Android Mobile Pentest 101

Lecture 10.4 – Creating Exploit: Intent & Filter

Goal: Understand basic android intent & filter

Introduction

- This lecture will help you understand Android Intent & Intent Filter.

What’s Intent & Intent Filter?

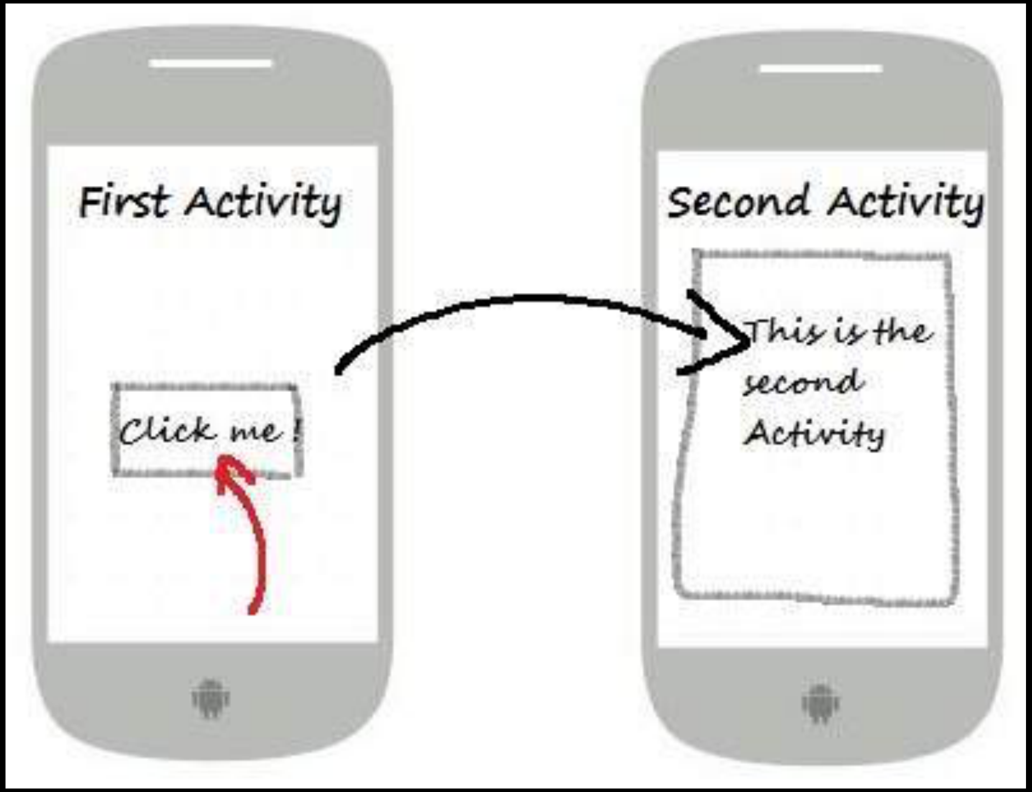
- Mentioned here: https://developer.android.com/guide/components/intents-filters
- An Intent is a messaging object you can use to request an action from another app component.
- There are 2 common types of Intent: Explicit & Implicit

Explicit Intent

- Explicit intent going to be connected internal world of application, suppose if you wants to connect one activity to another activity
- You'll typically use an explicit intent to start a component in your own app, because you know the class name of the activity or service you want to start

Explicit Intent

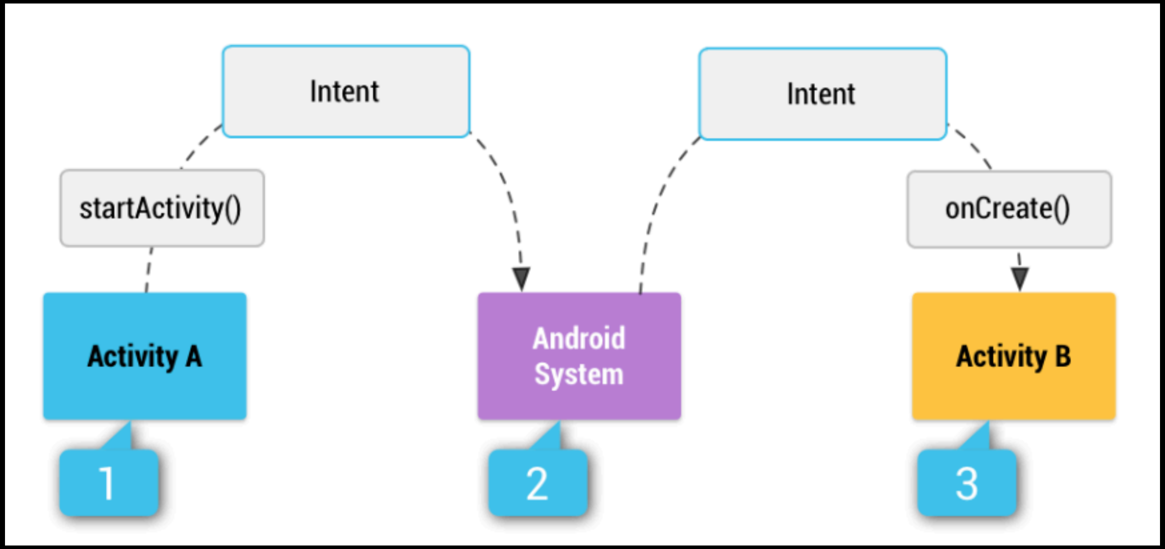
```
// Explicit Intent by specifying its class name
Intent i = new Intent(FirstActivity.this, SecondActivity.class);

// Starts TargetActivity
startActivity(i);
```



