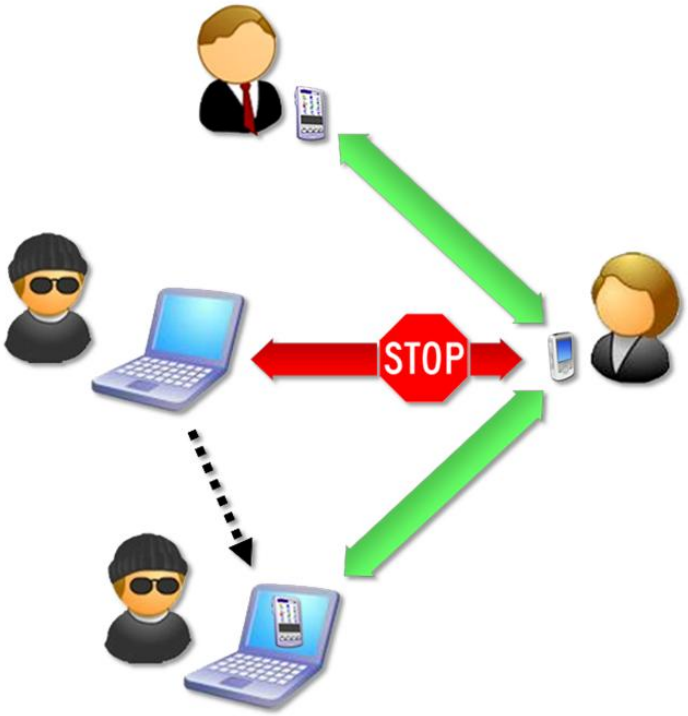
REVISIÓN DEL ATAQUE BLUE MAC SPOOFING



¿TODAVÍA PIENSAS QUE BLUETOOTH ES SEGURO?

Alberto Moreno Tablado

mossec
MOBILE SECURITY SOFTWARE

seguridad mobile
el Blog de Gospel

INTRODUCCIÓN

La mayoría de usuarios de teléfonos móviles Bluetooth ha tenido la necesidad alguna vez de emparejar su teléfono con otro dispositivo con el fin de transferir archivos vía Bluetooth o conectarse a equipos manos libres o receptores GPS. Es un hecho que la conducta habitual suele ser mantener esos enlaces activos aun cuando estos se encuentren en desuso o la conexión haya sido esporádica. ¿Qué ocurriría si cada uno de esos enlaces activos pudiera convertirse en una puerta trasera a nuestro teléfono, con acceso transparente al control total de las funciones del teléfono y los archivos almacenados? En efecto, dado que todos los mecanismos de seguridad empleados por Bluetooth se realizan a nivel de dispositivo, y no de usuario, suplantar la identidad de un dispositivo emparejado y utilizar sus credenciales de confianza para acceder a un teléfono sin que el usuario se percate resulta una acción trivial. En esto consiste el ataque ***Blue MAC Spoofing***.

El ataque ***Blue MAC Spoofing***, al contrario que cualquier ataque publicado hasta la fecha que afecte a teléfonos móviles Bluetooth, no explota una implementación incorrecta de Bluetooth por parte de los fabricantes, sino un fallo del estándar en sí mismo. Se trata de una vulnerabilidad intrínseca a los mecanismos de seguridad utilizados por Bluetooth y, por ello, no sólo afecta a todos los teléfonos móviles Bluetooth, sino a cualquier equipo que haga uso de esta tecnología de comunicaciones inalámbricas.

MECANISMOS DE SEGURIDAD EN BLUETOOTH

A fin de poder entender el desarrollo del ataque, es importante conocer los mecanismos de seguridad que utiliza Bluetooth y porque son fácilmente explotables debido a su diseño.

- **Autenticación**

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

  La primera vez que dos dispositivos intentan comunicarse, se lanza un procedimiento de inicialización denominado *emparejamiento* para crear una clave de enlace común de una forma segura. El procedimiento estándar requiere que el usuario de cada dispositivo introduzca un código de seguridad Bluetooth, conocido como PIN, de hasta 16 bytes de longitud que debe ser el mismo en ambos casos. A partir de este código PIN Bluetooth, la dirección BD_ADDR de cada dispositivo y varios números aleatorios de 128 bits se obtiene la clave de enlace común a ambos dispositivos a través de los algoritmos E22 y E21.

  Una vez que los dispositivos emparejados disponen de la clave de enlace, utilizan esta clave común para autenticarse automáticamente en sucesivas conexiones. El proceso de autenticación está basado en un esquema de desafío/respuesta que comprueba la identidad del dispositivo que intenta conectarse en el destino.

- **Autorización**

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

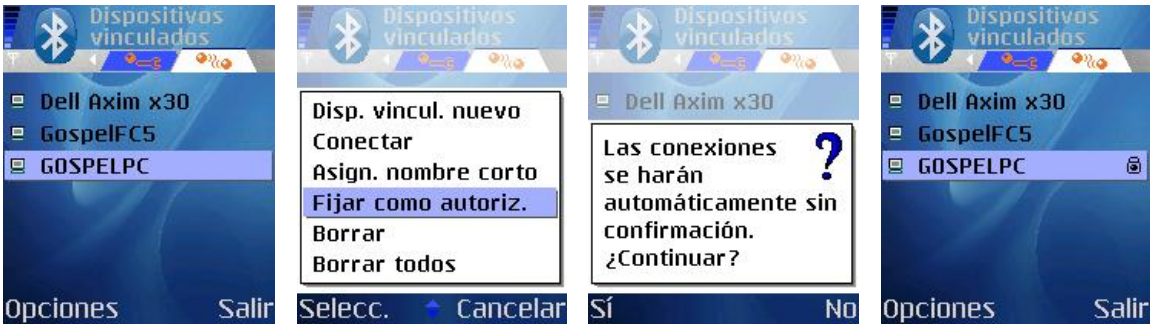
  El mecanismo de autorización en dispositivos Bluetooth se lleva a cabo mediante *niveles de confianza* y se gestiona mediante una lista de dispositivos de confianza que determina la capacidad de acceso a los servicios: total, parcial o restringida y nula.

  - Un dispositivo de confianza dispone de acceso sin restricciones a todos los servicios.
  - Un dispositivo no confiable dispone de acceso restringido a uno o varios servicios o incluso no se le permite el acceso a ningún servicio.

  Todo dispositivo Bluetooth que implemente servicios con autorización dispone de una base de datos interna con una lista de dispositivos de confianza y que tiene el siguiente formato:

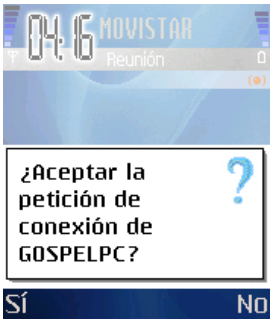
Campo	Estado	Contenido
BD_ADDR	Obligatorio	Dirección MAC del dispositivo
Nivel de confianza	Obligatorio	De confianza / No de confianza (Booleano)
Clave de enlace	Obligatorio	Clave de enlace
Nombre	Opcional	Nombre del dispositivo
Class of Device	Opcional	Identificador de la clase de dispositivo

En la mayoría de teléfonos móviles es habitual solicitar automáticamente al usuario si desea marcar un dispositivo como autorizado justo después de haberse emparejado con el mismo, aunque también se añade la opción de hacer esto posteriormente de forma manual. Por lo tanto, es posible considerar que un dispositivo emparejado es también un dispositivo autorizado.



En el caso de que un dispositivo de confianza intente acceder a un servicio autorizado, no se requiere ningún procedimiento de confirmación, accede de forma transparente.

En el caso de que un dispositivo no confiable intente acceder a un servicio restringido, se requiere un procedimiento de confirmación explícito al usuario para permitir o denegar el acceso de ese dispositivo a ese determinado servicio.



LA REALIDAD DE LOS MECANISMOS DE SEGURIDAD EN BLUETOOTH

Tras la publicación de los primeros ataques a teléfonos móviles Bluetooth, en especial el ataque ***Bluesnarf*** [1], los fabricantes tomaron mayor conciencia de la necesidad de fortificar el acceso a los perfiles Bluetooth que soportaban sus dispositivos manufacturados.

Se decidió que, en adelante:

- Todos los perfiles Bluetooth debían requerir autenticación, a excepción de aquellos perfiles cuya funcionalidad quedaría limitada por el *modelo de uso*. Por ejemplo: el perfil de Carga de Objetos utilizado para transferencia simple y espontánea de archivos (tarjetas de visitas, contactos, etc.) y marketing de proximidad.

- Todos los perfiles Bluetooth debían requerir autorización, con la posibilidad de que aquellos dispositivos ya emparejados fueran autorizados automáticamente o pudieran ser marcados como autorizados por el usuario.

Con esta medida, el escenario de ataque a teléfonos móviles se transformó. Dado que la implementación de los fabricantes iba a ser robusta, siguiendo las recomendaciones del estándar Bluetooth, la nueva estrategia es atacar al estándar directamente, ¿cómo saltarse los mecanismos de seguridad utilizados por Bluetooth?

Si nos tomamos un tiempo para estudiar detenidamente la arquitectura de seguridad en Bluetooth, salta a la vista la simplicidad de su diseño y lo débil que resulta.

