Android Hook Injection Documentation

e.KRAAL

INNOVATION HUB

TASK :TEST THE CODE

SOURCE :https://github.com/406345/android-inject-hook/

by

(w3slee)wbq6@tutanota.com

July 26, 2021

NOTE :

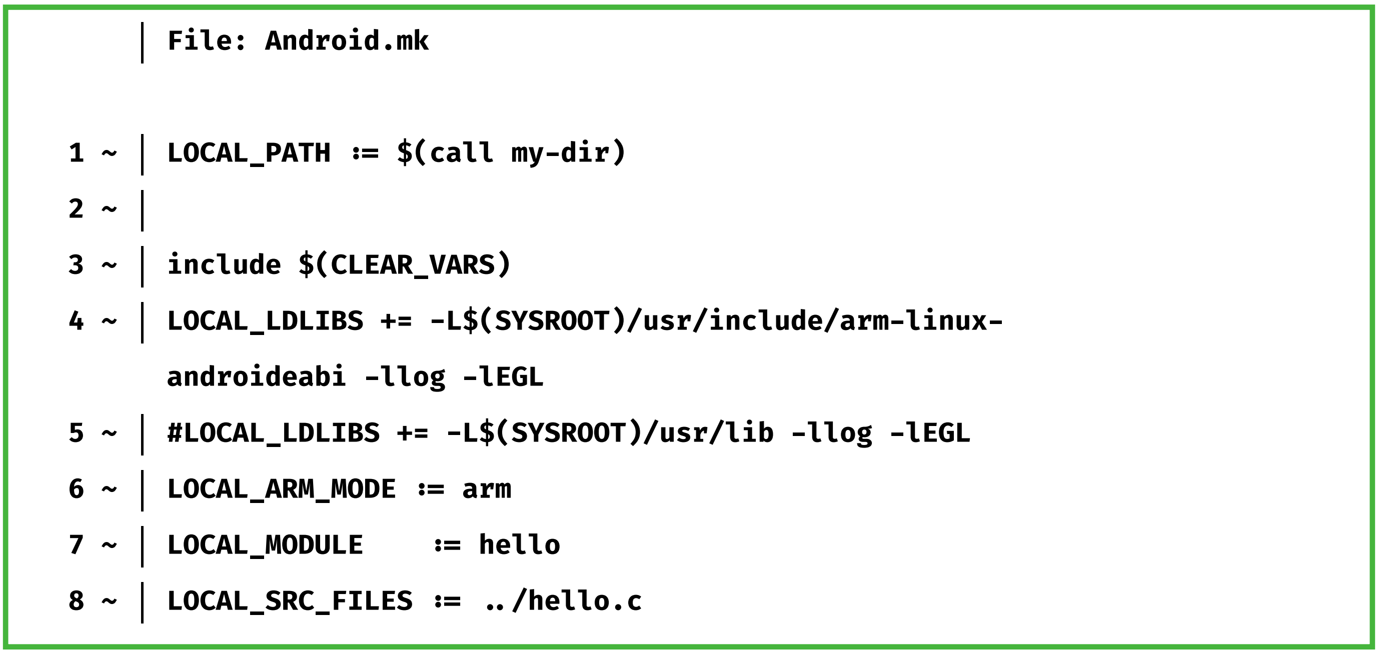
After cloning the project from GitHub, the source code could not be compiled as pulled. Some changes have to be made. The compilation errors I encountered are listed below and some of the step I took to resolve them.

The main objective is to get the code running and test execution on various architectures it was compiled for

BUGS ENCOUNTERED WHILE COMPILING THE PROJECT

```
[armeabi-v7a] Compile thumb  : inject <= inject.c
jni/../inject.c:3:10: fatal error: 'asm/user.h' file not found
#include "asm/user.h"
         ^~~~~~~~~~~~
1 error generated.
make: *** [/opt/android-ndk/build/core/build-binary.mk:476: obj/
local/armeabi-v7a/objs/inject/__/inject.o] Error 1
```

