Basic Courses of Android Security

移动安全

残夜

2015/10/19

whitecell-lab

专注二进制与移动安全，来自最具艺术气质的白细胞移动安全组的精英团队。

目录

Dalvik 虚拟机

- Dalvik 虚拟机介绍
- Dalvik 汇编语言基础
- Dalvik 版本HellWorld
- 破解第一个程序

Dex和ODex文件格式

- Dex文件结构解析
- ODex文件结构解析
- 另类APK破解方法

Smali文件格式

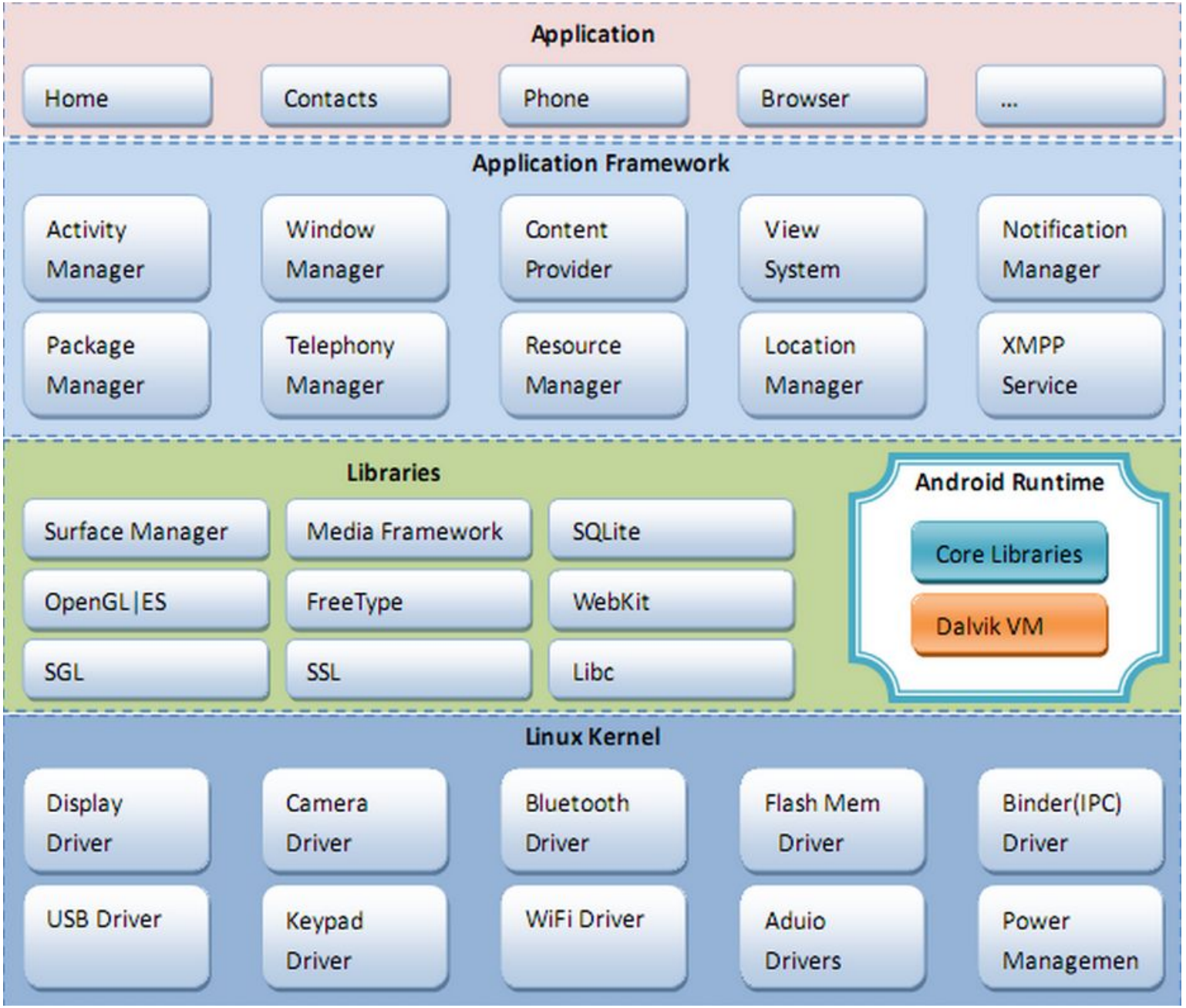
- Smali文件结构解析
- IDA Pro破解实例

简介

Android（安卓），是一个以Linux为基础的开源移动设备操作系统，主要用于智能手机和平板电脑，由Google成立的Open Handset Alliance（OHA，开放手持设备联盟）持续领导与开发中。Android已发布的最新版本为Android 5.0(Lollipop)。

Android系统最初由安迪·鲁宾（Andy Rubin）等人开发制作，最初开发这个系统的目的是创建一个数码相机的先进操作系统；但是后来发现市场需求不够大，加上智能手机市场快速成长，于是Android被改造为一款面向智能手机的操作系统。於2005年8月被美国科技企业Google收购。2007年11月，Google与84家制造商、开发商及电信营运商成立开放手持设备联盟来共同研发改良Android系统，随後，Google以Apache免费开放原始码许可证的授权方式，发布了Android的原码，让生产商推出搭载Android的智能手机，後来更逐渐拓展到平板电脑及其他领域上。

