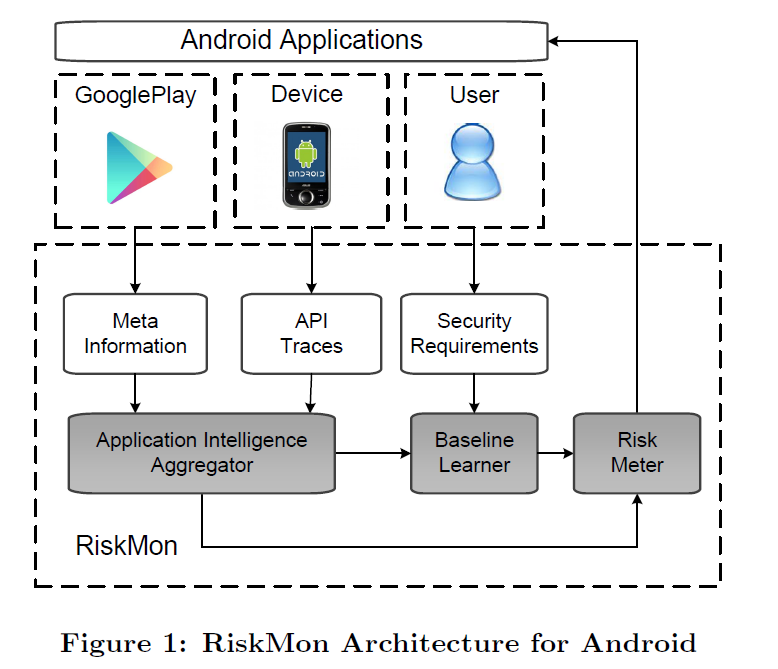
# 简介

1. 这不是一个已开发出的工具，而是提出的一种框架或者说是一种方法。
2. 论文中提到他们的小实现并给出了他们所实现的结果，但没有公开给出工具。
3. 该方法结合用户的简略期望和应用程序运行时的行为，使用机器学习（SVM）训练出一个准线，再对其他应用程序进行风险评估。
4. 该论文发表于2014年，文中数据多来自2013年。

# 来源

Y. Jing, G.-J. Ahn, Z. Zhao, and H. Hu, “RiskMon: Continuous and automated risk assessment of mobile applications,” in Proc. 4th ACM Conf. Data Appl. Secur. Privacy, 2014, pp. 99–110

# 方法流程



应用程序信息聚合（Application Intelligence Aggregator）

这部分主要是抽取应用程序的特征。

1. 运行时的特征主要是API调用（API Traces）的特征，因为应用程序与系统服务之间的交互是通过API的调用实现的。所以该方法提取了1003个受权限保护的API，而每个API都会有一个与之对应的Binder（安卓进程间通信的一种技术）事务，对于Binder事务的属性方面的特征为以下两个：

* Binder事务类型：长度为1003的布尔数组，为1表示相关的事务类型，其他为0
* 控制流方向：布尔型，0表示由应用程序创建（API调用），1表示由系统服务创建（API的回调）

而应用程序与系统服务之间的交互还应该考虑到内容（parcel），由于一些阻碍，这里抽取parcel的长度作为特征：

* 收到的parcel的长度
* 发送的parcel的长度

1. 元信息（Meta Information）也会被抽取出来作为特征，这部分主要来源于大众和开发者。

* 安装量：采用对数值
* 评论量：采用对数值
* 评分：1.0—5.0
* 类型：用一个二元组表示，取值在[-0.5，0.5]

基线学习（Baseline Learner）

这部分需要输入用户的安全需求，即让用户针对某一APP，分别对它所需的所有权限组进行相关性的评估，评估等级分为5个：相关、可能相关、中立、可能不相关、不相关。之后通过他们提出的算法或得训练集，训练集为一个二元组的集合（权限组向量和对应的相关性）。最后通过RSVM（Ranking Support Virtual Machine）学习出一个风险评估基线。

风险评估（Risk Meter）

通过待评应用程序与训练出的基线之间的偏离程度来对待评应用程序进行风险评估。

# 注意事项&问题

1. 没有成型的工具。
2. 感觉这个方法主要是基于用户的直觉和权限的，主观性比较强。
3. 其中有一个特征是应用的种类，而这个种类一般是由开发者说明的，若是恶意开发者，那么这种方法无法准确的评估风险。