

Bezpieczeństwo Aplikacji Mobilnych

Laboratorium 2 - sprawozdanie

Krzysztof Jachym

## 1. Pobranie .apk

Najpierw a adb shell listujemy wszystkie pakiety.

```
D:\Szkola\semestr3\BAM\lab2>adb shell
generic_x86_arm:/ $ pm list packages
package:com.google.android.networkstack.tethering
package:com.android.cts.priv.ctsshim
package:com.google.android.youtube
package:com.android.internal.display.cutout.emulation.corner
package:com.google.android.ext.services
```

Następnie sprawdzamy ścieżkę do wybranego pakietu

```
1|generic_x86_arm:/ $ pm path com.android.bluetooth
package:/system/app/Bluetooth/Bluetooth.apk
```

i komendą pull pobieramy plik apk na dysk

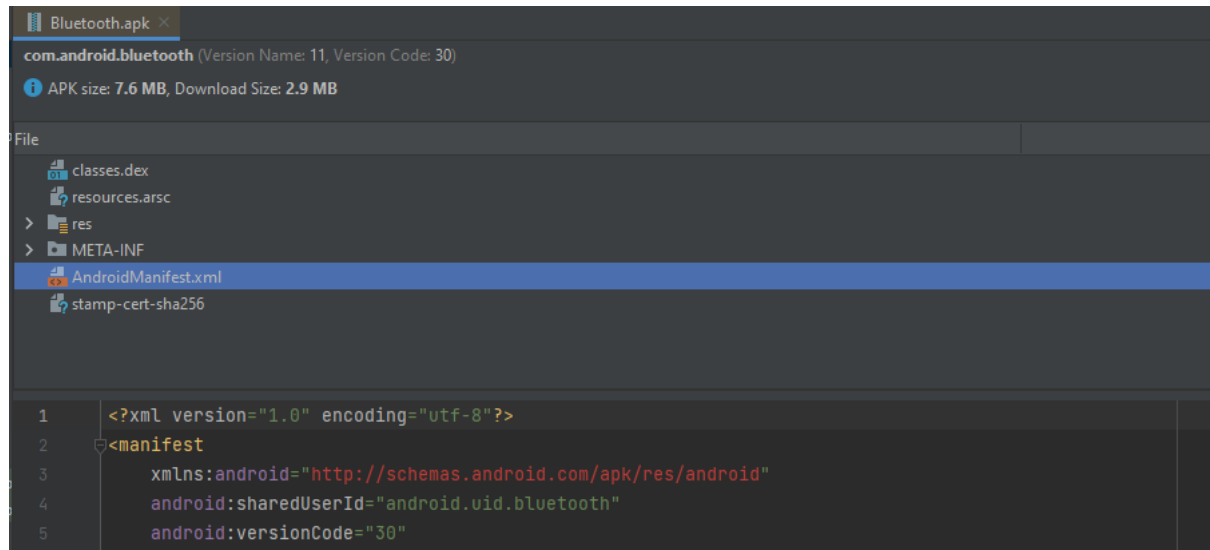
```
D:\Szkola\semestr3\BAM\lab2>adb pull /system/app/Bluetooth/Bluetooth.apk .
/system/app/Bluetooth/Bluetooth.apk: 1 file pulled, 0 skipped. 127.6 MB/s (7918941 bytes in 0.059s)
```

## 2. Inżynieria wsteczna apk

Używając narzędzia aapt wyświetlamy zawartość AndroidManifest.xml zawartego w apk:

```
D:\Szkola\semestr3\BAM\lab2>aapt dump xmltree Bluetooth.apk AndroidManifest.xml
N: android=http://schemas.android.com/apk/res/android
E: manifest (line=2)
  A: android:sharedUserId(0x0101000b)="android.uid.bluetooth" (Raw: "android.uid.bluetooth")
  A: android:versionCode(0x0101021b)=(type 0x10)0x1e
  A: android:versionName(0x0101021c)="11" (Raw: "11")
  A: android:compileSdkVersion(0x01010572)=(type 0x10)0x1e
  A: android:compileSdkVersionCodename(0x01010573)="11" (Raw: "11")
  A: package="com.android.bluetooth" (Raw: "com.android.bluetooth")
  A: platformBuildVersionCode=(type 0x10)0x1e
  A: platformBuildVersionName=(type 0x10)0xb
E: uses-sdk (line=6)
  A: android:minSdkVersion(0x0101020c)=(type 0x10)0x1e
  A: android:targetSdkVersion(0x01010270)=(type 0x10)0x1e
E: original-package (line=10)
  A: android:name(0x01010003)="com.android.bluetooth" (Raw: "com.android.bluetooth")
E: permission (line=13)
```