3.2.1 Authorisation and Authentication

Authorisation is the process of deciding if device X is allowed to have access to service Y. This is where the concept of 'trusted' exists. Trusted devices (authenticated and indicated as "trusted"), are allowed access to services.

3.2.2 Security Levels of Services

Authorisation Required: Access is only granted automatically to trusted devices (i.e., devices marked as such in the device database) or untrusted devices after an authorisation procedure.

Fuente: Apdo. 3.2 Security Levels – Bluetooth Security Architecture Version 1.0 (www.bluetooth.com)

Esto significa que un dispositivo autorizado puede acceder automáticamente a todos los servicios que requieran autorización. Para que un dispositivo sea considerado como autorizado debe estar marcado como tal en la lista de dispositivos de confianza y para ello debe tratarse también de un dispositivo autenticado (recordemos que el campo *clave de enlace* es obligatorio en la base de datos de dispositivos de confianza).

Sin embargo, un hecho importante que se omite es que si un servicio no requiere autenticación, la clave de enlace no entra en juego necesariamente y el acceso se basa únicamente en la dirección BD_ADDR de dispositivo, de forma que si existe en la lista de dispositivos de confianza, este queda autorizado.

[1] http://trifinite.org/trifinite_stuff_bluesnarf.html

4.2.1 Authentication

The authentication procedure is based on a challenge-response scheme […]. The verifier sends […] a random number (the challenge) to the claimant. The claimant calculates a response, that is a function of this challenge, the claimant's BD_ADDR and a secret key. The response is sent back to the verifier, that checks if the response was correct or not. […] A successful calculation of the authentication response requires that two devices share a secret key.

Fuente: Apdo. 4.2 Security - Core v2.0 + EDR (www.bluetooth.org, disponible para miembros del SIG)

Esto significa que la autenticación se basa en la dirección BD_ADDR de dispositivo y en la clave de enlace secreta compartida, de forma que si el esquema desafío/respuesta es positivo, este queda autenticado.

El esquema desafío/respuesta de autenticación transcurre de la siguiente forma:

1) El dispositivo reclamante envía su dirección BD_ADDR al dispositivo verificador.

2) El verificador devuelve un desafío aleatorio de 128 bits al reclamante.

3) El reclamante usa el algoritmo E1 para generar la respuesta de autenticación (SRES) de 32 bits, usando como parámetros de entrada la dirección BD_ADDR del reclamante, la clave de enlace almacenada y el desafío recibido. El verificador realiza la misma operación en paralelo.

4) El reclamante devuelve la respuesta SRES al verificador.

5) El verificador comprueba la respuesta SRES recibida por el reclamante con la respuesta SRES calculada por él.

6) Si los valores de SRES coinciden, el verificador autentica al reclamante.

En resumen,

- La autorización se basa únicamente en la dirección BD_ADDR de dispositivo.
- La autenticación se basa en la dirección BD_ADDR de dispositivo y en la clave de enlace secreta compartida.

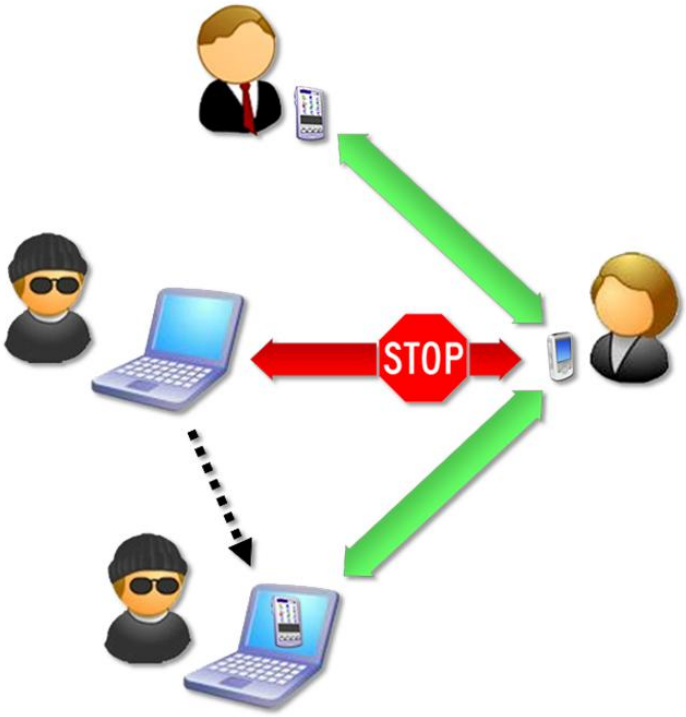
Dado que tanto el mecanismo de autorización como el esquema de desafío/respuesta utilizado para la autenticación verifican la identidad de dispositivos, no usuarios, surgen dos preguntas clave:

- ¿Qué pasa si un equipo atacante suplanta la dirección BD_ADDR de un dispositivo de confianza? ¿Queda autorizado en el dispositivo destino?
- ¿Qué pasa si un atacante tiene acceso a la clave de enlace de uno de los dispositivos emparejados? ¿Puede utilizarla para autenticarse en el otro dispositivo?

La respuesta es **sí.**

EL ATAQUE BLUE MAC SPOOFING

El ataque ***Blue MAC Spoofing*** permite suplantar la identidad de un dispositivo de confianza y/o emparejado para atacar un teléfono móvil y utilizar sus credenciales para acceder a perfiles que requieren autorización y/o autenticación.



Se denomina ***Blue MAC Spoofing*** por su analogía con el clásico ataque *MAC Spoofing* en redes Ethernet, el cual permite a un atacante suplantar la dirección MAC de un equipo para suplantar su identidad y llevar a cabo acciones maliciosas contra el resto de equipos de la red, ya sea interceptando las comunicaciones dirigidas al equipo suplantado o utilizando sus credenciales con el fin de acceder a un sistema con acceso limitado.

Puesto que hay dos mecanismos de seguridad en Bluetooth, el ataque ***Blue MAC Spoofing*** se puede desarrollar en dos niveles:

- Suplantación de la dirección BD_ADDR de un dispositivo de confianza para acceder a perfiles que requieren autorización.
- Suplantación de la dirección BD_ADDR y obtención de la clave de enlace generada durante el emparejamiento para acceder a perfiles que requieren autenticación.

ALCANCE DEL ATAQUE BLUE MAC SPOOFING

Para poder evaluar las consecuencias que tiene el hecho de desarrollar un ataque ***Blue MAC Spoofing*** con éxito sobre un teléfono móvil, es importante conocer los principales vectores de ataque en teléfonos Bluetooth.

Comandos AT

Los comandos AT son un conjunto de instrucciones codificadas que permiten configurar el teléfono móvil y enviarle órdenes a ejecutar. Básicamente, a través de los comandos AT un atacante puede realizar las siguientes acciones en un teléfono móvil:

- Realizar llamadas de voz y configurar desvíos de llamadas.
- Acceder a la agenda de contactos: leer, añadir, eliminar, …
- Acceder a la agenda de llamadas: últimas llamadas perdidas, recibidas y enviadas.
- Gestión de mensajes SMS: leer bandeja de entrada, escribir y enviar, eliminar, …

Acceso por OBEX

- A través de *OBEX Object Push* es posible el envío de archivos.
- A través de *OBEX File Transfer* es posible acceder al sistema de archivos del teléfono: subida, descarga, listado y borrado de archivos y directorios. Es posible acceder a archivos almacenados tanto en memoria del teléfono como en tarjetas extraíbles.

Veremos como la consecución con éxito del ataque ***Blue MAC Spoofing*** permite explotar ambos vectores de ataque.

DEMOSTRACIÓN PRÁCTICA DEL ATAQUE

Con el fin de demostrar el alcance del ataque ***Blue MAC Spoofing*** voy a basarme en tres escenarios habituales de interconexión de equipos Bluetooth. Cada uno de los escenarios permitirá observar lo fácil que resulta para un atacante suplantar la identidad de un dispositivo de confianza y/o emparejado con el fin de llevar a cabo ciertas acciones maliciosas contra un teléfono móvil.

El primer escenario tiene como objetivo demostrar cómo es posible saltarse el mecanismo de autorización suplantando la identidad de un dispositivo de confianza.

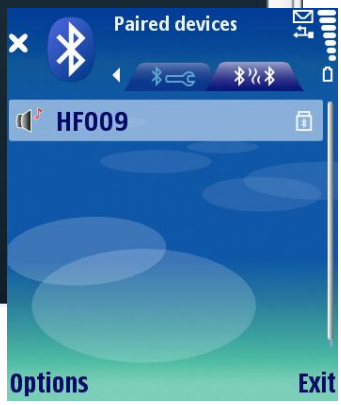
El segundo y el tercer escenario tienen como objetivo demostrar cómo es posible saltarse el mecanismo de autenticación suplantando la identidad de un dispositivo emparejado. En el segundo escenario, para acceder a los comandos AT; en el tercero, para acceder a archivos del teléfono.

En todos los escenarios, el equipo atacante será el mismo: un ordenador portátil con Fedora Core 5 y BlueZ, la pila de protocolos oficial para Linux.

