

# “手机+可穿戴设备”的低功耗蓝牙安全实验技术

梁敏<sup>1</sup>, 胡曦明<sup>1,2\*</sup>, 李鹏<sup>1,2</sup>, 马苗<sup>1,2</sup>

(1. 陕西师范大学 计算机科学学院, 陕西 西安 710119;

2. 现代教育技术教育部重点实验室, 陕西 西安 710119)

**摘要:** 可穿戴技术创新驱动了以可穿戴设备为支点的新移动应用领域飞速发展, 低功耗蓝牙作为其中的关键性技术成为近年来高校计算机类专业实验技术与实验教学改革关注的热点。针对当前教学缺乏低功耗蓝牙协议安全实验原理与实验技术的现状, 通过深入而系统地分析低功耗蓝牙协议体系结构、工作原理和安全威胁构建起实验原理教学体系, 进而提出了“手机+可穿戴设备”的新型实验技术并给出了协议测量和可视化分析等关键技术的实现方案。在此基础上, 应用“手机+可穿戴设备”实现了真实环境下低功耗蓝牙协议通知、写请求和写响应等交互过程的安全性分析, 并进一步通过报文窃听、伪造和篡改实现了重放攻击, 为面向一流本科课程和“新工科”建设的实验教学改革提供了新的技术途径。

**关键词:** 手机; 可穿戴技术; 低功耗蓝牙; 物联网; 实验技术

中图分类号: TP393

文献标识码: A

文章编号: 1673-629X(2020)11-0111-06

doi: 10.3969/j.issn.1673-629X.2020.11.021

## Bluetooth Low Energy Security Experiment Technology of “Smart Phone + Wearable Device”

LIANG Min<sup>1</sup>, HU Xi-ming<sup>1,2\*</sup>, LI Peng<sup>1,2</sup>, MA Miao<sup>1,2</sup>

(1. School of Computer Science, Shaanxi Normal University, Xi'an 710119, China;

2. Key Laboratory of Modern Teaching Technology of Ministry of Education, Xi'an 710119, China)

**Abstract:** The innovation of wearable technology has driven the rapid development of new mobile application fields with wearable devices as the fulcrum. Bluetooth Low Energy has become a hot spot in experimental technology research and experimental teaching reform in college computer major as an important technology in recent years. In view of the current lack of Bluetooth Low Energy protocol security experiment principle and experiment technology, through an in-depth and systematic analysis of the Bluetooth Low Energy protocol architecture, working principle and security threats, an experimental principle teaching system is constructed, and then a new experimental technology of “smart phone+wearable device” is proposed, and the implementation scheme of key technologies including protocol measurement and visual analysis is presented. On this basis, the application of “smart phone+wearable device” realizes the security analysis of the interactive process including Notification, Write Request and Write Response in Bluetooth Low Energy protocol in actual environment, and further realizes the replay attack by packet eavesdropping, forgery and tampering, which provides a new technical approach to the reform and innovation of experimental teaching for the first-class undergraduate courses and construction of “Emerging Engineering Education”.

**Key words:** smart phone; wearable technology; Bluetooth Low Energy; internet of things; experimental technology

## 0 引言

从20世纪60年代可穿戴概念的提出,到2012年

面向个人消费市场的首款智能可穿戴设备 Google glass 正式发布,再到近年来快速渗透到生物医学、健

收稿日期: 2020-05-29

修回日期: 2020-09-29

**基金项目:** 国家自然科学基金项目(61877037); 中央高校基本科研业务费专项资金资助项目(GK201503065); 陕西师范大学2020年教师教学模式创新与实践研究专项基金项目(JSJX2020Z28); 陕西师范大学2019年教师教学模式创新与实践研究专项基金项目(JSJX2019Z47)

**作者简介:** 梁敏(1999-),女,专业方向为计算机科学与技术;通讯作者:胡曦明(1978-),男,博士,讲师,硕导,研究方向为智慧教育、计算机教育;李鹏,博士,副教授,硕导,研究方向为移动计算、教育信息化;马苗,博士,教授,硕导,博导,研究方向为人工智能、智能系统。

