

DC5527.ORG

DEF CON GROUP

REVERSING ANDROID APPLICATIONS FOR FUN AND PROFIT

Maycon Maia Vitali
maycon@hacknroll.com

AGENDA

- Who am I?
- Hello Android!
- Reversing Toolset
- Static Analysis
 - (Short Introduction to) Smali Code
- Dynamic Analysis
 - Binary Instrumentation
- Let's Go
 - Patching WhatsApp Messenger (On-the-fly)
 - Patching WhatsApp Messenger (Binary APK)

WHO AM I?

- Maycon Maia Vitali
- Bsc & Msc in **Computer Science**
- Trustwave
 - Security Consultant @ **SpiderLabs**
 - **Member** of Mobile Application Security VT
- Hack N' Roll (Member & Founder)
- Certifications
 - **Offensive** Security Certified Expert (OSCE)
 - **Mobile** Application Penetration Test (MAPT)

HELLO WORD, ANDROID!
ANDROID FUNDAMENTALS

Application Components

- **Activities**
 - Entry point for interacting with the user
- **Services**
 - Keep an app running in the background
- **Content Providers**
 - App data that you can store in the file system
- **Broadcast Receivers**
 - Enables the system to deliver events

THE MANIFEST FILE

AndroidManifest.xml

- Application **information**
 - Name, Version, API Level, SDK version etc.
- User **permissions**
 - Internet Access, Camera, access external storage etc.
- **Components**
 - Activities, Services, Receivers and Providers
- Componentes **resources**

THE MANIFEST FILE

AndroidManifest.xml

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <manifest xmlns:android="http://schemas.android.com/apk/res/android"
3     package="com.example.android.basiccontactables"
4     android:versionCode="1"
5     android:versionName="1.0" >
6
7     <uses-permission android:name="android.permission.READ_CONTACTS"/>
8     <!-- Min/target SDK versions (<uses-sdk>) managed by build.gradle -->
9     <permission android:name="android"></permission>
10
11     <application
12         android:allowBackup="true"
13         android:icon="@drawable/ic_launcher"
14         android:label="@string/app_name"
15         android:theme="@style/Theme.Sample" >
16         <activity
17             android:name="com.example.android.basiccontactables.MainActivity"
18             android:label="@string/app_name"
19             android:launchMode="singleTop">
20             <meta-data
21                 android:name="android.app.searchable"
22                 android:resource="@xml/searchable" />
23             <intent-filter>
24                 <action android:name="android.intent.action.SEARCH" />
25             </intent-filter>
26             <intent-filter>
27                 <action android:name="android.intent.action.MAIN" />
28                 <category android:name="android.intent.category.LAUNCHER" />
29             </intent-filter>
30         </activity>
31     </application>
32 </manifest>
```

THE MANIFEST FILE

AndroidManifest.xml

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <manifest xmlns:android="http://schemas.android.com/apk/res/android"
3     package="com.example.android.basiccontactables"
4     android:versionCode="1"
5     android:versionName="1.0" >
6
7     <uses-permission android:name="android.permission.READ_CONTACTS" />
8     <!-- Min/target SDK versions (<uses-sdk>) managed by build.gradle -->
9     <permission android:name="android.permission.READ_CONTACTS" />
10
11     <application
12         android:allowBackup="true"
13         android:icon="@drawable/ic_launcher"
14         android:label="@string/app_name"
15         android:theme="@style/Theme.Sample" >
16         <activity
17             android:name="com.example.android.basiccontactables.MainActivity"
18             android:label="@string/app_name"
19             android:launchMode="singleTop">
20             <meta-data
21                 android:name="android.app.searchable"
22                 android:resource="@xml/searchable" />
23             <intent-filter>
24                 <action android:name="android.intent.action.SEARCH" />
25             </intent-filter>
26             <intent-filter>
27                 <action android:name="android.intent.action.MAIN" />
28                 <category android:name="android.intent.category.LAUNCHER" />
29             </intent-filter>
30         </activity>
31     </application>
32 </manifest>
```

Package
Informations

THE MANIFEST FILE

AndroidManifest.xml

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <manifest xmlns:android="http://schemas.android.com/apk/res/android"
3     package="com.example.android.basiccontactables"
4     android:versionCode="1"
5     android:versionName="1.0" >
6
7     <uses-permission android:name="android.permission.READ_CONTACTS"/>
8     <!-- Min/target SDK versions (<uses-sdk>) managed by build.gradle -->
9     <permission android:name="android"></permission>
10
11     <application
12         android:allowBackup="true"
13         android:icon="@drawable/ic_launcher"
14         android:label="@string/app_name"
15         android:theme="@style/Theme.Sample" >
16         <activity
17             android:name="com.example.android.basiccontactables.MainActivity"
18             android:label="@string/app_name"
19             android:launchMode="singleTop">
20             <meta-data
21                 android:name="android.app.searchable"
22                 android:resource="@xml/searchable" />
23             <intent-filter>
24                 <action android:name="android.intent.action.SEARCH" />
25             </intent-filter>
26             <intent-filter>
27                 <action android:name="android.intent.action.MAIN" />
28                 <category android:name="android.intent.category.LAUNCHER" />
29             </intent-filter>
30         </activity>
31     </application>
32 </manifest>
```

Permissions

THE MANIFEST FILE

AndroidManifest.xml

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <manifest xmlns:android="http://schemas.android.com/apk/res/android"
3     package="com.example.android.basiccontactables"
4     android:versionCode="1"
5     android:versionName="1.0" >
6
7     <uses-permission android:name="android.permission.READ_CONTACTS"/>
8     <!-- Min/target SDK versions (<uses-sdk>) managed by build.gradle -->
9     <permission android:name="android"></permission>
10
11     <application
12         android:allowBackup="true"
13         android:icon="@drawable/ic_launcher"
14         android:label="@string/app_name"
15         android:theme="@style/Theme.Sample" >
16         <activity
17             android:name="com.example.android.basiccontactables.MainActivity"
18             android:label="@string/app_name"
19             android:launchMode="singleTop">
20             <meta-data
21                 android:name="android.app.searchable"
22                 android:resource="@xml/searchable" />
23             <intent-filter>
24                 <action android:name="android.intent.action.SEARCH" />
25             </intent-filter>
26             <intent-filter>
27                 <action android:name="android.intent.action.MAIN" />
28                 <category android:name="android.intent.category.LAUNCHER" />
29             </intent-filter>
30         </activity>
31     </application>
32 </manifest>
```

Activity
Component

THE MANIFEST FILE

AndroidManifest.xml

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <manifest xmlns:android="http://schemas.android.com/apk/res/android"
3     package="com.example.android.basiccontactables"
4     android:versionCode="1"
5     android:versionName="1.0" >
6
7     <uses-permission android:name="android.permission.READ_CONTACTS"/>
8     <!-- Min/target SDK versions (<uses-sdk>) managed by build.gradle -->
9     <permission android:name="android"></permission>
10
11     <application
12         android:allowBackup="true"
13         android:icon="@drawable/ic_launcher"
14         android:label="@string/app_name"
15         android:theme="@style/Theme.Sample" >
16         <activity
17             android:name="com.example.android.basiccontactables.MainActivity"
18             android:label="@string/app_name"
19             android:launchMode="singleTop">
20             <meta-data
21                 android:name="android.app.searchable"
22                 android:resource="@xml/searchable" />
23             <intent-filter>
24                 <action android:name="android.intent.action.SEARCH" />
25             </intent-filter>
26             <intent-filter>
27                 <action android:name="android.intent.action.MAIN" />
28                 <category android:name="android.intent.category.LAUNCHER" />
29             </intent-filter>
30         </activity>
31     </application>
32 </manifest>
```

Resource

THE MANIFEST FILE

AndroidManifest.xml

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <manifest xmlns:android="http://schemas.android.com/apk/res/android"
3     package="com.example.android.basiccontactables"
4     android:versionCode="1"
5     android:versionName="1.0" >
6
7     <uses-permission android:name="android.permission.READ_CONTACTS"/>
8     <!-- Min/target SDK versions (<uses-sdk>) managed by build.gradle -->
9     <permission android:name="android"></permission>
10
11     <application
12         android:allowBackup="true"
13         android:icon="@drawable/ic_launcher"
14         android:label="@string/app_name"
15         android:theme="@style/Theme.Sample" >
16         <activity
17             android:name="com.example.android.basiccontactables.MainActivity"
18             android:label="@string/app_name"
19             android:launchMode="singleTop">
20             <meta-data
21                 android:name="android.app.searchable"
22                 android:resource="@xml/searchable" />
23             <intent-filter>
24                 <action android:name="android.intent.action.SEARCH" />
25             </intent-filter>
26             <intent-filter>
27                 <action android:name="android.intent.action.MAIN" />
28                 <category android:name="android.intent.category.LAUNCHER" />
29             </intent-filter>
30         </activity>
31     </application>
32 </manifest>
```

