GATTACKING BLUETOOTH智能设备

SławomirJasek，SecuRing。

Slawomir.Jasek@securing.p

l Slawomir Jasek@securing

摘要

本文档概述了蓝牙低能耗攻击的可能形式。 已经特别关注蓝牙堆栈的更高的GATT（通用属性配置文件）层。 介绍包括BLE的基本属性。 本节之后是可能的风险，攻击情景和建议的对策。 这些攻击情形由几个真实的漏洞补充，这些漏洞在测试设备的研究阶段和随附的移动应用程序中被识别出来。

最终，引入了一种新的开源工具，有助于BLE设备的安全评估。

1. 蓝牙低能量

顾名思义，蓝牙低功耗（也称为蓝牙智能或蓝牙4）技术从一开始就设计为节能。 根据一些制造商的说法，BT4芯片可以在单个纽扣电池上运行“数月到数年”（取决于使用和功率配置水平），尽管我们的测试无法复制这些结果。 除了在名称中使用“蓝牙”之外，BLE协议与以前的蓝牙版本（也称为BR，EDR，1.2,2,3 .....）的共享不多。 此版本具有新的RF堆栈（尽管它仍然在2.4 GHz ISM频段上运行），并且利用了其他使用场景。 专注于简化而不是吞吐量，从而使芯片不仅能耗更低，而且体积更小，成本更低。 这一关键特性成为市场上各种各样的新“物联网”设备和应用爆炸的催化剂。

1.1. BLE设备

可用性，低成本和易于实施使该技术在初创公司中非常受欢迎，这些公司开发了数百种不同的“智能”BLE产品。 当然，众筹项目只是实际实施的一部分，因为BLE也正在进入医疗，工业和政府设备。据预测，越来越多的BLE设备将以可穿戴设备，传感器，灯泡，袜子，杯子，医疗设备和其他智能产品的形式围绕着我们的生活。 许多这些连接的设备与任何重大风险无关，但有些设备可能具有严重的安全隐患（即门锁，警报，安全传感器，生物识别身份验证，银行令牌，键盘等）。 此外，许多设备会使用户面临潜在的隐私漏洞。

2. BLE通信

设备和移动应用之间的蓝牙低功耗通信通常遵循以下方案：

1. 设备（外围设备）广播广告。
2. 中央设备（移动电话）扫描广告。
3. 一旦接收到特定广告包，中央设备就停止扫描，并启动与广播外围设备的连接。
4. 中央设备浏览外围设备以获取可用服务。
5. 中央 设备 与...交换信息 外围设备 设备 运用 特征读/写/通知请求和响应。

根据使用场景，移动应用程序可以仅处理广告（2），而不启动与外围设备的直接连接。

下面是每个步骤的详细说明。

2.1. 广播广告

广播设备以指定的间隔和TX功率电平通告分组。 在RF层上，使用3个专用信道（在40个2MHz宽的信道中，2.4GHz ISM频带被BLE分割）广播广告，频率被优化以避免Wi-Fi干扰。 设备可以选择用于广告的频道：选择1,2或最常见的全部3个。

数据包的大小非常有限（31字节），并根据Bluetooth SIG [1]定义的规范进行格式化。

在连续字段中，设备可以广播，即其“服务”，“名称”或“制造商数据”（字段类型0xFF）。 制造商数据可以根据其他广泛认可的格式（未由Bluetooth SIG定义）格式化，例如Apple iBeacon或Google Eddystone。 供应商还可以实现自己的专有数据格式。

在较低层，广告数据可以被分成2个分组 - 一个由设备独立地广播，第二个是“扫描响应” - 响应于扫描查询请求被发送回特定的扫描设备。

广播分组在设计上对于范围内的所有收听设备是可见的（除了没有广泛采用的“定向广告”模式）。广播主要用于向移动应用“广告”设备存在，以及传输非私有数据，设备状态或传感器指示。

2.2. 听广告

“中央”设备（通常是智能手机）切换到扫描广告模式。 在此模式下，它接收附近设备的所有广告。 接下来，移动应用程序将所接收的广告与与给定设备相关的特定广告进行匹配。

