BLE 安全之虫洞攻击

笑然 / 2016-12-07 03:55:00 / 浏览数 2949 安全技术 漏洞分析 顶(0) 踩(0)

■■■■■■■■■
■■■■■■■■■■■■■■■■https://sec.xiaomi.com/article/19

0x00 前言

所谓『虫洞』，在天体物理中是通过扭曲空间，连接宇宙遥远区域间的一个隧道，通过穿越这个隧道可以完成『时空穿越』。其实我并不懂天体物理，这些是我 Google 来的。

在 BLE 安全中，有一种攻击近似于『虫洞』，可以在一瞬间让相隔万里的两个设备完成亲密接触。

这种攻击手法在 blackhat USA 2016 由安全研究者 Jasek 进行了阐述，同时 Jasek 公开了一篇详细介绍 BLE 安全的 White Paper『GATTACKING BLUETOOTH SMART DEVICES』和对 BLE 进行安全评估的工具 GATTacker。

PS：阅读本文需要有 BLE 基础，限于篇幅，本文不会对 BLE 展开细讲。

0x01 虫洞攻击原理

在谈论虫洞攻击之前让我们先简单了解下 BLE，BLE 是 Bluetooth Low Energy
（低功耗蓝牙）的缩写，和传统蓝牙类似，是一种近距离进行设备间无线连接和通讯的协议。BLE 和传统蓝牙除了名字相似外，其架构设计完全不同。BLE
物如其名，其具有极低的功耗，加上其使用简单，成本低廉，深受 IoT 的喜爱，目前在家庭、健康、医疗等领域使用广泛。比如我们所熟悉的手环，就是使用的 BLE 技术。

虽然 BLE 传输距离可以长达 100 米，但其仍然是一种近距离的无线通讯协议，其使用场景仍然需要两个设备进行近距离接触。大部分使用场景如下：

```
Phone <-- BLE --> Device
```

假设我们有一种需求是想让 BLE 的传输距离增加到 200 米，那么可以通过下面方式来实现：

```
Phone <-- BLE --> BLE Relay Device <-- BLE --> Device
```

我们通过一个 BLE Relay 设备来把 BLE 信号进行中继以达到 200 米的传输距离。更远的距离可以通过增强天线性能或者复用 Relay 设备来实现。

如果是地球的两端呢？应该没有人傻到采用优乐美奶茶绕地球的方式来完成 BLE 的传递。正常的思维会采用下面的方式来实现：

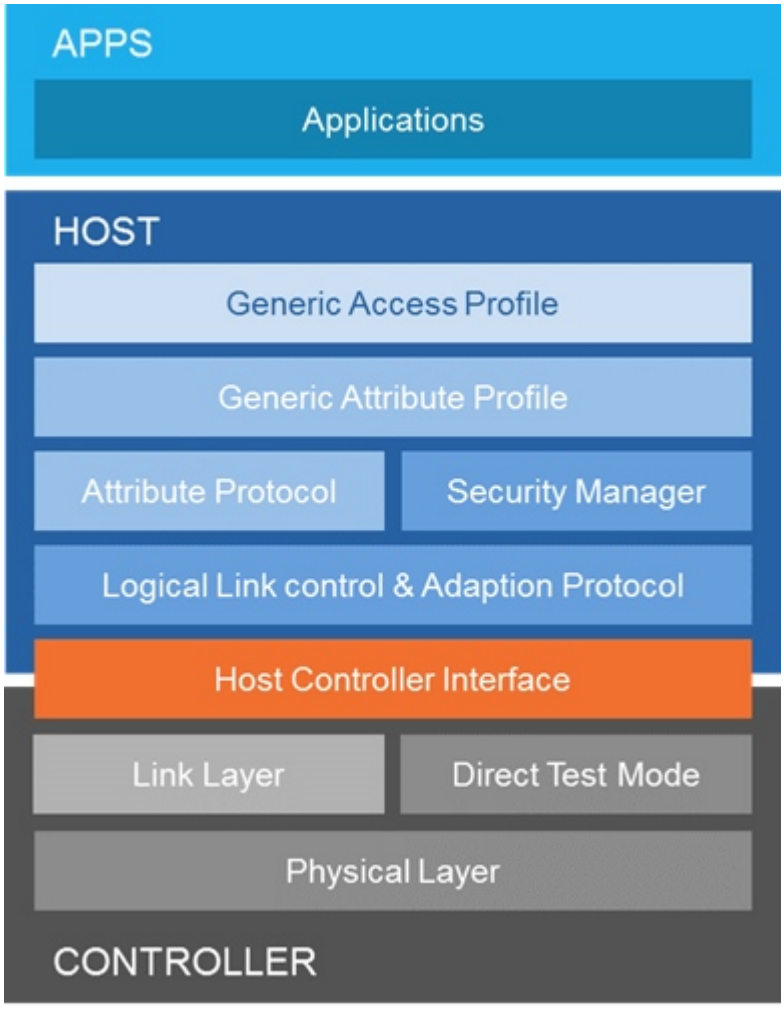
```
Phone <-- BLE --> BLE Peripheral <-- Tunnel --> BLE Central <-- BLE --> Device
```

