BLE-GATT浅析

icecolor / 2018-01-03 17:07:38 / 浏览数 3911 技术文章 技术文章 顶(0) 踩(0)

前言

BLE的应用范围越来越广，特别是在移动智能设备上。现在低功耗蓝牙（BLE）连接都是建立在 GATT (Generic Attribute Profile) 协议之上。GATT是一个在蓝牙连接之上的发送和接收很短的数据段的通用规范，这些很短的数据段被称为属性（Attribute）。

GATT负责两个BLE设备间通信的数据交互，是对功能数据最为重要的部分，GATT包括三层：
PROFILE、CHARACTERISTIC、SERVICE

CHARACTERISTIC是每个功能的对象，每个Servie都包含一个或多个CHARACTERISTIC，而PROFILE是他们的大类集合。（如图）

example：**手环

在Ubuntu下执行 'hcitool lescan'可扫描附近的BLE设备。

我们来抓包分析下**手环在交互时产生的数据，然后方便进行分析。

我用的设备是USBdongle,嗅探数据为SmartRF格式：

但是这种格式，使用起来很不方便，可以使用tibtle2pcap转换成libpcap的格式。

当你安装完Bluez协议栈后会给你自带两个工具，一个是hcitool，一个是Gattool。这两个工具本作为调试工具。特别是Gattool，它可连接蓝牙设备对其进行操作。所

经过抓包分析，找到了一处ATT Write Command控制指令，通过数据得知该 HandleVul为：0x0051 还有一处Alert level:Hight Alert■0X02■
根据蓝牙官方GATT CHARACTERISTIC文档描述

这是一种警报级别，也就是说**手环的震动就是根据这个数值分为震动级别。
有个APP是LightBlue。也可以做到这一点，但不是全部...例如下面的蓝牙灯泡就不可以。

演示Demo
https://v.qq.com/x/page/c0501jtxfkm.html

example：蓝牙灯泡

灯泡分析与**雷同，其实只要读懂了GATT，一半的设备都可以轻易的被'黑'。
通过扫描确定其MAC地址。

后对其目标进行设备进行数据分析，寻找write字段信息分析

跟踪字段信息并寻找其VULE字段值

抓包分析灯泡数据：
还是去分析它的Write Command，其Handle（操作句柄）为0x0019，数据值为08004701470147010000
Wirte Command与Write Request是有区别的，一个是写命令，一个是写请求，就以wirete command为例。
test vulue：

```
08004701470147010000
08000d07470147010000
08004701b223c64c0000
```

（PS：一些其他品牌的灯泡变色可能是根据RGB颜色对照表）
这个灯泡做了一些校验吧，若不通过APP直接用手机自带BLE连接会导致密钥不匹配。

使用Gattool可以直接操控灯泡开关，以及变色，若自己写个脚本，则可以让灯泡连续开关变色。。。
放个简单的Demo：
https://v.qq.com/x/page/q0501zyymd9.html
自己在家可以没事试着玩玩，没什么技术含量。

上一篇：企业安全建设—模块化蜜罐平台的设计... 下一篇：Web安全 -- BurpSuit...
1. 0 条回复

- 动动手指，沙发就是你的了！

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板