BLE 环境下的攻击与防范

肖心茹　徐文超　杨婧雯

大连理工大学软件学院
https://github.com/knowncold/BLE_Security

2017 年 12 月 26 日

概览

主要工作

- 了解蓝牙低功耗的工作机制
- 了解蓝牙攻击的研究现状
- 搭建攻击和实验环境
  - iBeacon
  - YUNMAI Light
  - MI band 2
- 寻找可能的改进方案

蓝牙

- 蓝牙是一种短距离、低功耗的无线网络标准，在计算机和通信设备以及手机、键盘、音频耳机等外围设备中得到了广泛的应用
- 蓝牙 4.0 包含两个标准
  - 传统蓝牙，兼容蓝牙 1.0，2.0，3.0
  - BLE 是蓝牙低能耗的简称 (Bluetooh Low Energy)，蓝牙低能耗技术是低成本、短距离、可互操作的鲁棒性无线技术，它利用许多智能手段最大限度地降低功耗

应用场景

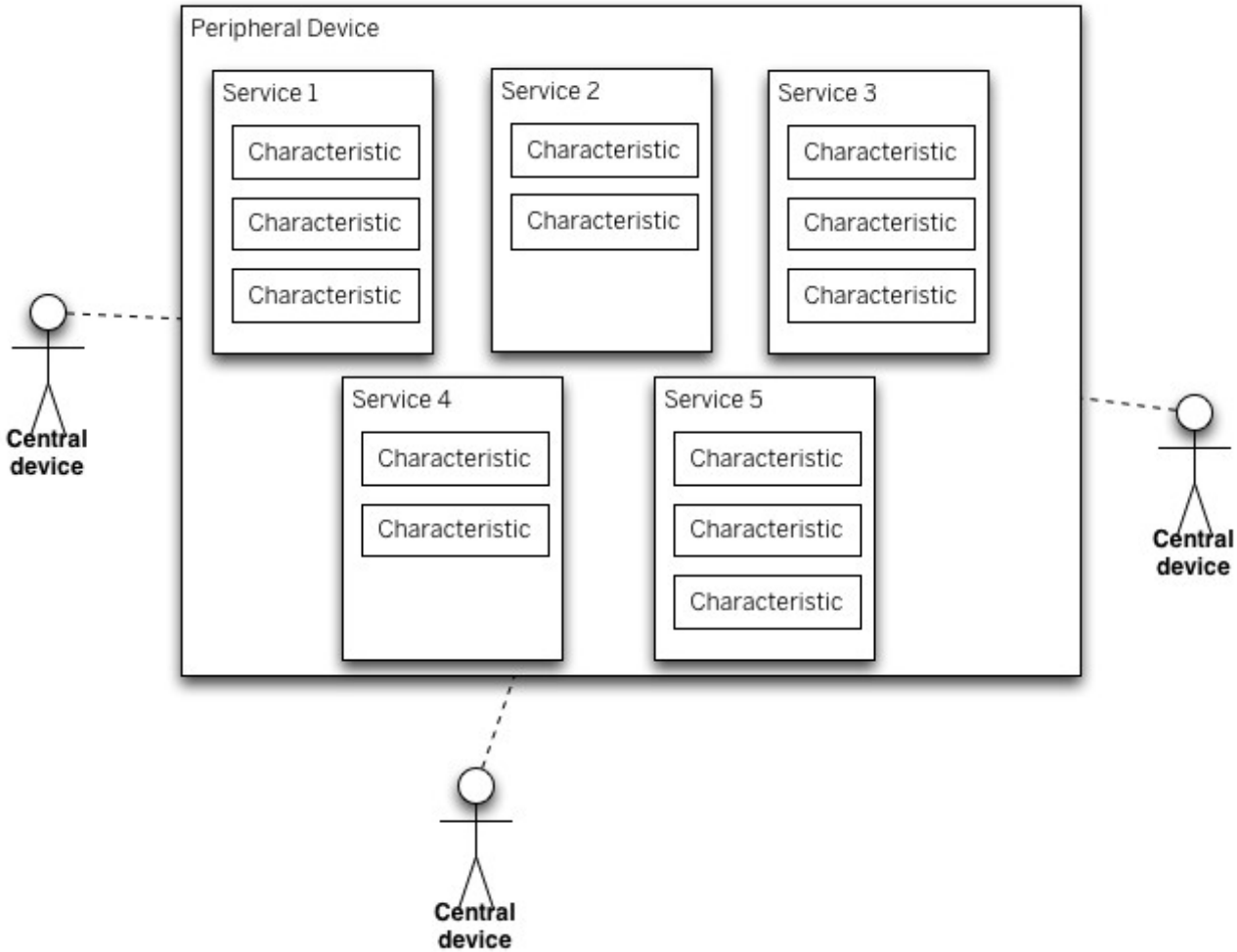
传统蓝牙

用于数据量比较大的传输场景，如语音，音乐，较高数据量传输等

低功耗蓝牙

应用于实时性要求比较高，但是数据速率比较低的产品，如遥控类的，如鼠标，键盘，遥控鼠标，传感设备的数据发送，如心跳带，血压计，温度传感器等

BLE


Peripheral Device
Service 1
Characteristic
Characteristic
Characteristic
Service 2
Characteristic
Characteristic
Service 3
Characteristic
Characteristic
Characteristic
Service 4
Characteristic
Characteristic
Service 5
Characteristic
Characteristic
Characteristic
Central device
Central device
Central device