Escenario 1

Un teléfono móvil *Nokia n80* se empareja con un equipo Manos Libres y marca este dispositivo como confiable. El objetivo del atacante es suplantar la identidad del Manos Libres y acceder al perfil de Carga de Objetos del teléfono, el cual requiere autorización, pero no autenticación, y permite el envío simple de archivos e intercambio de tarjetas de visita y contactos entre teléfonos.

```
gospel@GospelFC5:~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
[gospel@GospelFC5 ~]$ bluezscanner
+ BlueZScanner, por Gospel <gospel.endorasoft.es>

Detectando dispositivos ...

Dispositivo (1) encontrado:
        MAC: 00:12:D1:CE:EA:A7          Nombre: NOKIA N80
        Fabricante del Chip Bluetooth:
                - Texas Instruments Inc
        Tipo de dispositivo:
                - Phone > Smart phone

Dispositivo (2) encontrado:
        MAC: 00:08:E0:0E:55:79          Nombre: HF009
        Fabricante del Chip Bluetooth:
                - ATO Technology Ltd.
        Tipo de dispositivo:
                - Audio / Video > Wearable Headset Device
```



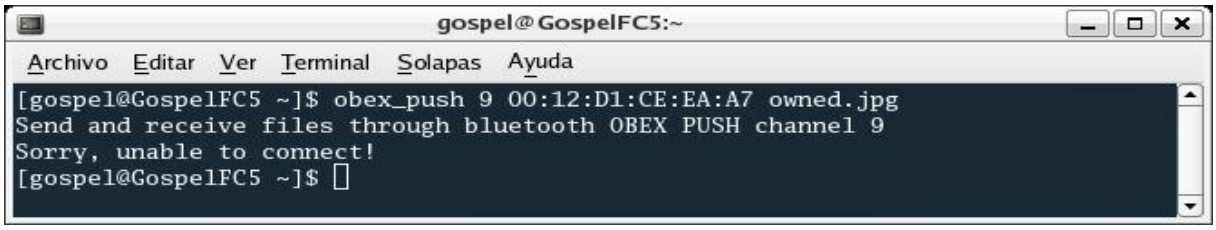
SALTÁNDONOS LA AUTORIZACIÓN…

El objetivo del atacante es conectarse al Perfil de Carga de Objetos (OBEX Object Push), disponible a través del canal 9, y enviar un archivo al teléfono.

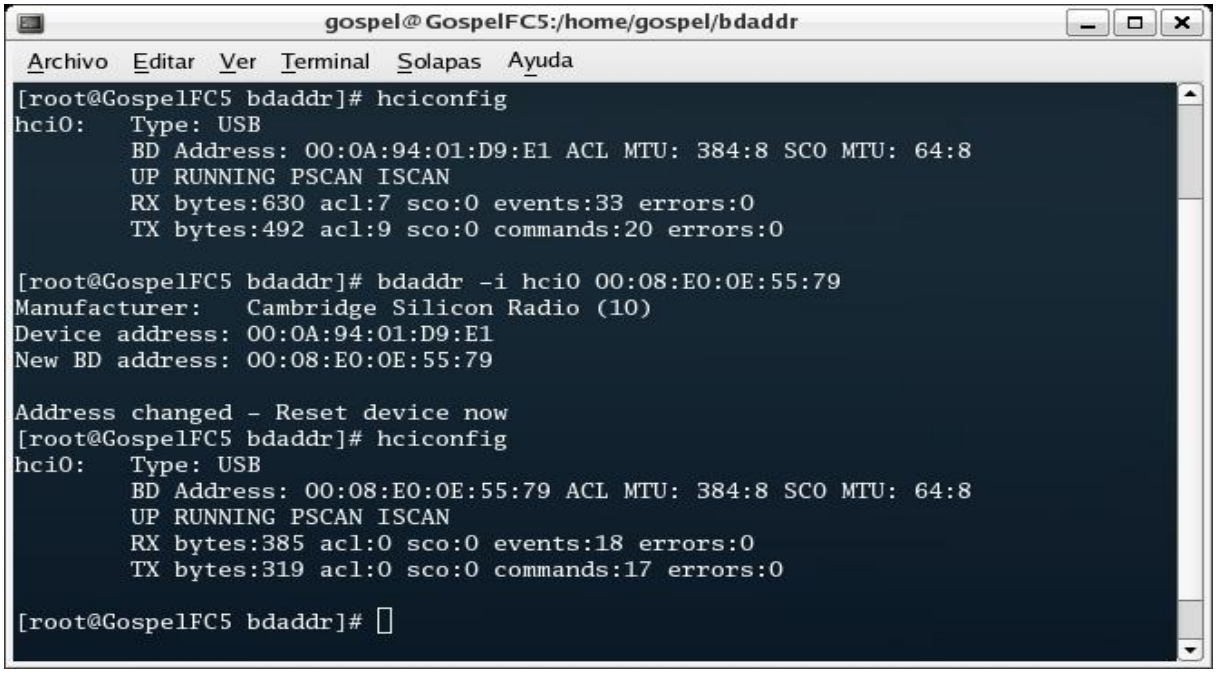
```
gospel@GospelFC5:~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
[gospel@GospelFC5 ~]$ bluezscanner -cp
+ BlueZScanner, por Gospel <gospel.endorasoft.es>

Detectando dispositivos ...

Dispositivo (1) encontrado:
        MAC: 00:12:D1:CE:EA:A7          Nombre: NOKIA N80
        Fabricante del Chip Bluetooth:
                · Texas Instruments Inc
        Class: 0x50020c [010100000000001000001100]
         - Servicios soportados (Service Classes):
                · Telephony (Cordless telephony, Modem, Headset service, ...)
                · Object Transfer (v-Inbox, v-Folder, ...)
         - Tipo de dispositivo (Device Class):
                · Phone > Smart phone
        Perfiles Bluetooth disponibles:
                · AVRCP Target (Channel: 0)
                · Hands-Free Audio Gateway (Channel: 28)
                · Headset Audio Gateway (Channel: 29)
                · SyncMLClient (Channel: 10)
                · OBEX File Transfer (Channel: 11)
                · Nokia OBEX PC Suite Services (Channel: 12)
                · Nokia SyncML Server (Channel: 13)
                · OBEX Object Push (Channel: 9)
                · Dial-Up Networking (Channel: 2)
                · (Channel: 1)
                · Imaging (Channel: 15)
```

Inicialmente, si el atacante intenta conectarse al Perfil de Carga de Objetos y enviar un archivo, al tratarse de un equipo no incluido en la lista de dispositivos de confianza, el usuario del *Nokia n80* deberá autorizar explícitamente la conexión.

Es muy probable que el usuario del *Nokia n80* no confié en el emisor del envío y por ello deniegue el intento de conexión.



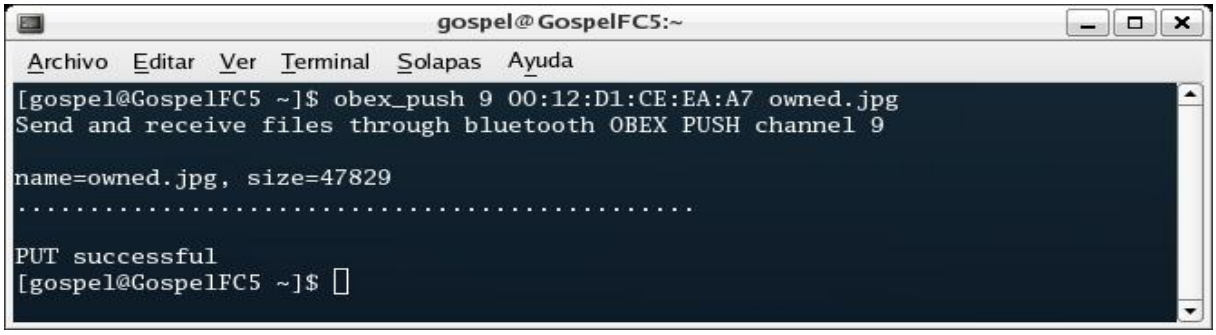
Para evitar el mecanismo de autorización, el atacante puede suplantar la identidad de un dispositivo de confianza del teléfono como, en este caso, el Manos Libres. El atacante debe conocer la dirección BD_ADDR del equipo a suplantar y cambiar la dirección BD_ADDR del módulo Bluetooth utilizado por su equipo por esta nueva. Para ello, el atacante puede hacer uso de la herramienta ***bdaddr***[2], que permite configurar la dirección BD_ADDR y otros parámetros en módulos hardware Bluetooth.



