



(照片部分由主办方添加)

ANDROID APP安全从入门到放弃

何勇亮 上海市信息安全测评认证中心



网络安全创新大会
Cyber Security Innovation Summit



高级等保测评师

CISP、CISSP、CISAW、PMP



等级保护测评、渗透测试
网络安全咨询、风险评估

Wechat: unicotech

1

APP安全初探

2

APP安全学习路径

3

一点体会



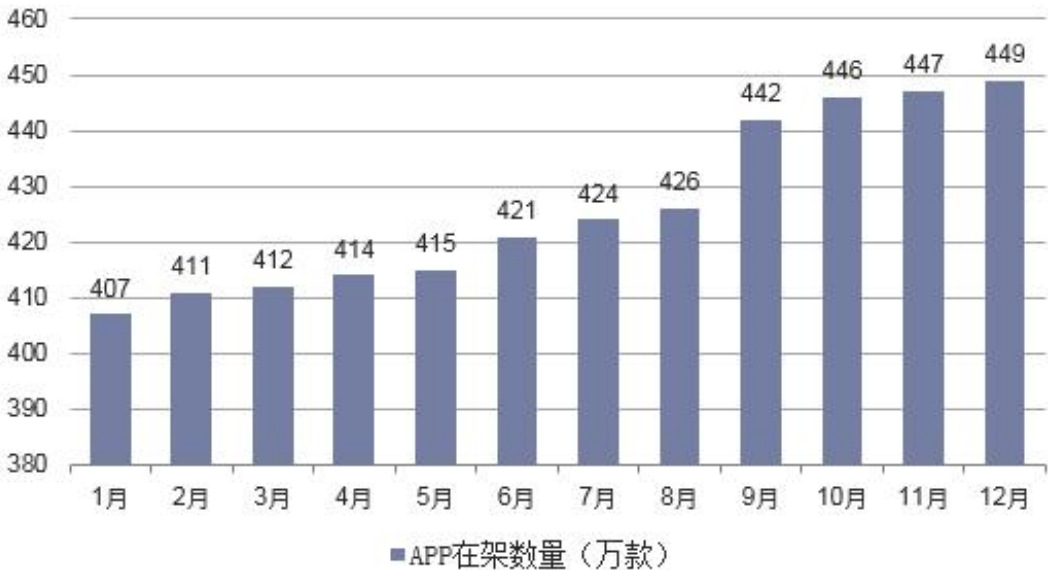
网络安全创新大会
Cyber Security Innovation Summit

Part 1

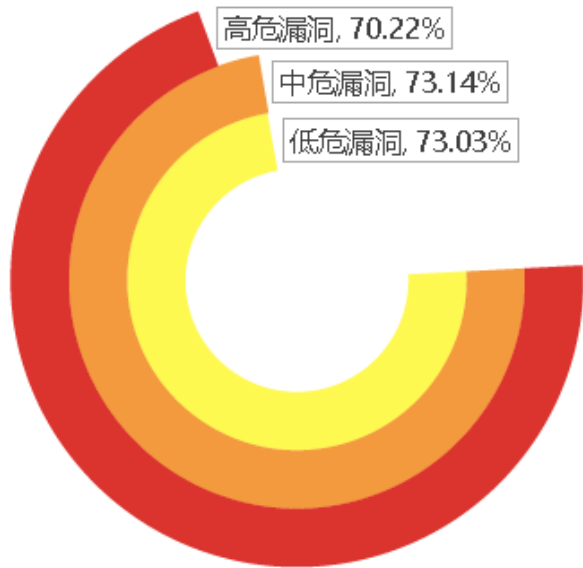
APP安全初探



2018年中国移动应用程序（APP）在架数量



数据来源：工业和信息化部，华经产业研究院



数据来源：2019金融行业移动APP安全观测报告



M1-平台使用
不当

M2-不安全的
数据存储

M3-不安全的
通信

M4-不安全的
身份验证

M5-加密不足

M6-不安全的
授权

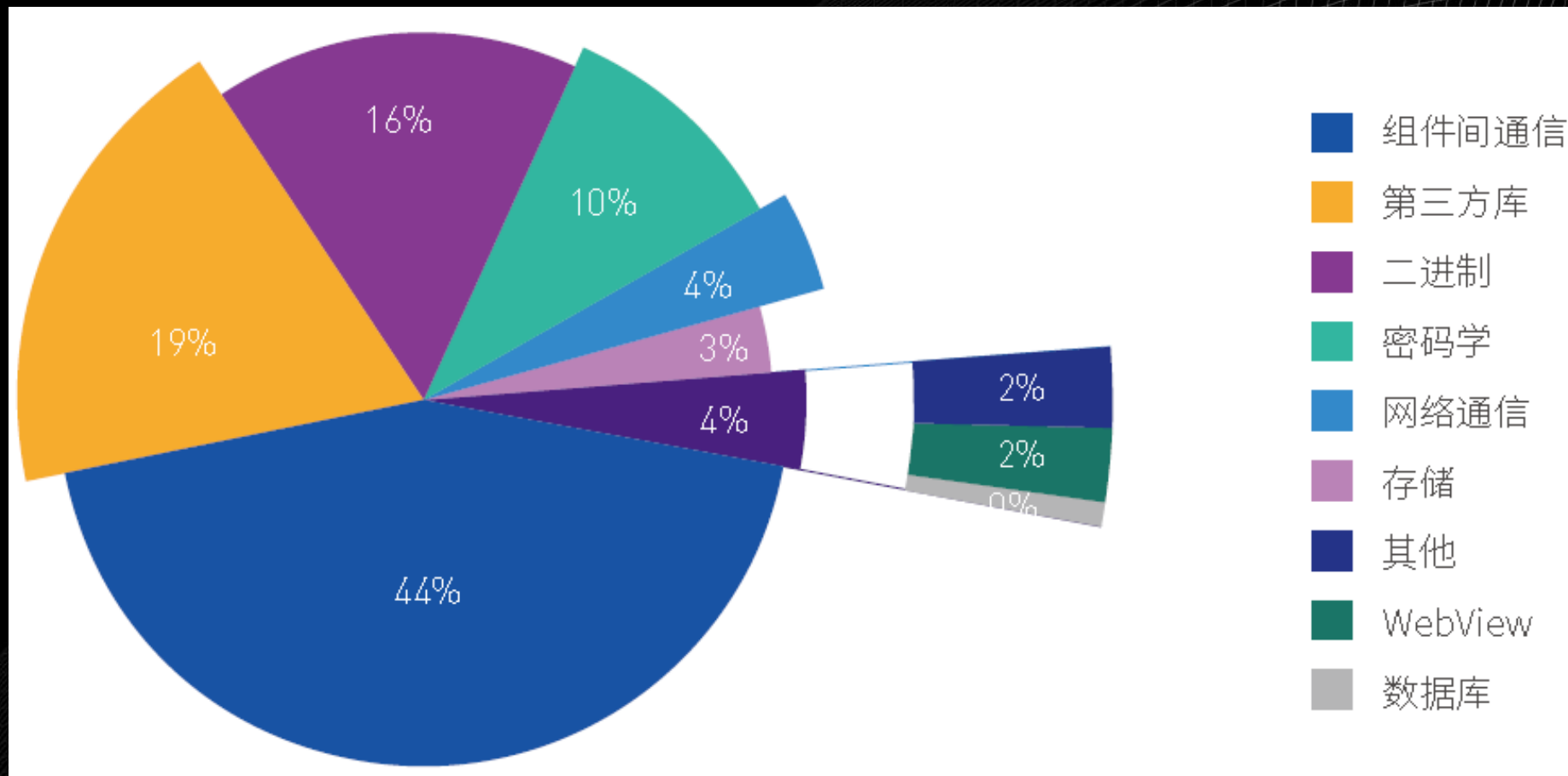
M7-客户端代
码质量问题

M8-代码篡改

M9-逆向工程

M10-无关的
功能

OWASP MOBILE TOP 10 2016



《YD/T 1438-2006 数字移动台应用层软件功能要求和测试方法》

《YD/T 2307-2011 数字移动通信终端通用功能技术要求和测试方法》

《JR/T 0092-2012中国金融移动支付客户端技术规范》

《JR/T 0095-2012中国金融移动支付应用安全规范》

《NIST SP800-163 Vetting the Security of Mobile Applications》

《OWASP移动安全测试指南》



【任职资格】

- 1、熟悉Java/C/C++开发语言，具有android开发经验，熟悉apk加载过程；
- 2、熟悉使用android反编译工具（IDA、ApkTool、Jeb2等）；
- 3、熟悉Smali语言、ARM、ARM指令；
- 4、熟悉IDA、GDB等调试工具的使用；
- 5、熟悉HTTP、TCP等网络协议及数据抓包、分析，熟悉常见公开加密算法；
- 6、熟悉android安全机制以及常见安全漏洞，2年android漏洞挖掘/分析经验；
- 7、熟悉Hook技术，有android应用破解经验，有脱壳经验者优先；
- 8、有一定的英文阅读能力，能熟练阅读英文技术文档、漏洞报告；
- 9、有一定的文档基础，可独立完成安全评估报告和事件分析报告；
- 10、有编写自动化渗透测试工具者优先；
- 11、上报过优质漏洞者优先；
- 12、对软件逆向领域有强烈的爱好。

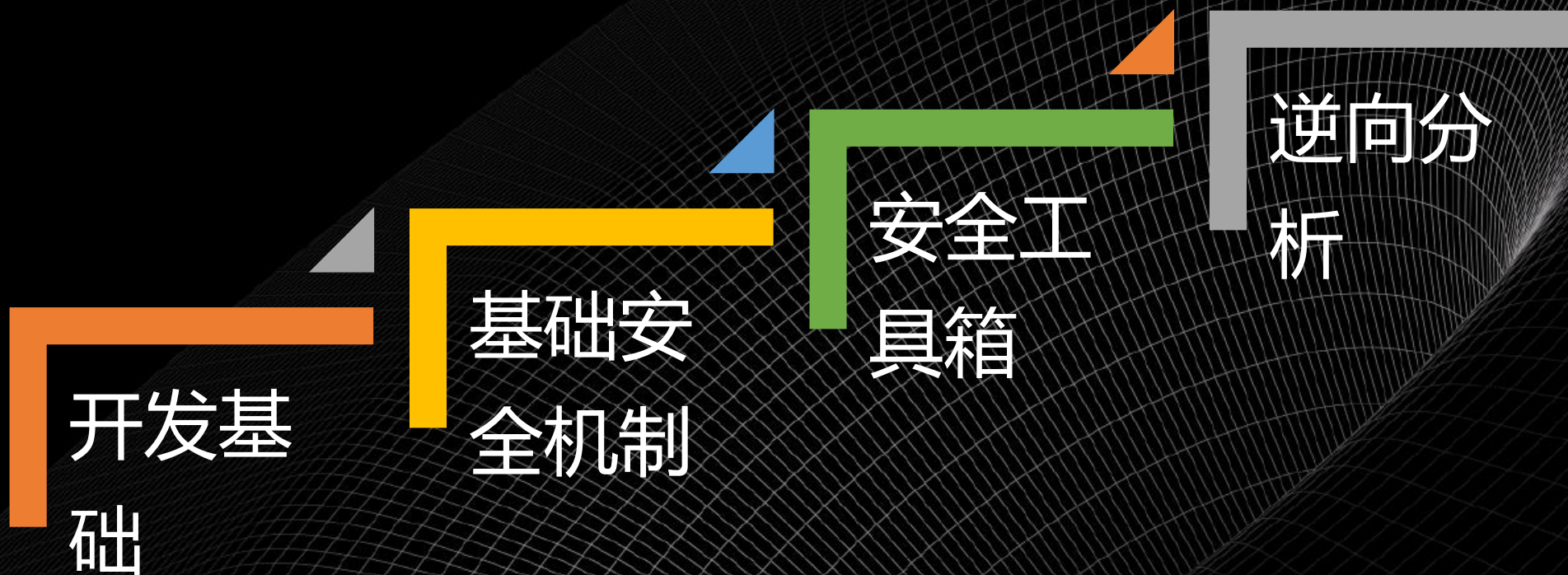
1. 3年以上相关经验；
2. 精通Smali语法、ARM指令，对逆向工程有浓厚兴趣；
3. 熟练掌握各种调试工具：IDA、Smali、Dedexer、Dexdump、Apktool、Dex2jar其中一种或多种；
4. 了解android的root原理，有实际root代码调试经验；
5. 能够使用ida或gdb对apk/elf/so等文件格式进行静态分析、动态调试、代码跟踪等；
6. 熟练Android平台下面的反调试、脱壳、加固等技术；
7. 熟悉Android安全机制，了解打包、反编译、破解流程,对apk静态注入和动态注入代码，掌握Xposed或libinject等hook框架，了解注入、Hook技术原理，能使用Frida、Xposed、Substrate等框架编写Hook代码；
8. 精通网络报文的捕获与分析，熟练使用tcpdump、fiddler、wireshark等各种协议分析工具；
9. 掌握C/C++、Java、python一门或者多门语言，拥有两年及以上Android或IOS研发经验；
10. 熟悉移动端安全机制、了解应用层常见漏洞，掌握基本的审计流程和代码保护方案。



