基于Dalvik指令流的Android安全分析系统

上海交通大学 密码与计算机安全实验室
Lab of Cryptology and Computer Security
http://loccs.sjtu.edu.cn

联系人：谷大武 教授 Email：dwgu@sjtu.edu.cn

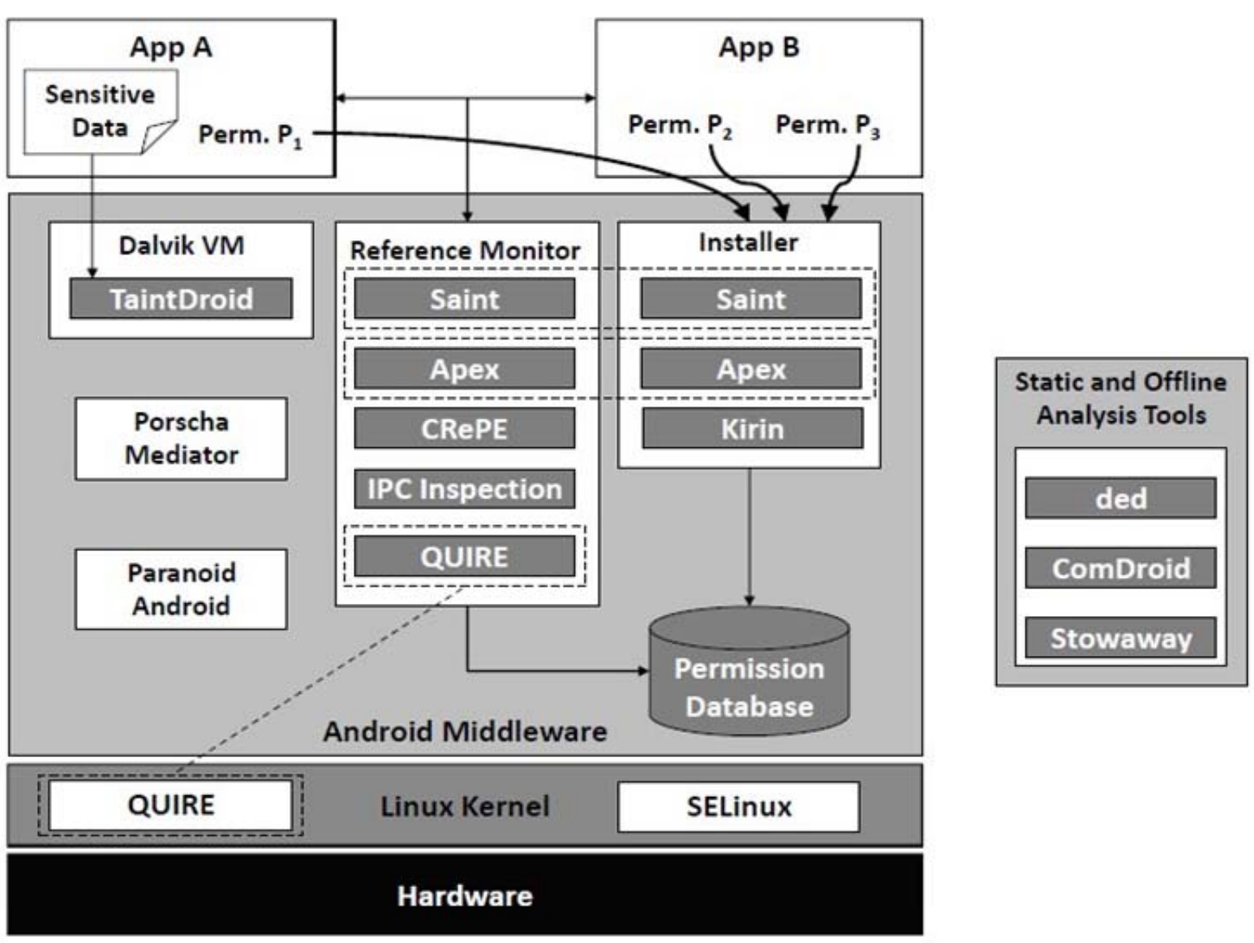
摘要

Android是以Linux为基础的半开源操作系统，主要用于移动设备，由Google成立的Open Handset Alliance（OHA，开放手持设备联盟）持续领导与开发中，其自诞生以来就受到各界的广泛重视。随着Android市场占有率不断提升，Android平台下的安全问题也日益凸显。我们提出基于Dalvik 虚拟机指令流的Android平台安全分析系统，系统通过监视Android底层Dalvik虚拟机的指令流来达到监控整个系统运行的目的，配合可供用户自行配置的安全策略，可以防范Android平台下绝大部分的安全问题与漏洞。