Android Mobile Pentest 101

© tsug0d, September 2018

Lecture 10.4 – Creating Exploit: Intent & Filter

Mục tiêu: Hiểu Intent & Filter

Introduction

- Bài này giúp bạn hiểu được intent và intent filter là gì

What’s Intent & Intent Filter?

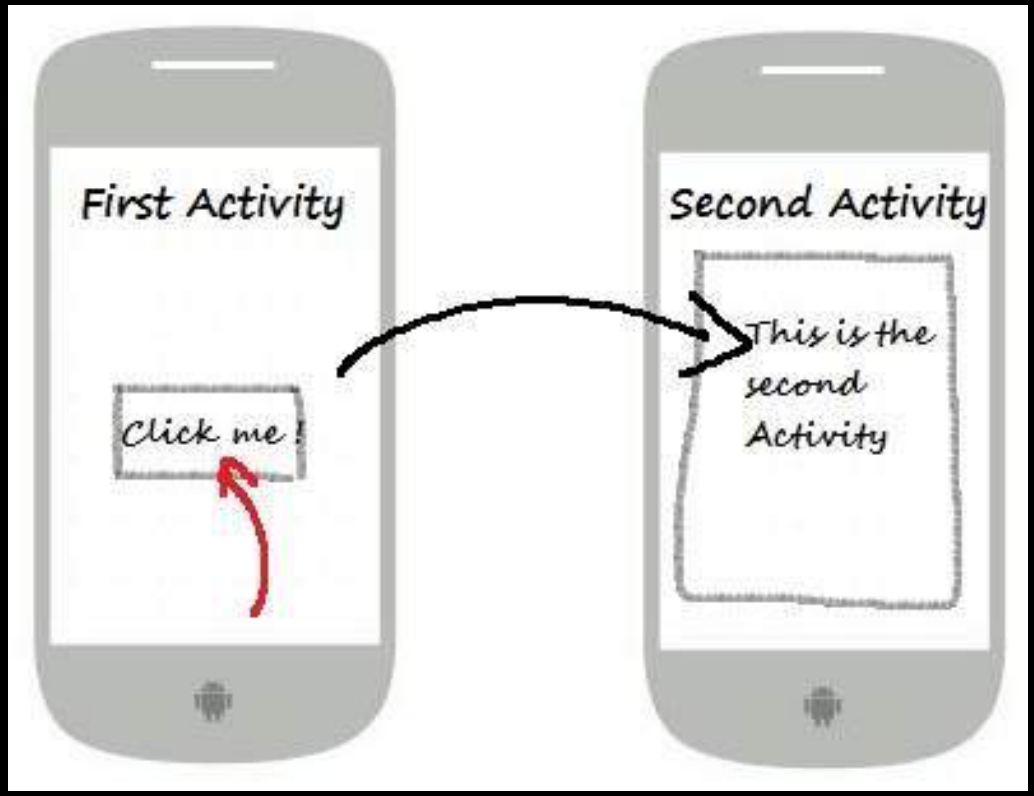
- Đề cập ở đây: https://developer.android.com/guide/components/intents-filters
- Intent đại khái là 1 lời nhắn, các thành phần của android sử dụng lời nhắn này để gọi nhau.
- Có 2 loại Intent: Explicit & Implicit

Explicit Intent

- Explicit intent dùng để gọi nội bộ app, thường là để activity A gọi activity B
- Vì sao? vì bạn biết được tên của activity hay service trong app, nên cứ thế mà gọi lên thôi.