Intent Filters

REVERSING TOOLSET

REVERSING TOOLSET

- adb
 - Android Debug Bridge
- unzip + dex2jar
 - Decompress apk file and convert .dex file to .class
- apktool + keytool + jarsigner
 - Decode/build/sign .apk files
- ByteCode Viewer <3
 - Last two toolset
- Frida <3
 - Android process instrumentation tool

ANDROID DEBUG BRIDGE

adb

- adb logcat
- adb forward <local> <remote>
- adb kill-server
- **adb install <apk>**
- adb start-server
- **adb uninstall <pkg>**
- **adb devices -l**
- adb sideload <file>
- **adb push <local>... <remote>**
- **adb pull <remote>... <local>**
- adb root
- adb unroot
- adb -s <specific device> ...

ANDROID DEBUG BRIDGE

adb

```
{20:09} [maycon@darkstar ~/Research/Android]
$> adb start-server
* daemon not running. starting it now on port 5037 *
* daemon started successfully *

{20:09} [maycon@darkstar ~/Research/Android]
$> adb devices -l
List of devices attached
4d0541327b0b5000      device usb:3-3 product:cm_logands model:GT_S7272 device:logands

{20:09} [maycon@darkstar ~/Research/Android]
$> adb shell
shell@logands:/ $ su
root@logands:/ # id
uid=0(root) gid=0(root) context=u:r:init_shell:s0
root@logands:/ # uname -a
Linux localhost 3.4.5-03lp #1 SMP PREEMPT Tue Jul 19 23:21:03 UTC 2016 armv7l GNU/Linux
root@logands:/ # █
```


ANDROID DEBUG BRIDGE

adb

```
{20:09} [maycon@darkstar ~/Research/Android]
$> adb start-server
* daemon not running. starting it now on port 5037 *
* daemon started successfully *

{20:09} [maycon@darkstar ~/Research/Android]
$> adb devices -l
List of devices attached
4d0541327b0b5000      device usb:3-3 product:cm_logands model:GT_S7272 device:logands

{20:09} [maycon@darkstar ~/Research/Android]
$> adb shell
shell@logands:/ $ su
root@logands:/ # id
uid=0(root) gid=0(root) context=u:r:init_shell:s0
root@logands:/ # uname -a
Linux localhost 3.4.5-03lp #1 SMP PREEMPT Tue Jul 19 23:21:03 UTC 2016 armv7l GNU/Linux
root@logands:/ #
```

ANDROID DEBUG BRIDGE

adb

```
{20:09} [maycon@darkstar ~/Research/Android]
$> adb start-server
* daemon not running. starting it now on port 5037 *
* daemon started successfully *

{20:09} [maycon@darkstar ~/Research/Android]
$> adb devices -l
List of devices attached
4d0541327b0b5000      device usb:3-3 product:cm_logands model:GT_S7272 device:logands

{20:09} [maycon@darkstar ~/Research/Android]
$> adb shell
shell@logands:/ $ su
root@logands:/ # id
uid=0(root) gid=0(root) context=u:r:init_shell:s0
root@logands:/ # uname -a
Linux localhost 3.4.5-03lp #1 SMP PREEMPT Tue Jul 19 23:21:03 UTC 2016 armv7l GNU/Linux
root@logands:/ #
```

ANDROID DEBUG BRIDGE

adb

```
{20:09} [maycon@darkstar ~/Research/Android]
$> adb start-server
* daemon not running. starting it now on port 5037 *
* daemon started successfully *

{20:09} [maycon@darkstar ~/Research/Android]
$> adb devices -l
List of devices attached
4d0541327b0b5000      device usb:3-3 product:cm_logands model:GT_S7272 device:logands

{20:09} [maycon@darkstar ~/Research/Android]
$> adb shell
shell@logands:/ $ su
root@logands:/ # id
uid=0(root) gid=0(root) context=u:r:init_shell:s0
root@logands:/ # uname -a
Linux localhost 3.4.5-03lp #1 SMP PREEMPT Tue Jul 19 23:21:03 UTC 2016 armv7l GNU/Linux
root@logands:/ #
```

DECOMPRESS APK FILE

unzip + dex2jar

```
{20:37} [maycon@darkstar ~/Research/Android/WhatsApp]
$> ln -s WhatsApp-Messenger_v2.17.107.apk WhatsApp-Messenger_v2.17.107.zip

{20:37} [maycon@darkstar ~/Research/Android/WhatsApp]
$> unzip WhatsApp-Messenger_v2.17.107.zip -d unzip &> /dev/null

{20:37} [maycon@darkstar ~/Research/Android/WhatsApp]
$> ls unzip/
AndroidManifest.xml  assets  classes.dex  lib  META-INF  res  resources.arsc

{20:37} [maycon@darkstar ~/Research/Android/WhatsApp]
$> dex2jar -o WhatsApp-Messenger_v2.17.107.jar unzip/classes.dex
dex2jar unzip/classes.dex -> WhatsApp-Messenger_v2.17.107.jar
Detail Error Information in File ./classes-error.zip
Please report this file to http://code.google.com/p/dex2jar/issues/entry if possible.

{20:38} [maycon@darkstar ~/Research/Android/WhatsApp]
$> □
```

DECOMPRESS APK FILE

unzip + dex2jar

```
{20:37} [maycon@darkstar ~/Research/Android/WhatsApp]
$> ln -s WhatsApp-Messenger_v2.17.107.apk WhatsApp-Messenger_v2.17.107.zip

{20:37} [maycon@darkstar ~/Research/Android/WhatsApp]
$> unzip WhatsApp-Messenger_v2.17.107.zip -d unzip &> /dev/null

{20:37} [maycon@darkstar ~/Research/Android/WhatsApp]
$> ls unzip/
AndroidManifest.xml  assets  classes.dex  lib  META-INF  res  resources.arsc

{20:37} [maycon@darkstar ~/Research/Android/WhatsApp]
$> dex2jar -o WhatsApp-Messenger_v2.17.107.jar unzip/classes.dex
dex2jar unzip/classes.dex -> WhatsApp-Messenger_v2.17.107.jar
Detail Error Information in File ./classes-error.zip
Please report this file to http://code.google.com/p/dex2jar/issues/entry if possible.

{20:38} [maycon@darkstar ~/Research/Android/WhatsApp]
$> □
```

DECOMPRESS APK FILE

unzip + dex2jar

```
{20:37} [maycon@darkstar ~/Research/Android/WhatsApp]
$> ln -s WhatsApp-Messenger_v2.17.107.apk WhatsApp-Messenger_v2.17.107.zip

{20:37} [maycon@darkstar ~/Research/Android/WhatsApp]
$> unzip WhatsApp-Messenger_v2.17.107.zip -d unzip &> /dev/null

{20:37} [maycon@darkstar ~/Research/Android/WhatsApp]
$> ls unzip/
AndroidManifest.xml  assets  classes.dex  lib  META-INF  res  resources.arsc

{20:37} [maycon@darkstar ~/Research/Android/WhatsApp]
$> dex2jar -o WhatsApp-Messenger_v2.17.107.jar unzip/classes.dex
dex2jar unzip/classes.dex -> WhatsApp-Messenger_v2.17.107.jar
Detail Error Information in File ./classes-error.zip
Please report this file to http://code.google.com/p/dex2jar/issues/entry if possible.

{20:38} [maycon@darkstar ~/Research/Android/WhatsApp]
$> □
```

