物联网研究-智能手环

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	IoT Research – Smartbands		
原文作者	Christian Funk	**原文发布日期**	2015 年 3 月 31 日
作者简介	Christian Funk 目前就职于卡巴斯基实验室，是卡巴斯基实验室全球分析和研究团队德国区的主管。https://de.linkedin.com/pub/christian-funk/98/b91/771		
原文发布单位	卡巴斯基实验室		
原文出处	http://securelist.com/analysis/publications/69412/iot-research-smartbands/		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
免责声明	本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

物联网研究-智能手环

Christian Funk

2015 年 3 月 31 日

摘要

如今，技术促进硬件和软件工具的开发以记录和分析我们生活的各个方面。这开辟了关注生活的新方式，并且以改善我们的健康和健身为目的。该领域的一大趋势健身追踪器（如智能手环）是当前最流行的形式，这是由一个我们戴在手腕的硬件设备与手机（用来控制该设备，获取和观察记录的数据）绑定使用的设备。我们将自己非常私人的及敏感的数据输入这些小工具，让它们了解最真实的自己。作为一家安全公司，这给我们造成了大问题：

- 收集哪类数据？
- 会有怎样的风险，风险在哪？
- 哪些组织会对掌握这些信息感兴趣，这会带来什么后果？
- 用户如何保护自己的数据？

本报告对来自三家龙头供应商的追踪设备和与其相应的移动应用进行了调查，以了解当前的安全状态及可穿戴健身追踪器的保密性。

它是什么？

量化自我，智能手环及人们要达到的目标。

我们经常衡量我们日常生活的各个方面，这是由于人想要确保安全的本性所致。我们通常会在某个特定的时间点为自己设定目标，并定期检查自己的表现如何。

我们通常会衡量：

- 贸易：财政目标、项目计划、薪资
- 健康：体重、身高、视力、健康指数
- 运动：心跳次数、骑单车或跑步的里程及高度、平均速度

但是，被称为“量化自我”的运动涉及更多。它希望超越常规。这一运动已经存在了多年，来自世界各地的人们相聚在一起交流信息、讨论他们的经验、并形成自我追踪的文化。通过测量日常生活中被传统的测量方案忽视的细节，寻找更健康，更有意义的生活。

目前，这种健康生活的视角吸引了大量的关注。多数上班族只有在上下班换乘过程中、购物或走向咖啡机时才得到锻炼。越来越多的人在家办公、网购，所以他们连家都不用离开。同时，人们比以往更关注自己的身体，无论是在健康方面还是在引人注目的外形上。

有几种测量我们的健康、健身及活跃程度的方法。心跳监视可以帮助我们控制锻炼，并得到我们身体状况的真实反馈。里程计帮助骑车者测量他们骑车所达到的里程数、高度和平均速度。 但以上这些工具的帮助有限。因为，在运动过后，它们就会被取下来，所以，其它日常活动如走路和工作都不会被记录。如果我们多部设备，每台设备上的数据依然是独立的且永远不相关。

我们将自己的个人资料输入健康追踪器，并诚邀它们了解最真实的自己。

智能手环是这样发挥作用的。我们要将设备全天戴在手腕上，以记录我们的活动水平、睡眠时长和睡眠质量。这一代的设备仍然记录单次快拍，但其高频记录集使它看起来像动态流。这有点像摄影，但有区别，它融合单次快拍和和拍摄，使用镜头的恒定流来创建动态影像。通过收购和关联不同的有关健康的恒定流，我们便可得到有关日常生活的额外利益和信息，其中一些利益和信息可能我们从来没意识到。这便描绘出一幅更完整的我们日常生活方式的画面。

人的本性就是不断追求突破。收集并可视化日常生活中我们的活动，有助于激励我们为自己树立更高的标准。有了智能手环，用户可以尝试击败自己的目标，并且也可以与家人、朋友、同事及其他来自在线培训组的人员一起比赛，进步。这些由供应商云网络的生态系统连接，也可以通过社交网络共享信息。

