抗疫用蓝牙健康监测设备信息安全实验技术

张 蒙[1],胡曦明[1,2*],吴振强[1,2],王 亮[1,2]
(1. 陕西师范大学 计算机科学学院,陕西 西安 710119;
2. 现代教学技术教育部重点实验室,陕西 西安 710119)

摘 要:面向大众随时随地开展生命体征常规监测成为疫情防控的刚性需求,家用级蓝牙健康监测设备凭借廉价、易用的产品优势契机跨界填补医用刚需的同时也因产品的信息安全认证缺失造成安全隐患,聚焦现实需求经文献调查发现不依赖专业检测环境的蓝牙设备信息安全实验技术成为确保疫情防控信息安全的新课题。在此基础上,提出了基于个人移动端“手机+笔记本电脑”打造模块化、便携式、轻量级蓝牙健康监测设备信息安全实验技术并给出总体架构以及检测接入、检测操作、报文分析、安全性检测等详细工作过程,实现对蓝牙体温计、蓝牙血压计的接入控制,信息保密性,信息完整性和身份认证等四项检测,为抗疫一线“随时、随地、随手”检测设备信息安全性提供新的技术途径。

关键词:疫情防控;蓝牙;信息安全;实验技术;网络安全
中图分类号:TP393 **文献标识码**:A **文章编号**:1673-629X(2022)05-0130-06
doi:10.3969/j.issn.1673-629X.2022.05.022

Bluetooth Health Monitoring Equipment for Anti-epidemic Information Security Experimental Technology

ZHANG Meng[1], HU Xi-ming[1,2*], WU Zhen-qiang[1,2], WANG Liang[1,2]
(1. School of Computer Science, Shaanxi Normal University, Xi'an 710119, China;
2. Key Laboratory of Modern Teaching Technology, Ministry of Education, Xi'an 710119, China)

Abstract: Routine monitoring of vital signs for the general public anytime and anywhere has become an inelastic demand for epidemic prevention and control. With the product advantage of cheap and easy to use, the household bluetooth health monitoring equipment crosses the field to fill the medical inelastic demand, but it also causes security risks at the same time due to the lack of information security certification of products. Focusing on realistic needs, it is found through literature survey that bluetooth device information security experimental technology that does not rely on professional detection environment has become a new topic to ensure information security for epidemic prevention and control. On this basis, we propose a modular, portable and lightweight bluetooth health monitoring device information security experimental technology based on the personal mobile terminal "mobile phone + laptop" and give the overall architecture and detailed work processes such as detection access, detection operation, packet analysis, security detection, etc, implement four tests for access control, information confidentiality, information integrity and identity authentication for bluetooth thermometers and bluetooth blood pressure monitors, which provides a new technical way to test equipment information security anytime and anywhere on the frontline of anti-epidemic.

Key words: epidemic prevention and control; bluetooth; information security; experimental techniques; network security

0 引 言

随着疫情防控常态化,面向大众随时随地开展大规模、低成本、无接触式生命体征自动采集与监控井喷式爆发并成为疫情防控的刚性需求,而生活中常见的蓝牙体温枪、臂式体温仪、蓝牙血压计等蓝牙智能健康监测设备凭借价格低廉与简便易用的产品优势正好契合医院[1]、社区[2]、车站[3]、商超、学校等民生一线普及体温、心率、血压等生命体征常规性监测的急迫需求。这类家用级蓝牙电子消费品迅速填补并挤占医用级抗疫医护设备市场[4],由此催生众多无医用设备生产资质的信息产业厂家纷纷涌入并密集推出“枪、仪、计、器”等形形色色的蓝牙健康监测设备迎合疫情防

收稿日期:2021-06-28 **修回日期**:2021-10-28
基金项目:陕西省科技计划重点研发项目(2020GY-221);2021 年陕西省省级一流本科课程建设项目(166,陕教〔2021〕107 号)
作者简介:张 蒙(2000-),女,研究方向为计算机科学与技术;通讯作者:胡曦明(1978-),男,博士,副教授,硕导,研究方向为智慧教育、计算机教育。