由于扫描需要大量电力，为了节省电池，通常在接收到第一匹配广告后立即停止扫描过程。

接下来，移动应用程序解释所接收的数据，并执行适当的动作。 在几种情况下（例如，信标，某些传感器，获取设备的状态），移动应用程序不需要启动与设备的进一步连接。

2.3. 连接到设备

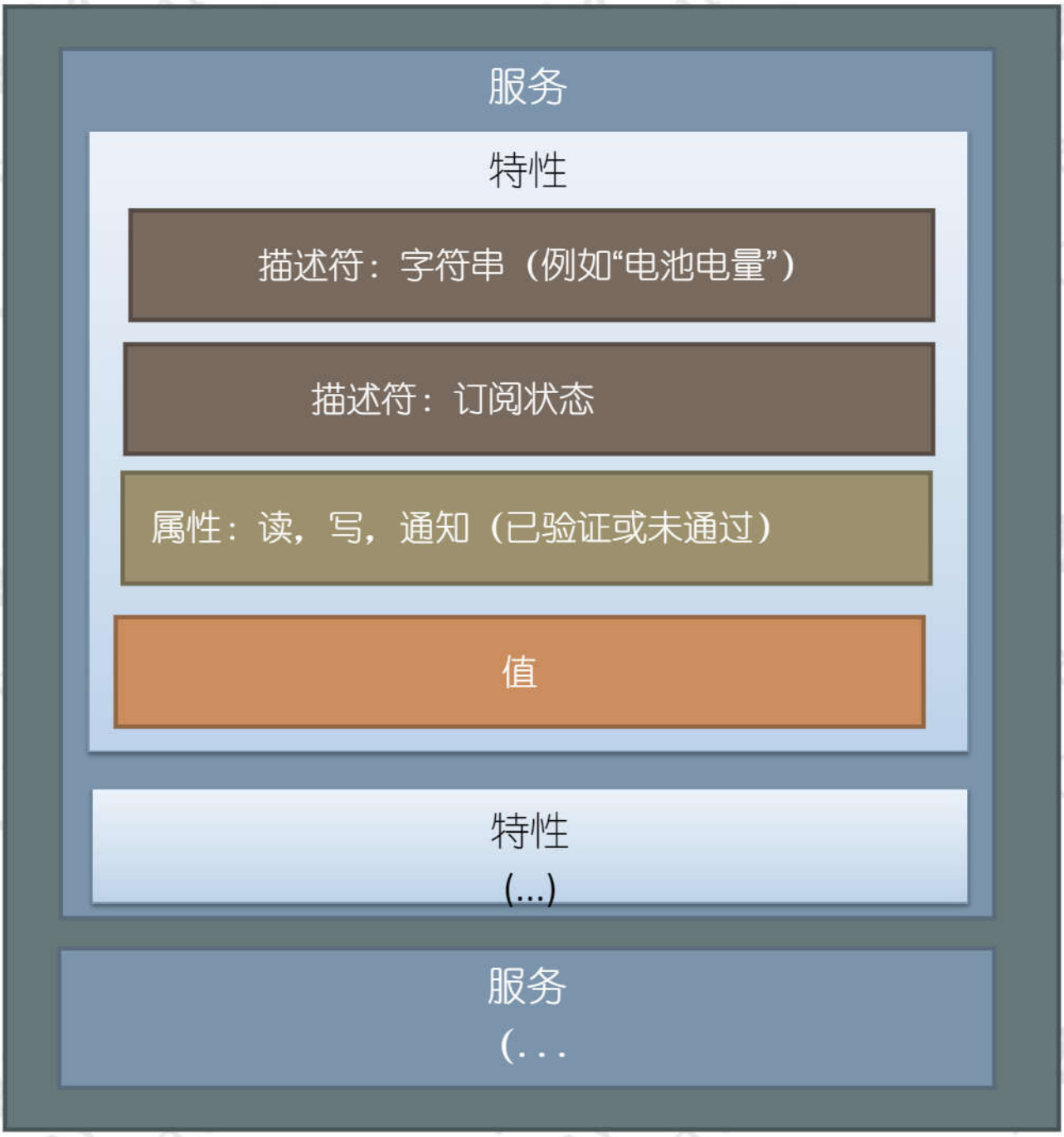
如果使用方案需要与设备交换更多数据，则启动定向连接。 通常对具有匹配广告的设备的MAC地址执行连接尝试。 然而，取决于移动应用，可以将MAC地址与特定的先前存储的MAC（例如，匹配给定的灯泡）或定义的供应商类进行比较。 例如，按照反编译的Android源代码过滤特定供应商的MAC地址：

```
private static boolean isBlueRadiosModuleAddress (String paramString)
{
  int i = paramString.substring (0,8) .compareTo ( “EC: FE: 7E”) ;
  boolean bool = false;
  if (i == 0)
    {bool = true;
  }
  返回布尔;
}
```

大多数设备一次只允许一个活动连接。

2.4. GATT数据结构：服务，特征，描述符

设备使用通用属性配置文件（GATT）[2]特征，描述符和服务来交换数据。 下图描绘了他们之间的关系：



特征包含单个值（“属性”），可以读取，写入或订阅通知（章节中的详细信息） 2.6).

