风控反欺诈之设备信息

目录

备注：部分内容来源于网络，如有侵权请私信管理 Vivian：wmyd80，谢谢

前言

随时互联网金融行业的发展，面临的黑产挑战越发严峻。而设备指纹在风控反欺诈中发挥着很重要的作用。今天仅针对于反欺诈之设备信息的全貌和关键细节介绍，应用场景不做深入解析。

反欺诈是风控的一个重要环节，也是一个很重要的技术范围。现在的贷款领域，多是采用获取用户设备指纹，获取通讯录，以及运营商报告，甚至其他外卖，网约车，社保，公积金，淘宝等的历史消费信息，依赖此进行审核，从而确定是否放贷以及提额或者降额标准。而在线交易本身很难进行唯一性身份确认，需要其他信息辅助判断，用户是否为本人操作等各种行为确认和行为分析。设备信息的应用就显得尤为重要。

一、定义

用我们个人身份证举例子，可以把手机设备理解成一个人，姓名（设备名称），身份证号码（设备序列号），身份证没有没有冒用（设备盗用篡改假冒等）。

所以说设备信息就是用于唯一标识出该设备的设备特征或者独特的设备标识。

二、常见元素

一般都是基于某些设备信息，通过一些设备指纹算法会将这些信息组合起来，作为该设备的唯一标识符，常见的元素如下

1）SIM 卡信息

2）WIFI 信息

3）硬盘信息

4）内存信息

5）摄像头信息

6）软件版本以及其他硬件信息

设备指纹一般都是基于以上内容，进行一个唯一 hash 值得构建，但是这方面就会有偏差，ios 的设备有些信息是无法获取到的，安卓会好很多，但是有人会说 H5 呢，怎么办？这个就各个公司不一样了，有能力的，可以采用一些底层协议，比如通过构建一个 http 请求，tcp 层甚至链路层去分析协议，从而构建唯一 hash，有些还可以通过渲染一个图像，记录像素情况，耗用情况以及渲染时间，甚至渲染过程，从而构建唯一 hash，其目的一般是为了标识唯一设备。就比如每个人都有不一样的指纹，重复的概率低之又低，如果有个全人类的指纹库，那么根据指纹就能找到对应的人。

设备指纹的目的，一方面是嵌入 sdk，获取众多设备甚至手机 app 使用情况等信息，一方面就是标识这个设备。这样，同一个设备在不同平台，甚至不同人基于同一个手机去贷款，就很方便标识出来了。具体使用上，不同公司是不一样的，有的关注 GPS，有的关注 ip，有的关注硬盘信息甚至 wifi 列表，这个就看如何应用。

三、设备指纹历史应用场景

早期，在一些对安全要求非常高的线上场景中，例如网上银行在线交，常常使用纯 U 盾这样的纯硬件技术去追踪业务主体。虽然这很安全，但是随着互联网的发展，这种“控件”+“U 盾”的结合方式已经越来越落伍。

1、用户体验非常差：需要冗长安装、更新流程，普通用户难以操作，使用不够友好。

2、移动互联网的发展：而 iOS，Android 等移动互联网入口都不支持控件。

3、使用范围的狭隘：不仅仅在移动端，某些控件在 pc 端适用范围都很小，很多只支持 PC 上的 IE 内核浏览器。同时 Chrome 和 Firefox 等份额较大的桌面浏览器也在逐步淘汰控件的使用。

4、漏洞风险加大：基于控件的本地溢出漏洞层出不穷，用户很容易中木马或者被钓鱼，反而给系统的安全造成严重危害。

由于业务场景实际需要，设备指纹产品应运而生。设备指纹技术可以为每一个操作设备生成一个全球唯一的设备 ID，用于唯一表示出该设备特征。

四、设备指纹目前应用场景

防垃圾注册、防撞库、防薅羊毛、反刷单、精准营销、支付反欺诈、授信反欺诈、用户画像分析、复杂关系网络等，涉及领域电商、支付、信贷等。仅依赖 IMEI 和 IDFA 这种易篡改很那满足业务快速发展的防控需要。