健康管理、智慧教育、体育运动等社会生产生活的各个领域,可穿戴设备发展进程前阶段长时间的寂静冷清与现阶段短时间内井喷爆发形成了鲜明对比。这背后的决定性因素在于近年来可穿戴技术在生物传感、网络通信和低功耗管理等方面取得的突破性进展,其中作为关键技术之一的低功耗蓝牙 BLE (Bluetooth low energy)<sup>[1]</sup> 由于可以有效实现高密度小微传感器之间的长时间短距离无线通信而成为技术与市场共同关注的热点<sup>[2]</sup>。在此驱动下,国内多所高校重点针对蓝牙通信开展了积极的实验教学改革与探索,例如:哈尔滨工程大学控制工程实验中心马忠丽提出基于蓝牙数据无线传输实验系统开展实验教学的方法<sup>[3]</sup>;东华大学倪林将基于物联网的短距无线通信技术系统引入实验教学<sup>[4]</sup>;华东师范大学的高明华提出基于 App Inventor 在线开发系统的蓝牙通信实验教学方法<sup>[5]</sup>。

如今,基于移动云交换的可穿戴系统为“云时代”的发展开辟了新思路<sup>[6]</sup>,随着智能可穿戴设备进一步融入到生理、支付、生活轨迹等个人隐私活动中<sup>[7]</sup>,针对低功耗蓝牙的安全性开展实验教学改革的重要性和紧迫性更加突显。西北工业大学王静将小米手环和支付宝相结合进行可穿戴设备免密支付的安全性研究,对可穿戴设备的支付环境进行了安全性评估<sup>[8]</sup>;国防科技大学刘强围绕可穿戴设备的数据安全和隐私保护,以可穿戴健康跟踪设备 Fitbit 为研究对象开展安全与隐私实例分析<sup>[9]</sup>;西安电子科技大学刘晴晴剖析了手环和智能家居面临的安全威胁<sup>[10]</sup>。可以看到,当前的研究进展多停留在实例讲授、行为管理、安全评估等零散的安全性理论分析层面,缺乏在低功耗蓝牙协议层面上开展攻击与防御的整套实验技术。在国家一流本科课程改革<sup>[11]</sup>和“新工科”建设背景下<sup>[12]</sup>,面向未来新一代移动应用对高素质复合型创新人才培养需求,低功耗蓝牙协议安全实验技术与教学应用成为亟待研究的重要课题。

## 1 低功耗蓝牙协议工作原理与安全性分析

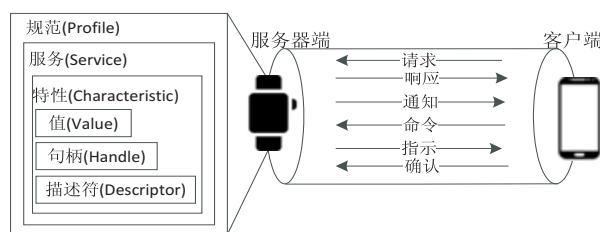
### 1.1 工作原理

低功耗蓝牙协议制定了通信方之间的标准化数据交互格式与交互流程,由蓝牙 4.0 技术规范和 CSR Mesh 协议等一系列标准具体定义<sup>[13]</sup>。虽然相关协议和标准持续更新<sup>[14]</sup>,但协议体系结构相对稳定,从上至下分别是应用层、主机层和控制器层。

从协议功能上看,主机层既负责为应用层提供网络传输服务和通信安全保障,又负责对控制器层收发蓝牙信号进行逻辑链路控制、报文解封装与封装和密钥管理等操作。从协议结构上看,主机层又可进一步划分为通用访问协议 GAP (generic access profile)、通

用属性规范 GATT (generic attribute profile)、属性协议 ATT (attribute protocol) 等协议子板块。

其中,通用属性规范 GATT 是实现低功耗蓝牙通信的基础和支撑,负责将服务器端的原始数据结构化形成“特性—服务—规范”三层嵌套的数据格式,从而为整个通信过程提供通用的信息存储和共享功能,如图 1 所示。