网络安全创新大会
Cyber Security Innovation Summit

Part 2

APP安全学习路径

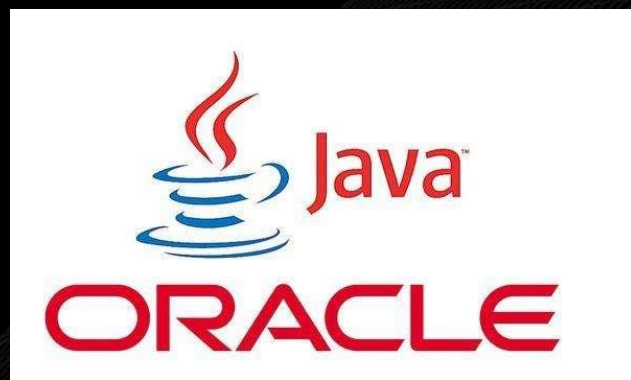




开发基础：开发环境构建



网络安全创新大会
Cyber Security Innovation Summit





开发基础：语言基础



网络安全创新大会
Cyber Security Innovation Summit



Kotlin 1.1
language for JVM, Android & JS

C/C++永不过时的语言

服务器，嵌入式，物联网，移动互联网，信息安全，游戏
应用领域无处不在！



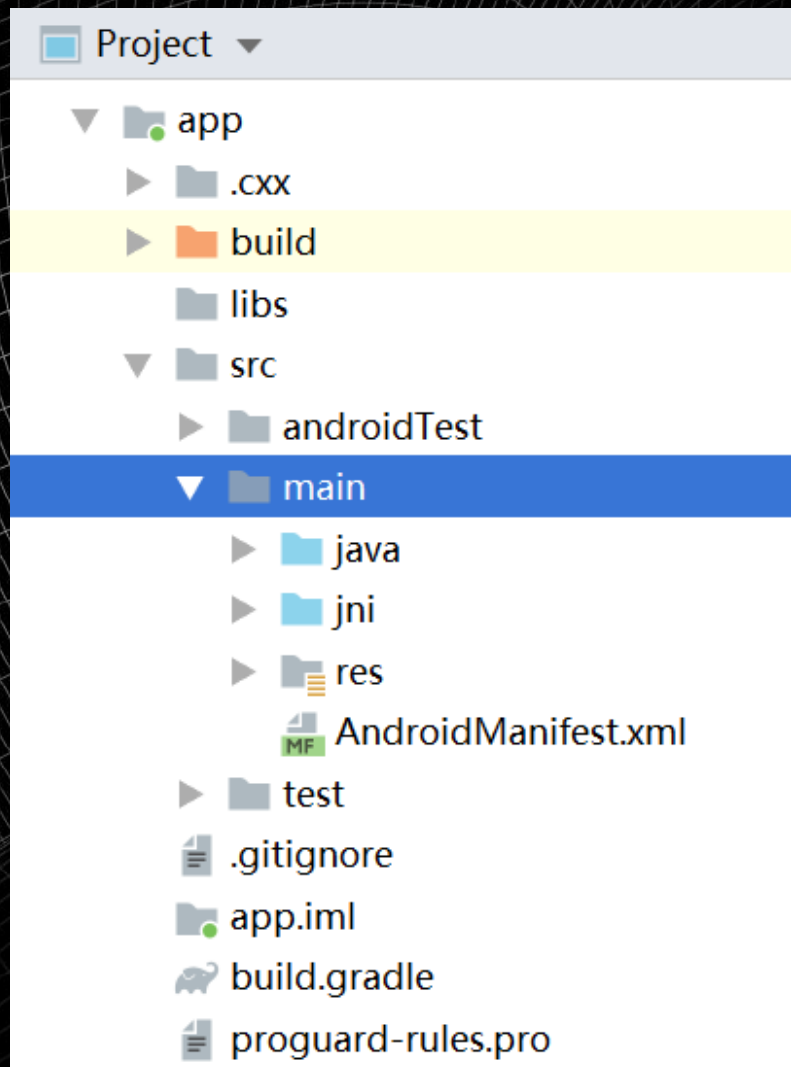
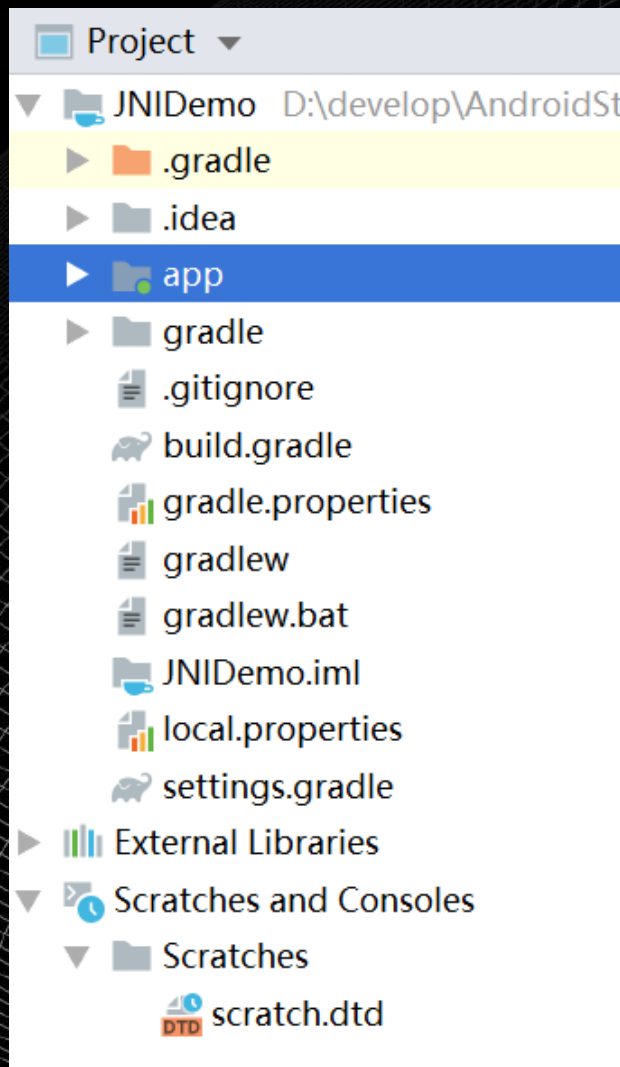
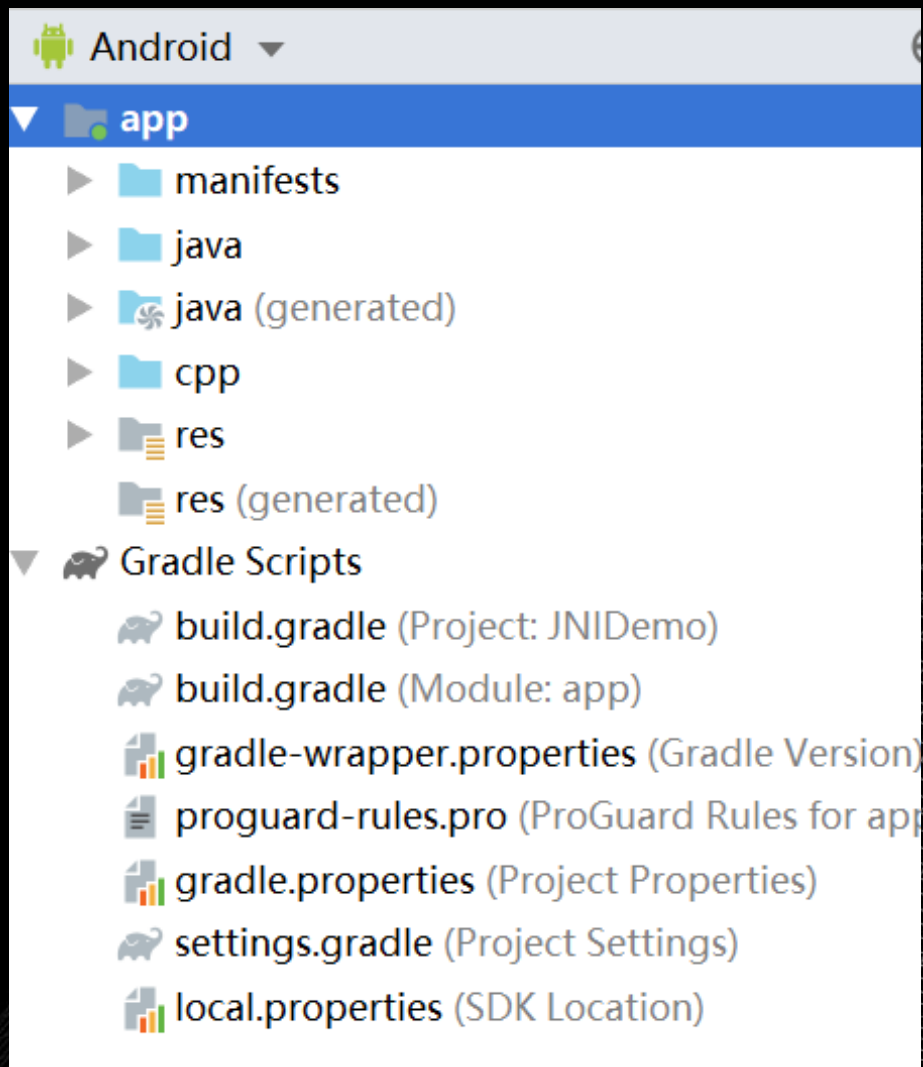
pythonTM



开发基础：项目文件结构



网络安全创新大会
Cyber Security Innovation Summit





```
| AndroidManifest.xml
| classes.dex
| out.txt
| resources.arsc
|
|—assets
|   | adbd.15.png
|   | adbd.16.png
|   | adbd.17.png
|   | adbd.21.png
|   |
|   —META-INF
|       | CERT.RSA
|       | CERT.SF
|       | MANIFEST.MF
|       |
| —res
```