智能手环是什么，它们如何工作？

基础智能手环即一般采用橡胶为腕带表面以减震并防水的腕带。该设备的技术核心要么牢牢地嵌入该智能手环之中，要么以小胶囊的形式置于腕带内。如果腕带受损或随着时间的

推移被磨损，第二种款式允许用户改变腕带。

蓝牙模块：	主界面将收集到的数据上传到智能手机应用程序并下载新指令，如在规定的时间震动响铃。
振动马达：	正如其在智能手机一样，该马达通过使设备震动以通知用户某些事情，如电池电量低、预定时间响铃。
运动传感器：	与智能手机的运动传感器相似，该运动传感器监测回转并加速运作。供应商定义的算法接着将运动转化为易懂的单位，如步数。
电池：	基础智能手环的电池通常为 35 – 70 毫安，比智能手机的电池容量（2，000-4，000 毫安）小了很多。由于组件少，所以它们更节能，根据其收集的数据量和耗电功能开启的次数，智能手环可持续运作一到两周。
电源/同步按钮：	多数智能手环可一键操作以同步启动/关闭与之对应的手机。
电源插孔：	通过 USB 接口给设备电池充电。
显示：	基础智能手环提供 LED 或点阵显示，显示电池充电或类似时间或步数的基本信息。

功能

不同的智能手环具有类似的功能。它们都是基于测量活动程度、运动时长和睡眠质量，基于热量平衡信息等。

主要功能：

- 计步器和大致里程数
- 热量消耗
- 睡眠记录器（睡眠时长和睡眠质量）
- 自定义健身计划及与实际活动的对比

更多功能：

- 营养摄入及其与活动中所消耗热量的对比
- 好友列表、短信功能、活动对比
- 基于被测试的睡眠阶段设定温和的智能起床闹铃
- 秒表
- 训练图表
- 第三方扩展（如果有的话）

进一步探究整个系统

这些设备收集哪些数据？

本文研究的健身追踪器具有类似功能集，各供应商对该应用程序收集的数据达成了共识。

必须收集：

- 姓名 （或昵称）
- 出生日期（或出生年份）
- 身高
- 体重
- 性别
- 电子邮件地址
- 帐户密码

选择性收集：

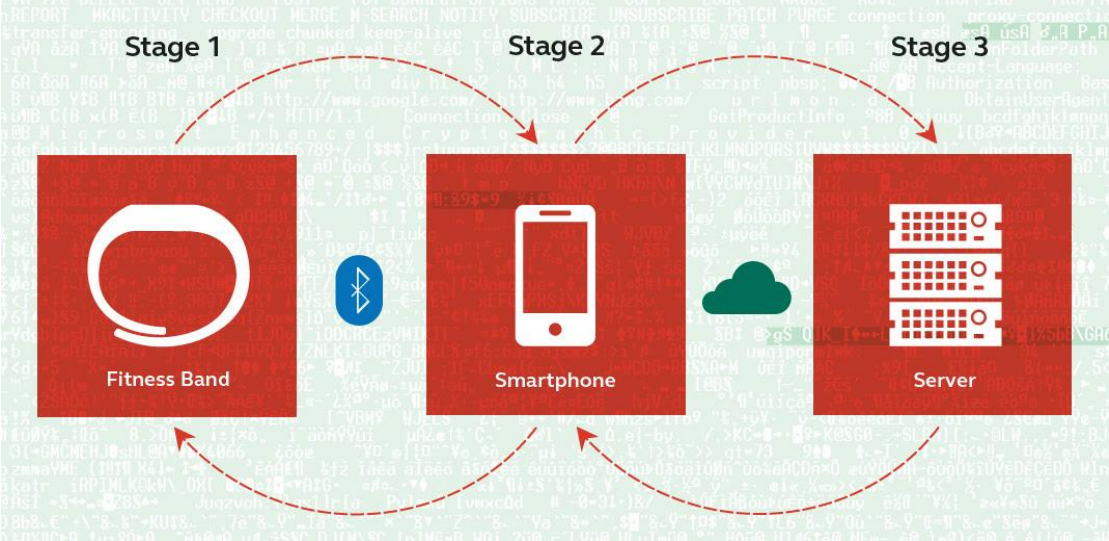
- 国籍
- 训练计划
- 体重目标
- 训练目标（每日行走步数，睡眠时长）
- 营养计划
- 照片
- 心情
- 使用相同健身追踪器的朋友
- 。。。。。。

该应用程序会自动显示从绑定手机获取的正确定位。可以调节体重和身高的计量单位，以便于用户在英制和公制系统之间进行选择，但是，该计量单位的初始设置和与绑定手机的定位一致。

有些健身追踪器允许用户控制他们在好友列表分享的内容，但不支持控制与云服务分享的内容。

收集及处理信息

数据采集和处理工作通过包含智能手环本身、智能手机（Android 或 iOS 系统）或计算机（使用 Windows 或 OSX 系统）在内的工作链完成，使用相应的应用程序来处理数据和供应商的云服务以提供深层分析，并存储历史数据。为了同步各个组件，该系统使用蓝牙和互联网（通过 3G / 4G，无线网络或有线连接）。