我们在Android底层的Dalvik虚拟机中进行深度插装，为上层提供数个可组合的基础分析接口，这些接口可以在上层由用户自行配置，用户根据自己的实际需要来决定监控内容、监控方式、反馈方式等，以达到所需要的安全性。

研究现状

Android平台下常见的安全增强研究主要集中于静态分析、改进Reference Monitor、Installer这三个方面。极少数的研究会对底层的虚拟机进行改动。下图展示了目前学术界的一些关于增强Android安全机制的研究。

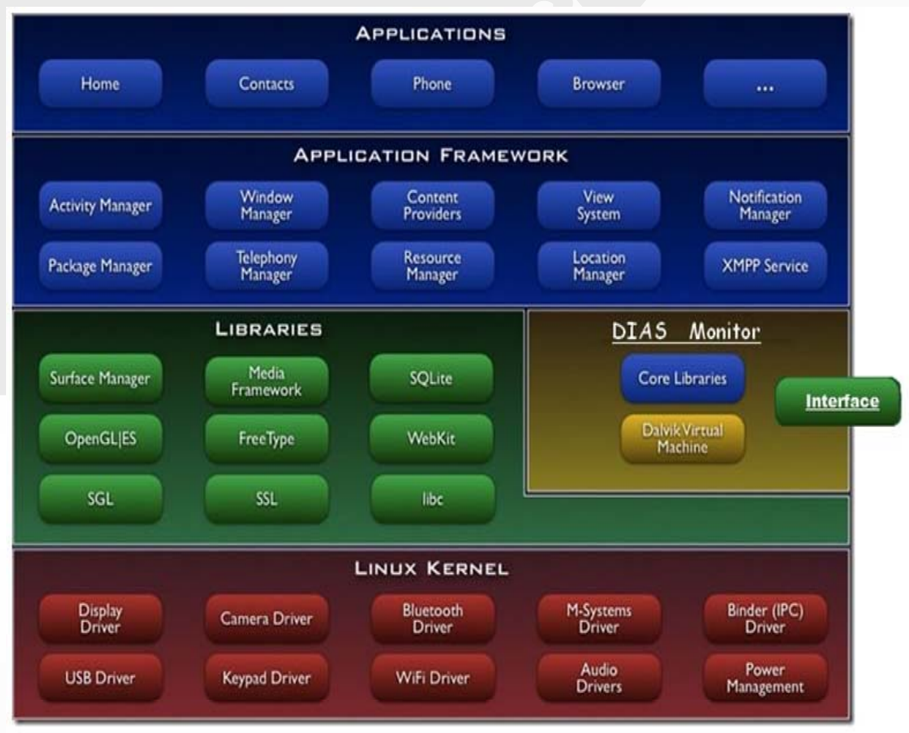
待解决问题
- 缺乏对底层数据操作的监视
- 方案可扩展性不高
- 插装过度影响系统运行效率



相关成果
- Android Malware Forensics: Reconstruction of Malicious Events—Juanru Li, Dawu Gu, Yuhao Luo(2012)

Dalvik指令流分析系统(DIAS)