【视频】简述安卓历史-brief history of Android [VERGE]_高清.mp4



系统、工具

系统及开发环境

- win7/win8
- (My)Eclipse+ADT/AndroidStudio
- JDK1.7

Android测试工具

- APKTools、Dex2jar、IDApro6.1及以上版本、jd-gui、
- Drozer

Web漏洞测试工具

- Wireshark、burpsuite
- sqlmap

Dalvik Virtual Machine

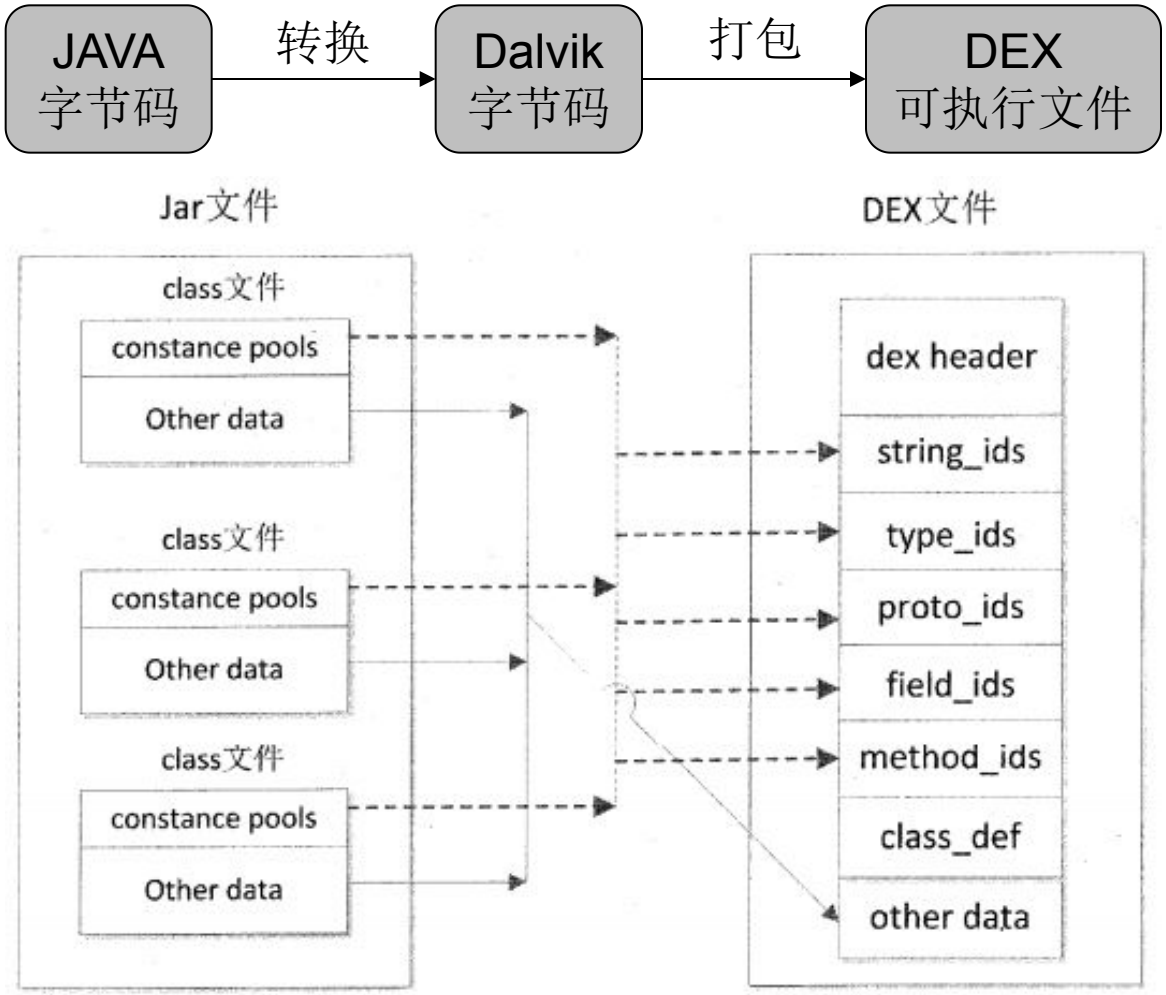
Dalvik 虚拟机

概述

- 作者：丹·伯恩斯坦（Dan Bornstein）
- Android平台的核心组件
- 特点：
  - 体积小，占用内存空间小
  - 专有的DEX可执行文件格式，体积更小，执行速度更快
  - 32位索引值
  - 基于寄存器架构，并拥有一套完整的指令系统
  - 提供对象周期管理、堆栈管理、线程管理、安全和异常管理以及垃圾回收等功能
  - 所有的Android程序都运行在Android系统进程里，每个进程对应着一个Dalvik虚拟机实例

与JAVA虚拟机的区别

- JAVA字节码和Dalvik字节码



