

# 《Android系统安全和反编译实战》

## 图书基本信息

书名：《Android系统安全和反编译实战》

13位ISBN编号：9787115393036

出版时间：2015-8-1

作者：杨峻

页数：529

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：[www.tushu000.com](http://www.tushu000.com)

# 《Android系统安全和反编译实战》

## 内容概要

《Android系统安全和反编译实战》循序渐进地讲解了Android系统安全方面的基本知识，从Android系统介绍开始到综合实例的实战过程，全程剖析了Android系统安全、应用安全开发和加密、解密方面的核心知识。全书共17章，主要内容包括，Android技术核心框架分析、获取并编译源代码、Android系统的安全机制、内存安全机制、Binder通信安全机制、Android虚拟机基础、Dalvik VM的运作流程、DEX文件详解、编写安全的应用程序、应用安全策略、文件加密、电话系统的安全机制、短信系统的安全机制、网络防火墙系统、文件加密系统等核心技术。

《Android系统安全和反编译实战》适合Android初学者、Android应用开发者、Android安全架构研究人员、Android底层开发人员和Android源代码分析人员学习，也可以作为相关培训学校和大专院校相关专业的教学用书。

## 书籍目录

### 第1章 Android技术概述

1

#### 1.1 智能手机系统介绍

1

#### 1.2 搭建Android应用开发环境

2

##### 1.2.1 安装Android SDK的系统要求

2

##### 1.2.2 安装JDK

2

##### 1.2.3 获取并安装Eclipse和Android SDK

5

##### 1.2.4 安装ADT

7

##### 1.2.5 设定Android SDK Home

8

##### 1.2.6 验证开发环境

9

##### 1.2.7 创建Android虚拟设备 (AVD)

9

##### 1.2.8 启动AVD模拟器

10

##### 1.2.9 解决搭建环境过程中的常见问题

12

### 第2章 Android技术核心框架分析

15

#### 2.1 简析Android安装文件

15

##### 2.1.1 Android SDK目录结构

15

##### 2.1.2 android.jar及内部结构

16

##### 2.1.3 阅读SDK帮助文档

16

##### 2.1.4 常用的SDK工具

17

#### 2.2 演示官方实例

19

#### 2.3 剖析Android系统架构

23

##### 2.3.1 Android体系结构介绍

23

##### 2.3.2 Android应用工程文件组成

25

## 2.4 简述五大组件

27

### 2.4.1 用Activity来表现界面

27

### 2.4.2 用Intent和Intent Filters

实现切换

28

### 2.4.3 Service为你服务

28

### 2.4.4 用Broadcast Intent/Receiver发送广播

29

### 2.4.5 用Content Provider

存储数据

29

## 2.5 进程和线程

29

### 2.5.1 先看进程

29

### 2.5.2 再看线程

30

### 2.5.3 应用程序的生命周期

30

## 第3章 获取并编译源码

33

### 3.1 在Linux系统中获取

Android源码

33

### 3.2 在Windows平台获取

Android源码

34

### 3.3 分析Android源码结构

36

#### 3.3.1 应用程序

38

#### 3.3.2 应用程序框架

39

#### 3.3.3 系统服务

39

#### 3.3.4 系统程序库

41

#### 3.3.5 系统运行库

44

#### 3.3.6 硬件抽象层

44

## 3.4 编译源码

45

### 3.4.1 搭建编译环境

46

3.4.2 开始编译	46
3.4.3 在模拟器中运行	47
3.4.4 常见的错误分析	48
3.4.5 实践演练——演示两种编译Android程序的方法	49
3.5 编译Android Kernel	52
3.5.1 获取Goldfish内核代码	52
3.5.2 获取MSM内核代码	55
3.5.3 获取OMAP内核代码	55
3.5.4 编译Android的Linux内核	55
3.6 编译源码生成SDK	57
第4章 Android系统的安全机制	61
4.1 Android安全机制概述	61
4.1.1 Android的安全机制模型	61
4.1.2 Android的安全框架概述	62
4.2 分析Linux系统的安全机制	63
4.2.1 Linux用户权限基础	63
4.2.2 进程	68
4.3 分析Android系统的安全机制	70
4.3.1 沙箱模型介绍	70
4.3.2 应用程序的安全机制	72
4.3.3 分区加载机制	73
第5章 内存安全机制——匿名共享内存系统	74
5.1 分析Ashmem驱动程序	74