控市场需求。

不可否认,应急之下家用级蓝牙健康监测设备成功跨界填补医用刚需,既可化解基层一线疫情防控“燃眉之急”,亦可助力信息技术产业拓展市场,但是家用级蓝牙健康监测设备的信息安全性也因跨界出现监管“真空”,现有国家食品药品监督管理体系尚未对此建立相应信息安全认证标准来规范生产厂商与产品市场,由此导致被监测民众的个人信息、生命体征和生活习惯等私密数据在采集与传输过程中因设备安全漏洞面临恶意盗用、非法篡改等严重安全威胁,研究一种适用于基层一线人员不依赖专业检测环境即可自主开展蓝牙健康监测设备信息安全检验的实验技术成为确保疫情防控信息安全的现实需求,同时也可倒逼厂商升级优化产品,以技术创新赋能健康监测细分市场育新机、开新局。

1　蓝牙健康监测设备信息安全研究现状

以中国知网(CNKI)收录 2008–2021 年的普刊和核刊为文献统计源,分别以关键词“可穿戴医疗设备”或“智慧医疗”并含“蓝牙”以及“安全技术”或“实验技术”,通过检索、筛选得到学术文献 23 篇,通过文献调查法和主题聚类分析蓝牙健康监测设备安全性技术发展现状与趋势,如表 1 所示。

表 1　蓝牙健康监测设备文献调查情况

研究主题	数量	具体内容	研究方向
系统方案	16 篇	加密方案 8 篇	面向理论
		认证方案 3 篇	面向理论
		综合设计 5 篇	理论与实践
协议与算法	4 篇	安全协议 1 篇	面向理论
		算法设计 2 篇	面向理论
		算法改进 1 篇	理论与实践
系统研发	2 篇	技术开发 1 篇	面向实践
		攻击检测 1 篇	面向实践
课程教学	1 篇	实验教学 1 篇	面向教学

(统计来源:2008–2021 中国知网 CNKI 收录期刊)

(1)偏重面向理论研究安全防御,缺乏面向实践安全检测。

总体来看,安全防御理论性研究文献占比 60.9%,集中聚焦三个主题。一是加密算法,例如武汉大学马方方提出基于本地差分隐私模型的隐私保护算法防御可穿戴设备数值型敏感数据泄露威胁[5],中国电子科技集团公司第二十研究所王乐提出基于匿名化算法与属性加密相融合的隐私保护算法有效实现用户隐私信息保护[6];二是认证方式,武汉大学王俊提出基于 PUF 和 IPI 的轻量级双因子认证协议有效阻止可穿戴设备面临的妥协和假冒等攻击[7];三是安全协议,信息工程大学耿君峰建立基于蓝牙安全查询、寻呼及会话更新安全协议防御用户位置隐私泄露威胁[8]。安全防护不等同于防御技术,其中还应包括真实场景下设备的安全效能检测技术,当前重防御理论研究而轻面向真实设备“真刀真枪”安全检测的失衡现状易导致“研”与“用”难以形成闭环。

(2)专业化安全检测技术服务于科研实验而非公共应用。

现有为数不多围绕手环、Fitbit、智能手表等蓝牙健康监测设备信息安全检测的研究,一方面是技术性综述,例如国防科技大学刘强基于可穿戴健康跟踪设备 Fitbit 进行可穿戴设备安全与隐私实例分析和隐私保护技术总结[9]。另一方面是高校、研究所等科研机构开展加密算法、安全协议研发过程中为实现原型验证服务的附属,例如天津大学金志刚基于物联网智能锁通过利用 CPN 模型分析仿真实验验证加固后的通信模型能更有效抵御非法重放攻击以及窃听[10]。

从技术特征分析,上述安全防护实验技术专业性强、操作复杂度高、实现成本大,仅适用于科研人员在实验室等专门环境下开展。着眼后疫情时代,常态化大众生命体征监测有升格为社会公共卫生服务保障体系重要组成的发展趋势,低技术门槛、便携高效可供实地实时检验蓝牙健康监测设备信息安全性的实验技术是保障防疫信息安全亟待研究的新课题。