每个服务和特征由关联的UUID（通用唯一标识符）标识。 典型服务（例如电池电量，设备信息）使用蓝牙规范[3]中定义的短UUID值。

要创建自己的专有服务和特性，供应商必须定义自己的长UUID值。

示例：GATTacker工具探索的Apple Watch的专有UUID服务和特征值：

```
"uuid": "d0611e78bbb44591a5f8487910ae4366",
    "name": null,
    "type": null,
    "startHandle": 10,
    "endHandle": 14, "特
    征" : [
        {
            "uuid": "8667556c9a374c9184ed54ee27d90049",
            "name": null,
            "properties": [
                "写",
                "notify",
                "extendedProperties"
            ],
            "价值": "", "描述
            符": [
                {
                    "处理": 13,
                    "uuid": "2900",
                    "价值": ""
                },
                {
                    "处理": 14,
                    "uuid": "2902",
                    "价值": ""
                }
            ],
            "startHandle": 11,
            "valueHandle": 12
        }
    ]
```

特征可以具有相关的描述符。 可能的描述符类型在相应的规范[4]中定义。

两个最常用的描述符是：0x2901（人类可读的用户描述）和0x2902 -“客户端特征配置”，它描述了当前的订阅状态。

2.5. 浏览设备的服务

在启动连接之后，中央设备扫描外围设备以获取所有可用的服务，特征和描述符。

由于服务扫描过程需要多个请求和响应，因此移动操作系统会存储特定设备的缓存值，以优化流程。例如，Android操作系统将GATT缓存存储在/ data / misc / bluedroid：bt_config.xml和gatt_cache_ <MAC_ADDR>文件中。

2.6. 阅读，写作和通知

根据通用属性配置文件（GATT）执行对特征的读取和写入，通用属性配置文件定义给定应用程序的服务，特征和属性的结构化列表。

如前所述，每个特征都具有定义其可能操作的关联属性：读取，写入，通知。 这些属性可以单独使用或一致使用（例如，读取+写入，写入+通知，读取+写入+通知）。

每个动作也可能需要“身份验证”，这意味着连接的加密（通常这些设备是配对的）。 在这种情况下，初始读或写请求之后是来自设备的“授权不足”响应。 一旦设备建立加密连接，对这种特性的连续读或写请求就会正常进行。

读写请求传输单个值。 要从设备获取更多数据或接收定期更新，请使用通知。 中央设备订阅特定特性，外围设备异步发送数据。

从技术上讲，订阅是作为对专用描述符（0x2902）的写请求执行的。 读取此描述符值将返回当前订阅状态。

写请求可以有或没有响应，并且通知可以由接收者未确认或确认（也称为“指示”）。

实际上，低级通信使用与特定特征相关联的整数句柄号来执行。

3. 稳定安全

3.1. BLE安全 – 规范

根据规范[5]，蓝牙低功耗“提供了若干功能，以涵盖用户数据的加密，信任，数据完整性和隐私”。

3.1.1. 加密

为了加密传输，BLE设备经历配对过程。 在此过程中，他们设置了长期密钥，然后用于保护连续的连接。 可用选项包括：

- “正常工作”
- 密钥输入
- 带外

蓝牙规范4.2版引入了椭圆曲线作为补充。 在撰写本白皮书时，支持此版本协议的设备尚未普及。

应根据设备输入/输出功能（显示，是/否按钮，键盘）选择配对方法。 例如，没有显示器的设备显然不能使用密钥输入。 前两个选项最常见，Out Of Band未被广泛采用。

引用规范：“Just Works和Passkey Entry不提供任何被动窃听保护”。 嗅探配对过程允许从PIN值导出长期密钥，并因此解密传输。 在“Just Works”的情况下，使用的静态PIN值为：000000。使用Crackle工具[6]可以强制破解密码输入PIN输入值。

