Free for All! Assessing User Data Exposure to Advertising Libraries on Android

MAR 3RD, 2016

论文下载

Abstract

这篇文章分析了Android平台上广告库可能引起的用户数据泄露问题，并提出了一个分析APP潜在问题的框架。
作者认为，单纯分析现在的广告库是否泄露用户数据并没什么意义，要分析未来的广告库能对用户隐私有多大的威胁，于是假设了一个最恶劣的广告库 广告库泄露用户隐私的四种方式：

- 未保护的API，获取用户的应用列表
- 从宿主APP继承权限，访问敏感数据（账户信息）
- 继承权限，访问私有文件
- 继承权限，监视用户输入

解决的问题,在广告库可以通过以上方式获得相关信息的情况下：

- 分析一个APP是否可能泄露数据

- 证明通过获取应用列表可以用来推测用户信息
- 建立了一个APP引进广告库从而带来风险的评估平台

Threat Model

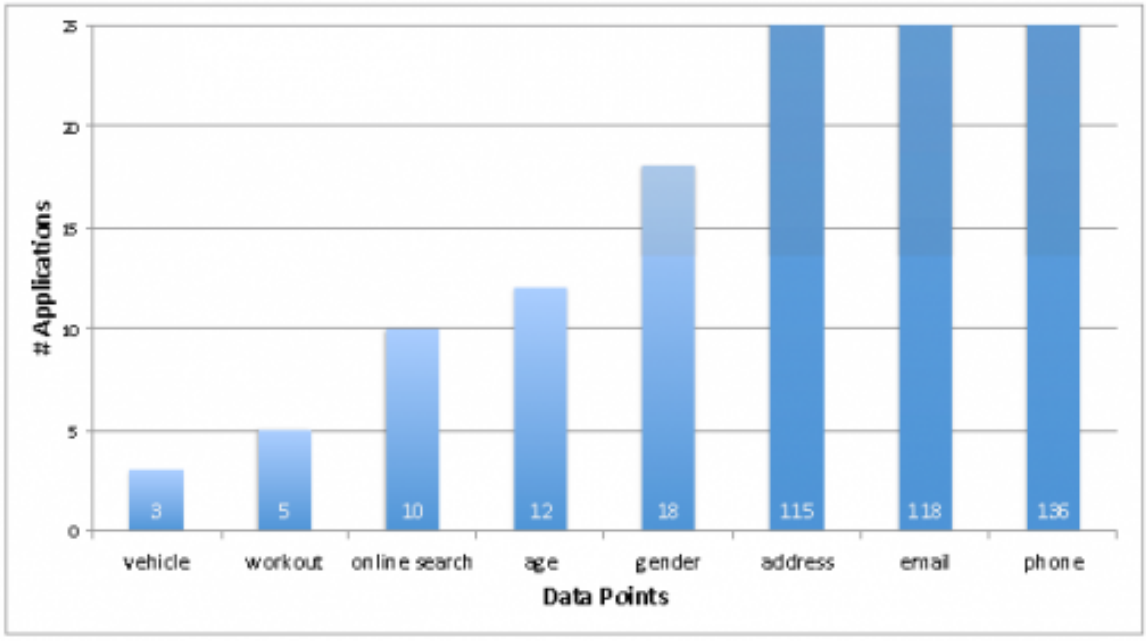
作者将广告库泄露隐私的方式分为两类，**in-app**和**out-app**，前者指的是宿主APP的敏感API，生成的文件以及资源文件中的信息可以被广告库利用，后者指的是与宿主APP无关的信息泄露。

