

RSACONFERENCE2014

FEBRUARY 24 - 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

Beginners Guide to Reverse Engineering Android Apps

SESSION ID: STU-W02B

Pau Oliva Fora

Sr. Mobile Security Engineer
viaForensics
@pof



Agenda

- ◆ Anatomy of an Android app
- ◆ Obtaining our target apps
- ◆ Getting our hands dirty: reversing the target application
- ◆ Demo using Santoku Linux

RSACONFERENCE2014

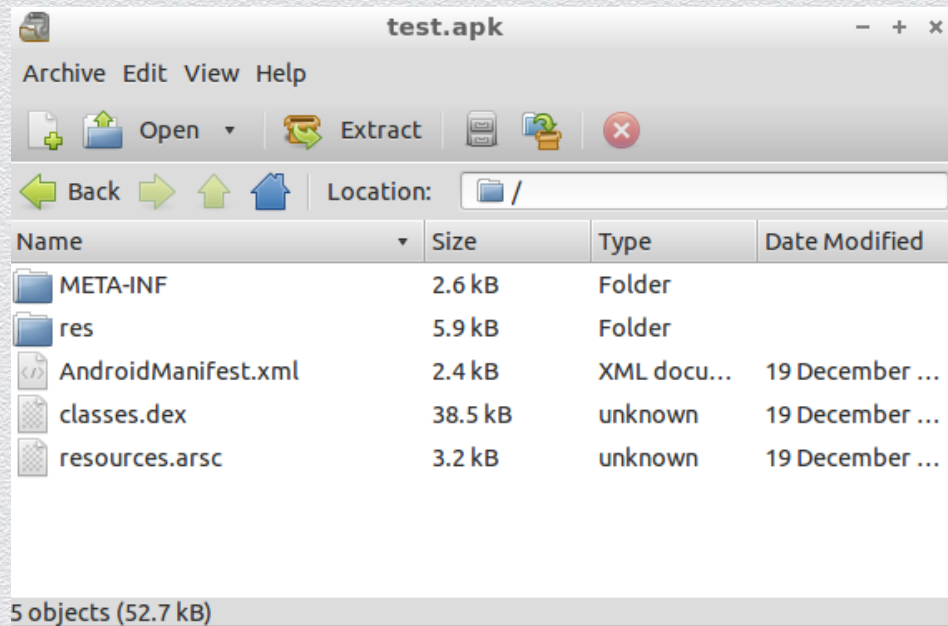
FEBRUARY 24 - 28 | MOSCONE CENTER | SAN FRANCISCO



Anatomy of an Android app


Anatomy of an Android app

- ◆ Simple ZIP file, renamed to “APK” extension
- ◆ App resources
- ◆ Signature
- ◆ Manifest (binary XML)



RSA[®]CONFERENCE2014

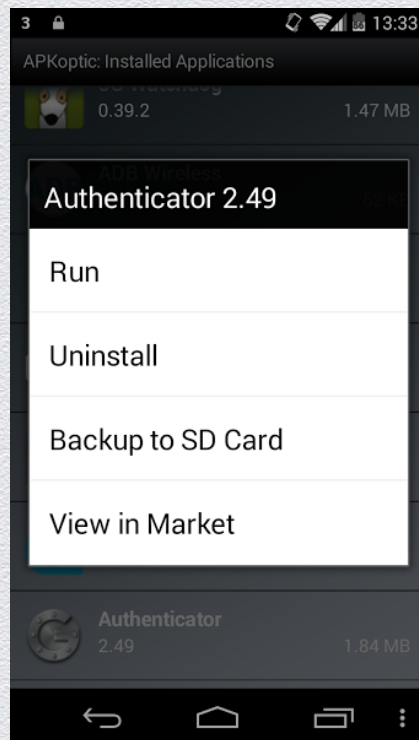
FEBRUARY 24 - 28 | MOSCONE CENTER | SAN FRANCISCO



**Obtaining our target
apps**

Getting the APK from the phone

- ◆ Backup to SD Card:
 - ◆ APKOptic
 - ◆ Astro file manager
 - ◆ etc...



