

目录

前言	1.1
iOS逆向心得概述	1.2
总体对策	1.2.1
iPhone	1.3
初始化开发环境	1.3.1
常用目录	1.3.2
app	1.4
相关文件目录和数据	1.4.1
Bundle	1.4.1.1
Data	1.4.1.2
Shared AppGroup	1.4.1.3
二进制文件路径	1.4.2
ObjC	1.5
运行时	1.5.1
objc_msgSend	1.5.1.1
Class	1.5.2
私有成员属性	1.5.2.1
扩展属性	1.5.2.2
属性值	1.5.3
计算类的属性值	1.5.3.1
Xcode和Frida属性值不一致	1.5.3.2
动态调试	1.6
调试代码逻辑	1.6.1
寻找函数触发时机	1.6.1.1
寻找变量改动时机	1.6.1.2
改变运行逻辑	1.6.1.3
Xcode调试	1.6.2
函数调用堆栈	1.6.2.1
函数名不一致	1.6.2.1.1
iOSOpenDev	1.6.3
log日志	1.7
头文件	1.8
抓包	1.9
tweak插件	1.10
通用	1.11
从汇编反推代码逻辑	1.11.1
附录	1.12
参考资料	1.12.1

iOS逆向：心得集锦

- 最新版本: v0.5.5
- 更新时间: 20240305

简介

把iOS逆向中的，各种不适合、不方便、不应该放到某个其他独立子教程中的心得，都整理过来，放到此处iOS逆向心得集锦中，方便参考

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_experience_collection: iOS逆向：心得集锦](#)

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：心得集锦 book.crifan.org](#)
- [iOS逆向：心得集锦 crifan.github.io](#)

离线下载阅读

- [iOS逆向：心得集锦 PDF](#)
- [iOS逆向：心得集锦 ePUB](#)
- [iOS逆向：心得集锦 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：2024-03-06 09:25:18

iOS逆向心得概述

把[iOS逆向](#)中的，各种不适合、不方便、不应该放到某个其他独立[子教程](#)中的心得，都整理过来，放到此处iOS逆向心得集锦中，方便参考。

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：2024-03-05 22:31:20

iOS逆向的总体对策

TODO:

- 【整理】iOS逆向心得：不同app的逆向破解出的难度不同
 - 【整理】iOS逆向破解越狱开发：相关工具
-

iOS安全对应的逆向破解对策

针对[iOS安全](#)的防护手段，目前能想到的，iOS逆向破解的办法：

- iOS的代码混淆
 - 被反编译后，也只能看到乱码的函数
 - 部分防止被破解，被猜测到核心逻辑
- iOS的加壳？
 - 没法加壳
 - 但是也可以去研究看看，是否有机会
- iOS代码运行期间，动态下载要运行的核心代码（二进制格式？）
 - 增加核心逻辑的安全性
 - 好像涉及到虚拟机之类的
 - 注：对应的iOS逆向，则是：unicorn等 模拟器 虚拟机，模拟运行对应的指令
- iOS的抓包方面的：加https证书验证？ssl pinning？
 - 甚至（参考抖音的做法）去本地ssl证书验证
 - 只有破解hook后，才能Charles抓包看到https明文
 - 后记：[\[原创\]绕过抖音SSL Pinning-iOS安全-看雪论坛-安全社区|安全招聘|bbs.pediy.com](#)
 - 1.加入自己的证书2.干掉所有的证书3.不让他验证证书。很显然，你用的是第二种

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：2024-03-05 22:31:25

iPhone

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: 2024-02-26 09:38:47

初始化开发环境

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: 2024-02-26 09:38:47

iPhone中常用目录

iOS逆向期间，常常会涉及到很多目录，且其中有些是有（软链接等）关系的。整理如下：

- /etc/ == /private/etc/
- /var/ == /private/var/
 - /User/ == /var/mobile/ == /private/var/mobile/
 - /tmp/ == /private/var/tmp/

->

举例：

- Bundle目录 入口=根目录
 - /private/var/containers/Bundle/Application/
 - ==
 - /var/containers/Bundle/Application/

