智能可穿戴传感系统（SWS）综合分析

1. 物联网的业务功能分析

1.1. 定义：智能可穿戴传感系统是指将各类提升人体体力或感知能力、监视人体健康的智能可穿戴设备所组成的系统。

1.2. 目前的智能可穿戴产品的存在形态

目前可穿戴设备主要有以下几种存在形态：智能眼镜、智能手环、智能手表及其他。

1.3. 智能穿戴的实现需要一个中心设备作为连接点——通常是智能手机。所有的设备都需要通过有线或无线的方式连接到中心点。

身体部位	设备举例	应用场景
头部	帽子、眼镜、耳机	疲劳检测、便携式电脑
脖子	项链，领带	智能控制、相机
身体	衬衫、夹克、领带	健康、姿势检测
腰部	腰带、	动作检测、定位
上臂	臂环	动作检测、加强上肢力量
下臂/手腕	手环、手表	健康检测、与手机交互、便携式电脑
手	戒指、手套	打开门锁、可触屏手套、智能语音助手
大腿	裤子	加强下肢力量
小腿	袜子	用于检测腿部受伤的压力传感器、姿势检测
脚	袜子	导航、健康检测

2. 安全问题分析

智能可穿戴设备的安全问题比较类似，以智能手环为例进行分析。

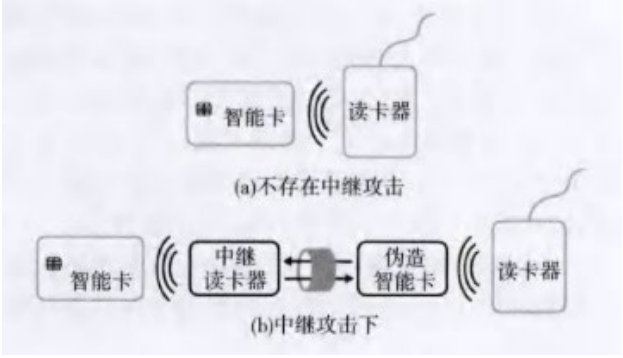
当下的智能手环有很多应用场景，不同的应用场景有不同的安全问题

2.1. NFC：部分智能手环中集成 NFC，可以用于交通卡、移动支付等场景。NFC 技术是通过射频波在两个设备之间进行短距离信息传输。也就意味着只要攻击者和被攻击设备的距离足够近，就可以用天线来接收所传输的数据，使得数据被窃取。这是 NFC 攻击的第一个场景，但由于需要很近的距离，因此这种攻击不常见。

NFC 的另一个重要攻击场景是数据篡改。即发送数据时，数据被监听者篡改，这里的

监听者不一定是第三者，甚至可能是设备的持有者。设备所有者可以通过篡改 NFC 传送的数据来欺骗与其通信的设备。

除此之外，最常见的 NFC 攻击是 NFC 中继攻击。如下图



NFC 中继攻击，即在智能卡与读卡器之间有一个中继的攻击者，窃取了智能卡中的信息，并模拟智能卡在读卡器上进行消费等其他操作。

NFC 中还存在一些其他的安全问题，不在此讨论。

2.2. 蓝牙

智能手环通过蓝牙与手机相连接并传送个人健康数据。目前市面上的智能穿戴设备多采用低功耗蓝牙技术，使用手机 APP 通过蓝牙与设备进行通信。这些设备往往使用 Just Work 配对模式，且对蓝牙指令的来源不经过认证，攻击者往往通过其他途径获取到设备的蓝牙指令后即可直接控制设备。虽然使用起来十分便利，但牺牲了安全性，隐私很容易被盗用。此外，与 NFC 类似，蓝牙也会存在中间人攻击，带来可穿戴设备的安全问题。

3. 防护方法探讨

3.1. NFC

对于 NFC 中存在的安全问题，仅针对中继攻击进行讨论。NFC 中继攻击本质上是扩大了智能卡与读卡器之间的通信距离，本质上无需理解传送的信息，因此无法通过加密来实现防护。由于扩大了通信距离，信息的传输时间会变长，可以利用这一点，测量消息从读卡器发出到接收到的时间，并将其与阈值对比，判断是否遭到中继攻击。

3.2. 蓝牙

对于蓝牙中存在的安全问题，一个最直接的方法就是让智能设备采用安全性更高的蓝牙协议，但这又会带来耗电量大的问题。可以考虑在软件上采用混合加密来增强安全性。

参考文献:

1. Adam J. Mills, Richard T. Watson, Leyland Pitt, Jan Kietzmann,Wearing safe: Physical and informational security in the age of the wearable device.http://www.sciencedirect.com/science/article/pii/S0007681316300805
2. Haselsteiner E, Breitfuß K. Security in near field communication (NFC)[C]//Workshop on RFID security. sn, 2006: 12-14.
3. 谢俊,刘军荣,陆海宁,林秋,谷大武,郭筝.RFID 系统与 EMV 系统中的中继攻击[J].信息技术,2015,39(12):13-16.