Do It Yourself Bluetooth Sniffer

a 20 min walkthrough

Kaept'n Karacho

May 16, 2007

WARNING!

(This can totally brick your hardware.)

Software

- Frontline Test Equipment FTS4BT
- Free Download: `http://www.fte.com`
- Serial Number (depends on BDADDR)
- Install!

Supported BT-Dongle

Needed

- BT-Dongle: CSR BC4 EXT or FLASH
- Chipset needs flash memory: internal or external
- BC4 for EDR sniffing

Should work

- Fujitsu Siemens - Amazon ASIN: B000CNF1CM
- Cellink BTA-6030 - Amazon ASIN: B000C6K070

Supported?

```
# hciconfig hciX revision
hciX:   Type: USB
        BD Address: 00:13:DE:AD:BE:AF ACL MTU: 0:0
SCO MTU: 0:0
        Build 3683
        Chip version: BlueCore4-External
        Max key size: 56 bit
        SCO mapping:  HCI
```

Firmware exchange

Tools

- dfutool - update firmware
- bccmd - modify firmware settings

both available via bluez-cvs

CVS checkout

- modules: libs, utils

```
# cvs -d:pserver:anonymous:cvs.bluez.org:/cvsroot\\
/bluez login
# cvs -d:pserver:anonymous:cvs.bluez.org:/cvsroot\\
/bluez co -P $module
```

Compile & install

```
# ./bootstrap
# ./configure --enable-all
# make
# make install
```

Backup your firmware

```
# dfutool -d hciX archive backup.dfu
```

Upgrade your firmware

- firmware (only for BC4): $InstallDirWindows/Bluetooth ComProbe Firmware/airsniffer52b4.dfu

```
# dfutool -d hciX update airsniffer52b4.dfu
```

Frontline software checks for vendor id and product id!

Backup settings

```
# bccmd -d hciX pslist -s 0x000f > pskey_backup
```

Where is PSI?

```
# bccmd -d hciX memtypes
psi (0x0001) = EEPROM (1)
psf (0x0002) = EEPROM (1)
psram (0x0008) = RAM (transient) (2)
```

Change product id

```
# bccmd -d hciX psget -s 0x000f 0x02bf
USB product identifier: 0x0001 (1)
# bccmd -d hciX psset -s 0x0002 0x02bf 0x0002
# bccmd -d hciX psget -s 0x000f 0x02bf
USB product identifier: 0x0002 (2)
```

Change vendor id (often optional)

```
# bccmd -d hciX psget -s 0x000f 0x02be
USB vendor identifier: 0x0bf8 (3064)
# bccmd -d hciX psset -s 0x0002 0x02be 0x0a12
# bccmd -d hciX psget -s 0x000f 0x02be
USB vendor identifier: 0x0a12 (2578)
```

Did everything work?

```
# bccmd -d hciX coldreset
# lsusb
Bus 002 Device 010: ID 0a12:0002 Cambridge
Silicon Radio, Ltd Bluetooth Dongle (HCI mode)
```

Now reboot (Windows). BTW, you could have done everything using Windows and the Casira tools.

Run the Sniffer

- run "Bluetooth ComProbe Maintenance Utility" and press "Check Configuration" button
- you are now READY TO SNIFF!!!11
- run "Air (Basic)"