in-app数据集的建立：

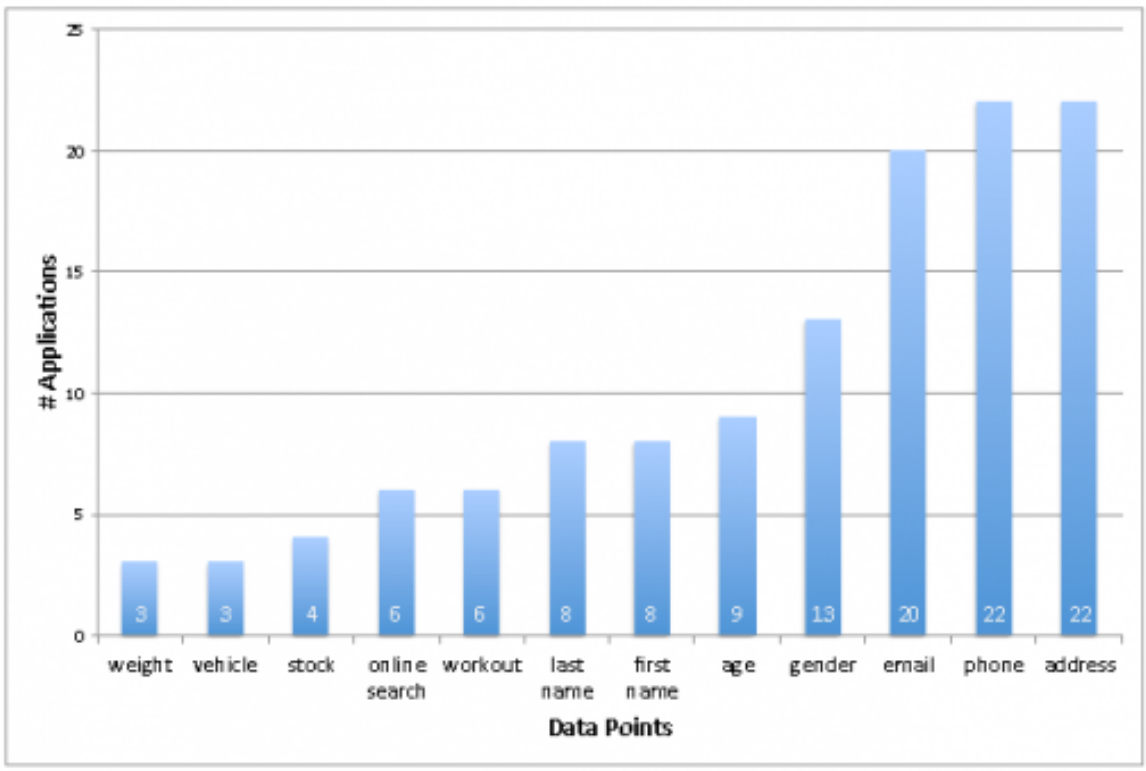
TABLE I: Datasets

Name	Number	Description
Full Dataset (FD)	2535	Unique apps collected from the 27 Google Play categories.
Level One Dataset (L1)	262	Apps randomly selected from FD.
Level Two Dataset (L2)	35	Apps purposively selected from L1.
App Bundle Dataset (ABD)	243	App bundles collected through survey.

L1是只考虑APP通过权限以及本地文件泄露隐私的情况，L2是只考虑窃取用户输入的情况：



(a)



(b)

out-app数据集的建立:

