精译版

利用传感器窃取手机 PIN 码

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	Phone Hack Uses Sensors To Steal PINs		
原文作者	Tom Spring	原文发布日期	2017 年 4 月 12 日
作者简介	Tom Spring 是 Threatpost 的副主编。 https://www.linkedin.com/in/zpring/		
原文发布单位	Threatpost		
原文出处	https://threatpost.com/phone-hack-uses-sensors-to-steal-pins/124945/		
译者	安天技术公益翻译组	校对者	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
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。		

利用传感器窃取手机 PIN 码

Tom Spring

2017 年 4 月 12 日

研究人员利用智能手机生成的传感器数据创建了一种窃取用户 PIN 码的方法。研究人员表示，在确定手机用户输入的四位 PIN 码时，该方法的成功率达到了 74%。

英国纽卡斯尔大学的研究人员创建了一个名为 PINlogger.js 的 JavaScript 应用程序，该程序能够访问手机传感器生成的数据，包括 GPS、摄像头、麦克风、加速度计、磁力计、距离、陀螺仪、计步器和 NFC 协议。

纽卡斯尔大学计算机科学学院的研究员 Maryam Mehrenzhad 写道："研究表明，尽管存在这种威胁，但是人们并不了解其风险，大多数人对目前智能手机中 25 种不同传感器的大多数都不了解。"

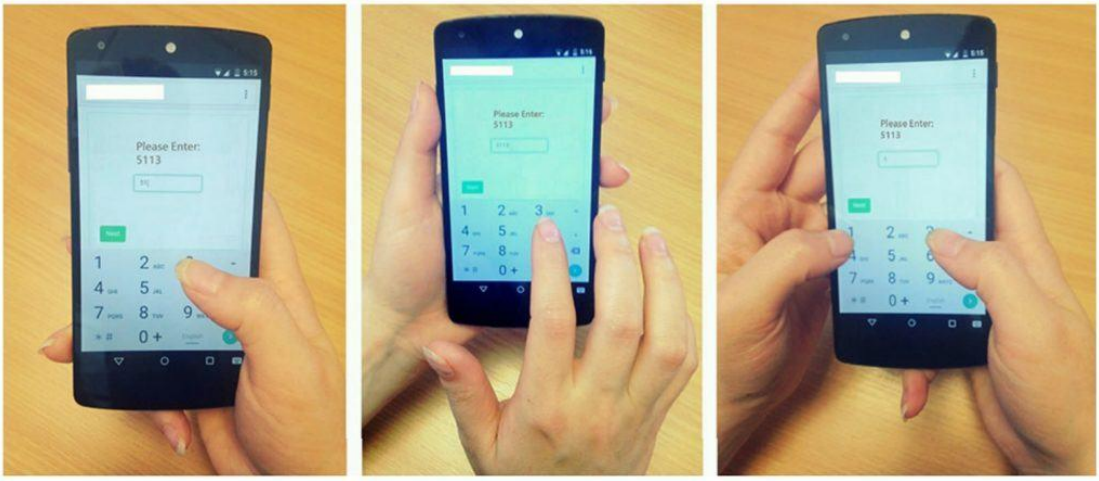
很可能的攻击场景是，用户被诱骗通过智能手机的浏览器访问恶意网页。该网站运行着 PINlogger.js JavaScript，能够通过浏览器捕获手机传感器数据。研究人员指出，移动设备上的许多传感器不需要用户允许，就能够利用网站或 web 浏览器应用程序收集传感器数据。

研究人员写道："假设，用户在使用移动浏览器时以 iframe 或其他标签的形式加载了恶

意网页内容。此时，攻击代码已经开始监听用户与手机的交互并获取传感器序列了。”

基于 JavaScript 的浏览器攻击会对用户构成安全威胁。研究人员在上周发布的报告中说，与应用程序攻击不同，浏览器攻击不需要安装任何应用程序，也不需要用户许可。研究人员使用 50 个 PIN 码的样本库，发现其脚本在第一次尝试时猜测用户 PIN 码的成功率是 74%，在第二次和第三次尝试时成功率则增加至 86%和 94%。

“根据我们打字的方式（无论是单手持手机，用大拇指打字，还是一只手持手机，另一只手打字；无论是触摸还是滑动），手机都会以某种方式倾斜，攻击者很容易识别与 Touch Signatures（触屏特征）有关的倾斜模式。”计算机科学学院的高级研究员兼研究合伙人 Siamak Shahandashti 写道。



用户在 PIN 界面的不同输入方法

研究人员指出，大多数用户关心诸如摄像头或 GPS 等显而易见的传感器，但是不关心不太明显的传感器。

“对于某些浏览器，我们发现如果您在手机或平板电脑上打开一个托管恶意代码的页面，在不关闭上一个选项卡的情况下打开网银账户，恶意代码就会窥探您输入的个人信息。”Mehrnezhad 说。

这也适用于处于锁定状态的手机，恶意应用程序或网站能够捕获用于访问手机的 PIN 数据。

研究人员表示，他们已经联系了浏览器供应商，告知了可能的攻击场景。

研究人员指出，一些移动浏览器厂商，如 Mozilla，Firefox 和 Apple Safari，已经解决了

部分问题。

以 Firefox 浏览器为例，从 46 版（2016 年 4 月发布）开始，该浏览器限制了 JavaScript 对运动和方向传感器的访问。研究人员指出，如果 web 试图被隐藏，苹果 iOS 9.3 的安全更新（2016 年 3 月发布）会暂停运动和方向数据的使用。

目前还不清楚 Google 采取了什么措施。研究人员在报告中指出："Google Chromium 团队的成员确认了这个问题，认为这个问题仍未得到解决。" Google 还未对该问题做出回应。

研究人员建议用户定期更改 PIN 码和密码。他们还建议用户在不使用后台应用程序和浏览器时将其关闭。

"请及时更新手机操作系统和应用程序，只从经批准的应用程序商店下载和安装应用程序，并审核手机上的应用程序的权限。"