跟踪设备和手机之间的持续同步需要稳定的蓝牙连接。这对手机电池的使用时长影响很大。然而，追踪器可以在不进行同步的情况下，在任何地点都可持续存储 2-30 天（取决于设备和所记录的数据量）数据。为确保最佳的用户体验，多数供应商建议一直开启蓝牙。

第一步：记录数据并短期存储

第二步：处理并关联数据，发送控制智能手环的指令

第三步： 长期存储，基于网络界面进行更好的观察和深入分析

智能手环目前正处于过渡状态。该产品的流行正在促使更高级的产品进入市场，并且对不同款式需求在不断增长。目前我们所知道的智能手环的类型即基础智能手环；未来的智能手环将增加处理功能，而不仅仅是收集数据。一些公司已经有将智能手环与运动传感器，心跳监视器相结合的方案。

与云同步所需流量大约为每天 1-2MB，这取决于手环的模式、活动水平及其使用的功能。没有移动互联网平台支持的用户只能通过无线网络运行该需求。

潜在的攻击向量

一般来说，需要在同一个系统内进行数据传输的设备越多，该传输链就越容易受到攻击。多数智能手环环境使用上述方案。其它类型的健身追踪器关掉只能手环，其将数据记录在智能手机本身或不提供云服务。对于这类型的智能手环，不适用于某些攻击向量。

追踪设备和手机的同步

智能手环需要全天佩戴；然而，其用户可能会时不时地取掉手环。因此，就会出现手环在某段时间内无人监管，任何有兼容设备及相应的应用程序(通常是免费的)的人员，这时，理论上都能做到与该设备同步并获取其记录的数据。当该设备处于行窃范围时，数据可能被传送至盗贼的智能手机。

智能手环和健身追踪器内的信息，包括非常个人的用户资料。这些资料可能用来针对用户：

- 敲诈
- 在互联网上进行公开谴责

远不止如此，窃贼同样对受害者的训练计划感兴趣，因为他们可以通过受害者的训练计划掌握受害者的住所在哪些时间段没人在家。

好消息是，每个我们检测的智能手环都有针对这类风险进行综合保护的功能。其应用程序会与手机解绑，并通知用户该智能手环以断开连接。对于窃贼来说他们只能得到当前收集的信息，或是上次同步时的信息。然而，由于目前只对一小部分智能手环进行了测试，所以，这类攻击向量仍会应用于其他设备。

坏消息是，正如我的同事 Roman Unuchek 在他的博客“How I hacked my smart bracelet”（《我如何“黑”了自己的智能手环》）中指出的，该保护机制易受此类攻击的影响。此类攻击能够攻击认证进程，读取追踪器记录的数据并执行其中的代码。根据 Roman Unuchek 的研究，窃贼甚至可以在用户毫不知情的情况下劫持目标设备。

手机和服务器的同步

智能手机应用程序和云服务器之间的同步是一个交叉点 ,数据流不仅包括收集的数据还包括访问用户帐户的认证。智能手环是在几年前打入市场的，一些好奇的安全研究人员浏览流量；一场轩然大波紧随其后，很多供应商在此进程中失去了加密性，这意味着所有的数据都以明文传输，数据可以被任何人读取。

> 智能手机应用程序和云服务器之间的同步是一个交叉点。

幸运的是，本文测试的所有智能手环供应商都做了充分准备，他们都对自己的应用程序（TLS/SSL）进行了加密。这样，想通过无线网络盗用流量就没那么容易了。

攻击手机

随着新的样本数量向上扬函数一样不断增加，移动恶意软件一直是近几年的热门话题。2004-2013 年间，卡巴斯基实验室分析了近 200，000 个移动恶意软件代码样本。仅 2014 年就增加了 295，539 个样本。然而，远不止这些。这些代码样本会被重新使用且重新打包：2014 年，我们发现 4,643,582 个移动恶意软件安装包（其数量在 2004-2013 年发现的 10,000,000 个安装包之上）。 移动恶意软件的月攻击量从 2013 年 8 月的每月 69,000 起增加到 2014 年 3 月的每月 644,000 起（是之前的 10 倍）。