2　基于个人移动端的信息安全检测实验技术

2.1　总体架构

遵循“随时、随地、随手”不依赖专业检测设备开展无损检测实验的设计原则和技术要求,提出基于个人移动端“手机+笔记本电脑”打造模块化、便携式、轻量级蓝牙健康监测设备信息安全实验技术,总体架构如图 1 所示。

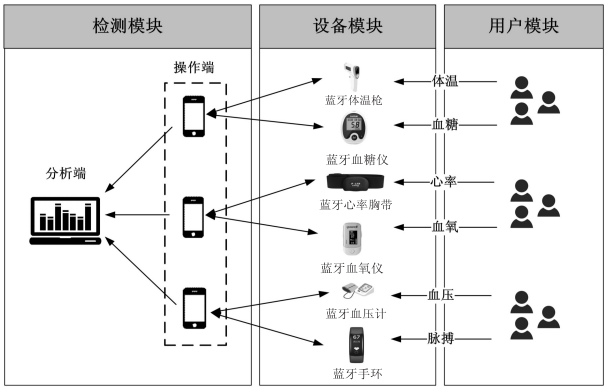

图 1　蓝牙检测设备信息安全实验技术总体架构

(1)用户模块。

在医院、学校、机场等社会公共场所,医务、安保、地勤等一线疫情防控工作人员,采用定点架设、手持临检或定时采集等方式对园区出入者、集中隔离者、重点人群等进行体温、血压、血氧、心率等常规性体征监测。

(2)设备模块。

体温枪、血糖仪、血压计等常用蓝牙健康监测设备,实现对被测者常规生命体征的实时、定时或阶段性采集,并及时将采集数据通过蓝牙传输至检测模块。

(3)检测模块。

采用“手机+笔记本电脑”,其中手机通过系统升级、APP 安装等操作将普通智能手机打造成安全检测“操作端”,可实现实时收集、监测上传的蓝牙报文并可向设备下发多种特定检测报文,整个交互过程由笔记本电脑通过 Wireshark 等可视化协议分析软件开展报文分析,报文交互与报文分析相结合从而实现安全性检测。

