CS-898AE

Surya Devathi
n659a624

PaperCritique-4

1.

Privacy leak, is an event where the sensitive data from a device is depicted by an iOS application and this information is sent to 3rd party device without the user's knowledge.

2.

Checking an iOS application for privacy leaks includes 3 major steps, which are:

a. Reconstructing of control flow graph of the application:
   The code parts from sensitive sources to sinks are interpreted but using this control flow graph.
b. Reachability analysis:
   This is used for analyzing the presence of paths which connect the nodes that are giving out sensitive information to the nodes that are interacting with the network.
c. Dataflow analysis:
   This analysis is used to check whether the sensitive information is actually flowing from source to sink.

3.

Extracting control flow graph from objective C binaries includes the following steps:

a. building a class hierarchy:
   This is done in Mach-O file which stores the basic info above the structure.
b. Resolving method calls:
   'objc_msgSend', dispatch function which is used in object if C to perform method calls to get back the data and to show which direction the object is pointing towards.
c. Backward slicing:
   To define the values in the target registers or to record all the instructions that matter.
d. Generating the CFG:
   The values that are generated in the above step that is backward slicing are verified if they are reasonable.

4.

Finding potential privacy leaks includes the following steps:

a. Checking graph for the presence of paths which connect the nodes that are giving out sensitive information to the nodes that are interacting with the network.
b. Spotting the sources where the leakage of sensitive data is happening.
c. Dataflow analysis on the paths, to enhance the precision of PiOS.
d. Recognizing the message dispatch function methods.