AppSec Labs Ltd.
info@appsec-labs.com
https://appsec-labs.com

R U aBLE?
BLE Application Hacking

Bluetooth®
NOT SO SMART

Tal Melamed
Application Security Expert
Tal@AppSec-Labs.com

OWASP Israel

- What is BLE?
- BLE security
- BLE pairing
- Discovering services
- Cloning the device
- BLE MitM
- Available tools
- What's next?

about://me

- Tech Lead @ AppSec Labs

  Tal@AppSec-Labs.com
- Application Security Expert
- Follow me @ appsec.it
- https://github.com/nu11p0inter
- http://sl.owasp.org/talmelamed

amdocs
embrace challenge
experience success

Check Point
SOFTWARE TECHNOLOGIES LTD.

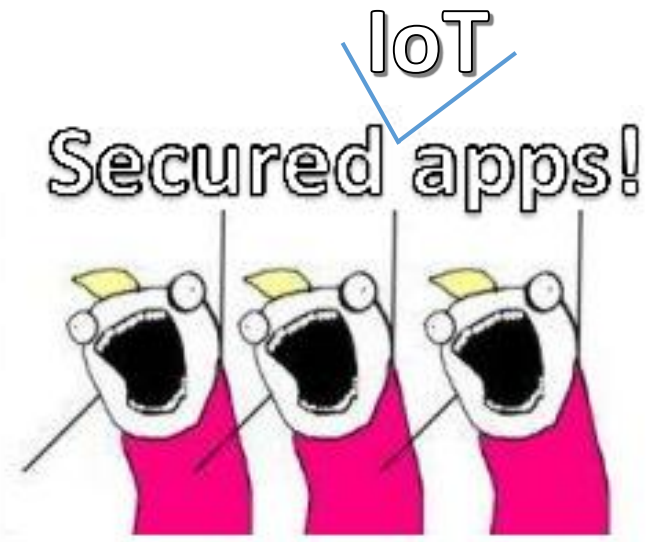
RSA
The Security Division of EMC

OWASP Israel

AppSec Labs

AppSec Application security Labs

https://appsec-labs.com/



OWASP Israel

AppSec Labs

Industry vectors:

AppSec Labs provides its high end services to the following industry vectors:

- High Tech software development
- Banking and financing
- National security
- **IoT**
- Cloud
- Pharmaceuticals
- Commerce
- Travel and transport
- IT Security products
- Biometrics
- Education
- Gaming
- Government
- Telecommunications

amdocs
AVG
LIVEPERSON
Taboola
intel
HITB
Hewlett Packard Enterprise
TEVA
NCR
bmc
RESURGENS ATLANTA GA
black hat
at&t
AXA
Cellcom
888.com
IAI
MOTOROLA
Akamai
DEFCON
NTT
bank hapoalim
NYU Langone MEDICAL CENTER
WiX
VERINT
RAFAEL
OWASP Israel

Before we start

- AppSec Labs – Securing the IoT
  - Sounds like a buzz
  - PenTesting RF Operated Devices, OWASP 2016
  - Azure IoT partner
  - https://appsec-labs.com/iot-security/
- What we offer?
  - SDLC, Training, Penetration-testing, Consulting
- This presentation is a result of a preliminary research on BLE security and part of a wide research for IoT Security

What is BLE?

- Bluetooth Low Energy
  - a.k.a Bluetooth Smart, part of Bluetooth 4
  - Designed to be power-efficient
  - Claimed to operate “month to years” on a single battery
  - Significantly smaller and cheaper.
  - Operates at 2.4 GHz (same as Bluetooth Classic)
  - Short range (<100m)
- Low cost and ease of implementation lead BLE to be widely used among IoT devices and applications
- Used among medical, industrial and government equipment
  - Wearables, sensors, lightbulbs, medical devices, and many other smart-products.
- 48 billion IoT devices expected by 2021, and Bluetooth—predicted to be in nearly one-third of those devices

To save you some questions

- BLE vs BT Classic
  - Different architecture (Master-Slave)
  - Different modulation parameters
  - Different channels
  - Different channel-hopping scheme
  - Different packet format
  - Different packet whitening

Where is the risk?

TECHNOLOGY NEWS | Tue Oct 4, 2016 | 3:58pm EDT

J&J warns diabetic patients: Insulin pump vulnerable to hacking

And for me?

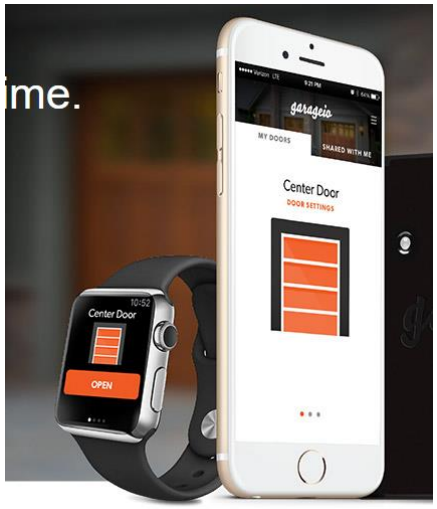
- OMG, your baby has 41° -
  take him to the hospital!

- Your blood sugar is way up. You should get your insulin…

Ok, medical but…

What else?

- Opens the Garage door

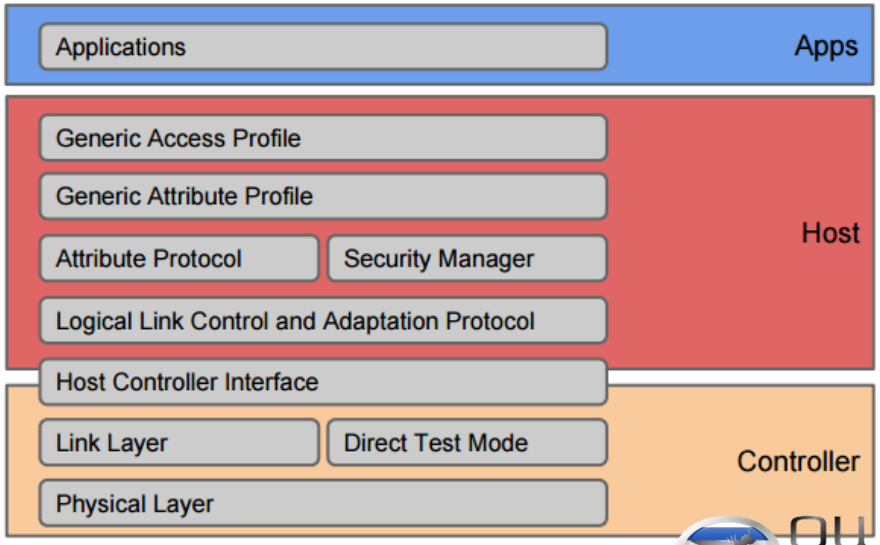


- Are you drunk?

