

《iOS应用逆向工程：分析与实战》

图书基本信息

书名：《iOS应用逆向工程：分析与实战》

13位ISBN编号：9787111450726

10位ISBN编号：7111450728

出版时间：2014-1-20

出版社：机械工业出版社

作者：沙梓社,吴航,刘瑾

页数：265

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.tushu111.com

《iOS应用逆向工程：分析与实战》

内容概要

《ios应用逆向工程：分析与实战》是ios应用逆向工程方面的权威著作，三位作者都是ios领域内的专家，拥有扎实的理论知识和丰富的实践经验。本书内容以工具+代码的形式全面、系统地展开知识点，由浅入深，图文并茂地带着读者一步步探索常规ios app之外的世界。

《ios应用逆向工程：分析与实战》分为四大部分，分别是概念、工具、理论和实战。前三部分介绍ios逆向分析领域的背景、知识体系，以及相应的工具集、理论知识；第四部分则通过4个实际案例来将前面的知识以实战的方式展开。第一部分为概念篇，简单介绍ios逆向分析的概念以及ios平台系统架构。第二部分为工具篇，介绍一系列基于mac和ios平台的配套工具，并且重点讲解其中的class-dump、theos、reveal、ida、gdb等5个工具的使用方法，前3个侧重于使用，后2个侧重于分析。第三部分为理论篇，主要讲述ios逆向/越狱方向的进阶必备理论知识。第四部分为实战篇，通过对3个app store app及1个系统app进行逆向分析的实战操作，让读者能够了解并同步实践已掌握的知识。

书籍目录

《ios应用逆向工程：分析与实战》	
推荐序一	
推荐序二	
自序	
前言	
第一部分 概念篇	
第1章 ios 逆向工程简介 2	
1.1 ios 软件逆向工程的要求 2	
1.2 ios 软件逆向工程的作用 2	
1.2.1 与安全相关的ios 逆向工程 4	
1.2.2 与开发相关的ios 逆向工程 5	
1.3 ios 软件逆向工程的一般过程 6	
1.3.1 系统分析 7	
1.3.2 代码分析 7	
1.4 ios 软件逆向工程用到的工具 8	
1.4.1 监测工具 8	
1.4.2 开发工具 9	
1.4.3 反编译器 9	
1.4.4 调试器 10	
1.5 小结 11	
第2章 越狱ios 平台简介 12	
2.1 ios 系统架构 12	
2.1.1 ios 目录结构 13	
2.1.2 ios 文件权限 15	
2.2 ios 程序类型 16	
2.2.1 application 16	
2.2.2 dynamic library 19	
2.2.3 daemon 19	
2.3 小结 20	
第二部分 工具篇	
第3章 mac 工具集 22	
3.1 class-dump 22	
3.1.1 class-dump 介绍及下载 22	
3.1.2 class-dump 使用演示 23	
3.1.3 关于class-dump 的补充说明 25	
3.2 theos 25	
3.2.1 theos 简介 25	
3.2.2 theos 安装及编译 26	
3.2.3 theos 用法简介 28	
3.2.4 theos 开发tweak 示例 47	
3.3 reveal 49	
3.3.1 reveal 简介 49	
3.3.2 reveal 安装及功能扩展 50	
3.4 ida 55	
3.4.1 ida 简介 55	
3.4.2 ida 使用说明 56	
3.4.3 ida 分析示例 65	