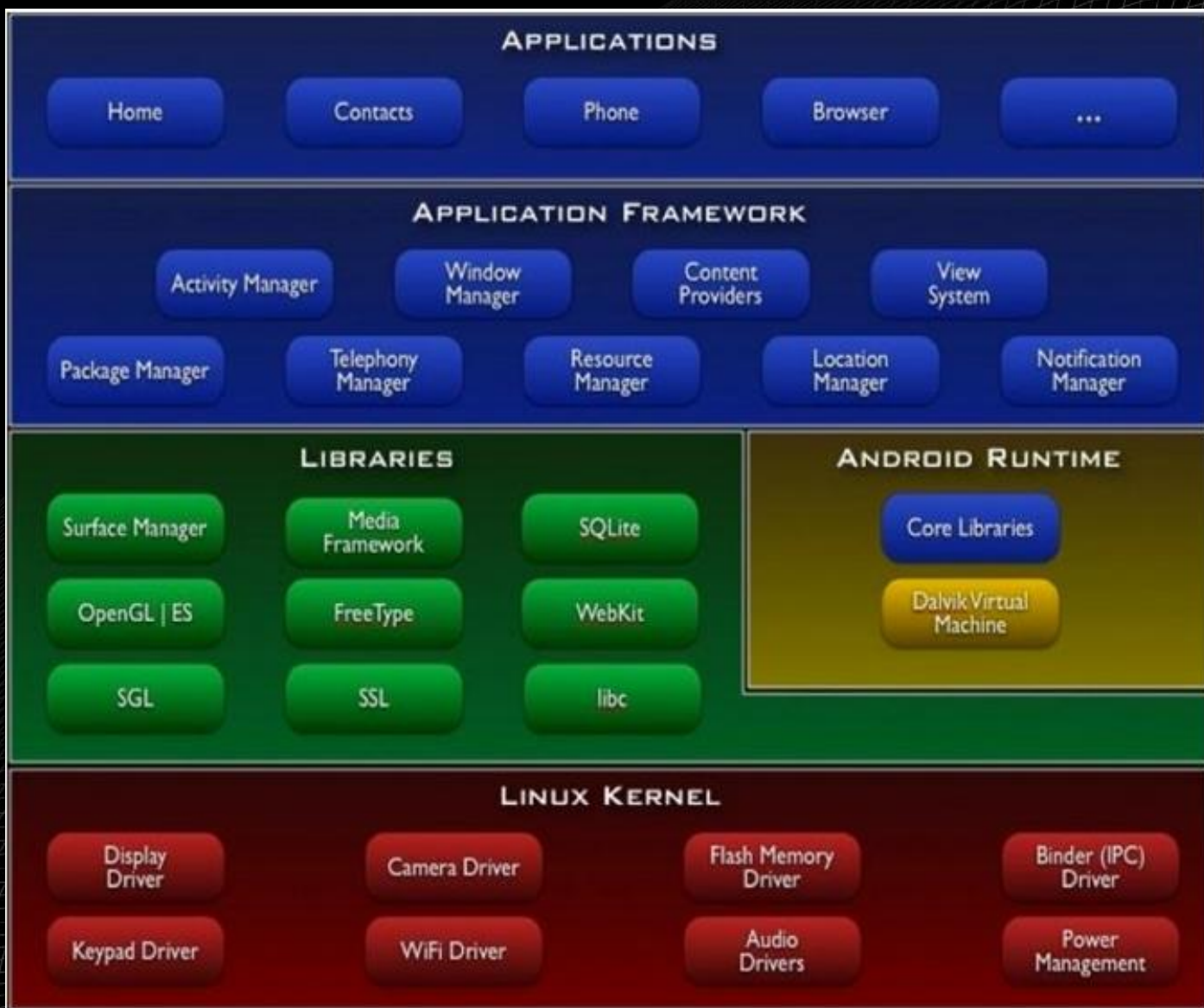
```
└res
  └drawable
    | ic_launcher.png
    |
    └drawable-hdpi-v4
      | ic_launcher.png
      |
      └drawable-ldpi-v4
        | ic_launcher.png
        |
        └drawable-mdpi-v4
          | ic_launcher.png
          |
          └drawable-xhdpi-v4
            | ic_launcher.png
```



基础安全机制：ANDROID系统架构



网络安全创新大会
Cyber Security Innovation Summit





应用层（代码安全、接入权限）

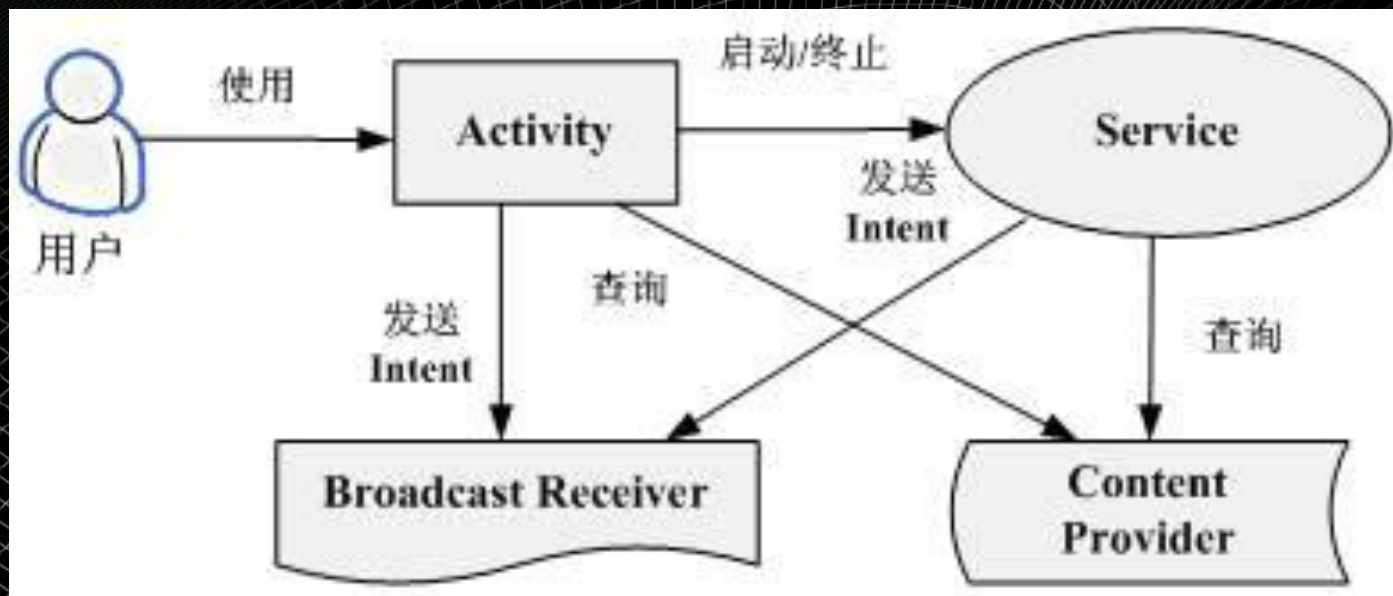
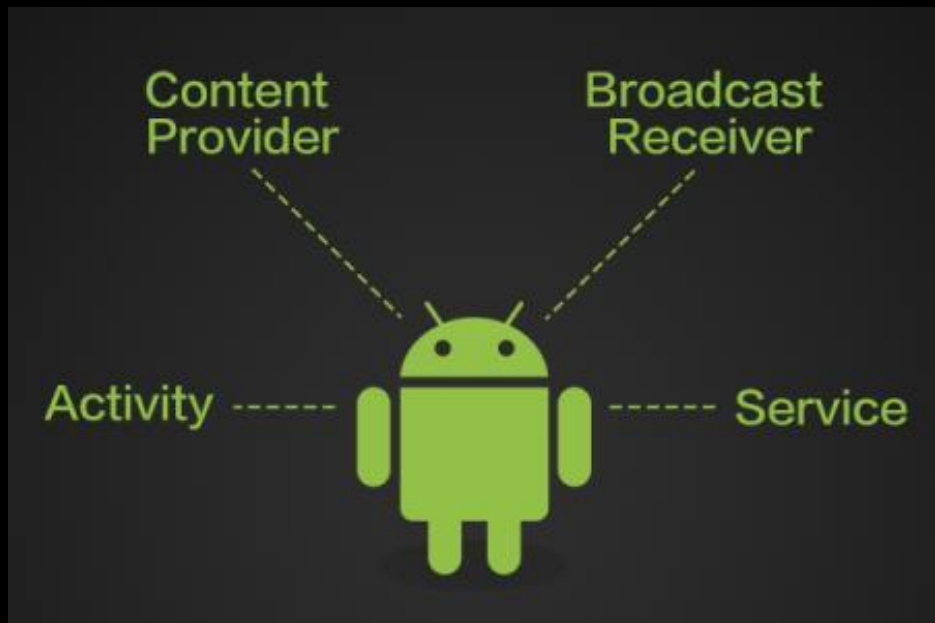
应用框架（数字证书）

**SSL
（网络安全）**

**SQLite
（数据库安全）**

**虚拟机
（安全沙箱）**

Linux Kernel（文件访问控制）





基础安全机制：AndroidManifest.xml



网络安全创新大会
Cyber Security Innovation Summit

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android" package="com.unico.jnidedemo">
    <application
        android:allowBackup="true"
        android:icon="@mipmap/ic_launcher"
        android:label="JNIDemo"
        android:roundIcon="@mipmap/ic_launcher_round"
        android:supportRtl="true"
        android:theme="@style/AppTheme">
        <activity android:name=".MainActivity">
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />
                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
    </application>
</manifest>
```

```
<?xml version="1.0" encoding="utf-8"?>
<manifest>
    <uses-sdk/>
    <uses-configuration/>
    <uses-feature/>
    <uses-permission/>
    <permission/>
    <permission-tree/>
    <permission-group/>
    <instrumentation/>
    <supports-screens/>
    <application>
        <activity>
            <intent-filter>
                <action/>
                <category/>
            </intent-filter>
        </activity>
        <activity-alias>
            <intent-filter></intent-filter>
            <meta-data/>
        </activity-alias>
        <service>
```

```
        <service>
            <intent-filter></intent-filter>
            <meta-data/>
        </service>
        <receiver>
            <intent-filter></intent-filter>
            <meta-data/>
        </receiver>
        <provider>
            <grant-uri-permission/>
            <meta-data/>
        </provider>
        <uses-library/>
    </application>
</manifest>
```



tools

- android.bat
- ddms.bat
- draw9patch.bat
- emulator.exe
- emulator64-crash-service.exe
- emulator-arm.exe
- emulator-check.exe
- emulator-crash-service.exe
- emulator-mips.exe
- emulator-x86.exe
- hierarchyviewer.bat
- jobb.bat
- lint.bat
- mkcard.exe
- monitor.bat
- monkeyrunner.bat
- NOTICE.txt
- package.xml
- source.properties

platform-tools

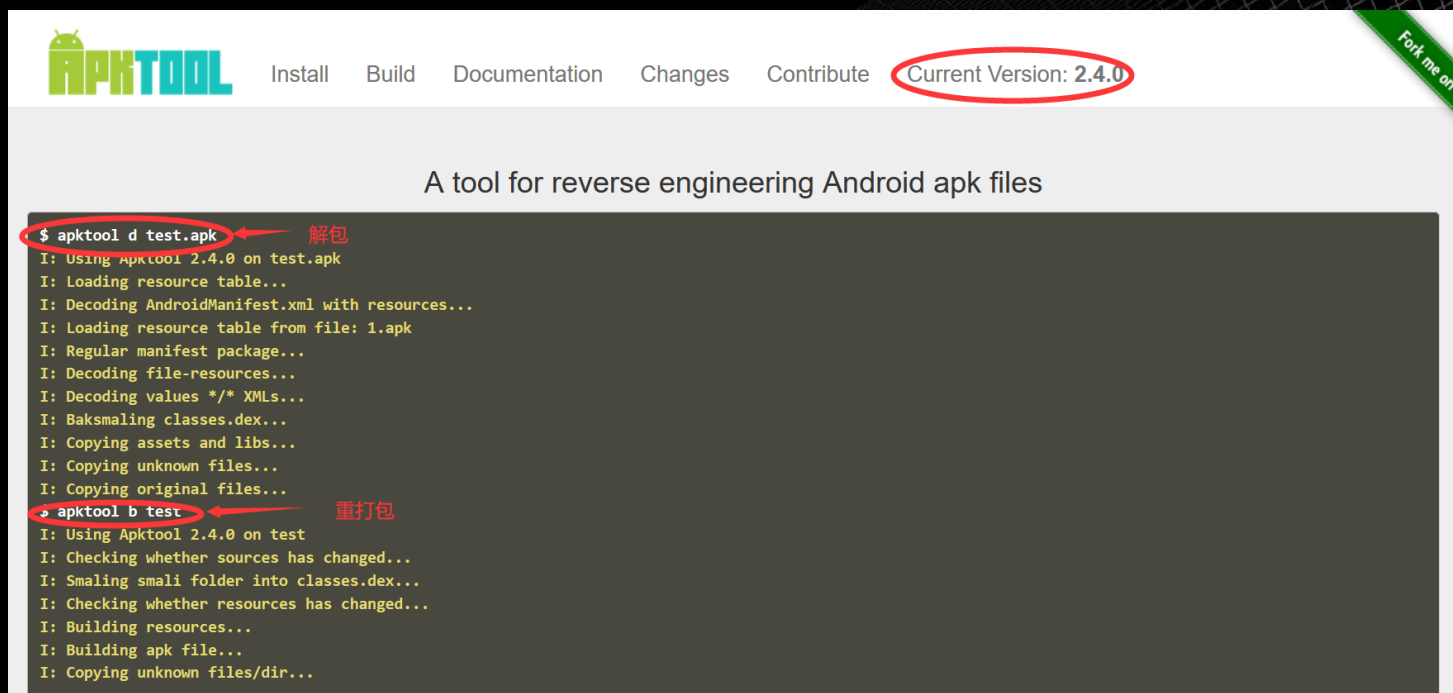
- api
- lib64
- systrace
- adb.exe
- AdbWinApi.dll
- AdbWinUsbApi.dll
- dmtracedump.exe
- etc1tool.exe
- fastboot.exe
- hprof-conv.exe
- libwinpthread-1.dll
- make_f2fs.exe
- mke2fs.conf
- mke2fs.exe
- NOTICE.txt
- package.xml
- source.properties
- sqlite3.exe

build-tools

- lib
- lib64
- renderscript
- aapt.exe
- aapt2.exe
- aarch64-linux-android-ld.exe
- aidl.exe
- apksigner.bat
- arm-linux-androideabi-ld.exe
- bcc_compat.exe
- core-lambda-stubs.jar
- d8.bat
- dexdump.exe
- dx.bat
- i686-linux-android-ld.exe

<https://ibotpeaches.github.io/Apktool/>

<http://www.rover12421.com/shakaapktool>



The screenshot shows the Apktool website with the current version 2.4.0 circled in red. Below the website header, there is a terminal window showing the commands and output for decompiling and rebuilding an APK. The terminal output is as follows:

```
$ apktool d test.apk
I: Using Apktool 2.4.0 on test.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: 1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
$ apktool b test
I: Using Apktool 2.4.0 on test
I: Checking whether sources has changed...
I: Smaling smali folder into classes.dex...
I: Checking whether resources has changed...
I: Building resources...
I: Building apk file...
I: Copying unknown files/dir...
```

Red arrows and labels point to the commands in the terminal: "apktool d test.apk" is labeled "解包" (Decompile) and "apktool b test" is labeled "重打包" (Rebuild).

- 反编译资源文件到原始格式（包括resources.arsc, classes.dex, 9.png以及XML等）；
- 将资源文件打包回二进制APK / JAR；
- 组织和处理依赖于框架资源的APK；

<https://bitbucket.org/JesusFreke/smali/>

```
[redacted] java -jar baksmali-2.3.4.jar -h
usage: baksmali [--version] [--help] [<command> [<args>]]

Options:
  --help, -h, -? - Show usage information
  --version, -v - Print the version of baksmali and then exit

Commands:
  deodex<de,x> - Deodexes an odex/oat file
  disassemble<dis,d> - Disassembles a dex file.
  dump<du> - Prints an annotated hex dump for the given dex file
  help<h> - Shows usage information
  list<l> - Lists various objects in a dex file.

See baksmali help <command> for more information about a specific command

[redacted] java -jar smali-2.3.4.jar -h
usage: smali [-v] [-h] [<command> [<args>]]

Options:
  -h, -?, --help - Show usage information
  -v, --version - Print the version of baksmali and then exit

Commands:
  assemble<ass,as,a> - Assembles smali files into a dex file.
  help<h> - Shows usage information

See smali help <command> for more information about a specific command
```


+ + >_ 安全工具箱: dex2jar/enjarify



网络安全创新大会
Cyber Security Innovation Summit

<https://github.com/pxb1988/dex2jar/>

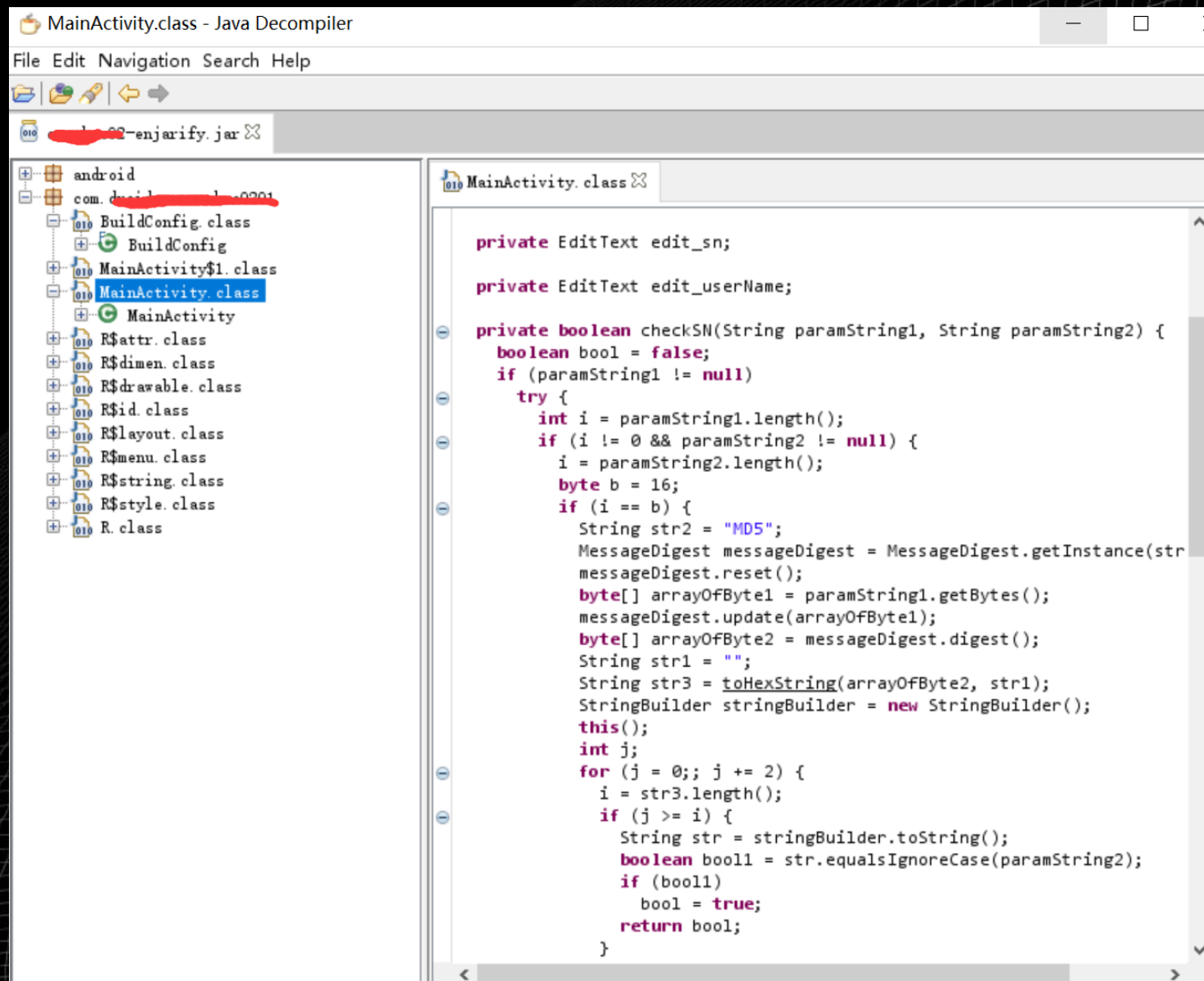
<https://github.com/Storyyeller/enjarify>

```
I:\crackme02>d2j-dex2jar.bat classes.dex  
dex2jar classes.dex -> .\classes-dex2jar.jar
```

```
I:\crackme02>cd\enjarify-master  
> .\enjarify.bat crackme02.apk  
Output written to crackme02-enjarify.jar  
288 classes translated successfully, 0 classes had errors
```

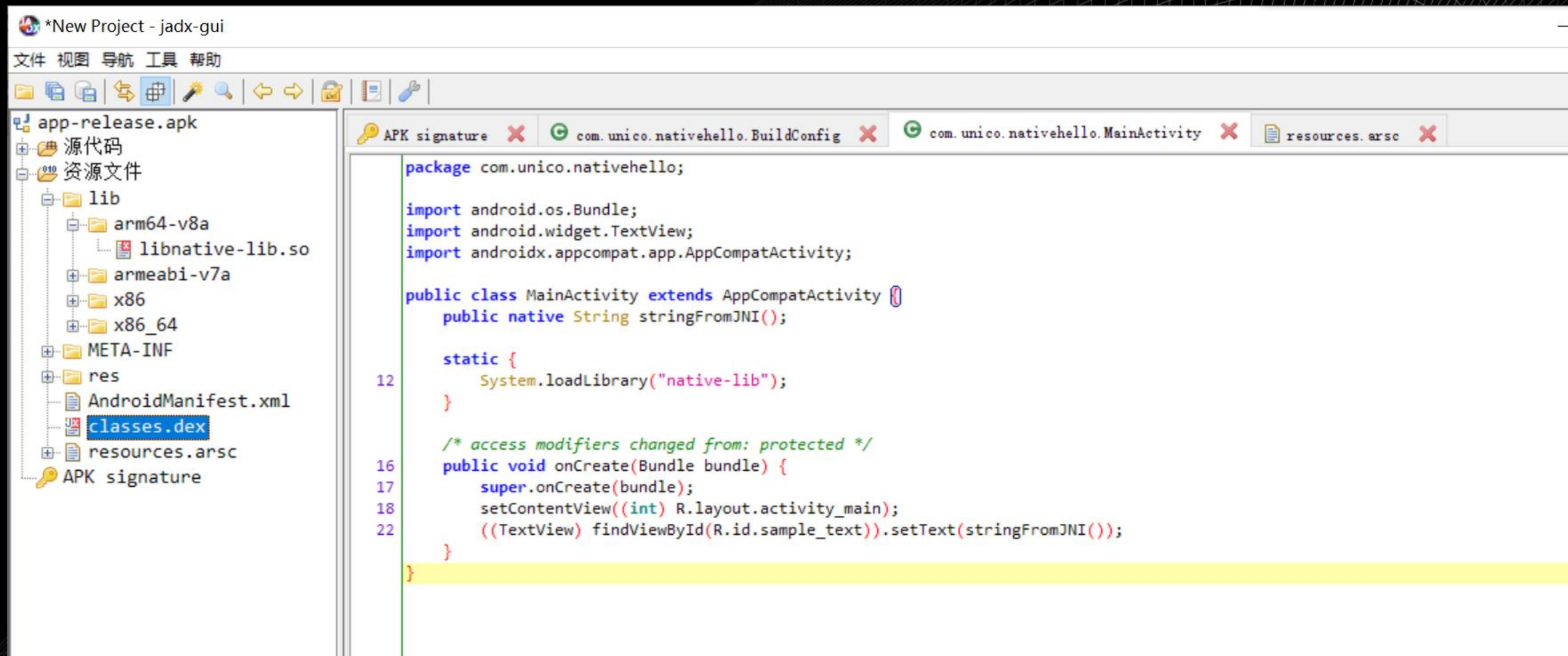


<http://java-decompiler.github.io/>





<https://github.com/skylot/jadx/>





安全工具箱: JEB



网络安全创新大会
Cyber Security Innovation Summit

<https://www.pnfsoftware.com/>

JEB3 Beta - D:\androidtest\UC-crackme.apk

文件 编辑 导航 行为 Native 调试器 窗口 帮助

工程浏览器

- D:\androidtest\UC-crackme.apk
 - UC-crackme.apk
 - com.uc.uc_crackme
 - Manifest
 - Certificate
 - Bytecode

过滤器: 输入"Enter" 来确认

Bytecode/层级

- android
 - com
 - uc
 - uc_crackme
 - BuildConfig
 - MainActivity
 - R

Bytecode/Disassembly

```
# Dalvik Disassembly (29 classes, 37 methods, 1177 fields)
# Package: com.uc.uc_crackme
# Application: android.app.Application [debuggable]
# (1 activity, 0 service, 0 provider, 0 receiver)
# ! Main Activity: com.uc.uc_crackme.MainActivity (MainActivity)

.class public final R$anim
.super Object

.annotation system EnclosingClass
    value = R
.end annotation

.annotation system InnerClass
    accessFlags = 0x19
    name = "anim"
.end annotation