与JAVA虚拟机的区别

- JAVA虚拟机和Dalvik虚拟机架构不同

Hello.java

```
public class hello {
public int foo(int a, int b) {
return (a + b) * (a - b);
}
public static void main(String[] argc) {
Hello hello = new Hello();
System.out.println(hello.foo(5,3));
}
}
```

- 生成class文件 javac Hello.java
- 生成dex文件 dx –dex –output=Hello.dex Hello.class

与JAVA虚拟机的区别

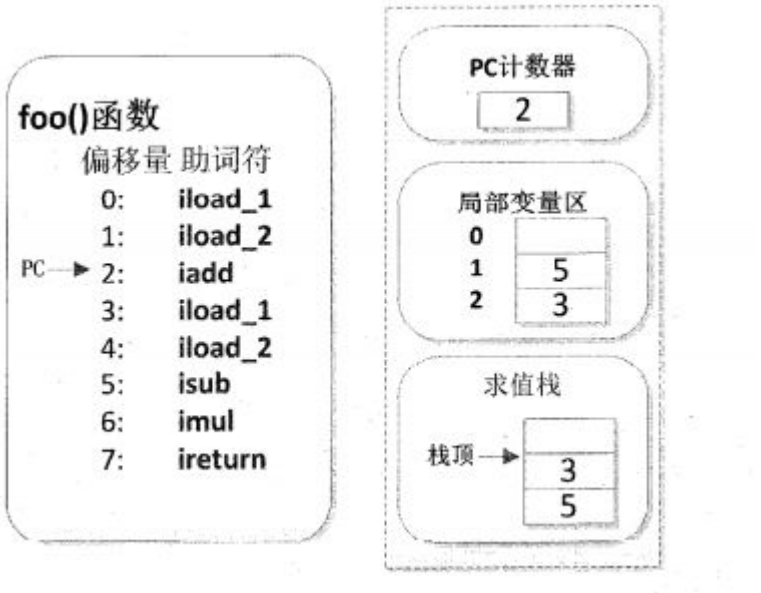
- Javap查看java字节码
  javap –c –classpath .Hello

```
public int foo(int, int);
  Code:
   0:   iload_1
   1:   iload_2
   2:   iadd
   3:   iload_1
   4:   iload_2
   5:   isub
   6:   imul
   7:   ireturn
```