所有本文测试的智能手环供应商都对其应用程序（TLS/SSL）进行了加密。

典型的网络犯罪分子的作案手法即利用合法的应用程序或应用程序名作为他们传播恶意软件的载体（主要是对第三方应用程序的网站）。一个移动恶意软件通常仅打包在一个安装包内，但有时候，为了增加成功率，犯罪分子甚至会把几百个恶意软件打包在一个安装包内，继而发送给不同的用户群。适用于智能手环的恶意的伪造应用程序会请求用户的登录凭证，进而劫持该帐户及该帐户上的所有信息都是完全可行的。 与其他来自该被攻击手机的数据（如来自社交网络应用程序的入住登记 GPS 坐标）结合来进行进一步网络犯罪。

然而，智能手机的日常使用形成了更高的风险。这些设备很容易丢失。例如，据伦敦地铁系统报道，2013 年超过 15，000 部手机在地铁丢失。[1]。如果没有开启锁屏，任何一个拿到该手机的人都能看到手机内所有的信息，这也包括存储在健身追踪器的信息。本文测试的所有智能手环应用程序都没有单独锁定其应用程序的功能。

攻击云服务器

攻击者除了针对单个设备和用户外，还针对云服务器本身，并试图访问其中所有用户的记录。

正如某个领先的智能手环供应商的用户门户在 2011 年表明的，有时根本不需要复杂的黑客技能。所有的用户资料都由某知名搜索引擎编入索引，使对仅在这些用户资料中发现的

特有表达在互联网的搜索变得更简单。这时，用户可以选择将他们的资料设置为“私人”，但这些资料都默认设置为“公开”。此外，用户可以手动输入来描述他们的活动和一定的时限，如查找怎样对减肥最有帮助。这意味着，即使是最私人的 “活动”，包括时长及所消耗热量的信息对每个人都是公开可见的[2]。随后，供应商针对该问题采取了措施。这种情况，充分体现了错误配置和/或松懈的隐私政策很容易导致信息和隐私泄漏。

追踪器的用户可以选择将自己的资料设置为“隐私”，但这些资料都被默认设置为“公开”。

和传统的用户名+密码的模式一样，某智能手环供应商的 API（应用程序编程接口）允许用户通过用户 ID 和智能手环序列号访问自己的数据。然而 如果第三方拥有所需的信息，便可在用户毫不知情的情况下下载数据。

2014 年，我们发现了众多的针对网络服务器的 A 类漏洞，如 Shellshock 或 Heartbleed。这些攻击以更改 IP 地址脚本的方式对全世界展开攻击。该攻击所收集的数据量及其可能带来的影响尚不明确。云服务也未能幸免于此攻击，并被当做有利可图的目标。发现下一个大型漏洞只是时间问题。

其他潜在的陷阱

根据美国麻省理工学院的研究，某智能手环因为其他蓝牙设备（如计算机、手机和其他智能手环等）扫描用户环境而臭名昭著。该智能手环还收集这些设备的地址信息，并通过其手机应用程序将收集到的信息传送至该供应商的服务器。这样，该供应商便可创建每个用户的基础设施环境概况。

此外，该智能手环自身使用的 BTLE（蓝牙低功耗）使其能够不时改变设备地址来规避追踪佩戴者。然而，该供应商并没有使用这一功能。

伪造的智能手环应用程序，请求登录用户凭证是可行的。

某个被检测的智能手环应用程序为了深入分析用户的健康和活动 ,邀请用户安装来自第三方的附加应用程序来整合并关联收集到的数据。可能的扩展包括在训练过程中使用 GPS 记录关联标准数据，使用专用的应用程序作进一步的可视化，应用程序提供附加的体重控制模式，应用程序鼓励用户要健康饮食（如多吃水果），如果用户完成了所有目标，甚至还提

供奖金奖励（由未完成目标的用户支付）。

如果被整合，用户变自动同意与供应商分享这些数据。

最后一种是这几十年来的经典陷阱。为了图省事，人们往往选择一号通用。多数人有一个主要的电子邮件地址，该地址同样也是他在其他网站和服务的用户名。现在，如果这些帐户中的一个由于服务器端的攻击而被攻击（每周都会发生），或是由于恶意软件感染窃取某个机器的登录凭证，这意味着使用相同的密码的其他帐户处于大规模危险中。众所周知网络罪犯会用窃取到的帐户名和密码尝试着在各大门户网站进行登录，如网店，在线支付系统，社交网络和其他任何可能窃取现金的数字平台。