Getting the APK from the phone

- ◆ Using ADB (Android Debug Bridge):
 - ◆ adb shell pm list packages
 - ◆ adb pull /data/app/package-name-1.apk

```
santoku@santoku-VirtualBox:~$ adb shell pm list packages |grep -v "(google|android)"
package:com.tf.thinkdroid.sg
package:es.vodafone.mobile.mivodafone
package:com.anydo
package:org.eslack.rootadb
package:com.saurik.substrate
package:com.viaforensics.cydiadynamicanalyzer
package:com.simyo
package:eu.chainfire.supersu
santoku@santoku-VirtualBox:~$ adb pull /data/app/com.simyo-1.apk
626 KB/s (1620854 bytes in 2.527s)
santoku@santoku-VirtualBox:~$
```


Downloading the APK from Google Play

- ◆ Using unofficial Google Play API:
 - ◆ <https://github.com/egirault/googleplay-api>
- ◆ Using a web service or browser extension:
 - ◆ <http://apps.evozi.com/apk-downloader/>
 - ◆ <http://apify.ifc0nfig.com/static/clients/apk-downloader/>




APK
downloader

Downloading the APK from Google Play

- ◆ Using [http://apkdownloader.com](#)
- ◆ Using [http://apkdownloader.com](#)
- ◆ Using [http://apkdownloader.com](#)

Package name or Google Play URL

Please make sure package name or URL is valid



In this example : **com.evozi.deviceid** is the package name

Generate Download Link

Advanced Setting ▾

APK
downloader

RSA[®]CONFERENCE2014

FEBRUARY 24 - 28 | MOSCONE CENTER | SAN FRANCISCO



**Getting our hands
dirty: reversing the
target application**

Disassembling



DEX



Smali

Apktool

- ◆ apktool - <https://code.google.com/p/android-apktool/>
 - ◆ Multi platform, Apache 2.0 license
 - ◆ Decode resources to original form (and rebuild after modification)
 - ◆ Transforms binary Dalvik bytecode (classes.dex) into Smali source

```
santoku@santoku-VirtualBox:/tmp/apk$ apktool d test.apk
I: Baksmaling...
I: Loading resource table...
I: Loaded.
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /home/santoku/apktool/framework/1.apk
I: Loaded.
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Done.
I: Copying assets and libs...
santoku@santoku-VirtualBox:/tmp/apk$ ls -l test/
total 16
-rw-rw-r-- 1 santoku santoku 1156 Jan  3 16:05 AndroidManifest.xml
-rw-rw-r-- 1 santoku santoku  262 Jan  3 16:05 apktool.yml
drwxrwxr-x 5 santoku santoku 4096 Jan  3 16:05 res
drwxrwxr-x 3 santoku santoku 4096 Jan  3 16:05 smali
santoku@santoku-VirtualBox:/tmp/apk$
```


Smali

```
santoku@santoku-VirtualBox: /tm.../smali/com/viaforensics/android - + x
File Edit Tabs Help
prologue
.line 55
invoke-virtual {p0}, Ljava/lang/Object; ->getClass()Ljava/lang/Class;

move-result-object v0

invoke-virtual {v0}, Ljava/lang/Class; ->getName()Ljava/lang/String;

move-result-object v0

const-string v1, "Error message: "

invoke-static {v0, v1, p1}, Landroid/util/Log; ->e(Ljava/lang/String;Ljava/lang/String;Ljava/lang/Throwable;)I

.line 56
invoke-virtual {p1}, Ljava/lang/Exception; ->getMessage()Ljava/lang/String;

move-result-object v0

invoke-virtual {p0, v0}, Lcom/viaforensics/android/ExtractAllData; ->showErrorOccurredToast(Ljava/lang/String;)V

25,5 22%
```