2.2 工作过程

蓝牙健康监测设备信息安全检测步骤以及对应的设备配置与详细操作,如图 2 所示。

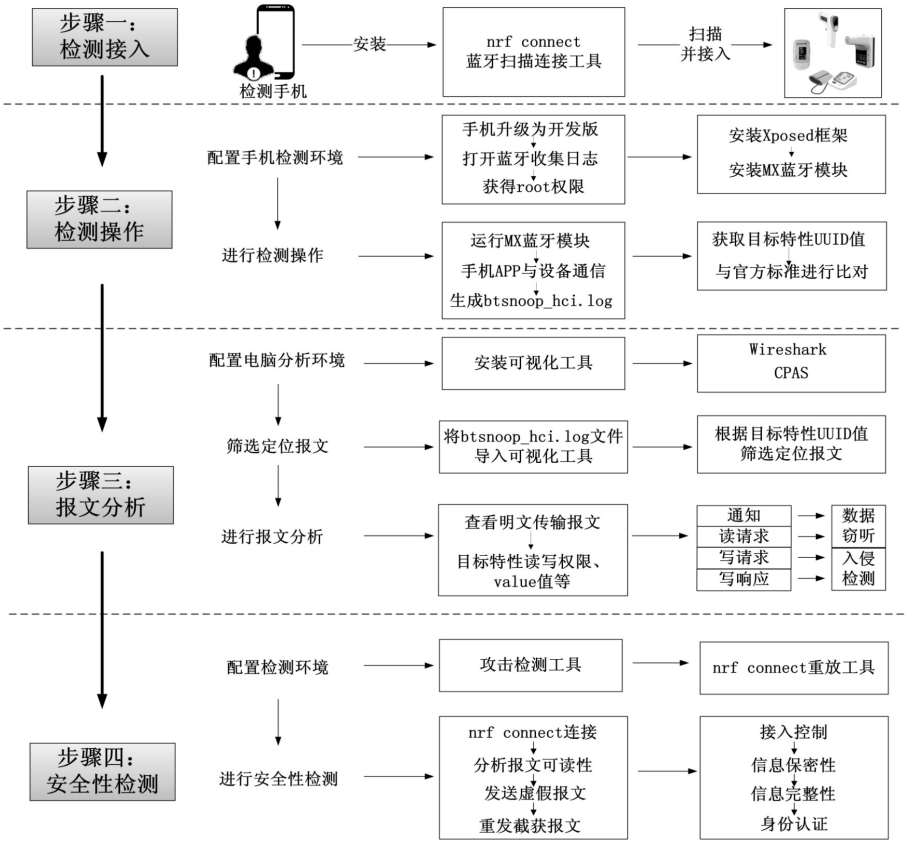

图 2 配置与操作

(1)检测接入。

按照“随时、随地、随手”开展检测的性能设计,操作端手机运行蓝牙扫描连接 APP(例如:nrf connect),先扫描获取被检测设备在蓝牙连接中的名称,再以该名称查找设备 MAC 地址,然后即可针对该地址进行发起检测接入。

(2)检测操作。

采用基于手机“btsnoop_hci. log+MX 蓝牙模块”的测量技术。btsnoop_hci. log 是 Android 系统自动生成的蓝牙调试文件,记录蓝牙设备与手机通信的所有数据,支持对蓝牙 hci 以上协议层的详细分析;MX 蓝牙模块是 Android 系统 Xposed 框架中提供蓝牙控制和测试的服务实体[11]。配置手机检测环境:手机系统升级后安装 Xposed 框架并运行 MX 蓝牙模块实时监测,获得目标特性 UUID 值和对应通知、读或写的内容;然后将该目标特性 UUID 值与 Bluetooth SIG 定义的“标准 Characteristics UUID 表格”进行比对查找,进而判断其含义与是否符合标准规定。“btsnoop_hci. log+MX 蓝牙模块”相比 EN-dongle 等专用设备的传统测量技术更加适用于抗疫一线非专业人员操作使用。

(3)报文分析。

检测操作过程中获取的 btsnoop_hci. log 是以机器可读的特定格式来记录蓝牙数据[12],只能通过可视化分析工具进行语义解析才能将其翻译为可读的协议报文。为此,采用“Wireshark+CPAS”,将 Wireshark 结构清晰的嵌套式报文结构和 CPAS 分析内容为自然语言的优点综合运用,实现对目标功能 UUID 值精准定位等深度报文分析。

首先,电脑同时运行 Wireshark 与 CPAS,将操作端手机产生的蓝牙抓包日志 btsnoop_hci. log 导入电脑,根据检测操作阶段获得的目标特性 UUID 值精准筛选定位报文;然后,利用 Wireshark 和 CPAS 判断该设备是否为明文传输,若为明文传输则进一步读取目标特性值的读写权限、value 值和句柄值等关键信息;最后,通过 CPAS 实现对通知、写操作等关键报文的分析,为安全性检测提供支撑。

(4)安全性检测。

面对市场上种类繁多的蓝牙健康监测设备,如何基于“手机+笔记本电脑”而非专业检测设备,实现高效、便捷并且较为全面与有深度的信息安全性检测是关键。该文设计四类针对性安全检测项,分别是:接入控制、信息保密性、信息完整性和身份认证,形成有效涵盖健康监测设备工作全流程的信息安全检测链。

接入控制:在用户手机正常接入被检测设备的情况下,检测手机运行实验 APP(例如:nrf connect)针对被检测设备新发起强制性接入请求,利用多端同时接入设备的互斥性[13],实现对设备准入、用户认证等接入控制的安全性检测。

信息保密性:检测手机捕获与被检测设备的通信报文,利用笔记本电脑可视化工具读取报文内容,分析报文是否明文传输、目标特性格式和内容,实现对编码格式、加密程度等信息保密性的安全性检测。

信息完整性:在报文分析的基础上,利用检测手机运行手机实验 APP(例如:nrf connect)在未经授权情况下向被检测设备发送格式正确、内容更改的虚假报文,判断设备是否能保持数据真实性和可信性,实现对数据恢复、检验修正[14]等信息完整性的安全性检测。

