Bluetooth Security

Why bother?

Talking about

- What is Bluetooth?
- Basic look at Bluetooth device address
- Vulnerabilities in Bluetooth devices
- Types of attacks (passive, active)
- Recommendations

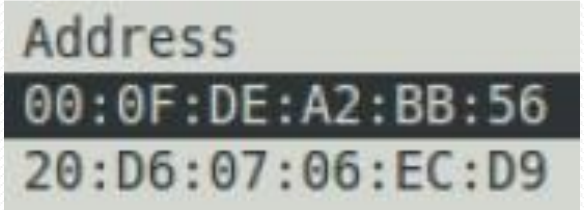
What is Bluetooth?

- Wireless communications technology
- Operates at the 2.4 GHz Industrial, Scientific and Medical (ISM) band
- Frequency Hopping (FH)
- Not line of sight
- Usually ranges up to 30 meters
- Managed by the Bluetooth Special Interest Group (Bluetooth SIG)

Bluetooth Device Address

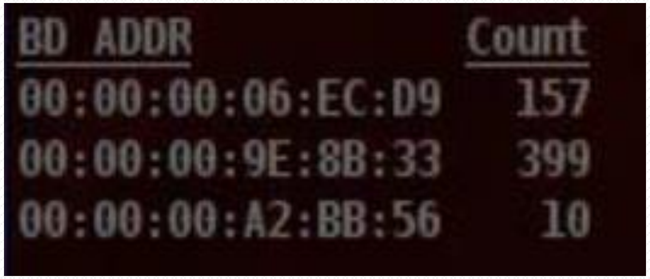
- All Bluetooth have a Bluetooth Device Address (BD_ADDR 48 bits)
    - NAP – Non-significant Address Part 16 bits
    - UAP – Upper Address Part 8 bits
    - LAP – Lower Address Part 24 bits
- Uniquely identifies the device
- Can be picked up off the air

Bluetooth Device Address 2



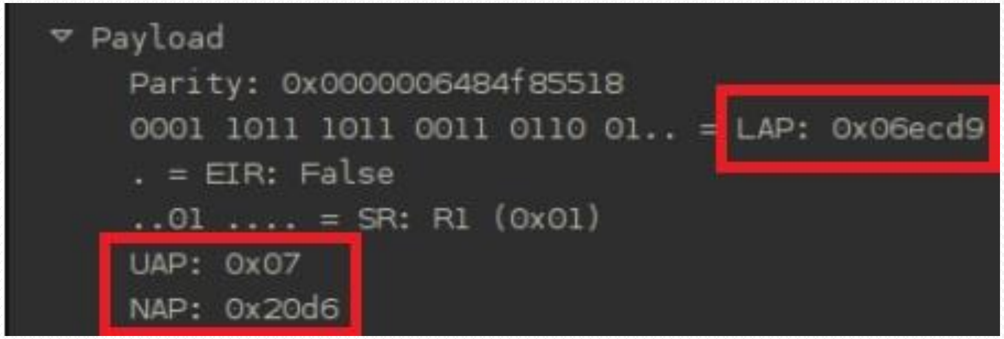
```
Address
00:0F:DE:A2:BB:56
20:D6:07:06:EC:D9
```

BTScanner picks up devices’ BD_ADDRs



```
BD_ADDR              Count
00:00:00:06:EC:D9      157
00:00:00:9E:8B:33      399
00:00:00:A2:BB:56       10
```

Packets captured with Kismet



```
▿ Payload
    Parity: 0x0000006484f85518
    0001 1011 1011 0011 0110 01.. = LAP: 0x06ecd9
    . = EIR: False
    ..01 .... = SR: R1 (0x01)
    UAP: 0x07
    NAP: 0x20d6
```

