

目录

前言	1.1
iPhone越狱概述	1.2
越狱前	1.3
背景知识	1.3.1
jailbreak	1.3.1.1
tethered类型	1.3.1.2
respring	1.3.1.3
uicache	1.3.1.4
越狱工具	1.3.2
unc0ver	1.3.2.1
checkra1n	1.3.2.2
越狱中	1.4
给iPhone越狱	1.4.1
unc0ver	1.4.1.1
checkra1n	1.4.1.2
越狱后	1.5
恢复越狱	1.5.1
文件管理	1.5.2
包管理器	1.5.3
爱思助手	1.5.4
安装ipa	1.5.5
子教程	1.6
附录	1.7
参考资料	1.7.1

iOS逆向开发：iPhone越狱

- 最新版本: v2.2
- 更新时间: 20230628

简介

iOS逆向开发系列教程之iPhone越狱，先是越狱的概述，然后是越狱前需要了解的背景知识，包括jailbreak、tethered类型、respring、uicache，以及常见越狱工具unc0ver、checkra1n等；接着介绍越狱中的，即如何用unc0ver、checkra1n等工具给iPhone手机越狱，以及越狱后的各种事项，包括恢复越狱、文件管理、包管理器、辅助工具爱思助手和安装ipa。

源码+浏览+下载

本书的各种源码、在线浏览地址、多种格式文件下载如下：

HonKit源码

- [crifan/ios_re_iphone_jailbreak: iOS逆向开发：iPhone越狱](#)

如何使用此HonKit源码去生成发布为电子书

详见：[crifan/honkit_template: demo how to use crifan honkit template and demo](#)

在线浏览

- [iOS逆向开发：iPhone越狱 book.crifan.org](#)
- [iOS逆向开发：iPhone越狱 crifan.github.io](#)

离线下载阅读

- [iOS逆向开发：iPhone越狱 PDF](#)
- [iOS逆向开发：iPhone越狱 ePUB](#)
- [iOS逆向开发：iPhone越狱 Mobi](#)

版权和用途说明

此电子书教程的全部内容，如无特别说明，均为本人原创。其中部分内容参考自网络，均已备注了出处。如发现有侵权，请通过邮箱联系我 [admin 艾特 crifan.com](mailto:admin@crifan.com)，我会尽快删除。谢谢合作。

各种技术类教程，仅作为学习和研究使用。请勿用于任何非法用途。如有非法用途，均与本人无关。

鸣谢

感谢我的老婆陈雪的包容理解和悉心照料，才使得我 [crifan](#) 有更多精力去专注技术专研和整理归纳出这些电子书和技术教程，特此鸣谢。

其他

作者的其他电子书

本人 crifan 还写了其他 150+ 本电子书教程，感兴趣可移步至：

[crifan/crifan_ebook_readme: Crifan的电子书的使用说明](#)

关于作者

关于作者更多介绍，详见：

[关于CrifanLi李茂 – 在路上](#)

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新： 2023-06-28 23:26:04

iPhone越狱概述

- 给iPhone越狱
 - iOS 13
 - 常用越狱工具
 - checkra1n
 - unc0ver
 - 核心越狱步骤
 - 可以直接手动用工具（unc0ver、checkra1n等）去越狱
 - 也可以借助爱思助手去越狱
 - 爱思助手里面有个一键越狱集成了很多方便的工具，简化了越狱过程
 - iOS 15+
 - 概述
 - palera1n
 - 支持A8-A11的iOS 15.0 - iOS 16.5的rootful和rootless越狱
 - XinaA15
 - 支持A12+的iOS 15.0 - iOS 15.1.1的rootless越狱
 - Dopamine
 - 支持A12-A15, M1的iOS 15.0 - iOS 15.4.1的rootless越狱
 - 详解
 - iOS逆向：iOS15越狱
- 越狱后
 - 文件管理
 - 爱思助手的文件管理
 - ssh登录
 - scp通过ssh拷贝
 - Filza文件管理器

TODO:

- 【整理】iOS的iPhone越狱和改机相关知识
- 【已解决】Activator是什么
-
- 【无法解决】iPhone X用爱思助手的unc0ver越狱失败：正在安装unc0ver越狱，失败
- 【无法解决】用爱思助手通过unc0ver给iPhone X越狱
- 【已解决】手动用unc0ver去给iPhone X越狱
- 【已解决】Mac中用Cydia Impactor去安装unc0ver到iPhone X
- 【已解决】iPhone X中用unc0ver越狱
- 【已解决】iPhone X用unc0ver越狱后越狱失败爱思助手仍显示未越狱
- 【已解决】Cydia Impactor安装unc0ver的ipa报错：file provision.cpp:1 what Please sign in with an app-specific password
- 【已解决】生成Apple ID的app专用密码
- 【记录】给iPhone X初始化准备越狱开发环境

越狱前

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2022-06-21 13:51:47

背景知识

越狱前，要了解很多基本概念和背景知识，下面就来详细介绍相关内容。

- 其他相关
 - rootful普通越狱 vs rootless无根越狱
 - 详见：
 - [rootless和rootful · iOS逆向：iOS15越狱](#)

crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新：2023-06-28 22:12:21

jb = jailbreak =越狱

- 技术角度
 - 越狱=iOS越狱=iOS jailbreak = iPhone越狱
 - 含义：获取iOS设备的Root权限的技术手段
- 类比：iPhone=iOS系统，就像一个监狱
 - 普通iPhone的用户，就像在监狱内，虽然被iOS系统管理约束着，也很安全，但是失去了很多自由
 - 想要更加自由，就要从监狱中逃出来 = 越狱
 - 摆脱iOS系统的约束，拥有更多自由
 - 可以安装更多更好的插件、应用等，做之前非越狱时的不能做的各种事情

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新：2023-06-28 21:55:00

tethered类型

即：完美越狱 vs 不完美越狱 vs 半完美越狱 vs 半不完美越狱

- 核心逻辑：2种类型
 - 重启后，是否要（用特殊软件）引导才能开机
 - 是
 - 全越狱=完美越狱
 - 越狱后的iPhone可以正常关机和重启
 - 否
 - 半越狱=不完美越狱
 - iPhone重启后
 - 屏幕就会一直停留在启动画面，也就是“白苹果”状态
 - 或者能正常开机，但已经安装的破解软件都无法正常使用
 - 需要将设备与PC连接后，使用软件进行引导才能使用
 - 重启后，是否还保留越狱状态
 - 是
 - 全越狱
 - 否
 - 半越狱
- 2种核心逻辑组合出4种：越狱类型=Types of Jailbreaks
 - `untethered = Untethered jailbreak` = 完美越狱：不需要引导启动
 - 指设备在进行重启后，越狱状态仍被完整保留
 - `semi-untethered = Semi-untethered jailbreak` = 半完美越狱
 - 指设备在重启后，将丢失越狱状态；而若想要再恢复越狱环境，只需在设备上进行某些操作即可恢复越狱
 - `tethered = Tethered jailbreak` = 不完美越狱：需要引导启动
 - 当处于此状态的iOS设备开机重启后，之前进行的越狱程序就会失效，用户将失去Root权限，需要将设备连接电脑来使用（如特定版本下的红雪（redsn0w））等越狱软件进行引导开机以后，才可再次使用越狱程序。否则设备将无法正常引导
 - `semi-tethered = Semi-tethered jailbreak` = 半不完美越狱
 - 指设备在重启后，将丢失越狱状态，并恢复成未越狱状态。如果想要恢复越狱环境，必须连接计算机并在越狱工具的引导下引导来恢复越狱状态

=> 典型越狱效果：

- 很久之前：越狱后，就一直保持越狱状态（完美越狱）
 - 重启iPhone也能保持越狱状态
- 现在：越狱后，重启iPhone会丢失越狱（半完美越狱）
 - 所以重启iPhone后，往往还要去：恢复越狱
 - 恢复越狱，等于重新执行一遍越狱流程，重新（再次）越狱

respring

- Respring = Reboot SpringBoard =重启桌面=注销

iOS系统内有个默认的，自带的应用： SpringBoard

也就是你所看到的： iPhone的桌面

每次安装越狱插件，为了使得越狱插件生效，则需要，重启桌面，也就是Respring

常见的重启桌面的方式有：

- 图形界面操作
 - Filza 安装ipa后-> 右上角 -> 动作 -> 注销 (== Respring)
 - palera1n越狱后， palera1n的app 中-> Tools -> Respring



