

# Android应用安全防护和逆向分析



[Android应用安全防护和逆向分析\\_下载链接1](#)

著者:姜维

出版者:机械工业出版社

出版时间:2017-12-1

装帧:平装

isbn:9787111584452

本书全面介绍Android应用的安全防护方法与逆向分析技术，分为四篇：基础篇、防护篇、工具篇、操作篇，共26章。基础篇包括第1~7章，主要介绍移动应用安全的基础知识，包括Android中NDK开发知识、逆向中需要用到的命令、编译之后的apk包含的四

类主要文件格式解析等。防护篇包括第8~14章，主要介绍移动应用安全防护的相关技术，包括混淆、签名校验、反调试检测等安全策略，Android应用升级权限、降低权限等，配置文件中的问题，应用签名机制，apk的加固策略，so文件的加固策略等。工具篇包括第15~19章，主要介绍逆向分析常用的工具以及使用场景，包括如何开启设备的总调试开关，反编译器apktool、Jadx、Xposed、Cydia Substrate等。操作篇包括第20~26章，主要介绍Android中的逆向分析技巧，包括静态方式和动态方式，介绍Android中开发会遇到的系统漏洞及修复方式，最后分析了Android中一个非常经典的文件加密病毒样本。

作者介绍:

姜维

某知名互联网公司开发者，参与过多个移动App开发项目，对Android安全问题情有独钟，深入分析过Android源代码和各类移动应用病毒，逆向分析实战经验

目录: 对本书的赞誉

前言

基础篇

第1章 Android中锁屏密码加密算法分析 2

1.1 锁屏密码方式 2

1.2 密码算法分析 2

1.2.1 输入密码算法分析 2

1.2.2 手势密码算法分析 7

1.3 本章小结 9

第2章 Android中NDK开发 10

2.1 搭建开发环境 10

2.1.1 Eclipse环境搭建 10

2.1.2 Android Studio环境搭建 12

2.2 第一行代码：HelloWorld 14

2.3 JNIEnv类型和jobject类型 18

2.3.1 JNIEnv类型 19

2.3.2 jobject参数obj 19

2.3.3 Java类型和native中的类型映射关系 19

2.3.4 jclass类型 19

2.3.5 native中访问Java层代码 20

2.4 JNIEnv类型中方法的使用 21

2.4.1 native中获取方法的Id 22

2.4.2 Java和C++中的多态机制 24

2.5 创建Java对象及字符串的操作方法 27

2.5.1 native中创建Java对象 27

2.5.2 native中操作Java字符串 28

2.6 C/C++中操作Java中的数组 32

2.6.1 操作基本类型数组 32

2.6.2 操作对象类型数组 33

2.7 C/C++中的引用类型和ID的缓存 36

2.7.1 引用类型 36

2.7.2 缓存方法 37

2.8 本章小结 38

第3章 Android中开发与逆向常用命令

总结 39

3.1 基础命令 39

3.2 非shell命令 40

|                               |     |
|-------------------------------|-----|
| 3.3 shell命令                   | 45  |
| 3.4 操作apk命令                   | 49  |
| 3.5 进程命令                      | 50  |
| 3.6 本章小结                      | 52  |
| 第4章 so文件格式解析                  | 53  |
| 4.1 ELF文件格式                   | 53  |
| 4.2 解析工具                      | 54  |
| 4.3 解析ELF文件                   | 57  |
| 4.4 验证解析结果                    | 60  |
| 4.5 本章小结                      | 61  |
| 第5章 AndroidManifest.xml文件格式解析 | 62  |
| 5.1 格式分析                      | 62  |
| 5.2 格式解析                      | 63  |
| 5.2.1 解析头部信息                  | 63  |
| 5.2.2 解析String Chunk          | 63  |
| 5.2.3 解析ResourceId Chunk      | 68  |
| 5.2.4 解析Start Namespace Chunk | 70  |
| 5.2.5 解析Start Tag Chunk       | 72  |
| 5.3 本章小结                      | 82  |
| 第6章 resource.arsc文件格式解析       | 83  |
| 6.1 Android中资源文件id格式          | 83  |
| 6.2 数据结构定义                    | 85  |
| 6.2.1 头部信息                    | 85  |
| 6.2.2 资源索引表的头部信息              | 85  |
| 6.2.3 资源项的值字符串资源池             | 86  |
| 6.2.4 Package数据块              | 87  |
| 6.2.5 类型规范数据块                 | 88  |
| 6.2.6 资源类型项数据块                | 89  |
| 6.3 解析代码                      | 93  |
| 6.3.1 解析头部信息                  | 93  |
| 6.3.2 解析资源字符串内容               | 94  |
| 6.3.3 解析包信息                   | 96  |
| 6.3.4 解析资源类型的字符串内容            | 97  |
| 6.3.5 解析资源值字符串内容              | 98  |
| 6.3.6 解析正文内容                  | 99  |
| 6.4 本章小结                      | 105 |
| 第7章 dex文件格式解析                 | 106 |
| 7.1 dex文件格式                   | 106 |
| 7.2 构造dex文件                   | 107 |
| 7.3 解析数据结构                    | 108 |
| 7.3.1 头部信息Header结构            | 108 |
| 7.3.2 string_ids数据结构          | 112 |
| 7.3.3 type_ids数据结构            | 115 |
| 7.3.4 proto_ids数据结构           | 116 |
| 7.3.5 field_ids数据结构           | 118 |
| 7.3.6 method_ids数据结构          | 119 |
| 7.3.7 class_defs数据结构          | 120 |
| 7.4 解析代码                      | 128 |
| 7.4.1 解析头部信息                  | 128 |
| 7.4.2 解析string_ids索引区         | 129 |
| 7.4.3 解析type_ids索引区           | 130 |
| 7.4.4 解析proto_ids索引区          | 130 |
| 7.4.5 解析field_ids索引区          | 131 |
| 7.4.6 解析method_ids索引区         | 132 |