.field public static final abc_fade_in:I = 0x7F040000

.field public static final abc_fade_out:I = 0x7F040001

.field public static final abc_slide_in_bottom:I = 0x7F040002

.field public static final abc_slide_in_top:I = 0x7F040003

.field public static final abc_slide_out_bottom:I = 0x7F040004

.field public static final abc_slide_out_top:I = 0x7F040005

.method public constructor <init>()V
    registers 1

```

描述 十六进制格式 Disassembly Graph 字符串

日志 Terminal

检查更新中...

检查更新出错

Creating a new project (primary file: D:\androidtest\UC-crackme.apk)

Adding artifact to project: D:\androidtest\UC-crackme.apk

{UC-crackme.apk > UC-crackme.apk}: 284 resource files were adjusted

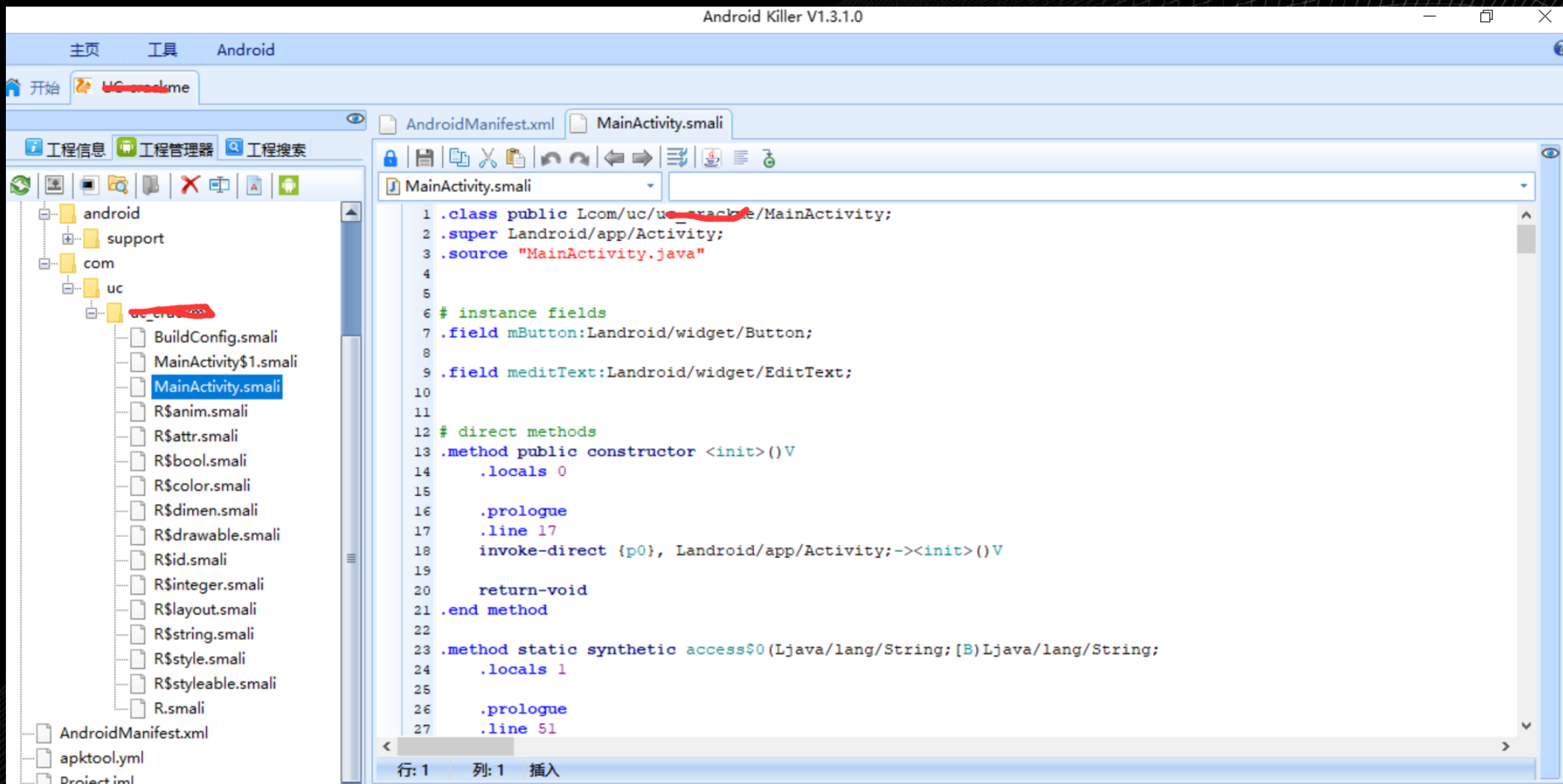
过滤器: 输入"Enter" 来确认

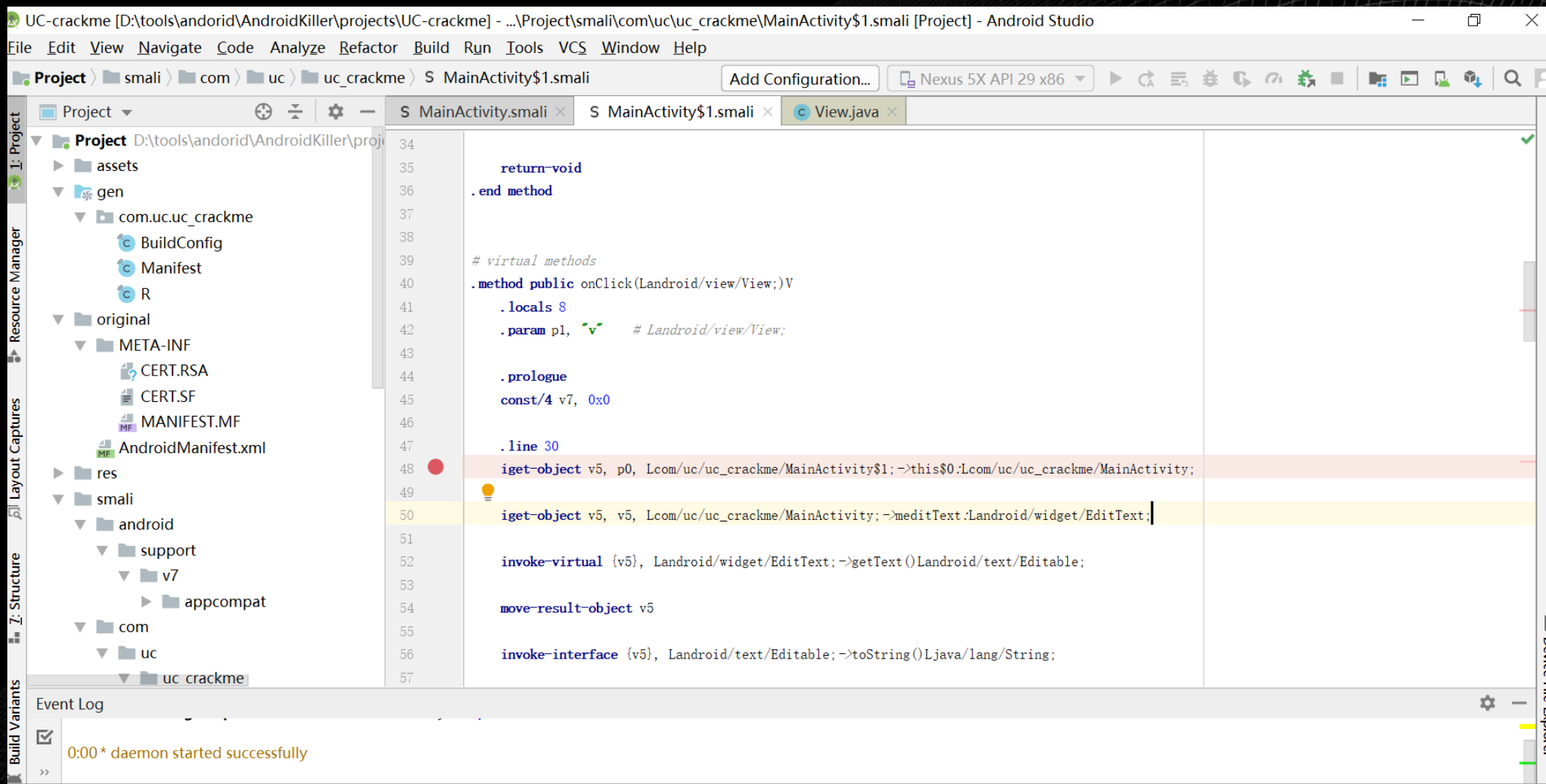


安全工具箱: Android Killer



网络安全创新大会
Cyber Security Innovation Summit



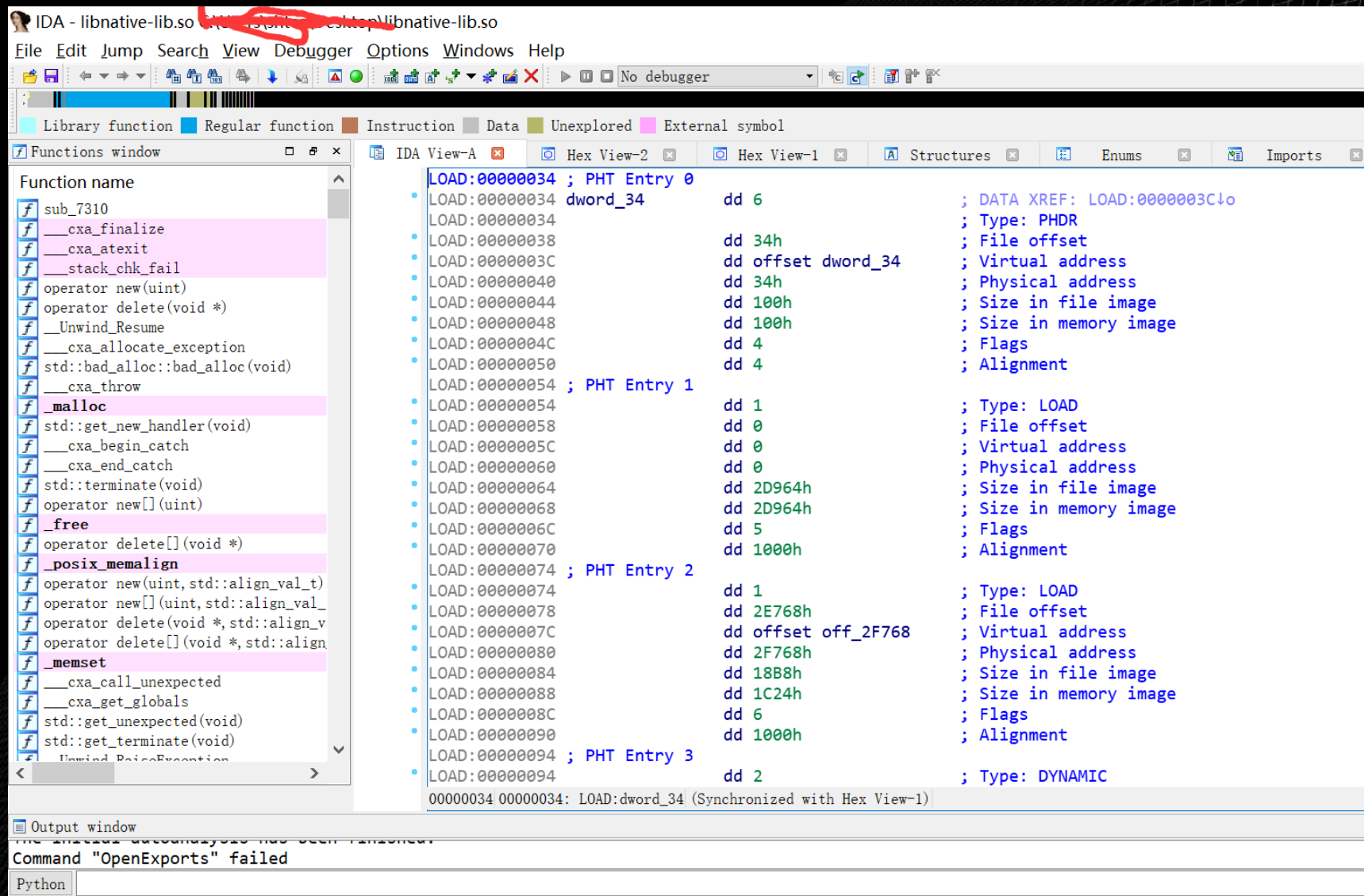




安全工具箱：IDA Pro



网络安全创新大会
Cyber Security Innovation Summit



<https://repo.xposed.info/>



Xposed Module Repository

Home

[Xposed Installer \(framework\)](#)

[Browse modules](#)

[Donate](#)

[Contact](#)

[Log in](#)

Welcome to the Xposed Module Repository!

On this site, you can [browse and download modules](#) for the [Xposed Framework](#). It is managed by rovo89, the inventor of Xposed.

Getting support


- For any questions about **modules**, you must use the respective support thread. If there's none, contact the author directly. Do **NOT** use any of the links below.
- If - and only if - you have issues with this **website**, use the [Contact](#) form.
- If - and only if - you have issues or need support for the Xposed **framework** or **installer**, use [this XDA subforum](#). Make sure you check for existing answers first via search function, first and recent posts. If you think you have discovered a bug, make sure it occurs even if you have no modules activated and it doesn't occur if you uninstall Xposed.


Uploading your modules

<http://www.cydiasubstrate.com/>

Cydia Substrate

The powerful code modification platform behind Cydia.

Find us on Twitter  ...

Find us on Facebook  ...



Hello! We have just released Substrate for Android, a project that we hope will be as interesting to that community as it has been for the last four years on iOS. However, please understand that our testing has so far only been "internal", and lots of things can go wrong "in the field": **keep backups** ;P. We encourage interested Android users to join our IRC channel, [#android on irc.saurik.com](#).

Remix Software

*Extensions: the cool alternative to apps!
Modify behavior without patches or ROMs.*

Substrate makes it easy to modify software, even without the source code, and in a way that allows users to easily choose which changes they want.

