CS-898AE Paper Critique – 5

Aishwarya Ajay Venkatesha
E425P738

1. What are the major challenges in static analysis of Android app

- In static analysis, the main challenge is to manage the rate of false alarms without neglecting the other functions of the applications.
- Android, an event-based system has a chance of generating method calls due to the control flow which is worked by the events, to detect all the flow paths and not create false paths in the process is a tough challenge.
- Android has a huge sets of library code in its runtime which is really important for the app and as is an event-based system it uses libraries a lot which further makes it expensive.
- It also uses different paths for various purposes and managing all these paths is tough.

2. Please explain the major steps of Amandroid.

The following are the major steps in Amandroid:

- In accord with static analysis, it converts the dalvik byte code to an intermediate representation.
- This further gives rise to an environment model which imitates the Interactivity off an android system with the application.
- The analysis here is done based on components. A data flow graph (DFG) is created for every component and also a DDG is created which has clear information.
- Now this data is used on different levels of security analysis as we use DDG for an information leak.

3. Please find the major differences between Flowdroid and Amandroid from the paper.

Soln: The following are the differences between flowdroid and amandroid:

Flowdroid	Amandroid
This framework cannot support multiple security analysis.	This framework supports my multiple security analysis.

It cannot calculate or point to information for all objects.	It can calculate all objects point to point information.
It cannot handle ICC and security issues where intercommunication is involved.	It handles both ICC and Inter component communication.
It creates a call graph based on soot.	It creates a call graph with the dataflow analysis.