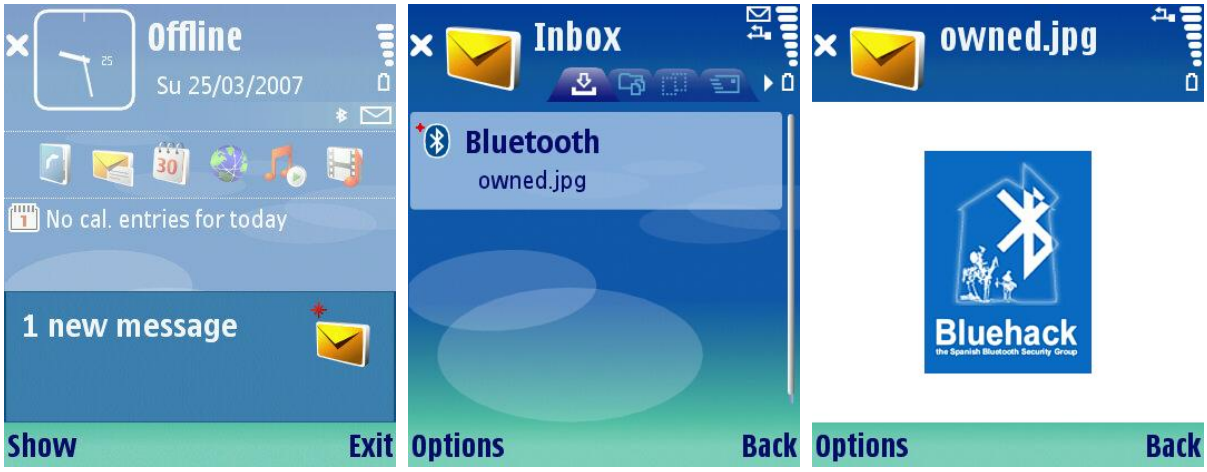
[2] https://stage.maemo.org/svn/maemo/projects/connectivity/bluez-utils/tags/bluez-utils-3.7osso6/test/bdaddr.c

A partir de ese momento, el atacante está en disposición de conectarse a un perfil del teléfono móvil que requiera autorización de forma transparente ya que, a ojos del teléfono, el intento de conexión proviene de un dispositivo incluido en la lista de dispositivos de confianza.

Así pues, el atacante puede intentar conectarse de nuevo al Perfil de Carga de Objetos del teléfono y enviar el archivo. Esta vez, la conexión se realizará sin que el usuario del teléfono se percate de la acción.



El archivo enviado por el equipo atacante será automáticamente recibido por el teléfono móvil y almacenado en la bandeja de entrada de mensajes sin que el usuario haya tenido que autorizar la recepción del mismo.

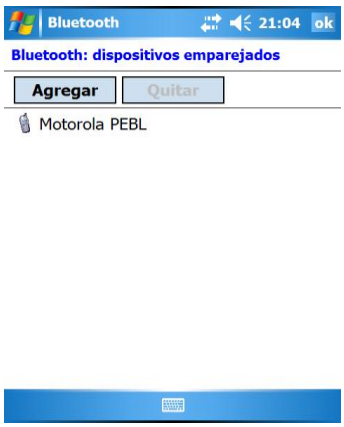


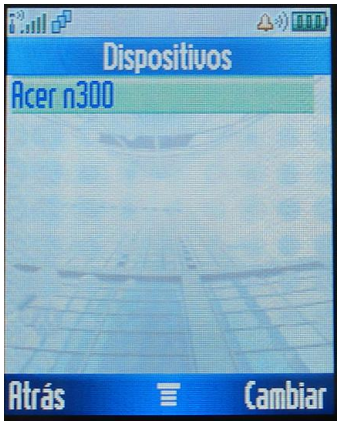
Escenario 2

Un teléfono móvil *Motorola PEBL* se empareja con una PDA *Acer n300* y marca este dispositivo como confiable. El objetivo del atacante es suplantar la identidad de la PDA y conectarse al Perfil de Auriculares del teléfono, el cual requiere autenticación a aquellos dispositivos emparejados y permite el acceso a los comandos AT.

SALTÁNDONOS LA AUTENTICACIÓN…

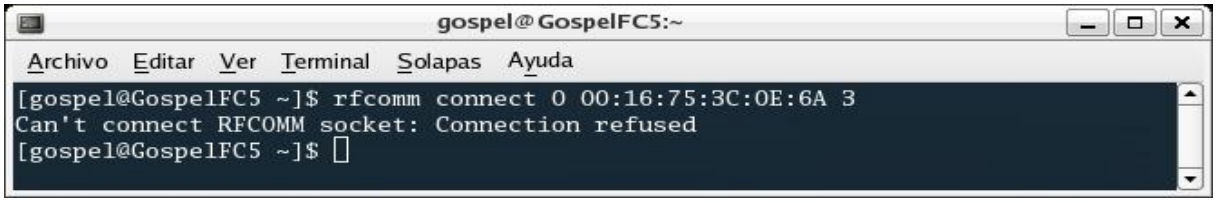
Para demostrar cómo es posible saltarse el mecanismo de autenticación suponemos que la PDA *Acer n300* y el teléfono *Motorola PEBL* están emparejados.



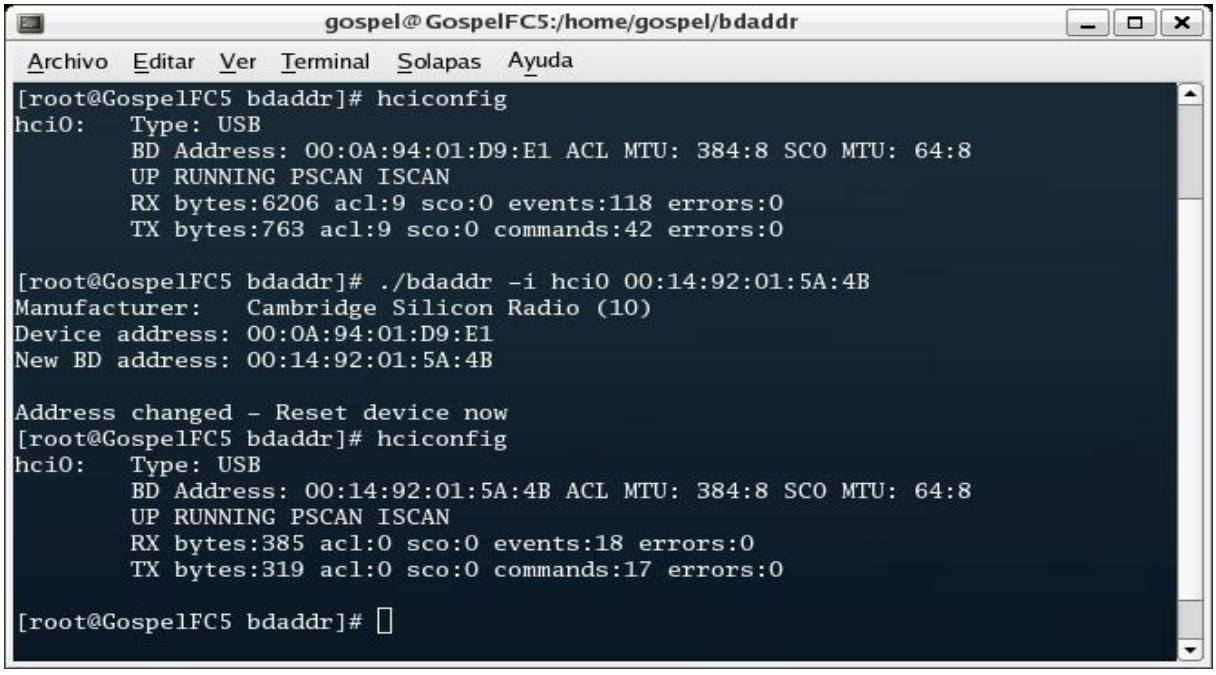


El objetivo del atacante es conectarse al Perfil de Auriculares, disponible en el canal 3 y acceder al juego de comandos AT.

Inicialmente, si el atacante intenta conectarse al Perfil de Auriculares, al tratarse de un equipo desconocido (no incluido en el histórico de dispositivos conectados anteriormente), el teléfono *Motorola PEBL* denegará automáticamente el intento de conexión.



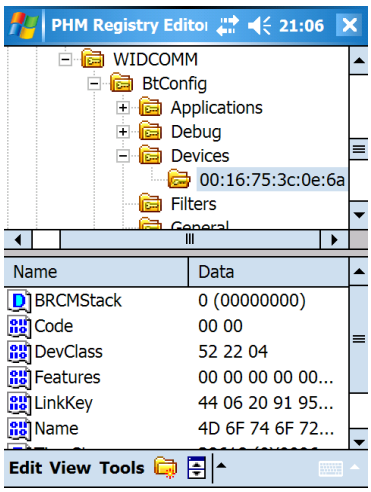
Para saltarse el mecanismo de autenticación, el atacante puede suplantar la identidad de un dispositivo emparejado con el teléfono como, en este caso, la PDA. El atacante debe conocer la dirección BD_ADDR del equipo a suplantar y cambiar la dirección BD_ADDR del módulo Bluetooth utilizado por su equipo por esta nueva con ayuda de la herramienta ***bdaddr***.

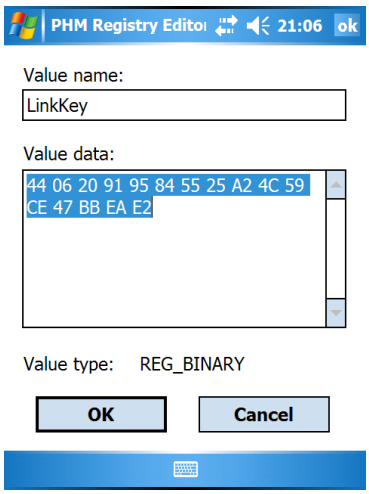


Adicionalmente, debe obtener la clave de enlace generada durante el emparejamiento de la PDA con el teléfono *Motorola PEBL* e instalar esa clave de enlace en el equipo atacante.