- Possibly anything!

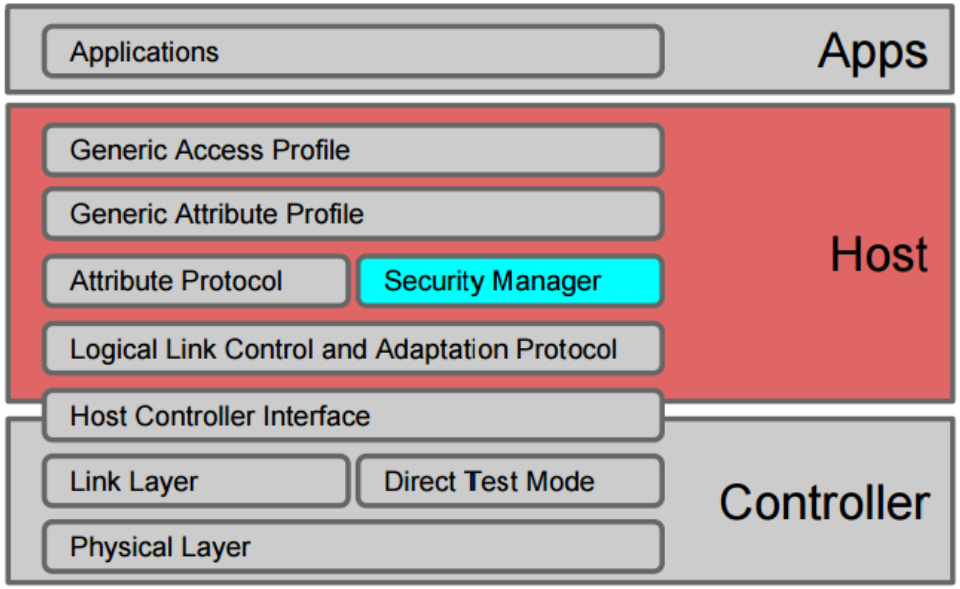
BLE Architecture

- Apps
  - Applications are built on top
  - Interacts with host layer only
  - Different API's depending on the application environment
- Host
  - Sits on top of the Radio
  - Provides API to applications
- Controller
  - Radio Control
  - Connection Linking
  - Radio Testing
  - Interface to Host



BLE Security - Security Manager

- Three phase process on connection
  - Pairing feature exchange
  - Short term key generation
  - Transport specific key distribution
- Implements a number of cryptographic functions
- Memory and processing requirements are lower for responding (saves power)

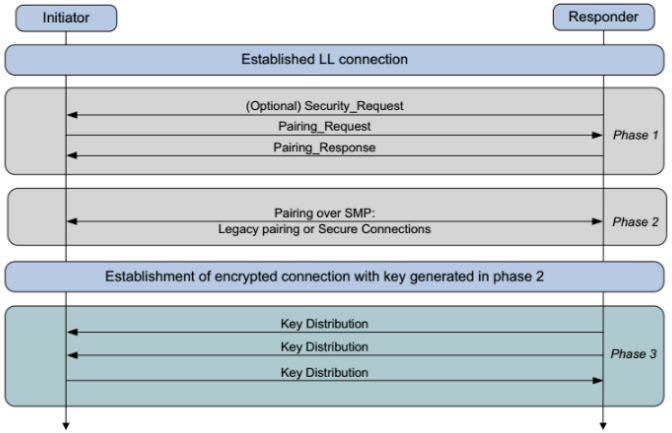


BLE Security

- Uses AES-128 with CCM encryption engine
- Uses Key Distribution to share various keys
  - Identity Resolving Key is used for privacy
  - Signing Resolving Key provides fast authentication without encryption
  - Long Term Key is used
- Pairing encrypts the link using a Temporary Key (TK)
  - Derived from passkey
  - Then distribute keys
- Asymmetric key model
  - Slave gives keys to master with a diversifier
  - Slave can then recover keys from the diversifier

BLE Security: Pairing

- Performed to establish keys in order to encrypt a link.
- The keys can be used to encrypt a link in future reconnections, verify signed data, or perform random address resolution.
- 3-phase for paring
  - Pairing Feature Exchange
  - Short Term Key (STK) Generation (legacy pairing)
  - Long Term Key (LTK) Generation (Secure Connections)
  - Transport Specific Key Distribution



BLE Security: Pairing

- How to determine the temporary key (TK)?
  - **Just Works**
    - Legacy, most common
    - Devices without display cannot implement other
    - Its actually a key of zero, that's why it just works...
  - **6-digit PIN**
    - In case the device has a display
    - 1m options (BFable)
  - **Out of band (OOB)**
    - Does not share secret key over the 2.4 GHz band (used by protocol)
    - Makes use of other mediums (e.g. NFC)
    - Once secret keys are exchanged, encrypts the channel
    - Not common (understatement – haven't seen one yet)

- "None of the pairing methods provide protection against a passive eavesdropper" -Bluetooth Core Spec

Why not DH?

