos suplantar la identidad de un dispositivo de confianza del teléfono como, en este caso, es el celular Black Phone Bla que se encuentra autorizado. Para eso debemos conocer la dirección MAC del equipo a suplantar y cambiar la dirección MAC del módulo Bluetooth utilizado por su equipo por esta nueva.

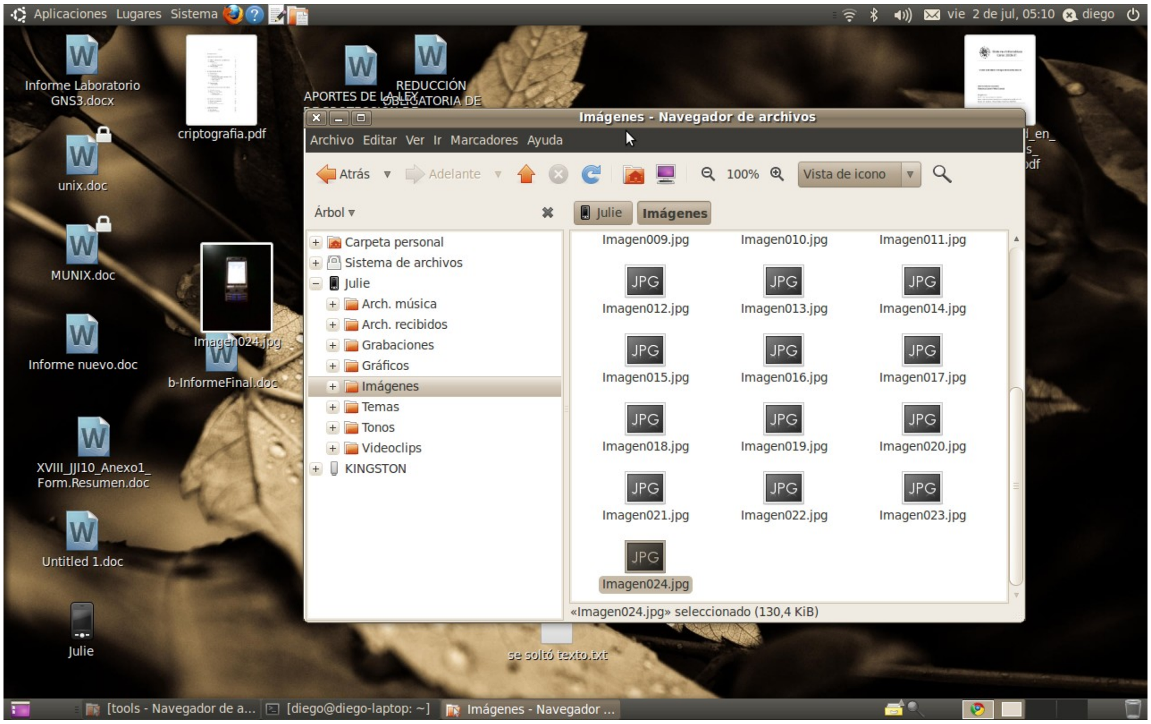
Para ello, el atacante puede hacer uso de la herramienta bdaddr, para simular el número de MAC.



Luego de configurar la MAC en nuestro equipo, seleccionamos los dispositivos Bluetooth a nuestro alcance,



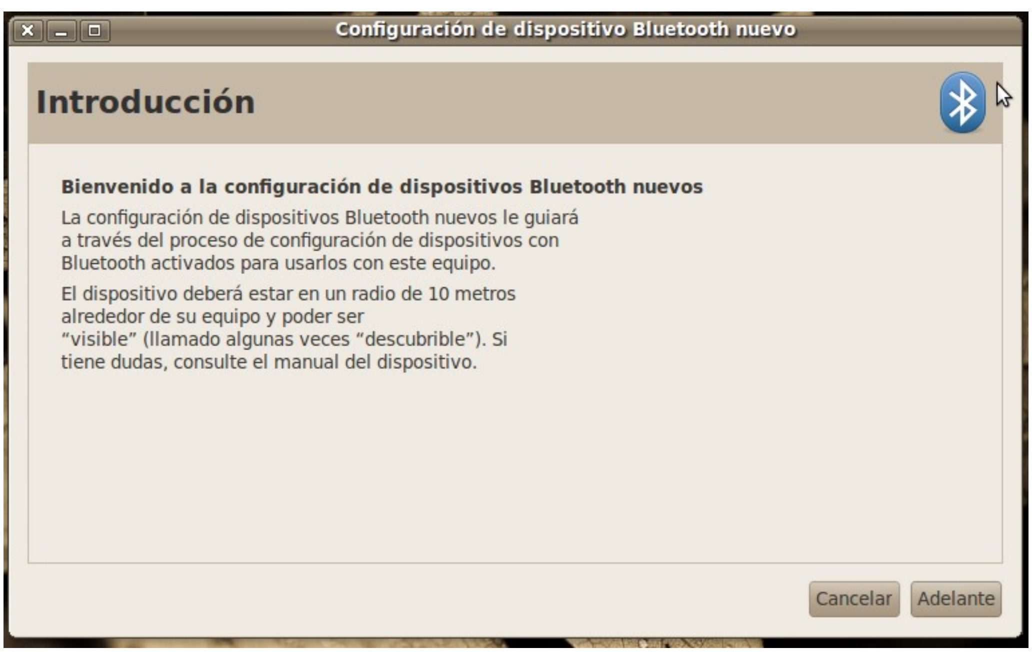
Y podemos acceder a los archivos de la tarjeta de Memoria sin autenticarnos.



