我如何“黑”了自己的智能手环

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	How I Hacked My Smart Bracelet		
原文作者	Roman Unuchek	**原文发布日期**	2015 年 3 月 26 日
作者简介	Roman Unuchek 是卡巴斯基实验室的高级恶意软件分析员。 www.linkedin.com/pub/roman-unuchek/7b/b36/a49/en		
原文发布单位	卡巴斯基实验室		
原文出处	http://securelist.com/blog/research/69369/how-i-hacked-my-smart-bracelet/		
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，		

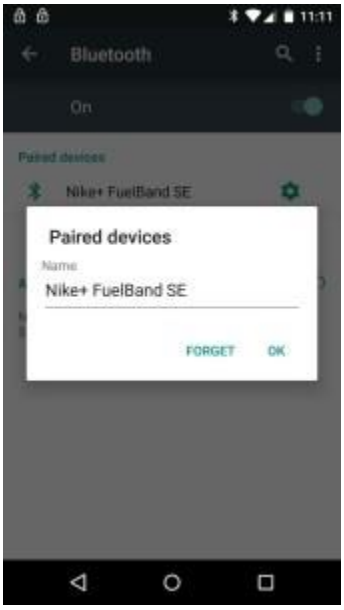
	及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。

我如何“黑”了自己的智能手环

Roman Unuchek

2015 年 3 月 26 日

故事始于几个月前，我得到了一个流行品牌的健身手环。这是一种可穿戴设备，所以我安装了特别针对可穿戴设备开发的 Android Wear 应用程序。该应用程序能够轻松地连接到健身手环。

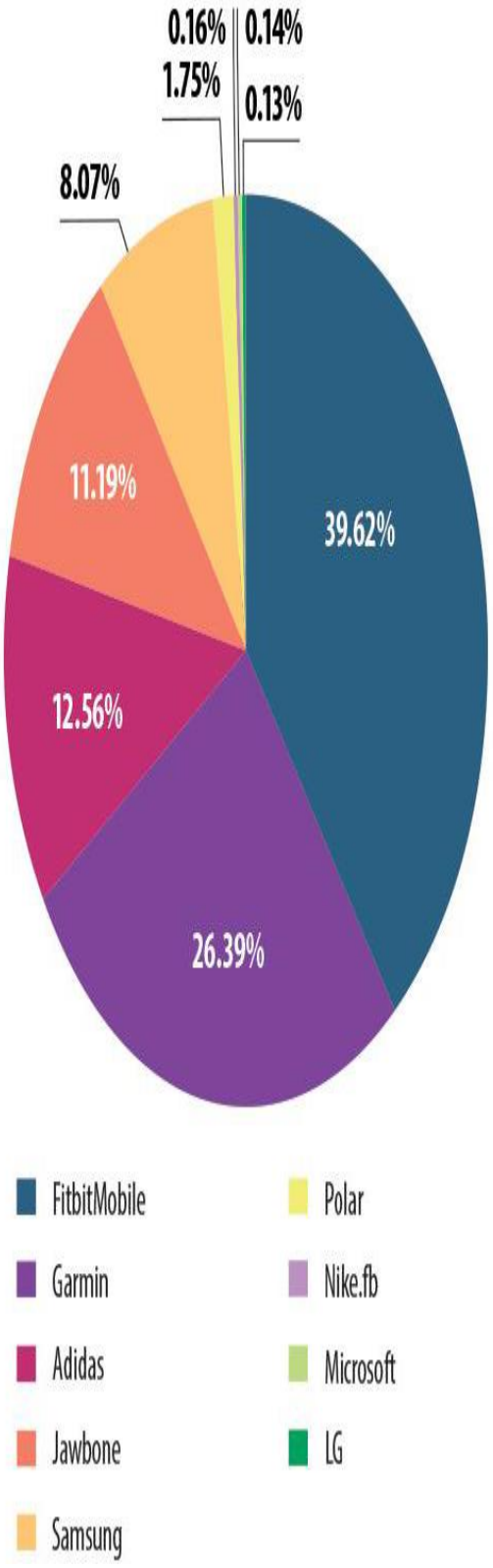


但是，有一些奇怪的问题：该程序可以连接到 Nike+ Fuel Band SE，但我的手环是另一品牌！不久后，我意识到我的同事有一个 Nike 手环--他甚至没有注意到我已经连接到他的设备了。

