

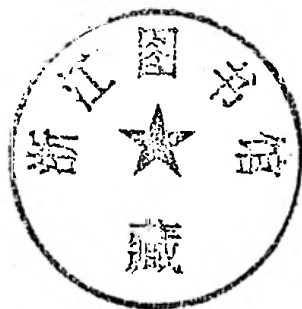


ZT000013692413 9



iOS应用 逆向与安全

刘培庆 / 著



电子工业出版社

Publishing House of Electronics Industry

北京·BEIJING

内 容 简 介

本书从正向开发、工具的使用、逆向实战及安全保护等方面,对 iOS 应用的逆向与安全进行了讲解。本书内容包括基本概念、逆向环境的准备、常用逆向分析工具、类的结构、App 签名、Mach-O 文件格式、hook 原理等,并通过在越狱平台和非越狱平台上的逆向分析实例,带领读者学习逆向分析的思路和方法。在应用安全及保护方面,本书内容涉及网络传输、安全检测、代码混淆等。

本书适合高校计算机相关专业的学生、iOS 开发工程师、逆向工程师、越狱开发工程师、iOS 安全工程师及应用安全审计人员阅读参考。

未经许可,不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有,侵权必究。

图书在版编目(CIP)数据

iOS 应用逆向与安全 / 刘培庆著. —北京:电子工业出版社, 2018.6

(安全技术大系)

ISBN 978-7-121-34099-4

I. ①i… II. ①刘… III. ①移动终端—应用程序—程序设计—安全技术 IV. ①TN929.53

中国版本图书馆 CIP 数据核字(2018)第 081246 号

策划编辑:潘 昕

责任编辑:潘 昕

印 刷:三河市君旺印务有限公司

装 订:三河市君旺印务有限公司

出版发行:电子工业出版社

北京市海淀区万寿路 173 信箱 邮编 100036

开 本:787×980 1/16 印张:25.25 字数:535 千字

版 次:2018 年 6 月第 1 版

印 次:2018 年 6 月第 1 次印刷

定 价:85.00 元

凡所购买电子工业出版社图书有缺损问题,请向购买书店调换。若书店售缺,请与本社发行部联系,联系及邮购电话:(010) 88254888。

质量投诉请发邮件至 zltz@phei.com.cn, 盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式:(010) 51260888-819, faq@phei.com.cn。

推荐序

第一次和刘培庆见面是在 2017 年，西湖大道的碧桃小馆。

四月的杭州已是初夏，只穿一件单衣的我，后背仍被汗水浸湿。昏暗的餐厅里，刘培庆坐在角落，一件牛仔夹克扣到顶，看上去又闷又热。我眉头一皱，心生不悦：这人真傻。

高温败了胃口，团购的双人餐，俩大老爷们儿竟然没吃完。结账走人，我们在涌金门一带的巷弄里穿行消食，有一搭没一搭地聊着。刘培庆说，他放弃了晋升的机会，跳到了另一个更辛苦的部门，是因为新部门的业务更吸引他。放弃更舒适的环境和更高的薪水去追求兴趣？兴趣值几个钱？这人真傻。

是夜一别，我们各自忙于生活，很久没有再会。五月某天，微信上突然弹出刘培庆的名字，“狗神，你那本书有没有打算再出一版，帮你更新一下”，然后向我介绍了他的更新计划，原来是在《iOS 应用逆向工程》的基础上更深入了。我觉得他的内容定位有些超出原书目标读者的水平，于是建议他当作技术博客发出来，算是委婉的回绝。你的原创内容，放在我的书里，如果广受欢迎，名气岂不全让我赚了？这人真傻。

七月的艳阳炙烤着大地，室内活动陡然增多。我要去滨江的 HZEcers 英语角分享出书经历，地点恰好就在网易旁边，于是邀请了他。没想到这哥们儿把女朋友带了来，两人在活动中一前一后，紧张地用生涩的英语做自我介绍：“Good afternoon everyone, my name is Liu Peiqing...” 他的生物专业小女友梳着齐刘海，戴着圆框眼镜，英语比他溜得多：“...recently I'm learning programming, because I want to have more common topics with my boyfriend...” 单纯的出发点，真是傻得可爱。也只有这样的傻姑娘，才会爱上这样的傻小子吧？

