安全小课堂六十四期【移动端设备指纹】

京东安全应急响应中心 2017-07-07

你可能已经习惯在打车、网上购物之后使用手机支付App付费，只要将手指轻轻放在Home键上，就可以完成付款，这种方便的体验是此前无法想象的。但显然，指纹识别技术也是经历了多年发展才变得成熟、易用。JSRC **安全小课堂第六十四期**，邀请两位老师分享移动端设备指纹技术，本期小课堂邀请到了**傅春奇**、**骑虎打狗**老师进行分享,同时感谢JSRC白帽子们的精彩讨论。

什么是移动端设备指纹？具体有哪些用途？

京安小妹

移动设备指纹是指通过在网站或者移动端嵌入脚本或SDK来采集终端用户环境的非敏感设备特征细信息从而建立一套设备标识库,相当于为每一位互联网用户的访问设备分配了唯一的设备标识。

在我看来，移动端设备指纹是指移动客户端鉴别用户操作设备唯一性的标识，也就是常见的设备绑定机制的识别信息。它一般应用于比较敏感app客户端（比如银行、钱包、理财）的设备激活上，用来充当用户的明文密码不慎泄露，被异地、不同设备登录时的二次保护校验，在一定程度上保护了账号安全；并且，从另一角度来讲，同一个账户登录设备指纹的新增、更换都会成为企业数据风控的重要指标。

讲师： 傅春奇、骑虎打狗

移动端设备指纹具体能解决什么问题呢?

京安小妹

移动端设备指纹首先能解决的就是账户安全问题。就如上面所说，设备指纹越来越多的被用于同一账户不同设备登录时的二次校验，为用户的资金安全带来了保证。另一方面从宽泛的角度，移动指纹的采集必然要收集用户使用的设备信息，这样企业就对用户群体的设备情况有了一个“大数据”层次的掌握，就好比有多少iphone土豪用户，多少小米大众用户等等，这样就便于更好的定位推介产品。
垃圾注册、刷单、羊毛党、刷投票、防撞库。在发现同一设备进行某些操作的次数过多，或者操作时间在不正常的时段，可以发出警报，进入二次验证的过程。
在广告营销方面，原始的线上广告投放是所有用户看到的都是同一个广告，有些用户未必需要，引起视觉干扰，影响客户使用情绪，最重要的是还造成了资源的浪费。而通过设备指纹，可以搜集用户访问网站信息，分析用户需求，进行深度的营销推广，实现更精准的广告推送。

讲师： 傅春奇、骑虎打狗

移动端设备指纹的实现原理是什么?

京安小妹

移动端设备指纹的实现首先是要采集到用户设备的基本信息，比如Android上可以是手机厂商、设备ID、手机卡信息、系统相关信息等：
基本原理是，通过多个条件进行区分，使得所有条件的具体选择能直接具体到每一个人。

讲师： 傅春奇、骑虎打狗

白帽子提问:移动端比pc端要安全，这个理解有问题么?

移动端很多时候只影响一个用户，web影响一大片。

讲师： 傅春奇、骑虎打狗

设备指纹技术还存在哪些问题（不足）？如何来提高呢?

京安小妹

第一个不足是即便是收集了设备指纹的多个维度信息，也无法确保设备唯一性，特别是Android手机上，山寨机共用一个IMEI、Mac地址的大有厂在，模拟器设备信息更是可以各种伪造。对于这种就是尽可能的收集更多的相关信息和不常用但具有标识作用的信息，让伪造成为困难；
第二个智能化趋势的不足就是设备指纹只识设备不识环境、不识人，很简单的例子就是我的手机丢了，被别人捡到，在相差比较远的地点、不常用的Wifi环境下启动了具有自动登录功能的APP，这时候单单依赖设备指纹就有问题了，所以大厂便开始采取“识人”：脸部识别、声音解锁、设备硬件指纹解锁等。
另外，如果成功掌握了设备指纹所使用的算法，通过hook修改，可以伪造“指纹”，所以进行“识人”是一个必要的过程。

讲师： 傅春奇、骑虎打狗

本期JSRC 安全小课堂到此结束。更多内容请期待下期安全小课堂如果还有你希望出现在安全小课堂内容暂时未出现，也欢迎留言告诉我们。

安全小课堂的往期内容开通了自助查询，回复“安全小课堂”或者点击阅读原文进行查看。

简历请发送：cv-security@jd.com

微信公众号：jsrc_team

新浪官方微博：京东安全应急响应中心

阅读原文