尽管最常用的配对选项容易受到被动拦截，但其想法是它应该只在安全的环境中执行一次。 在创建初始绑定之后，使用“长期密钥”正确地保护传输。

3.1.2. 随机MAC地址

为了防止跟踪，规范允许频繁地改变设备的MAC地址。 只有配对设备才能解析当前MAC。

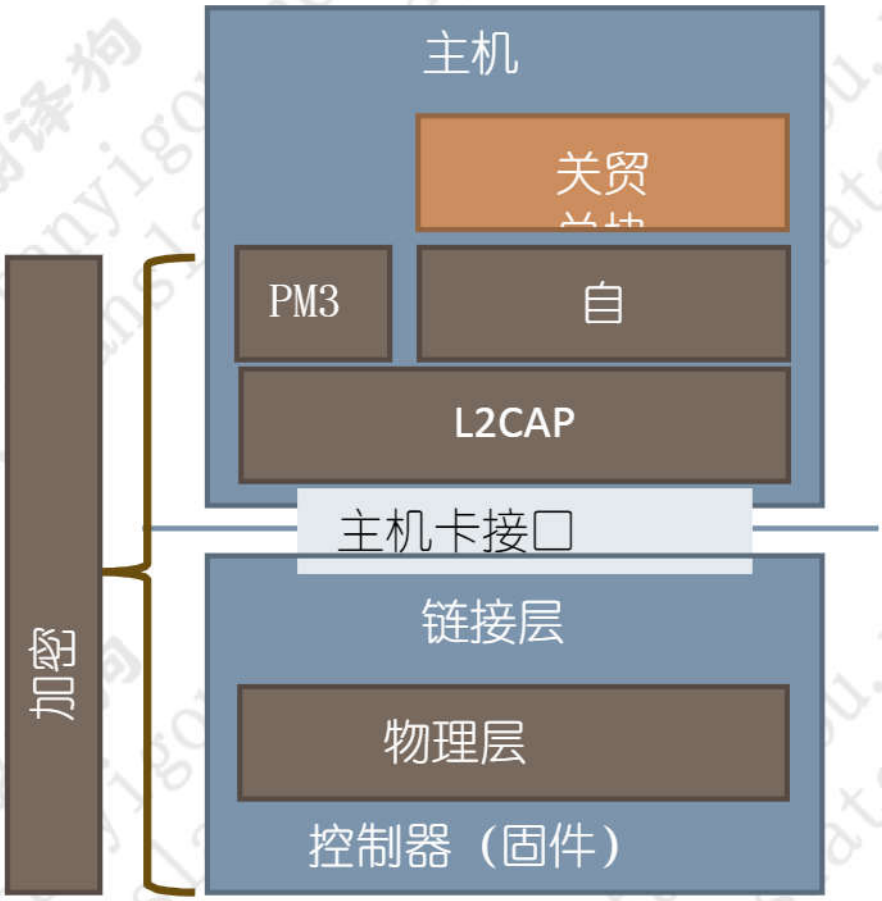
3.1.3. 白名单

可以创建已接受设备的MAC地址的白名单。

3.2. BLE安全 – 练习

大量设备不实现上述安全特征。 对于许多设备的使用场景（例如收银机，具有远程共享功能的设备，管理信标的“车队”），不可能在安全的环境中执行配对过程。 一些供应商没有将任何重大风险与拦截传输的可能性联系起来，因此他们接受它。 其他人努力遵守各种要求：可用性，多个用户或设备，云备份等。蓝牙安全功能由操作系统处理，移动应用程序无法完全控制此过程。 共享访问权限或将其传输到其他设备并不容易。 这就是为什么这些开发人员决定使用GATT读/写/通知请求在未加密的蓝牙LE链路上创建自己的安全机制。 最常见的功能包括安全身份验证（主要遵循质询 – 响应方案）和数据加密。 通常，只有硬件支持的算法

- AES – 与其自己的专有协议结合使用。



除智能手机和智能手表外，MAC随机化目前尚未得到广泛采用。 即使设备声明“随机”MAC类型，它通常也不会定期切换。 随机化也可能导致白名单实现出现问题，这种情况也很少见。

4. 可能的攻击

4.1. 攻击广告

解释由设备广播的广告的移动应用程序可以通过广告欺骗来攻击。

大多数电池供电设备优化广告间隔以最小化其功耗。 在包括“干扰”原始设备的攻击情形中，攻击者可能通过以最小可能间隔广播广告来滥用质量 - 比原始设备频繁得多。 如LINK 2.2中所述，移动应用程序将解释第一个收到的广告 - 在这种情况下，它很可能是欺骗性广告。

另外，由于大多数设备在活动连接期间不广播广告，因此通过保持与原始设备的连接，可以防止其广播。

使用新引入的工具的功能来记录所有广播的数据包，然后使用可配置（默认为最小）间隔来广告它们，从而实现广告欺骗。 只要有可能，它会同时保持与原始设备的连接。

最简单的攻击是拒绝服务。 为了成功执行它，所有必要的是宣传“克隆”设备，甚至不设置相应的服务。 受害者的移动应用程序将尝试连接到它，并且无法访问所需的设备功能，并将再次开始扫描广告。 克隆服务集的攻击效率更高，但不会将请求转发给原始设备。 在这种情况下，受害者的移动应用程序在尝试重新连接之前会保持与克隆设备的连接时间更长。

4.1.1. 示例漏洞

家庭自动化拒绝服务

示例：家庭自动化移动应用程序具有通过广告包中断的关联连接设备（灯泡，智能插头等）的状态。通过欺骗广告包中的设备状态 - 例如将其状态通告为“关闭”而实际上设备处于“开启”状态 - 可以阻止应用程序的功能。 实际上，受攻击的用户无法使用移动应用程序控制设备。

对于该应用，广告信号必须从受攻击设备的匹配MAC地址广播，因为移动应用通过其MAC存储特定设备。 因此，攻击涉及克隆受攻击设备的MAC地址。

防盗接近

这是服务于行李锁定设备的移动应用程序的防盗功能的示例，其取决于设备广播的特定广告分组的可用性。

攻击场景依赖于使用其MAC地址欺骗设备广播的广告数据包。 防盗移动应用程序没有注意到广告

被欺骗了，结果有可能“妥协”被认为受到保护的行李。

灯塔滥用

以下是移动应用程序的示例，该应用程序在访问特定位置时向用户授予忠诚度积分。 在收集了一定数量的积分后，可以将它们换成免费服务。 在接收到由位于现场的信标设备广播的特定iBeacon数据之后，移动应用程序自动确认访问。