" A future version of this specification will include elliptic curve cryptography and Diffie-Hellman public key exchanges…"

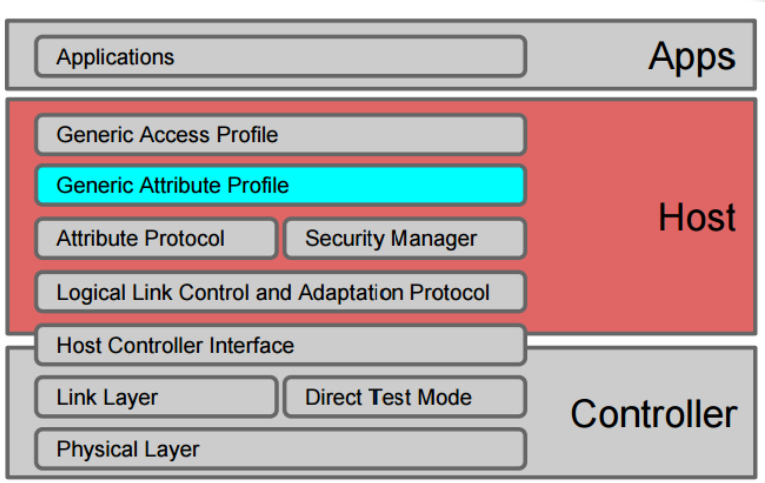
- Well, that's too bad, I already bought the device!

So? Is it secure or not?

- In practice, ~80% of tested devices do not implement BLE-layer encryption
- Mobile apps cannot control the pairing (OS level)
- Why?
  - As always, security is left behind (cost, time, etc.)
  - Multiple users/apps using the same devices
  - Access sharing
  - Backups to the cloud
  - Public access devices (e.g. cash register)
  - Hardware, software or even UX compatibilities/requirements

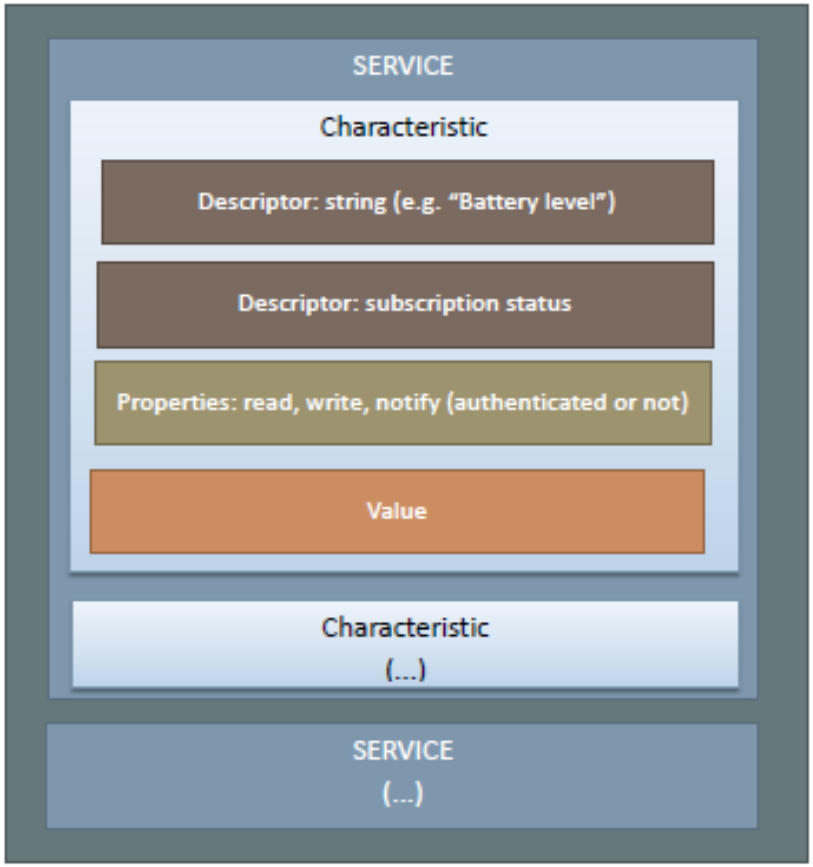
GATT

- Generic Attribute Profile (GATT) used by BLE to communicate with each other
- Client Server Architecture
  - Built on top of ATT (Attribute Protocol)
  - GATT Server stores data using ATT
  - GATT Server accepts ATT requests to serve and save attributes
- Organized in data objects
  - Profiles
  - Services
  - Characteristics

