Android Security & Exploitation

Aditya Gupta (@adi1391)

Founder, Attify (http://attify.com)

adi@attify.com

Certifications : http://securitytube-training.com
Pentester Academy : http://PentesterAcademy.com

Reversing Android apps

Application Reversing

Baksmali

- Smali Decompiler
- Converts dex to smali
- java -jar baksmali.jar classes.dex
- https://code.google.com/p/smali/ downloads/list

Smali

- Another tool to convert back .smali files to original form
- Everything wrapped in APKTool
- Simple Exercise

Hands-on with Smali

- Syntax is loosely based on Jasmin's/Dedexer's syntax
- Less overhead and easier to {de|re} compile dex files
- "Hello World" in smali

Smali

- Smali representation of

  Object blah = null;
  blah.toString();

- Becomes

  const v0,0 //initialize the first local register to null or 0
  invoke-virtual{v0}, Ljava/lang/Object ;-> toString()

Smali

- There are two naming schemes for registers - the normal v naming scheme and the p naming scheme for parameter registers

- v0 - the first local register
- v1 - the second local register
- v2 or p0 - the first parameter register
- v3 or p1 - the second parameter register

APKTool

- Wrapper around smali and baksmali
- apktool d appname.apk
- apktool b foldername/ appname.apk

APKTool

- C0C0N CTF

- Find out the secret key

Other way of Reversing

- Two Approaches
  - Apktool (Smali and baksmali)
  - JD-GUI + Dex2Jar
- Other decompilers : JADx, JEB etc.

Dex2Jar + JD-GUI

- ./d2j-dex2jar.sh appname.apk

- Open the .jar file in JD-GUI

Early Android Licensing code

LicenseValidator.smalli constants

```
.field private static final ERROR_CONTACTING_SERVER:I = 0x101
.field private static final ERROR_INVALID_PACKAGE_NAME:I = 0x102
.field private static final ERROR_NON_MATCHING_UID:I = 0x103
.field private static final ERROR_NOT_MARKET_MANAGED:I = 0x3
.field private static final ERROR_OVER_QUOTA:I = 0x5
.field private static final ERROR_SERVER_FAILURE:I = 0x4
.field private static final LICENSED:I = 0x0
.field private static final LICENSED_OLD_KEY:I = 0x2
.field private static final NOT_LICENSED:I = 0x1
```

LicenseValidator.smali verify

```
.sparse-switch
0x0 -> :sswitch_d3
0x1 -> :sswitch_de
0x2 -> :sswitch_d3
0x3 -> :sswitch_11d
0x4 -> :sswitch_f3
0x5 -> :sswitch_101
0x101 -> :sswitch_e5
0x102 -> :sswitch_10f
0x103 -> :sswitch_116
.end sparse-switch
```

Source : http://www.androidpolice.com/2010/08/23/exclusive-report-googles-android-market-license-verification-easily-circumvented-will-not-stop-pirates/