智能手环、健身追踪器和其他配件的商业模式

由数百万用户的智能手环和其他可穿戴设备收集的个人信息的洪流，激发了其他人员及网络罪犯对其的关注。

这类信息对不同行业的企业和机构具有很高的价值。

保险公司

保险公司根据风险评估进行运作。为了有效地做到这一点，必须收集并评估数据以计算收取客户适当的保费。收集的数据越有价值，越能好好发展企业业务。这边是健身追踪器发挥作用的关键。什么样的数据能比客户的实时数据流数据更好？在编写保险项目时，一些保险公司为想要分享他们自己的健身追踪器收集的信息的客户指定特别计划。同时也会向可以证明自己的生活方式健康，有旅游的付款凭单，并参加了额外的健身课程的客户提供资金奖励作为回报。[4]

被测试的智能手环中没有一种有锁定应用程序的功能。

怎么可能出问题？该方案可能会适得其反。想象一下，一个不反对极限运动的狂热的健身爱好者。如果其追踪设备和智能手机会定期发送有关其驱车前往一个臭名昭著的危险的山地车下坡的数据，会怎么样？智能手机发送的 GPS 数据和汽车以每小时 40 公里的速度从山坡开下来时，由于轮胎碾压石头而产生的额外的“步数”，这些数据都表明该健身爱好者可

能从事危险运动，并可能会让保险公司感到不快。基于该客户的高风险数据，保险公司会增加其保险费用。根据世界各地法律地位的不同，鉴于此追踪设备记录的数据，保险公司可能会拒保此类高风险客户。

除了健身跟踪器，还有其他工具和应用程序正在以实现最优量化而进行开发，像具有集成传感器的牙刷，可以通过三维蓝牙和专用智能手机应用程序的蓝牙来监测刷子的运动[5]。该应用程序包括迷你游戏来教授、激励和奖励用户，尤其是儿童。它还追踪用户多久刷一次牙，每次刷多久。保险公司（尤其是牙科保险）同样很乐意收集到此类数据。

企业

企业同样为他们的员工配备健身追踪器。已经有企业向员工提供这类设备以评估他们的健康，并激励向健康的生活方式迈进。英国石油公司（BP）提出了“员工健康计划”，员工被指定要达到某一目标，如果达到，公司会提供像健康保险费这样的奖励 [6]。想要参加此计划的员工要彻底暴露隐私，还应考虑到该项目的潜在后果。

广告业

目前市场上还没有允许用户选择禁止向云输入数据流的移动应用程序。因此，供应商可以迅速了解用户的习惯及健康状况。根据隐私策略，他们可以基于该用户的信息和活动来定制广告。即使是一般的娱乐或活动，广告也可以专注于特定的用户群，例如：初学者可以得到跑鞋和基础运动服，而针对资深运动员的广告，向他们提供更昂贵的设备，用于夜间出行的 LED 大灯，或者特殊的运动营养品。所有的报价都可以折合为用户的本国货币，并根据应用程序内设置的体重和身高，针对不同的性别提供合适尺寸的装备。

其他各方

北加利福尼亚发生地震后，智能手环供应商 Jawbone，在其博客发表了一个图表，该图表显示了此次地震对震中附件不同区域的人们睡眠的影响[7]。所有的数据来源于成千上万的客户，汇总并以匿名形式显示于该图表。该数据使 Jawbone 有了显示地震对人类影响的新形式，而不是像以往显示震中附近区域地震仪震动频率。世界各地许多新闻网站都刊登了此图表。

收集的数百万用户的个人资料激起了网络罪犯的

欲望。

2014 年标志着智能手环记录的数据第一次在法庭中使用，对于今后的案件开辟了道路。该案件中的女子，坦率地提供了其智能手环中的数据以证明她由于车祸而受伤，只能有限的活动。她的信息与第三方其他与她年龄相仿的女性的数据进行了比较[8]。该案件中数据的使用是没有争议的，该女子坦率提供了她的数据来证明她的观点。智能手环的用户要记住，供应商通常在其用户协议和隐私政策条款做出明确表示，用户可以公开信息以回应法院的命令。用户还要了解，所收集的数据不一定只能在数据收集国使用，同样也可在司法权不同的其他国家使用。

根据耶路撒冷的希伯来大学的研究人员，通过将用户的 GoPro 摄像头戴在头上并抖动它，可以在几秒钟内识别用户（根据某范例）[9]。这就提出了一个问题，根据这种算法，个体智能手环用户是否可以通过其活动和睡眠模式来识别。