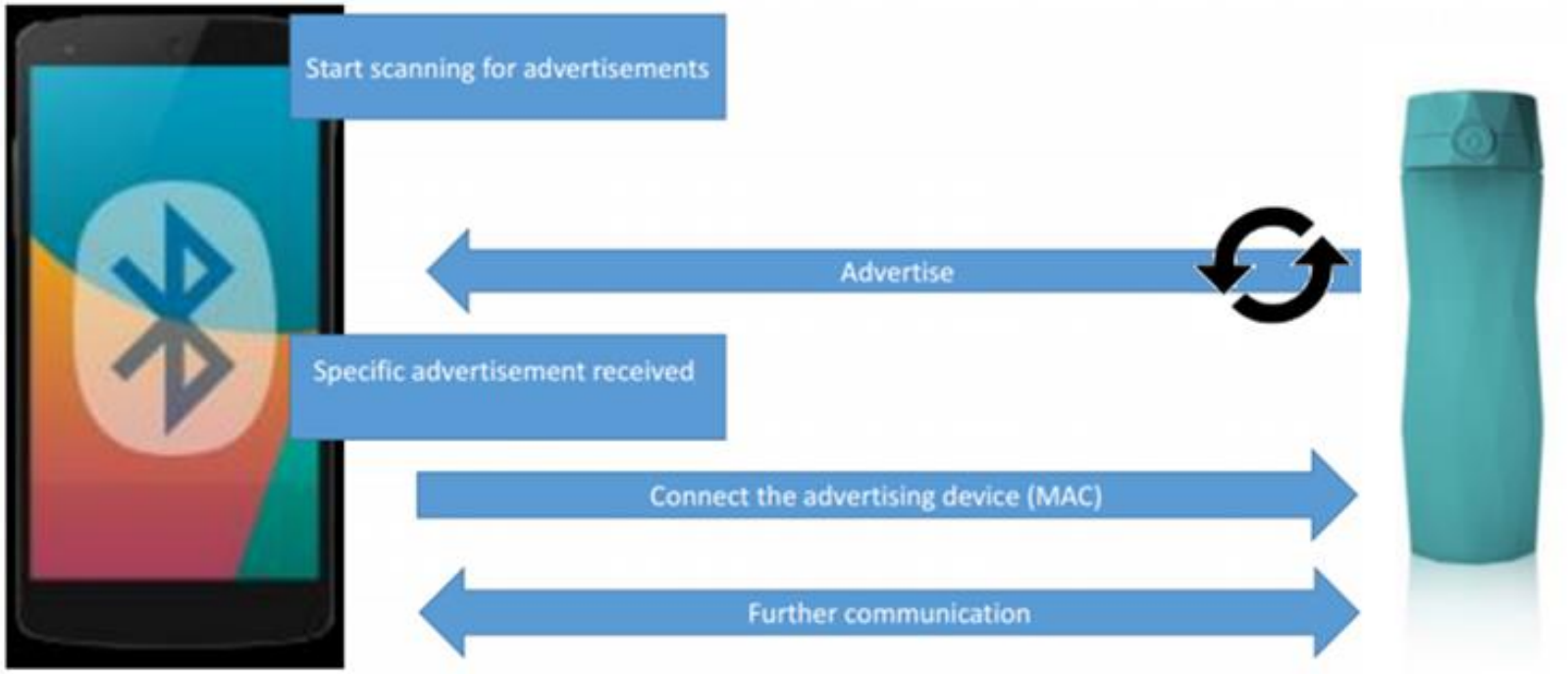


GATT

- Services & characteristic are identified by an associated UUID
- A characteristic contains a single value (“attribute”)
  - Can be read, written to or subscribed for notifications

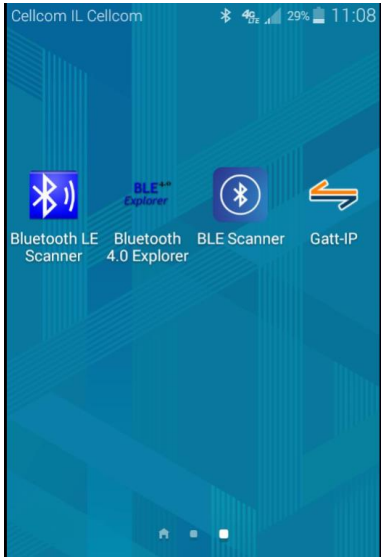


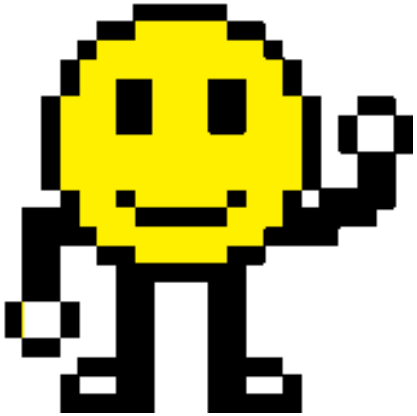
Typical flow



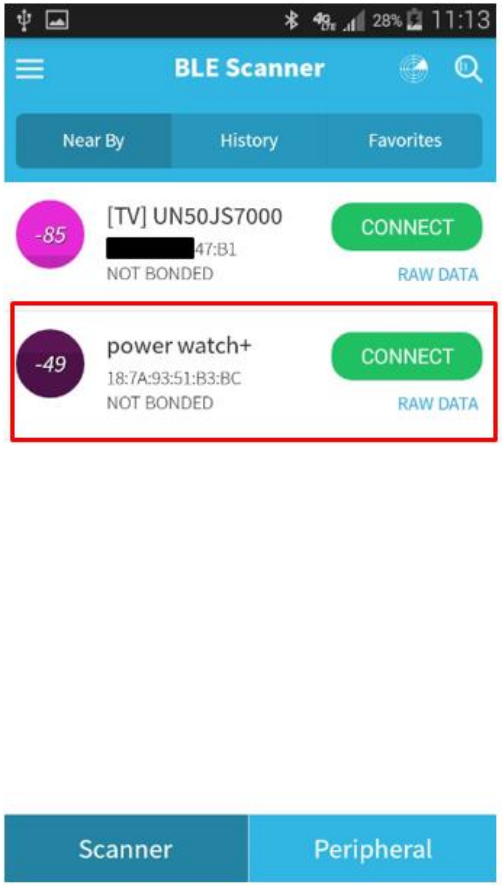
How does that work?

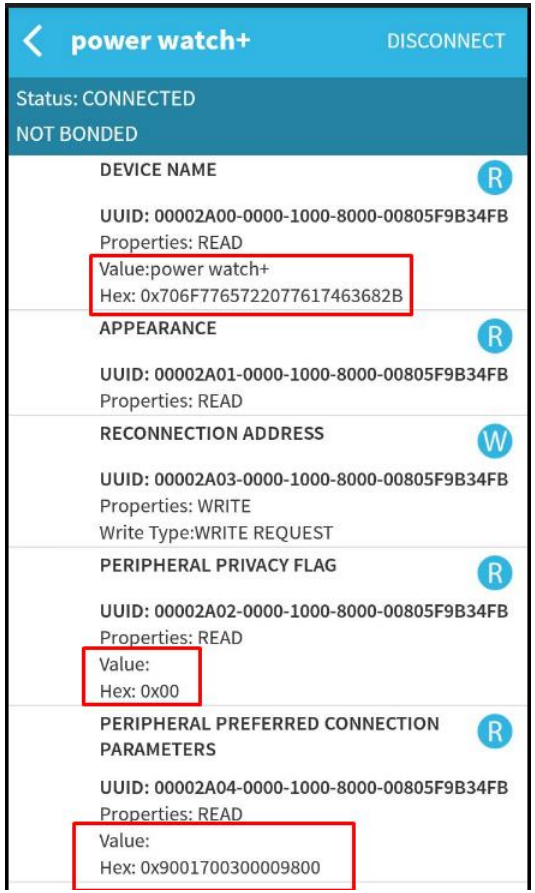
Hello everyone!
I am a BLE device
and these are my services