Możemy zrobić to również z wewnątrz android studio:



Z pliku manifestu aplikacji Bluetooth.apk możemy wywnioskować między innymi:  
Wymaga bardzo wielu uprawnień (razem ponad 50):

```
<uses-permission
    android:name="android.permission.RECEIVE_BOOT_COMPLETED" />

<uses-permission
    android:name="android.permission.ACCESS_BLUETOOTH_SHARE" />

<uses-permission
    android:name="android.permission.ACCESS_COARSE_LOCATION" />

<uses-permission
    android:name="android.permission.INTERNET" />

<uses-permission
    android:name="android.permission.BLUETOOTH" />

<uses-permission
    android:name="android.permission.BLUETOOTH_ADMIN" />

<uses-permission
    android:name="android.permission.BLUETOOTH_PRIVILEGED" />
```

Wykorzystuje bibliotekę javax.obex:

```
<uses-library
    android:name="javax.obex" />
```

Składa się z wielu różnych serwisów i receiverów:

```

<service
    android:name="com.android.bluetooth.sap.SapService"
    android:enabled="@ref/0x7f03001a"
    android:process="@ref/0x7f0e006c">

    <intent-filter>

        <action
            android:name="android.bluetooth.IBluetoothSap" />
        </intent-filter>
    </service>

```

```

<receiver
    android:name="com.android.bluetooth.opp.BluetoothOppHandoverReceiver"
    android:permission="com.android.permission.WHITELIST_BLUETOOTH_DEVICE"
    android:process="@ref/0x7f0e006c">

    <intent-filter>

        <action
            android:name="android.bluetooth.opp.intent.action.WHITELIST_DEVICE" />

        <action
            android:name="android.bluetooth.opp.intent.action.STOP_HANDOVER_TRANSFER" />
        </intent-filter>
    </receiver>

```

Wypakowujemy plik apk i konwertujemy plik .dex do .jar:

```

D:\Szkola\semestr3\BAM\lab2>.\dex-tools-2.1\d2j-dex2jar.bat classes.dex -o classes.jar
Picked up _JAVA_OPTIONS: -Xmx512M
dex2jar classes.dex -> classes.jar

```

Korzystając z serwisu javadecompilers dekompilujemy jar:

## Decompile Results


### Decompile Results

File Name: classes.jar

Decompiler: jadx

Job status: Done.

 [Twitter](#)  [Facebook](#)  [Stumbleupon](#)

 [classes.jar](#) > [sources](#) > [org](#) > [android](#) > [btsap](#) > [SapApi.java](#)

```
package org.android.btsap;

import com.google.protobuf.micro.ByteStringMicro;
import com.google.protobuf.micro.CodedInputStreamMicro;
import com.google.protobuf.micro.CodedOutputStreamMicro;
```

Przeglądając kod możemy znaleźć implementację aktywności z pliku manifestu:

```
<activity
    android:theme="@ref/0x01030239"
    android:label="@ref/0x7f0e0022"
    android:name="com.android.bluetooth.opp.BluetoothOppLauncherActivity"
    android:enabled="@ref/0x7f030016"
    android:process="@ref/0x7f0e006c">

    <intent-filter>

        <action
            android:name="android.intent.action.SEND" />
```

```
public class BluetoothOppLauncherActivity extends Activity {

    /* renamed from: D */
    private static final boolean f1725D = true;
    private static final Pattern PLAIN_TEXT_TO_ESCAPE = Pattern.compile("[<>&]| {2,}|\r?\n");
    private static final String TAG = "BluetoothOppLauncherActivity";

    /* renamed from: V */
    private static final boolean f1726V = false;

    /* JADX WARNING: Removed duplicated region for block: B:21:0x00ec A[SYNTHETIC, Splitter:B:21:0x00ec] */
    /* JADX WARNING: Removed duplicated region for block: B:49:0x0198 A[SYNTHETIC, Splitter:B:49:0x0198] */
    /* JADX WARNING: Removed duplicated region for block: B:57:0x01bb A[SYNTHETIC, Splitter:B:57:0x01bb] */
    /* JADX WARNING: Removed duplicated region for block: B:64:0x01df A[SYNTHETIC, Splitter:B:64:0x01df] */
    /* JADX WARNING: Unknown top exception splitter block from list: {B:61:0x01c3=Splitter:B:61:0x01c3, B:18:0x00cd=Splitter:B:18:0x00cd} */
    /* Code decompiled incorrectly, please refer to instructions dump. */
    private android.net.Uri creatFileForSharedContent(android.content.Context r11, java.lang.CharSequence r12) {
```

