读书笔记

现有的杀毒软件大多依靠已知的恶意软件的特征提取，本文提出一种不依赖于已知样本的特征和签名的检测zero-day Android malware的方法，开发了一个名为RiskRanker的自动化系统，能够分析应用程序是否具有恶意的行为。RiskRanker可以从安卓应用市场的大量应用程序中准确地筛选出zero-day Android malware，该系统共采用二阶分析，一阶分析模块通过评估风险简单地处理未经混淆操作的应用程序，二阶分析模块捕获某些特定的行为，如加密和动态代码加载。