I made changes to the Makefile which made it possible to compile the shared library for the specified arm architecture the source file was compiled for.



```
File: Android.mk

LOCAL_PATH := $(call my-dir)

include $(CLEAR_VARS)
LOCAL_LDLIBS += -L$(SYSROOT)/usr/include/arm-linux-androideabi -llog -lEGL
#LOCAL_LDLIBS += -L$(SYSROOT)/usr/lib -llog -lEGL
LOCAL_ARM_MODE := arm
LOCAL_MODULE    := hello
LOCAL_SRC_FILES := ../hello.c
```

Android Security: Model

- Android Permission and Protection
  + Grant by Package Information (Permission Information)
    - Restrict by Package Location(System or User)
    - Restrict by Package Signature

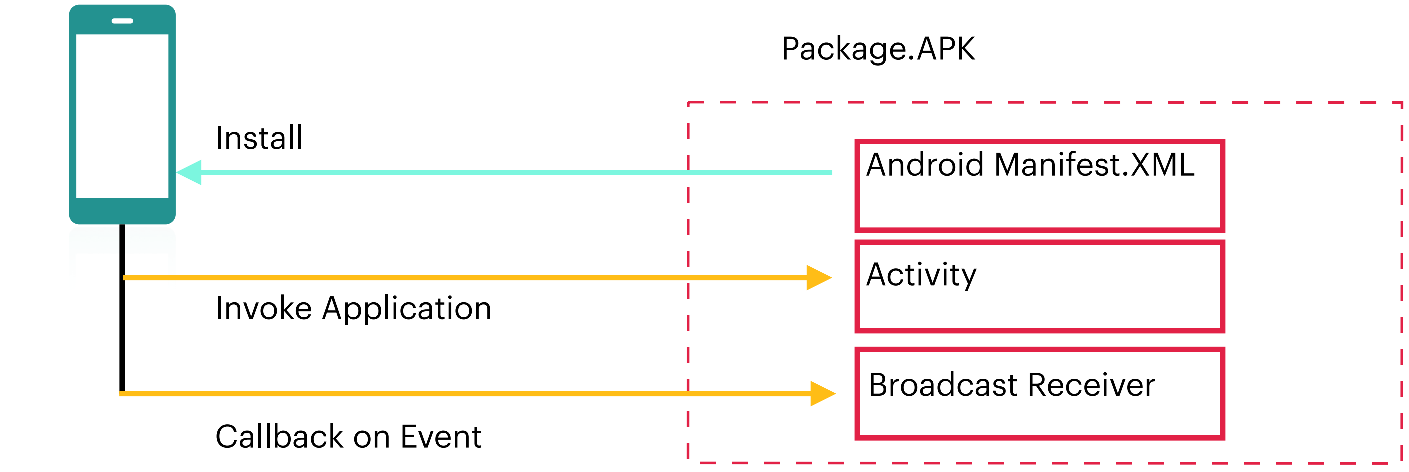
  + Grant by UID/PID (Backdoor?)

- Priorities of Activity (User-Interface Element)

+ Grant by Package Information (Intent Filters)
-Restrict by Package Location (System Only)

- Legacy Linux Security Model
  - Grant/Restrict: UID/GID/PID.

Android System



Android Application Model

Package contents

An APK file is an archive that usually contains the following files and directories:

META-INF directory:

- **MANIFEST.MF:** the Manifest file
- **The certificate of the application.**
- **CERT.SF:** The list of resources and a SHA-1 digest of the corresponding lines in the MANIFEST.MF file;

lib:

the directory containing the compiled code that is platform dependent; the directory is split into more directories within it:

armeabi-v7a:

compiled code for all ARMv7 and above based processors only

arm64-v8a:

compiled code for all ARMv8 arm64 and above based processors only[10]

x86: compiled code for x86 processors only

x86_64: compiled code for x86 64 processors only

~~mips~~ and **~~armeabi~~** are **Deprecated since NDK r17[11][12]**

res:

the directory containing resources that are not compiled into resources.arsc

assets: a directory containing applications assets, which can be retrieved by the **AssetManager**.

AndroidManifest.xml: An additional Android manifest file, describing the name, version, access rights, referenced library files for the application. This file may be in Android binary XML that can be converted into human-readable plaintext XML with tools such as AXMLPrinter2, apktool, or Androguard.

classes.dex: The classes compiled in the dex file format understandable by the Dalvik virtual machine and by the Android Runtime.

resources.arsc: a file containing precompiled resources, such as binary XML for example.