特性 (characteristic) 是组织数据的基本结构,采用通用唯一识别码 UUID (universally unique identifier) 作为数据结构的标识,数据结构本身由特性值 (value)、句柄 (handle) 和描述符 (descriptor) 构成,是通信读写操作的基本对象。服务 (service) 是面向功能来组织的一组特性及其相关的行为规范,以人类可读的形式定义设备间读写等操作过程。规范 (profile) 是一组预先定义的服务的集合,是应用的最终体现。

低功耗蓝牙通信的客户端和服务端基于 GATT 给出的特性进行数据传输,相互之间读写操作包括请求、响应、通知、命令、指示和确认等六种类型,具体由 GATT 定义。整个通信过程的访问权限由服务器端负责管理。

### 1.2 安全威胁

安全问题是大规模可穿戴设备部署面临的障碍之一<sup>[15]</sup>。2016 年爆发的 Mirai 恶意软件正是基于物联网设备的漏洞形成大型僵尸网络并广泛传播,严重威胁到可穿戴设备的使用<sup>[16]</sup>,谷歌恒温器和耐克运动手环均被研究者证实存在信息安全隐患<sup>[17]</sup>。由此可见,可穿戴设备的安全问题不容小觑。在基础层面看来,可将可穿戴设备所面临的安全风险分为设备数据安全、系统和应用软件安全以及传输安全三个方面。

#### (1) 设备安全。

可穿戴设备为了提高续航时间,通常降低低功耗蓝牙服务器端的输入权限检查等级甚至取消安全保护机制,仅在手机等客户端部署安全保护机制,从而使得可穿戴设备运行过程中无法检查输入数据的合法性,恶意攻击者可在用户未授权的情况下,非法入侵设备欺骗用户生理数据信息,对用户进行实时非法监控,威胁用户的个人隐私安全和身心健康。

#### (2) 系统和应用软件安全。

可穿戴设备通常与手机上的对应官方软件搭配使

用,当手机的应用软件存在漏洞时,可穿戴设备同样受到信息安全威胁。例如,恶意攻击者可以通过对智能手环官方应用软件进行 Android 逆向工程和 Hook 攻击,挖掘可穿戴设备与应用软件交互过程的数据信息和读写漏洞,实施对智能手环的数据窃取和篡改。

### (3) 传输安全。

可穿戴设备通过低功耗蓝牙技术与手机通信时,一般采用明文传输的方式,并且服务器端安全校验能力弱、设备识别码易被截取、授权管理不严,在简化传输过程的同时也带来了身份标识被窃取和数据泄露的安全威胁。另外,由于可穿戴设备采取间歇性运行的工作模式,只能依靠设备自身的硬件升级和算法改进保障通信安全,存在一定安全隐患。

## 2 基于“手机+可穿戴设备”的新型实验技术

### 2.1 总体设计

#### (1) 实验环境搭建。

总体上,采用模块化的系统设计思路,基于“手机+可穿戴设备”的方法配置低功耗蓝牙安全实验环境,具体分为可视化分析模块、数据采集和测量模块以及数据通信模块,如图 2 所示。

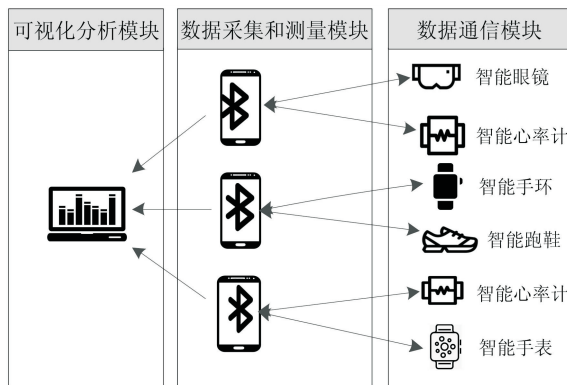


图 2 基于“手机+可穿戴设备”的低功耗蓝牙安全实验环境

数据通信模块中的可穿戴设备与数据采集和测量模块中的手机通过低功耗蓝牙进行交互,双方设备的交互数据由数据采集与测量模块实时记录,并以机器特定的日志文件类型保存在手机中。可视化分析模块对数据采集和测量模块记录的交互数据进行可视化处理,将日志文件解码为人类可读的报文格式。模块化的实验环境设计可根据低功耗蓝牙协议攻击、防御的安全性实验需求进行横向和纵向扩展,具有灵活、便捷和可操作性强的特点。