在那之后，我决定做一些研究，看看我的手环安全性如何。

智能手环：与智能手机通信

如今，市场上有很多品牌的手环。KSN（卡巴斯基安全网络）提供了控制流行的健身追踪器的 Android 应用程序在移动设备上的安装统计数据（统计数据来自自愿免费提供数据的 KSN 用户）。



控制不同制造商的健身追踪器的 Android 应用程序的安装情况

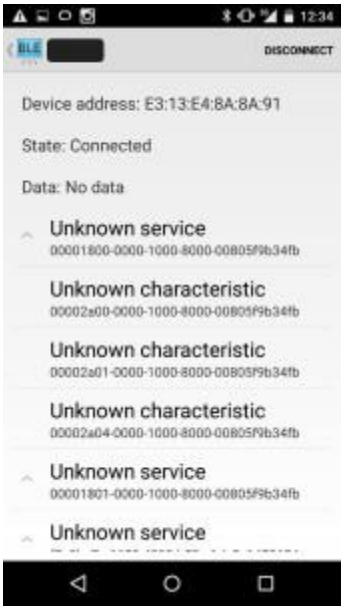
虽然这个统计表明了 Android 应用程序的普及（我们不能保证这些设备都有用户），但是也在一定程度上反映了可穿戴设备的普及情况。

为了与智能手机通信，大多数健身手环使用蓝牙 LE 技术（也被称为蓝牙智能）。对我们来说，这意味着设备可以用不同于常规蓝牙的方式连接。没有匹配的密码，因为大多数手环不具有屏幕和/或键盘。

在某些情况下，您可以在所有者不知情的情况下连接到可穿戴设备。

这些手环使用 GATT（通用属性资料），这意味着每一个可穿戴设备包含一组服务，而每一个服务又具有一组特征。每个特征包含一个字节缓冲区和一个描述符列表，并且每个描述符包含一个值：字节缓冲区。

为了证明这一点，我使用了 Android SDK 的一些现成代码--连接到蓝牙 LE 设备的应用程序通常这样做。我不必编写任何新的代码行；只是简单地在 Android Studio 中打开现有项目并点击启动。



上面的截图显示了我试图用这个应用程序连接到我的健身手环。在这里，我们看到了服务和它们的特征。然而，根据特征获取手环的数据是不容易的—这要求连接和验证。在一些其它设备的情况下，我可以根据特征和描述符读取数据。这可能是用户数据。

扫描

因此，使用 Android SDK 的一个应用程序，我可以连接到某些设备。之后，我开发了自己的应用程序，它会自动搜索蓝牙 LE 设备，试图连接到他们，并获取其服务列表。

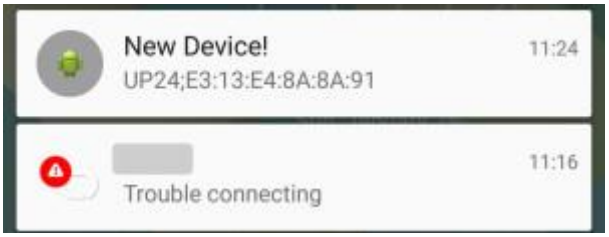
利用此应用程序，我进行了几次扫描。

- 在莫斯科地铁中，在 2 个多小时的时间里，我可以连接到 19 个设备：11 个 FitBit 和 8 个 Jawbone。
- 在美国华盛顿州贝尔维尤的一个健身房中，在 1 个多小时的时间里，我连接到了 25 个设备：20 Fitbit，其他 5 个分别是 Nike，Jawbone，Microsoft，Polar 和 Quans。
- 在墨西哥坎昆的 SAS2015 研讨会上，在 2 个多小时的时间里，我连接到了 10 个健身追踪器：3 个 Jawbone 和 7 个 FitBit。

从刚才 6 个小时的扫描中，我就能够连接到 54 个设备，尽管存在 2 个严重的限制：

1. 虽然规格表明了连接的最大距离为 50 米，但是在现实中，超过 6 米就很难连接到设备了。
2. 貌似无法连接到已经与另一部手机相连的设备。因此，如果您的手环连接到了您的手机，就没有人可以连接到它，甚至也不会扫描到它。

