读书笔记

本文描述了一个高度精确的分类方法来检测安卓恶意软件，这个方法静态地提取了一个数据流特征，这个特征是关于用户怎么输入会触发敏感的API调用，称为user-trigger dependence，分类方法利用了用户输入行为和敏感的API调用的关系。触发器是指用户的输入或操作行为，是在程序中定义的变量。本文的分类方法识别程序中合法的行为模式，而不是恶意的模式，分类是基于程序中是否有这些合法的属性。