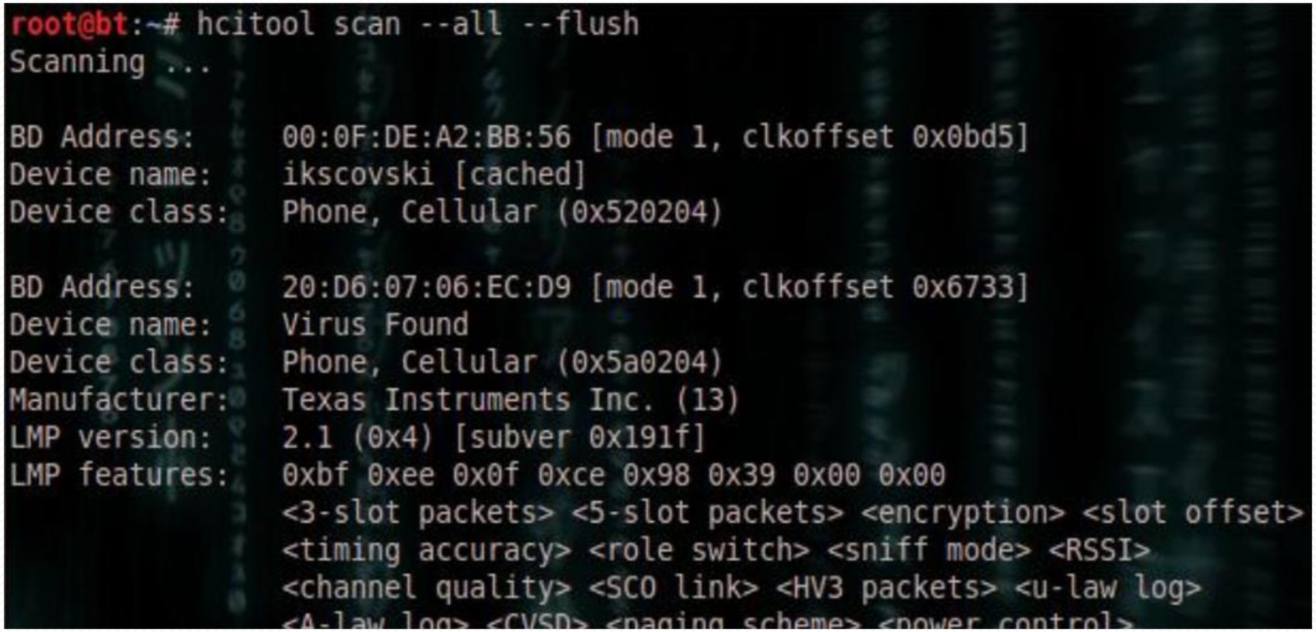
BD_ADDR seen in wireshark. A Frequency Hop Synchronisation occurred revealing the BD_ADDR

Vulnerabilities

- Depends on the Bluetooth version on the device
- Once the device is discoverable it can be attacked
- No user Authentication
- Default Settings
- Short PIN Codes (v2.1)
- Man-In-The-Middle attacks (v2.1, v3.0)
- Bluetooth headsets can be tricked into communicating with an illegitimate device.