#### (2) 实验流程设计。

基于手机和可穿戴设备搭建实验环境,开展低功耗蓝牙协议分析和安全性实验,实验总体流程如图 3

所示。

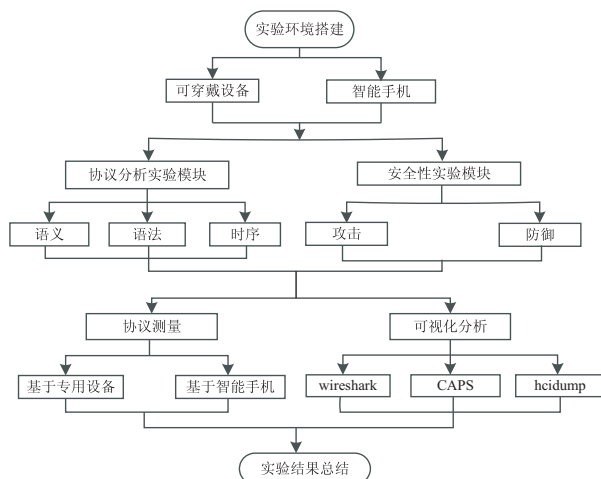


图 3 实验流程设计

首先,通过协议分析实验解读低功耗蓝牙协议的语义、语法和时序等信息,安全性实验基于协议分析的结果,向可穿戴设备发起数据重放攻击并进行防御方法探究。其次,将协议分析实验和安全性实验进行可视化处理,借助可视化工具进行抓包分析、数据提取和数据解码,利用实际报文测试实验项目,最后对实验结果进行总结归纳。

### 2.2 关键技术

#### (1) 协议测量。

对低功耗蓝牙协议嗅探和测量,仍是当前实验的技术难点。通常蓝牙通信模块基于数据包的访问码自动进行过滤<sup>[18]</sup>,由于过滤行为发生在底层的硬件层面,单纯采用上层软件抓包的方法难以获取到报文,必须采用“硬件+软件”的方法予以解决。目前可行的低功耗蓝牙协议测量方法分为两种主要的技术与方法:一是基于专业设备的传统协议测量方法,常用的设备有 EN-dongle 与 Ubertooth one 平台;二是基于手机的协议测量方法,主要工具包括 btsnoop\_hci. log 日志和 Xposed 模块。从性能对比来看,基于专用设备的方法具有可视化程度高和专业性强的优点,但因依赖专用硬件和 PC 端而存在便携性差和成本高等缺点;基于智能手机的测量方法解除了硬件设备限制,适用于面向大规模学生开展理论与实践相结合的自主性、探究性实验,可视化效果和测量精度通够达到实验教学的要求。

为此,该文提出基于手机的协议测量技术,采用“btsnoop\_hci. log 日志+Xposed 模块”的方法,相比基于 EN-dongle 等专用设备的传统协议测量技术更加便捷、灵活且成本更低,同时支持学生随时随地自主开展探究性实验。

btsnoop\_hci. log 日志是 Android 系统为开发人员提供的低功耗蓝牙调试文件,其中记录了低功耗蓝牙



通信过程中的所有数据报文,支持对低功耗蓝牙的通信机制进行详细分析。Xposed 是 Android 系统中进行深度控制 and 安全性测试的框架服务程序,其中的 MX 蓝牙抓包模块支持对低功耗蓝牙数据通信过程进行实时监测。在进行蓝牙协议测量时,为实时监测并详细记录通信双方的交互内容,通常将两种方法结合使用,具体实现大致分为三个步骤:①通过 MX 蓝牙抓包模块可实现对当前手机上运行的低功耗蓝牙通信进程进行实时的数据采集;②对具体命令进行定位,从而获取目标功能对应特性的 UUID 和写入值;③将记录了整个过程的 btsnoop\_hci. log 日志导入可视化工具,利用获取的特性 UUID 值进行目标筛选,从而实现从 btsnoop\_hci. log 日志记录的大量无关报文中对低功耗蓝牙报文的逐个精准测量。