Discovering Services





BLE cmd basics

- # hciconfig hci0 up/down/reset
- # hcitool lescan
- # hcidump -x -t hci0

```
root@AppSecLabs:~# hciconfig
hci0:   Type: BR/EDR  Bus: USB
        BD Address: 00:22:D0:B9:6D:B2  ACL MTU: 310:10  SCO MTU: 64:8
        UP RUNNING
        RX bytes:13854 acl:0 sco:0 events:389 errors:0
        TX bytes:3721 acl:0 sco:0 commands:150 errors:0

root@AppSecLabs:~# hcitool lescan
LE Scan ...
F8:04:2E:87:47:B1 (unknown)
F8:04:2E:87:47:B1 (unknown)
18:7A:93:51:B3:BC (unknown)
18:7A:93:51:B3:BC power watch+
F8:04:2E:87:47:B1 (unknown)
```

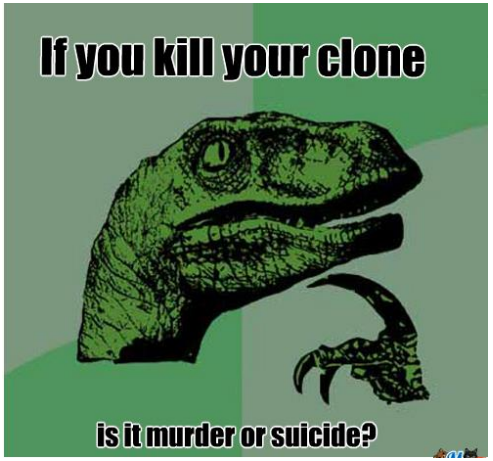
gatttool

```
root@AppSecLabs:~# gatttool --device=18:7A:93:51:B3:BC --interactive
[18:7A:93:51:B3:BC][LE]> connect
Attempting to connect to 18:7A:93:51:B3:BC
Connection successful
[18:7A:93:51:B3:BC][LE]> characteristics
handle: 0x0002, char properties: 0x02, char value handle: 0x0003, uuid: 00002a00-0000-1000-8000-00805f9b34fb
handle: 0x0004, char properties: 0x02, char value handle: 0x0005, uuid: 00002a01-0000-1000-8000-00805f9b34fb
handle: 0x0006, char properties: 0x08, char value handle: 0x0007, uuid: 00002a03-0000-1000-8000-00805f9b34fb
handle: 0x0008, char properties: 0x02, char value handle: 0x0009, uuid: 00002a02-0000-1000-8000-00805f9b34fb
handle: 0x000a, char properties: 0x02, char value handle: 0x000b, uuid: 00002a04-0000-1000-8000-00805f9b34fb
handle: 0x000d, char properties: 0x22, char value handle: 0x000e, uuid: 00002a05-0000-1000-8000-00805f9b34fb
handle: 0x0011, char properties: 0x02, char value handle: 0x0012, uuid: 00002a25-0000-1000-8000-00805f9b34fb
handle: 0x0014, char properties: 0x02, char value handle: 0x0015, uuid: 00002a29-0000-1000-8000-00805f9b34fb
handle: 0x0017, char properties: 0x02, char value handle: 0x0018, uuid: 00002a23-0000-1000-8000-00805f9b34fb
```

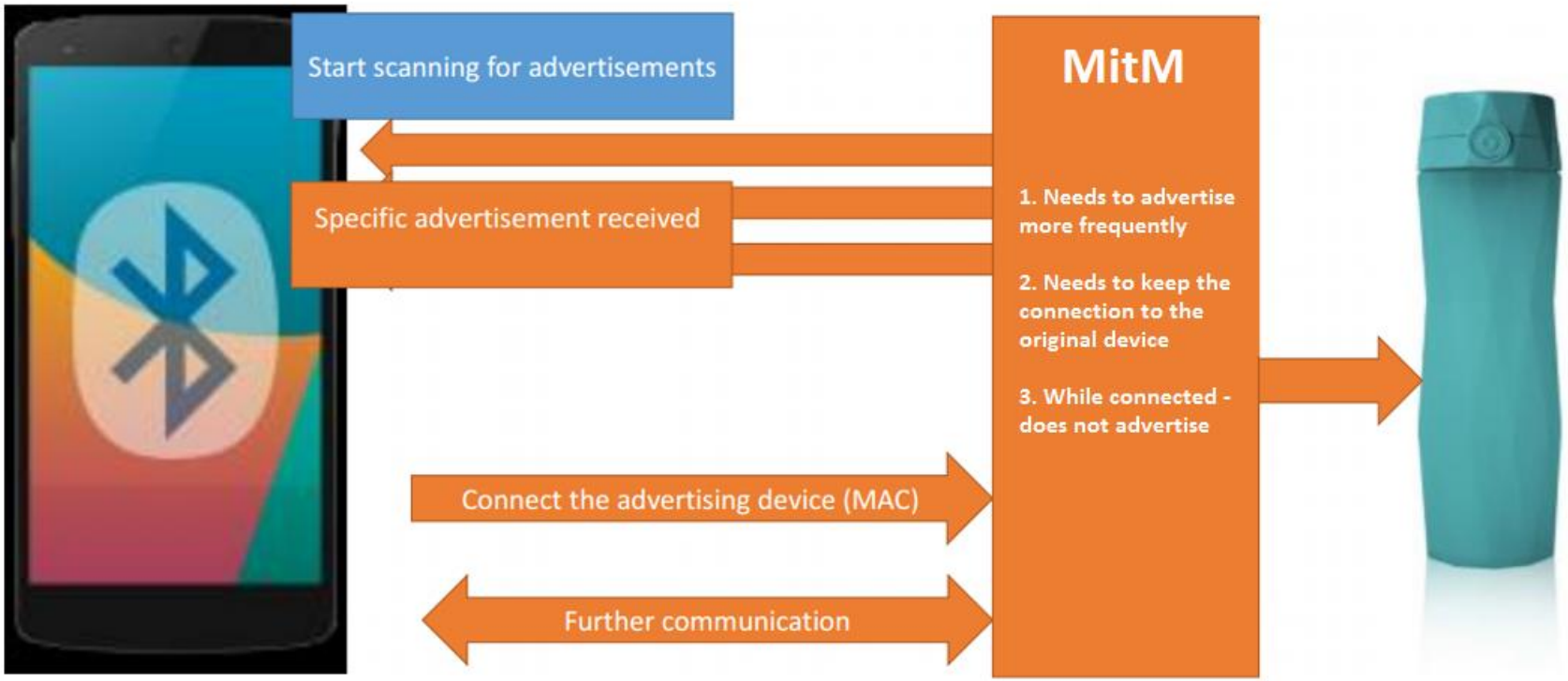
```
[18:7A:93:51:B3:BC][LE]> char-read-uuid 0000fff5-0000-1000-8000-00805f9b34fb
handle: 0x0048   value: 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12
[18:7A:93:51:B3:BC][LE]>
[18:7A:93:51:B3:BC][LE]> char-read-hnd 0x0047
Characteristic value/descriptor: 02 48 00 f5 ff
[18:7A:93:51:B3:BC][LE]>
[18:7A:93:51:B3:BC][LE]> char-write-cmd 0x0007 0100
[18:7A:93:51:B3:BC][LE]> char-write-req 0x0007 2609000358000001000000059 -listen
Error: Characteristic Write Request failed: Attribute value length is invalid
[18:7A:93:51:B3:BC][LE]>
[18:7A:93:51:B3:BC][LE]> char-write-req 0x0007 0100 -listen
Characteristic value was written successfully
[18:7A:93:51:B3:BC][LE]>
```

