# 要知道，可穿戴设备也会被攻击

**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** | The Wearable Future Is Hackable. Here's What You Need To Know | | |
| **原文作者** | Gary Davis | **原文发布日期** | 2015 年 2 月 18 日 |
| **作者简介** | Gary Davis 是首席消费者安全专员，通过消费者镜头，他与内部小组密切合作，按照安全控件的需要，驱使产品战略的一致性。https://blogs.mcafee.com/author/gary-davis | | |
| **原文发布单位** | 迈克菲实验室 | | |
| **原文出处** | https://blogs.mcafee.com/consumer/hacking-wearable-devices | | |
| **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。<br>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。<br>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。<br>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。 |

# 要知道，可穿戴设备也会被攻击

Gary Davis

2015 年 2 月 1 8 日

几乎在现有的每部科幻电影内，都至少有一个有部分人类和部分机器特性的角色。他们是半机械人。《星球大战》中的 Luke Skywalker( 卢克·天行者) )拥有一只机器手；Robocop《机器战警》也是；《星际迷航》中的 Geordi LaForge 有一副可佩带护目镜。他们都依赖科技使自己的生活更便捷。

那样的半机械人未来时代已不是科幻小说，而是现实。你应该感谢日常作业中追踪、分析及协助你的可穿戴设备使之成为现实。这会是流行趋势：ABI 调查估计：截至 2019 年，将会有七亿八千万可穿戴设备投入使用，包括健康追踪器、智能手表、智能眼镜，甚至是心脏监护器。但是，穿戴式计算会带来某些风险。最突出的是：网络罪犯取得访问用户数据权的潜在风险。

网络罪犯是如何取得用户数据的访问权？

可穿戴设备空间内最薄弱的链接是用户的手机，而不是可穿戴设备本身。这是因为，可穿戴设备常常通过“蓝牙”（短程无线频谱）来链接用户的移动设备。此类频谱用来发送和接收可穿戴设备和手机间的数据。这使得用户的手机成为黑客攻击的首要目标。

通常，黑客通过恶意软件加载应用程序取得用户手机内数据的访问权。这类应用程序的设计常常旨在使其看起来像流行的应用程序，但其实确有很大不同即此类应用程序不标记版权追究。

黑客可利用这类恶意的应用程序开展种种活动，譬如，没有用户的允许拨打电话、发送和接收文本、通过 GPS 对用户定位、记录任何一个用户输入可穿戴设备的医疗问题。重点是：一旦他们得到用户移动设备的允许，他们就可以大量控制设备并拥有大量资源。

接着，黑客可利用这些数据进行不同形式的诈骗。难倒他们会骗你的医生开碰巧在黑市畅销特殊处方？是的，黑客正是如此。清晨出去慢跑？对窃贼来说是个好消息。此类个人信息仅仅是用于捕获用户的移动设备的皮毛。

然而，这类威胁并不局限于可穿戴设备。物联网（为分析和优化各类电子设备，如：洗衣机、电冰箱而把设备与互联网相连的现象）也会使用户数据处于危险中。但是，这些改变生活的设备可通过教育和行业规范（我们正在努力的两件事）来保护。

你要如何保卫你的可穿戴设备和个人信息呢？以下是几点提示：

- **使用 PIN（身份识别号码）。** 你所有的移动设备都应该有身份识别号码。这项基本的安保措施是阻止盗取你个人数据的临时黑客或窃贼的好方法。

- **限制共享。** 多数可穿戴设备不需要访问用户的所有信息。你可通过只输入可穿戴设备需要的信息来减少你的可穿戴设备共享机密信息的可能性。另外，经常核查移动设备内可穿戴设备应用程序的请求权限。难倒它真的需要访问你的位置、你的相册和你的通讯录？如果不是，务必要适当改变这些设置。

- **使用全方位安全防护。** 当然，保卫可穿戴设备环境内最薄弱的链接-手机，将会对维持你的数据安全有很大帮助。但是，当你储存智能手机备份的计算机也被攻击了会怎么样呢？你已经被 McAfee LiveSafe™服务所覆盖，我们的全方位安全解决方案几乎覆盖了你的每件设备。如果你的计算机已有防护，可免费将 McAfee Mobile Security 下载到你的 Android 或 iOS 设备上。