Passive Attacks

- Carried out to gather information from Bluetooth devices



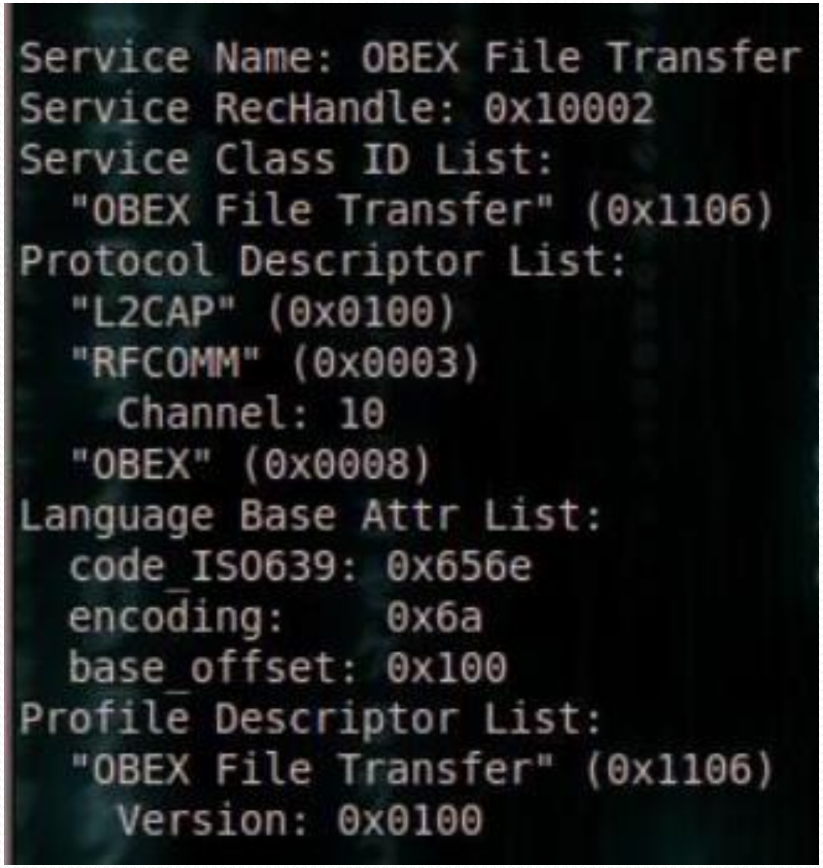
```
root@bt:~# hcitool scan --all --flush
Scanning ...

BD Address:      00:0F:DE:A2:BB:56 [mode 1, clkoffset 0x0bd5]
Device name:     ikscovski [cached]
Device class:    Phone, Cellular (0x520204)

BD Address:      20:D6:07:06:EC:D9 [mode 1, clkoffset 0x6733]
Device name:     Virus Found
Device class:    Phone, Cellular (0x5a0204)
Manufacturer:    Texas Instruments Inc. (13)
LMP version:     2.1 (0x4) [subver 0x191f]
LMP features:    0xbf 0xee 0x0f 0xce 0x98 0x39 0x00 0x00
                 <3-slot packets> <5-slot packets> <encryption> <slot offset>
                 <timing accuracy> <role switch> <sniff mode> <RSSI>
                 <channel quality> <SCO link> <HV3 packets> <u-law log>
                 <A-law log> <CVSD> <paging scheme> <power control>
```

HCI tool used to gather information on device

Passive Attacks continued



```
Service Name: OBEX File Transfer
Service RecHandle: 0x10002
Service Class ID List:
  "OBEX File Transfer" (0x1106)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
    Channel: 10
  "OBEX" (0x0008)
Language Base Attr List:
  code_ISO639: 0x656e
  encoding:    0x6a
  base_offset: 0x100
Profile Descriptor List:
  "OBEX File Transfer" (0x1106)
    Version: 0x0100
```

SDP (Service Detection Protocol) tool picks up services on the device

Active Attacks

- Man-In-The-Middle
- Bluesnarf
- Car whisper

Why bother with Bluetooth Security?

- To a hacker, a little piece of information can go a long way
- Skilled hackers can retrieve entire contact list from off the phone along with other personal information
- Privacy is important
- Remember the CIA (Confidentiality, Integrity and Availability)
- They are cyber devices too.

So what do we do?

- Run and hide? I can’t see them so they can’t see me

So what do we do 2?

- Switch off Bluetooth when not in use
- Set device to hidden or invisible
- Minimise the amount of devices you need to pair with
- When pairing devices, do it privately
- Do not accept pairing or files from unknown devices
- Remove paired devices that are no longer needed
- Change default settings on devices

Sources of information

- NIST publications
- Bluetooth Special Interest Group https://www.bluetooth.org