Cloning the device

- Scan devices
- Listen to advertisements
- Clone
- Advertise cloned services
- Let client connect to your “fake device”.
- MitM!



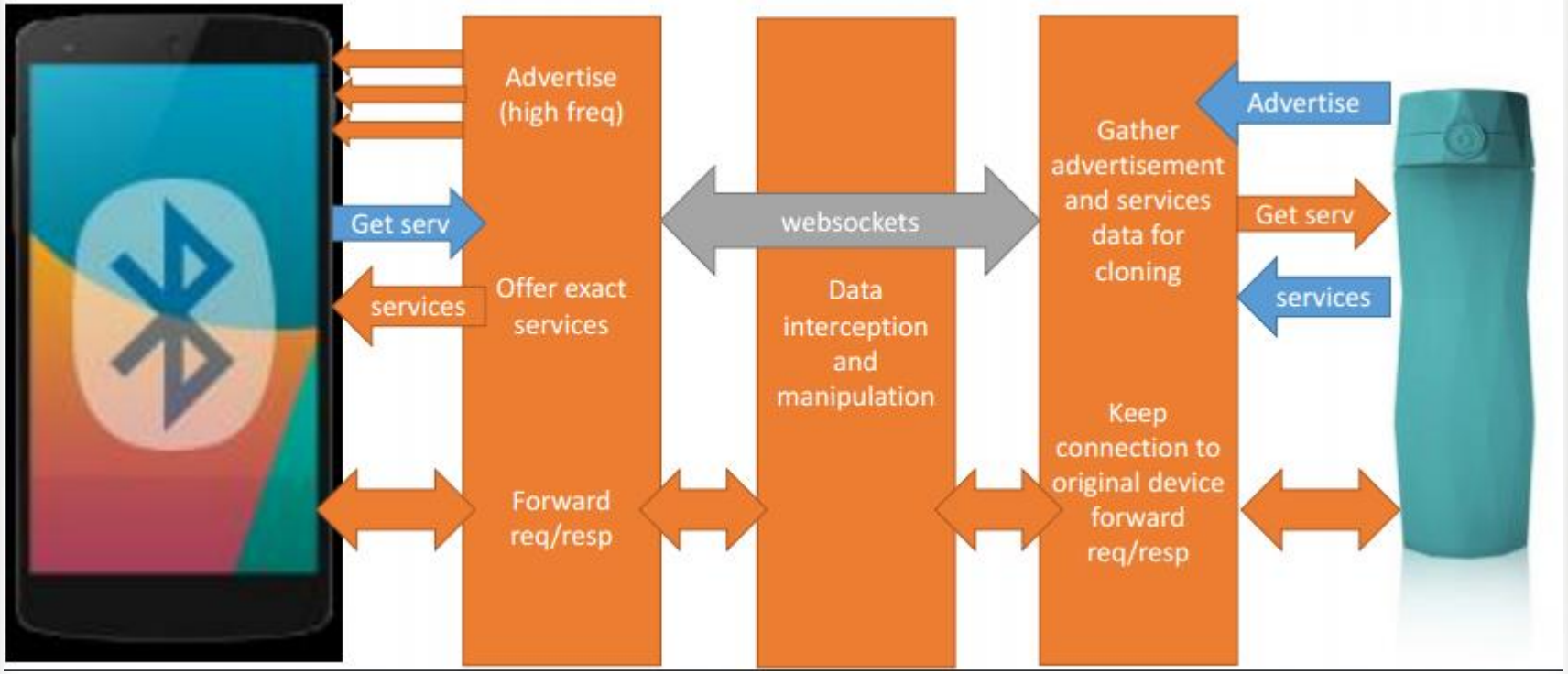
Normal MitM


Start scanning for advertisements
Specific advertisement received
MitM
1. Needs to advertise more frequently
2. Needs to keep the connection to the original device
3. While connected - does not advertise
Connect the advertising device (MAC)
Further communication

