Lab 2: Static Analysis of API Usages in Java Classes

Lab Overview

The goal of this lab is to understand how to perform custom static analysis on Java programs. Particularly, you need to implement a static analysis tool to study the API usages of Java class files, compiled with Android libraries. Java/Android APIs can access critical system resources including GPS location, SMS service, etc., and misusing these sensitive functionalities may lead to severe security problems such as capability leakage and data exfiltration. In this lab, you need to figure out which APIs are being used in a compiled Java class through automated static analysis. To this end, you need to extend Soot, a Java analysis framework, and develop a custom analyzer.

Requirement

You are required to submit your source code and a written lab report. In this brief report, you need to use screenshots to explain your implementation and present your analysis result.

Lab Environment

This lab needs to be conducted using Java SDK, Soot library and Android library. You can download the Soot and Android library files (**soot-2.5.0.jar, sootclasses_j9-trunk-jar-with-dependencies.jar and android-17.jar**) from `lab2.zip` at
https://drive.google.com/open?id=1bZyBFt_R51OKqQveI0_wa7P62TddPNuv
The `lab2.zip` file also contains the template of analysis code and the target Java class file to be analyzed. To run Soot, it requires to install Java SDK (later than Java 5, preferably Java 7 or Java 8). If you install Java 9, you should use **sootclasses_j9-trunk-jar-with-dependencies.jar** to compile your analysis code and run Soot. If you install a version older than Java 9, you should use **soot-2.5.0.jar** instead.

Task: Record API Usages in Java Classes

Decompress the `lab2.zip` file and `cd` to the `lab2/` directory. In this directory, you can find the source code of analyzer template under the `analyzer/` directory and the target Java class to be analyzed (`Unknown.class`) under the `unknown/test/` directory. Your task is to complete the `SimpleAPILookupTransformer.java` file in `analyzer/` to implement the analysis.

To compile the analyzer, you can run the following commands in the `lab2/` directory:

```
javac -cp one_version_of_sootclass.jar:. analyzer/SimpleAPILookupTransformer.java
javac -cp one_version_of_sootclass.jar:. analyzer/AnalysisMain.java
```

To run the analyzer, you can run the following command in the `lab2/` directory:

```
java -cp one_version_of_sootclass.jar:android-17.jar:. analyzer.AnalysisMain ./unknown
```

Hint: To implement the code, you need to understand Soot APIs, which can be found at:
https://www.sable.mcgill.ca/soot/doc/index.html
https://soot-build.cs.uni-paderborn.de/public/origin/develop/soot/soot-develop/jdoc/