身份认证:检测手机作为中间人截获用户手机与被检测设备通信报文后,运行重放工具(例如:nrf connect)向被检测设备发送相同报文,利用设备鉴别可信任用户和恶意攻击者程度以及资源访问、使用权限,实现对身份识别、授权机制等身份认证的安全性检测。

3　蓝牙健康监测设备信息安全性实验

针对市面畅销的蓝牙体温计、蓝牙血压计等多种抗疫用蓝牙健康监测设备作为被检测设备开展接入控制、信息保密性、信息完整性和身份认证等四项检测。

3.1　实验原理

利用手机实验 APP(例如:nrf connect)对被检测设备发起强制性接入请求实现接入控制检测;通过捕获并分析通信报文实现信息保密性检测;基于前两种检测获取信息,通过主动注入虚假报文或重放截获报文篡改数据或欺骗攻击实现信息完整性和身份认证检测,实验原理拓扑如图 3 所示。

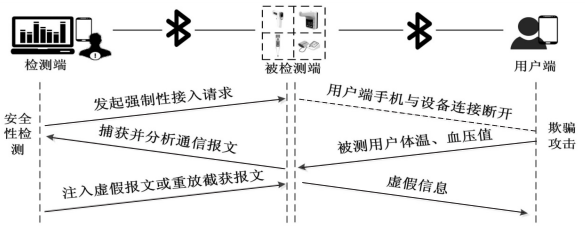

图 3　实验原理拓扑

在实验中的实验设备分工和参数如表 2 所示。

表 2　实验设备分工和参数

对象	分工	设备型号	蓝牙地址
	被检测端	Bluetooth Thermometer	98:DA:30:08:C3:74
	被检测端	Yuwell-BP-YE8900	C0:30:00:23:49:91
	检测端	Redmin 5A	D8:32:E3:94:CD:23

3.2　蓝牙健康监测设备的信息安全实验

3.2.1　接入控制

手机实验 APP nrf connect 进行接入控制检测。这款软件适用于中小学、医院等非专业设备、非专业人员使用,原因如下:一是该软件集合蓝牙扫描、连接和发送报文等多种功能;二是可直接在应用市场免费下载安装,获取方便;三是该软件可直接接入无密码、验证码等用户认证的蓝牙设备。实验结果表明,nrf connect 发出接入请求后顺利与设备建立连接,证明两种实验设备缺乏用于接入控制的用户认证等手段,如图 4 所示。

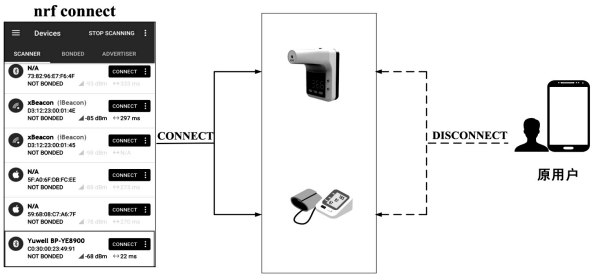

图 4　接入控制检测

3.2.2　信息保密性

(1)报文分析阶段得出蓝牙血压计当前时间设置功能为句柄值 0x0031,名称 Current Time、UUID 值 00002A2B 的写操作特性,写入内容在报文中以明文传输。报文显示手机将血压计时间设置为 2020/11/16/22:53:32,对应 MX 蓝牙抓包命令行语句为:00002A2B 写:E4070B10143520000000。简单分析得出十六进制表示的命令 E4070B10143520000000 对应十进制表示的时间 2020/11/16/22:53:32。

(2)报文分析阶段得出体温监测仪体温警报值通

知功能为句柄值 0x0012，UUID 值 4D540001 的特性，写入内容为 55AA090100017A0185，协议格式不符合 Bluetooth SIG 定义的“标准 Characteristics UUID 表格”，无法直接破译。根据反复测试（通过每次体温测量通知内容与此值进行比对），得出此值的含义为 37.8℃。两种设备信息保密性程度报文分析如图 5 所示。