通过简单地欺骗iBeacon数据，可以在不进入实际位置的情况下获得点数。

在这种情况下，攻击可以简化为重复移动应用程序在此过程中发送到服务器端API的HTTP请求。 iBeacon UUID，主要和次要特定数量

bers在请求参数中发送：

在该请求的参数之间发送的GPS位置也可能容易被欺骗，因此不应该用作可靠的保护形式。

信标映射站点的可用性（例如 http://wikibeacon.org/map） 允许在特定位置定位信标信号可以使攻击更容易远程调用。

4.1.2. 攻击对策

为了防止广告滥用，信标供应商引入了“改组”（也称为“加密”）和广播值的签名选项。 通告的数据包以预定义的频率更改其值，并且该值可以仅使用供应商的移动应用程序进行“解码”。 但是，这些机制必须克服一些限制 - 在硬件和软件方面，以及对离线使用要求的妥协。 由于供应商以绝密知识产权的方式保护“改组”算法的技术细节，因此可能会引起人们对该机制是否由专业密码师进行适当审查的担忧。

根据风险等级，理想的解决方案是不依赖于接收的广告包来获得关键功能。

4.2. 被动拦截

未被加密的传输可被被动窃听者拦截。 蓝牙拦截不再需要复杂或昂贵的硬件。 有几种经济实惠的硬件选项可以帮助完成这项任务，包括Great Scott Gadgets开源的Ubertooth [7]。

为了本研究的目的，使用了基于nRF51822 Nordic BLE模块的简单USB加密狗。 在撰写本文时，它在制作人的网站上以29.95美元的价格提供[8]。

该设备附带软件，可将嗅探的数据包提供给Wireshark网络分析仪。

使用新引入的工具，主动攻击也可以拦截传输的数据。

4.2.1. 示例漏洞Smart

Finder

示例“智能查找器”设备以静态6位密码的形式实现认证
从移动应用程序以明文形式发送到设备的特性写入。 下面的screendump显示使用GATTacker工具截获的密码（'123456'）：

```
>> Write:  0d583700447b98d61f6ec3340bdfbab8 -> 0d583701447b98d61f6ec3340bdfbab8 : 123456 ( 4V)
<< Read:   0d583700447b98d61f6ec3340bdfbab8 -> 0d583711447b98d61f6ec3340bdfbab8 : 01 ( )
<< Read:   0d583700447b98d61f6ec3340bdfbab8 -> 0d583708447b98d61f6ec3340bdfbab8 : 06 ( )
<< Read:   1803 (Link Loss) -> 2a06 (Alert Level ) : 00 ( )
>> Write:  1802 (Immediate Alert) -> 2a06 (Alert Level ) : 01 ( )
```