Explicit Intent

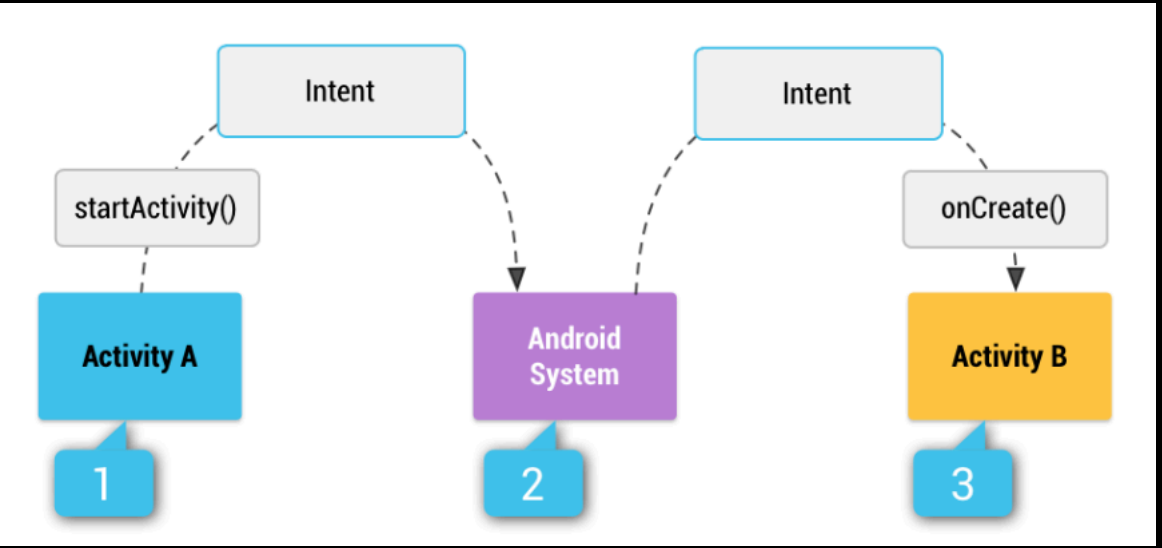
```
// Explicit Intent by specifying its class name
Intent i = new Intent(FirstActivity.this, SecondActivity.class);

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



Implicit Intent

- Implicit Intent thường không cần tên của target
- Implicit Intents được sử dụng để gọi thành phần của app khác.

Implicit Intent



[1] Activity A tạo 1 Intent với 1 lời “mời gọi đối tượng" cụ thể rồi đưa nó vào startActivity().

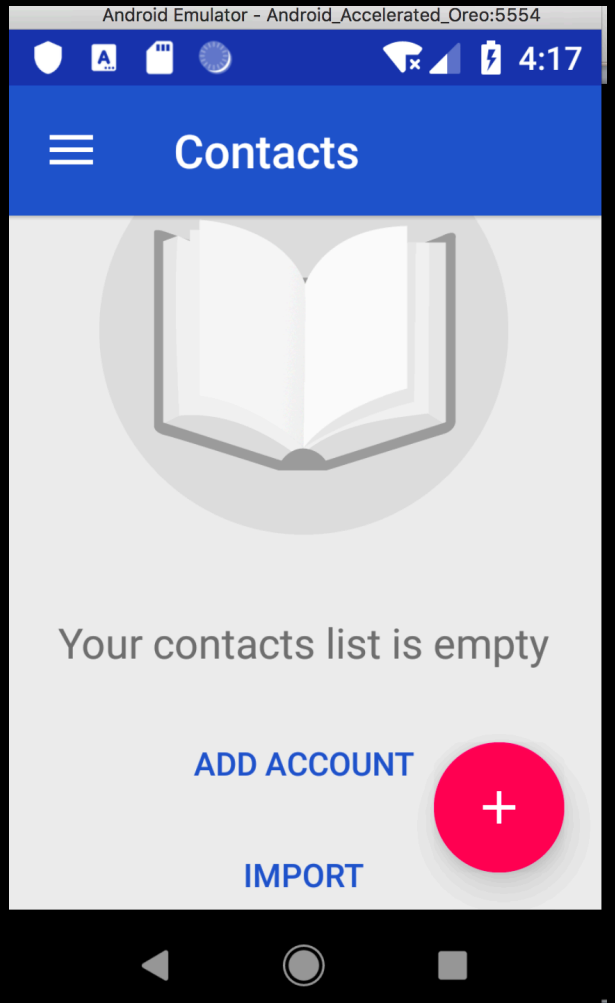
[2] The Android System tự tìm các app có cái đối tượng được định nghĩa trong “intent filter”của app khác Khi tìm được rồi thì,

[3] Hệ thống gọi activity (Activity B) bằng các gọi onCreate() method của nó và đem vào 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);
  }
```



Intent Filters

- Như vậy nghĩa là thích gọi gì thì gọi à? hông!
- Android OS sử dụng intent filters để định nghĩa Activities, Services, và Broadcast receivers nào được gọi
- Tag <intent-filter> trong file manifest để định nghĩa

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>
```

- Ví dụ app của mình define như này thì :
- Activity của app khác có thể gọi android.intent.action.VIEW, hoặc com.example.MyApplication.LAUNCH, android.intent.category.DEFAULT.
- The <data> element định nghĩa kiểu activity được gọi lên, ở đây là http://