funkcja uruchamiająca inną aktywność

```
public void launchDevicePicker() {
    if (!BluetoothOppManager.getInstance(this).isEnabled()) {
        Intent intent = new Intent(this, BluetoothOppBtEnableActivity.class);
        intent.setFlags(VCardConfig.FLAG_REFRAIN_QP_TO_NAME_PROPERTIES);
        startActivity(intent);
        return;
    }
    Intent intent2 = new Intent("android.bluetooth.devicepicker.action.LAUNCH");
    intent2.setFlags(8388608);
    intent2.putExtra("android.bluetooth.devicepicker.extra.NEED_AUTH", false);
    intent2.putExtra("android.bluetooth.devicepicker.extra.FILTER_TYPE", 2);
    intent2.putExtra("android.bluetooth.devicepicker.extra.LAUNCH_PACKAGE", "com.android.bluetooth");
    intent2.putExtra("android.bluetooth.devicepicker.extra.DEVICE_PICKER_LAUNCH_CLASS", BluetoothOppReceiver.class);
    startActivity(intent2);
}
```

fragment funkcji onCreate wysyłający broadcast

```
} else if (action.equals("android.btopp.intent.action.OPEN")) {  
    Uri data = getIntent().getData();  
    Intent intent3 = new Intent();  
    intent3.setAction(action);  
    intent3.setClassName("com.android.bluetooth", BluetoothOppReceiver.class.getName());  
    intent3.setDataAndNormalize(data);  
    sendBroadcast(intent3);  
    finish();  
}
```

Dekompilacja z użyciem apktool:

```
D:\Szkola\semestr3\BAM\lab2>apktool d Bluetooth.apk  
Picked up _JAVA_OPTIONS: -Xmx512M  
I: Using Apktool 2.6.1 on Bluetooth.apk  
I: Loading resource table...  
I: Decoding AndroidManifest.xml with resources...  
I: Loading resource table from file: C:\Users\Krysztor\AppData\Local\Temp\apktool\Bluetooth.apk\resources.apktool\resources.apktool  
I: Regular manifest package...  
I: Decoding file-resources...  
I: Decoding values */* XMLs...  
I: Baksmaling classes.dex...
```

ponowne budowanie:

```
D:\Szkola\semestr3\BAM\lab2>apktool b Bluetooth  
Picked up _JAVA_OPTIONS: -Xmx512M  
I: Using Apktool 2.6.1  
I: Checking whether sources has changed...  
I: Smaling smali folder into classes.dex...  
I: Checking whether resources has changed...  
I: Building resources...  
I: Building apk file...  
I: Copying unknown files/dir...  
I: Built apk...
```

Zgodnie z oczekiwaniami nie możemy zainstalować aplikacji:

```
D:\Szkola\semestr3\BAM\lab2\Bluetooth\dist>adb install Bluetooth.apk  
Performing Streamed Install  
adb: failed to install Bluetooth.apk: Failure [INSTALL_PARSE_FAILED_NO_CERTIFICATES:  
/data/app/vmdl1164828267.tmp/base.apk: Failed to collect certificates from /data/app/  
t to get length of null array]
```

Tworzymy keystore:

```
D:\Szkola\semestr3\BAM\lab2\Bluetooth\dist>keytool -genkey -keystore test.keystore -validity 3650 -alias test
Picked up _JAVA_OPTIONS: -Xmx512M
Enter keystore password:
Keystore password is too short - must be at least 6 characters
Enter keystore password:
Re-enter new password:
What is your first and last name?
[Unknown]: As Df
What is the name of your organizational unit?
[Unknown]: GHJK
What is the name of your organization?
[Unknown]: Qwer
What is the name of your City or Locality?
[Unknown]: Tyui
What is the name of your State or Province?
[Unknown]: OP
What is the two-letter country code for this unit?
[Unknown]: ZX
Is CN=As Df, OU=GHJK, O=Qwer, L=Tyui, ST=OP, C=ZX correct?
[no]: yes
```

i podpisujemy apk

```
D:\Szkola\semestr3\BAM\lab2\Bluetooth\dist>jarsigner -keystore test.keystore -verbose Bluetooth.apk test
Picked up _JAVA_OPTIONS: -Xmx512M
Enter Passphrase for keystore:
adding: META-INF/MANIFEST.MF
adding: META-INF/TEST.SF
adding: META-INF/TEST.DSA
signing: AndroidManifest.xml
signing: classes.dex
signing: res/anim/fragment_close_enter.xml
signing: res/anim/fragment_close_exit.xml
signing: res/anim/fragment_fade_enter.xml
signing: res/anim/fragment_fade_exit.xml
signing: res/anim/fragment_fast_out_extra_slow_in.xml
signing: res/anim/fragment_open_enter.xml
signing: res/anim/fragment_open_exit.xml
signing: res/drawable/bt_incomming_file_notification.xml
```