DECOMPRESS APK FILE

unzip + dex2jar

```
{20:37} [maycon@darkstar ~/Research/Android/WhatsApp]
$> ln -s WhatsApp-Messenger_v2.17.107.apk WhatsApp-Messenger_v2.17.107.zip

{20:37} [maycon@darkstar ~/Research/Android/WhatsApp]
$> unzip WhatsApp-Messenger_v2.17.107.zip -d unzip &> /dev/null

{20:37} [maycon@darkstar ~/Research/Android/WhatsApp]
$> ls unzip/
AndroidManifest.xml  assets  classes.dex  lib  META-INF  res  resources.arsc

{20:37} [maycon@darkstar ~/Research/Android/WhatsApp]
$> dex2jar -o WhatsApp-Messenger_v2.17.107.jar unzip/classes.dex
dex2jar unzip/classes.dex -> WhatsApp-Messenger_v2.17.107.jar
Detail Error Information in File ./classes-error.zip
Please report this file to http://code.google.com/p/dex2jar/issues/entry if possible.

{20:38} [maycon@darkstar ~/Research/Android/WhatsApp]
$> □
```

DECOMPRESS APK FILE

unzip + dex2jar

```
{20:37} [maycon@darkstar ~/Research/Android/WhatsApp]
$> ln -s WhatsApp-Messenger_v2.17.107.apk WhatsApp-Messenger_v2.17.107.zip

{20:37} [maycon@darkstar ~/Research/Android/WhatsApp]
$> unzip WhatsApp-Messenger_v2.17.107.zip -d unzip &> /dev/null

{20:37} [maycon@darkstar ~/Research/Android/WhatsApp]
$> ls unzip/
AndroidManifest.xml  assets  classes.dex  lib  META-INF  res  resources.arsc

{20:37} [maycon@darkstar ~/Research/Android/WhatsApp]
$> dex2jar -o WhatsApp-Messenger_v2.17.107.jar unzip/classes.dex
dex2jar unzip/classes.dex -> WhatsApp-Messenger_v2.17.107.jar
Detail Error Information in File ./classes-error.zip
Please report this file to http://code.google.com/p/dex2jar/issues/entry if possible.

{20:38} [maycon@darkstar ~/Research/Android/WhatsApp]
$> □
```


DECOMPRESS APK FILE

unzip + dex2jar

```
{20:37} [maycon@darkstar ~/Research/Android/WhatsApp]
$> ln -s WhatsApp-Messenger_v2.17.107.apk WhatsApp-Messenger_v2.17.107.zip

{20:37} [maycon@darkstar ~/Research/Android/WhatsApp]
$> unzip WhatsApp-Messenger_v2.17.107.zip -d unzip &> /dev/null

{20:37} [maycon@darkstar ~/Research/Android/WhatsApp]
$> ls unzip/
AndroidManifest.xml  assets  classes.dex  lib  META-INF  res  resources.arsc

{20:37} [maycon@darkstar ~/Research/Android/WhatsApp]
$> dex2jar -o WhatsApp-Messenger v2.17.107.jar unzip/classes.dex
dex2jar unzip/classes.dex -> WhatsApp-Messenger_v2.17.107.jar
Detail Error Information in File ./classes-error.zip
Please report this file to http://code.google.com/p/dex2jar/issues/entry if possible.

{20:38} [maycon@darkstar ~/Research/Android/WhatsApp]
$> □
```

apktool + keytool + jarsigner

```
{21:11} [maycon@darkstar ~/Research/Android]
$> apktool
Apktool v2.2.2 - a tool for reengineering Android apk files
with smali v2.1.3 and baksmali v2.1.3
Copyright 2014 Ryszard Wiśniewski <brut.alll@gmail.com>
Updated by Connor Tumbleson <connor.tumbleson@gmail.com>

usage: apktool
  -advance,--advanced      prints advance information.
  -version,--version        prints the version then exits
usage: apktool if|install-framework [options] <framework.apk>
  -p,--frame-path <dir>    Stores framework files into <dir>.
  -t,--tag <tag>           Tag frameworks using <tag>.
usage: apktool d[ecode] [options] <file_apk>
  -f,--force               Force delete destination directory.
  -o,--output <dir>        The name of folder that gets written. Default is apk.out
  -p,--frame-path <dir>    Uses framework files located in <dir>.
  -r,--no-res              Do not decode resources.
  -s,--no-src              Do not decode sources.
  -t,--frame-tag <tag>     Uses framework files tagged by <tag>.
usage: apktool b[uild] [options] <app_path>
  -f,--force-all          Skip changes detection and build all files.
  -o,--output <dir>        The name of apk that gets written. Default is dist/name.apk
  -p,--frame-path <dir>    Uses framework files located in <dir>.

For additional info, see: http://ibotpeaches.github.io/Apktool/
For smali/baksmali info, see: https://github.com/JesusFreke/smali
```

apktool + keytool + jarsigner

```
{21:11} [maycon@darkstar ~/Research/Android]
$> apktool
Apktool v2.2.2 - a tool for reengineering Android apk files
with smali v2.1.3 and baksmali v2.1.3
Copyright 2014 Ryszard Wiśniewski <brut.alll@gmail.com>
Updated by Connor Tumbleson <connor.tumbleson@gmail.com>

usage: apktool
  -advance,--advanced      prints advance information.
  -version,--version        prints the version then exits
usage: apktool if|install-framework [options] <framework.apk>
  -p,--frame-path <dir>    Stores framework files into <dir>.
  -t,--tag <tag>           Tag frameworks using <tag>.
usage: apktool d[ecode] [options] <file_apk>
  -f,--force               Force delete destination directory.
  -o,--output <dir>        The name of folder that gets written. Default is apk.out
  -p,--frame-path <dir>    Uses framework files located in <dir>.
  -r,--no-res              Do not decode resources.
  -s,--no-src              Do not decode sources.
  -t,--frame-tag <tag>     Uses framework files tagged by <tag>.
usage: apktool b[uild] [options] <app_path>
  -f,--force-all          Skip changes detection and build all files.
  -o,--output <dir>        The name of apk that gets written. Default is dist/name.apk
  -p,--frame-path <dir>    Uses framework files located in <dir>.

For additional info, see: http://ibotpeaches.github.io/Apktool/
For smali/baksmali info, see: https://github.com/JesusFreke/smali
```

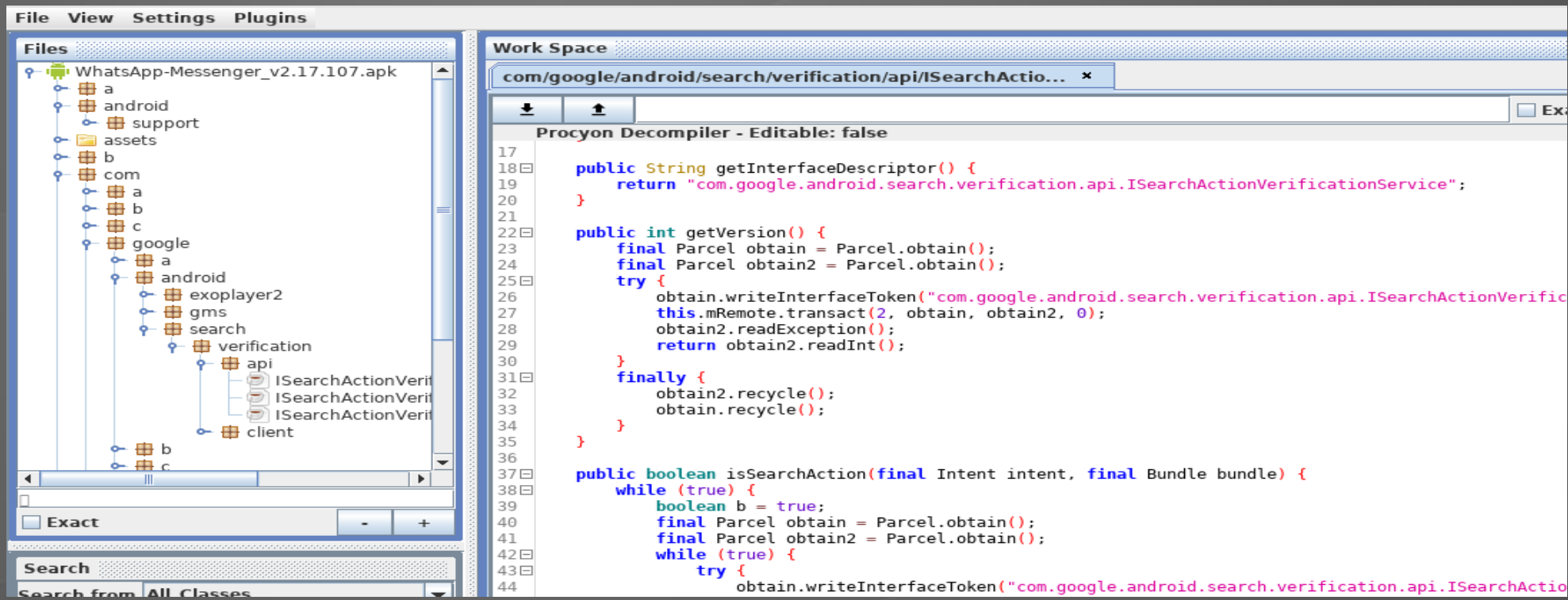
apktool + keytool + jarsigner

```
$ vim ./build_sign_install.sh
```

```
30 echo "Building new APK file.."
31 $APKTOOL build -o "${APP_BUILD_FILE}" "${APP_SRC_PATH}"
32
33 # Create the keystore (if not yet)
34 if [ ! -f "$KEYSTORE_FILE" ]; then
35     echo "Creating keystore..."
36
37     $KEYTOOL -genkey -v \
38         -keystore "${KEYSTORE_FILE}" -keyalg RSA \
39         -keysize 2048 -validity 365 -alias "${APP_NAME}"
40 fi
41
42 echo "Signing new APK file.."
43 $JARSIGNER -verbose \
44     -sigalg SHA1withRSA -digestalg SHA1 \
45     -keystore "${KEYSTORE_FILE}" \
46     "${APP_BUILD_FILE}" "${APP_NAME}"
47
```