有没有更私密的方式来追踪用户的健身

比智能手环更私密的替代品（自己了解为目的的），包括电子计步器和健身追踪器应用程序。两者都可以作为单一的设备系统，从而切断会影响普通智能手环系统的潜在的攻击向量。

健身跟踪器应用程序通常使用一个内部陀螺仪传感器和加速度计来追踪活动。追踪器的应用程序缺乏传感器来测量人们的睡眠，也没有其他智能设备的一些功能。被称为电子计步器的专用计步器的设备，提供类似的功能集，而且对智能手机来说比较省电。有些产品可以与智能手机进行同步，有些则是完全自行运作。它们可以揣在口袋里或夹在腰带上。

对智能手环用户的建议

为了尽量减少数据被泄露的风险，提几点建议。这些建议中的多数不仅适用于智能手环用户，也适用于任何一个使用存储个人资料应用程序的用户：

- 只使用你需要的功能，避免发布任何一条你不想存储于云的个人信息。
- 每个帐户都要使用级别高且不同的密码
- 开启智能手机锁屏，并使用访问保护。

- 如果可以的话，对手机进行加密。
- 如果可以，对每部设备使用安全解决方案。
- 阅读应用程序的许可协议，并留意该设备会使用什么样的个人信息。
- 安装应用程序并更新操作系统
- 卸载/删除不再需要的应用程序
- 在不需要的时候关闭手机的蓝牙和定位服务（这样也可以节省电池耗电）

结论

至今，智能手环已经打入市场将近十年，因此，与其他小配件相比，他们已被大家熟知。虽然像没有加密或公开用户配置文件的一些时日已久的安全问题仍然存在，但这表明，安全仍是许多公司今后要思考的问题。安全也是一个过程；越来越多的漏洞出现在驱动程序、协议和整个服务器生态系统，供应商需要检测漏洞和漏洞风景，并迅速修复客户端（智能手机应用程序）和服务器端（云服务）的漏洞以确保客户数据。

不过安全性同时取决于制造商和用户。每个参与房必须了解健身追踪器所收集的用户数据的价值和敏感性。通常，当发生了有关个人数据的攻击，用户的姓名、电子邮件地址、生日、信用卡信息或密码等数据都会受到影响。在这种情况下，受到攻击的信息更个人。它包含了健康和身体相关的数据，包括用户通常只向亲近的人吐露的细节，或者甚至是只会告诉医生的隐私。

智能手环供应商掌握着对第三方和用户都有很高价值的大量信息。但是，如果供应商决定向任意一方泄露这些信息（冒着失去用户信任的风险），第三方需要谨慎对待这些数。毕竟，万一用户将智能手环待在自己的宠物狗身上以获得数据，并想用这些数据来获取保险公司的优惠怎么办?

虽然智能手环是相对较早的技术，但他们仍然是促进我们利用的量化自己设备发展的一片沃土。与早期技术整合，并结合创新技术，新型设备正在不断涌现。像智能手表和谷歌 Glass 即这一领域的未来发展趋势。

附录：参考文献

(1) More than 15,000 lost mobile phones on London Underground pose security risks
http://www.v3.co.uk/v3-uk/news/2318727/more-than-15-000-lost-mobile-phones-on-london-underground-pose-security-risks

(2) Dear Fitbit users, kudos on the 30 minute of vigorous sex activity last night
http://gizmodo.com/5817784/dear-fitbit-users-kudos-on-the-30-minutes-of-vigorous-sexual-activity-last-night

(3) Security Analysis of Wearable Fitness Devices (Fitbit)
https://courses.csail.mit.edu/6.857/2014/files/17-cyrbritt-webbhorn-specter-dmiao-hacking-fitbit.pdf

(4) Insurance company Generali wants to collect fitness data from customers (German)
http://www.heise.de/newsticker/meldung/Neue-Krankenversicherung-Generali-will-Fitnessdaten-von-Versicherten-sammeln-2461512.html

(5) Kolibree, Smart Tooth Brush
http://kolibree.com/en/

(6) Wearables at work mean big business, says Fitbit CEO
http://www.cnbc.com/id/101318809#

(7) How the Napa Earthquake Affected Bay Area Sleepers
https://jawbone.com/blog/napa-earthquake-effect-on-sleep/

(8) Fitbit Data now being used in the Court Room
http://www.forbes.com/sites/parmyolson/2014/11/16/fitbit-data-court-room-personal-injury-claim/

(9) Egocentric Video Biometrics
http://arxiv.org/abs/1411.7591