|                                 |     |
|---------------------------------|-----|
| 7.4.7 解析class_def区域             | 132 |
| 7.5 本章小结                        | 134 |
| 防护篇                             |     |
| 第8章 Android应用安全防护的基本策略          | 136 |
| 8.1 混淆机制                        | 136 |
| 8.1.1 代码混淆                      | 136 |
| 8.1.2 资源混淆                      | 136 |
| 8.2 签名保护                        | 138 |
| 8.3 手动注册native方法                | 140 |
| 8.4 反调试检测                       | 144 |
| 8.5 本章小结                        | 145 |
| 第9章 Android中常用权限分析              | 147 |
| 9.1 辅助功能权限                      | 147 |
| 9.2 设备管理权限                      | 148 |
| 9.3 通知栏管理权限                     | 149 |
| 9.4 VPN开发权限                     | 149 |
| 9.5 本章小结                        | 150 |
| 第10章 Android中的run-as命令          | 151 |
| 10.1 命令分析和使用                    | 151 |
| 10.2 Linux中的setuid和setgid概念     | 159 |
| 10.3 Android中setuid和setgid的使用场景 | 162 |
| 10.4 run-as命令的作用                | 165 |
| 10.5 调用系统受uid限制的API             | 166 |
| 10.6 本章小结                       | 168 |
| 第11章 Android中的allowBackup属性     | 169 |
| 11.1 allowBackup属性介绍            | 169 |
| 11.2 如何获取应用隐私数据                 | 170 |
| 11.3 如何恢复应用数据                   | 175 |
| 11.4 本章小结                       | 175 |
| 第12章 Android中的签名机制              | 176 |
| 12.1 基本概念                       | 176 |
| 12.2 Android中签名流程               | 182 |
| 12.3 Android中为何采用这种签名机制         | 191 |
| 12.4 本章小结                       | 192 |
| 第13章 Android应用加固原理              | 193 |
| 13.1 加固原理解析                     | 193 |
| 13.2 案例分析                       | 195 |
| 13.3 运行项目                       | 206 |
| 13.4 本章小结                       | 208 |
| 第14章 Android中的so加固原理            | 209 |
| 14.1 基于对so中的section加密实现so加固     | 209 |
| 14.1.1 技术原理                     | 209 |
| 14.1.2 实现方案                     | 210 |
| 14.1.3 代码实现                     | 210 |
| 14.1.4 总结                       | 220 |
| 14.2 基于对so中的函数加密实现so加固          | 221 |
| 14.2.1 技术原理                     | 221 |
| 14.2.2 实现方案                     | 223 |
| 14.2.3 代码实现                     | 224 |
| 14.3 本章小结                       | 230 |
| 工具篇                             |     |
| 第15章 Android逆向分析基础              | 232 |
| 15.1 逆向工具                       | 232 |

