Android Intent

*Abstract*—The malicious Android application can get the intent information from “Intent app” if the Show Activity has same action name as the hacker’s application activity in Intent Filters.

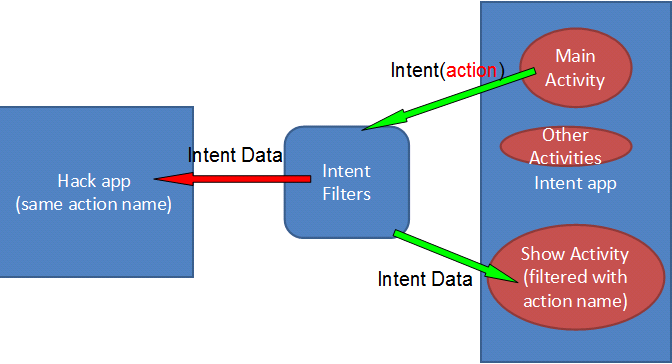
# Introduction

From Android documentation:

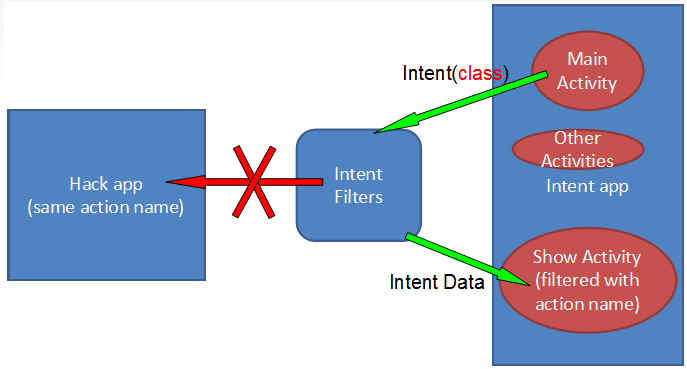
<http://developer.android.com/guide/components/intents-filters.html>

“When you create an implicit intent, the Android system finds the appropriate component to start by comparing the contents of the intent to the intent filters declared in the manifest file of other apps on the device. If the intent matches an intent filter, the system starts that component and delivers it the Intent object. If multiple intent filters are compatible, the system displays a dialog so the user can pick which app to use.”

As shown below, the hacker app sets up an activity to listen for an intent with intent.setAction(actionName). If actionName happens to be the same as the Intent Filter’s action name, then the hacker app may intercept the intent data sent by Main Activity to Show Activity (the legitimate receiver). The system will show a dialog box to ask the user to choose between two apps, which one should respond to the intent.



To prevent this attack, the sender can use intent.setClassName() to specify the class and activity name of the receiver. Now the Hacker App cannot capture and respond to the intent.



# Lab Activity

Create an application *TestIntent* with package name *android.testintent;* one activity *TestIntentActivity* with layout name *main*. Here is the source code for TestIntentActivity.java:

|  |
| --- |
| package android.testintent;  import android.app.Activity; import android.content.Intent; import android.os.Bundle; import android.view.View; import android.view.View.OnClickListener; import android.widget.Button; import android.widget.EditText;  public class TestIntentActivity extends Activity { /\*\* Called when the activity is first created. \*/ String name; String password; @Override public void onCreate(Bundle savedInstanceState) { super.onCreate(savedInstanceState); setContentView(R.layout.main); final Button logb=(Button)findViewById(R.id.logb); final EditText Uname=(EditText)findViewById(R.id.uname); final EditText Pword=(EditText)findViewById(R.id.pword); // final String name; // final String password; logb.setOnClickListener(new OnClickListener() { public void onClick(View v) { name=Uname.getText().toString(); password=Pword.getText().toString();  Intent intent = new Intent();  intent.putExtra("username", name);  intent.putExtra("password", password);  intent.setAction("android.testintent.Login"); //intent.setClassName("android.testintent","android.testintent.Login"); startActivity(intent); }});  }} |

Here is the source code for Login.java:

|  |
| --- |
| package android.testintent;  import android.app.Activity; import android.os.Bundle; import android.widget.TextView;  public class Login extends Activity {  @Override public void onCreate(Bundle savedInstanceState) { super.onCreate(savedInstanceState); setContentView(R.layout.loginlayout); final TextView text=(TextView)findViewById(R.id.logindata); // text.setText("babo"); text.setText("UserName: "+getIntent().getStringExtra("username")+"\nPassword: "+getIntent().getStringExtra("password")); } } |

Here is AndroidManifest.xml

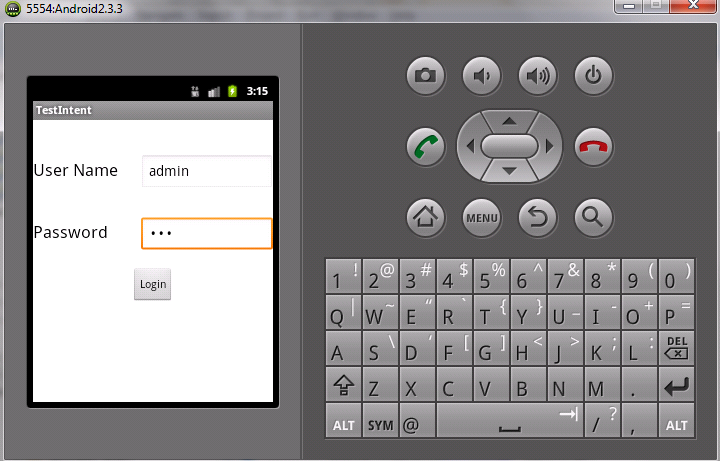
|  |
| --- |
| <?xml version="1.0" encoding="utf-8"?> <manifest xmlns:android="<http://schemas.android.com/apk/res/android>" package="android.testintent" android:versionCode="1" android:versionName="1.0"> <uses-sdk android:minSdkVersion="8" />  <application android:icon="@drawable/icon" android:label="@string/app\_name"> <activity android:name=".Login" android:theme="@android:style/Theme.NoTitleBar" /> <activity android:name=".Login" android:label="Login" > <intent-filter> <action android:name="android.testintent.Login" /> <category android:name="android.intent.category.DEFAULT" /> </intent-filter> </activity>  <activity android:name=".TestIntentActivity" android:label="@string/app\_name"> <intent-filter> <action android:name="android.intent.action.MAIN" /> <category android:name="android.intent.category.LAUNCHER" /> </intent-filter> </activity>  </application> </manifest> |