Developers support this by building their changes as "substrate extensions" that are loaded into all of the processes they want to take control of.

By using the provided API to make all changes in asubstrate.com the developers can safely adapt the

...for iOS

*Supported on versions 2.0 through 9.1,
including second-generation AppleTV.*

To install Substrate, you will need to "jailbreak" your device, as making changes to other software is not something that Apple normally allows.

Depending on your iOS version and device, you will need to use one of a few different jailbreaking tools such as redsn0w or evasi0n.

The various jailbreaking tools install Cydia Installer, which you can then use to install Substrate and any

...for Android

*Supported on versions 2.3 through 4.3,
including Kindle Fire, CyanogenMod, and Intel.*

While Android itself is "open", the devices that run it often aren't. Before installing Substrate, you will first need to get root access on your device.

Depending on which device you have, and which version of Android, this process differs; we therefore can't provide a simple recommendation.

Once you have root, you will need to install our APK, run the application, click Install, and grant

Demo地址: <https://github.com/zencodex/cydia-android-hook>

官方教程: <http://www.cydiasubstrate.com/id/20cf4700-6379-4a14-9bc2-853fde8cc9d1>

SDK下载地址: http://asdk.cydiasubstrate.com/zips/cydia_substrate-r2.zip

<https://www.frida.re/>

FRIDA

[OVERVIEW](#)

[DOCS](#)

[NEWS](#)

[CODE](#)

[CONTACT](#)

Dynamic instrumentation
toolkit for developers, reverse-
engineers, and security
researchers.

Scriptable

Portable

Free

Battle-tested




安全工具箱: DROZER



网络安全创新大会
Cyber Security Innovation Summit

<https://labs.f-secure.com/tools/drozer/>



Advisories /var/log/messages Tools Archive Careers

DROZER

Comprehensive security and attack framework for Android.

drozer helps to provide confidence that Android apps and devices being developed by, or deployed across, your organisation do not pose an unacceptable level of risk. By allowing you to interact with the Dalvik VM, other apps' IPC endpoints and the underlying OS.

drozer provides tools to help you use and share public exploits for Android. For remote exploits, it can generate shellcode to help you to deploy the drozer Agent as a remote administrator tool, with maximum leverage on the device.

Have you validated the security of the Android apps and devices released by, or used in, your organisation?

DOWNLOAD

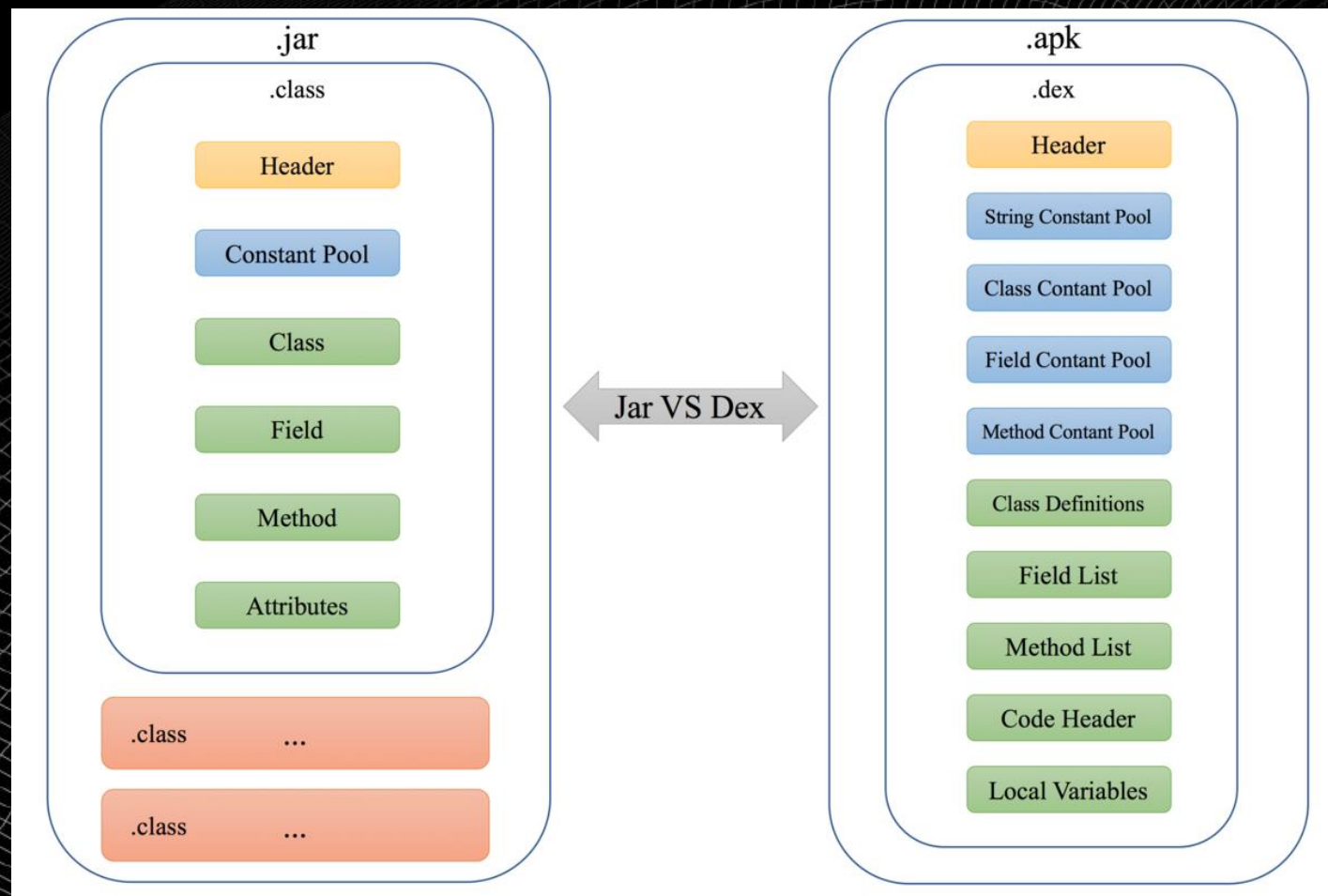
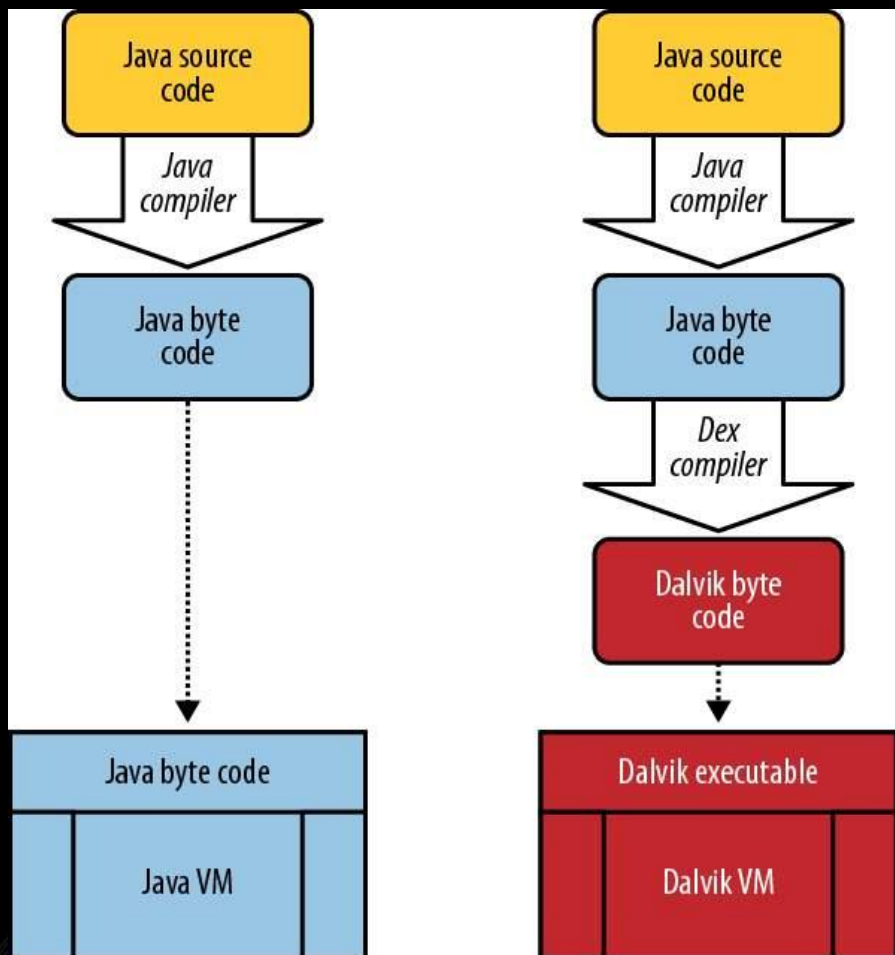
**DOWNLOAD THE DROZER
USER GUIDE**

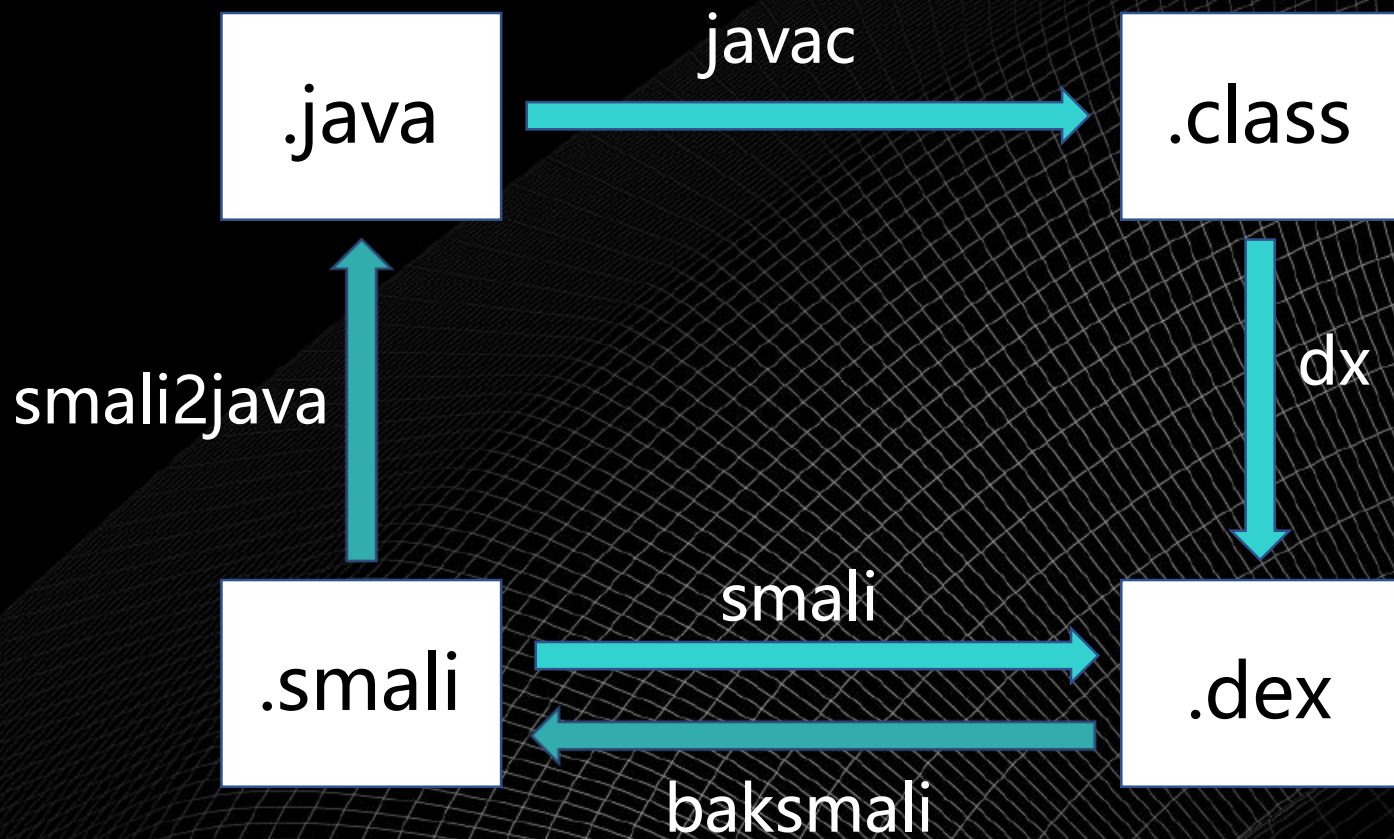


逆向分析：DVM vs JVM



网络安全创新大会
Cyber Security Innovation Summit





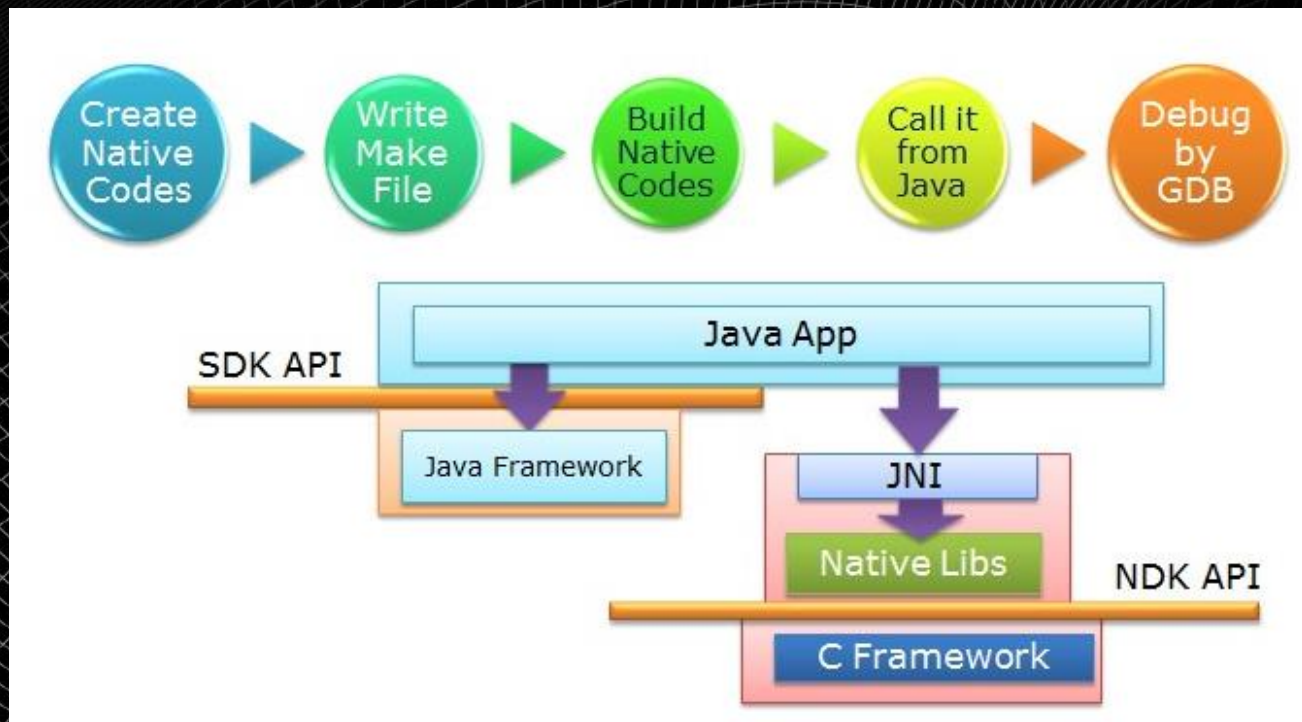
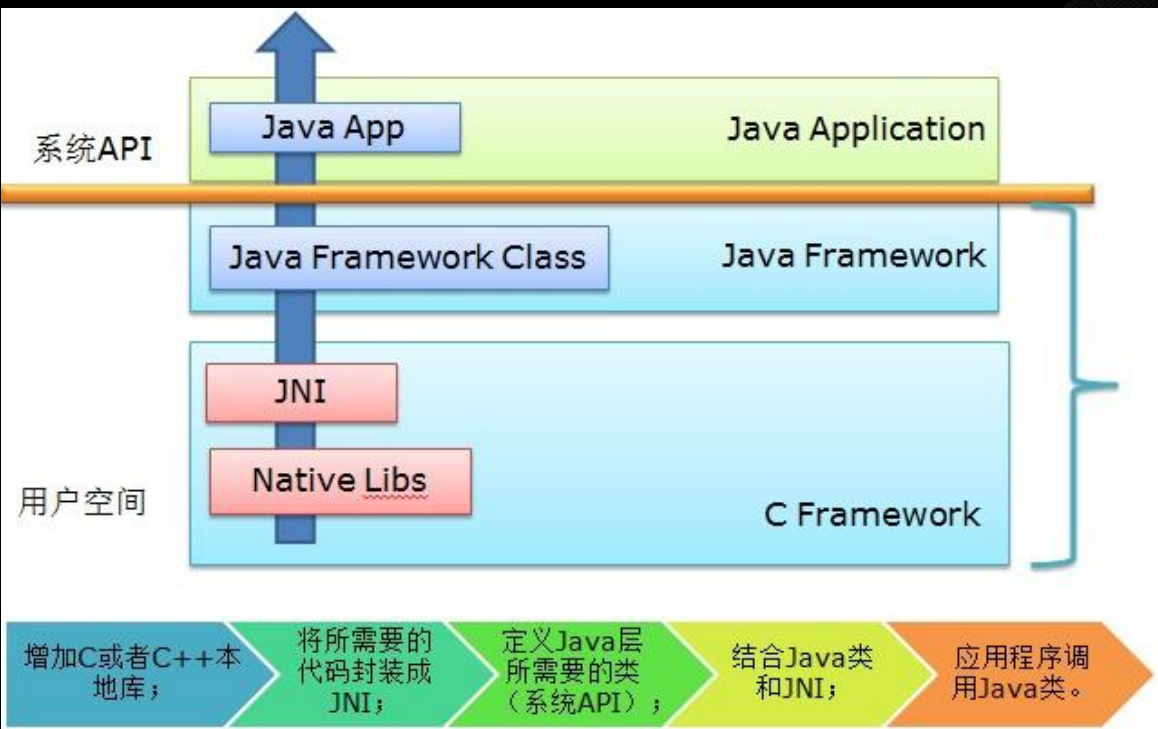


逆向分析：smali语言简介