我们通过额外的 BLE Central/Peripheral 设备以及 Tunnel 来完成 BLE 的传递。

放在 BLE 安全攻击模型中，我们可以把 BLE Peripheral <-- Tunnel --> BLE Central 部分称之为『虫洞』，通过『虫洞』来对正常的 BLE
通讯设备完成同一时间点甚至超越时间上的跨时空攻击。

0x02 虫洞攻击实现

实现『虫洞』攻击之前，我们还需要稍微再了解一下 BLE 协议，参考下图的 BLE 协议结构



BLE 协议结构

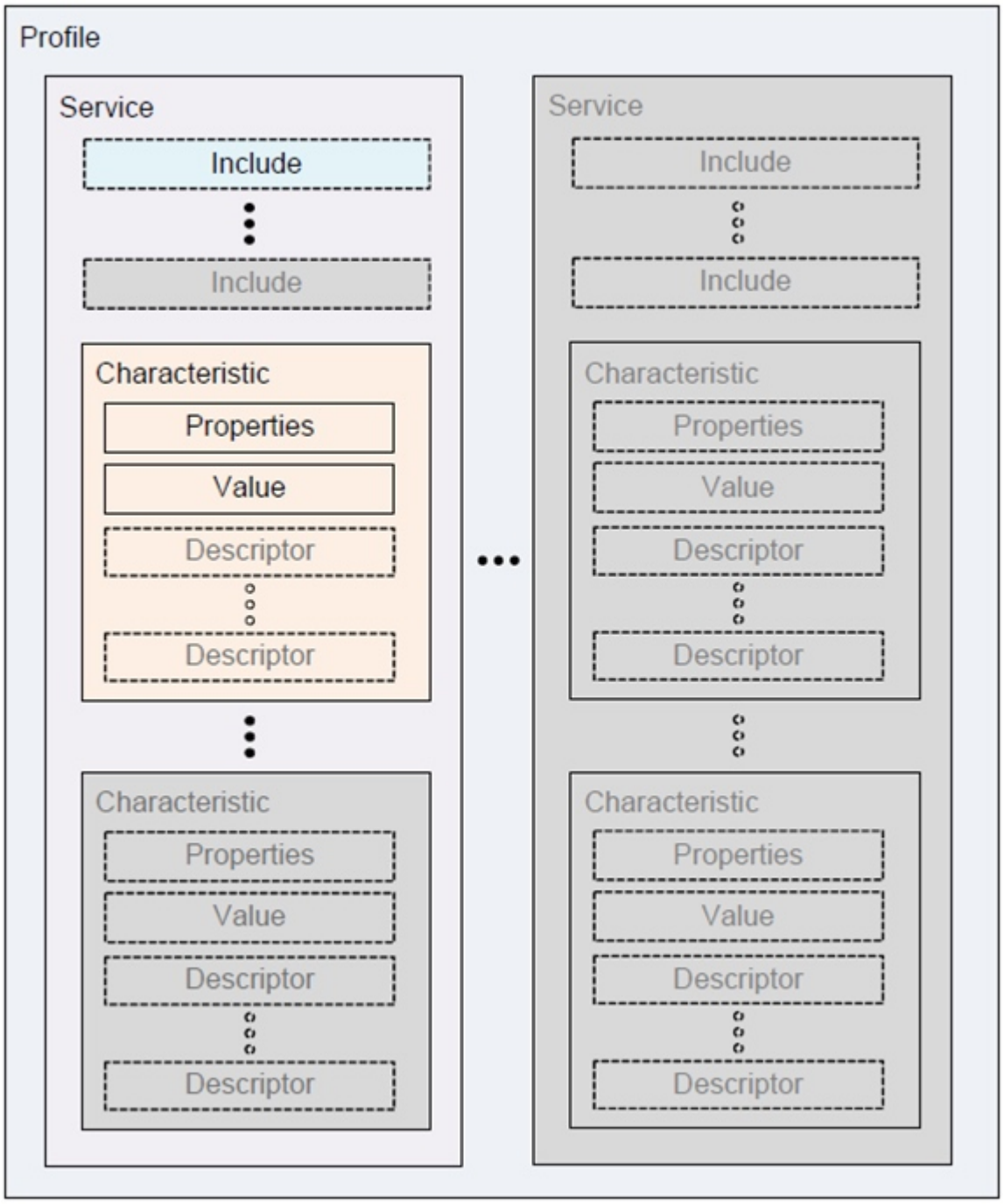
BLE 协议有很多部分组成，但是我们主要关注两部分：

- GAP（Generic Access Profile）
- GATT（Generic Attribute Profile）

GAP GAP 用于让两个设备进行连接。GAP 为设备定义多个角色，其中最重要的两个分别是：Central 和 Pheipheral。

- Pheipheral 发出广播，可以被 Central 设备进行扫描和连接，比如手环；
- Central 扫描 Pheipheral 设备，并对其进行连接，比如手机；

GATT GATT 用于让两个设备进行连接后的通讯。GATT 定义设备之间通过 Service 和 Characteristic 的东西来进行通讯，不同的 Characteristic 代表设备的不同功能。GATT 的结构如下：



了解了 GAP 和 GATT 之后，再来回忆一下『虫洞』攻击的模型 BLE Peripheral <-- Tunnel --> BLE Central，也就是说我们需要实现三部分功能，分别是 BLE Peripheral、Tunnel、BLE Central。

BLE Central

- 连接到 Device，获取其所有 Service 和 Characteristic，以及设备名称和 MAC 等信息，通过 Tunnel 传输到 BLE Peripheral，供 BLE Peripheral 伪造 Device。同时保持和 Device 的连接，用于后续对 Device 进行操作；

Tunnel

- websocket，socket，xmpp、http 等等，whatever，只要能够远程通讯都可以，用于BLE Central 和 BLE Pheipheral 之间数据传输；

BLE Peripheral

- 接收 BLE Central 传送过来的 Device 相关数据，完全伪造 Device，供 Phone 进行连接。把后续 Phone 对 Device 的操作通过 Tunnel 传输到 BLE Central 端；

