Capita selecta: Android security

André Jacobs — r0370664

27 november 2016

1 Step 1: Application analysis

For this first step I have chosen the application tiny flashlight [1][2]
Using apktool to decompile the apk following permissions were found in the `AndroidManifest.xml` file:

```
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
<uses-permission android:name="android.permission.CAMERA"/>
<uses-permission android:name="android.permission.FLASHLIGHT"/>
<uses-permission android:name="android.permission.WAKE_LOCK"/>
<uses-permission android:name="android.permission.VIBRATE"/>
<uses-permission android:name="android.permission.INTERNET"/>
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
<uses-permission android:name="com.devuni.flashlight.CONTROL_LIGHT"/>
```

I used the included `pyparser.py` script I have written to first parse the `ALL_API_CALLS.txt` file and then look through all the smali files using a series of `grep` operations. The result of this script can be found in the file called `result`.
This shows that following permissions were used:

- android.permission.READ_SMS: this seems to be used for reading notitications regarding download requests. This permission is not stated in the manifest.
- android.permission.CHANGE_WIFI_STATE: This is used to process some sort of transaction. This permission is also not stated in the manifest.
- android.permission.NFC: Not stated in the manifest
- android.permission.VIBRATE: used by the AudioManager and NotificationManager of the application. This permission is requested in the manifest.
- com.android.browser.permission.READ_HISTORY_BOOKMARKS: not requested
- android.permission.CAMERA: used to access flashlight, requested in manifest
- android.permission.INTERNET: Used by http client component, requested in manifest
- android.permission.WRITE_EXTERNAL_STORAGE: Used by UI component and to save settings not requested in manifest
- android.permission.ACCESS_FINE_LOCATION: used by the LocationManager, probably for ads. Not requested in manifest.
- android.permission.KILL_BACKGROUND_PROCESSES: used for placing ads in the main UI thread. Not requested in manifest.
- android.permission.READ_PHONE_STATE: Not requested
- android.permission.ACCESS_NETWORK_STATE: requested in manifest
- android.permission.SYSTEM_ALERT_WINDOW: not requested in manifest
- android.permission.WRITE_SETTINGS: not requested in manifest
- android.permission.WAKE_LOCK: requested in manifest

2 Step 3

Flowdroid found following sinks and sources:

- `<android.util.Log: int i(java.lang.String,java.lang.String)>("SMSSPY",$r7)`

  from the following sources:

  - `android.content.Intent (in <de.mobinauten.smsspy.EmergencyService: int onStartCommand(android.content.Intent,int,int)>)`

- `virtualinvoke <android.content.Context: android.content.ComponentName startService(android.content.Intent)>($r2)`

  from the following sources:

  - `android.content.Context (in <de.mobinauten.smsspy.EmergencyBroadcastReceiver: void onReceive(android.content.Context,android.content.Intent)>)`
  - `android.content.Intent (in <de.mobinauten.smsspy.EmergencyBroadcastReceiver: void onReceive(android.content.Context,android.content.Intent)>)`

- `staticinvoke <android.util.Log: int i(java.lang.String,java.lang.String)>("SMSSPY", $r5)`

  from the following sources:

  - `android.content.Intent (in <de.mobinauten.smsspy.EmergencyBroadcastReceiver: void onReceive(android.content.Context,android.content.Intent)>)`

Referenties

[1] https://play.google.com/store/apps/details?id=com.devuni.flashlight&utm_source=www.apk4fun.com

[2] https://www.apk4fun.com/apk/1823/