- 志愿者装上作者提供的APP之后，应用列表会被上传，并且志愿者还被要求做一些测试，包括感兴趣的分类等，共收集了243分数据。

Pluto: Framework Design And Implementation

Pluto分为两部分，in-app Pluto主要作用是离线分析APP。

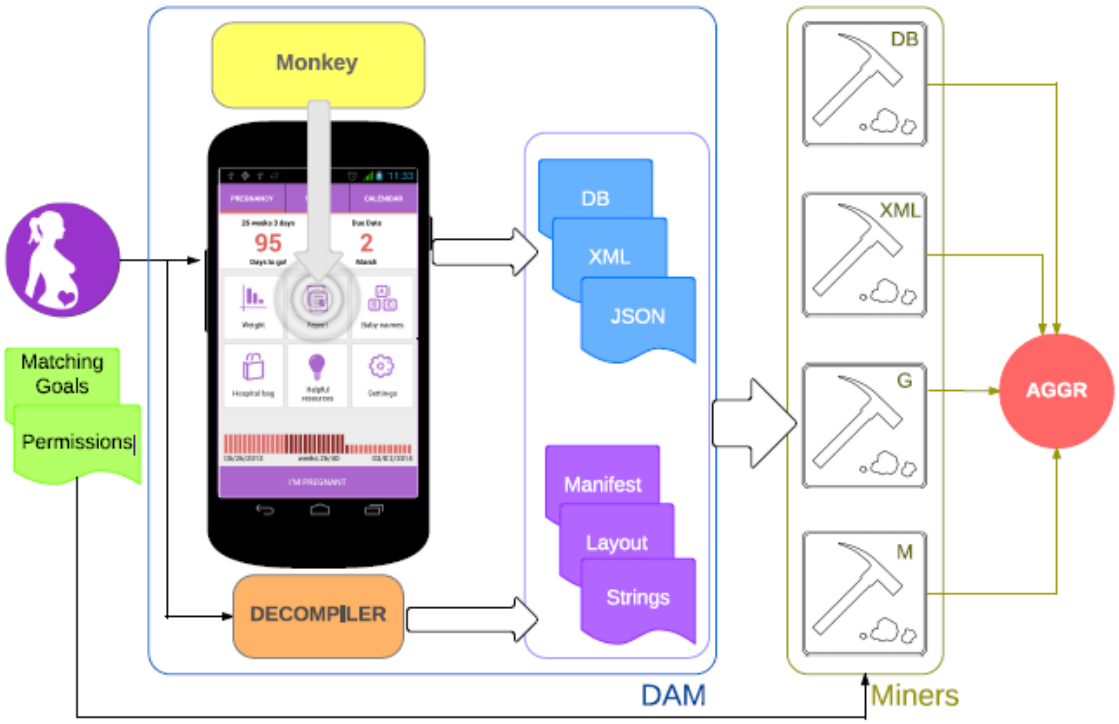


Fig. 2: Design of In-app Pluto

动态分析，静态解包之后得到的一些文件，进行数据挖掘和自然语言处理 out-app pluto 利用机器学习，推测用户信息，推测用户感兴趣的分类。

Evaluation

对in-app部分的测试，用pluto跑了FD,L1和L2。

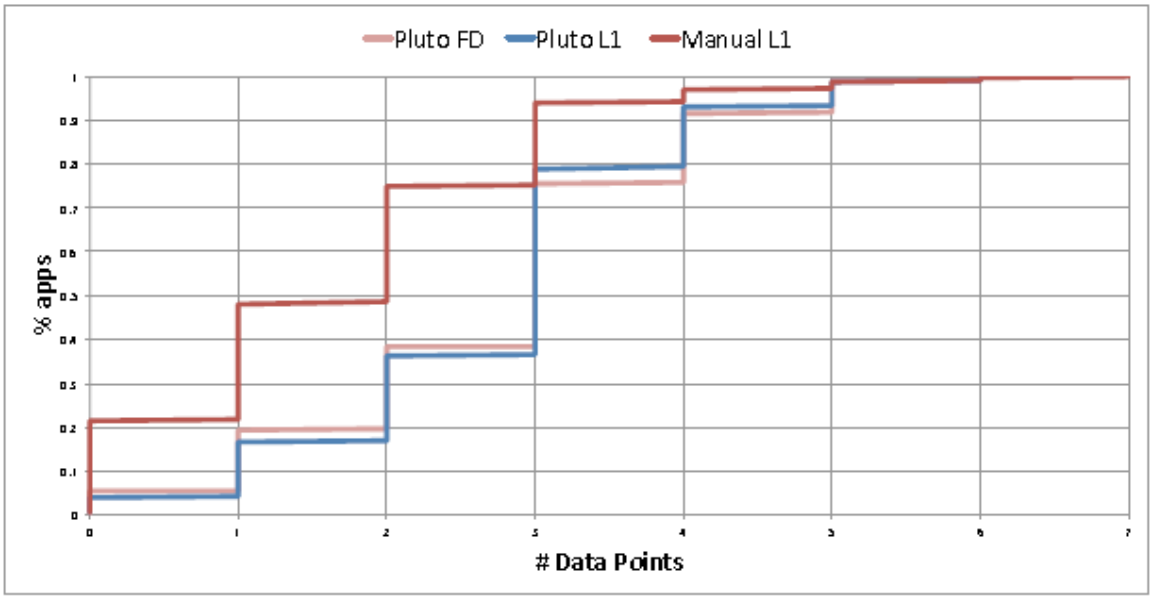


Fig. 3: CDF of apps and number of data points (level-1)

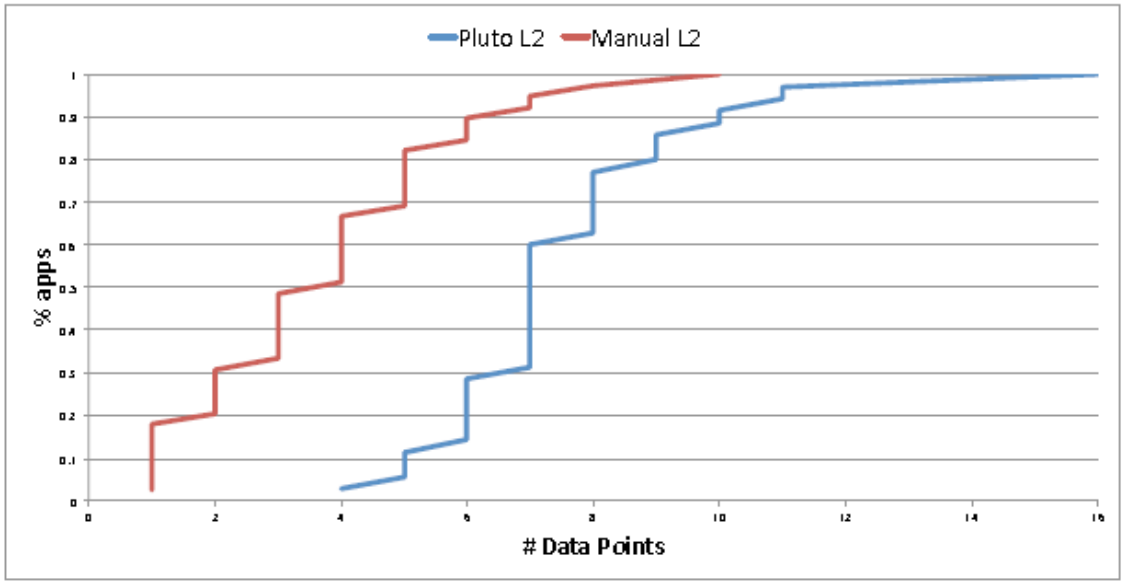


Fig. 4: CDF of apps and number of data points (level-2)