- XinaA15越狱后， XinaA15 的app中-> 注销 = Respring



- 命令行操作:

- 进入命令行方式
 - Mac中通过ssh进入iPhone的命令行
 - iPhone中通过终端类插件进入命令行

- 具体命令

- `killall SpringBoard`

uicache =清除界面缓存

- `uicache` = 清除界面（图标的）缓存
 - 概述：iOS的桌面中保存了所有app的图标icon，通过uicache可以刷新缓存，显示最新结果
 - refresh icon cache of jailbroken apps
 - 典型使用场景=效果
 - 越狱iPhone中
 - 安装 deb 插件后，app桌面图标没出现，用了 uicache 后，app桌面图标就出现了
 - 删除了 app 后，由于某些原因，桌面上仍然残留app的图片 -» 需要 uicache 后，桌面上的app图标才消失
 - 如何使用=如何运行 uicache
 - 方式1：命令行直接运行 `uicache`
 - 注：很多越狱工具（`unc0ver`、`checkra1n`、`palera1n` 等）自带 `uicache` 命令行工具
 - 举例：
 - `palera1n` 越狱后，`uicache`位置： `/usr/bin/uicache`
 - 方式2：UI图形界面工具中运行
 - 举例1：`Filza` 安装deb插件后，右上角 -» 动作 -» `uicache`

```
iPhone8-150:~ root# which uicache  
/usr/bin/uicache
```



- 举例2：palera1n越狱后， palera1n的app 中-》 Tools -> UI Cache



uicache内部实现细节

- uicache内部实现原理
 - uicache重启和刷新了如下相关内容
 - SpringBoard
 - lsd
 - installd
 - ~/Library/Caches/SpringBoardIconCache
 - ~/Library/Caches/SpringBoardIconCache-small
 - ~/Library/Caches/com.apple.iconsCache
- uicache源码中涉及到的内容

```
killall -SIGSTOP SpringBoard  
killall lsd  
rm -rf ~/Library/Caches/SpringBoardIconCache  
rm -rf ~/Library/Caches/SpringBoardIconCache-small
```

```
rm -rf ~/Library/Caches/com.apple(IconsCache)
killall installd
killall -SIGCONT SpringBoard
launchctl stop com.apple.SpringBoard
```

uicache的help语法帮助

```
iPhone8-150:~ root# uicache --help
Usage: uicache [-afhlr] [-i id] [-p path] [-u path]
Modified work Copyright (C) 2021, Procursus Team. All Rights Reserved.

Update iOS registered applications and optionally restart SpringBoard

-a, --all           Update all system and internal applications
-f, --force          Force -a to reregister all Applications
                     and modify App Store apps
-p, --path <path>  Update application bundle at the specified path
-U, --unregister <path> Unregister application bundle at the specified path
-r, --respring        Restart SpringBoard and backboarrrd after
                     updating applications
-l, --list            List the bundle ids of installed apps
-i, --info <bundleid> Give information about given bundle id
-h, --help             Give this help list.

Contact the Procursus Team for support.
```

越狱工具

确认iPhone信息和版本

- 记录】iPhone6的手机基本信息
- 【记录】Mac中连接iOS 12.4.5的iPhone6

越狱工具的选择

- 越狱工具的选择
 - 【整理】iOS iPhone破解和越狱相关的基础知识
 - 【整理】不同版本iOS系统的越狱工具的选择
 - 【整理】ios 13 越狱工具的选择
 - 【整理】iOS越狱工具对比：checkra1n、unc0ver、Electra、Pangu等
 - 【已解决】iOS的半越狱和全越狱
 - 【整理】iOS越狱工具：Pangu盘古
 - 【整理】越狱工具软件：奥德赛 Odyssey

结论：

- iOS <15.0
 - 说明：越狱工具大多都很成熟和稳定，用的人也很多
 - 针对的iOS系统版本
 - 多数都是：iOS 12 ~ iOS 14
 - iOS <12，基本上很少用了
 - 常用
 - checkra1n
 - unc0ver
- iOS >15.0
 - 概述
 - 基本可用的
 - palera1n
 - XinaA15
 - Dopamine
 - 根据个人经验，稳定程度大概是：xinaA15 > palera1n > Dopamine
 - 详解
 - iOS逆向：iOS15越狱

unc0ver

- unc0ver
 - 主页
 - <https://unc0ver.dev/>

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2023-03-02 22:19:39

checkra1n

- checkra1n
 - 主页
 - <https://checkra.in>

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2023-03-02 22:19:08

越狱中

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2022-06-21 13:49:28

给iPhone越狱

crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新: 2023-03-02 22:22:52

unc0ver

TODO:

- 【已解决】iPhone中用unc0ver去给iOS越狱
 - 【记录】用unc0ver重新恢复越狱后的iPhone中的效果
 - 【已解决】给用unc0ver越狱的iPhone7恢复越狱状态
 - 【记录】unc0ver越狱iPhone7的完整log日志
 - 【记录】用unc0ver还原卸载越狱环境
-

checkra1n

TODO:

- 【已解决】Mac中给iOS 12.4.5的iPhone6中安装checkra1n
 - 【研究】用unc0ver越狱iOS 13的iPhone
 - 【已解决】Mac中用checkra1n越狱iOS 12.4.5的iPhone6
-

越狱后

- 【整理】已越狱后的iPhone和iOS相关知识
- 【整理】已越狱iOS的ipa安装工具：Cydia Impactor
- 【整理】已越狱的iPhone有哪些有用的有价值的扩展插件
- 【已解决】iPhone6中重新激活和开启越狱状态
- 【记录】新iPhone测试机iPhone7P越狱环境准备

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新：2022-06-21 13:57:34

恢复越狱

TODO:

- 【记录】给之前用checkra1n越狱的iPhone6恢复越狱
-

现在主流越狱工具，比如 `unc0ver`，都是 半完美越狱：iOS（iPhone）重启后，越狱就丢失了

-> 具体现象是：点击 `Cydia` 等软件会闪崩无法打开

此时，就需要去：恢复越狱

即把之前越狱的流程再走一遍

-> 即可恢复越狱状态。

crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新：2022-10-27 21:37:40

文件管理

越狱后的iPhone，可以有很多文件管理方面的工具：

- 文件管理
 - ssh
 - OpenSSH
 - 免密登录
 - scp：导入 导出 文件
 - Filza
 - 文件管理
 - 爱思助手
 - 安装ipa
 - Filza
 - 爱思助手
-

TODO：

- 【已解决】从已越狱iPhone中拷贝文件到Mac中
- 【已解决】已越狱iOS中通过Cydia安装文件管理器
- 【已解决】从已越狱iPhone中拷贝文件到Mac中

其他：

- iFile（收费）
 - 【未解决】iPhone中安装和使用iFile查看iOS是否已越狱
 - 【未解决】Cydia安装BigBoss源的iFile出错：无法购买Cydia is not yet prepared to accept money

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新：2022-10-23 14:53:35

包管理器

概述：越狱后，往往会通过包管理器去安装越狱开发所需的各种插件和工具。比如OpenSSH用于ssh登录、Filza用于管理文件、TrollStore用于安装ipa等等。

具体详见独立教程：

[iOS逆向开发：越狱包管理器](#)

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新：2023-03-13 23:02:31

爱思助手

- 【记录】Mac中用爱思助手检测和确认iPhone是否已越狱
- 【记录】已越狱的iOS中用爱思助手安装app软件：微信
- 【已解决】用Mac版爱思助手给iOS13的iPhone7越狱
- 【记录】iPhone6中试用爱思极速版
- 【已解决】Mac中爱思助手看不到iPhone的越狱文件系统全部文件内容
- 【已解决】Mac中用爱思助手安装抖音ipa到越狱iPhone中

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2022-06-21 14:06:53

安装ipa

- Filza
 - 【整理】iOS逆向心得：越狱iPhone异常时的现象：Filza安装ipa卡死

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新：2022-06-21 13:40:13

子教程

当前教程主要介绍，普通的iPhone越狱的内容，关于更新版的 `ios 15+` 的越狱，详见：

- 子教程
 - [iOS逆向：iOS15越狱](#)

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新：2023-06-28 23:25:20

附录

下面列出相关参考资料。

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2022-06-19 08:09:37

参考资料

- 【已解决】iOS的半越狱和全越狱
-

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2023-06-28 22:50:33