Taddong

Seguridad en Bluetooth

To Blue, or Not to Blue: That is the Question

Raúl Siles

FIST – Fiberparty 2010

26 febrero 2010

2010 © Taddong S.L. Todos los derechos reservados

Taddong

www.taddong.com

Raúl Siles
Founder & Senior Security Analyst

Índice

- Tecnologías Bluetooth
- Seguridad en el estándar Bluetooth
- Amenazas y vulnerabilidades en Bluetooth
- Ataques contra manos libres Bluetooth:
  - Descubriendo el lado oculto…
  - Captura e inyección de audio
- Recomendaciones de seguridad y defensas

2010 © Taddong S.L. Todos los derechos reservados

Dedicado a …

Imágenes de pitufos: www.smurf.com

2010 © Taddong S.L. Todos los derechos reservados

Tecnologías Bluetooth

- Comunicaciones inalámbricas personales
- Movilidad, flexibilidad, sencillez, etc
- Interoperabilidad
- Sustituir los cables: USB, serie, paralelo…
- Bajo consumo y bajo coste
- Ausencia de infraestructuras:
  - ¿Quién tiene el control?

2010 © Taddong S.L. Todos los derechos reservados

Especificación Bluetooth

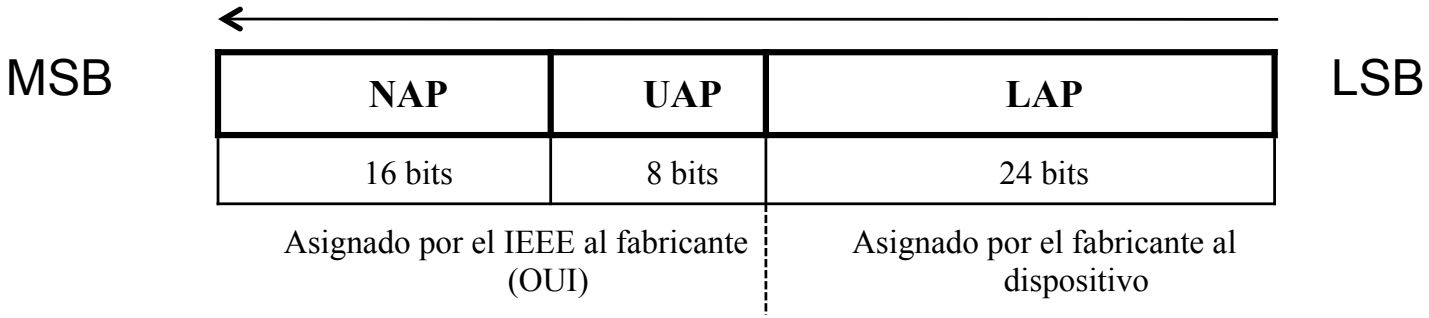
- Radio frecuencia: rango sin licencia
  - 2,402 a 2,480 Ghz (79 canales de 1 Mhz)
  - FHSS (1600 saltos/segundo)
- Estándar IEEE 802.15.1 (v2.1 ó v3.0)
- Clase de dispositivo: 1, 2 ó 3
  - Distancia ≈ +100, 10 ó 1 m (100-1 mW)
- Ancho de banda: +2,1 Mbps ó 24Mbps

http://www.ieee802.org/15/

2010 © Taddong S.L. Todos los derechos reservados

Dirección del dispositivo

- BD_ADDR
  - Bluetooth Device ADDRess
- 48 bits (6 bytes) ≈ MAC 802
- Empleada en el patrón de salto
- Empleada como algo **secreto**



2010 © Taddong S.L. Todos los derechos reservados

Seguridad en el estándar Bluetooth

- Patrón de salto (BD_ADDR y reloj)
  - BD_ADDR no está en las cabeceras
- Modos de seguridad: 1, 2 y 3 (LMP)
- Autentificación:
  - PIN
  - Claves de enlace
- Autorización: acceso/confirmación usuario
- Cifrado: E0