- 3.5 其他工具 68
 - 3.5.1 itools 68
 - 3.5.2 dyld_decache 69
 - 3.5.3 mesasqlite 69
- 3.6 小结 70
- 第4章 ios 工具集 71
 - 4.1 sbsettings 71
 - 4.2 mobilesubstrate 72
 - 4.3 openssh 73
 - 4.4 gdb 74
 - 4.4.1 gdb 简介 74
 - 4.4.2 gdb 的使用说明 74
 - 4.5 cycript 85
 - 4.6 其他常用工具 88
 - 4.6.1 bigboss recommendedtools 88
 - 4.6.2 appcrackr 88
 - 4.6.3 ifile 89
 - 4.6.4 mobileterminal 89
 - 4.6.5 vi improved 90
 - 4.6.6 sqlite 90
 - 4.6.7 top 91
 - 4.6.8 syslogd 92
 - 4.7 小结 92
- 第三部分 理论篇
- 第5章 objective-c 相关的ios逆向理论基础 94
 - 5.1 tweak 的作用原理 94
 - 5.1.1 objective-c 语言的特性 94
 - 5.1.2 mobilesubstrate 96
 - 5.2 tweak 的编写套路 97
 - 5.2.1 灵感的来源 98
 - 5.2.2 分析文件，寻找切入点 99
 - 5.2.3 定位目标函数 102
 - 5.2.4 测试函数功能 104
 - 5.2.5 解析函数参数 105
 - 5.2.6 class-dump 的局限性 108
 - 5.3 实例演示 108
 - 5.3.1 得到灵感 108
 - 5.3.2 分析文件 109
 - 5.3.3 定位函数 115
 - 5.3.4 测试函数 117
 - 5.3.5 编写实例代码 117
 - 5.4 小结 119
- 第6章 arm 汇编相关的ios逆向理论基础 120
 - 6.1 arm 汇编基础 120
 - 6.1.1 基本概念 121
 - 6.1.2 arm/thumb 指令解读 123
 - 6.1.3 arm 调用规则 129
 - 6.2 在ida 中分析目标文件 131
 - 6.2.1 分析函数实现细节 132

- 6.2.2 验证分析结果 139
- 6.3 在gdb中分析目标文件 142
 - 6.3.1 跟踪代码执行流程 142
 - 6.3.2 动态更改代码 147
- 6.4 小结 157
- 第四部分 实战篇
- 第7章 实战1：去除oplayerlite的广告 160
 - 7.1 oplayer lite 简介 160
 - 7.2 分析源代码结构，并定位广告横幅的代码 161
 - 7.2.1 class-dump 获取.h文件 161
 - 7.2.2 猜测广告横幅的出现位置 161
 - 7.2.3 分析playviewController.h 162
 - 7.3 去除广告横幅，节省流量 167
 - 7.3.1 找到“准备”广告的位置 167
 - 7.3.2 追溯到网络连接的起点 173
 - 7.4 编写调试代码 175
 - 7.4.1 编写tweak_oplayerlite.xml 175
 - 7.4.2 编辑control 176
 - 7.4.3 编辑removeoplayerads.plist 176
 - 7.4.4 编辑makefile 177
 - 7.4.5 编译+打包 177
 - 7.4.6 安装 177
 - 7.5 调试去广告插件 177
 - 7.6 代码结果整理 178
 - 7.7 小结 179
- 第8章 实战2：whatsapp消息拦截 180
 - 8.1 whatsapp 简介 180
 - 8.2 分析源代码结构，并定位监听点 180
 - 8.2.1 class-dump 获取.h文件 180
 - 8.2.2 导入xcode 182
 - 8.2.3 找到whatsappAppDelegate 182
 - 8.2.4 找到chatmanager 183
 - 8.3 编写调试代码 184
 - 8.3.1 分析函数列表 184
 - 8.3.2 编写tweak_whatsapp.xml 185
 - 8.3.3 编辑control 186
 - 8.3.4 编辑monitor.plist 186
 - 8.3.5 编辑makefile 186
 - 8.3.6 编译+打包 187
 - 8.3.7 安装 187
 - 8.4 调试运行监听插件 187
 - 8.4.1 运行whatsapp，ssh连接 187
 - 8.4.2 发送/接收消息，监控日志 188
 - 8.4.3 保存数据 189
 - 8.5 代码结果整理 194
 - 8.6 小结 195
- 第9章 实战3：instagram图片保存 196
 - 9.1 instagram 简介 196
 - 9.2 分析源代码结构，并定位图片展示点 196