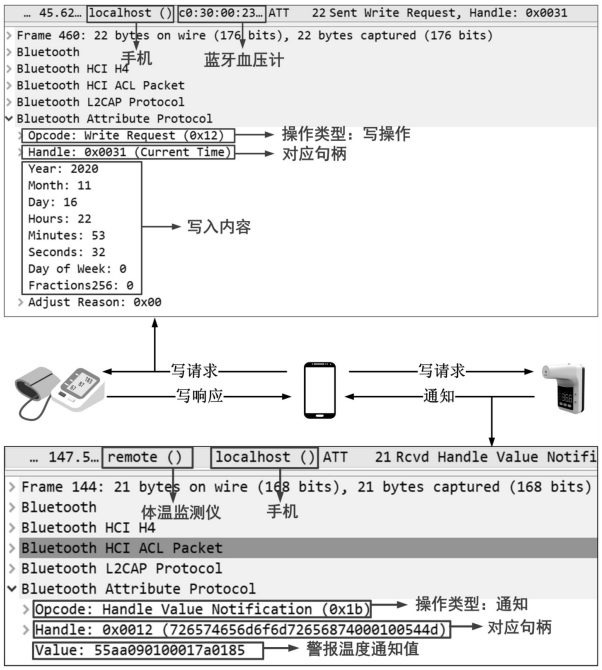

图 5 信息保密性检测

3.2.3 信息完整性和身份认证

（1）对蓝牙血压计的信息完整性检测。

MX 蓝牙模块显示当前时间设置语句为：00002A2B 写：E5070218152E18000000，依据之前翻译思路对应时间 2021/2/24/21：48：24，利用 nrf connect 向句柄值 0x0031、UUID 值 0x2A2B 的特性，写入 E5070218152E18000000，观察血压计当前时间又被改为 2021/2/24/21：48：24，与当前真实时间不符，数据被篡改导致蓝牙血压计的信息完整性被破坏[15]，如图 6 所示。

由此可知，十六进制命令前四位代表年，后面依次为月、日、时、分、秒，可以随意写入符合此结构的数据，例如向句柄值 0x0031、UUID 值 0x2A2B 的特性写入 F3070312152118000000，蓝牙血压计显示时间被更改为 2035/3/18/21：33：24。

（2）对体温监测仪的身份认证检测。

报文分析阶段得出体温监测仪写操作为句柄值 0x0010、UUID 值 4D540002 的特性，写入内容为 55aa050105，功能为设置体温警报默认值（37.8℃）。手机端 APP 向该特性写入此值后，体温监测仪会向手机通过句柄值 0x0012，UUID 值 4D540001 的特性发送一条值为 55AA090100017A0185 的通知，即在信息保密性检测阶段破译出的 37.8℃。以此为基础进行重放攻击。

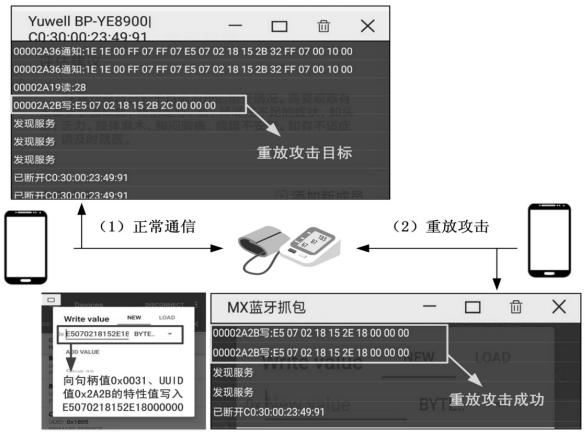

图 6 蓝牙血压计信息完整性检测

首先手机 APP 端更改体温警报值为 37.6℃，同时 MX 蓝牙模块显示手机向体温监测仪通过句柄值 0x0010，UUID 值 4D540002 的特性写入 55AA09020001780184（更改成功）。然后利用 nrf connect 连接体温监测仪，向句柄值 0x0010，UUID 值 4D540002 的特性写入 55aa050105，进行重放攻击，意图触发设置体温报警默认值（37.8℃）功能。MX 蓝牙模块显示体温监测仪再次向手机通过句柄值 0x0012，UUID 值 4D540001 的特性发送值为 55AA090100017A0185 的通知，证明重放攻击操作将体温警报值设置为默认值 37.8℃，查看手机 APP 页面验证，与预期结果相同，体温警报值通过重放攻击复置为 37.8℃，如图 7 所示。