没过多久，我的论坛上出现了一个名为 MonkeyDev 的工具，是刘培庆写的，号称“原有 iOSOpenDev 的升级，非越狱插件开发集成神器”。我大致浏览了一下，看上去挺复杂，技术含量挺高，但竟然是开源的?! 从 Git 提交记录来看，刘培庆一直在花时间维护它，免费供大家使用。这个年头，还有这样的雷锋，做这样的好事？这人真傻。

金秋十月，刘培庆又在微信上找我，说他要出书了，邀请我写个序。坦白地说，以刘培庆、

James 等 90 后为代表的新一代 iOS 逆向工程师鼓捣出来的新技术，我其实看不懂，也跟不上；同时，因为对库克的失望，我早已不再往苹果系技术上投入更多的精力。我已然从原来技术舞台的主角沦为了看客。“后浪”竟然找已经“死在沙滩上”的“前浪”写序？这人真傻。

但是，傻子刘培庆就在这样的评价中朝着自己的目标一步步前进，最终写出了《iOS 应用逆向与安全》，推动了行业的发展。

他让我想起了行业内的其他傻子。

四年前，另一个傻子，不知天高地厚地出版了《iOS 应用逆向工程》，填补了市场的空白，受到了读者的欢迎。这个傻子办了个名叫 iOSRE 的论坛，为所有 iOS 逆向工程爱好者提供免费、自由、平等、纯净的交流平台，却不做广告、不收赞助，自掏腰包维护论坛。这人真傻。

一个来自加拿大的傻子，为越狱 iOS 写了个名叫 Activator 的插件，全球总下载量近 2 亿次——据说这是乔布斯最喜爱的越狱插件。如果每次下载只收 1 毛钱，这个傻子也能成为千万富翁，可是他却把 Activator 免费提供给大家使用。这人真傻。

一个大学辍学的美国傻子，为越狱 iOS 提供了一套名为 Theos 的开发工具，它的简单易用吸引了大量人才进入这个领域，为越狱开发的黄金 5 年揭开了序幕。为了维护这套免费、开源的工具，他每天熬夜到凌晨 2 点，义务解决用户的问题，优化它的体验，却分文不取。这人真傻。

一个被亲生父母遗弃的傻子，都没正经上过大学，就自不量力地想要“Think different”。他创造的产品改变了世界，却积劳成疾，英年早逝，留给后人一句“Stay hungry, stay FOOLISH”。这人真傻。

“……”

我不害怕全世界就剩下我一个傻瓜

我要坚持到底，用我的方式

别在意这世界的奇妙

……”

感谢刘培庆这样的傻子们。世界因为你们，变得可爱了一些。

沙梓社

2018 年 3 月 28 日夜，于杭州

前 言

2015年，通过校招，我以 Windows 安全方向进入网易，组内安排投入 iOS 安全方向的研究。当时，我连苹果产品都没用过，于是攒了点钱，在淘宝上买了一台可越狱的 iPad 来研究。因为之前也没有接触过 Objective-C，无法深入阅读当时在网上找到的教程，所以只能跟着敲敲代码，看看效果。后来，通过研读念茜的文章，以及国外博客上的一些教程，把基本工具实践了一番，“狗神”沙梓社的书出版后，把他的书认真看了一遍，才算是踏进了门槛。

在那一段学习过程中，我对新的知识点都是囫圇吞枣，一直停留在工具的使用上，没有形成完整的知识体系和深层的认识，一旦出现问题就要花很长的时间去解决。这一点在后面张平引荐我去做网易云课堂的教学视频时感受尤为深刻——当你要规划整个课程时，你必须从全局出发考虑问题，仅仅根据自身的经验、知道工具的使用方法是不足的，只有理解和掌握原理，才能达到举一反三的效果。虽然从准备资料、制作 PPT 到最后录制视频的过程挺累的，但在这个过程中，我加深了对知识点的理解。这是我第一次录制视频课程，由于经验不足，导致了部分视频在终端的显示字体太小等问题，但总的来说，还是要感谢那些信任我、购买了我的视频课程的人。

后来，有几个朋友建议我出本书，把掌握的东西分享出来，也让新人少踩点坑。当时我是有点犹豫的。我不仅担心写书会占用很多时间，也担心自己的水平不够、写得不好。后来，想到视频里面的一些内容需要更新，很多知识点可以补充和完善，加上书籍的学习和沉淀效果也比视频好一些，我就开始做准备，规划每一章的完成时间，每天下班后或者周末在电脑前整理资料、写书，也挺充实的。现在，这本书终于和你见面了，希望书中的内容能够帮助你扩充自己的知识面，少走弯路，成为技术大牛。