Decompiling – Java Decompiler



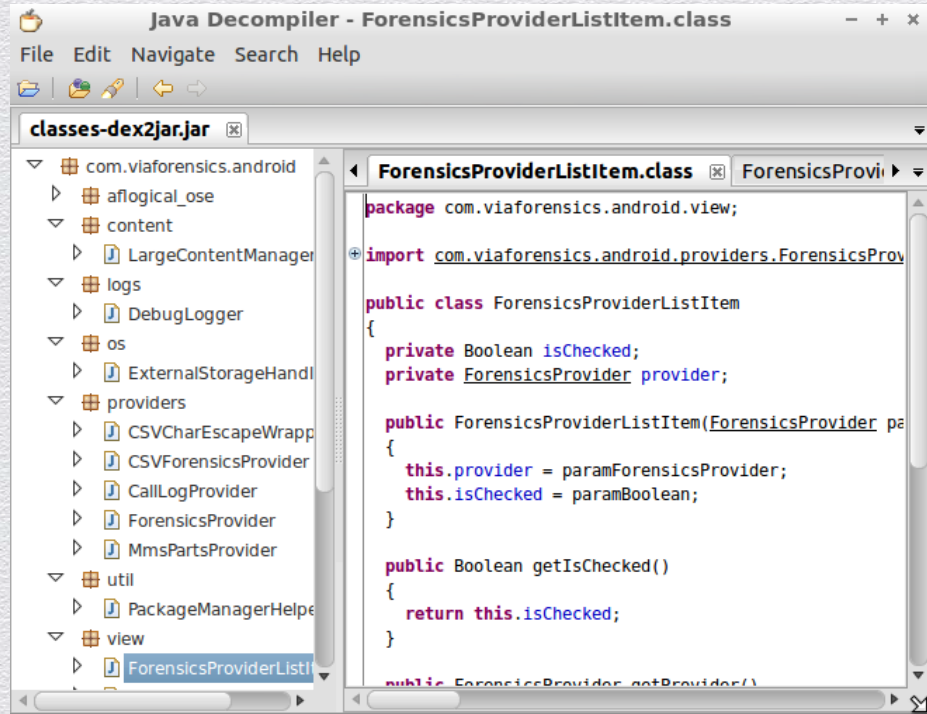
Dex2Jar

- ◆ dex2jar - <https://code.google.com/p/dex2jar/>
 - ◆ Multi platform, Apache 2.0 license
 - ◆ Converts Dalvik bytecode (DEX) to java bytecode (JAR)
 - ◆ Allows to use any existing Java decompiler with the resulting JAR file

```
santoku@santoku-VirtualBox:/tmp/apk$ unzip test.apk classes.dex
Archive:  test.apk
  inflating: classes.dex
santoku@santoku-VirtualBox:/tmp/apk$ d2j-dex2jar classes.dex
dex2jar classes.dex -> classes-dex2jar.jar
santoku@santoku-VirtualBox:/tmp/apk$ ls -l classes*
-rw-rw-r-- 1 santoku santoku 38520 Dec 19  2011 classes.dex
-rw-rw-r-- 1 santoku santoku 31589 Jan  3 16:27 classes-dex2jar.jar
santoku@santoku-VirtualBox:/tmp/apk$
```


Java Decompilers

- ◆ Jd-gui - <http://jd.benow.ca/>
 - ◆ Multi platform
 - ◆ closed source
- ◆ JAD - <http://varanekas.com/jad/>
 - ◆ Multi platform
 - ◆ closed source
 - ◆ Command line
- ◆ Others: Dare, Mocha, Procyon, ...



The screenshot shows the Java Decompiler application window titled "Java Decompiler - ForensicsProviderListItem.class". The interface includes a menu bar (File, Edit, Navigate, Search, Help) and a toolbar. The left pane displays a file tree for "classes-dex2jar.jar" with the following structure:

- com.viaforensics.android
 - aflogical_ose
 - content
 - LargeContentManager
 - logs
 - DebugLogger
 - os
 - ExternalStorageHandl
 - providers
 - CSVCharEscapeWrapp
 - CSVForensicsProvider
 - CallLogProvider
 - ForensicsProvider
 - MmsPartsProvider
 - util
 - PackageManagerHelpe
 - view
 - ForensicsProviderListI

The right pane shows the decompiled Java code for "ForensicsProviderListItem.class":

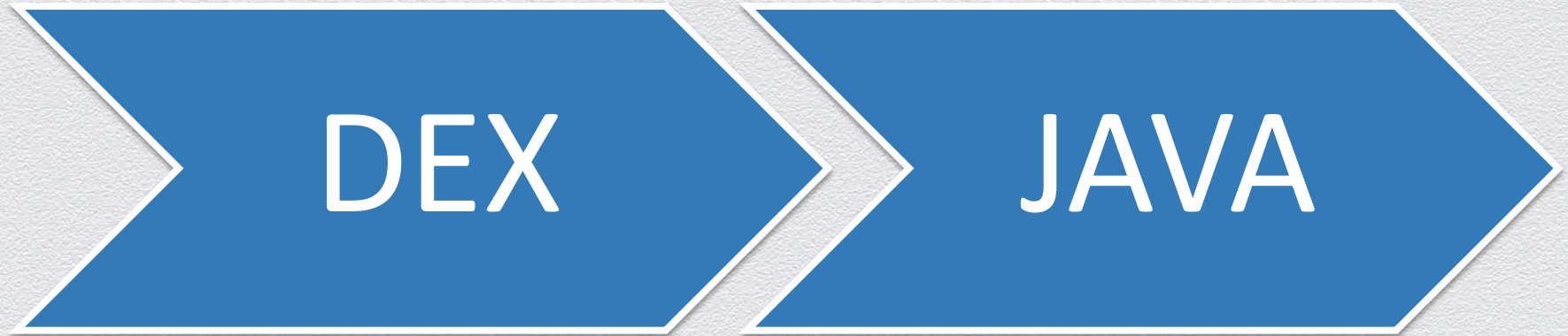
```
package com.viaforensics.android.view;
import com.viaforensics.android.providers.ForensicsProv
public class ForensicsProviderListItem
{
    private Boolean isChecked;
    private ForensicsProvider provider;

    public ForensicsProviderListItem(ForensicsProvider pa
    {
        this.provider = paramForensicsProvider;
        this.isChecked = paramBoolean;
    }

    public Boolean getIsChecked()
    {
        return this.isChecked;
    }

    public ForensicsProvider getProvider()
```