附录

根目录下文件目录和内容：

```
iPhone8-143:/ root# pwd
/
iPhone8-143:/ root# ls -lh
total 1.5K
drwxrwxr-x 107 root admin 3.4K Dec 25 11:14 Applications/
drwxr-xr-x 7 root wheel 306 Dec 4 2020 Developer/
drwxr-xr-x 25 root wheel 800 Dec 13 10:48 Library/
drwxr-xr-x 4 root wheel 128 Jan 8 2021 System/
lrwxr-xr-x 1 root wheel 11 Dec 13 11:07 User -> /var/mobile/
drwxr-xr-x 61 root wheel 2.0K Dec 13 10:48 bin/
drwxr-xr-x 2 root wheel 64 Oct 28 2006 boot/
drwxrwxr-t 2 root admin 64 Jun 28 2018 cores/
dr-xr-xr-x 4 root wheel 1.4K Dec 13 11:01 dev/
lrwxr-xr-x 1 root wheel 11 Jun 28 2018 etc -> private/etc/
drwxr-xr-x 2 root wheel 64 Oct 28 2006 lib/
drwxr-xr-x 2 root wheel 64 Oct 28 2006 mnt/
drwxr-xr-x 7 root wheel 224 Jan 8 2021 private/
drwxr-xr-x 40 root wheel 1.3K Dec 13 10:48 sbin/
lrwxr-xr-x 1 root wheel 15 Jun 28 2018 tmp -> private/var/tmp/
drwxr-xr-x 12 root wheel 384 Dec 13 10:48 usr/
lrwxr-xr-x 1 root admin 11 Jun 28 2018 var -> private/var/
iPhone8-143:/ root#
```

app

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: 2024-02-26 09:38:47

app相关文件目录和数据

TODO:

- 【整理】iOS逆向心得: app完全卸载后仍有可能有app相关的数据
 - 【整理】iOS逆向心得: Keychain数据库
 - 【未解决】iOS逆向WhatsApp: 调试IdentityKeypairData调用SecItemAdd写入Keychain数据库的具体逻辑
 - 【整理】iOS逆向: Keychain数据库字段含义
-

iOS的app安装后, 相关数据和内容:

- 文件目录
 - Bundle 目录
 - 根目录: /private/var/containers/Bundle/Application/
 - Data 目录
 - 根目录: /private/var/mobile/Containers/Data/Application/
 - Shared AppGroup 目录
 - 根目录: /private/var/mobile/Containers/Shared/AppGroup/
- 数据
 - Keychain数据
 - Keychain-2.db
 - 位置: /private/var/Keychains/keychain-2.db
 - 相关函数
 - 写入数据: SecItemAdd
 - 更新数据: SecItemUpdate

举例

WhatsApp

- WhatsApp
 - WhatsApp
 - Bundle 目录
 - /private/var/containers/Bundle/Application/B42F04DD-E264-401B-A72C-C00B240A1E81/
 - Data 目录
 - /private/var/mobile/Containers/Data/Application/3856AB23-E286-4EE0-B06E-A0519A591AA8/
 - AppGroup目录
 - /private/var/mobile/Containers/Shared/AppGroup/D70C70AC-D347-4640-9667-1AA86D05CB65/
 - 数据
 - Keychain数据
 - Keychain-2.db
 - 位置: /private/var/Keychains/keychain-2.db

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: 2024-02-26 09:55:16

Bundle

TODO:

- 【已解决】越狱iPhone中确定iOS的app的Data目录位置
-

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: 2024-02-26 10:01:06

Data

TODO:

- 【已解决】越狱iPhone中确定iOS的app的Bundle目录位置
-

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: 2024-02-26 10:01:14

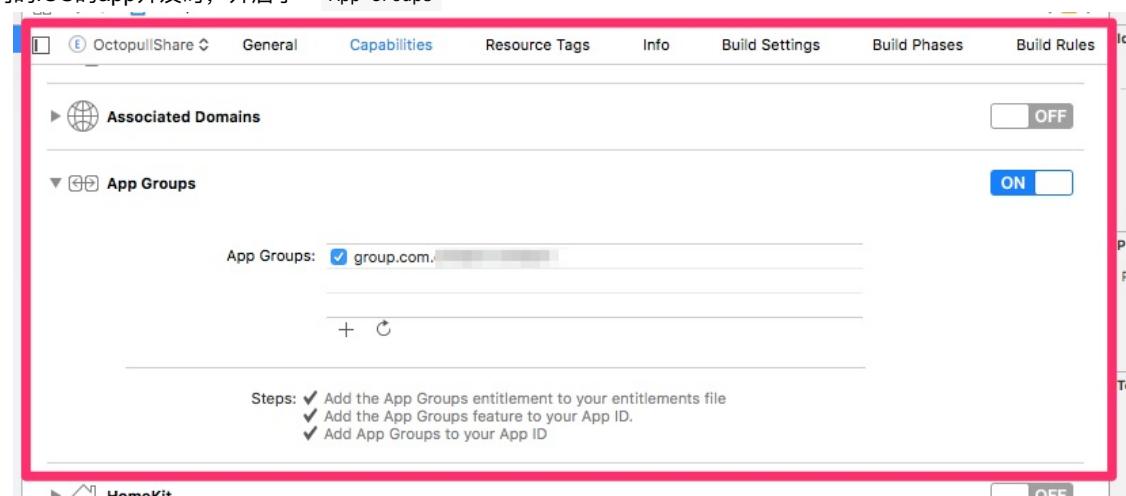
Shared AppGroup

TODO:

- 【已解决】越狱iPhone中确定iOS的app的Shared AppGroup目录位置
- 【记录】iOS函数：NSFileManager的containerURLForSecurityApplicationGroupIdentifier:
- 【未解决】尝试改变包名去解决container_create_or_lookup_app_group_path_by_app_group_identifier

如何获取 Shared AppGroup 的路径

- Xcode正向开发
 - 正向的iOS的app开发时，开启了：`App Groups`



- 代码

```
[NSFileManager containerURLForSecurityApplicationGroupIdentifier:]
```

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: 2024-02-26 09:59:32

二进制文件路径

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: 2024-02-26 09:38:47

ObjC

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: 2024-02-26 09:38:47

运行时

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: 2024-02-26 09:38:47

objc_msgSend

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: 2024-02-26 09:38:47

Class

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: 2024-02-26 09:38:47

私有成员属性

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: 2024-02-26 09:38:47

扩展属性

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: 2024-02-26 09:38:47

属性值

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: 2024-02-26 09:38:47

计算类的属性值

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: 2024-02-26 09:38:47

Xcode和Frida属性值不一致

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: 2024-02-26 09:38:47

动态调试

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: 2024-02-26 09:38:47

调试代码逻辑

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: 2024-02-26 09:38:47

寻找函数触发时机

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: 2024-02-26 09:38:47

寻找变量改动时机

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: 2024-02-26 09:38:47

改变运行逻辑

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: 2024-02-26 09:38:47

Xcode调试

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: 2024-02-26 09:38:47

函数调用堆栈

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: 2024-02-26 09:38:47

函数名不一致

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: 2024-02-26 09:38:47

iOSOpenDev

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: 2024-02-26 09:38:47

log日志

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: 2024-02-26 09:38:47

头文件

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: 2024-02-26 09:38:47

抓包

可以自己搭建服务器抓包

举例，别人的：

抓包的时候可以自己搭建服务器，用于嗅探记录，拦截请求数据包，或者叫转发数据包，记录当前传入和传出的参数，也就是请求和响应的各种参数记录下来，类似于这种效果：

```

--- 机器参数.
-- @table rfaker
-- @string name 设备名称 e.g. "“xxx”的 iPhone"
-- @string hw_machine_name e.g. "iPhone 11 Pro Max"
-- @string ssid e.g. "TP_LINK_E-BoJingEr-557-OFFICE"
-- @tparam integer create_time e.g. 創建时间 1054709286
-- @string locale_identifier e.g. "CN"
-- @string remark 备注 e.g. null
-- @number lon e.g. 123.98118244667
-- @string app_times e.g. null
-- @string network_state e.g. "WIFI"
-- @string localtion e.g. null
-- @string idfa e.g. "91566BBD-C5E6-48B0-85CA-6E0C68663F69"
-- @string hw_machine e.g. "iPhone12,5"
-- @string carrier_name e.g. "數碼通"
-- @string build_version e.g. "18G82"
-- @string system_version e.g. "14.7.1"
-- @number lat e.g. 33.814002430383
-- @string current_radioaccess_technology e.g. "CTRadioAccessTechnologyLTE"
-- @string mobile_network_code e.g. "06"

--- 当前参数.
-- @function faker
-- @apiget http://127.0.0.1:1688/api/v1/machine/faker
-- @treturn rfaker 返回当前工作参数
-- @usage
-- -- -- 返回结果如: (json)
-- {
--   "name": "“xxx”的 iPhone",
--   "hw_machine_name": "iPhone 11 Pro Max",
--   "ssid": "TP_LINK_E-BoJingEr-557-OFFICE",
--   "create_time": 1054709286,
--   "locale_identifier": "CN",
--   "remark": null,
--   "lon": 123.98118244667,
--   "app_times": null,
--   "network_state": "WIFI",
--   "localtion": null,
--   "idfa": "91566BBD-C5E6-48B0-85CA-6E0C68663F69",
--   "hw_machine": "iPhone12,5",
--   "carrier_name": "數碼通",
--   "build_version": "18G82",
--   "system_version": "14.7.1",
--   "lat": 33.814002430383,
--   "current_radioaccess_technology": "CTRadioAccessTechnologyLTE",
--   "mobile_network_code": "06"
-- }
```

tweak插件

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: 2024-02-26 09:38:47

通用

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: 2024-02-26 09:38:47

从汇编反推代码逻辑

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: 2024-02-26 09:38:47

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: 2024-02-26 09:37:43

参考资料

- 【未解决】iOS的app安装和使用后相关内容：数据、文件、目录
-
-

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：2024-02-26 09:44:39