### (2) 可视化分析。

手机中的 btsnoop\_hci. log 日志是以机器可读的特定格式来记录低功耗蓝牙数据,只能通过可视化分析工具进行语义解析才能将其翻译为人类可读的协议报文。该文经实验发现适用于低功耗蓝牙协议可视化分析的工具具有 Wireshark、CPAS 和 hcidump。

Wireshark 可以从 btsnoop\_hci. log 日志中解析出低功耗蓝牙报文,解析结果仅以嵌套的形式表示协议封装关系,保留识别码和数据组织格式等具体参数,适于分析设备双方的读写流程并解读设备的读写数值。CPAS(ComProbe protocol analysis system)是 Frontline 公司提供的蓝牙协议分析软件,其可以将 btsnoop\_hci. log 日志解码为可读性更强的树状结构,但解码结果中不包含识别码等参数,因此无法获得具体读写内容,仅适于粗略分析通信流程。hcidump 是 Kali 系统自带的低功耗蓝牙抓包工具,通过终端命令行进行操控,结果显示可读性较差,适用于对实验结果进行补充性分析。

## 3 低功耗蓝牙安全实验与教学应用

### 3.1 协议安全性分析实验

行走步数记录和闹钟提醒是手环的基础功能,分别对应低功耗蓝牙协议中的通知、写请求和写响应等传输模式。本实验选取步数记录功能和闹钟设置功能的具体交互过程作为研究对象,通过测量上述传输模式的协议报文并解析其安全性,为低功耗蓝牙的攻击与防御提供实验基础。

#### 3.1.1 配置与操作

##### (1) 实验环境配置。

- ①手机获取 Root 权限;
- ②下载 XposedInstaller 应用后安装 Xposed 框架;
- ③手机安装嗅探工具 MX 蓝牙抓包模块;

##### ④PC 端安装协议分析仪器 Wireshark, CAPS。

##### (2) 实验设备操作。

对照低功耗蓝牙通信机制(如图 1 所示),服务器端与客户端通过六种基本操作进行数据交互,实现相应功能。针对客户端与服务器端之间的数据交互,选取手环的闹钟设置和行走步数记录两个功能为实验研究对象,采用“btsnoop\_hci. log 日志+Xposed 模块”的协议测量方法对两者分别进行实验,解读语义、语法和时序等设备通信配置信息,设备配置操作具体步骤如图 4 所示。

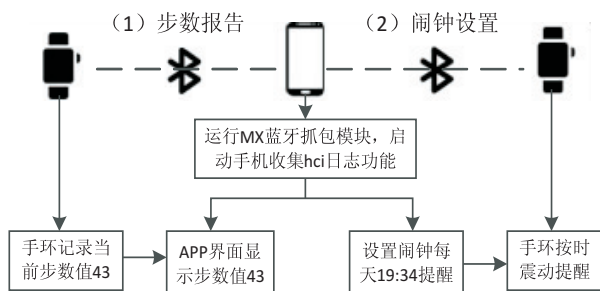


图 4 设备配置操作的具体步骤

#### 3.1.2 测量与分析

##### (1) 步数报告。

通过佩戴手环行走测试发现,手环向手机传输步数信息时,根据 Xposed 模块 MX 蓝牙抓包模块所显示的字段可知,此时手环先后分别以通知的形式向手机中 UUID 值为 0000ff06 的特性传输 8 位步数值信息代码 2a000000、2b000000 和 2c000000。为进一步解读低功耗蓝牙的通信机制,将 btsnoop\_hci. log 日志导入 Wireshark 中,找出上述过程对应的实际报文,结果如图 5 所示。