### 3. Podmiana zainstalowanej aplikacji

Kopiowanie na dysk

```
package:com.google.android.inputmethod.latin
package:com.android.theme.icon_pack.circular.android
package:com.google.android.apps.restore
generic_x86_arm:/ $ pm path com.example.exampleapp
package:/data/app/~~8Er3OB9tTzVWnUwXSbkTMw==/com.example.exampleapp-
generic_x86_arm:/ $ exit

D:\Szkola\semestr3\BAM\lab2>adb pull /data/app/~~8Er3OB9tTzVWnUwXSbkTMw==/base.apk .
/data/app/~~8Er3OB9tTzVWnUwXSbkTMw==/com.example.exampleapp...le pull

D:\Szkola\semestr3\BAM\lab2>
```



Dekompilacja:

```
D:\Szkola\semestr3\BAM\lab2>apktool d base.apk
Picked up _JAVA_OPTIONS: -Xmx512M
I: Using Apktool 2.6.1 on base.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: C:\Users\Krysztor\AppData\Local\apktool\framework\1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
I: Copying META-INF/services directory
```

Zmiana dotyczy tekstu na przycisku w głównej aktywności, plik `/base/res/layout/MainActivity.xml`:

```
<?xml version='1.0' encoding='utf-8'?>  
    <TextView  
        android:id="@+id/textView1"  
        android:layout_width="fill_parent"  
        android:padding="10.0dip"  
        android:text="Get decompiled bozo"  
        android:layout_height="wrap_content">  
        <EditText  
            android:id="@+id/userName"  
            android:layout_width="fill_parent"  
            android:layout_height="wrap_content"/>  
    </TextView>
```

Ponowne budowanie:

```
D:\Szkola\semestr3\BAM\lab2>apktool b base
Picked up _JAVA_OPTIONS: -Xmx512M
I: Using Apktool 2.6.1
I: Checking whether sources has changed...
I: Smaling smali folder into classes.dex...
I: Checking whether resources has changed...
I: Building resources...
I: Copying libs... (/kotlin)
I: Copying libs... (/META-INF/services)
I: Building apk file...
I: Copying unknown files/dir...
I: Built apk...
```

Podpisanie poprzednio utworzonym kluczem:

```
D:\Szkoła\semestr3\BAM\lab2\base\dist>jarsigner -keystore test.keystore -verbose base.apk test
Picked up _JAVA_OPTIONS: -Xmx512M
Enter Passphrase for keystore:
  adding: META-INF/MANIFEST.MF
  adding: META-INF/TEST.SF
  adding: META-INF/TEST.DSA
signing: META-INF/services/kotlinx.coroutines.CoroutineExceptionHandler
signing: META-INF/services/kotlinx.coroutines.internal.MainDispatcherFactory
signing: AndroidManifest.xml
signing: classes.dex
signing: kotlin/annotation/annotation.kotlin_builtins
signing: kotlin/collections/collections.kotlin_builtins
signing: kotlin/coroutines/coroutines.kotlin_builtins
signing: kotlin/internal/internal.kotlin_builtins
signing: kotlin/kotlin.kotlin_builtins
signing: kotlin/ranges/ranges.kotlin_builtins
signing: kotlin/reflect/reflect.kotlin_builtins
```

Odinstalowujemy poprzednią wersję i instalujemy zmienioną:

```
D:\Szkola\semestr3\BAM\lab2>adb uninstall com.example.exampleapp
Success
```

otrzymaliśmy błąd.

```
D:\Szkola\semestr3\BAM\lab2\base\dist>adb install base.apk
Performing Streamed Install
adb: failed to install base.apk: Failure [INSTALL_FAILED_TEST_ONLY: installPackageLI]
```

żeby go naprawić należy zmodyfikować plik manifestu i zbudować i podpisać plik ponownie

```
android:testOnly="false"
```

Po tej zmianie udało się zainstalować apk

```
D:\Szkola\semestr3\BAM\lab2\base\dist>adb install base.apk
Performing Streamed Install
Success
```

Wyniki zmian są widoczne na ekranie głównym