BYTECODE VIEWER

procyon + CFR + JD-GUI + FernFlower + Krakatau



STATIC ANALYSIS

Introduction to Smali Language

INTRODUCTION TO SMALI

Registers

- Virtual Registers
 - Up to 64k registers
 - 128 first are the most common (v0, v1, v2 ...)
 - Can store everything (int, float, Object ...)
 - Two naming schema:
 - Local: v0, v1, v2...
 - Params: p0, p1, p2...

Local	Param	
v0		First local register
v1		Second local register
v2	p0	First param register
v3	p1	Second param registers
v4	p2	Third param register

INTRODUCTION TO SMALI

Data Type

- Primitive Data Type
 - I – int
 - J – long
 - Z – boolean
 - D – double
 - F – float
 - S – short
 - C – char
 - V – void (when return value)
- Classes:
 - *Ljava/lang/Object;*
- Arrays:
 - *[I*
 - *[Ljava/lang/Object;*
 - *[[I*
- List of types: simple concatenation
 - *getAttr(Landroid/util/AttributeSet;[III)*

INTRODUCTION TO SMALI

Java → Smali

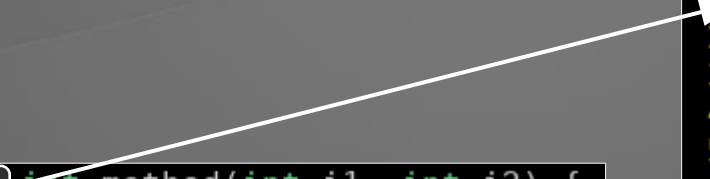
```
1 public int method(int i1, int i2) {  
2     int i3 = i1 * i2;  
3     return i3 * 2;  
4 }
```

```
1 .method public method(II)I  
2 .limit registers 4  
3  
4 ; this: v1 (Ltest2;  
5 ; parameter[0] : v2 (I)  
6 ; parameter[1] : v3 (I)  
7  
8     mul-int        v0, v2, v3 ; v0 = v2 * v3  
9     mul-int/lit-8   v0, v0, 2 ; v0 = v0 * 2  
10  
11     return v0  
12  
13 .end method
```

INTRODUCTION TO SMALI

Java → Smali

```
1 public int method(int i1, int i2) {  
2     int i3 = i1 * i2;  
3     return i3 * 2;  
4 }
```




```
1 .method public method(II)I  
2 .limit registers 4  
3  
4 ; this: v1 (Ltest2;  
5 ; parameter[0] : v2 (I)  
6 ; parameter[1] : v3 (I)  
7  
8     mul-int        v0, v2, v3 ; v0 = v2 * v3  
9     mul-int/lit-8   v0, v0, 2 ; v0 = v0 * 2  
10  
11     return v0  
12  
13 .end method
```

INTRODUCTION TO SMALI

Java → Smali

```
1 public int method(int i1, int i2) {  
2     int i3 = i1 * i2;  
3     return i3 * 2;  
4 }
```



```
1 .method public method(II)I  
2 .limit registers 4  
3  
4 ; this: v1 (Ltest2;  
5 ; parameter[0] : v2 (I)  
6 ; parameter[1] : v3 (I)  
7  
8     mul-int        v0, v2, v3 ; v0 = v2 * v3  
9     mul-int/lit-8   v0, v0, 2 ; v0 = v0 * 2  
10  
11     return v0  
12  
13 .end method
```

INTRODUCTION TO SMALI

Java → Smali

```
1 public int method(int i1, int i2) {  
2     int i3 = i1 * i2;  
3     return i3 * 2;  
4 }
```

```
1 .method public method (II) I  
2 .limit registers 4  
3  
4 ; this: v1 (Ltest2;  
5 ; parameter[0] : v2 (I)  
6 ; parameter[1] : v3 (I)  
7  
8     mul-int        v0, v2, v3 ; v0 = v2 * v3  
9     mul-int/lit-8  v0, v0, 2  ; v0 = v0 * 2  
10  
11     return v0  
12  
13 .end method
```

INTRODUCTION TO SMALI

Java → Smali

```
1 public int method(int i1, int i2) {  
2     int i3 = i1 * i2;  
3     return i3 * 2;  
4 }
```

```
1 .method public method(I)I  
2 .limit registers 4  
3  
4 ; this: v1 (Ltest2;  
5 ; parameter[0] : v2 (I)  
6 ; parameter[1] : v3 (I)  
7  
8     mul-int        v0, v2, v3 ; v0 = v2 * v3  
9     mul-int/lit-8   v0, v0, 2 ; v0 = v0 * 2  
10  
11     return v0  
12  
13 .end method
```

INTRODUCTION TO SMALI

Java → Smali

```
1 public int method(int i1, int i2) {  
2     int i3 = i1 * i2;  
3     return i3 * 2;  
4 }
```

```
1 .method public method(II)I  
2 .limit registers 4  
3  
4 ; this: v1 (Ltest2;  
5 ; parameter[0] : v2 (I)  
6 ; parameter[1] : v3 (I)  
7  
8     mul-int        v0, v2, v3 ; v0 = v2 * v3  
9     mul-int/lit-8   v0, v0, 2 ; v0 = v0 * 2  
10  
11     return v0  
12  
13 .end method
```

INTRODUCTION TO SMALI

Java → Smali

```
1 public int method(int i1, int i2) {  
2     int i3 = i1 * i2;  
3     return i3 * 2;  
4 }
```

```
1 .method public method(II)I  
2 .limit registers 4  
3  
4 ; this: v1 (Ltest2;) [highlighted]  
5 ; parameter[0] : v2 (I)  
6 ; parameter[1] : v3 (I)  
7  
8     mul-int        v0, v2, v3 ; v0 = v2 * v3  
9     mul-int/lit-8   v0, v0, 2 ; v0 = v0 * 2  
10  
11     return v0  
12  
13 .end method
```

INTRODUCTION TO SMALI

Java → Smali

```
1 public int method(int i1, int i2) {  
2     int i3 = i1 * i2;  
3     return i3 * 2;  
4 }
```

```
1 .method public method(II)I  
2 .limit registers 4  
3  
4 ; this: v1 (Ltest2;  
5 ; parameter[0] : v2 (I)  
6 ; parameter[1] : v3 (I)  
7  
8 mul-int v0, v2, v3 ; v0 = v2 * v3  
9 mul-int/lit-8 v0, v0, 2 ; v0 = v0 * 2  
10  
11 return v0  
12  
13 .end method
```


INTRODUCTION TO SMALI

Java → Smali

```
1 public int method(int i1, int i2) {  
2     int i3 = i1 * i2;  
3     return i3 * 2;  
4 }
```

```
1 .method public method(II)I  
2 .limit registers 4  
3  
4 ; this: v1 (Ltest2;  
5 ; parameter[0] : v2 (I)  
6 ; parameter[1] : v3 (I)  
7  
8     mul-int        v0, v2, v3    ; v0 = v2 * v3  
9     mul-int/lit-8   v0, v0, 2    ; v0 = v0 * 2  
10  
11     return v0  
12  
13 .end method
```