读者对象

本书介绍了 iOS 开发、逆向和安全等方面的内容，面向以下读者：

- 高校计算机相关专业的学生

- iOS 开发工程师
- 逆向工程师
- 越狱开发工程师
- iOS 安全工程师
- 应用安全审计人员

近几年，iOS 开发人员数量激增。正向开发人员应该努力提升自己的竞争力，掌握一些底层技能，为自己开发的应用保驾护航。逆向新人也不要一味追求工具的使用和功能的实现，应该静下心来，基础知识掌握得扎实一些，后面的问题自然迎刃而解。

如何阅读本书

考虑到很多逆向分析人员缺乏正向开发和安全保护方面的知识，本书将分成以下 4 个部分进行讲解。

- 第 1 章 ~ 第 3 章是快速上手部分，内容包括一些基本概念的介绍，环境的准备，以及一些常用逆向分析工具的使用和原理。
- 第 4 章 ~ 第 6 章是正向知识储备和进阶部分，内容包括逆向过程中一些理论知识的深入讲解，例如类的结构、App 签名、Mach-O 文件格式、hook 原理等。
- 第 7 章是逆向实战部分，通过在越狱平台和非越狱平台上的逆向分析实例，带领读者学习逆向分析的思路和方法。
- 第 8 章是安全保护部分，内容包括应用安全及保护方面的知识，涉及网络传输加密、动态保护、代码混淆等。

尽管不同的人感兴趣的方面可能不一样，但我还是建议读者能够从头开始阅读本书，并把书中提到的每个知识点都实践一遍，以加深理解。

本书的源代码可以在 GitHub 上面找到：

<https://github.com/AloneMonkey/iOSREBook>

声明

本书的写作花费了大量的时间和心血，我只是想帮助大家在学习过程中少走弯路、拓宽知识面、增加技术积累，所以，请支持正版书籍，坚决抵制盗版！另外，本书内容仅供技术学习和研究之用，请勿将本书内容用于非法商业用途。

勘误

由于知识水平有限，写作过程也比较匆忙，书中难免出现错误及不足，欢迎各位读者指正。同时，我为本书开设了一个提交 issue 的项目：

<https://github.com/AloneMonkey/iOSREBook-issues>

致谢

感谢我的家人，在我成长的路上一直支持我、鼓励我。

感谢我异地三年的女友，很抱歉没有陪在你的身边。即便如此，你总是不离不弃，一直支持我的选择。

感谢念茜、狗神及在我的学习路上给予我帮助的人，感谢在网易期间的所有同事，是你们让我不断成长。

感谢电子工业出版社提供的平台，感谢编辑潘昕对本书内容的把控和指导。

感谢正在阅读本书的你，谢谢你的支持和信任。

刘培庆

2018年4月，于杭州

目 录

第 1 章 概述

1.1 逆向工程简介.....	1	1.3 应用保护手段.....	3
1.1.1 iOS 逆向学习基础.....	1	1.3.1 数据加密.....	3
1.1.2 iOS 逆向的流程.....	1	1.3.2 程序混淆.....	4
1.1.3 iOS 逆向使用的工具.....	2	1.3.3 安全监测.....	4
1.1.4 iOS 逆向的应用场景.....	2	1.4 本书工具.....	4
1.2 应用面临的安全风险.....	2	1.4.1 效率工具.....	4
1.2.1 静态修改文件.....	3	1.4.2 实用工具.....	5
1.2.2 动态篡改逻辑.....	3	1.4.3 逆向工具.....	5
1.2.3 协议分析.....	3		

第 2 章 越狱设备

2.1 什么是越狱.....	6	2.4.2 文件权限.....	17
2.2 Cydia.....	6	2.5 Cydia Substrate.....	18
2.3 SSH.....	7	2.5.1 MobileHooker.....	19
2.3.1 安装 OpenSSH.....	8	2.5.2 MobileLoader.....	19
2.3.2 配置 dropbear.....	10	2.5.3 Safe mode.....	20
2.3.3 修改默认密码.....	11	2.6 越狱必备工具.....	21
2.3.4 公钥登录.....	11	2.6.1 adv-cmds.....	21
2.3.5 通过 USB 登录.....	13	2.6.2 appsync.....	21
2.4 iOS 系统结构.....	14	2.6.3 iFile.....	21
2.4.1 文件目录.....	15	2.6.4 scp.....	22