Create another application HackerApp. Within its MainActivity class:

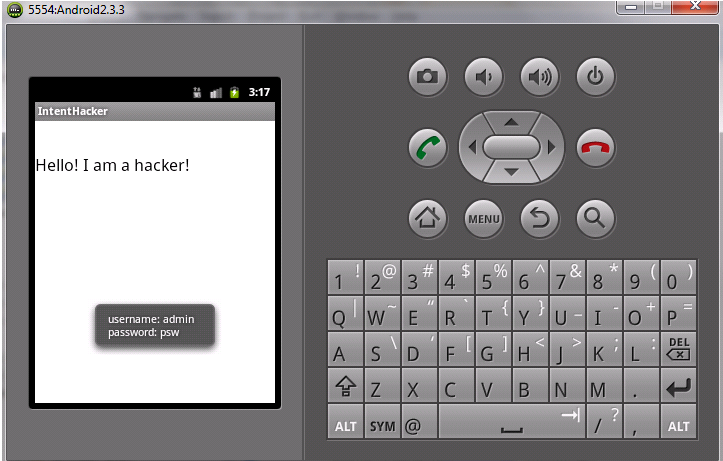
|  |
| --- |
| **protected** **void** onCreate(Bundle savedInstanceState) {  **super**.onCreate(savedInstanceState);  setContentView(R.layout.*activity\_main*);  Toast.*makeText*(getBaseContext(), "username "+**this**.getIntent().getStringExtra("username")+";password "+  **this**.getIntent().getStringExtra("password"), Toast.*LENGTH\_LONG*).show();  } |

In its AndroidManifest.xml:

|  |
| --- |
| <intent-filter>  <action android:name=*"android.testintent.Login"* />  <category android:name=*"android.intent.category.DEFAULT"* />  </intent-filter> |

Start both TestIntent and HackerApp on the same phone. Enter user name/password and press Login button. 

A dialog box comes up and asks the user to choose “Complete action using HackerApp or Login”。 If you choose HackerApp, then it captures and responds to the intent:

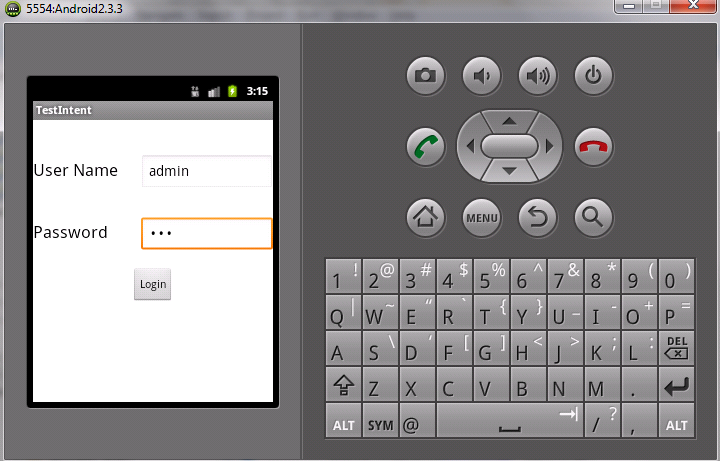


As a remedy, if you change the two lines in TestIntentActivity.java to:

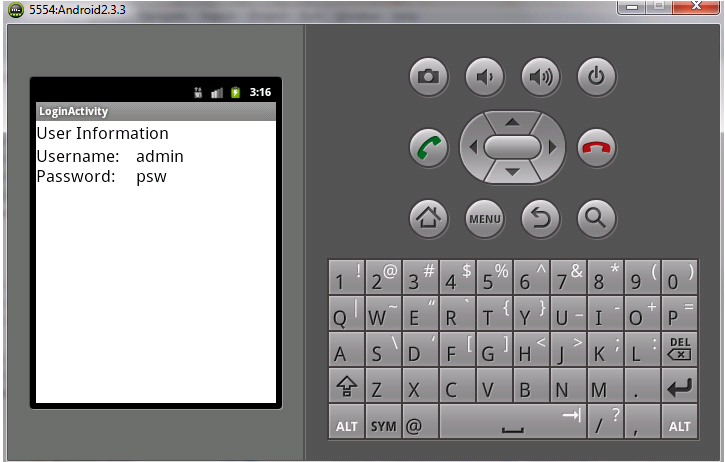
//intent.setAction("android.testintent.Login");

intent.setClassName("android.testintent","android.testintent.Login");

Again start both TestIntent and HackerApp on the same phone. Enter user name/password and press Login button, the correct login screen should come up and display the entered user name and password:



After clicking on Login:



Even though I have provided most of the source code, the code is still incomplete, since all the layout XML files are not provided. Based on the UI shown above, create 2 complete applications that can demonstrate the above steps successfully. If you reuse the source code provided here, then please make sure to use the appropriate statements in the XML files to set android:id, e.g., “android:id="@+id/XXXXX" to match the resource ID in the corresponding java file.

# Report

Please include step-by-step screenshots in the lab report, with your name in English as the username, and your student ID as the password.