Los medios de obtención de la clave de enlace escapan al alcance de este documento. Simplemente daremos por hecho que el atacante tiene acceso al registro de la PDA, donde se almacena la clave de enlace en texto claro, ya sea por acceso físico o mediante la explotación de alguna vulnerabilidad en el sistema operativo Windows Mobile de la PDA.

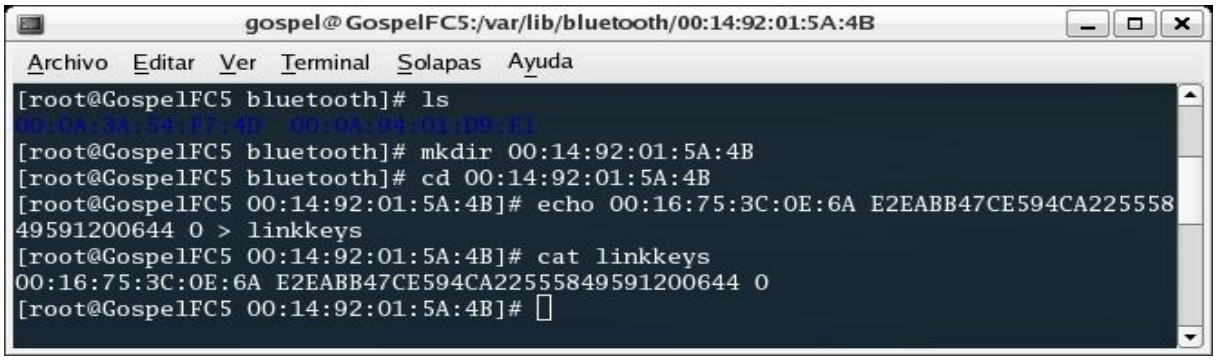
En aquellas PDAs con Windows Mobile 5.0 y pila de protocolos Bluetooth Broadcom/Widcomm, las claves de enlace generadas durante el emparejamiento con otros dispositivos Bluetooth se almacenan en la clave de registro *HKLM\Software\WIDCOMM\BtConfig\Devices\BD_ADDR\LinkKey*. Sin embargo, es necesario tener en cuenta que aunque estas claves de enlace se almacenan en texto claro, lo hacen con un desorden de *endianness*.





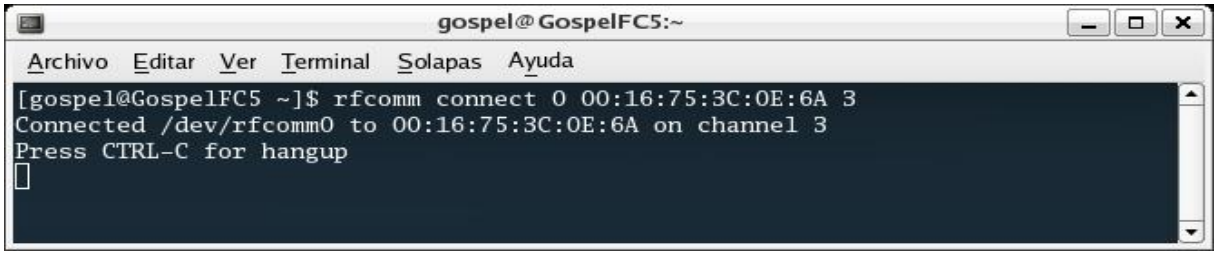
Una vez que el atacante obtiene la clave de enlace, debe instalarla en su equipo Linux atacante, en el fichero *\var\lib\bluetooth\BD_ADDR del módulo Bluetooth\linkkeys* con el siguiente formato:

BD_ADDR del dispositivo emparejado	Clave de enlace de 16 bytes	0



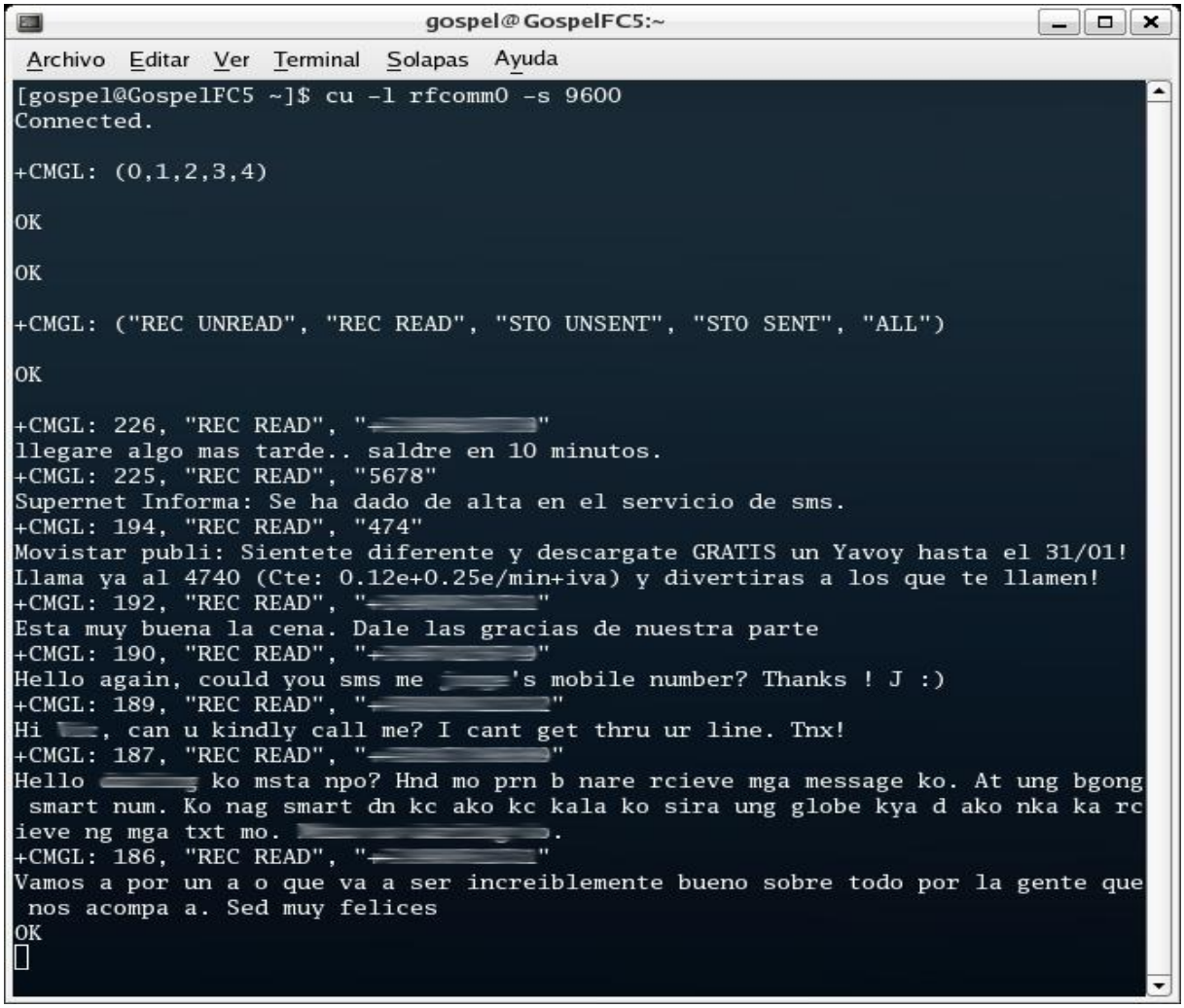
A partir de ese momento, el atacante está en disposición de conectarse a un perfil del teléfono móvil que requiera autenticación de forma transparente ya que, a ojos del teléfono, el intento de conexión proviene de un dispositivo emparejado.

Así pues, el atacante puede intentar conectarse de nuevo al Perfil de Auriculares del teléfono y, esta vez, la conexión se realizará con éxito y sin que el usuario del teléfono se percate de la acción.



