

# 《iOS应用逆向工程 第2版》

## 图书基本信息

书名：《iOS应用逆向工程 第2版》

13位ISBN编号：9787111494369

出版时间：2015-4-1

作者：沙梓社,吴航

页数：386

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](http://www.tushu111.com)

# 《iOS应用逆向工程 第2版》

## 内容概要

你是否曾因应用上线的第一天即遭破解而无奈苦恼，想要加以防范，却又束手无策？

你是否曾为某一应用深深折服，想要借鉴学习，却又无从下手？

你是否已不满足于public API，想要进军Cydia开发，却又求学无门？

你是否已产生“不识Apple真面目，只缘身在App Store中”的危机感，想要通过阅读来一窥这冰山一角外的整个北极，却又找不到合适的书？

你是否已经因无法跨越开发路上的重重障碍而断了研究iOS逆向工程的念头？Are you a quitter？看完本书，相信你会有全新的感受！

全球第一本讲解iOS8应用逆向工程的实战手册，作者毫无保留地分享了数年来在iOS逆向工程领域的经验。

内容系统深入，逻辑紧密，实战性强，从iOS系统架构等理论出发，以多个实例贯穿全书，阐述class-dump、Theos、Cycrypt、Reveal、IDA、LLDB等常用工具的使用，通俗易懂。

总结提炼出一套从UI观察切入代码分析的iOS应用逆向工程方法论，授人以渔。

# 《iOS应用逆向工程 第2版》

## 作者简介

沙梓社，iOS越狱社区骨灰级活跃份子，思路开阔思想传统，对苹果的研究痴迷到连女朋友都没有的地步。作品见诸于Cydia，有SMSNinja、LowPowerBanner、DimInCall等。

吴航，十余年程序开发经验的资深码农，历经方正、NEC、Juniper等国内国外知名IT企业，2011年进入iOS领域，专注于iOS app/逆向等方向的开发，主要作品有安全管家、知乎月刊HD等。

## 书籍目录

推荐序一	
推荐序二	
第2版序	
第1版序	
前言	
第一部分 概念篇	
第1章 iOS逆向工程简介 3	
1.1 iOS逆向工程的要求 3	
1.2 iOS应用逆向工程的作用 4	
1.2.1 安全相关的iOS逆向工程 5	
1.2.2 开发相关的iOS逆向工程 6	
1.3 iOS应用逆向工程的过程 7	
1.3.1 系统分析 7	
1.3.2 代码分析 8	
1.4 iOS应用逆向工程的工具 8	
1.4.1 监测工具 9	
1.4.2 反汇编工具 9	
1.4.3 调试工具 10	
1.4.4 开发工具 11	
1.5 小结 11	
第2章 越狱iOS平台简介 12	
2.1 iOS系统结构 12	
2.1.1 iOS目录结构简介 13	
2.1.2 iOS文件权限简介 16	
2.2 iOS二进制文件类型 17	
2.2.1 Application 17	
2.2.2 Dynamic Library 20	
2.2.3 Daemon 20	
2.3 小结 22	
第二部分 工具篇	
第3章 OSX工具集 25	
3.1 class-dump 25	
3.2 Theos 27	
3.2.1 Theos简介 27	
3.2.2 安装Theos 28	
3.2.3 Theos用法介绍 30	
3.2.4 Theos开发tweak示例 51	
3.3 Reveal 53	
3.4 IDA 57	
3.4.1 IDA简介 57	
3.4.2 IDA使用说明 58	
3.4.3 IDA分析示例 68	
3.5 iFunBox 71	
3.6 dyld_decache 72	
3.7 小结 73	
第4章 iOS工具集 74	
4.1 CydiaSubstrate 74	

- 4.1.1 MobileHooker 74
- 4.1.2 MobileLoader 84
- 4.1.3 Safe mode 84
- 4.2 Ccrypt 85
- 4.3 LLDB与debugserver 89
  - 4.3.1 LLDB简介 89
  - 4.3.2 debugserver简介 90
  - 4.3.3 配置debugserver 90
  - 4.3.4 用debugserver启动或附加进程 91
  - 4.3.5 LLDB的使用说明 92
  - 4.3.6 LLDB使用小提示 107
- 4.4 dumpdecrypted 107
- 4.5 OpenSSH 111
- 4.6 usbmuxd 112
- 4.7 iFile 113
- 4.8 MTerminal 114
- 4.9 syslogd to /var/log/syslog 115
- 4.10 小结 115
- 第三部分 理论篇
- 第5章 Objective-C相关的iOS逆向理论基础 119
  - 5.1 tweak在Objective-C中的工作方式 119
  - 5.2 tweak的编写套路 121
    - 5.2.1 寻找灵感 121
    - 5.2.2 定位目标文件 123
    - 5.2.3 定位目标函数 127
    - 5.2.4 测试函数功能 129
    - 5.2.5 解析函数参数 130
    - 5.2.6 class-dump的局限性 133
  - 5.3 实例演示 133
    - 5.3.1 得到灵感 134
    - 5.3.2 定位文件 135
    - 5.3.3 定位函数 143
    - 5.3.4 测试函数 145
    - 5.3.5 编写实例代码 145
  - 5.4 小结 147
- 第6章 ARM汇编相关的iOS逆向理论基础 148
  - 6.1 ARM汇编基础 148
    - 6.1.1 基本概念 149
    - 6.1.2 ARM/THUMB指令解读 152
    - 6.1.3 ARM调用规则 159
  - 6.2 tweak的编写套路 161
    - 6.2.1 从现象切入App, 找出UI函数 162
    - 6.2.2 以UI函数为起点, 寻找目标函数 173
  - 6.3 LLDB的使用技巧 203
    - 6.3.1 寻找函数调用者 203
    - 6.3.2 更改进程执行逻辑 208
  - 6.4 小结 211
- 第四部分 实战篇
- 第7章 实战1: Characount for Notes 8 215