INTRODUCTION TO SMALI

Java → Smali

```
1 public int method(int i1, int i2) {  
2     int i3 = i1 * i2;  
3     return i3 * 2;  
4 }
```

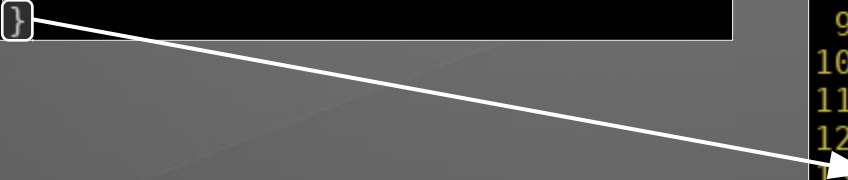
```
1 .method public method(II)I  
2 .limit registers 4  
3  
4 ; this: v1 (Ltest2;  
5 ; parameter[0] : v2 (I)  
6 ; parameter[1] : v3 (I)  
7  
8     mul-int        v0, v2, v3 ; v0 = v2 * v3  
9     mul-int/lit-8   v0, v0, 2 ; v0 = v0 * 2  
10  
11     return v0  
12  
13 .end method
```

INTRODUCTION TO SMALI

Java → Smali

```
1 public int method(int i1, int i2) {  
2     int i3 = i1 * i2;  
3     return i3 * 2;  
4 }
```

```
1 .method public method(II)I  
2 .limit registers 4  
3  
4 ; this: v1 (Ltest2;  
5 ; parameter[0] : v2 (I)  
6 ; parameter[1] : v3 (I)  
7  
8     mul-int        v0, v2, v3 ; v0 = v2 * v3  
9     mul-int/lit-8  v0, v0, 2  ; v0 = v0 * 2  
10  
11     return v0  
12  
13 .end method
```



INTRODUCTION TO SMALI

Smali → Java

```
1 .method private swap([II)V
2 .limit registers 5
3
4 ; this: v2 (Ltest10;)
5 ; parameter[0] : v3 ([I
6 ; parameter[1] : v4 (I)
7
8     aget                v0, v3, v4    ; v0 = v3[v4]
9
10    add-int/lit-8       v1, v4, 1     ; v1 = v4 + 1
11    aget                v1, v3, v1    ; v1 = v3[v1]
12    aput                v1, v3, v4    ; v3[v4] = v1
13
14    add-int/lit-8       v1, v4, 1     ; v1 = v4 + 1
15    aput                v0, v3, v1    ; v3[v1] = v0
16
17    return-void
18 .end method
```

INTRODUCTION TO SMALI

Smali → Java

```
1 .method private swap([II)V
2 .limit registers 5
3
4 ; this: v2 (Ltest10;)
5 ; parameter[0] : v3 ([I
6 ; parameter[1] : v4 (I)
7
8     aget                v0, v3, v4    ; v0 = v3[v4]
9
10    add-int/lit-8        v1, v4, 1    ; v1 = v4 + 1
11    aget                 v1, v3, v1    ; v1 = v3[v1]
12    aput                 v1, v3, v4    ; v3[v4] = v1
13
14    add-int/lit-8        v1, v4, 1    ; v1 = v4 + 1
15    aput                 v0, v3, v1    ; v3[v1] = v0
16
17    return-void
18 .end method
```

```
1
2
3
4
5
6
7
```

INTRODUCTION TO SMALI

Smali → Java

```
1 .method private swap([II)V
2 .limit registers 5
3
4 ; this: v2 (Ltest10;)
5 ; parameter[0] : v3 ([I
6 ; parameter[1] : v4 (I)
7
8     aget                v0, v3, v4    ; v0 = v3[v4]
9
10    add-int/lit-8       v1, v4, 1     ; v1 = v4 + 1
11    aget                v1, v3, v1    ; v1 = v3[v1]
12    aput                v1, v3, v4    ; v3[v4] = v1
13
14    add-int/lit-8       v1, v4, 1     ; v1 = v4 + 1
15    aput                v0, v3, v1    ; v3[v1] = v0
16
17    return-void
18 .end method
```

```
1
2
3
4
5
6
7
```

INTRODUCTION TO SMALI

Smali → Java

```
1 .method private swap([II)V
2 .limit registers 5
3
4 ; this: v2 (Ltest10;)
5 ; parameter[0] : v3 ([I
6 ; parameter[1] : v4 (I)
7
8     aget                v0, v3, v4    ; v0 = v3[v4]
9
10    add-int/lit-8       v1, v4, 1     ; v1 = v4 + 1
11    aget                v1, v3, v1    ; v1 = v3[v1]
12    aput                v1, v3, v4    ; v3[v4] = v1
13
14    add-int/lit-8       v1, v4, 1     ; v1 = v4 + 1
15    aput                v0, v3, v1    ; v3[v1] = v0
16
17    return-void
18 .end method
```

```
1 private
2 {
3
4
5
6
7 }
```

INTRODUCTION TO SMALI

Smali → Java

```
1 .method private swap([II)V
2 .limit registers 5
3
4 ; this: v2 (Ltest10;)
5 ; parameter[0] : v3 ([I
6 ; parameter[1] : v4 (I)
7
8     aget                v0, v3, v4    ; v0 = v3[v4]
9
10    add-int/lit-8        v1, v4, 1    ; v1 = v4 + 1
11    aget                 v1, v3, v1    ; v1 = v3[v1]
12    aput                 v1, v3, v4    ; v3[v4] = v1
13
14    add-int/lit-8        v1, v4, 1    ; v1 = v4 + 1
15    aput                 v0, v3, v1    ; v3[v1] = v0
16
17    return-void
18 .end method
```

```
1 private
2 {
3
4
5
6
7 }
```


INTRODUCTION TO SMALI

Smali → Java

```
1 .method private swap([II)V
2 .limit registers 5
3
4 ; this: v2 (Ltest10;)
5 ; parameter[0] : v3 ([I
6 ; parameter[1] : v4 (I)
7
8     aget                v0, v3, v4    ; v0 = v3[v4]
9
10    add-int/lit-8        v1, v4, 1    ; v1 = v4 + 1
11    aget                 v1, v3, v1    ; v1 = v3[v1]
12    aput                 v1, v3, v4    ; v3[v4] = v1
13
14    add-int/lit-8        v1, v4, 1    ; v1 = v4 + 1
15    aput                 v0, v3, v1    ; v3[v1] = v0
16
17    return-void
18 .end method
```

```
1 private void
2 {
3
4
5
6
7 }
```

INTRODUCTION TO SMALI

Smali → Java

```
1 .method private swap([II)V
2 .limit registers 5
3
4 ; this: v2 (Ltest10;)
5 ; parameter[0] : v3 ([I
6 ; parameter[1] : v4 (I)
7
8     aget                v0, v3, v4    ; v0 = v3[v4]
9
10    add-int/lit-8       v1, v4, 1     ; v1 = v4 + 1
11    aget                v1, v3, v1    ; v1 = v3[v1]
12    aput                v1, v3, v4    ; v3[v4] = v1
13
14    add-int/lit-8       v1, v4, 1     ; v1 = v4 + 1
15    aput                v0, v3, v1    ; v3[v1] = v0
16
17    return-void
18 .end method
```

```
1 private void
2 {
3
4
5
6
7 }
```

INTRODUCTION TO SMALI

Smali → Java

```
1 .method private swap([II)V
2 .limit registers 5
3
4 ; this: v2 (Ltest10;)
5 ; parameter[0] : v3 ([I
6 ; parameter[1] : v4 (I)
7
8     aget                v0, v3, v4    ; v0 = v3[v4]
9
10    add-int/lit-8       v1, v4, 1     ; v1 = v4 + 1
11    aget                v1, v3, v1    ; v1 = v3[v1]
12    aput                v1, v3, v4    ; v3[v4] = v1
13
14    add-int/lit-8       v1, v4, 1     ; v1 = v4 + 1
15    aput                v0, v3, v1    ; v3[v1] = v0
16
17    return-void
18 .end method
```

```
1 private void swap
2 {
3
4
5
6
7 }
```