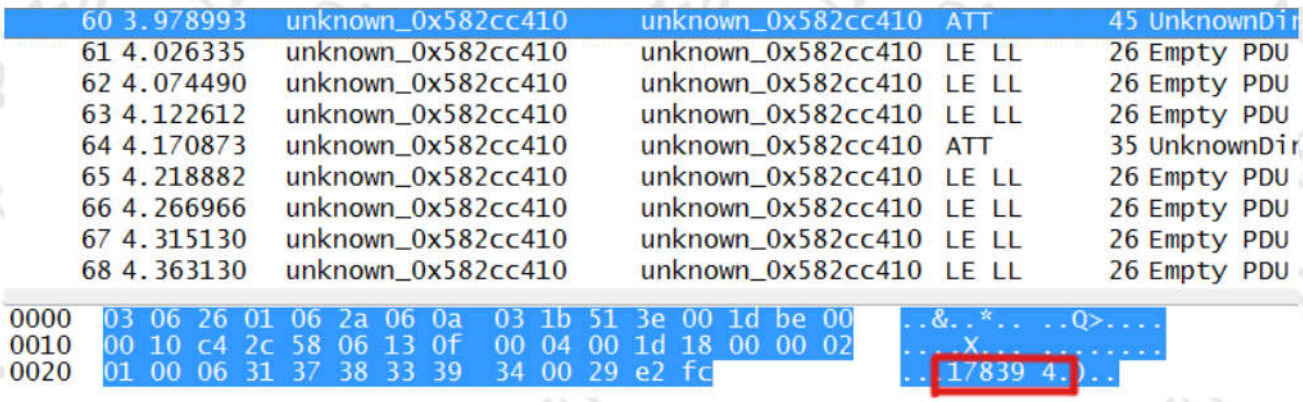
灯塔管理

信标设备通常通过静态密码进行管理。 每个设备都配置了自己的个人密码，通过服务器端API传递给移动应用程序。 接下来，在大多数情况下，密码以明文形式发送到设备。

OTP身份验证令牌

检查了“一次性密码”令牌设备，该设备通过蓝牙LE从设备自动传输6位数指示来提供移动应用程序认证功能。

设备和移动应用程序之间的传输未加密，并且可能被动拦截。 下面是在Wireshark网络分析器中解码的被动拦截数据包中的明文标记值：



4.3. 主动拦截

当攻击者调用与设备和移动应用程序的连接时，可以主动拦截未加密的蓝牙连接，并在它们之间中继消息。 这些设备被解释为它们彼此直接对话，而实际上传输是由攻击者控制的。 这种攻击通常被称为“中间人”（MiTM）。 在这种情况下，攻击者可以窃听，改变或将数据注入传输。

在所提出的工具中实现了主动攻击的“概念证明”。 它为受害者的移动应用程序“克隆”原始设备。 使用前面提到的策略（保持与原始设备的连接，并更频繁地做广告），它确保受害者连接到它而不是设备。 接下来，它可以转发和篡改交换的数据，充当拦截“代理”。

在克隆原始设备的MAC地址时，重要的是“克隆”设备服务和特性以及完全匹配的句柄号。 否则，它将与移动OS GATT缓存不匹配，并且移动应用程序将无法正常通信。 另见章节 2.5.

修改和注入设备之间交换的数据的能力可能导致各种攻击可能性。 攻击取决于数据的形式及其传输方式，以及设备或移动应用程序在接收特定数据时将执行的反应。

4.3.1. 漏洞示例数据操作

通过不安全的蓝牙智能链接连接到移动应用程序的销售点设备示例。 事务数据已正确加密，但设备允许一些不受保护的命令（以及其他“显示文本”）。 实际上，通过切换移动应用程序发送的原始文本，并在反编译的Android应用程序中基于算法计算正确的CRC，可以在支付过程中在设备上显示任意文本。 攻击不允许窃取卡片数据，但是弱点可能会与卖家的社交工程结合使用 - 例如，在提供无效PIN后，在设备上显示“交易处理”消息。

命令注入

例如，经测试的汽车解锁设备实施其自己的挑战 – 响应认证，随后是未经加密的命令和在这种认证的会话中与移动应用交换的响应。

在不改变身份验证过程的情况下，“Mid-in-the-Midlle”攻击者能够拦截经过身份验证的会话。 接下来，他们主动丢弃移动应用程序发送的原始命令，而是召唤其他命令。 可用的命令包括覆盖当前的认证密钥，这可能导致完全控制受影响的设备。

另外，后台的移动应用服务在检测到附近的车载设备的情况下自动执行认证，而不管接近自动解锁功能是打开还是关闭。 通过模拟原始设备的存在并远程转发数据包，这种行为可以更容易地攻击远离设备的毫无戒心的受害者。

重播

与上述汽车解锁装置相反，智能锁通信协议的一个示例确实涉及加密所有经认证的命令。 但是，该机制不包括防止重放加密数据包的保护。 在质询响应认证过程期间，每次移动应用程序响应给定的质询值计算相同的会话加密密钥。

在攻击的第一步中，入侵者可以窃听质询 – 响应认证过程，然后加密通信。 接下来，在认证过程期间，通过冒充原始设备，攻击者可以向移动应用程序提供先前记录的挑战值。 因此，应用程序将计算与窃听的密钥匹配的会话加密密钥。 在此之后，攻击者可以重放记录的加密设备响应，移动应用程序将使用相同的密钥正确解密它们。

在智能锁的情况下，入侵者能够误导用户，他们调用“latch”命令，认为锁被正确锁存，而实际上用户调用的命令没有传递给实际的设备。 毫无戒心的用户离开了房屋，确信门被锁定，而攻击者可以进入。

4.3.2. 攻击对策

应正确加密传输 – 使用蓝牙链路层安全功能，或 – 更高层专有协议。 为了正确实施加密，另见章节 4.5.3.

通过适当的设计和独立评估来防止专有协议中的漏洞。

4.4. 攻击暴露的服务

如果设备提供无需身份验证即可访问的服务，则攻击者可能会以各种方式滥用这些服务以接近受影响的设备。

4.4.1. 示例漏洞

模块的AT接口

在示例性设备中使用的蓝牙模块实现了供应商的服务，其允许使用GATT对预定义特征的写/通知请求直接连接到模块的串行AT接口。 界面没有受到保护。 因此，未经身份验证的攻击者可以自由更改蓝牙模块的配置。 根据制造商的文档，它可能会破坏设备的功能，并可能在物理上损坏它。

在GATTacker工具中实现了专用模块，允许在受影响的设备中识别此类服务，检测服务是否已锁定，并向其发出AT命令。

蛮力

一个示例性设备没有响应于暴力密码猜测而实现其软锁特征。 因此，攻击者可以猜测在有限时间内保护对设备访问的6位数密码。

不正确的随机数发生器

嵌入在设备中的某些模块不提供内置随机数生成器。 为了生成随机数据，开发人员可以使用不够随机的可用输入。 一个示例解决方案是使用当前温度输入乘以设备的序列号[9]。