互联网金融业务流程中常见的业务流程

1、授信审批

1）注册：可疑设备感知，恶意注册防范

2）申请：手机信用卡、网络发卡识别信用卡欺诈申请（高风险申请）

2、交易监控

1）登录、密码找回：可以设备感知

2）支付：支付交易密码

3）欺诈交易：支付是否常用设备等

4）团伙欺诈：刷信用、刷流水、薅羊毛、刷单、洗钱

5）敏感交易前的可疑设备感知

五、好的设备指纹产品特性

从用户体验角度上，用户无感知，具有免安装、动态更新、跨平台兼容、防篡改等。

1、 准确性

准确率高，不同设备生成的设备指纹保证不会重复，确保设备指纹生成的唯一性。

个人的常用设备总是有限的，一段时间内一般不会超过 5 个以上。

1）主动采集要素、精准识别设备

2）多维度要素综合决策

2、稳定性

设备系统升级或少量参数变更，设备指纹码不会发生变更。

1）结合被动采集要素。多维度决策增强稳定性

2）适配时间、空间、操作变化

3、安全性

不会再网络传输中杯篡改、注入导致生成设备伪码。

1）识别终端环境风险

2）防篡改、防盗用、接口反作弊

4、易用性

1）支持本地话部署或者云模式

2）业务系统埋点成本低

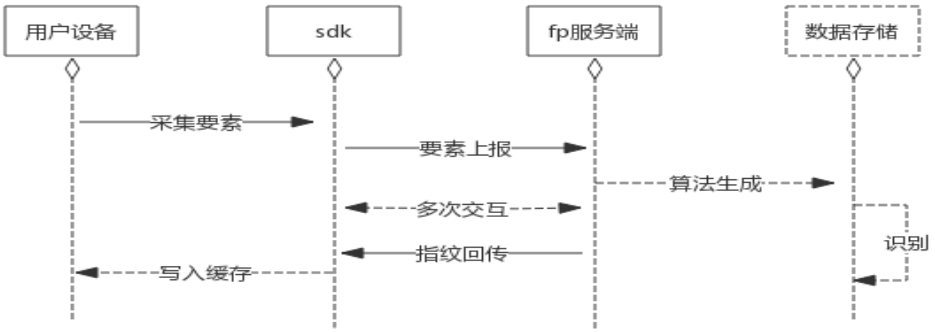
5、适用性

1）服务消耗资源少

2）本地化部署延迟 100ms 之内

六、设备信息集成方式

集成方式：浏览器（即 web/wap）植入 JS 集成，APP 通过 SDK 集成实现。如上图，客户端集成非常简单，只需要几行代码，核心在于采集要素传输加密和服务端算法加工。



备注：图片来源于网络，侵删

采集要素即设备中的硬件本身信息以及软件设置信息。

采集要素示例（部分）：CPU 指令集、蓝牙 MAC 地址、硬件信息、制造商、设备显示的版本包、厂商信息、屏幕分辨率信息、系统版本、系统总内存、系统总容量、SD 卡总容量、系统可用内存、系统可用容量、SD 卡可用容量等。

常见的要素示例如下：

IMEI：International Mobile Equipment Identity，存储与手机里的国际移动设备标识串号。

IDFA：Identifier For Advertising，iOS 独有的广告标识符。单要素应用场景有：比如你在淘宝里搜索了某个商品之后，你在用浏览器去浏览网页的时候，那个网页的广告就会给你展示相应的那个商品的广告。

UDID：Unique Device Identifier，唯一设备标识码。

MEID 号， 移动设备识别码(Mobile Equipment Identifier)是 CDMA 手机的身份识别码，也是每台 CDMA 手机或通讯平板唯一的识别码。通过这个识别码，网络端可以对该手机进行跟踪和监管。但只适用于 CDMA 制式的手机。

七、设备指纹生成方式（技术实现方式）

1、 主动式

主动采集设备 N 多信息，比如 UA、MAC 地址、设备 IMEI 号、广告追踪 ID 等与客户端上生成唯一的 device_id。局限性有：不同生态的平台对用户隐私数据开放权限不同，很难统一生成唯一识别码，且无法实现 Web 和 App 跨域统一。主动式设备指纹另一个局限性，由于强依赖客户端代码，这种方式生成的指纹在反欺诈的场景中对抗性较弱。

2、 被动式

被动式设备指纹技术在终端设备与服务器通信的过程中，从数据报文的 OSI 七层协议中，提取出该终端设备的 OS、协议栈和网络状态相关的特征集，并结合机器学习算法以标识和跟踪具体的终端设备。

