Mobile Phone Security

Dr. Digvijaysinh Rathod
Associate Professor
(Cyber Security and Digital Forensics)
National Forensic Sciences University with status of National Imporatance

digvijay.rathod@gfsu.edu.in

Disassembling DEX files / Reverse Engineering

using

HaxDump

Dexdump

Dex2Jar and JD-GUI

Disassembling DEX files

✓Android’s build process compiles Java source code to bytecode (.class file) and later converts it, along with resources, into .dex (Dalvik Executable a.k.a DEX) format to run efficiently on Android devices.

✓**MyCode.java → MyCode.class → MyCode.dex**

✓This allows you to create the Dalvik Virtual Machine bytecode from a dex file.

Disassembling DEX files - Dexdump

✓Dexdump tools is used to perform following task

✓**Dalvik Virtual Machine Code 🡐 Dex file**

✓This allows you to create the Dalvik Virtual Machine bytecode from a dex file.

✓To compile the Dalvik Bytecode to Java source code there are no official tools.

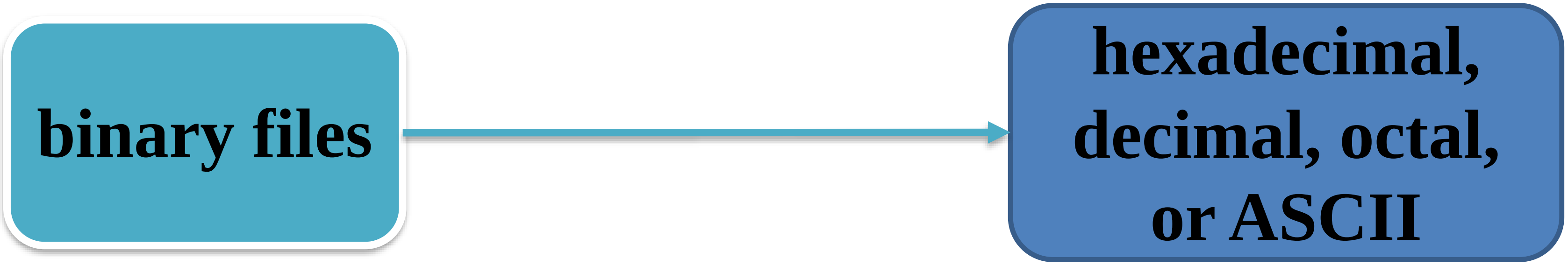
Disassembling DEX files - Dexdump

- ✓Extract classes and methods from an APK file
  - ✓ dexdump [path/to/file.apk]
- ✓Display header information of DEX files contained in an APK file
  - ✓ dexdump -f [path/to/file.apk]
- ✓Display the dis-assembled output of executable sections
  - ✓dexdump -d [path/to/file.apk]
- ✓Output results to a file
  - ✓dexdump -o [path/to/file] [path/to/file.apk]

Hexdump

✓Hexdump helps you investigate the contents of binary files.

✓Hexdump is a utility that displays the contents of binary files in hexadecimal, decimal, octal, or ASCII.



binary files

hexadecimal, decimal, octal, or ASCII

✓It’s a utility for inspection and can be used for data recovery, reverse engineering, and programming.

Hexdump

- ✓Syntax:
  - ✓hd [OPTIONS...] [FILES...]
  - ✓-b : One-byte octal display.
  - ✓-c : One-byte character display
  - ✓-d : Two-byte decimal display
  - ✓n length : Where length is an integer. Interprets only ‘length’ bytes of output.
  - ✓-o: Two-byte octal display.

https://www.geeksforgeeks.org/hexdump-command-in-linux-with-examples/

Dex2Jar

✓Dex2Jar is a freely available tool to work with Android “.dex

✓As you may aware that “.dex” files are compiled Android application code file.

✓Android programs are compiled into “.dex” (Dalvik Executable) files, which are in turn zipped into a single “.apk” file on the device.” and Java “.class” files.

https://resources.infosecinstitute.com/

Dex2Jar

✓The “.dex” files can be created automatically by Android, by translating the compiled applications written in the Java programming language.

✓The core feature of Dex2Jar is to convert the classes.dex file of an APK to classes.jar or vice versa.

✓So, it is possible to view the source code of an Android application using any Java decompiler, and it is completely readable.

https://resources.infosecinstitute.com/

Dex2Jar – Practical

- ✓Here, we get .class files and not the actual Java source code that was written by the application developer.
- ✓it is possible to get “.smali” files directly from the classes.dex file or vice versa.
- ✓That means you can change the source code of an application directly working with this format.

https://resources.infosecinstitute.com/

Dex2Jar

- ✓d2j-dex2jar –h
- ✓d2j-dex2jar –d filename.apk

https://resources.infosecinstitute.com/

JD-GUI

- ✓JD-GUI is a standalone graphical utility that displays Java source codes of “.class” files.

- ✓You can browse the reconstructed source code with the JD-GUI for instant access to methods and fields.

- ✓If you open the “.jar” file with JD-GUI, you can view the source code of the application which is Java classes in a readable format, and it is also very easy to navigate through the code.

- ✓http://java-decompiler.github.io/

- ✓Jd-gui classes_dex2jar.jar

https://resources.infosecinstitute.com/

Mobile Phone Security

Dr. Digvijaysinh Rathod
Associate Professor
(Cyber Security and Digital Forensics)
Institute of Forensic Science
Gujarat Forensic Sciences University

digvijay.rathod@gfsu.edu.in