2010 © Taddong S.L. Todos los derechos reservados

Amenazas y vulnerabilidades en Bluetooth

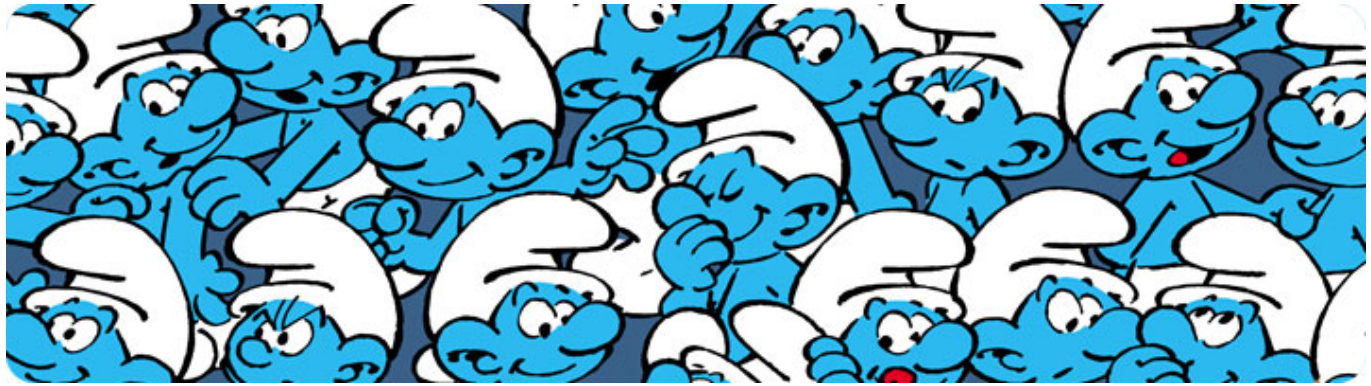
- Privacidad:
  - Comunicaciones
  - Almacenamiento
  - Dispositivos
- Objetivos
  - Móviles
  - Manos libres, teclados, etc

- Disp. visibles
- Rango de señal
- Suplantación
- Bluesnarfing, bluebugging, blueline, etc
- Captura tráfico
- PIN cracking…