INTRODUCTION TO SMALI

Smali → Java

```
1 .method private swap ([I) V
2 .limit registers 5
3
4 ; this: v2 (Ltest10;)
5 ; parameter[0] : v3 ([I
6 ; parameter[1] : v4 (I)
7
8     aget                v0, v3, v4    ; v0 = v3[v4]
9
10    add-int/lit-8       v1, v4, 1     ; v1 = v4 + 1
11    aget                v1, v3, v1    ; v1 = v3[v1]
12    aput                v1, v3, v4    ; v3[v4] = v1
13
14    add-int/lit-8       v1, v4, 1     ; v1 = v4 + 1
15    aput                v0, v3, v1    ; v3[v1] = v0
16
17    return-void
18 .end method
```

```
1 private void swap
2 {
3
4
5
6
7 }
```

INTRODUCTION TO SMALI

Smali → Java

```
1 .method private swap ([I) V
2 .limit registers 5
3
4 ; this: v2 (Ltest10;)
5 ; parameter[0] : v3 ([I
6 ; parameter[1] : v4 (I)
7
8     aget                v0, v3, v4    ; v0 = v3[v4]
9
10    add-int/lit-8       v1, v4, 1     ; v1 = v4 + 1
11    aget                v1, v3, v1    ; v1 = v3[v1]
12    aput                v1, v3, v4    ; v3[v4] = v1
13
14    add-int/lit-8       v1, v4, 1     ; v1 = v4 + 1
15    aput                v0, v3, v1    ; v3[v1] = v0
16
17    return-void
18 .end method
```

```
1 private void swap( int array[], int i )
2 {
3
4
5
6
7 }
```

INTRODUCTION TO SMALI

Smali → Java

```
1 .method private swap([II)V
2 .limit registers 5
3
4 ; this: v2 (Ltest10;)
5 ; parameter[0] : v3 ([I
6 ; parameter[1] : v4 (I
7
8     aget                v0, v3, v4    ; v0 = v3[v4]
9
10    add-int/lit-8       v1, v4, 1      ; v1 = v4 + 1
11    aget                v1, v3, v1     ; v1 = v3[v1]
12    aput                v1, v3, v4     ; v3[v4] = v1
13
14    add-int/lit-8       v1, v4, 1      ; v1 = v4 + 1
15    aput                v0, v3, v1     ; v3[v1] = v0
16
17    return-void
18 .end method
```

```
1 private void swap( int array[], int i )
2 {
3
4
5
6
7 }
```

INTRODUCTION TO SMALI

Smali → Java

```
1 .method private swap([II)V
2 .limit registers 5
3
4 ; this: v2 (Ltest10;)
5 ; parameter[0] : v3 ([I]
6 ; parameter[1] : v4 (I)
7
8     aget                v0, v3, v4    ; v0 = v3[v4]
9
10    add-int/lit-8       v1, v4, 1     ; v1 = v4 + 1
11    aget                v1, v3, v1    ; v1 = v3[v1]
12    aput                v1, v3, v4    ; v3[v4] = v1
13
14    add-int/lit-8       v1, v4, 1     ; v1 = v4 + 1
15    aput                v0, v3, v1    ; v3[v1] = v0
16
17    return-void
18 .end method
```

```
1 private void swap( int array[], int i )
2 {
3
4
5
6
7 }
```

INTRODUCTION TO SMALI

Smali → Java

```
1 .method private swap([II)V
2 .limit registers 5
3
4 ; this: v2 (Ltest10;)
5 ; parameter[0] : v3 ([I
6 ; parameter[1] : v4 (I)
7
8   aget          v0, v3, v4    ; v0 = v3[v4]
9
10  add-int/lit-8  v1, v4, 1     ; v1 = v4 + 1
11  aget          v1, v3, v1     ; v1 = v3[v1]
12  aput          v1, v3, v4     ; v3[v4] = v1
13
14  add-int/lit-8  v1, v4, 1     ; v1 = v4 + 1
15  aput          v0, v3, v1     ; v3[v1] = v0
16
17  return-void
18 .end method
```

```
1 private void swap( int array[], int i )
2 {
3
4
5
6
7 }
```


INTRODUCTION TO SMALI

Smali → Java

```
1 .method private swap([II)V
2 .limit registers 5
3
4 ; this: v2 (Ltest10;)
5 ; parameter[0] : v3 ([I
6 ; parameter[1] : v4 (I
7
8   aget          v0, v3, v4    ; v0 = v3[v4]
9
10  add-int/lit-8  v1, v4, 1     ; v1 = v4 + 1
11  aget          v1, v3, v1     ; v1 = v3[v1]
12  aput          v1, v3, v4     ; v3[v4] = v1
13
14  add-int/lit-8  v1, v4, 1     ; v1 = v4 + 1
15  aput          v0, v3, v1     ; v3[v1] = v0
16
17  return-void
18 .end method
```

```
1 private void swap( int array[], int i )
2 {
3     int temp = array[i];
4
5
6
7 }
```

INTRODUCTION TO SMALI

Smali → Java

```
1 .method private swap([II)V
2 .limit registers 5
3
4 ; this: v2 (Ltest10;)
5 ; parameter[0] : v3 ([I)
6 ; parameter[1] : v4 (I)
7
8     aget                v0, v3, v4    ; v0 = v3[v4]
9
10    add-int/lit-8        v1, v4, 1    ; v1 = v4 + 1
11    aget                v1, v3, v1    ; v1 = v3[v1]
12    aput                v1, v3, v4    ; v3[v4] = v1
13
14    add-int/lit-8        v1, v4, 1    ; v1 = v4 + 1
15    aput                v0, v3, v1    ; v3[v1] = v0
16
17    return-void
18 .end method
```

```
1 private void swap( int array[], int i )
2 {
3     int temp = array[i];
4
5
6
7 }
```

INTRODUCTION TO SMALI

Smali → Java

```
1 .method private swap([II)V
2 .limit registers 5
3
4 ; this: v2 (Ltest10;)
5 ; parameter[0] : v3 ([I
6 ; parameter[1] : v4 (I)
7
8     aget                v0, v3, v4    ; v0 = v3[v4]
9
10    add-int/lit-8        v1, v4, 1    ; v1 = v4 + 1
11    aget                v1, v3, v1    ; v1 = v3[v1]
12    aput                v1, v3, v4    ; v3[v4] = v1
13
14    add-int/lit-8        v1, v4, 1    ; v1 = v4 + 1
15    aput                v0, v3, v1    ; v3[v1] = v0
16
17    return-void
18 .end method
```

```
1 private void swap( int array[], int i )
2 {
3     int temp = array[i];
4     array[i] = array[i+1];
5     array[i+1] = temp;
6 }
7 }
```

INTRODUCTION TO SMALI

Smali → Java

```
1 .method private swap([II)V
2 .limit registers 5
3
4 ; this: v2 (Ltest10;)
5 ; parameter[0] : v3 ([I
6 ; parameter[1] : v4 (I)
7
8     aget                v0, v3, v4    ; v0 = v3[v4]
9
10    add-int/lit-8       v1, v4, 1      ; v1 = v4 + 1
11    aget                v1, v3, v1      ; v1 = v3[v1]
12    aput                v1, v3, v4      ; v3[v4] = v1
13
14    add-int/lit-8       v1, v4, 1      ; v1 = v4 + 1
15    aput                v0, v3, v1      ; v3[v1] = v0
16
17    return-void
18 .end method
```

```
1 private void swap( int array[], int i )
2 {
3     int temp = array[i];
4     array[i] = array[i+1];
5     array[i+1] = temp;
6 }
7 }
```

INTRODUCTION TO SMALI

Smali → Java

```
1 .method private swap([II)V
2 .limit registers 5
3
4 ; this: v2 (Ltest10;)
5 ; parameter[0] : v3 ([I
6 ; parameter[1] : v4 (I)
7
8     aget                v0, v3, v4    ; v0 = v3[v4]
9
10    add-int/lit-8        v1, v4, 1    ; v1 = v4 + 1
11    aget                 v1, v3, v1    ; v1 = v3[v1]
12    aput                 v1, v3, v4    ; v3[v4] = v1
13
14    add-int/lit-8        v1, v4, 1    ; v1 = v4 + 1
15    aput                 v0, v3, v1    ; v3[v1] = v0
16
17    return-void
18 .end method
```

```
1 private void swap( int array[], int i )
2 {
3     int temp = array[i];
4
5     array[i] = array[i+1];
6     array[i+1] = temp;
7 }
```

INTRODUCTION TO SMALI

Smali → Java

```
1 .method private swap([II)V
2 .limit registers 5
3
4 ; this: v2 (Ltest10;)
5 ; parameter[0] : v3 ([I
6 ; parameter[1] : v4 (I
7
8     aget                v0, v3, v4    ; v0 = v3[v4]
9
10    add-int/lit-8       v1, v4, 1      ; v1 = v4 + 1
11    aget                v1, v3, v1     ; v1 = v3[v1]
12    aput                v1, v3, v4     ; v3[v4] = v1
13
14    add-int/lit-8       v1, v4, 1      ; v1 = v4 + 1
15    aput                v0, v3, v1     ; v3[v1] = v0
16
17    return-void
18 .end method
```

```
1 private void swap( int array[], int i )
2 {
3     int temp = array[i];
4
5     array[i] = array[i+1];
6     array[i+1] = temp;
7 }
```

DYNAMIC ANALYSIS

Binary Instrumentation

Frida

Introduction

- Inject Javascript to explore native applications
- Compatible with many OS
 - Windows, MacOS, Linux, iOS, Android and QNX.
- Extremely useful for...
 - ... custom debugger.
 - ... hook any function.
 - ... spy on Crypt API.
 - ... trace application code.
- No source-code needed.