Decompiling – Android (Dalvik) decompiler



Dalvik Decompileers

- ◆ Transforming DEX to JAR loses important metadata that the decompiler could use.
 - ◆ Pure Dalvik decompilers skip this step, so they produce better output
- ◆ Unfortunately there are not as many choices for Android decompilers as for Java decompilers:
 - ◆ Open Source: Androguard's DAD - <https://code.google.com/p/androguard/>
 - ◆ Commercial: JEB - <http://www.android-decompiler.com/>
 - ◆ Others?

RSACONFERENCE2014

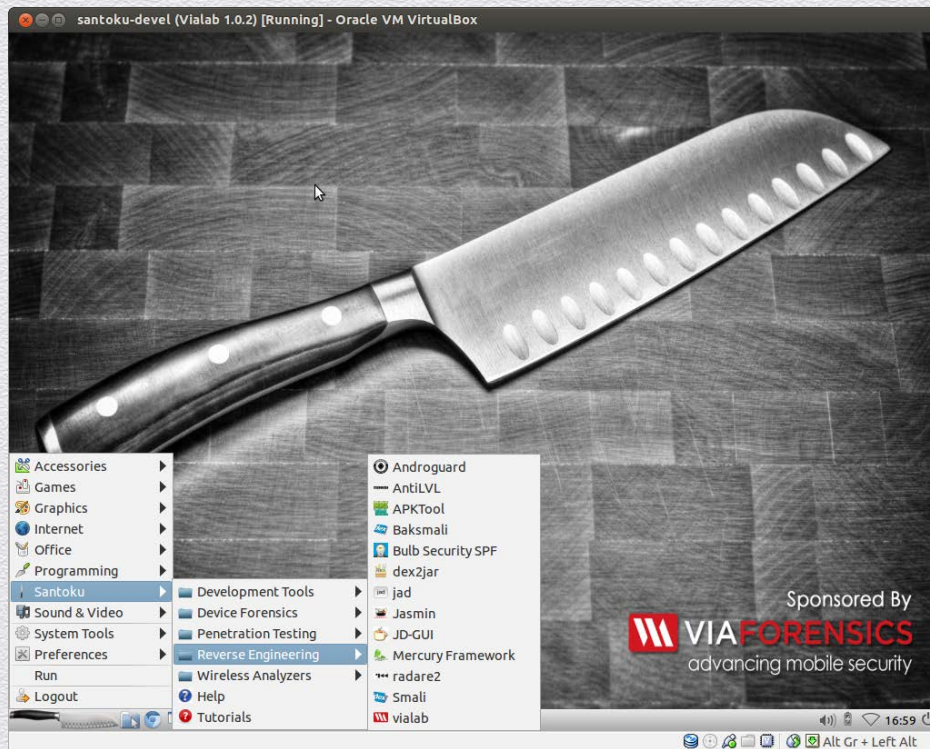
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



Demo – Santoku

Demo – Santoku Linux

- ◆ Santoku Linux - <https://santoku-linux.com/>
- ◆ Mobile Forensics
- ◆ Mobile Malware analysis
- ◆ Mobile application assessment



Summary

- ◆ APK files are ZIP files, can be extracted with any unzip utility
- ◆ Apktool helps extracting binary resources, and allows repacking
- ◆ Dex2jar converts Dalvik Bytecode to Java Bytecode
- ◆ Pure Android decompilers are better
- ◆ Santoku Linux has all the tools you need to reverse engineering mobile apps

Q&A | Contact | Feedback

◆ Thanks for listening...

 @pof

 github.com/poliva

 poliva@viaforensics.com