- 9.2.1 用class-dump获取.h文件 196
- 9.2.2 导入xcode 198
- 9.2.3 找到appdelegate 198
- 9.2.4 注入reveal 199
- 9.2.5 寻找图片页相关class 200
- 9.3 保存图片 205
 - 9.3.1 尝试保存图片 205
 - 9.3.2 对.h文件进行瘦身 206
 - 9.3.3 编译测试 208
- 9.4 弹出提示菜单 208
 - 9.4.1 弹出菜单代码 208
 - 9.4.2 使用theos新增函数 210
 - 9.4.3 使用runtime新增函数 211
- 9.5 代码结果整理 214
- 9.6 小结 215
- 第10章 实战4：ios电话操作 216
 - 10.1 常用电话操作 216
 - 10.2 分析源代码结构，并定位电话操作的代码 216
 - 10.2.1 class-dump获取.h文件 216
 - 10.2.2 寻找拨打电话的函数 217
 - 10.2.3 寻找接听电话的函数 229
 - 10.2.4 寻找挂断电话的函数 234
 - 10.2.5 寻找删除通话记录的函数 236
 - 10.2.6 寻找拦截电话的方法 238
 - 10.3 编写调试代码 250
 - 10.3.1 编写tweak_phoneoperation.xml 250
 - 10.3.2 编辑control 254
 - 10.3.3 编辑phoneoperation.plist 255
 - 10.3.4 编辑makefile 255
 - 10.3.5 编译+打包+安装 255
 - 10.4 调试电话操作插件 255
 - 10.5 代码结果整理 257
 - 10.6 小结 257
- 越狱开发一览 258
- 沙箱逃脱 263
- 编写tweak——新时代的hacking 265

精彩短评

- 1、看似厚厚的一书，其实有很多是逆向过程的代码片段，颇有占位置凑页数之嫌。不过书写的不错，庖丁解牛，看的很过瘾。
- 2、手机越狱，安装相关工具，分析APP，hook 某些函数，做出相关插件，适合越狱开发者，个人对这种越狱插件开发没兴趣，但是通过逆向去分析一些优秀APP的架构还是不错的。倒是建议以加强APP的安全为方向，讲解一些代码混淆、加解密、反逆向的技术点，这样才有看头！
- 3、还不错，介绍了不少工具
- 4、逆向的第一本书
- 5、涉及底层细节不多 但是 适合初学者 指了个方向
- 6、我原本以为这本书是来教我反编译，我能看到优秀app的源代码，代码架构，实现方式，感觉是选错了。Sandbox还是太强大了。逆向，原来是对原来的应用进行修改，重新打包成deb的过程，或者利用越狱开发工具开发然后打包成deb的过程。主要适用于越狱开发者。
- 7、入门读物，class_dumper阶段
- 8、确实如之前的评论所说，术多道少，但是这个时间点，内容已经算十分时髦。但是反而也能观之，IT万变不离其宗，归根到底就还是C和Unix，再同时看看《深入理解计算机系统》和《Unix环境高级编程》会受益匪浅！——写于巴萨中场3：0奥萨苏纳的半场休息
- 9、应该说是从“术”的角度来将iOS逆向入门的基础，对系统底层有一定了解（非理解）的人就可以读，不难。如果读者有汇编基础或者ARM体系结构方面基础，那读起来将相对轻松好懂一些。
- 10、列出了很多东西
- 11、基本上都是干货，明显地感觉到实战派与学院派所著书之差异，书中的内容足于为略知iOS开发的人员进行tweak开发引路，不足之处在于实战派的作者们大量篇幅描述tweak的分析与开发过程，实际这个过程可以百花齐放，如果能对这个过程能在理论上进行总结，提出一套论就更好，总的来说是好书，只是有些重术轻道。

《iOS应用逆向工程：分析与实战》

精彩书评

1、这绝对不是一本将官方文档Copy过来的所谓的”快速入门指南“这绝对不是一本不接地气夸夸其谈实际上啥内容都没有的所谓的马桶读物这是一本难得的由国内的作者写的有很多干货的经典参考逆向工程、反编译、破/解对于很多开发者同学们都比较神秘且具有非常强大的吸引力。作者通过一个个实例介绍了整套流程，深浅适当。不过！！！！！！书的纸张质量实在配不上这内容啊！！

《iOS应用逆向工程：分析与实战》

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.tushu111.com