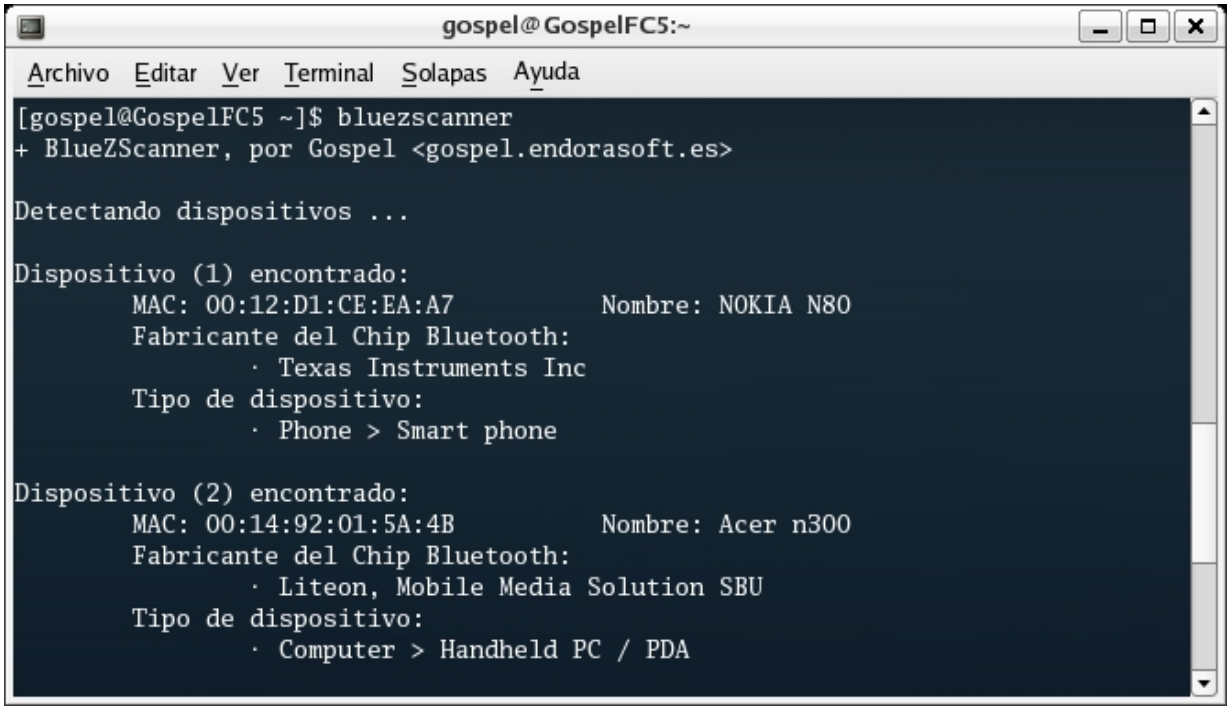
Con la conexión establecida, el atacante puede enviar comandos AT al *Motorola PEBL* y realizar acciones tales como acceder a la agenda de contactos o realizar llamadas de voz.

O acceder a la bandeja de entrada de mensajes SMS ;)



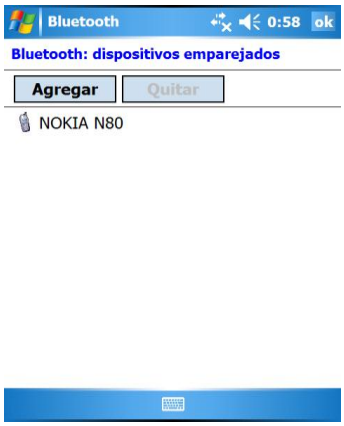
Escenario 3

Un teléfono móvil *Nokia n80* se empareja con una PDA *Acer n300* y marca este dispositivo como confiable. El objetivo del atacante es suplantar la identidad de la PDA y conectarse al Perfil de Transferencia de Archivos del teléfono, el cual requiere autenticación y permite el acceso al sistema de archivos para poder descargarse ficheros almacenados en la memoria y en la tarjeta extraíble.

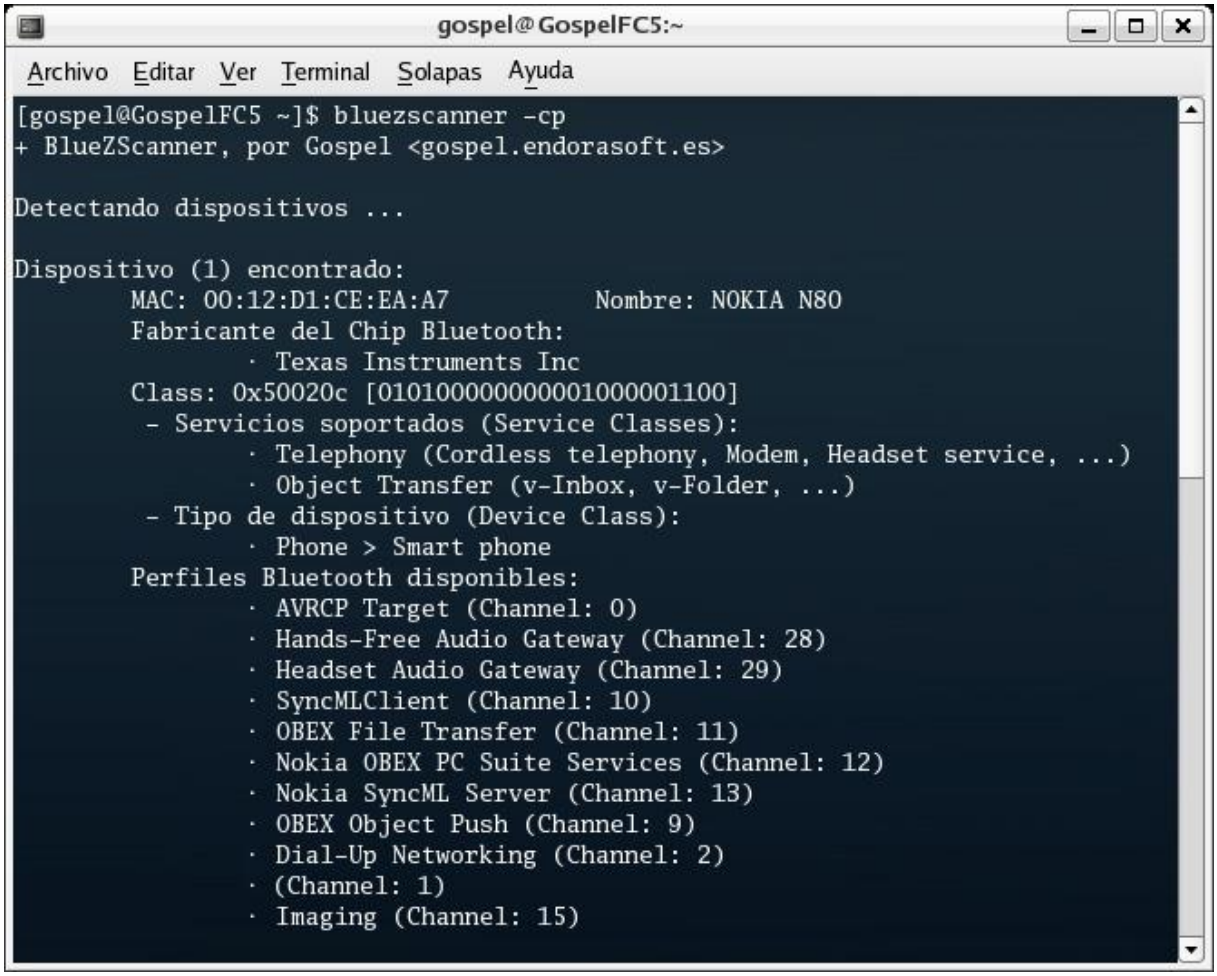


SALTÁNDONOS LA AUTENTICACIÓN…

Para demostrar cómo es posible saltarse el mecanismo de autenticación suponemos que la PDA *Acer n300* y el teléfono *Nokia n80* están emparejados.

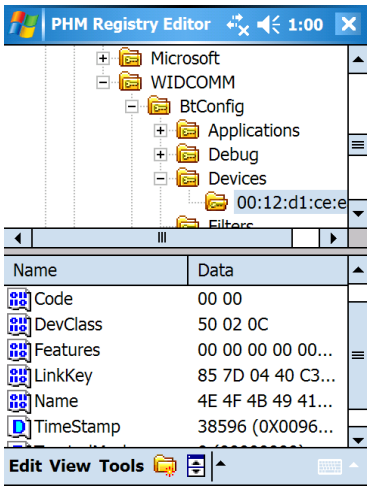


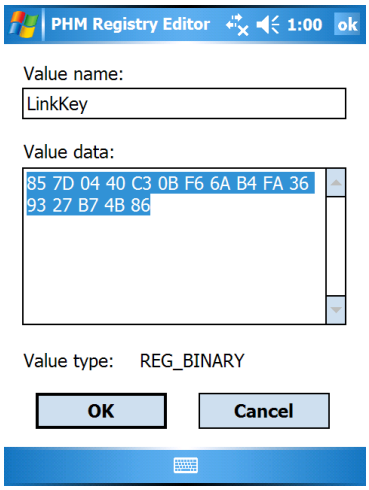
El objetivo del atacante es conectarse al Perfil de Transferencia de Archivos (OBEX File Transfer), disponible en el canal 11 y acceder a archivos almacenados en el teléfono.

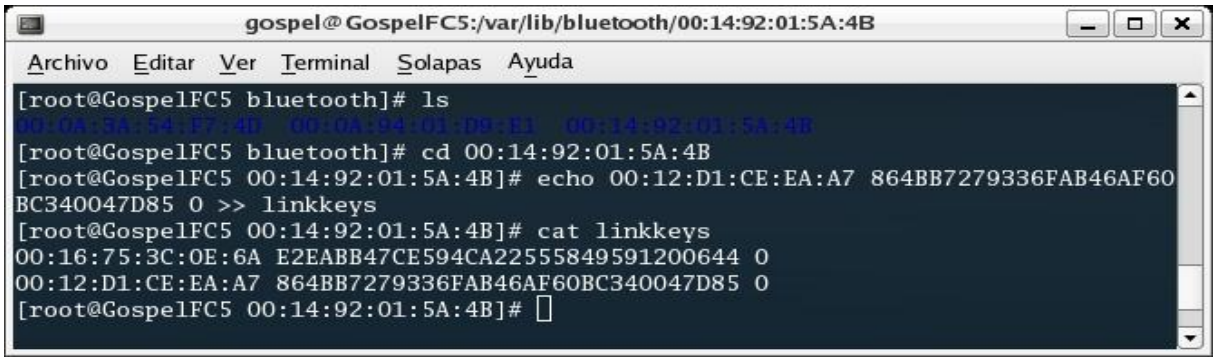


Inicialmente, si el atacante intenta conectarse al Perfil de Transferencia de Archivos, al tratarse de un equipo no autenticado, se lanza el proceso de emparejamiento de dispositivos con intercambio de clave PIN.

