COMP 4632
Practicing Cybersecurity: Attacks and Counter-measures

Week 9 Lab Exercise – Lab Sheet B

Topic: *Hacking Mobile Application*

Lab Objective

In this lab, you will try to perform some hacking on android application. This will include tasks to modify the application and aim at achieving the following objectives:

- De-compile mobile application
- Modifying application package and content
- Rebuild the application for mobile devices

Task B1 – String Modification and Logic Tweaking for Android Application Package

In this task, we will walk through the steps to de-compile the mobile application, modify strings in the application code and logic, then rebuild the application package.

Task B1.1 Preparation task

- Open up a terminal in the Kali Linux VM
- Install necessary libraries and download APK signing tools

```
sudo apt-get install lib32stdc++6 lib32z1 lib32z1-dev
cd ~/
wget
'http://connortumbleson.com/apktool/googlecode/apktool1.4.7.tar.bz2'
tar -jxvf apktool1.4.7.tar.bz2
wget 'http://files.cnblogs.com/shenhaocn/autosign.zip'
unzip autosign.zip
```

Task B1.2 De-compiling the mobile application

- Extract and de-compile the APK file

```
java -jar ~/apktool1.4.7/apktool.jar d ./WorldCup.apk ./apk-output
```

- Modify the date string so that spinners will still be enabled for selection after World Cup started.

```
vi ./apk-output/smali/com/hkbc/worldcup/GoalActivity.smali
```

- Try to search for “const-string” to look for string similar to date format (e.g. const-string v0, "20151030") and change it to a future one (e.g. const-string v0, "20151231").

Task B1.3 Modify the program flow to allow user to register again

- After user registered for the first time, personal information cannot be changed anymore. By modifying the program flow, register Activity can appear again.

```
vi ~/apk-output/smali/com/hkbc/worldcup/GoalActivity.smali
```

Task B1.4 Application Compiling and Signing

The modified application needed to be re-compiled and signed before installing on any device or emulator.

- To recompile the application

```
java -jar ~/apktool1.4.7/apktool.jar b ./apk-output
```

- To sign the application

```
java -jar ~/autosign.jar ./apk-output/dist/WorldCup.apk
```

- Installing the application

```
adb install -r ./apk-output/dist/WorldCup.apk
```

End of Lab