BLE

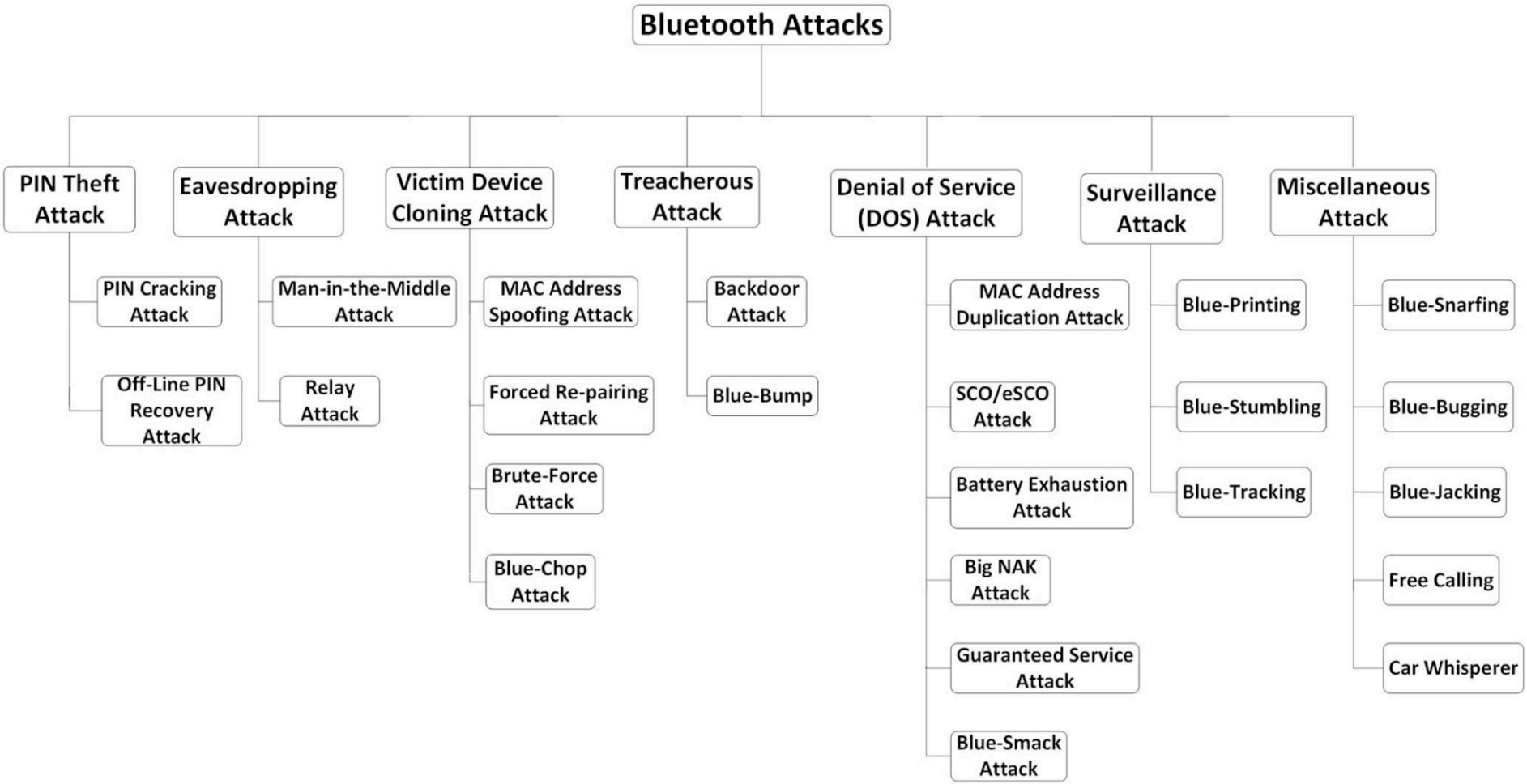
GAP

Generic Access Profile
控制设备连接和广播，GAP 使设备被其他设备可见，并决定了设备是否可以或者怎样与其他设备交互。例如 iBeacon 设备就只是向外广播，不支持连接，小米手环就等设备就可以与中心设备连接。

GATT

Generic Attribute Profile
定义两个 BLE 设备通过 Service 和 Characteristic 进行通信。
GATT 连接是独占的，一个 BLE 外设同时只能被一个中心设备连接；一旦外设被连接，它就会马上停止广播，对其他设备不可见；当中心设备断开，它又开始广播。