图 7 体温监测仪身份认证检测

实验表明,此款体温监测仪缺乏身份认证机制,无法判断连接、通信对方是否可信任,攻击者很容易利用身份认证缺失漏洞恶意扰乱正常通信。

4　结束语

蓝牙健康监测设备现有身份认证机制、加密措施简单,数据编码[16]复杂程度低,黑客容易破译、攻击。通过数字签名技术[17]、时间戳技术[18]等加强设备本身的安全性,同时用户也应尽量减少在未知网络下的连接,减少隐私泄露的风险。

通过对不同种类蓝牙健康监测设备的安全性进行实验探究,分析对比不同品牌、不同产地的医疗设备的蓝牙传输协议,并进行不同种类的、轻量级、操作便捷的安全性检测,为非专业网络安全人员使用蓝牙健康监测设备过程中测试设备安全性提供了不依赖于专业设备的实验技术,为“抓抗疫、促发展、保安全”提供技术支撑。

参考文献:

[1] 陈　璇. 物联网技术在儿童医院的应用[J]. 物联网技术,2017,7(8):63-64.

[2] 方勇军,骆星九,邓亲恺. 监护仪在社区医疗模式中的发展与应用[J]. 医疗卫生装备,2013,34(1):86-88.

[3] 浙江省经济和信息化厅. 浙江:软件抗疫很“硬核”[N]. 中国电子报,2020-03-06(003).

[4] David Su. 2021 年物联网领域发展趋势预测:无线互联技术需求日益增长[J]. 单片机与嵌入式系统应用,2021,21(4):92.

[5] 马方方,刘树波,熊星星,等. 可穿戴设备数值型敏感数据本地差分隐私保护[J]. 计算机应用,2019,39(7):1985-1990.

[6] 王　乐,杨哲荣,刘容京,等. 基于属性加密算法的可穿戴设备系统隐私保护方法研究[J]. 信息网络安全,2018(6):77-84.

[7] 王　俊,刘树波,梁　才,等. 基于 PUF 和 IPI 的可穿戴设备双因子认证协议[J]. 通信学报,2017,38(6):127-135.

[8] 耿君峰,黄一才,郁　滨. 蓝牙位置隐私保护安全协议设计[J]. 系统仿真学报,2014,26(4):897-902.

[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] 金志刚,吴　桐,李　根. 基于短距离无线通信的物联网智能锁安全机制研究[J]. 信息网络安全,2019,19(10):16-23.

[11] 梁　敏,胡曦明,李　鹏,等. “手机+可穿戴设备”的低功耗蓝牙安全实验技术[J]. 计算机技术与发展,2020,30(11):111-116.

[12] 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.

[13] 荣雪宇,车忠根. 一款医用可穿戴计算机系统的设计与实现[J]. 计算机技术与发展,2011,21(7):206-209.

[14] WANT R,SCHILIT B,LASKOWSKI D. Bluetooth LE finds its niche[J]. IEEE Pervasive Computing,2013,12(4):12-16.

[15] PALLAVI S,NARAYANAN V A. An overview of practical attacks on BLE based IOT devices and their security[C]//2019 5th international conference on advanced computing & communication systems (ICACCS). Coimbatore:IEEE,2019:694-698.

[16] LOUNIS K,ZULKERNINE M. Bluetooth low energy makes " just works" not work[C]//2019 3rd cyber security in networking conference (CSNet). Quito:IEEE,2019:99-106.

[17] 王　煜,朱　明,夏　演. 非对称加密算法在身份认证中的应用研究[J]. 计算机技术与发展,2020,30(1):94-98.

[18] DIAN F J,YOUSEFI A,SOMARATNE K. A study in accuracy of time synchronization of BLE devices using connection-based event[C]//2017 8th IEEE annual information technology, electronics and mobile communication conference (IEMCON). Vancouver:IEEE,2017:595-601.