Para evitar el mecanismo de autenticación, el atacante puede suplantar la identidad de la PDA a partir de su dirección BD_ADDR y la clave de enlace obtenida tal y como se ha visto en el anterior escenario con el *Motorola PEBL*.

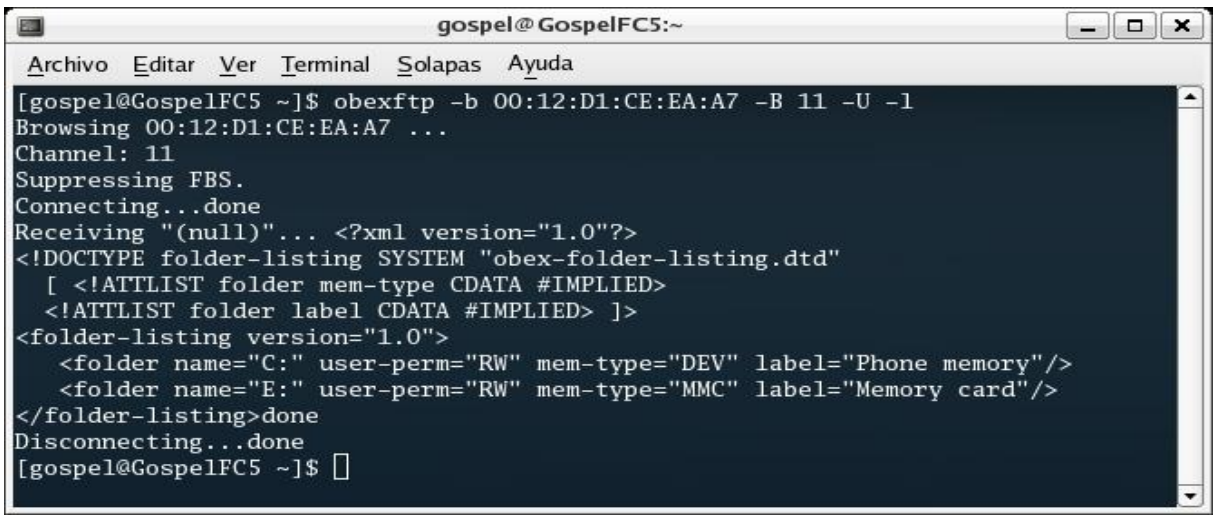


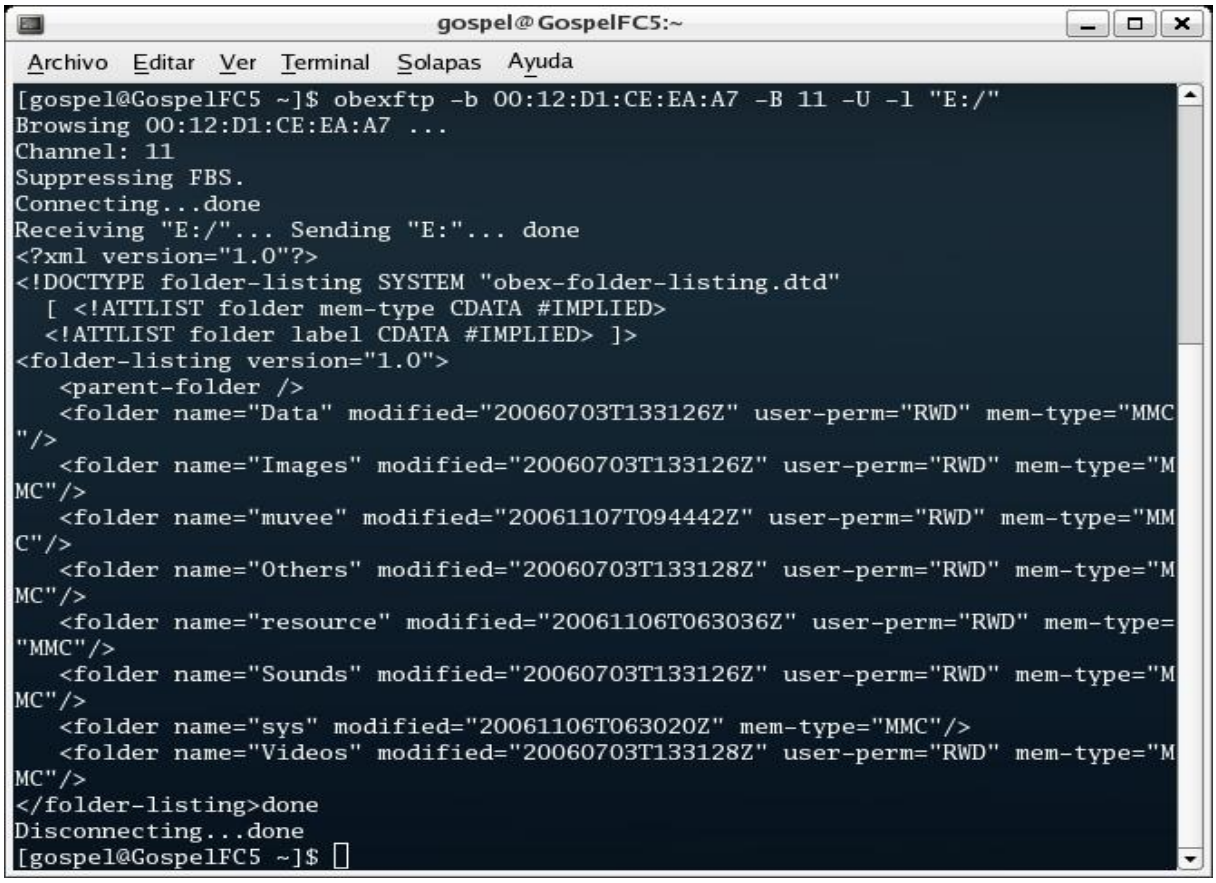




A partir de ese momento, el atacante está en disposición de conectarse al Perfil de Transferencia de Archivos del teléfono móvil de forma transparente y llevar a cabo las siguientes acciones:

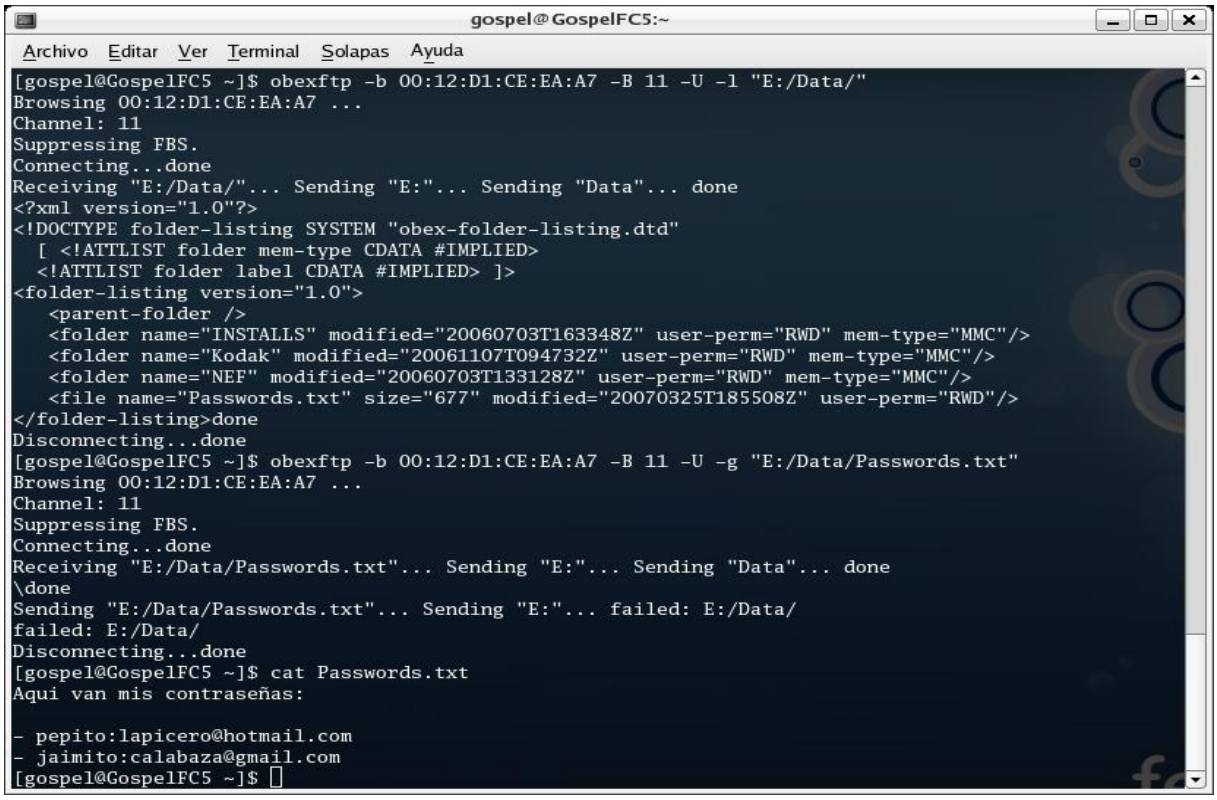
Listar los archivos y recorrer los directorios.