第3章 逆向工具详解

3.1 应用解密	23	3.4 Cycrypt	43
3.1.1 dumpdecrypted	23	3.4.1 开发集成 Cycrypt	44
3.1.2 Clutch	28	3.4.2 使用 Cycrypt 越狱	45
3.1.3 小结	30	3.4.3 使用 Cycrypt 分析应用	46
3.2 class-dump	30	3.4.4 Cycrypt 的高级用法	49
3.2.1 class-dump 的使用	30	3.5 抓包	52
3.2.2 class-dump 的原理	33	3.5.1 Charles 抓包	53
3.2.3 OC 和 Swift 混编	40	3.5.2 修改网络请求	55
3.3 Reveal	41	3.5.3 HTTPS 抓包	59
3.3.1 开发集成 Reveal	41	3.5.4 Wireshark 抓包	60
3.3.2 越狱注入 Reveal	42		

第4章 开发储备

4.1 App 的结构及构建	66	4.3.1 类与方法的底层实现	84
4.1.1 获取应用包	66	4.3.2 运行时类的结构	89
4.1.2 应用包的格式	71	4.3.3 消息机制	91
4.1.3 应用的构建过程	72	4.3.4 runtime 的应用	94
4.2 界面结构和事件传递	76	4.4 App 签名	98
4.2.1 界面的组成	76	4.4.1 配置 Xcode 签名	98
4.2.2 界面事件的响应	79	4.4.2 App 签名的原理	100
4.3 类与方法	83	4.4.3 重签名	107

第5章 分析与调试

5.1 静态分析	109	5.2.1 LLDB 调试	128
5.1.1 Hopper	109	5.2.2 LLDB 解密	141
5.1.2 IDA	118	5.2.3 用 Xcode 调试第三方应用	144
5.1.3 静态库分析	125	5.2.4 LLDB 的高级调试技巧	151
5.2 动态调试	128	5.3 Theos	167

5.3.1	Theos 的安装	168	5.4.1	安装 MonkeyDev	178
5.3.2	Theos 的基本应用	168	5.4.2	Logos Tweak	179
5.3.3	Theos 的高级应用	172	5.4.3	CaptainHook Tweak	181
5.4	MonkeyDev	177	5.4.4	Command-line Tool	185

第6章 逆向进阶

6.1	程序加载	186	6.3.4	AArch64 指令	233
6.1.1	dyld 简介	186	6.3.5	栈和方法	236
6.1.2	dyld 加载流程	187	6.3.6	Objective-C 汇编	245
6.2	Mach-O 文件格式	206	6.4	hook	247
6.2.1	Mach-O 文件的基本格式	206	6.4.1	Method Swizzle	247
6.2.2	Mach-O 头部	208	6.4.2	fishhook	248
6.2.3	Load Command	210	6.4.3	Cydia Substrate	253
6.2.4	虚拟地址和文件偏移	214	6.4.4	Swift hook	256
6.2.5	懒加载和非懒加载	217	6.5	动态库	259
6.2.6	Code Signature	223	6.5.1	编译和注入	260
5.3	ARM 汇编	228	6.5.2	导出和隐藏符号	260
6.3.1	ARM 架构和指令集	228	6.5.3	C++ 和 OC 动态库	263
6.3.2	AArch64 寄存器	229	6.5.4	其他常见问题	267
6.3.3	指令集编码	231			

第7章 实战演练

7.1	越狱设备分析	270	7.2.3	编写 hook 代码	303
7.1.1	分析准备	270	7.2.4	制作非越狱 Pod	304
7.1.2	开始分析	272	7.2.5	小结	308
7.1.3	编写 Tweak	284	7.3	Frida 实战应用	309
7.1.4	安装与小结	287	7.3.1	Frida 的安装	309
7.2	非越狱设备分析	288	7.3.2	Frida 的初级使用	311
7.2.1	创建 MonkeyDev 项目	288	7.3.3	Frida 的高级使用	319
7.2.2	非越狱逆向实战	291	7.3.4	小结	326

欢迎访问：电子书学习和下载网站 (<https://www.shgis.com>)

文档名称：《IOS应用逆向与安全》刘培庆 著.pdf

请登录 <https://shgis.com/post/3257.html> 下载完整文档。

手机端请扫码查看：