5.1.1 基础数据结构	74
5.1.2 初始化处理	75
5.1.3 打开匿名共享内存 设备文件	76
5.1.4 内存映射	78
5.1.5 实现读写操作	79
5.1.6 锁定和解锁	81
5.1.7 回收内存块	86
5.2 分析C++访问接口层	87
5.2.1 接口MemoryBase	87
5.2.2 客户端实现	90
5.2.3 接口MemoryBase	94
5.3 分析Java访问接口层	97
5.4 内存优化机制	100
5.4.1 sp和wp简析	100
5.4.2 详解智能指针	102
5.5 Android内存系统的安全 机制分析	118
5.5.1 Ashmem匿名共享内存 的机理	119
5.5.2 使用Low Memory Killer 机制实现安全和高效	119
第6章 Binder通信安全机制（上）	121
6.1 Binder机制基础	121
6.1.1 选择Binder机制的 原因——简洁快速、 低耗内存、更加安全	121
6.1.2 Binder安全机制的	

必要性	122
6.1.3 Android的进程间通信 ( IPC ) 机制Binder	122
6.1.4 Service Manager是Binder 机制的上下文管理者	123
6.1.5 Service Manager服务	137
6.2 分析Binder驱动程序	140
6.2.1 分析数据结构	140
6.2.2 分析设备初始化	150
6.2.3 打开Binder设备文件	151
6.2.4 内存映射	152
6.2.5 释放物理页面	156
6.2.6 分配内核缓冲区	157
6.2.7 释放内核缓冲区	158
6.2.8 查询内核缓冲区	160
第7章 Binder通信安全机制 ( 下 )	162
7.1 Binder封装库	162
7.1.1 类BBinder	163
7.1.2 类BpRefBase	165
7.1.3 类IPCThreadState	166
7.2 初始化Java层Binder框架	168
7.3 分析MediaServer的通信机制	170
7.3.1 MediaServer的入口函数	170
7.3.2 ProcessState	171
7.3.3 defaultServiceManager	173
7.3.4 注册MediaPlayerService	

179	
7.3.5	分析StartThread Pool和 join Thread Pool
188	
7.4	总结进程通信机制的安全性
190	
7.4.1	进程先线程安全
190	
7.4.2	远程过程调用机制 ( RPC )
191	
7.4.3	实现线程安全方法
192	
7.4.4	Binder中的安全策略
193	
第8章	Android虚拟机基础
194	
8.1	Dalvik VM和JVM的差异
194	
8.2	Dalvik虚拟机的主要特征
195	
8.3	Dalvik VM架构
196	
8.3.1	Dalvik虚拟机的代码结构
196	
8.3.2	dx工具
198	
8.3.3	Dalvik VM的进程管理
198	
8.3.4	Android的初始化流程
198	
8.4	Dalvik VM控制VM命令详解
199	
8.4.1	基本命令
199	
8.4.2	扩展的JNI检测
199	
8.4.3	断言
200	
8.4.4	字节码校验和优化
200	
8.4.5	Dalvik VM的运行模式
201	
8.4.6	死锁预测
201	
8.4.7	dump堆栈追踪
202	
8.4.8	dex文件和校验
202	

8.4.9 产生标志位	202
8.5 Dalvik VM进程管理	202
8.5.1 Zygote基础	202
8.5.2 Dalvik的进程模型	211
8.5.3 Dalvik的进程通信	215
8.6 Zygote（孕育）进程	218
8.6.1 Zygote基础	218
8.6.2 分析Zygote的启动过程	219
第9章 Dalvik VM的运作流程	233
9.1 Dalvik VM相关的可执行程序	233
9.1.1 dalvikvm、dvz和app_process简介	233
9.1.2 对比app_process和dalvikvm的执行过程	234
9.2 初始化Dalvik VM	236
9.2.1 开始虚拟机的准备工作	236
9.2.2 初始化跟踪显示系统	237
9.2.3 初始化垃圾回收器	237
9.2.4 初始化线程列表和主线程环境参数	237
9.2.5 分配内部操作方法的表格内存	238
9.2.6 初始化虚拟机的指令码相关的内容	238
9.2.7 分配指令寄存器状态的内存	239
9.2.8 分配指令寄存器状态的内存和最基本用的Java库	

239	
9.2.9 初始化使用的Java类库	
线程类	
240	
9.2.10 初始化虚拟机使用的	
异常Java类库	
241	
9.2.11 初始化其他对象	
242	
9.3 启动Zygote	
250	
9.3.1 在init.rc中配置zygote	
启动参数	
250	
9.3.2 启动Socket服务端口	
250	
9.3.3 加载preload-classes	
251	
9.3.4 加载preload-resources	
252	
.....	
第10章 DEX文件详解	
第11章 编写安全的应用程序	
第12章 应用安全策略	
第13章 文件加密	
第14章 电话系统的安全机制	
第15章 短信系统的安全机制	
第16章 网络防火墙系统实现	
第17章 文件加密系统实现	

# 《Android系统安全和反编译实战》

## 版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:[www.tushu000.com](http://www.tushu000.com)