# 功能简介

RiskInDroid（**Ri**sk **In**dex for An**droid**）是用Java编写的Android应用定量风险分析的工具（用于检查应用程序的权限）和Python（用于计算基于应用程序的权限一个风险值）。该工具通过scikit-learn（一种Python的机器学习库）使用分类技术，以便为给定的应用程序生成介于0和100之间的数值风险值。特别是在RiskInDroid中使用了scikit-learn的以下分类器（这个列表是在广泛的经验性评估之后选择的）：

支持向量机（SVM）

多项式朴素贝叶斯（MNB）

梯度提升（GB）

Logistic回归（LR）

与其他工具不同的是，RiskInDroid并没有考虑到声明在应用清单中的权限，而是对应用程序进行逆向工程以检索字节码，然后通过静态分析推断哪些权限实际使用哪些权限，这样，每个分析的应用程序的4组权限：

声明的权限 - 从应用程序清单中提取

利用权限 - 在字节码中声明和实际使用

Ghost权限 - 未声明，但在字节码中使用

无用的权限 - 声明，但从未在字节码中使用

从上述权限集合（仅考虑Android权限的正式列表）中，构建特征向量（由0s和1s构成）并赋予分类器，然后计算风险值。RiskInDroid的精度和可靠性已经在由6K个恶意软件样本和112K个应用组成的数据集上进行了实证测试。

# 来源

https://github.com/ClaudiuGeorgiu/RiskInDroid

# 使用步骤

#### 使用Docker

这是使用**RiskInDroid**的建议方式，因为唯一的要求是安装Docker。确保在先前创建的RiskInDroid目录（包含该目录的文件夹Dockerfile）中执行以下命令：

＃这将需要一些时间，因为很多东西都必须下载

$ docker build -t riskindroid。

$ docker run -p 8080：80 riskindroid＃现在在浏览器中打开http：// localhost：8080 /

在线Demo的命令

$ docker run -d --restart = always -p 80:80 -p 443：443 -v “ $ PWD / app / upload ”：/ var / www / app / upload / riskindroid

#### 使用Python

这个方法已经过测试，可以在Ubuntu 16.04上运行。Python 3.5和Java必须安装在您的计算机上，您也可以选择安装p7zip-full，以便自动提取数据库存档，而且这也可以通过使用任何其它兼容工具提取的内容手工完成RiskInDroid/app/database/permission\_db.7z的RiskInDroid/app/database目录。确保在以前创建的RiskInDroid目录中执行以下命令：

＃如果没有使用virtualenv（https://virtualenv.pypa.io/），跳过下面的两行

$ virtualenv -p python3 venv

$ source venv / bin / activate＃安装RiskInDroid需求

$ pip3 install -r requirements.txt＃ Run RiskInDroid

$ python3 app / app.py＃现在在浏览器中打开http：// localhost：5000 /

# 结果