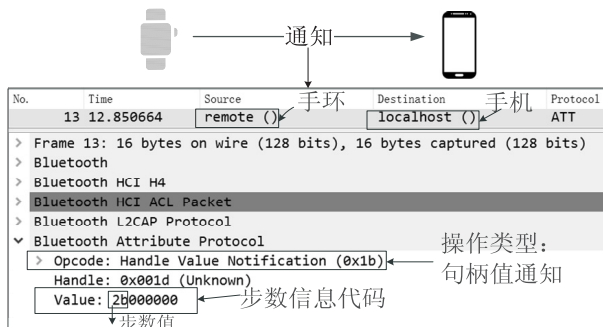


图 5 步数报告关键报文

由图 5 可知,手环具体采用句柄值通知 (handle value notification) 的方式向手机传输步数信息。句柄值通知是保证客户端及时接收属性状态更新信息的重要机制,当服务器端的属性状态更新结束后,可以在任意时刻主动发送该通知,并且不要求客户端返回响应报文,适用于对信息时效性有一定要求的传输场景。值 (value) 是步数信息的表示代码,由 8 位十六进制数组成,非零部分是当前步数值,当值为“2b000000”时,

对应手环所记录的用户行走步数为 43 步。

## (2) 闹钟设置。

在手机端打开闹钟提醒模式,在手机端设置手环于每天的 19:34 按时震动,此时从 MX 蓝牙抓包模块显示字段可知,手机以写请求的形式向手环中 UUID 值为 0000ff05 的特性写入 22 位闹钟设置信息代码 040101140211132211007f。为进一步解析其中的传输控制细节和具体含义,将此时生成的 btsnoop\_hci. log 日志导入 Wireshark,筛选出步数信息传输的实际报文,结果如图 6 所示。

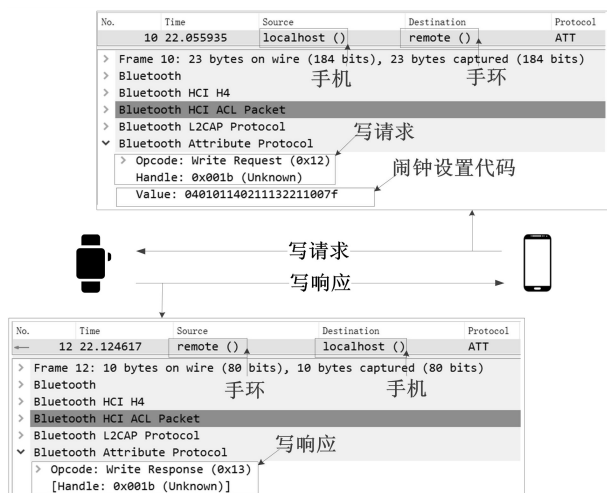


图 6 闹钟设置协议报文解析

通过实际操作反馈并且结合图 6 协议报文解析结果可知,用户在手机端设置闹钟提醒后,手机向手环发送携带闹钟设置信息的写请求,向句柄 0x001b 写入值“040101140211132211007f”,其中“132211”由高到低依次表示十六进制计数的时钟、分钟和秒钟,转换成十进制可得闹钟设置提醒时间为 19:34:17,对应设备操作部分的 19:34 提醒配置。当手环接收写请求并修改对应特性值后,向手机返回对句柄 0x001b 的写响应,写响应不含任何数值,仅用于流控,一旦手机收到了确认信息,它便能确定手环收到了携带闹钟设置信息的写请求。

## 3.2 重放攻击与防御实验

从以上实验结果可以看到,手环与手机之间采用明文方式进行数据传输,用户数值信息易被第三方设备探测并解析,这是进一步开展攻击与防御实验的基础,以下以重放攻击为例展开实验。

### 3.2.1 操作与配置

本实验设计通过配置蓝牙适配器的 PC 机作为攻击端,向周围存在的手环发起重放攻击并探讨防御措施,PC 机连接蓝牙适配器并安装 Kali 系统,通过 Kali 系统的嗅探工具 hcidump 监听低功耗蓝牙协议报文,再利用 Kali 系统的低功耗蓝牙调试工具 gatttool 发送伪造报文从而实现重放攻击。整个攻击过程中,