Frida

Installation Instructions (client)

```
{11:29} [maycon@darkstar ~]
$> virtualenv FridaLast
New python executable in /home/maycon/FridaLast/bin/python2
Not overwriting existing python script /home/maycon/FridaLast/bin/python (you m
Installing setuptools, pip, wheel...done.
{11:30} [maycon@darkstar ~]
$> source FridaLast/bin/activate
(FridaLast) {11:30} [maycon@darkstar ~]
$> pip install frida
Collecting frida
Requirement already satisfied: pygments>=2.0.2 in ./FridaLast/lib/python2.7/sit
Requirement already satisfied: prompt-toolkit>=0.57 in ./FridaLast/lib/python2.
Requirement already satisfied: colorama>=0.2.7 in ./FridaLast/lib/python2.7/sit
Requirement already satisfied: wcwidth in ./FridaLast/lib/python2.7/site-packag
Requirement already satisfied: six>=1.9.0 in ./FridaLast/lib/python2.7/site-pac
Installing collected packages: frida
Successfully installed frida-9.1.22
(FridaLast) {11:30} [maycon@darkstar ~]
$> □
```

Frida

Installation Instructions (client)

```
{11:29} [maycon@darkstar ~]
$> virtualenv FridaLast
New python executable in /home/maycon/FridaLast/bin/python2
Not overwriting existing python script /home/maycon/FridaLast/bin/python (you m
Installing setuptools, pip, wheel...done.
{11:30} [maycon@darkstar ~]
$> source FridaLast/bin/activate
(FridaLast) {11:30} [maycon@darkstar ~]
$> pip install frida
Collecting frida
Requirement already satisfied: pygments>=2.0.2 in ./FridaLast/lib/python2.7/sit
Requirement already satisfied: prompt-toolkit>=0.57 in ./FridaLast/lib/python2.
Requirement already satisfied: colorama>=0.2.7 in ./FridaLast/lib/python2.7/sit
Requirement already satisfied: wcwidth in ./FridaLast/lib/python2.7/site-packag
Requirement already satisfied: six>=1.9.0 in ./FridaLast/lib/python2.7/site-pac
Installing collected packages: frida
Successfully installed frida-9.1.22
(FridaLast) {11:30} [maycon@darkstar ~]
$> 
```

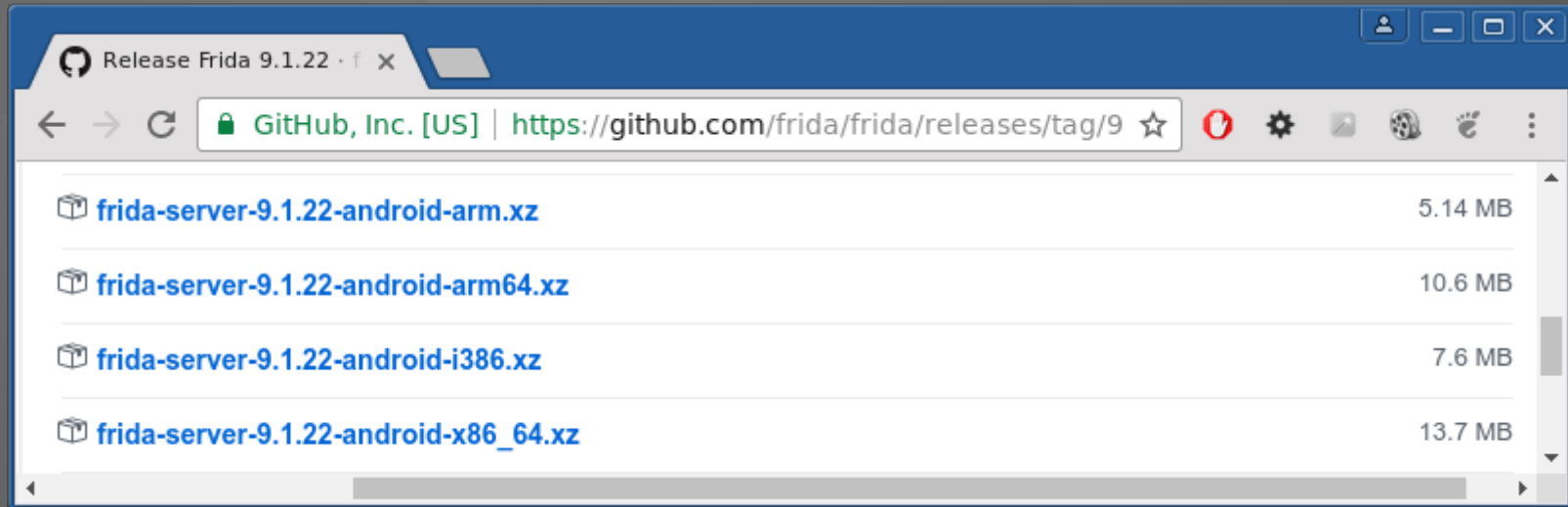
Frida

Installation Instructions (client)

```
{11:29} [maycon@darkstar ~]
$> virtualenv FridaLast
New python executable in /home/maycon/FridaLast/bin/python2
Not overwriting existing python script /home/maycon/FridaLast/bin/python (you m
Installing setuptools, pip, wheel...done.
{11:30} [maycon@darkstar ~]
$> source FridaLast/bin/activate
(FridaLast) {11:30} [maycon@darkstar ~]
$> pip install frida
Collecting frida
Requirement already satisfied: pygments>=2.0.2 in ./FridaLast/lib/python2.7/sit
Requirement already satisfied: prompt-toolkit>=0.57 in ./FridaLast/lib/python2.
Requirement already satisfied: colorama>=0.2.7 in ./FridaLast/lib/python2.7/sit
Requirement already satisfied: wcwidth in ./FridaLast/lib/python2.7/site-packag
Requirement already satisfied: six>=1.9.0 in ./FridaLast/lib/python2.7/site-pac
Installing collected packages: frida
Successfully installed frida-9.1.22
(FridaLast) {11:30} [maycon@darkstar ~]
$> 
```

Frida

Instalation Instructions (server)



Frida
frida-ps

```
{11:43} [maycon@darkstar ~]  
$> adb shell su -c '/data/local/tmp/frida-server-9.1.22-android-arm'
```

maycon@darkstar:~ 119x46

```
(FridaLast) {11:44} [maycon@darkstar ~]
```

```
$> frida-ps -U 2>&1 | head -n 10
```

PID	Name
1444	adbd
4155	android.process.acore
1962	android.process.media
1419	audiotd
1434	bkmgrd
2492	com.android.calendar
2476	com.android.deskclock
2745	com.android.email

```
(FridaLast) {11:44} [maycon@darkstar ~]
```

\$V

Frida

frida-trace

```
(FridaLast) {11:49} [maycon@darkstar ~]  
$> frida-trace -U -i open com.android.browser  
Instrumenting functions...  
open: Auto-generated handler at '/home/maycon/_handlers_/libc.so/open.js'  
Started tracing 1 function. Press Ctrl+C to stop.  
/* TID 0x3bc7 */  
10463 ms open(pathname=0x400be7b2, flags=0x2)  
/* TID 0x3ba4 */  
10475 ms open(pathname=0x6087a658, flags=0x2)  
10476 ms open(pathname=0x6087a658, flags=0x2)  
10478 ms open(pathname=0x6087a658, flags=0x2)  
/* TID 0x3b9a */  
10516 ms open(pathname=0x400be7b2, flags=0x2)  
/* TID 0x3b8d */  
10635 ms open(pathname=0x400be7b2, flags=0x2)  
/* TID 0x3ba7 */  
10728 ms open(pathname=0x400be7b2, flags=0x2)  
10761 ms open(pathname=0x400be7b2, flags=0x2)  
10789 ms open(pathname=0x400be7b2, flags=0x2)
```

