WoWWee MiP

Arnaud RAMEY

March 24, 2015

Contents

joost.damad.be safaribooksonline

0.1 Discover all primary services

1 Install bluez v5.3

TODO

http://www.bluez.org/download/ → bluez-5.27.tar.xz

bluez 5.27 :

```
$ sudo apt-get install libdbus-1-dev libudev-dev libical-dev
Error : "checking systemd system unit dir... configure: error: systemd system
   ↪ unit directory is required"
```

http://askubuntu.com/questions/343663/ubuntu-13-04-and-bluez-5-8-configure-error-systemd-system-unit-directory-is-re

```
$ ./configure --prefix=/usr --mandir=/usr/share/man --sysconfdir=/etc --
   ↪ localstatedir=/var --enable-experimental --with-systemdsystemunitdir=/lib/
   ↪ systemd/system --with-systemduserunitdir=/usr/lib/systemd
$ make
```

2 XPeria developer options

For people who are facing problems in accessing developer settings here's the trick

Go to Settings → About phone

Tap on the build number 7 times

Enjoy developer options

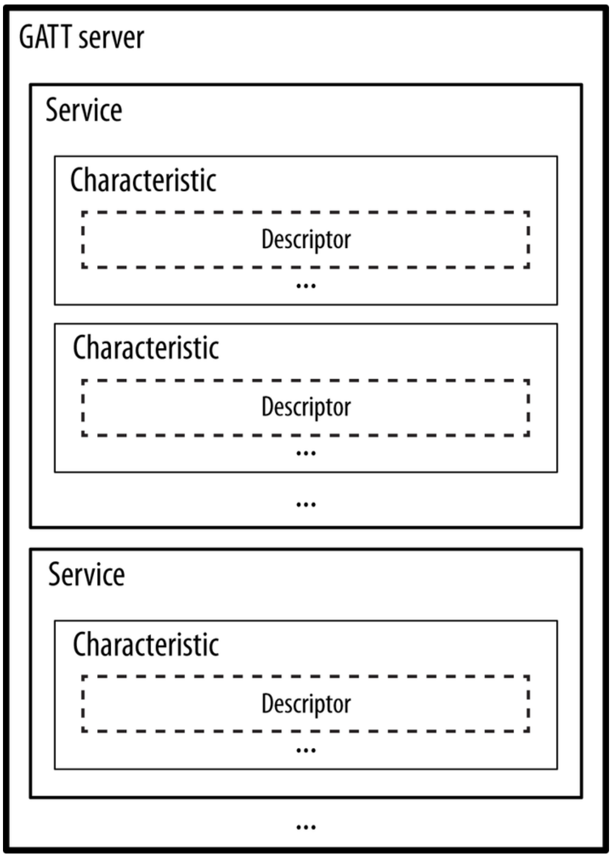

Figure 1: Data structures of GATT

3 Using bluetooth device

```
$ hciconfig
Devices:
  hci1  00:1A:7D:DA:71:11
```

Resetting Bluetooth (from ubuntu-fr.org) :

```
$ sudo rfkill unblock all
$ sudo hciconfig hci1 up

$ sudo hcitool -i hci1 lescan
D0:39:72:B7:AF:66 (unknown)
D0:39:72:B7:AF:66 Bubi
```

4 Connecting to MiP

```
$ sudo gatttool -i hci1 -b D0:39:72:B7:AF:66 -I
> connect
```

Get handles:

```
http://www.jaredwolff.com/blog/get-started-with-bluetooth-low-energy/
http://i-miss-erin.blogspot.fr/2010/12/gatttool-in-bluez-over-bredr.html
```

```
> primary
attr handle: 0x0011, end grp handle: 0x0014 uuid: 0000ffe5-0000-1000-8000-00805
    ↪ f9b34fb
Send Data Service: 0xFFE5
attr handle: 0x000c, end grp handle: 0x0010 uuid: 0000ffe0-0000-1000-8000-00805
    ↪ f9b34fb
Receive Data Service: 0xFFE0
```

4.1 Discover characterstics

```
> characteristics
handle: 0x0012, char properties: 0x0c, char value handle: 0x0013, uuid: 0000ffe9
    ↪ -0000-1000-8000-00805f9b34fb
Send Data WRITE Characteristic: 0xFFE9
handle: 0x000d, char properties: 0x10, char value handle: 0x000e, uuid: 0000ffe4
    ↪ -0000-1000-8000-00805f9b34fb
Receive Data NOTIFY Characteristic: 0xFFE4
```

4.2 Discover All Characteristic Descriptors

```
> char-desc
```

5 Sending orders

References:

- WowWeeLabs
- MiP-BLE-Protocol
- Command doc

LEDs are characteristics;

```
serviceId: MIPSendDataService,   ffe5
characteristicId: MIPSendDataWrite,   ffe9
value: SetChestLED;  0x84 r g b
```

Set head LED:

```
> char-write-cmd 0x0013 8A0202020201
```

Sounds:

```
> char-write-cmd 0x0013 0602

> char-read-hnd 0x000e
> char-write-cmd 0x0013 780060
```

Set volume:

```
char-write-cmd 13 1501
```

6 Reading infos

https://stackoverflow.com/questions/25536695/wowwee-mip-command-over-bluetooth-in-linux-shell-with-gatttool
http://www.compulab.co.il/utilite-computer/forum/viewtopic.php?f=77&t=1639
Read LED:

```
char-write-cmd <handle> value
> char-read-hnd 0x83
```

Get firmware version:

```
> char-write-cmd 0x0013 14
Notification handle = 0x000e value: 31 34 30 45 30 33 31 36 30 32
```

Translating thanks to rapidtables:

```
31 34 30 45 30 33 31 36 30 32 > 140E031602
```

Now parse each pair of consecutive chars : it is a int written in hex format, convert into decimal format:

```
14:20 0E:14 03:03 16:22 02:02
```

The first int corresponds to the calling code: here $0x14$ for the firmware version.

Non interactive: http://www.humbug.in/2014/using-gatttool-manualnon-interactive-mode-read-ble-devices/

```
$ sudo gatttool -i hci0 -b D0:39:72:B7:AF:66 --char-write-req -a 0x0013 -n 14 --listen
Characteristic value was written successfully
Notification handle = 0x000e value: 31 34 30 45 30 33 31 36 30 32

$ timeout .3 gatttool -i hci0 -b D0:39:72:B7:AF:66 --char-write-req -a 0x0013 -n 14 --listen
Characteristic value was written successfully
Notification handle = 0x000e value: 31 34 30 45 30 33 31 36 30 32
```

Cut after two lines: https://superuser.com/questions/402979/kill-program-after-it-outputs-a-given-line-from-a-shell-script

Combine both:

```
timeout 1 gatttool -i hci1 -b D0:39:72:B7:AF:66 --char-write-req -a 0x0013 -n 14 --listen | grep -m 1 "value:"
```

7 Gatttool example

https://gitorious.org/bluez/moreira-bluez-mainline/raw/0831238284de7dcf994bf9e2c350bb9acdc959e2:attrib/gatttool.c

http://people.csail.mit.edu/albert/bluez-intro/c404.html