hcidump 实时监听蓝牙适配器接口,从而实现对实验数据测量和可视化分析,实验拓扑如图 7 所示,图中设备地址均为蓝牙地址。

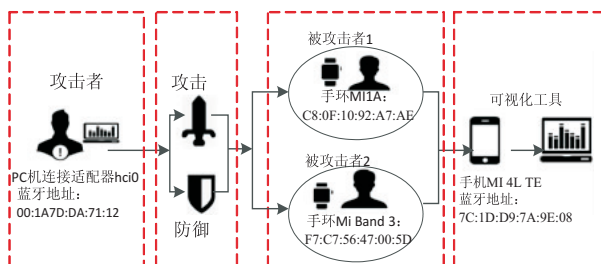


图 7 重放攻击实验拓扑

### 3.2.2 测试与分析

重放攻击就是伪造窃听到的报文,再重新发送给数据接收方,扰乱接收方正常工作,进而破解设备的数据保护机制。数据的嗅探和解读是重放攻击的基础,在数据未加密的情况下,攻击者可直接读取截获到的报文中显示的配置信息向设备发起重放攻击,具体实验划分为三个步骤:①对正常通信部分的关键报文进行解读,获取消息提醒功能实现的数据配置信息;②利用 gatttool 向手环重新输入对应命令,观察其是否与正常通信时的现象相吻合;③最后对实验结果进行分析,提出防御措施。

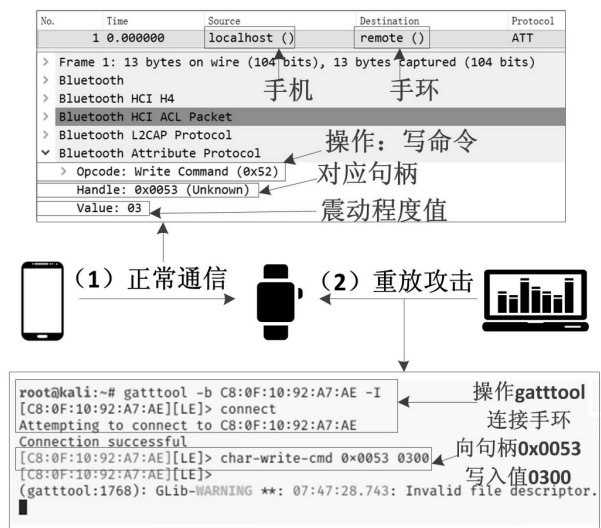


图 8 重放攻击过程可视化

#### (1) 正常通信。

重放攻击前,在手机应用中打开手环消息接收设置,手机接收到其他应用的消息提醒后,手环随即开启震动模式提醒用户。上述过程实际关键报文如图 8 所示,句柄 0x0053 对应的特性控制手环的震动模式,数值 03 为震动程度值,向句柄 0x0053 写入数值 03 即可使手环震动。

#### (2) 重放攻击。

首先在 kali 终端打开抓包工具打开抓包工 hcidump,具体命令 hcidump;然后选中目标进行连接,

使用低功耗蓝牙调试工具 gatttool 连接被攻击手环,具体命令:gatttool -b C8:0F:10:92:A7:AE -I;最后,向目标设备发起重放攻击,更改震动功能对应特性值,具体命令:char-write-cmd 0x0053 0300。

打开 hcidump 运行窗口查看蓝牙接口的报文收发记录,如图 9 所示。

```
root@kali:~# hcidump
HCI sniffer - Bluetooth packet analyzer ver 5.50
device: hci0 snap_len: 1500 filter: 0xffffffffffffff
< ACL data: handle 70 flags 0x00 dlen 9
  ATT: Write cmd (0x52)
    handle 0x0053 value 0x03 0x00
> HCI Event: Number of Completed Packets (0x13) plen 5
  handle 70 packets 1
> HCI Event: Disconn Complete (0x05) plen 4
  status 0x00 handle 70 reason 0x13
Reason: Remote User Terminated Connection
```

图 9 hcidump 抓包记录

可知 PC 机采用写命令的方式向手环发送了向句柄 0x0053 写入新值的命令,此时手环震动,重放攻击成功。

### (3) 攻击结果分析。

如图 8 所示,手机接收到消息后,通过向手环的句柄 0x0053 写入值“03”触发该手环震动。随后攻击端 PC 机伪造该过程,利用低功耗蓝牙调试工具 gatttool 中的“char-write-cmd”命令,将手环的句柄 0x0053 对应的属性值修改为 0300,达到手环非正常震动的攻击效果。通过对正常通信过程与重放攻击过程的关键报文对比可知,手环的通信系统不使用数据加密保护机制,攻击者可通过截获到的关键报文直接获得手环内部功能的配置信息,对手环发起重放攻击,危害手环的正常运行。