Frida

frida-trace (scripting)

./__handlers__/_libc.so/open.js

```
1 {
2   onEnter: function (log, args, state) {
3     log("open(" + "pathname=" + args[0] + ", flags=" + args[1] + ")");
4   },
5
6   onLeave: function (log, retval, state) {
7   }
8 }
```

```
10463 ms open(pathname=0x400be7b2, flags=0x2)
        /* TID 0x3ba4 */
10475 ms open(pathname=0x6087a658, flags=0x2)
10476 ms open(pathname=0x6087a658, flags=0x2)
10478 ms open(pathname=0x6087a658, flags=0x2)
        /* TID 0x3b9a */
10516 ms open(pathname=0x400be7b2, flags=0x2)
        /* TID 0x3b8d */
10635 ms open(pathname=0x400be7b2, flags=0x2)
        /* TID 0x3ba7 */
```

Frida

frida-trace (scripting)

./__handlers__/libc.so/open.js

```
1 {  
2   onEnter: function (log, args, state) {  
3     pathname = Memory.readCString(args[0]);  
4     log("open(" + "pathname=" + pathname + ", flags=" + args[1] + ")");  
5   },  
6  
7   onLeave: function (log, retval, state) {  
8   }  
9 }
```


Frida

frida-trace (scripting)

./__handlers__/libc.so/open.js

```
1 {  
2   onEnter: function (log, args, state) {  
3     pathname = Memory.readCString(args[0]);  
4     log("open(" + "pathname=" + pathname + ", flags=" + args[1] + ")");  
5   },  
6  
7   onLeave: function (log, retval, state) {  
8   }  
9 }
```

Frida

frida-trace (scripting)

./__handlers__/libc.so/open.js

```
1 {
2   onEnter: function (log, args, state) {
3     pathname = Memory.readCString(args[0]);
4     log("open(" + "pathname=" + pathname + ", flags=" + args[1] + ")");
5   },
6
7   onLeave: function (log, retval, state) {
8   }
9 }
```

```
/* TID 0x3ba4 */
2600 ms open(pathname=/data/data/com.android.browser/app_webview/Cache/e146954c45
2602 ms open(pathname=/data/data/com.android.browser/app_webview/Cache/e146954c45
2603 ms open(pathname=/data/data/com.android.browser/app_webview/Cache/e146954c45
/* TID 0x3b9a */
2625 ms open(pathname=/dev/ashmem, flags=0x2)
/* TID 0x3ba7 */
2770 ms open(pathname=/dev/ashmem, flags=0x2)
2787 ms open(pathname=/dev/ashmem, flags=0x2)
```

Frida

Hooking

```
1 import frida
2 import sys
3
4 package_name = "com.app.name"
5
6 def get_messages(message, data):
7     print message
8
9 def instrument_root_checks():
10
11     hook_code = """
12         Dalvik.perform(function () {
13             var MainActivity = Dalvik.use("com.app.name.MainActivity");
14
15             MainActivity.isPhoneRooted.implementation = function () {
16                 send("Called - isPhoneRooted()");
17                 return false;
18             };
19         });
20     """
21
22     return hook_code
23
24 device = frida.get_device_manager().enumerate_devices()[-1]
25 process.attach(package_name)
26
27 script = process.create_script(instrument_root_checks())
28 script.on('message', get_messages)
29 script.load()
30
31 sys.stdin.read()
```

Frida

Hooking

```
1 import frida
2 import sys
3
4 package_name = "com.app.name"
5
6 def get_messages(message, data):
7     print message
8
9 def instrument_root_checks():
10
11     hook_code = """
12         Dalvik.perform(function () {
13             var MainActivity = Dalvik.use("com.app.name.MainActivity");
14
15             MainActivity.isPhoneRooted.implementation = function () {
16                 send("Called - isPhoneRooted()");
17                 return false;
18             };
19         });
20     """
21
22     return hook_code
23
24 device = frida.get_device_manager().enumerate_devices()[-1]
25 process.attach(package_name)
26
27 script = process.create_script(instrument_root_checks())
28 script.on('message', get_messages)
29 script.load()
30
31 sys.stdin.read()
```

Frida

Hooking

```
1 import frida
2 import sys
3
4 package_name = "com.app.name"
5
6 def get_messages(message, data):
7     print message
8
9 def instrument_root_checks():
10
11     hook_code = """
12         Dalvik.perform(function () {
13             var MainActivity = Dalvik.use("com.app.name.MainActivity");
14
15             MainActivity.isPhoneRooted.implementation = function () {
16                 send("Called - isPhoneRooted()");
17                 return false;
18             };
19         });
20     """
21
22     return hook_code
23
24 device = frida.get_device_manager().enumerate_devices()[-1]
25 process.attach(package_name)
26
27 script = process.create_script(instrument_root_checks())
28 script.on('message', get_messages)
29 script.load()
30
31 sys.stdin.read()
```

Frida

Hooking

```
1 import frida
2 import sys
3
4 package_name = "com.app.name"
5
6 def get_messages(message, data):
7     print message
8
9 def instrument_root_checks():
10
11     hook_code = """
12         Dalvik.perform(function () {
13             var MainActivity = Dalvik.use("com.app.name.MainActivity");
14
15             MainActivity.isPhoneRooted.implementation = function () {
16                 send("Called - isPhoneRooted()");
17                 return false;
18             };
19         });
20     """
21
22     return hook_code
23
24 device = frida.get_device_manager().enumerate_devices()[-1]
25 process.attach(package_name)
26
27 script = process.create_script(instrument_root_checks())
28 script.on('message', get_messages)
29 script.load()
30
31 sys.stdin.read()
```

Frida

Hooking

```
1 import frida
2 import sys
3
4 package_name = "com.app.name"
5
6 def get_message(message, data):
7     print message
8
9 def instrument_root_checks():
10
11     hook_code = """
12         Dalvik.perform(function () {
13             var MainActivity = Dalvik.use("com.app.name.MainActivity");
14
15             MainActivity.isPhoneRooted.implementation = function () {
16                 send("Called - isPhoneRooted()");
17                 return false;
18             };
19         });
20     """
21
22     return hook_code
23
24 device = frida.get_device_manager().enumerate_devices()[-1]
25 process.attach(package_name)
26
27 script = process.create_script(instrument_root_checks())
28 script.on('message', get_message)
29 script.load()
30
31 sys.stdin.read()
```

Frida Hooking

```
1 import frida
2 import sys
3
4 package_name = "com.app.name"
5
6 def get_messages(message, data):
7     print message
8
9 def instrument_root_checks():
10
11     hook_code = """
12         Dalvik.perform(function () {
13             var MainActivity = Dalvik.use("com.app.name.MainActivity");
14
15             MainActivity.isPhoneRooted.implementation = function () {
16                 send("Called - isPhoneRooted()");
17                 return false;
18             };
19         });
20     """
21
22     return hook_code
23
24 device = frida.get_device_manager().enumerate_devices()[-1]
25 process.attach(package_name)
26
27 script = process.create_script(instrument_root_checks())
28 script.on('message', get_messages)
29 script.load()
30
31 sys.stdin.read()
```


Frida Hooking

```
1 import frida
2 import sys
3
4 package_name = "com.app.name"
5
6 def get_messages(message, data):
7     print message
8
9 def instrument_root_checks():
10
11     hook_code = """
12         Dalvik.perform(function () {
13             var MainActivity = Dalvik.use("com.app.name.MainActivity");
14
15             MainActivity.isPhoneRooted.implementation = function () {
16                 send("Called - isPhoneRooted()");
17                 return false;
18             };
19         });
20     """
21
22     return hook_code
23
24 device = frida.get_device_manager().enumerate_devices()[-1]
25 process.attach(package_name)
26
27 script = process.create_script(instrument_root_checks())
28 script.on('message', get_messages)
29 script.load()
30
31 sys.stdin.read()
```

DEMO

DC5527

DC5527

DC5527.ORG

DEF CON GROUP

THANK YOU!

Maycon Maia Vitali
maycon@hacknroll.com