Curso de dos días de seguridad en Bluetooth

2010 © Taddong S.L. Todos los derechos reservados

Ataques contra manos libres y auriculares Bluetooth



2010 © Taddong S.L. Todos los derechos reservados

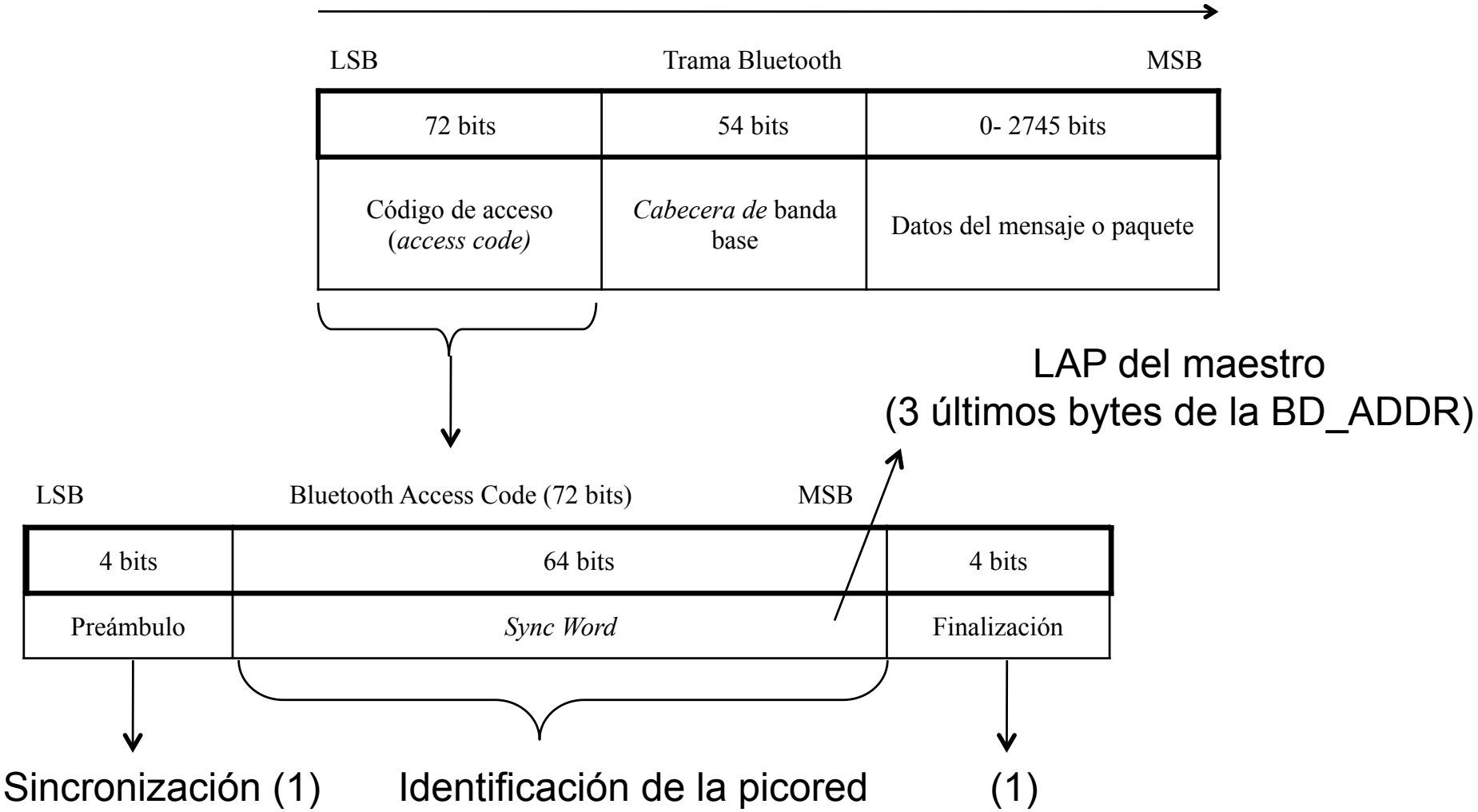
Descubriendo el lado oculto…

- Dispositivos Bluetooth ocultos:
  - Adivinación de la BD_ADDR
  - Fue visto previamente
  - Emparejamiento inicial
  - Combinación de tecnologías: WiFi & BT
  - Fuerza bruta sobre la BD_ADDR (2^{48})
  - ★ Obtención de parte de la BD_ADDR mediante captura de tráfico

Toda la seguridad de algunos dispositivos (auriculares o manos libres) está basada en la ocultación de la BD_ADDR: ¿PIN?

2010 © Taddong S.L. Todos los derechos reservados

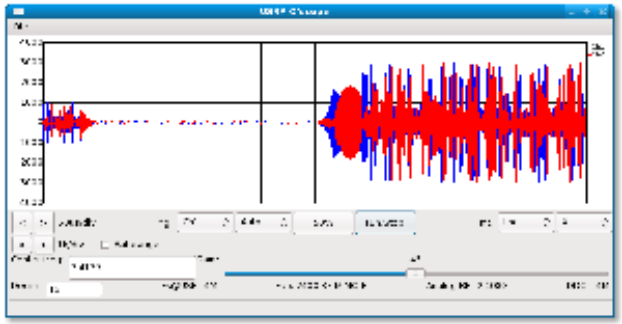
Obtención del LAP…

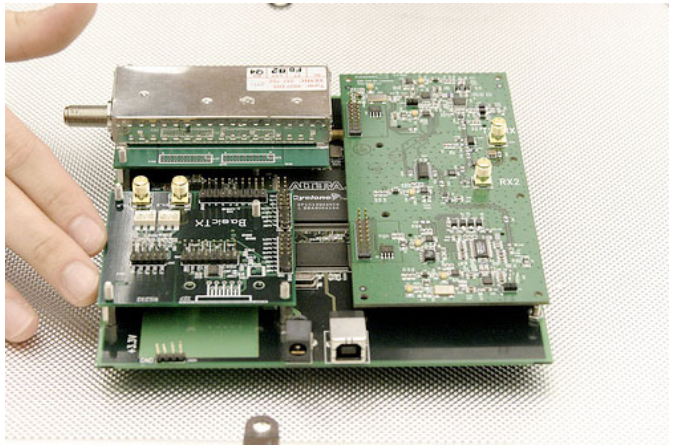


2010 © Taddong S.L. Todos los derechos reservados

USRP, GNU-Radio, gr-bluetooth, y el proyecto BNAP-BNAP

- USRP: Universal SW Radio Peripheral
- GNU-Radio: radio definida por SW
- Pila Bluetooth (D. Spill & A. Bittau)
- Proyecto BNAP-BNAP (J. Wright)
- BTScanner: parche para LAP





2010 © Taddong S.L. Todos los derechos reservados

Captura e inyección de audio en auriculares y manos libres

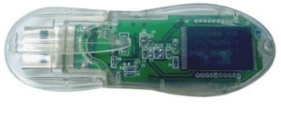
- Auriculares y manos libres
  - Dispositivos ocultos
  - PIN por defecto y fijo
- Si conoces el PIN… y descubres la BD_ADDR…
- Carwhisperer
  - Captura
  - Inyección

2010 © Taddong S.L. Todos los derechos reservados

Recomendaciones de seguridad y defensas

2010 © Taddong S.L. Todos los derechos reservados

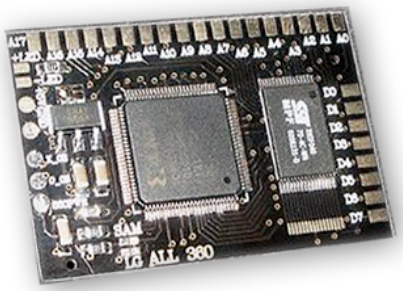
Uso de Bluetooth en las organizaciones



2010 © Taddong S.L. Todos los derechos reservados

Decálogo de recomendaciones (1)