### 3.2.3 攻击防御

分析重放攻击实验过程发现,攻击者可从手环与手机间的通信报文中解读出用户的个人数据信息,实施对手环的信息窃取、报文伪造和数据篡改。针对实验中可穿戴设备所暴露的安全威胁,提出以下防御方法。

(1) 将可穿戴设备与可信任的手机进行绑定,从通信源头保证信道的安全性和可靠性。作为用户,为保证个人信息安全,在进行蓝牙连接时谨慎确认所连接的对象是否合法,并在不使用设备时有意识关闭蓝牙功能。

(2) 开启手机防火墙。在手机端开启防火墙模式可有效阻止恶意攻击者的渗透侵入,从而保护应用中的用户个人数据和可穿戴设备配置信息,防止攻击者利用窃取到的关键数据发起攻击。

(3) 开启加密保护措施。低功耗蓝牙设备与手机进行数据传输时,可通过密钥鉴别待连接设备的合法性,对通信数据进行加密保护。

在实验教学中进行防御下的重放攻击验证实验,

学生可借助蓝牙扫描工具识别出潜在的非法设备,当非法设备进行攻击时手动断开蓝牙连接,并查看此时的数据报文交互过程,如报文显示连接失败,即可验证该方法可有效防御攻击。

## 4 结束语

可穿戴设备是现代工业制造与新一代生物、信息技术融合发展的产物,深刻体现了“人-机-网”深度互联支撑人类智慧生产生活的新一轮科技创新理念,在“万物互连”浪潮中开辟出又一战略性新产业领域。在新技术新模式新产业驱动新经济社会发展的大背景下,高校实验教育教学面临新的机遇与挑战。

该文提出基于“手机+可穿戴设备”开展低功耗蓝牙协议安全实验,既在实验技术层面为高校开展可穿戴技术理论与实践教学提供了高效易行的新方法,同时又在教学改革层面探索出基于手机、手环等个人设备当堂开展理论与实践一体化教学的新模式,对高校实验教学深入推进国家一流本科课程改革和瞄准未来新移动应用领域开展“新工科”建设提供了切实可行的新途径。

### 参考文献:

- [1] GOMEZ C, OLLER J, PARADELLS J. Overview and evaluation of bluetooth low energy: an emerging low-power wireless technology[J]. Sensors, 2012, 12(9): 11734-11753.
- [2] WANT R, SCHILIT B, LASKOWSKI D. Bluetooth LE finds its niche[J]. IEEE Pervasive Computing, 2013, 12(4): 12-16.
- [3] 马忠丽, 梁天添, 王乐. 基于蓝牙技术的数据无线传输实验系统设计与实现[J]. 实验室科学, 2010, 13(4): 70-72.
- [4] 倪林, 张义红, 杨义. 基于物联网的短距无线通信系统实验[J]. 实验室研究与探索, 2014, 33(11): 100-102.
- [5] 高明华, 肖佳豪, 许丽金, 等. 基于 App Inventor 设计的蓝牙通信实验的开发[J]. 实验技术与管理, 2018, 35(3): 128-130.
- [6] 王振杰, 王强民, 杨小玲. 基于移动云交换的智能 IoT 系统[J]. 计算机技术与发展, 2018, 28(10): 199-204.
- [7] PEREZA J, ZEADALLY S. Privacy issues and solutions for consumer wearables[J]. IT Professional, 2018, 20(4): 46-56.
- [8] 王静, 朱祎. 可穿戴设备下免密支付的安全性研究——以小米手环和支付宝相结合为例[J]. 科技和产业, 2017, 17(5): 144-152.
- [9] 刘强, 李桐, 于洋, 等. 面向可穿戴设备的数据安全隐私保护技术综述[J]. 计算机研究与发展, 2018, 55(1): 14-29.
- [10] 刘晴晴. 面向智能设备的蓝牙非协作式攻击技术研究[D]. 西安: 西安电子科技大学, 2019.

(下转第 122 页)