Covert Communication in Mobile Applications

DEC 30TH, 2015

论文下载：https://people.csail.mit.edu/mjulia/publications/Covert_Communication_in_Mobile_Applications_2015.pdf

Abstract & Introduction

作者提出的问题：

APP中会出现一些没有价值的通信，这些通信流量被禁用之后不会对用户使用产生任何影响。这些流量可能会泄露用户隐私，占用带宽，费电。

作者的解决方式：

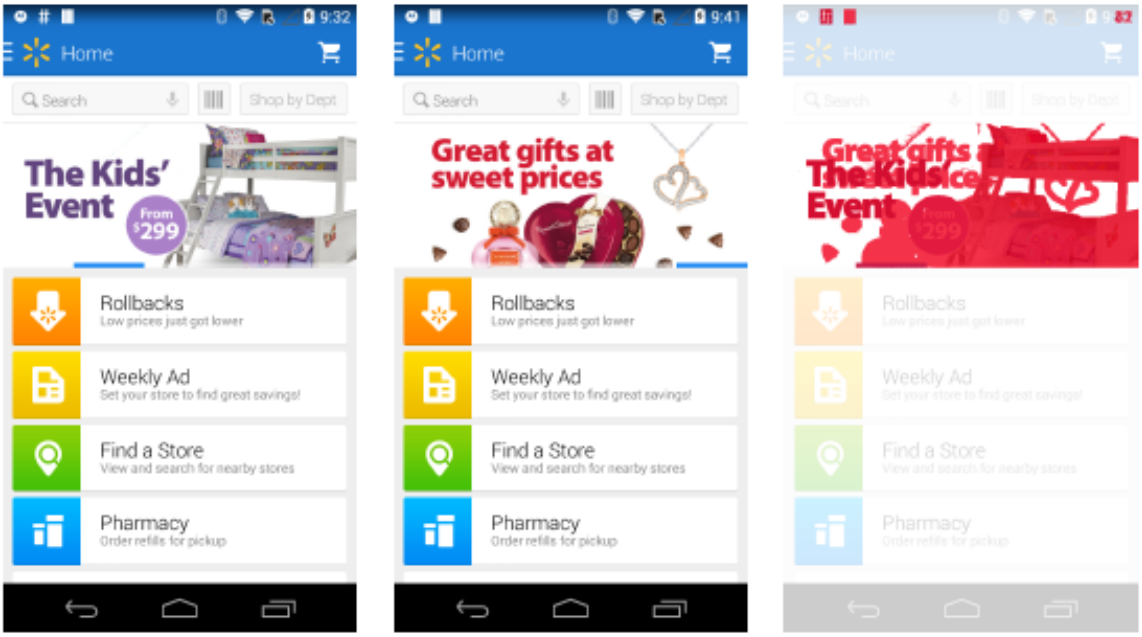
- 明确显示通信和隐式通信的定义
- 半自动动态检测APP中的隐式通信，测试了google play前20名应用，63%的通信是隐式的
- 提出静态批量检测方案，测试了google play前500的应用，46.2%的通信是隐式的

Communication In Android

动态分析APK：

1. 找到连接的声明
2. 对APK插桩，对单个连接直接返回异常，重打包APK
3. 按照所有的连接列表生成多个版本的APK
4. 自动化执行这些APK，比较执行结果

执行方法，人工使用APP，记录操作，覆盖尽可能多的功能。用同样的脚本跑其他的APP版本，在每个用户输入点之后截图，比较截图



(a) Screen 1. (b) Screen 2. (c) Diff. for (a) and (b).

选取了google play前20的应用作为样本，排除聊天应用和不能重打包的应用，留下13个，结果如下

TABLE II. ANALYZED APPLICATIONS.

