Hi Steve,

Wish you are having a nice day.

My name is Yingying Wang, a student from University of British Columbia. I and another student Lina Qiu, are currently working with a UBC professor, Julia Rubin, on a project comparing several static analysis tools of Android applications, namely, FlowDroid, IccTA, AmanDroid and DroidSafe. Hopefully, we would like to publish our comparison results and will send you the draft once we have it.

1. More Contexts:
We used the four tools to run analysis on DroidBench, IccBench, and several F-Droid applications with our customized source and sink list. When analyzing the results of FDroid applications by FlowDroid, we met some confusions that we cannot explain and would like to ask if you have any insights about it. Thanks in advance!

2. FlowDroid config we used:
We used the 1.5 release version and the config we used is:

java -Xmx64g -cp soot-trunk.jar:soot-infoflow.jar:soot-infoflow-android.jar:slf4j-api-1.7.5.jar:slf4j-simple-1.7.5.jar:axml-2.0.jar soot.jimple.infoflow.android.TestApps.Test $APK $SDK_25/android.jar --logsourcesandsinks --pathalgo contextsensitive --layoutmode none

3. Our question:

For this FDroid application, Adlock Plus (source code and .apk here), we manually identified 2 flows in the activity CrashReportDialog(see the code snippet below):

More Details about are:

- **Defined Sources:**
  - <org.apache.http.HttpResponse: org.apache.http.HttpEntity getEntity()> -> _SOURCE_
  - <org.apache.http.util.EntityUtils: java.lang.String toString(org.apache.http.HttpEntity)> -> _SOURCE_
- **Defined Sinks:**
  - <android.util.Log: int e(java.lang.String,java.lang.String)> -> _SINK_
- **Expected Flows:**
  - Flow1:
    - Source: Line 145: httpresponse.getEntity()
    - Sink: Line 145: Log.e(TAG, EntityUtils.toString(httpresponse,getEntity())) ;
  - Flow2:
    - Source: Line 145: EntityUtils.toString()
    - Sink: Line 145: Log.e(TAG, EntityUtils.toString(httpresponse.getEntity())) ;

- **Results reported by FlowDroid**
  - FlowDroid **successfully reported Flow2 but missed Flow1**; Reported path: (full result reported by FlowDroid in attachment)

> Found a flow to sink staticinvoke <**android.util.Log: int e(java.lang.String,java.lang.String)**>("CrashReportDialog", $r7), from the following sources:
> - $r7 = staticinvoke <**org.apache.http.util.EntityUtils: java.lang.String toString(org.apache.http.HttpEntity)**>($r21) (in <org.adblockplus.android.CrashReportDialog: void onOk(android.view.View)>)
> on Path [$r7 = staticinvoke <org.apache.http.util.EntityUtils: java.lang.String toString(org.apache.http.HttpEntity)>($r21), staticinvoke <android.util.Log: int e(java.lang.String,java.lang.String)>("CrashReportDialog", $r7)]

Our question is why FlowDroid missed the Flow1 in this case? It would be really helpful if you could provide any suggestions or insights on this. Thanks in advance!

4. Materials attached

For a whole picture of the story, we attached the following materials:

- Our customized source and sink list: ***SourcesAndSinks.txt.***
- Source code and apk of the FDroid application, Adlock Plug, that we analyzed: (.apk Blocked by email thus we uploaded it here: SourceCodeAndAPK)
- Analysis results of the app with FlowDroid: ***Internet.org.adblockplus.android_270.64G.txt***

Thanks for taking time to read such a long email! We look forward to hear your reply.

Wish you have a nice day,
Yingying & Lina