技术优势
- 轻量级
- 提供接口供用户自行配置安全策略
- 基于Dalvik虚拟机，动态监控底层数据，获取数据全面
- 基于底层架构，不宜被恶意程序检测到
- 移植性强



DIAS Monitor

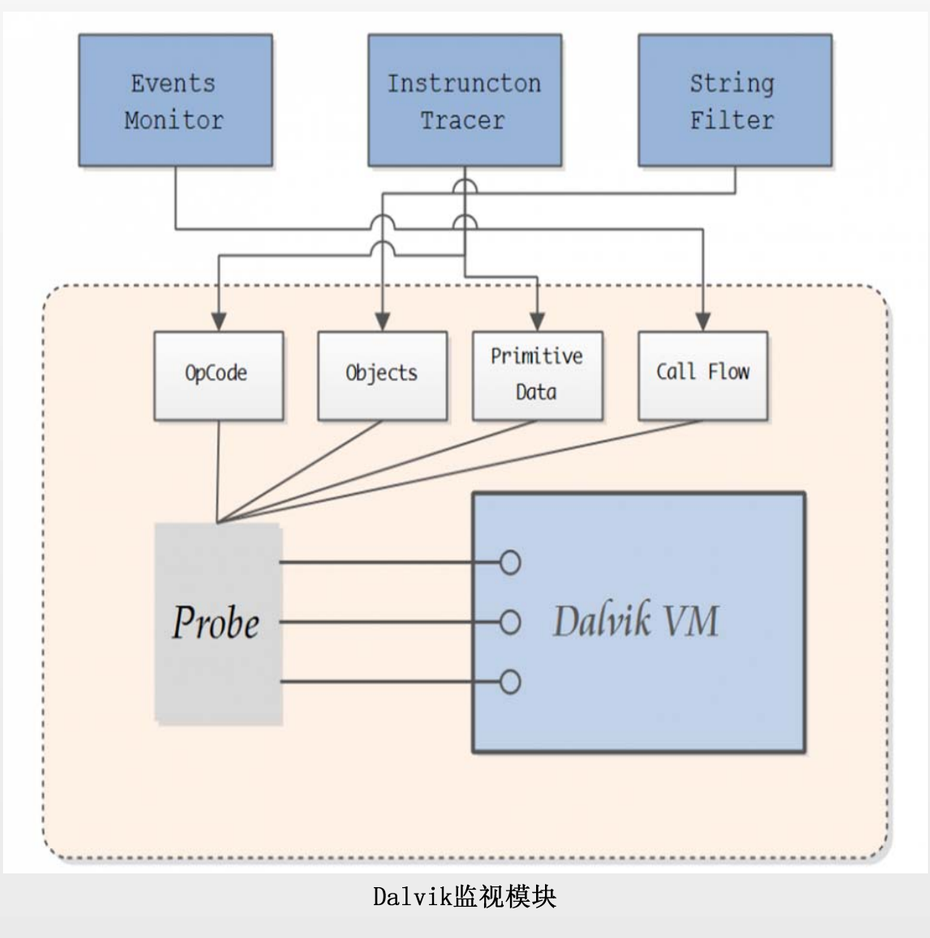
典型应用
- 防范提权攻击
- 防止权限泄漏
- 保护敏感数据
- 保护手机关键资源
- 配置多样化的安全策略

DIAS底层实现

首先在底层的Dalvik虚拟机中，我们会插装一个监控模块，根据用户的不同配置，监控模块可以向上层提供多种不同的监控接口：
- Opcode
- Object
- Data
- Call Flow
- …

这些监控接口互相组合就能还原出一系列Android平台下的事件(event)供上层分析使用。例如Event Mointor会使用到Call Flow接口提供的Api监控数据；Instruction Trace会使用到Opcode和Primitive Data。这些事件之间也可以相互的组合，以形成更高级的事件。

而具体监视哪些事件则由最上层的配置文件所决定，配置文件可以供用户根据不同的安全需要自行修改。通过配置文件，用户还可以选择不同事件的处理方式。



Dalvik监视模块