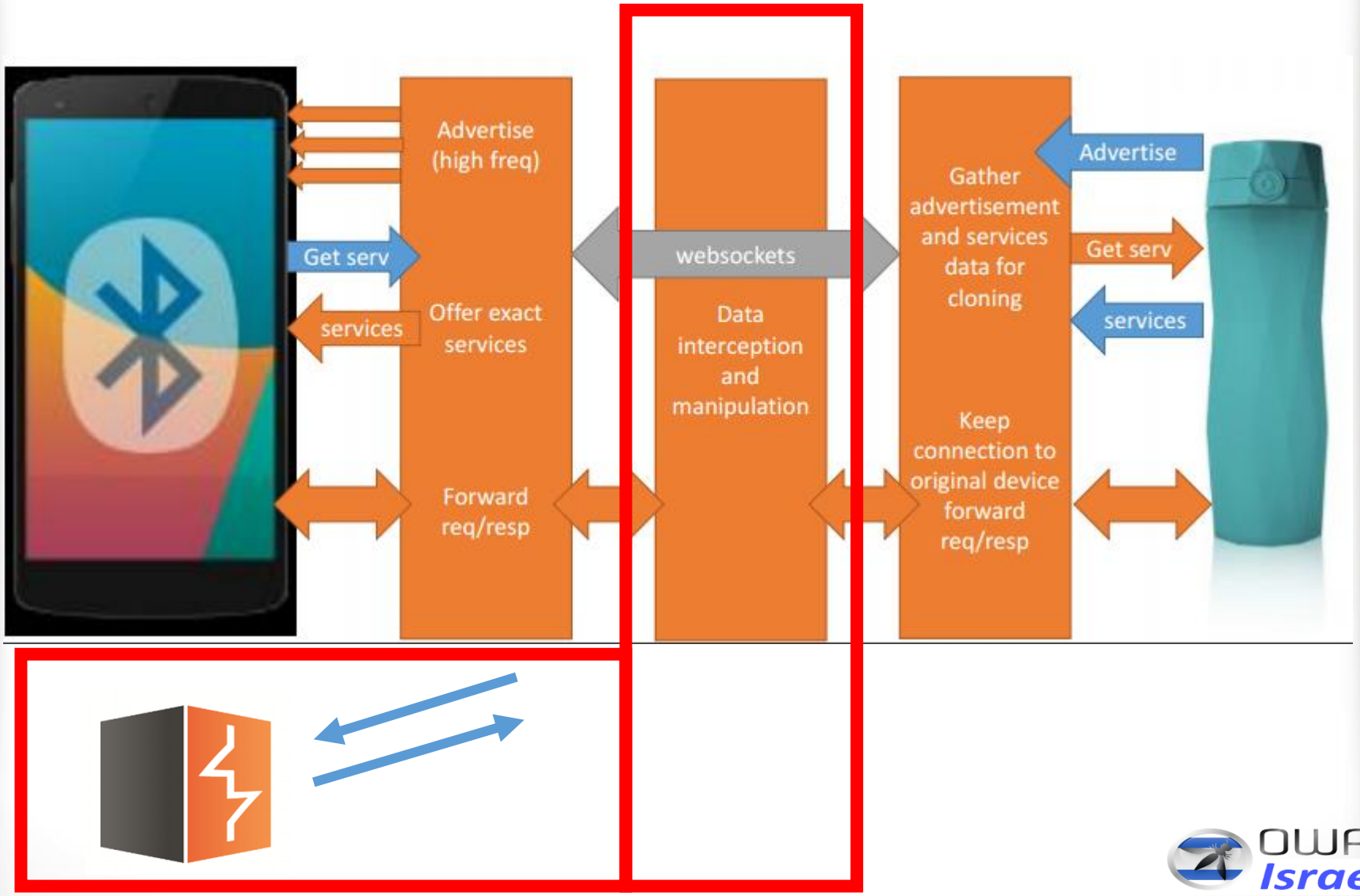
What do we need?

- CSR 4.0 dongle x2
  - One will service as the client
  - The other as the server
  - $2.70 in aliexpres