在许多情况下，随机性水平对安全性具有重要影响。 例如，在质询 - 响应认证过程中，设备生成随机质询，移动应用程序使用密码加密响应进行响应。 如果挑战值是可预测的，则活动的MITM攻击者可以模拟设备并欺骗移动应用程序以计算针对给定挑战的适当响应。 接下来，攻击者可以使用响应来验证实际设备。

无需身份验证即可提供过多服务

设备可能实施过多的服务，这些服务没有得到适当的保护。 因此，未经身份验证的攻击者可能会访问不打算公开的数据或配置选项。

起毛

向特征发送不正确的值可能会导致设备异常行为。

逻辑缺陷

根据设备的不同，可能会滥用各种场景，例如身份验证或访问控制旁路。 示例设备在内部mod-s寄存器中存储了多个认证密钥。 在身份验证期间，移动应用程序指示使用了哪个密钥。 攻击者可以使用超出范围的关键指标值，这取决于设备的逻辑 - 可以使用可预测的值进行初始化。 通过这种方式，攻击者能够绕过身份验证。

4.4.2. 攻击对策

在将设备运送到生产环境之前，请务必检查所有公开的服务。 不仅根据最小权限原则限制访问，还要仔细验证所有输入并防止逻辑缺陷。

对于某些设备，限时配置可能是防止滥用暴露服务的可接受方式。 例如，设备可能仅在加电或按下专用硬件按钮后的有限时间内暴露配置服务。

4.5. 攻击配对

设备可以实现受保护的特性，这需要加密连接。 在读取或写入这样的特征之前，设备需要经历配对过程并计算将保护连续连接的长期密钥。

根据设备配对的方式，可能仍然可以通过滥用实施和社会工程用户的弱点来攻击这种连接。

4.5.1. “正常工作”

可能最流行的配对方法 -“Just Works”- 通常不需要在设备上调用任何操作来执行新的配对。 在这种情况下，攻击者可以通过简单地接近设备并尝试访问受保护的特征来与设备建立新的绑定。 在保持与原始设备连接的同时，攻击者可以创建其“克隆”，并欺骗受害者的移动应用程序进行连接。如果移动应用程序未验证设备的MAC地址，则攻击者可以使用其自己的MAC地址来实现此目的。 移动操作系统根据其他设备的MAC地址检查当前配对状态，在这种情况下，受害者的智能手机将找不到与攻击者MAC的任何配对信息。 实际上，它将连接到它而不加密。 攻击者还可以在没有保护的情况下暴露克隆的服务，因为他不需要强制与受害者进行绑定。

如果受攻击的移动应用程序验证设备的MAC地址，则攻击者必须克隆它。 因此，移动操作系统不会与攻击者建立加密连接，因为攻击者不知道用于加密的长期密钥。 在大多数情况下，移动应用程序不会显示有关可能的MITM攻击的任何警告，并且用户将仅注意到他们无法连接到他们的设备。 实际上，迷失方向的用户可能会放弃配对他们的智能手机，并再次启动程序。 不幸的是，这次他们将与攻击者配对，从现在开始，他们将能够拦截流量。

4.5.2. 受PIN保护的配对

通过PIN保护配对，攻击者将无法自动与设备配对。 但是，他们可以欺骗用户重新启动配对。 与上述情况一样，他可以将设备与其MAC地址一起克隆。 移动操作系统将无法与此类设备建立安全连接，因为密钥不匹配。 并且用户可能会尝试删除配对并再次强制执行。 在用户使配对无效后，攻击者可以关闭其活动的“克隆”设备，并允许用户继续与原始配对

设备。 他们可以被动地嗅探配对过程，而不是主动拦截。 接下来，他们可以破解PIN并使用Crackle工具[6]恢复长期密钥。

了解长期密钥后，他们将能够进行主动拦截。

4.5.3. 攻击对策

应使用最强的可用配对方法，并保护所有特性。

仅在设备上执行所需操作后才允许配对启动 – 例如，按下专用的“恢复出厂设置”按钮。

移动应用程序应检测主动拦截的尝试，并适当地警告用户。 移动OS可以部分地提供这样的功能。

4.6. 白名旁路

白名单过滤基于接受设备的MAC地址。 攻击者可以通过将其MAC地址更改为列入白名单的MAC地址来绕过过滤。

5. 攻击条件，风险考虑

5.1. 物理范围

由于蓝牙操作范围有限，为了执行“中间人”攻击，攻击者必须靠近两个受攻击的设备。 这些设备不需要彼此靠近，因为攻击者可以通过Internet连接远程中继数据包。 GATTacker工具的模块化设计允许利用这种攻击场景。