第 2 个限制应该意味着：当手环连接到智能手机时，它就不会被攻击。但实际情况并非如此。举例说明：用我的应用程序扫描时，我能够阻断我的手环与其官方应用程序之间的通信，即使它们是连接起来的。



可能的情况是：我发现的设备从来没有连接到手机，或者我扫描时手环时它未连接到智能手机（也许手机上的蓝牙被禁用了）。然而，还有一种可能：尽管存在连接限制，已经连接的设备仍然可以连接到其他手机。不管是什么原因，潜在的欺诈者有充分的机会来连接到健身追踪器。

然而，在大多数情况下，除了连接，还需要进行验证，以便访问用户数据。下面，我们来看看我的手环的验证过程。

手环的验证

为了在智能手机上验证手环，官方应用程序使用了 4 个可用服务之一。每个服务的每个

特征被标记为“CharacteristicNotification”--应用程序通知手环它希望获得该特征的任何变化的通知。然后，应用程序获取每个特征的描述符列表，并设置“ENABLE_NOTIFICATION_VALUE”标识，通知手环它希望获得每个描述符的任何变化的通知。

此后，其中一个特征改变其值--字节缓冲区。该应用程序从手环读取该缓冲区：200f1f 标头和字节数组，姑且称之为 authBytes。

该应用程序创建一个新的数组。该数组的第一部分是被包含在应用程序中的常数数组，以 6dc351fd44 开始；第二部分就是 authBytes。该应用程序接收来自新数组的 MD5 值，并将其以下述结构发送回设备：

- 标头（201210051f）
- MD5
- 验证字节

然后，应用程序将其中的另一个数组发送至设备。

在此之后，手环开始振动，用户只需按下按钮即可完成验证过程。

使用官方应用程序，验证过程需要约 15 秒。我已经开发了仅需要 4 秒就能使手环振动的应用程序。

让用户按下按钮并不难，只需要一点耐心。您可以一遍一遍地执行验证过程，直到用户按下按钮或走出有效范围。

从刚才 6 个小时的扫描中，我就能够连接到 54 个设备，尽管存在 2 个严重的限制。

验证完成后，我的手环上的数据就可以被访问了。现在，可穿戴健身设备并不包含多少信息。通常情况下，它们统计步数、睡眠阶段、前一个小时左右的脉搏等。应用程序大约每小时一次将这些信息发送到云。

在验证之后，很容易在设备上执行命令。例如，改变应该将字节数组（以 f0020c 开始）发送到设备的时间，将日期的形式改为 YYYY MM DD DW HH MM SS MSMSMSMS。

其他的健身追踪器就更简单了：对于其中一些，连接后可以立即获取部分数据；Nike 应用程序代码甚至没有进行模糊，可以很容易读取（一项研究的结果在此处）。

结论

我的研究结果表明，在某些情况下，您可以在所有者不知情的情况下连接到可穿戴设备。

通过攻击手环，欺诈者无法获得所有用户数据，因为数据并不存储在手环或手机中，而是定期从手环传输到云中。

健身跟踪器正变得越来越流行，并提供更广泛的功能。也许在不久的将来，它们将包含多个传感器以及更多的用户信息（往往是医疗信息）。然而，这些设备的创作者似乎没有充分考虑安全性。

试想：如果具备脉搏传感器的手环被黑客攻击，当您在商店查看价格时店主可以查看您的脉搏情况，也可能通过这种手段了解人们对广告的反应。此外，被“黑”的具备脉搏传感器的可穿戴设备可以用作测谎仪。

> 欺诈者可以控制您的手环，使之不断震动，以停止震动为筹码勒索钱财。

当然，也有可能出现更有害的行动。例如，通过使用赎金木马，欺诈者可以控制您的手环，使之不断震动，以停止震动为筹码勒索钱财。

我们将这些发现上报给了我的手环的制造商。该公司将此定义为 UX（用户体验）bug 而非安全问题。出于道德和安全方面的原因，我们在此不公开手环的名称和型号。如果您担心网络犯罪分子利用我们发现的安全问题，请立即联系您的健身手环供应商，询问您的产品是否受到本文所述方法的影响。

我们也希望这篇文章不仅对用户有益，同时也对手环供应商有益，使这些设备从 IT 安全的角度来看更加安全。