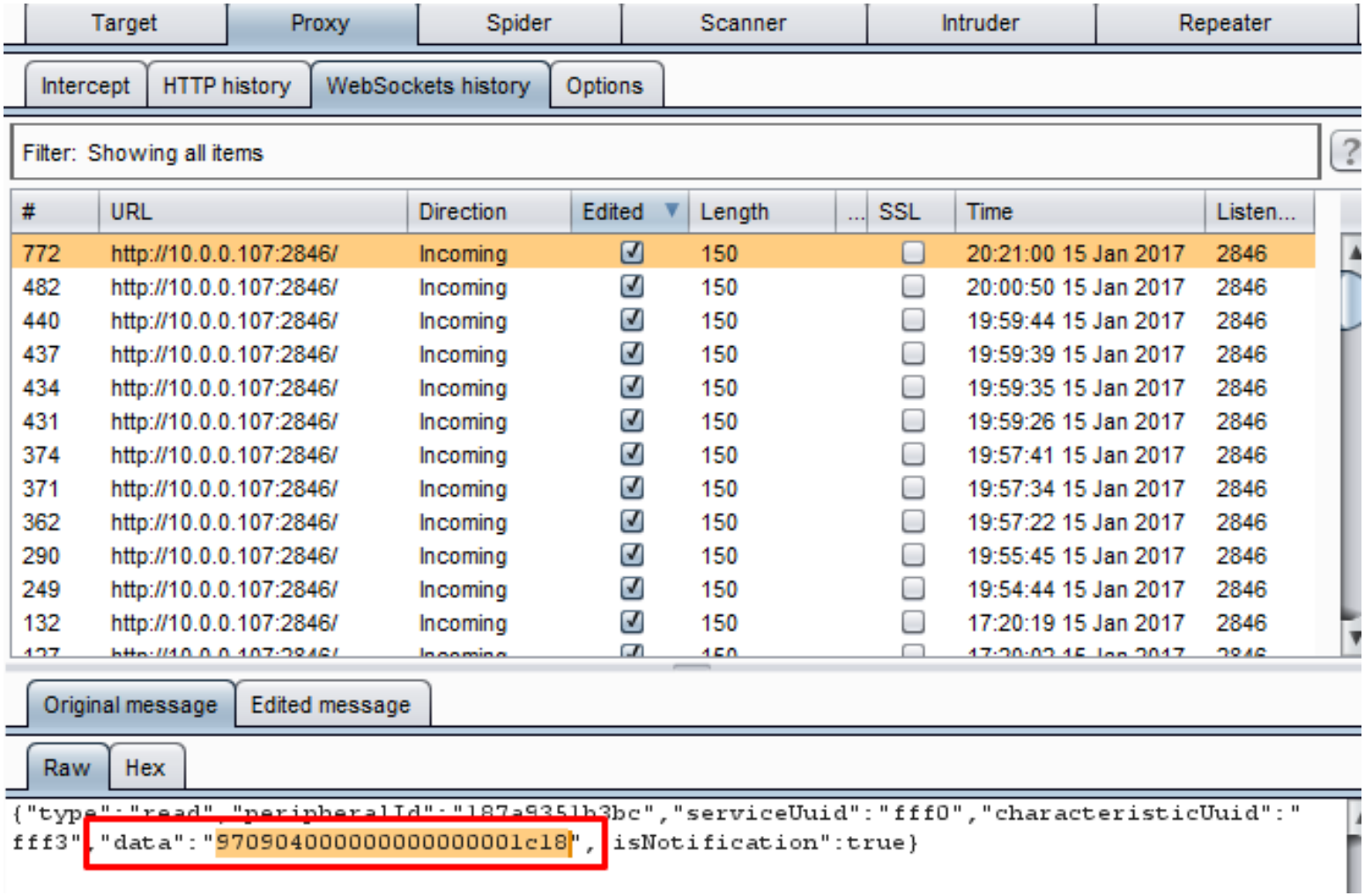
Desired MitM for BLE



Tampering


Advertise
(high freq)
Get serv
services
Offer exact
services
Forward
req/resp
websockets
Data
interception
and
manipulation
Gather
advertisement
and services
data for
cloning
Keep
connection to
original device
forward
req/resp
Advertise
Get serv
services

Tampering with data using Burp



gattacker

- BLE (Bluetooth Low Energy) security assessment using Man-in-the-Middle

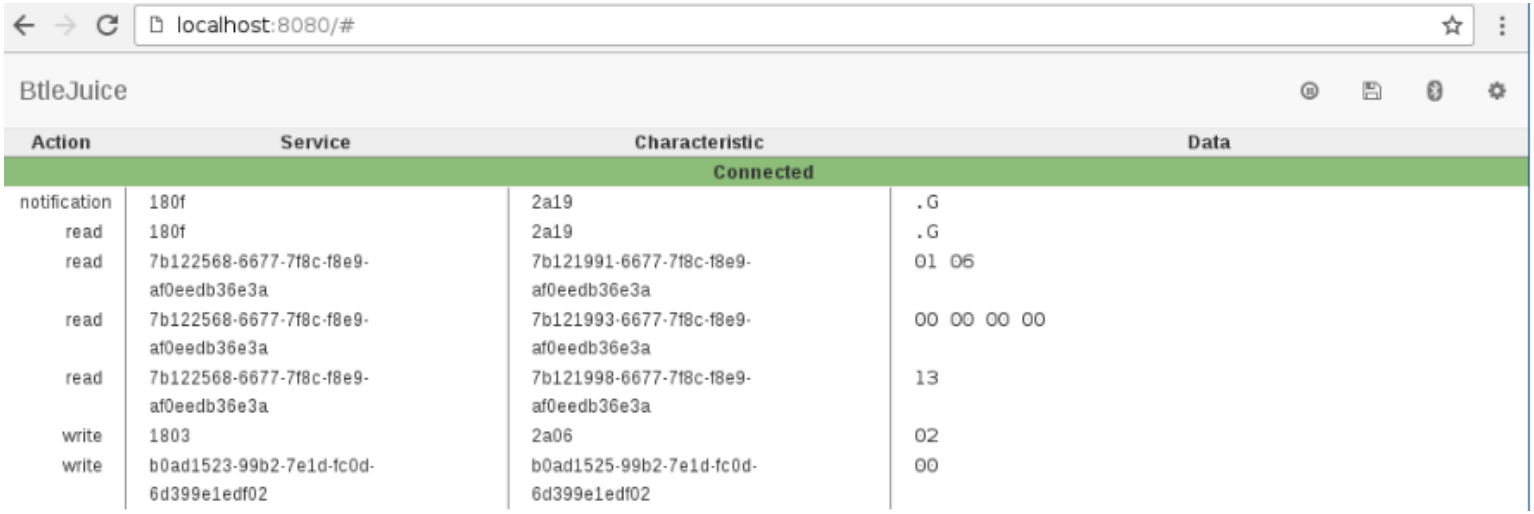
https://github.com/securing/gattacker

BtleJuice

- Bluetooth Smart (LE) Man-in-the-Middle framework

https://github.com/DigitalSecurity/BtleJuice

- Web interface



Action	Service	Characteristic	Data
		Connected	
notification	180f	2a19	.G
read	180f	2a19	.G
read	7b122568-6677-7f8c-f8e9-af0eedb36e3a	7b121991-6677-7f8c-f8e9-af0eedb36e3a	01 06
read	7b122568-6677-7f8c-f8e9-af0eedb36e3a	7b121993-6677-7f8c-f8e9-af0eedb36e3a	00 00 00 00
read	7b122568-6677-7f8c-f8e9-af0eedb36e3a	7b121998-6677-7f8c-f8e9-af0eedb36e3a	13
write	1803	2a06	02
write	b0ad1523-99b2-7e1d-fc0d-6d399e1edf02	b0ad1525-99b2-7e1d-fc0d-6d399e1edf02	00

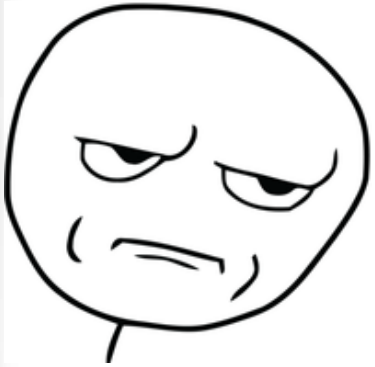
- Replay & on-the-fly data modification

Thanks

- Sławomir Jasek (gattacker, BH USA 2016)
- Damien Cauquil (Btlejuice, Hack.lu 2016)
- Zero_Chaos & Granolocks (DEF CON 24)
- Mike Ryan (lacklustre.net)
- Sandeep Mistry (github.com/sandeepmistry)

What's next?

- Bluetooth 5
  - Significantly increasing the range, speed and broadcast messaging capacity of Bluetooth applications
    - 4x the range, 2x the speed and 8x the broadcasting message capacity
    - "connectionless" IoT, advancing beacon and location-based capabilities
    - Improved interoperability and coexistence with other wireless technologies
    - Advance IoT experience by enabling simple and effortless interactions across the vast range of connected devices



https://www.bluetooth.com/bluetooth5

Thank you!

- Stay tuned: https://appsec-labs.com/iot-security/