Bluetooth Attack



使用的工具

软件

Kali Linux、hcitool、nRF Connect、nRF Toolbox、LightBlue

硬件

云麦好轻体脂秤、小米手环 2
Raspberry Pi、TI CC2540、iOS、Android、Arduino 101

iBeacon

概述

iBeacon 是苹果公司 2013 年 9 月发布的移动设备用 OS（iOS7）上配备的新功能。
其工作方式是，配备有低功耗蓝牙（BLE）通信功能的设备使用 BLE 技术向周围以广播形式发送自己特有的 ID，接收到该 ID 的应用软件会根据该 ID 采取一些行动。

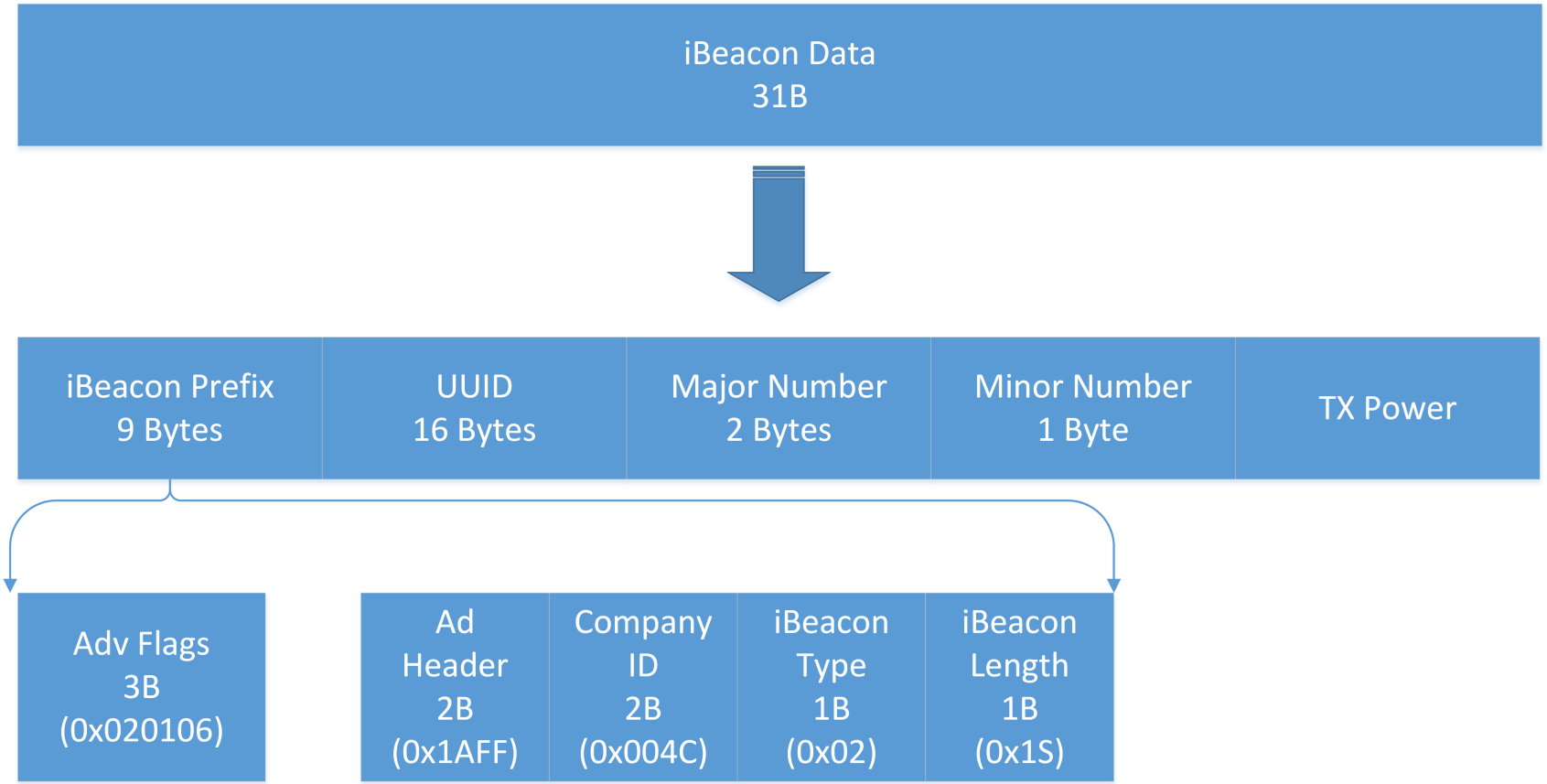
应用场景

iBeacon 使用 BLE 技术，成本相当低，作为一项定位技术，有各种各样的应用

- 商场，酒店等推送促销信息。可以定时定点地向客户推送他此时此刻最需要的消息
- 机场，体育场，博物馆等推送欢迎消息以及其他客户需要的消息（如航班信息等）

iBeacon

Packet



嗅探

由于使用的是广播的方式，使得嗅探攻击变得十分容易

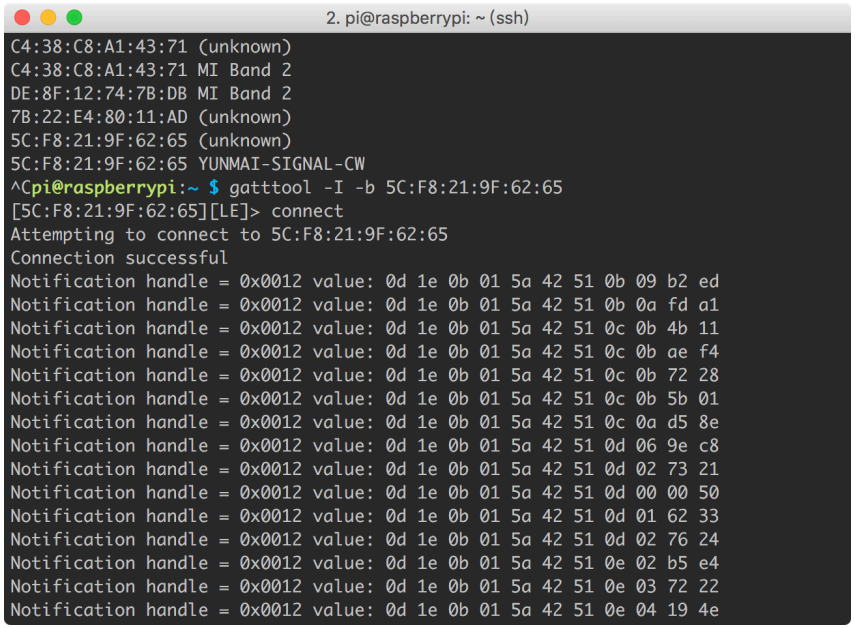
Spoofing attacks