最终，BLE Peripheral、Tunnel、BLE Central 三者实现了一个『虫洞』，拉近 Phone 和 Device 之间的距离，使其完成近距离接触。

只要网络可达，不在乎距离多远。

0x03 虫洞攻击相关工具

GATTacker https://github.com/securing/gattacker

Btlejuice https://github.com/DigitalSecurity/btlejuice

具体用法参见文档，具体实现参见代码。

0x04 攻击场景

在谈论『虫洞』时，我们一直在谈论距离，但是在实际的攻击场景中，距离并不是关键，关键的是攻击思想。下面罗列的攻击场景仅供参考

DDoS 在近距离，我们可以通过伪造 Device，使 Phone 强制连接我们伪造的 Device 以达到拒绝服务攻击的目的。

窃听或篡改数据 通过『虫洞』，我们可以洞悉 Phone 到 Device 的数据通讯，必要时候可以对数据进行篡改以达到我们想要的效果。

会话劫持 对于一些设备，通过『虫洞』，可以完成 Device 对 BLE Central 的认证，保持 BLE Central 对 Device 的连接，后续可以任意操作 Device。

当然攻击场景肯定不止上面提到的这三种，可以发散思维，想想还有什么攻击场景？

0x05 结尾

『虫洞』攻击其实就是 MITM，我并非故意标题党，而是我觉得在 IoT 快速发展的今天，形形色色的使用了 BLE
技术的智能设备已经深入到我们的生活中，并且在影响着我们的生活。手环、智能门锁、无钥匙进入、医疗设备等等，BLE
在为我们提供便利的同时，也埋伏着安全隐患。这种攻击虽然有前置条件，但是一旦发生轻则泄露个人隐私数据，重则造成财产损失，甚至对生命安全产生威胁。

希望本文会被相关从业者看到，能有些许思考。如果能够有些许影响，则更好不过。

0x06 参考资料

- http://www.gattack.io/ 中涵盖的 white paper、slides、code
- https://github.com/DigitalSecurity/btlejuice
- https://www.bluetooth.com/zh-cn/specifications/bluetooth-core-specification
- 以及与同事 rayxcp 的讨论

上一篇：某云PC客户端命令执行挖掘过程 下一篇：一句话极速爆破，简直6得不行【附带字典】

1. 0 条回复
   - 动动手指，沙发就是你的了！