```
.class public Lunico/hello/info/HelloWorld;    #定义类名
.super Ljava/lang/Object;                      #定义父类
.source "HelloWorld.java"                     #源文件名
# direct methods    #直接方法  (# virtual methods 为虚方法)
.method public constructor <init>()V          #构造函数
    .locals 0    #方法中使用到的局部变量个数
    .prologue    #代码起始指令
    .line 8    #源代码所在行数
    invoke-direct {p0}, Ljava/lang/Object;-><init>()V    #调用父类构造方法
    return-void    #返回空
.end method    #方法结束
.method public static main([Ljava/lang/String;)V    #对应 main 方法
    .locals 2    #方法包含两个局部 v0, v1
    .param p0, "args"    # [Ljava/lang/String;    # main 方法的参数 args 标记为 p0
    .prologue    #代码起始指令
    .line 10
    sget-object v0, Ljava/lang/System;->out:Ljava/io/PrintStream;    #将 System.out 这个静态变量赋给 v0
    const-string v1, "hello world"    #构造字符串
    #方法调用 (调用 v0 的方法 println , v1 是参数)
    invoke-virtual {v0, v1}, Ljava/io/PrintStream;->println(Ljava/lang/String;)V
    .line 11
    return-void
.end method
```

v命名法	p命名法	寄存器含义
v0	v0	第一个局部变量寄存器
...	...	中间的局部变量寄存器
vM-N	p0	第一个参数寄存器 (通常为调用对象)
...	...	中间参数寄存器
vM-1	pN-1	第N个参数寄存器

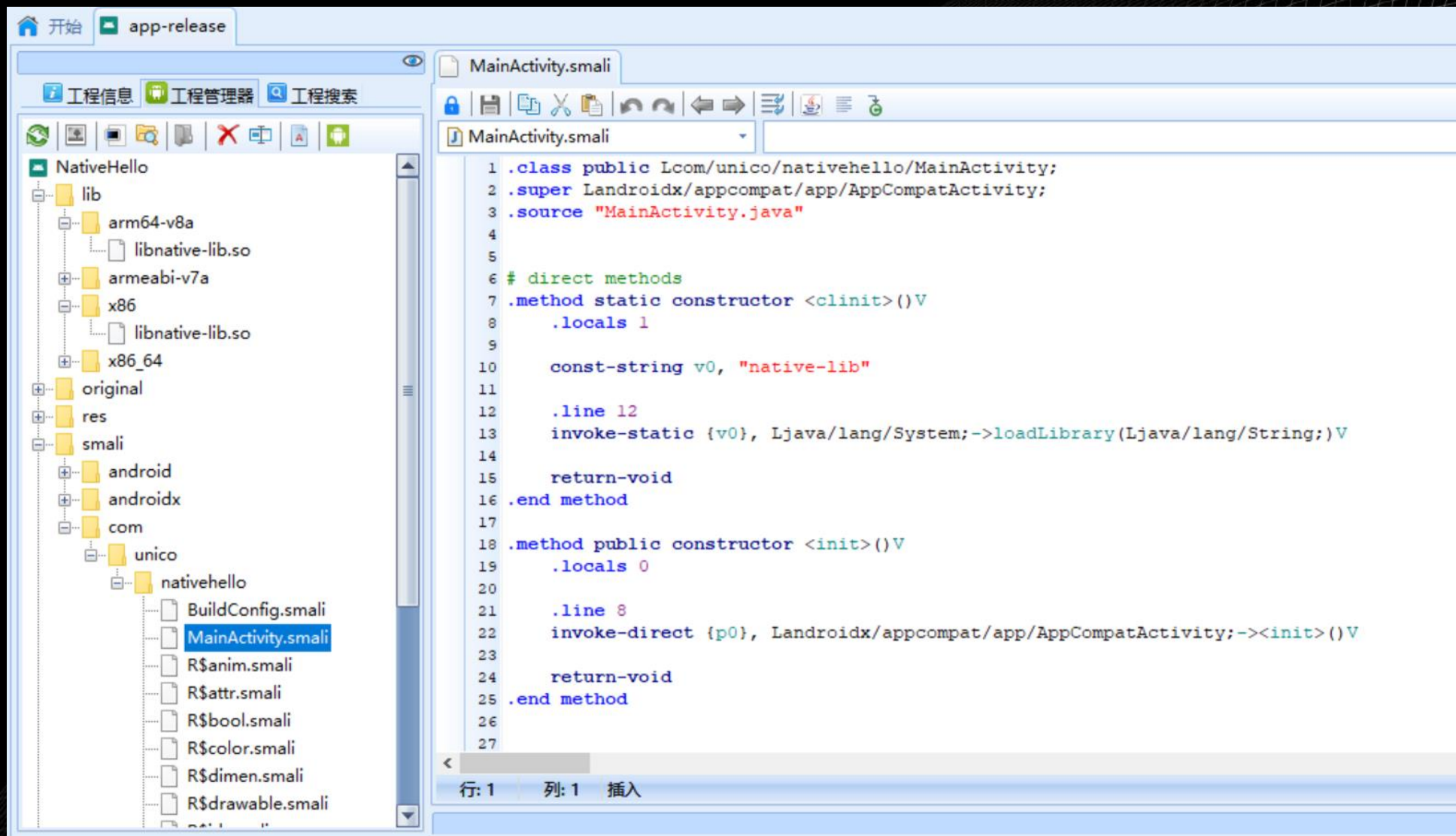




逆向分析: JNI Native开发



网络安全创新大会
Cyber Security Innovation Summit