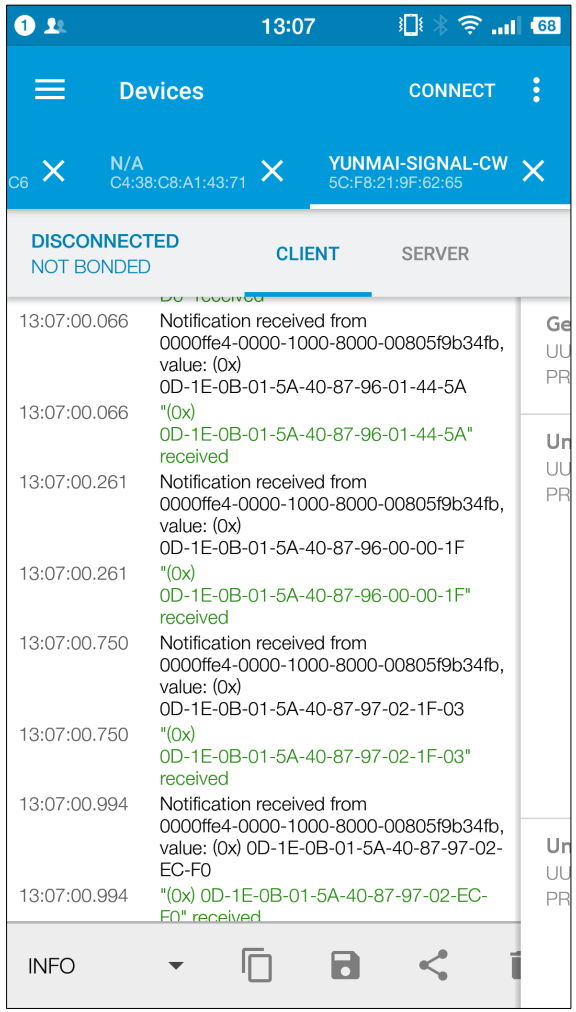
干扰应用的定位，传输错误的信息给云端

由于认证和加密体制的不完善，容易遭受 DoS 攻击，存在 RCE 漏洞，存在垃圾邮件的问题

YUNMAI Light

YUNMAI Light

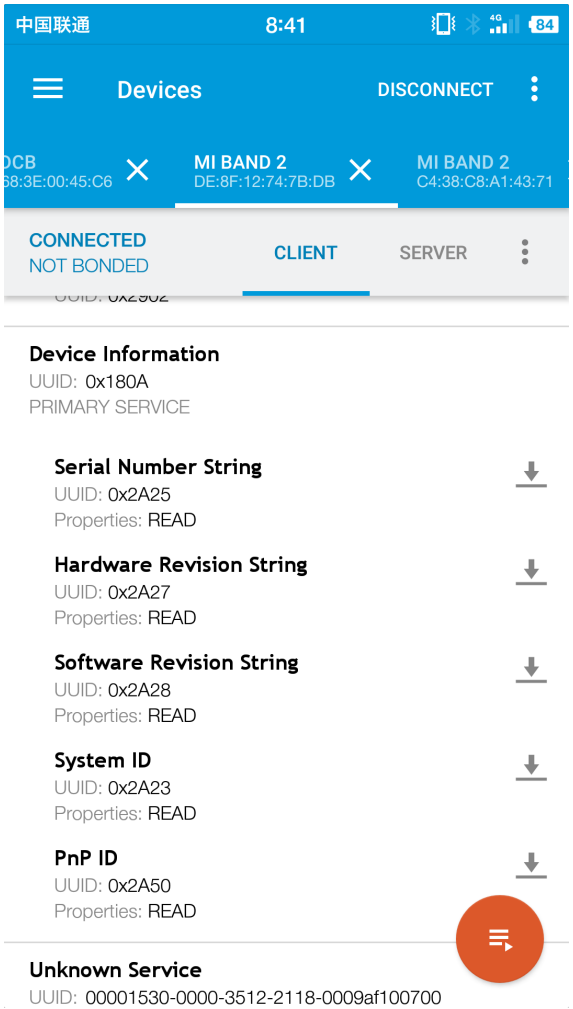




MI Band 2


1:10
88
小米手环2
85%
绑定后还未充电
屏幕解锁
未开启
来电提醒
未开启
手环闹钟
未开启
APP通知提醒
未开启
久坐提醒
未开启
更多
查找手环

MI Band 2


中国联通
8:41
84
Devices
DISCONNECT
MI BAND 2
DE:8F:12:74:7B:DB
MI BAND 2
C4:38:C8:A1:43:71
CONNECTED
NOT BONDED
CLIENT
SERVER
Device Information
UUID: 0x180A
PRIMARY SERVICE
Serial Number String
UUID: 0x2A25
Properties: READ
Hardware Revision String
UUID: 0x2A27
Properties: READ
Software Revision String
UUID: 0x2A28
Properties: READ
System ID
UUID: 0x2A23
Properties: READ
PnP ID
UUID: 0x2A50
Properties: READ
Unknown Service
UUID: 00001530-0000-3512-2118-0009af100700


21:48
48
小米手环2
佩戴方式
左手
手环显示设置
设置信息是否在手环上显示
时间样式
选择时间显示样式
抬腕亮屏
抬起手腕时手环显示信息
转腕切换手环信息
亮屏时转动手腕切换手环显示内容
心率辅助睡眠检测
用以提高睡眠检测精度(开启会降低续航时长)
玩转小米手环2
固件版本号
V1.0.1.59
蓝牙地址
C4:38:C8:A1:43:71
解除绑定

MI Band 2

Basic Service

UUID of Service:

`0000fee0-0000-1000-8000-00805f9b34fb`

Battery Info Characteristic:

`00000006-0000-3512-2118-0009af100700`

Alert Service

UUID of Service:

`00001802-0000-1000-8000-00805f9b34fb`

New Alert Characteristic:

`00002a06-0000-1000-8000-00805f9b34fb`

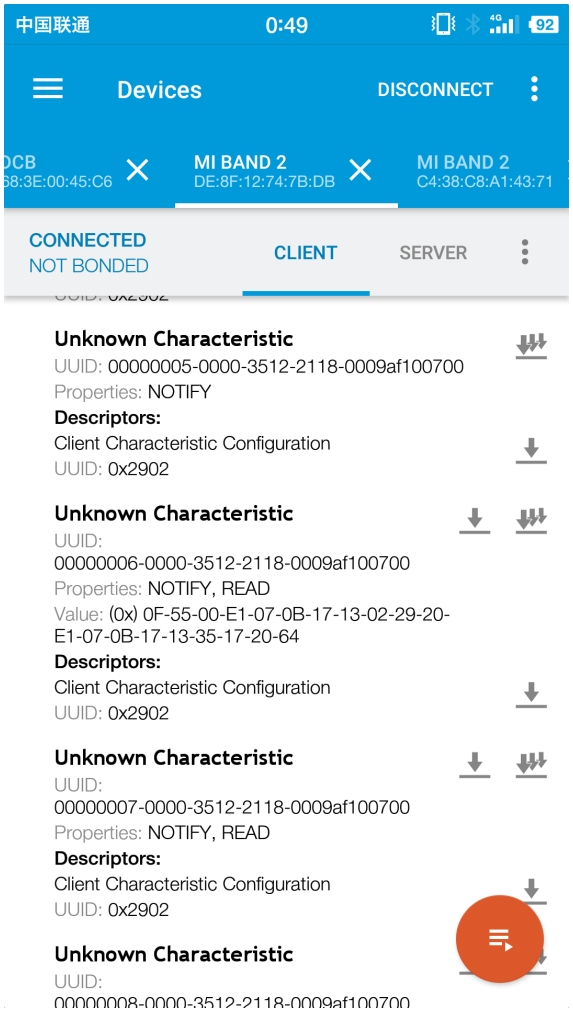
MI Band 2

Heart Rate Service

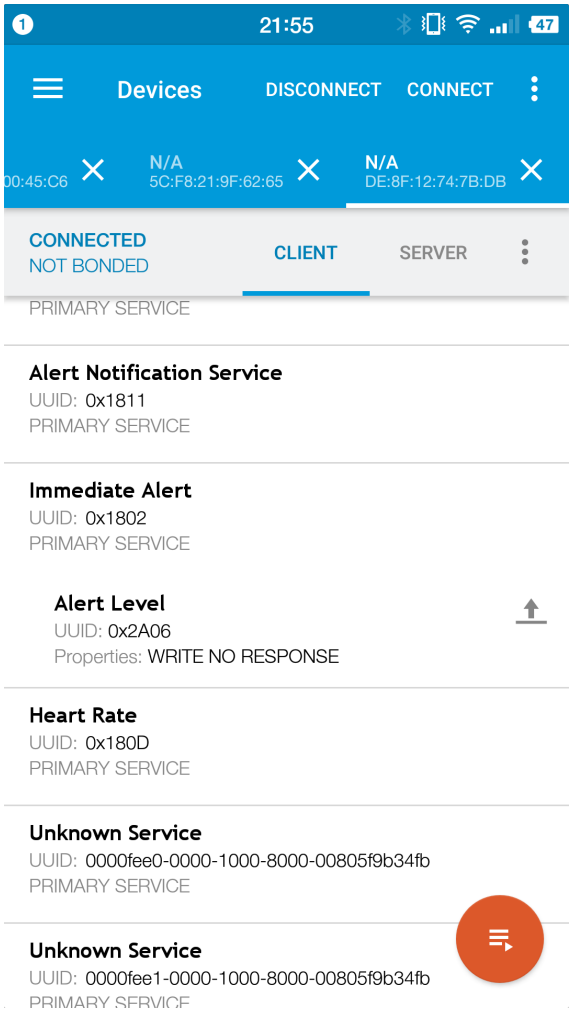
UUID of Service:
0000180d-0000-1000-8000-00805f9b34fb
Measurement Characteristic:
00002a37-0000-1000-8000-00805f9b34fb
Control Characteristic:
00002a39-0000-1000-8000-00805f9b34fb
Descriptor:
00002902-0000-1000-8000-00805f9b34fb

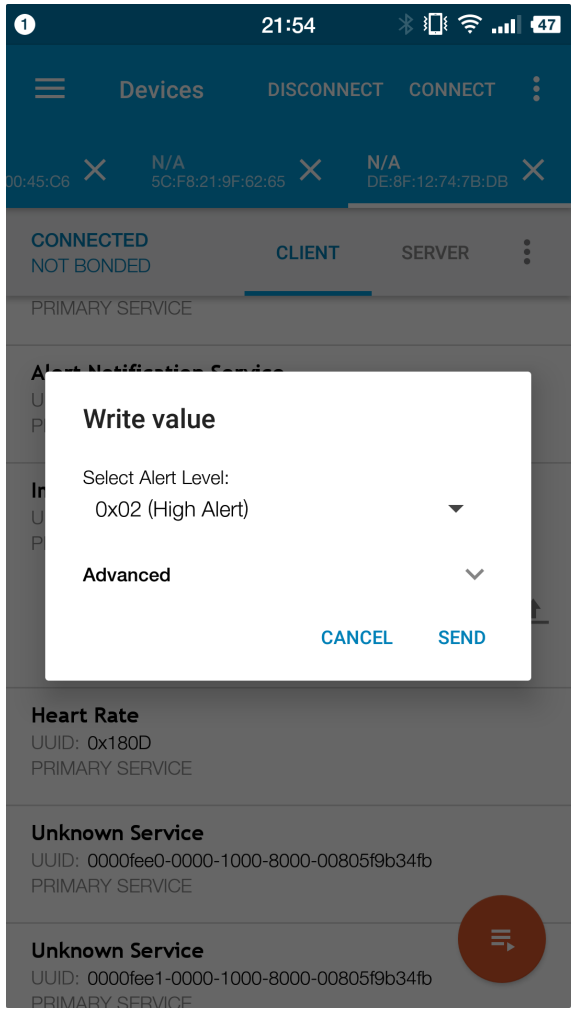
MI Band 2

```
public static Battery fromByte(byte[] b) {
        Battery battery = new Battery();
        battery.mBatteryLevel = b[0];
        battery.mStatus = Status.fromByte(b[9]);
        battery.mLastCharged = Calendar.getInstance();

        battery.mLastCharged.set(Calendar.YEAR, b[1]+2000);
        battery.mLastCharged.set(Calendar.MONTH, b[2]);
        battery.mLastCharged.set(Calendar.DATE, b[3]);

        battery.mLastCharged.set(Calendar.HOUR_OF_DAY, b[4]);
        battery.mLastCharged.set(Calendar.MINUTE, b[5]);
        battery.mLastCharged.set(Calendar.SECOND, b[6]);

        battery.mCycles = 0xffff & (0xff & b[7] | (0xff & b[8]) << 8);
        return battery;
}
```