- 7.1 备忘录 215
- 7.2 搭建tweak原型 216
  - 7.2.1 定位Notes的可执行文件 217
  - 7.2.2 class-dump出MobileNotes的头文件 218
  - 7.2.3 用Cycrypt找到浏览界面及其controller 218
  - 7.2.4 从NoteDisplayController找到当前note对象 220
  - 7.2.5 找到实时监测note内容变化的方法 223
- 7.3 逆向结果整理 227
- 7.4 编写tweak 228
  - 7.4.1 用Theos新建tweak工程“ CharacountForNotes8 ” 228
  - 7.4.2 构造CharacountForNotes8.h 229
  - 7.4.3 编辑Tweak.xml 229
  - 7.4.4 编辑Makefile及control 230
  - 7.4.5 测试 230
- 7.5 小结 233
- 第8章 实战2：自动将指定电子邮件标记为已读 234
  - 8.1 电子邮件 234
  - 8.2 搭建tweak原型 235
    - 8.2.1 定位Mail的可执行文件并class-dump它 237
    - 8.2.2 把头文件导入Xcode 238
    - 8.2.3 用Cycrypt找到Mailboxes界面的controller 239
    - 8.2.4 用Reveal和Cycrypt找到All Inboxes界面的delegate 240
    - 8.2.5 在MailboxContentViewController中定位“刷新完成”的响应函数 242
    - 8.2.6 从MessageMegaMail中拿到所有邮件 246
    - 8.2.7 从MFLibraryMessage中提取发件人地址，用MessageMegaMail标记已读 248
  - 8.3 逆向结果整理 254
  - 8.4 编写tweak 255
    - 8.4.1 用Theos新建tweak工程“ iOSREMailMarker ” 255
    - 8.4.2 构造iOSREMailMarker.h 255
    - 8.4.3 编辑Tweak.xml 256
    - 8.4.4 编辑Makefile及control 257
    - 8.4.5 测试 258
  - 8.5 小结 259
- 第9章 实战3：保存与分享微信小视频 260
  - 9.1 微信 260
  - 9.2 搭建tweak原型 261
    - 9.2.1 观察小视频播放窗口，寻找逆向切入点 261
    - 9.2.2 class-dump获取头文件 262
    - 9.2.3 把头文件导入Xcode 263
    - 9.2.4 用Reveal找到小视频播放窗口 264
    - 9.2.5 找到长按手势响应函数 265
    - 9.2.6 用Cycrypt定位小视频的controller 270
    - 9.2.7 从WCTimeLineViewController找到小视频对象 272
    - 9.2.8 从WCContentItemViewTemplateNewSight中提取WCDataItem对象 276
    - 9.2.9 从WCDataItem中提取目标信息 278
  - 9.3 逆向结果整理 288
  - 9.4 编写tweak 289
    - 9.4.1 用Theos新建tweak工程“ iOSREWVideoDownloader ” 289

- 9.4.2 构造iOSREWCVideoDownloader.h 289
- 9.4.3 编辑Tweak.xml 290
- 9.4.4 编辑Makefile及control 292
- 9.4.5 测试 293
- 9.5 彩蛋放送 294
  - 9.5.1 从UIMenuItem切入，找到小视频对象 294
  - 9.5.2 微信历史版本头文件个数变迁 295
- 9.6 小结 298
- 第10章 实战4：检测与发送iMessage 299
  - 10.1 iMessage 299
  - 10.2 检测一个号码或邮箱地址是否支持iMessage 299
    - 10.2.1 观察MobileSMS界面元素的变化，寻找逆向切入点 299
    - 10.2.2 用Cycrypt找出placeholder 302
    - 10.2.3 用IDA和LLDB找出placeholderText的一重数据源 308
    - 10.2.4 用IDA和LLDB找出placeholderText的N重数据源 311
    - 10.2.5 还原原始数据源生成placeholderText的过程 340
  - 10.3 发送iMessage 341
    - 10.3.1 从MobileSMS界面元素寻找逆向切入点 341
    - 10.3.2 用Cycrypt找出“Send”按钮的响应函数 342
    - 10.3.3 在响应函数中寻找可疑的发送操作 344
  - 10.4 逆向结果整理 369
  - 10.5 编写tweak 370
    - 10.5.1 用Theos新建tweak工程“iOSREMadridMessenger” 370
    - 10.5.2 构造iOSREMadridMessenger.h 371
    - 10.5.3 编辑Tweak.xml 372
    - 10.5.4 编辑Makefile及control 372
    - 10.5.5 用Cycrypt测试 373
  - 10.6 小结 373
- 越狱开发一览 375
- 沙箱逃脱 380
- 编写tweak——新时代的hacking 382

# 《iOS应用逆向工程 第2版》

## 精彩短评

- 1、简直不能太赞
- 2、真心不错，大大开阔了眼界，前提是有个IOS 8的越狱机器
- 3、逆向原理很有意思，基本上学会了就是一个套路，但最关键的还是逆向的思路以及汇编分析基础。多观察常用的app，自己写个好玩的tweak
- 4、干货很多，iOS逆向工程非常好的入门书籍。
- 5、打开了新世界的大门，拿到app就可以看到各种功能是怎么实现的



## 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](http://www.tushu111.com)