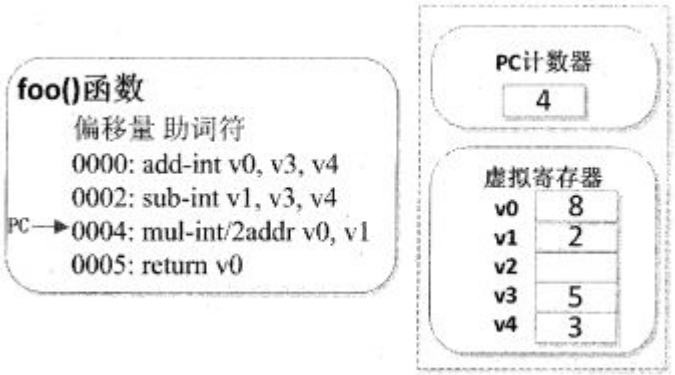
- Dexdump.exe查看Dalvik字节码
  dexdump.exe –d Hello.dex

```
Hello.foo:(II)I
0000: add-int v0, v3, v4
0002: sub-int v1, v3, v4
0004: mul-int/2addr v0, v1
0005: return v0
```

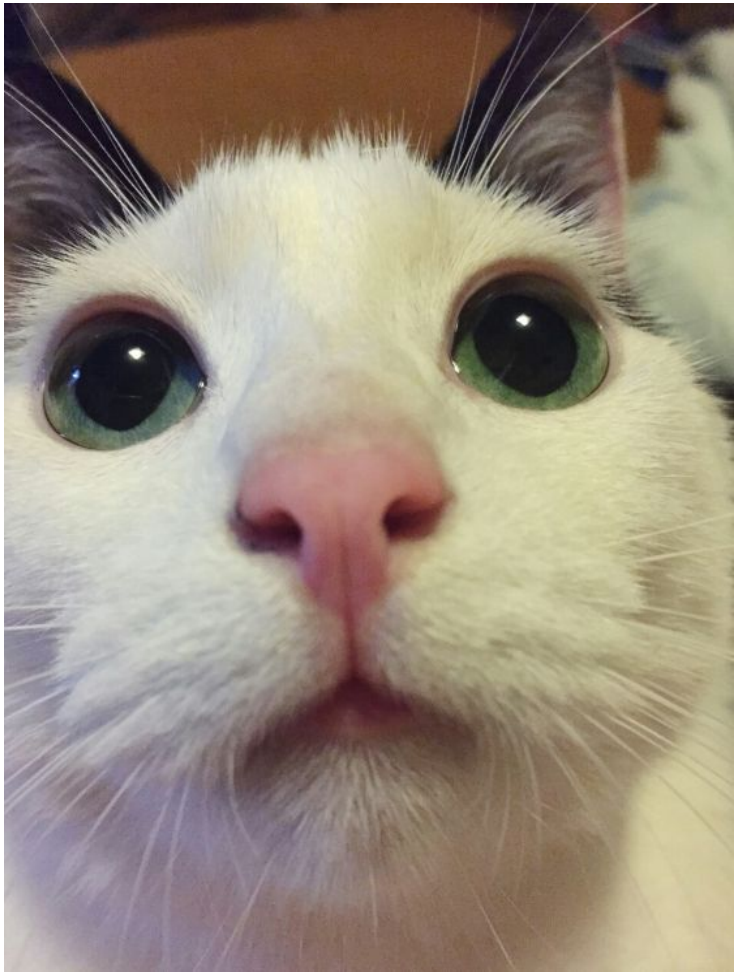
与JAVA虚拟机的区别



JVM运行状态



Dalvik VM运行状态



谢谢！

"when i look into the sky"

canye@whitecell-lab.org