某些移动应用程序具有接近功能，当不正确地实施时，可能会通过接近运行受影响的应用程序的智能手机远离设备及其原始位置来滥用。

此外，设备可能具有可以直接利用的漏洞，而无需与移动应用程序交互或拦截传输。 在这种情况下，攻击者只需要接近易受攻击的设备。

移动恶意软件可能会攻击受感染智能手机范围内的BLE设备。 这种恶意软件是远程操作的，理论上攻击在大规模上是可行的。

最终，出现了一种新的“Web蓝牙”标准，允许访问附近的BLE设备以获取网页[10]。 可以使用从远程网站调用的javascript来执行某些攻击。

5.2. 风险

风险取决于许多因素，包括设备，其使用和目标个体。

例如，来自普通人的智能腕带的当前脉冲计数对其他人不是很感兴趣。 但是，如果这个人是一个排名很高的官员，那么情况可能会发生巨大的变化，并且对手希望在重要的谈判中知道他们的脉搏。 要么

- 腕带脉冲指示用作银行应用程序中的生物特征认证。

6. 新工具

6.1. 建筑

该工具包含三个主要模块：

1. “中央”连接到原始设备。
2. “Peripheral” - 设备模拟器。
3. 数据拦截和操纵。

“中央”侦听广告，扫描设备的服务以便在“外围设备”中进行克隆，并转发在主动攻击期间交换的读/写/通知消息。

“外围”模块加载由“中央”模块收集的设备规范（服务，特征，描述符），并充当设备“仿真器”。 它允许“克隆”原始设备的MAC地址，成功拦截许多移动应用程序的通信所必需的，这可以验证MAC。 在这种情况下，设备交换GATT数据的属性的句柄号必须与原始设备的数字完全匹配。 否则，移动OS的GATT缓存将不匹配并阻止通信。

使用通过JSON格式的设备配置的钩子函数可以进行数据拦截和操作。 该工具中包含一些示例钩子函数源。

这些模块可以在同一系统上运行（至少有两个蓝牙4接口），也可以在不同的系统上运行。 它们使用websockets相互连接。 由于这种方法，可以链接通信 - 例如，在Web拦截代理中将BLE请求作为JSON文本进行操作。 也可以调用远程攻击 - 其中“中央”模块放置在受攻击设备附近，“外围”模块靠近受害者的智能手机 - 可以远离原始设备的位置。

6.2. 必要的硬件

每个模块（“中央”，“外围设备”）都需要蓝牙低功耗适配器。 最受欢迎的基于CSR 8510的USB加密狗价格约为10美元，并且使用Bluez bdaddr工具确认稳定的MAC地址变化。

该软件可用于Linux系统，并使用node.js编写。 它在Raspberry Pi上进行了测试。

6.3. 设备通信分析

6.3.1. 移动应用分析

移动应用程序反编译和代码分析对于理解与设备的通信非常有帮助。 应用程序调试日志可以另外加速该过程。

6.3.2. HCI转储

移动应用程序和外围设备之间交换的数据的被动分析也可以使用Android手机中的“蓝牙HCI监听日志”开发者选项功能来执行。 它将主机卡接口转储文件存储在/sdcard/btsnoop_hci.log中。 稍后可以使用Wireshark数据包分析器检查该文件。

7. 参考

[1] “通用访问配置文件分配的号码”，蓝牙SIG，[在线]。 可用：httPS：//www.bluetooth.org/en-我们/规格/分配的号码/仿制访问 -个人资料。

[2] “蓝牙GATT规范”，蓝牙SIG，[在线]。 可用：httPS：//www.bluetooth.com/specifications /通用的属性 - 概述。

[3] “蓝牙GATT服务规范”，蓝牙SIG，[在线]。 可用：https：//developer.bluetooth.org/gatt/services/Pages/ServicesHome.aspx。

[4] “GATT描述符规范”，蓝牙SIG，[在线]。 可用：https：//developer.bluetooth.org/gatt/descriptors/Pages/DescriptorsHomePage.aspx。

[5] “蓝牙智能安全”，蓝牙SIG，[在线]。 可用：https：//developer.bluetooth.org/TechnologyOverview/Pages/LE-Security.aspx。

[6] M. Ryan，“Crackle - 破解蓝牙智能加密”，[在线]。 可用：http://lacklustre.net/projects/crackle/。

[7] “Ubertooth One，”伟大的Scott Gadgets，[在线]。可用：https：//greatscottgadgets.com/ubertoothone/。

[8] “Bluefruit LE嗅探器，”Adafruit，[在线]。可用：httPS：//www.adafruit.co米/产品/2269。

[9] “蓝牙智能社区论坛：随机功能，”BlueGiga，[在线]。 可用：https：//bluegiga.zendesk.com/entries/59399217-Random-function。

[10] “网络蓝牙，”[在线]。 Available：http：//webbluetoothcg.github.io/web-bluetooth。