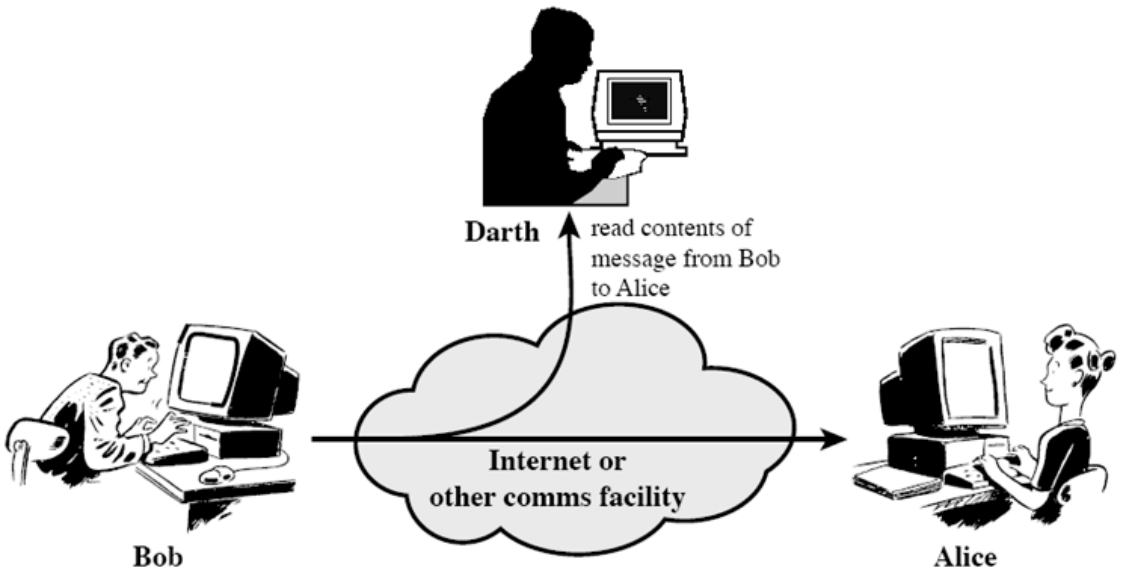
MI Band 2


21:55
Devices
DISCONNECT
CONNECT
00:45:C6
N/A
5C:F8:21:9F:62:65
N/A
DE:8F:12:74:7B:DB
CONNECTED
NOT BONDED
CLIENT
SERVER
PRIMARY SERVICE
Alert Notification Service
UUID: 0x1811
PRIMARY SERVICE
Immediate Alert
UUID: 0x1802
PRIMARY SERVICE
Alert Level
UUID: 0x2A06
Properties: WRITE NO RESPONSE
Heart Rate
UUID: 0x180D
PRIMARY SERVICE
Unknown Service
UUID: 0000fee0-0000-1000-8000-00805f9b34fb
PRIMARY SERVICE
Unknown Service
UUID: 0000fee1-0000-1000-8000-00805f9b34fb

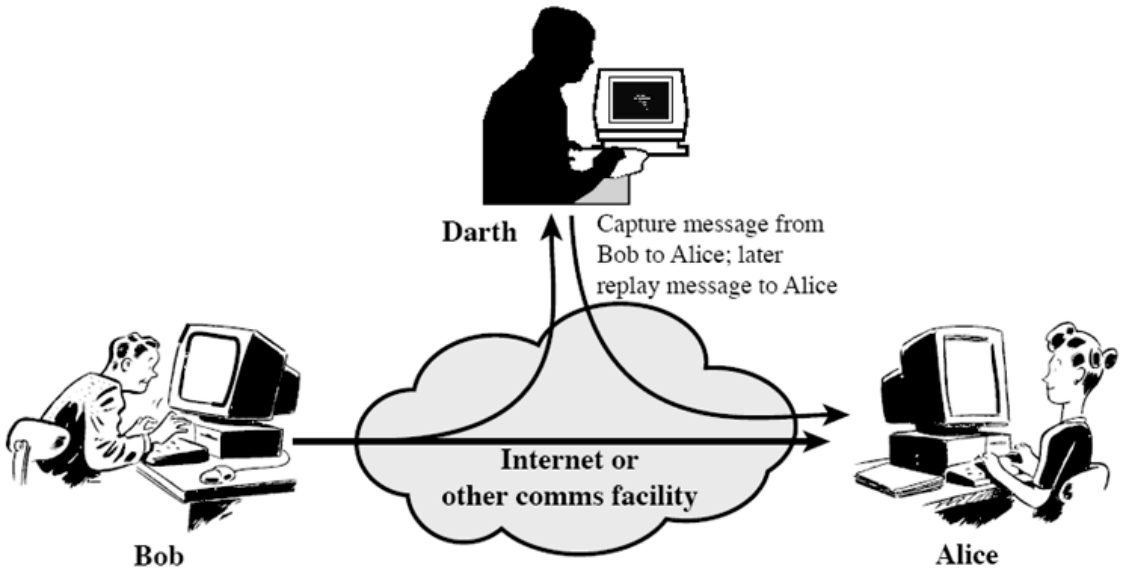

21:54
Devices
DISCONNECT
CONNECT
CONNECTED
NOT BONDED
CLIENT
SERVER
Write value
Select Alert Level:
0x02 (High Alert)
Advanced
CANCEL
SEND
Heart Rate
UUID: 0x180D
PRIMARY SERVICE
Unknown Service
UUID: 0000fee0-0000-1000-8000-00805f9b34fb
PRIMARY SERVICE
Unknown Service
UUID: 0000fee1-0000-1000-8000-00805f9b34fb