Applications	jar size (MB)	Total # of connection statements	# of triggered connection statements	# of covert (% of trig.)	# of covert in known A&A (% of total covert)
air.com.sgn.cookiejam.gp	2.7	17	3	2 (66.7%)	1 (50.0%)
com.crimsonpine.stayinline	3.2	15	2	2 (100.0%)	2 (100.0%)
com.devuni.flashlight	1.4	16	3	1 (33.3%)	1 (100.0%)
com.emoji.Smart.Keyboard	0.8	3	3	2 (66.7%)	0 (0.0%)
com.facebook.katana	0.6	3	0	-	-
com.grillgames.guitarrockhero	6.2	51	14	14 (100.0%)	6 (42.8%)
com.jb.emoji.gokeyboard	5.2	42	10	7 (70.0%)	0 (0.0%)
com.king.candycrushsaga	2.6	15	1	0 (0.0%)	-
com.pandora.android	5.7	57	12	9 (75.0%)	3 (33.3%)
com.spotify.music	5.4	20	7	2 (26.6%)	1 (50.0%)
com.twitter.android	5.9	21	10	3 (30.0%)	1 (33.3%)
com.walmart.android	5.8	33	8	5 (62.5%)	3 (60.0%)
net.zedge.android	6.5	37	8	4 (50.0%)	4 (100.0%)
Total		330	81	51 (62.9%)	22 (43.1%)

- 51个中22个是由advertisement and analytics (A&A)包引入的

- 在没有向用户声明的情况下，收集应用的performance，crash，usage data。甚至从手机开启之后一直收集发送信息
- twitter会隐式上传推文中照片以及视频的相关信息，有些包发送加密数据，沃尔玛应用调用第三方库手机扫描过的二维码信息。

Static Analysis For Classifying Connections

静态分析APP：

- 生成函数调用图
- 分析failer handler,根据不同情况判定显式还是隐式。
- 分析成功之后的函数调用，判断是否改变了UI

Experiments

首先测试静态分析方法的准确性，跑前面用动态分析跑过的几个APK。分析准确性和完备性，结果如下。

TABLE IV. COMPARISON WITH THE MANUALLY ESTABLISHED RESULTS.

Applications	Correctly detected covert		Execution time
	Precision	Recall	
air.com.sgn.cookiejam.gp	1/1 (100.0%)	1/2 (50.0%)	2min 11s
com.crimsonpine.stayinline	2/2 (100.0%)	2/2 (100.0%)	2min 24s
com.devuni.flashlight	1/2 (50.0%)	1/1 (100.0%)	1min 44s
com.emoji.Smart.Keyboard	2/2 (100.0%)	2/2 (100.0%)	1min 16s
com.grillgames.guitarrockhero	1/1 (100.0%)	1/14 (7.1%)	6min 14s
com.jb.emoji.gokeyboard	4/4 (100.0%)	4/7 (57.1%)	3min 22s
com.pandora.android	4/4 (100.0%)	4/9 (44.4%)	2min 41s
com.spotify.music	1/1 (100.0%)	1/2 (50.0%)	2min 51s
com.twitter.android	1/1 (100.0%)	1/3 (33.3%)	3min 3s
com.walmart.android	3/3 (100.0%)	3/5 (60.0%)	3min 2s
net.zedge.android	3/4 (75.0%)	3/4 (75.0%)	4min 13s
Average	93.2%	61.5%	2min 48s

检测可用性：

- 取前100的应用，排除之后剩下47个，重打包禁用所有检测出来的隐式通信，让测试人员正常使用，对比正常应用：30个是正常的，9个丢失广告，3个是小功能缺失，5个重要功能缺失
- 取前500的应用，攻找到46.2（8539/18480）的隐式通信。

TABLE V. TOP 10 COVERT COMMUNICATION CALLERS.

	Package	Description	Used in # (%) of Apps	Covert Calls (% of total calls)
1.	com.google.android	Google services	382 (76.4%)	1913 (49.9%)
2.	com.gameloft	Mobile games	17 (3.4%)	784 (87.4%)
3.	com.inmobi	A&A services	61 (12.2%)	615 (67.6%)
4.	com.millennialmedia.android	A&A services	78 (15.6%)	447 (58.8%)
5.	com.mopub.mobileads	A&A services	72 (14.4%)	320 (56.9%)
6.	com.tapjoy	A&A services	49 (9.8%)	277 (43.8%)
7.	com.facebook	Facebook services	112 (22.4%)	222 (24.3%)
8.	com.unity3d	Gaming services	77 (15.4%)	203 (41.8%)
9.	(default)	Default package of an application	23 (4.6%)	178 (48%)
10.	com.flurry	A&A services	95 (19%)	175 (35.3%)

特别指出gameloft的情况17个应用共有787个隐式连接。

Limitations

- 动态执行的代码覆盖率问题，不能检测跨应用之间通信。

- 静态分析时RPC不能分析，间接方式影响UI的没有考虑。