```
IDA View-A  Hex View-1  Structures  Enums  Imports
.text:000088A0 ; ===== S U B R O U T I N E =====
.text:000088A0
.text:000088A0 ; Attributes: bp-based frame
.text:000088A0
.text:000088A0         public __cxa_uncaught_exception
.text:000088A0 __cxa_uncaught_exception proc near          ; DATA XREF: LOAD:0000D30↑o
.text:000088A0 ; __unwind { // __gxx_personality_v0
.text:000088A0         push     ebp
.text:000088A1         mov      ebp, esp
.text:000088A3         push     ebx
.text:000088A4         and      esp, 0FFFFFF0h
.text:000088A7         sub      esp, 10h
.text:000088AA         call     $+5
.text:000088AF         pop      ebx
.text:000088B0         add      ebx, 285D9h
.text:000088B6         call     __cxa_get_globals_fast
.text:000088BB         test     eax, eax
.text:000088BD         jz        short loc_88C8
.text:000088BF         cmp      dword ptr [eax+4], 0
.text:000088C3         setnz    al
.text:000088C6         jmp      short loc_88CA
.text:000088C8 ; -----
.text:000088C8 loc_88C8:                                ; CODE XREF: __cxa_uncaught_exception+1D↑j
.text:000088C8         xor      eax, eax
.text:000088CA loc_88CA:                                ; CODE XREF: __cxa_uncaught_exception+26↑j
.text:000088CA         lea      esp, [ebp-4]
.text:000088CD         pop      ebx
```

ARM核心概念

- 寄存器
- 地址
- 异常和中断




ARM State General Registers and Program Counter

System & User	FIQ	Supervisor	Abort	IRQ	Undefined
r0	r0	r0	r0	r0	r0
r1	r1	r1	r1	r1	r1
r2	r2	r2	r2	r2	r2
r3	r3	r3	r3	r3	r3
r4	r4	r4	r4	r4	r4
r5	r5	r5	r5	r5	r5
r6	r6	r6	r6	r6	r6
r7	r7	r7	r7	r7	r7
r8	r8_fiq	r8	r8	r8	r8
r9	r9_fiq	r9	r9	r9	r9
r10	r10_fiq	r10	r10	r10	r10
r11	r11_fiq	r11	r11	r11	r11
r12	r12_fiq	r12	r12	r12	r12
r13	r13_fiq	r13_svc	r13_abt	r13_irq	r13_und
r14	r14_fiq	r14_svc	r14_abt	r14_irq	r14_und
r15 (PC)	r15 (PC)	r15 (PC)	r15 (PC)	r15 (PC)	r15 (PC)

ARM State Program Status Registers

CPSR	CPSR	CPSR	CPSR	CPSR	CPSR
	SPSR_fiq	SPSR_svc	SPSR_abt	SPSR_irq	SPSR_und

 = banked register

工作状态

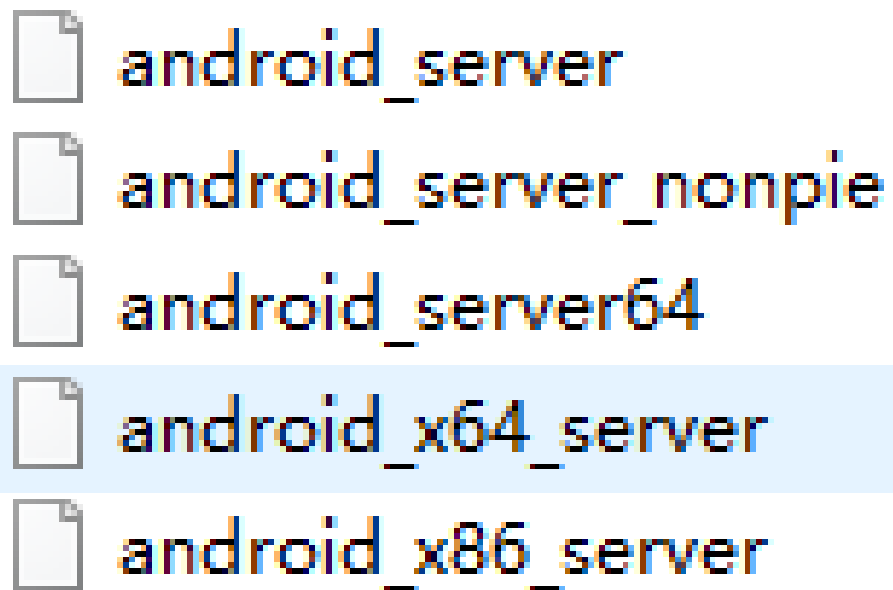
- ARM状态
- Thumb状态

工作模式

- 用户模式 (USR)
- 系统模式 (SYS)
- 快中断模式 (FIQ)
- 中断模式 (IRQ)
- 管理模式 (SVC)
- 中止模式 (ABT)
- 未定义模式 (UND)

前期准备

1. 拷贝IDA目录下dbgsrv/android_server至终端运行
2. 转发端口: adb forward tcp:pc_port tcp:mobile_port



- android_server
- android_server_nonpie
- android_server64
- android_x64_server
- android_x86_server

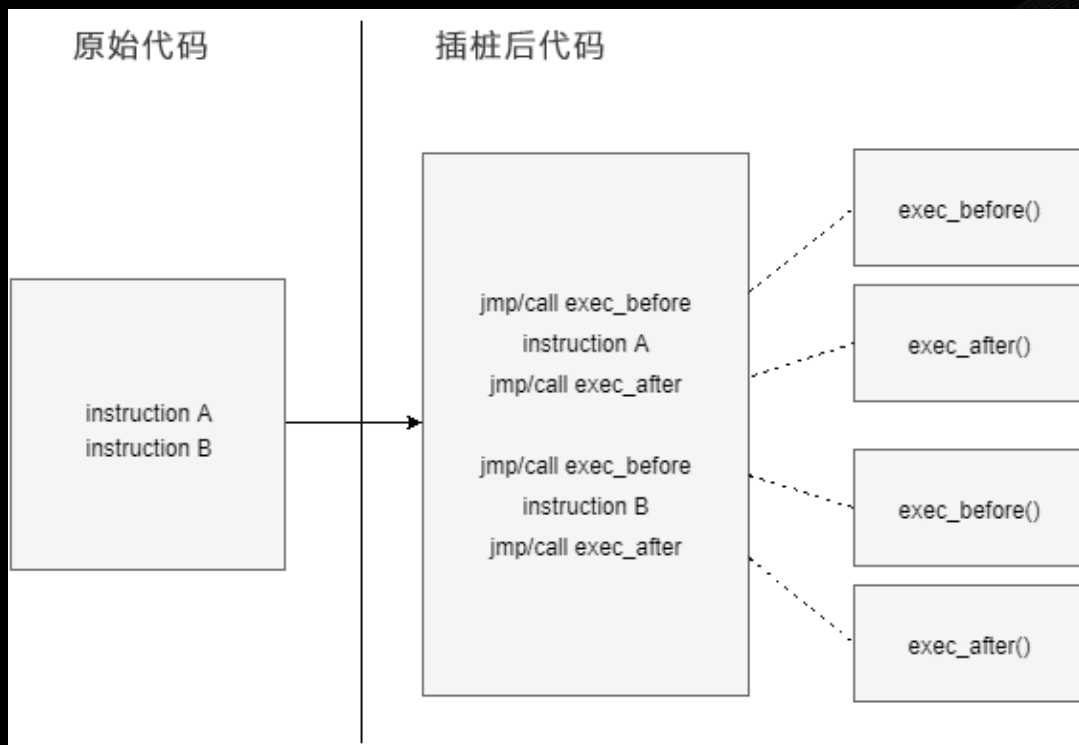


- 3、程序启动 `adb shell am start -D -n PackageName/ActivityName`
- 4、IDA挂接、选择Debugger->Attach to Process

```
2335 [32] /system/bin/logd
2336 [32] /sbin/healthd
2337 [32] /system/bin/sh
2338 [32] /system/bin/lmxd
2339 [32] /system/bin/servicemanager
2340 [32] /system/bin/vold
2342 [32] /system/bin/surfaceflinger
2348 [32] /system/bin/netd
2350 [32] /system/bin/flymed
2351 [32] /system/bin/debuggerd
2352 [32] /system/bin/debuggerd64
2356 [32] /system/bin/drmserver
2358 [32] /system/bin/mediaserver
2359 [32] /system/bin/installd
2361 [32] /system/bin/keystore /data/misc/keystore
2363 [32] /system/bin/mcDriverDaemon
2364 [32] /system/bin/gpsd /system/etc/gpsconfig.xml
2368 [32] /system/bin/cploadserver
2369 [32] /system/bin/nvmserver
2370 [32] /system/bin/eeh_server
2371 [32] /system/bin/rild -l /system/lib/libmarvell-ril.so -- -m NEZHA
2372 [32] /system/bin/immvibed -p 99 -u 1000
2373 [32] zygote
2374 [32] /system/bin/sdcard -u 1023 -g 1023 -l /data/media /mnt/shell/emulated ...
```

Line 1 of 87

OK Cancel Search Help



动态二进制插桩框架都有三种执行模式：
解释模式（Interpretation mode）、探测模式（probe mode）和JIT模式（just-in-time mode）

通过动态二进制插桩框架控制了程序的执行，就能够将插桩添加到执行程序中。我们可以在代码块之前和之后插入想要的代码，甚至也可以完全替换它们。



Frida获取设备

```
device = frida.get_usb_device()
device.on('spawn-added', spawn_added)
```

Frida载入hook代码

```
def spawn_added(spawn):
    if spawn.identifier.startswith("com.sh...test"):
        print('spawn_added:', spawn)
        hook(device, spawn.pid, "hook.js")
        device.resume(spawn.pid)
```

Hook native方法

```
Java.perform(function(){
    var getString = undefined;
    exports = Module.enumerateExportsSync("libtest.so");
    for(i=0; i<exports.length; i++){
        if(exports.name == "Java_com_example_hooktest_MainActivity_getString"){
            getString = exports.address;
            send("getInt is at " + getString);
            break;
        }
    }
})
```

Hook指定类方法

```
Java.perform(function x(){
    var AMapLocation = Java.use("com.amap.api.location.AMapLocation");
    AMapLocation.getLatitude.implementation = function(){
        result = this.getLatitude();
        console.log("AMapLocation getLatitude:" + result);
        console.log(printStack());
        return result;
    };
});
```

Hook加固类应用

```
if(Java.available) {
    Java.perform(function(){
        var application = Java.use("android.app.Application");
        application.attach.overload("android.content.Context").implementation = function(context) {
            var result = this.attach(context);
            var classloader = context.getClassLoader(); // get classloader
            Java.classFactory.loader = classloader;
            hook(); //hook实现
            return result;
        };
    });
}
```




网络安全创新大会
Cyber Security Innovation Summit

Part 3

一点体会



网络安全创新大会
Cyber Security Innovation Summit

任重道远，勤学苦练



CIS THANKS

网络安全创新大会
Cyber Security Innovation Summit