Solution

Cryptology & Web Security

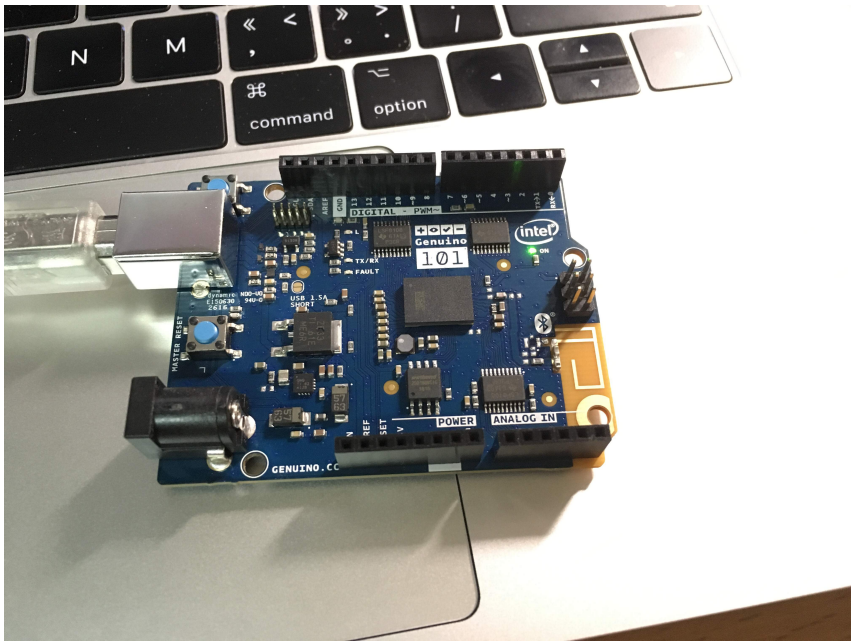


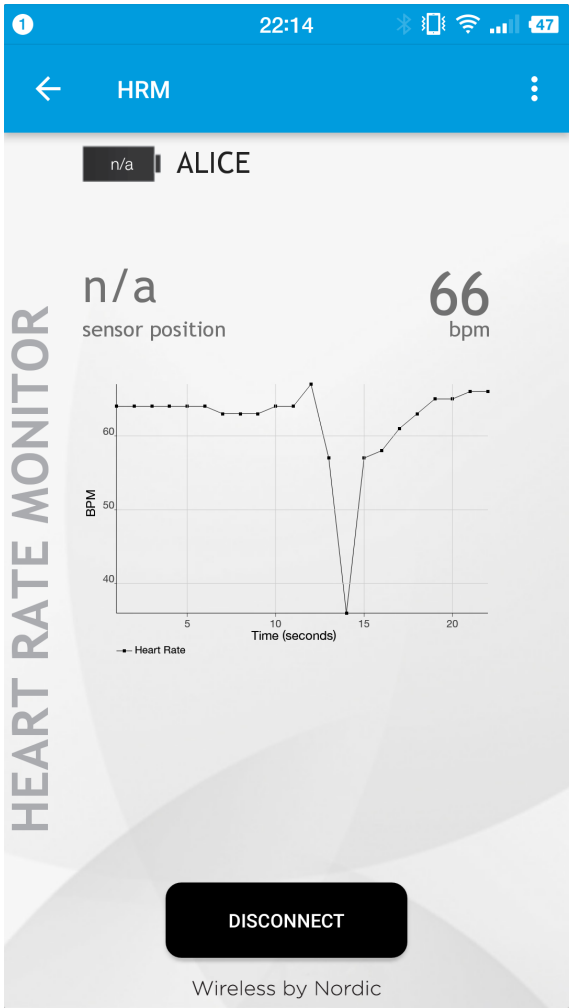
(a) Release of message contents


Darth
Capture message from
Bob to Alice; later
replay message to Alice
Internet or
other comms facility
Bob
Alice

(b) Replay

Solution


command
option
Genuino
101
POWER
ANALOG IN


22:14
HRM
n/a
ALICE
n/a
sensor position
66
bpm
HEART RATE MONITOR
BPM
60
50
40
5
10
15
20
Time (seconds)
Heart Rate
DISCONNECT
Wireless by Nordic

结论

加密和低功耗的冲突

运用加密的方式可以有效的防止嗅探攻击，但会增大功耗，与协议设计的初衷相违背，这种冲突是不可避免的。

安全性和低功耗的平衡

由于加密与低功耗之间不可避免的冲突，我们应该在安全性与低功耗之间寻找到一个平衡，牺牲一定的功耗来获得一定的安全性，根据不同应用对安全性的需求来考虑应该牺牲多大的功耗。

References

Shaikh Shahriar Hassan, Soumik Das Bibon, Md Shohrab Hossain, Mohammed Atiquzzaman

Security threats in Bluetooth technology

computers & security 2017 doi: 10.1016/j.cose.2017.03.008

The End