|                                   |     |
|-----------------------------------|-----|
| 15.2 逆向基本知识                       | 233 |
| 15.3 打开系统调试总开关                    | 233 |
| 15.4 本章小结                         | 237 |
| 第16章 反编译神器apktool和Jadx            | 238 |
| 16.1 逆向操作惯例                       | 238 |
| 16.2 反编译常见的问题                     | 238 |
| 16.3 分析apktool的源码                 | 240 |
| 16.4 解决常见问题                       | 249 |
| 16.5 apktool的回编译源码分析              | 254 |
| 16.6 Jadx源码分析                     | 256 |
| 16.7 本章小结                         | 258 |
| 第17章 Hook神器Xposed                 | 259 |
| 17.1 安装教程                         | 259 |
| 17.2 环境搭建                         | 259 |
| 17.3 编写模块功能                       | 260 |
| 17.4 运行模块                         | 264 |
| 17.5 本章小结                         | 265 |
| 第18章 脱壳神器ZjDroid                  | 266 |
| 18.1 ZjDroid原理分析                  | 266 |
| 18.2 工具命令分析                       | 268 |
| 18.3 工具日志信息                       | 272 |
| 18.4 工具用法总结                       | 272 |
| 18.5 工具使用案例                       | 273 |
| 18.6 本章小结                         | 276 |
| 第19章 Native层Hook神器Cydia Substrate | 277 |
| 19.1 环境搭建                         | 277 |
| 19.2 Hook Java层功能                 | 277 |
| 19.3 Hook Native层功能               | 279 |
| 19.4 框架使用事项说明                     | 283 |
| 19.5 本章小结                         | 283 |
| 操作篇                               |     |
| 第20章 静态方式逆向应用                     | 286 |
| 20.1 smali语法                      | 286 |
| 20.2 手动注入smali语句                  | 288 |
| 20.3 ARM指令                        | 288 |
| 20.4 用IDA静态分析so文件                 | 290 |
| 20.5 案例分析                         | 292 |
| 20.5.1 静态分析smali代码                | 292 |
| 20.5.2 静态分析native代码               | 300 |
| 20.6 本章小结                         | 303 |
| 第21章 动态调试smali源码                  | 304 |
| 21.1 动态调试步骤                       | 304 |
| 21.2 案例分析                         | 305 |
| 21.3 本章小结                         | 324 |
| 第22章 IDA工具调试so源码                  | 325 |
| 22.1 IDA中的常用快捷键                   | 325 |
| 22.2 构造so案例                       | 331 |
| 22.3 逆向so文件                       | 332 |
| 22.3.1 获取应用的so文件                  | 332 |
| 22.3.2 用IDA进行调试设置                 | 336 |
| 22.3.3 IDA调试的流程总结                 | 343 |
| 22.4 用IDA解决反调试问题                  | 343 |
| 22.5 本章小结                         | 355 |
| 第23章 逆向加固应用                       | 356 |

|                         |      |
|-------------------------|------|
| 23.1 逆向加固应用的思路          | 356  |
| 23.2 获取解密之后的dex文件       | 359  |
| 23.3 分析解密之后的dex文件内容     | 364  |
| 23.4 逆向方法               | 369  |
| 23.5 逆向测试               | 373  |
| 23.6 逆向加固应用的方法总结        | 374  |
| 23.7 本章小结               | 376  |
| 第24章 逆向应用经典案例分析         | 377  |
| 24.1 加壳原理分析             | 377  |
| 24.2 脱壳过程               | 380  |
| 24.3 如何还原应用             | 393  |
| 24.4 脱壳经验总结             | 394  |
| 24.5 本章小结               | 395  |
| 第25章 Android中常见漏洞分析     | 396  |
| 25.1 解压文件漏洞分析           | 396  |
| 25.1.1 漏洞场景             | 396  |
| 25.1.2 漏洞原因分析           | 398  |
| 25.1.3 漏洞案例分析           | 398  |
| 25.1.4 漏洞修复             | 399  |
| 25.1.5 漏洞总结             | 400  |
| 25.2 录屏授权漏洞分析           | 400  |
| 25.2.1 漏洞场景             | 400  |
| 25.2.2 漏洞原因分析           | 402  |
| 25.2.3 漏洞修复             | 402  |
| 25.2.4 漏洞总结             | 403  |
| 25.3 本章小结               | 403  |
| 第26章 文件加密病毒Wannacry样本分析 | 404  |
| 26.1 病毒样本分析             | 404  |
| 26.2 获取密码               | 405  |
| 26.3 文件解密               | 409  |
| 26.4 病毒分析报告             | 414  |
| 26.5 本章小结               | 414  |
| • • • • •               | (收起) |

[Android应用安全防护和逆向分析\\_下载链接1](#)

## 标签

Android

逆向

安全

Android进阶

计算机

黑客

Security

programming

## 评论

这本书很大一个问题是很多内容作者博客上都有，我也看过很多。当然非常鼓励这种分享精神，但是这样的话写书买书的意义又是何在呢？

-----  
内容比较全，深入还要靠自己吧//逆向大神，Mark

-----  
影印版速读而过。很多已经过时了，而且不够系统不够专业，不建议。

-----  
啰嗦不系统，作者博客大杂烩，看不下去

-----  
详细介绍了在安全领域使用的技术及应对方法

-----  
书里有料，但对初学者不是很友好，新手看非虫的那本好点

-----  
四哥书啊，很多内容都在博客里发表过文章，书中应该算是归纳的内容，重新梳理了一遍，干货满满。其中有so加密和section加密。

-----  
虽然前面有点啰嗦，但是技术并不过时，后面的实践部分相当棒，讲的比较详细。虽然安卓环境安装比较坑，Eclipse之类的环境也被安卓studio替代了，但是努力上手之后，还是很好用的，为我这种逆向小白，指明了安卓逆向的大致方向。作者还有博客以及个人网站，上面有各类知名app的实战教程，很是受用。努力跟着搭好环境，学习技术，最终也是解决了几个实际工作中遇到的需求（虽然实践的时候还需要一些其他的摸索），总之，感谢

-----  
[Android应用安全防护和逆向分析\\_下载链接1](#)

书评

-----  
[Android应用安全防护和逆向分析\\_下载链接1](#)