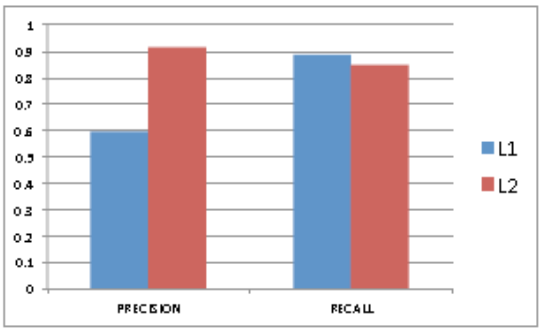


Fig. 5: **gender** prediction performance given the L1 and L2 ground truth.

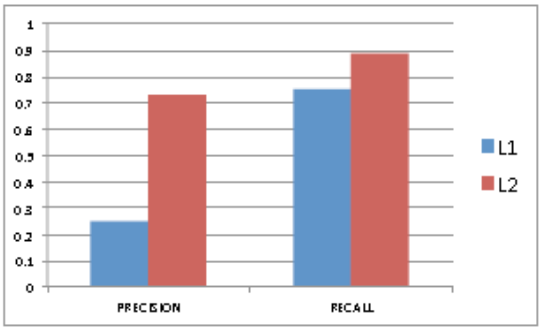


Fig. 6: **age** prediction performance given the L1 and L2 ground truth.

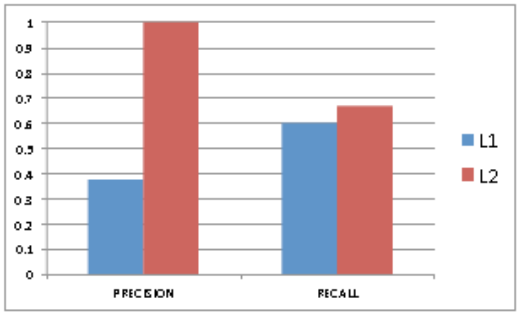


Fig. 7: **workout** prediction performance given the L1 and L2 ground truth.

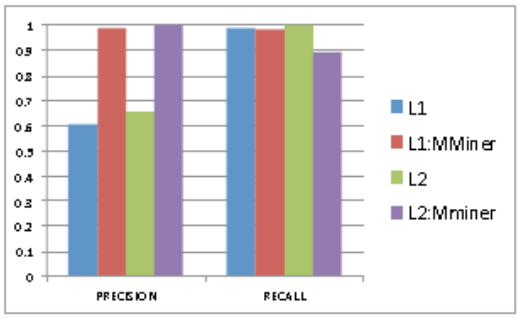


Fig. 8: **address** prediction performance in different configurations, given the L1 and L2 ground truth.

对out-app部分的测试：

TABLE V: The strongest co-installation patterns found by the CIP module when run on the survey app bundles.

Precedent	**Consequence**	**Conf**	**Lift**
com.facebook.katana	com.facebook.orca	0.79	2.10
com.lenovo.anyshare.gps	com.facebook.orca	0.75	2.01
com.viber.voip	com.facebook.orca	0.74	1.98
com.skype.raider	com.facebook.orca	0.71	1.88
com.skype.raider	com.viber.voip	0.70	2.32

TABLE VI: Performance of classifiers before dimension reduction

Classifier	Age		Marital Status		Sex	
	P(%)	**R**(%)	**P**(%)	**R**(%)	**P**(%)	**R**(%)
Random Forest	64.1	66.3	89.8	83.6	91.5	89.6
SVM	65.5	63.6	89.0	82.1	87.4	83.1
KNN	62.7	60.0	86.3	77.7	83.4	74.8

P = Weighted Precision, R = Weighted Recall

TABLE VII: Performance of classifiers after dimension reduction

Classifier	Age		Marital Status		Sex	
	P(%)	**R**(%)	**P**(%)	**R**(%)	**P**(%)	**R**(%)
Random Forest	88.6	88.6	95.0	93.8	93.8	92.9
SVM	44.8	35.4	66.9	50.5	80.9	70.1
KNN	85.7	83.6	92.5	91.2	91.6	89.9

P = Weighted Precision, R = Weighted Recall