1. ¡Apágalo! ¡Salvemos el planeta!
2. Dispositivo oculto o no visible
3. Habilitar sólo los perfiles necesarios (¿?)
4. Habilitar autentificación & autorización
5. Cambiar los valores por defecto:
   - Marca y modelo, propietario, etc
6. Actualizar software y firmware



2010 © Taddong S.L. Todos los derechos reservados

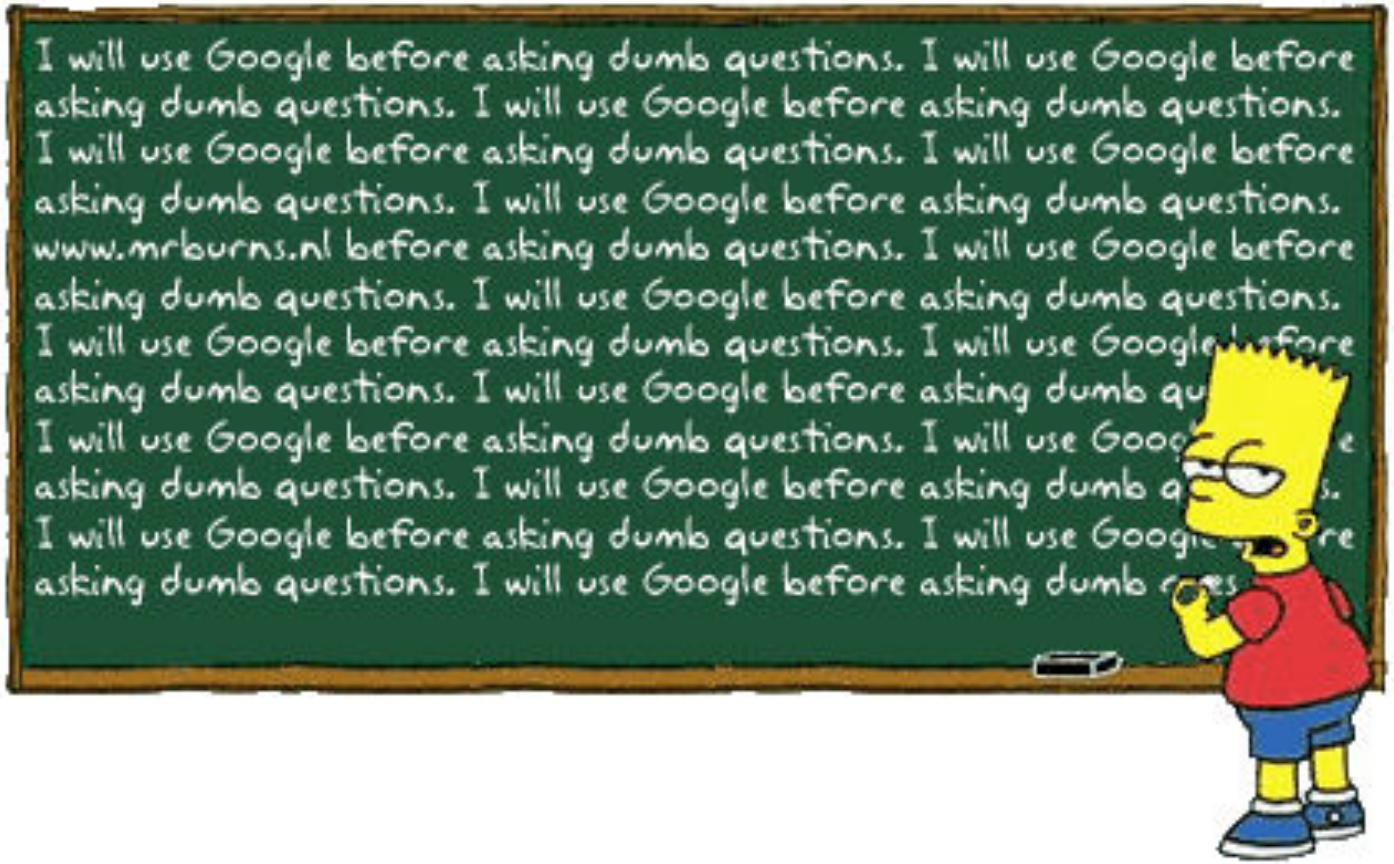
Decálogo de recomendaciones (2)

7. Uso en entornos peligrosos
   - Emparejamiento inicial
8. Selección del PIN y renovación
9. Intentos de conexión no solicitados
   - Marketing de proximidad
10. Gestión de la BD de dispositivos emparejados (… y ¡borrado!)

Dispositivos y uso autorizados, inventario, configuración por defecto, auditorías, pruebas de intrusión…

2010 © Taddong S.L. Todos los derechos reservados

¿Preguntas? ☺



2010 © Taddong S.L. Todos los derechos reservados

Taddong

www.taddong.com

raul@taddong.com