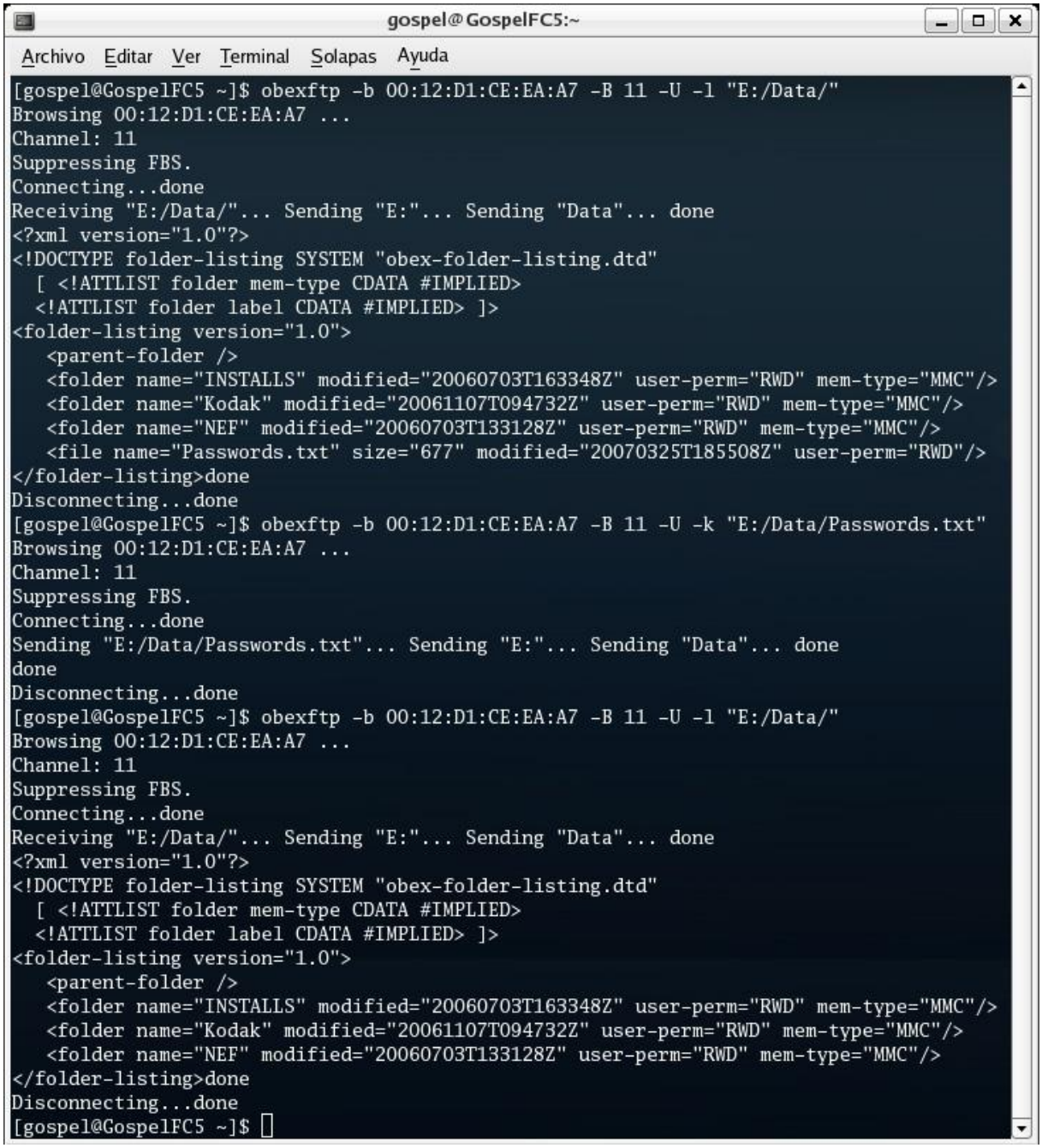

gospel@GospelFC5:~
Archivo Editar Ver Terminal Solapas Ayuda
[gospel@GospelFC5 ~]$ obexftp -b 00:12:D1:CE:EA:A7 -B 11 -U -l "E:/"
Browsing 00:12:D1:CE:EA:A7 ...
Channel: 11
Suppressing FBS.
Connecting...done
Receiving "E:/"... Sending "E:"... done
<?xml version="1.0"?>
<!DOCTYPE folder-listing SYSTEM "obex-folder-listing.dtd"
[<!ATTLIST folder mem-type CDATA #IMPLIED>
<!ATTLIST folder label CDATA #IMPLIED>]>
<folder-listing version="1.0">
<parent-folder />
<folder name="Data" modified="20060703T133126Z" user-perm="RWD" mem-type="MMC
"/>
<folder name="Images" modified="20060703T133126Z" user-perm="RWD" mem-type="M
MC"/>
<folder name="muvee" modified="20061107T094442Z" user-perm="RWD" mem-type="MM
C"/>
<folder name="Others" modified="20060703T133128Z" user-perm="RWD" mem-type="M
MC"/>
<folder name="resource" modified="20061106T063036Z" user-perm="RWD" mem-type=
"MMC"/>
<folder name="Sounds" modified="20060703T133126Z" user-perm="RWD" mem-type="M
MC"/>
<folder name="sys" modified="20061106T063020Z" mem-type="MMC"/>
<folder name="Videos" modified="20060703T133128Z" user-perm="RWD" mem-type="M
MC"/>
</folder-listing>done
Disconnecting...done
[gospel@GospelFC5 ~]$


gospel@GospelFC5:~
Archivo Editar Ver Terminal Solapas Ayuda
[gospel@GospelFC5 ~]$ obexftp -b 00:12:D1:CE:EA:A7 -B 11 -U -l "E:/Images/200703/"
Browsing 00:12:D1:CE:EA:A7 ...
Channel: 11
Suppressing FBS.
Connecting...done
Receiving "E:/Images/200703/"... Sending "E:"... Sending "Images"... Sending "200703"... done
<?xml version="1.0"?>
<!DOCTYPE folder-listing SYSTEM "obex-folder-listing.dtd"
[<!ATTLIST folder mem-type CDATA #IMPLIED>
<!ATTLIST folder label CDATA #IMPLIED>]>
<folder-listing version="1.0">
<parent-folder />
<file name="10032007001.jpg" size="1012872" modified="20070310T115944Z" user-perm="RWD"/>
<file name="25032007012.jpg" size="868327" modified="20070325T203648Z" user-perm="RWD"/>
</folder-listing>done
Disconnecting...done
[gospel@GospelFC5 ~]$

Descargarse archivos.



Eliminar archivos



CONCLUSIONES

La principal consecuencia que se deduce del ataque ***Blue MAC Spoofing*** es que si la seguridad de un equipo PC o PDA resulta comprometida, también puede verse comprometida la seguridad de aquellos teléfonos móviles Bluetooth emparejados con ese equipo.

If your box gets owned, your phone may, too.

En este artículo se ha demostrado que las claves de enlace almacenadas en PDAs con Windows Mobile 5.0 y pila de protocolos Bluetooth Broadcom/Widcomm están en texto claro. Se sabe que en Linux y MAC OS X también se almacenan en texto claro. Por el contrario, las claves de enlace almacenadas en equipos con Windows 2000, XP y Vista están cifradas en el registro y actualmente se está trabajando para conseguir mediante ingeniería inversa el algoritmo que permita obtener claves en texto claro. Depende de la pila de protocolos Bluetooth propietaria, pero es cuestión de tiempo…

SOLUCIÓN DE SEGURIDAD

En este documento se ha demostrado lo trivial que resulta suplantar la identidad de un dispositivo Bluetooth con el fin de acceder a otro utilizando sus credenciales. 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 ***Blue MAC Spoofing*** 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.

En el caso de modificar la especificación de Bluetooth e implementar otros mecanismos de seguridad más robustos, los nuevos dispositivos fabricados serían incompatibles con los que actualmente se encuentran en el mercado, lo cual generaría un conflicto de interoperabilidad.

Se puede afirmar, por tanto, que no existe una solución a corto plazo y que, mientras tanto, todos los equipos fabricados que implementen tecnología Bluetooth seguirán siendo vulnerables a este ataque.

Mi consejo es no 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, mi consejo es realizar un emparejamiento de nuevo cada vez que se vaya a producir la comunicación y eliminar el enlace al final de la misma. En el caso de conexiones frecuentes con un mismo dispositivo, se puede mantener el enlace activo, siempre que el dispositivo esté bajo nuestro control o resulte difícil para un atacante extraer las claves de enlace de tal equipo, como, por ejemplo, un Manos Libres.

Avisados quedáis… 

Alberto Moreno Tablado

Madrid, 4 de Mayo de 2007