_ _

<u>Configuración de Dispositivos con UBUNTU 10.4:</u>

Para poder intercambia información entre un dispositivo Bluetooth y una Laptop con Ubuntu 10.4. Hay que iniciar el aplicativo para configurar el BlueTooth.



Reconocer el dispositivo, en este caso es: MFU_PHONE.

Además de reconocer el dispositivo, se genera un PIN para introducir en celular dentro de los 15 segundos.

Una vez configurado el dispositivo, se puede intercambiar información.

6. CONCLUSIONES

Luego de analizar las vulnerabilidades del uso de Bluetooth en trasmisión de información, planteamos como conclusión principal que al desarrollar estos dispositivos se privilegio la rápida accesibilidad de la comunicación, que la seguridad en los dispositivos.
La seguridad en la tecnología bluetooth es bastante baja, ya que pueden tener acceso a un celular en cuanto se pueda suplantar la identidad de un dispositivo que se tenga autorizado en el mismo. Pudiendo extraer mensajes privados, números de teléfono, fotos almacenadas en el celular.

Solución de Seguridad

Analizando los programas Open Source, se puede suplantar la identidad de un dispositivo Bluetooth con el fin de acceder a otro utilizando la MAC de uno de los dispositivos. Esto se debe a que, en primera instancia, la arquitectura de seguridad en Bluetooth se definió a nivel de dispositivos, y no de usuarios. Dado que el ataque Bluesnarfing explota un fallo en los mecanismos de seguridad utilizados por Bluetooth y que estos están definidos en la especificación de su protocolo, con el fin de solucionar esta vulnerabilidad sería preciso modificar la especificación del estándar.

Nuestro consejo es evitar mantener activos en el teléfono aquellos enlaces con otros dispositivos Bluetooth emparejados más allá del tiempo necesario para su uso. En el caso de conexiones esporádicas o de baja periodicidad, aconsejamos realizar un emparejamiento de nuevo cada vez que se vaya a producir la comunicación y eliminar el enlace al final de la misma.

7. BIBLIOGRAFÍA

The Spanish Bluetooth Security Group (2005), “Seguridad en Bluetooth”, accedido desde http://bluehack.elhacker.net/proyectos/bluesec/bluesec.html

Viruslist.com (2006), “La seguridad de Bluetooth; Cacería de dispositivos Bluetooth (War-nibbling) en Año Nuevo”, accedido desde http://www.viruslist.com/sp/analysis?pubid=181198286

Taddong (2010), “Seguridad en Bluetooth”, accedido desde http://www.fistconference.org/files/seguridad_bluetooth_raulsilestaddong_fistfiberparty_feb2010.pdf

Alberto Moreno Tablado, (2006) “Seguridad en Bluetooth”, accedido desde http://www.telefonica.net/web2/telamarinera/docus/PFC.Seguridad.en.Bluetooth.pdf

Alberto Moreno Tablado (2009), “Bluetooth security mechanisms”, accedido desde

http://www.seguridadmobile.com/bluetooth/bluetooth-security/security-mechanisms.html

Bluetooth.com (2010), “Acerca del SIG Bluetooth”, accedido desde http://www.bluetooth.com/Spanish/SIG/Pages/default.aspx

Ezequiel M Sallis, “Bluetooth la Amenaza Azul”, accedido desde

http://simubucks.files.wordpress.com/2007/07/bluetooth-la-amenaza-azul-v20.pdf

http://es.wikipedia.org/wiki/Bluetooth