Smali Lab

Assigned: 2018/12/06

Due: 2018/12/20

Hao Xia(haoxia17@fudan.edu.cn) is the lead person for this assignment.

1 Introduction

The purpose of this lab is to learn smali. Smali is an assembler for the dex format used by dalvik, Android's Java VM implementation. If you want to reverse an Android application, you need to know smali. In this lab, we will use Apktool to help us reverse an Android application. This tool can decode resources to nearly original form.

2 Mission

Reverse an Android application

1. The apk file of the Android application is given under this directory. This file can be installed on Android Phone. If you do not have any Android Phones, you can install an Android simulator on your computer. Please read the install_emulator.pdf under this directory.
2. This application has some string calculation logic. You can enter a string and click the button “check”, and this application will give a calculation result. The mission is to reverse this application and find out the calculation code.

3 Tools

Apktool - A tool for reverse engineering Android apk files

Install Instructions

Quick Check

1. Is at least Java 1.8 installed?

2. Does executing java -version on command line / command prompt return 1.8 or greater?

3. If not, please install Java 8+ and make it the default. (Java 7 will also work at this time)

Installation for Apktool

Windows:

1. Move both files (apktool.jar & apktool.bat) to your Windows directory (Usually C://Windows)

2. If you do not have access to C://Windows, you may place the two files anywhere then add that directory to your Environment Variables System PATH variable.

3. Try running apktool via command prompt

Linux:

1. Rename apktool_linux to apktool

2. Move both files (apktool.jar & apktool) to /usr/local/bin (root needed)

3. Make sure both files are executable (chmod +x)

4. Try running apktool via cli

Mac OS X:

1. Rename apktool_mac to apktool
2. Move both files (apktool.jar & apktool) to /usr/local/bin (root needed)
3. Make sure both files are executable (chmod +x)
4. Try running apktool via cli

4 Reversing

Run the command "apktool d ics_lab_smali.apk" to reverse the application. You will find the main file in

./ics_lab_smali/smali/fudan/edu/cn/ics_lab_smali/MainActivity.smali

There are three question for you:

1. Through artificial reversal, use the java language to express the check function. The local variables are as consistent as possible with the name in smali. **(40 points)**

2. Find one input to get the result "err" **(30 points)**

3. Find one input to get the result "IXWJM" **(30 points)**