与主动式设备指纹技术相比，被动式设备指纹并不必须在设备终端上嵌入用于收集设备特征信息的 JS 代码或 SDK，其所需要的设备特征都是从终端设备发送过来的数据报文中提取，这也是其所谓“被动式”的原因。好适用范围更广，一些无法植入 SDK 和 JS 的场景也可以使用。同时跨 Web/App,以及同步浏览器同一兼容性识别，主动式设备指纹技术，因为相对来说更为简单直接，所以业界大部分设备指纹技术厂商提供的都是该类设备指纹服务。

被动式设备指纹技术，由于其需要使用机器学习技术构建设备指纹分类算法模型，具有较高的技术壁垒，因而还处于推广起步阶段。

3、 混合式

即既有主动采集部分，又有服务端算法生成部分。通过植入 SDK 和 JS，埋点在固定的业务场景，被动触发时的主动去采集要素，并与服务端交互，通过算法混淆加密后，在服务端生成唯一的设备指纹识 ID，同时写入唯一 ID 存于 app 应用缓存或浏览器 cookie 中。一定时间内，用户再次使用对应业务埋点页面时，无需大量重新上传采集要素，只需比对要素变化比例，通过加权比对，计算得出置信度数值，并通过阈值判断是否重新生成设备指纹码。正常用户在使用时理论上是无感知且很少会主动篡改设备指纹唯一 ID。

混合式设备指纹技术克服了主动式设备指纹和被动式设备指纹技术各自的固有的缺点，在准确识别设备的同时扩大了设备指纹技术的适用范围。对于 Web 页面或 App 内部的应用场景，可以通过主动式设备指纹技术进行快速的设备识别；而对于不同的浏览器之间、Web 页面与 App 之间的设备识别与比对关联，则可以利用被动式设备指纹的技术优势来实现。

八、分享举例

一般来说黑产通过群控手机撸羊毛。单一通过设备指纹虽然不能完全防住庞大、产业化、专业度高的黑产从业者，但可以极大提高黑产和恶意欺诈、骗贷、中介恶意包装等作案成本。比如黑产为了防止被设备指纹规则拦截，采用养设备的方式，即群控的设备农场。

1、广告营销

广告营销场景常常需要结合不同人群的兴趣爱好推送不同的广告，达到精准投放

的目的。很多时候需要定位到一个用户的设备，然后画一个基于兴趣的设备画像。对于这个场景的设备指纹，其实可以放弃一部分的“唯一性”，去迎合“稳定性”。因为这个时候业务考虑更多的是人群总体覆盖度，而不用纠结在是不是每一个人每一台设备都定位精准了。所以有时候我们会发现在手机的 app 里浏览一个商品，过段时间电脑上就推荐了，这不是什么黑科技，有可能广告厂商用的仅仅是你的外网 ip 当作设备指纹。如果实现精准推送投放的话，比如用户刷抖 y 短视频时，抖 y 的 DSB 会根据你的设备码生成用户标签画像，同时将你的信息实时推给各电商平台，电商平台根据用户在平台搜索过的意向关键词，在导流平台 Push 商品广告，从而实现实时精准营销，提高下单转化率。

2、设备异常环境识别

很多人误解，设备指纹只能做设备的唯一标识，也就是“设备 ID”的追踪。但其实设备指纹能做的远不止这些，甚至可以说设备 ID 的功能只占其全部功能的三成左右。当下国内最典型的是“账户”和”营销”这些场景，也是黑产获利最多的场景。这些场景里，黑产往往可以通过伪造新设备或者伪造某些系统底层参数(比如地理位置，imei 号等等)的方式来绕过业务的限制。上层设备指纹获取的所有参数都是伪造的，基于这些伪造的数据计算得到的设备 ID 就毫无意义了。就像一个美丽的空中楼阁，没有了深入地下的坚实基础。而夯实基础关键在于”系统环境异常的识别”。对于常见的黑产改机框架、改机软件、伪装软件等，设备指纹都一定要做到针对性的识别。只有确定当前的系统环境没有异常，设备 ID 才是可信、可用的。成熟的设备指纹产品，可以识别虚拟机、模拟器、以及代理侦测。