Implicit Intent

- These intents do not name a target and the field for the component name is left blank.
- Implicit intents are often used to activate components in other applications.

Implicit Intent



[1] Activity A creates an Intent with an action description and passes it to startActivity().

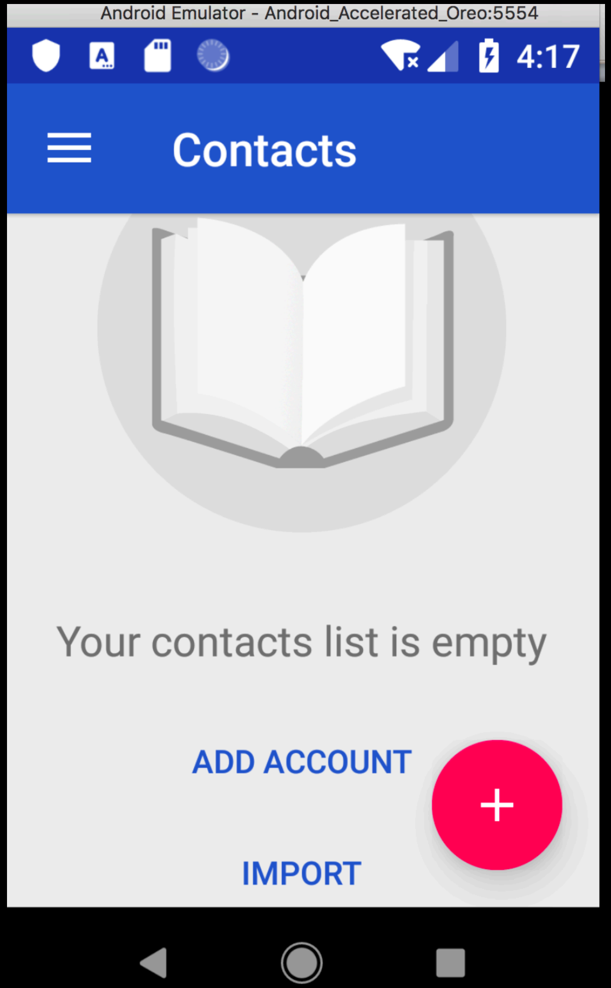
[2] The Android System searches all apps for an intent filter that matches the intent.

When a match is found,
[3] the system starts the matching activity (Activity B) by invoking its onCreate() method and passing it the Intent.

Implicit Intent

- Full code at: https://github.com/tsug0d/AndroidMobilePentest101/blob/master/lab/MainActivity.java_readcontact

```
@Override
  protected void onCreate(Bundle savedInstanceState) {
     super.onCreate(savedInstanceState);
     setContentView(R.layout.activity_main);
     Intent read_contact=new Intent();
     read_contact.setAction(android.content.Intent.ACTION_VIEW);
     read_contact.setData(ContactsContract.Contacts.CONTENT_URI);
     startActivity(read_contact);
  }
```



Android Emulator - Android_Accelerated_Oreo:5554

Your contacts list is empty

Intent Filters

- So the attacker will create the activity then free call component of other app without restriction? No!
- Android OS uses filters to pinpoint the set of Activities, Services, and Broadcast receivers that can handle the Intent with help of specified set of action, categories, data scheme associated with an Intent
- App use <intent-filter> element in the manifest file to list down actions, categories and data types associated with any activity, service, or broadcast receiver.

Intent Filters

```
<activity android:name=".CustomActivity"
  android:label="@string/app_name">

  <intent-filter>
          <action android:name="android.intent.action.VIEW" />
          <action android:name="com.example.MyApplication.LAUNCH" />
          <category android:name="android.intent.category.DEFAULT" />
          <data android:scheme="http" />
  </intent-filter>

</activity>
```

- Once this activity is defined along with above mentioned filters, other activities will be able to invoke this activity using either the android.intent.action.VIEW, or using the com.example.MyApplication.LAUNCH action provided their category is android.intent.category.DEFAULT.
- The <data> element specifies the data type expected by the activity to be called and for above example our custom activity expects the data to start with the "http://"