目录

移动端逆向：代码混淆和反代码混淆

- 最新版本：`v0.6.0`
- 更新时间：`20250124`

简介

移动端的代码混淆和反代码混淆，相关混淆方式、混淆工具和反混淆方式、反混淆工具等，以及iOS和Android相关的内容。

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/mobile_re_obfuscation_anti: 移动端逆向：代码混淆和反代码混淆

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

- 移动端逆向：代码混淆和反代码混淆 book.crifan.org
- 移动端逆向：代码混淆和反代码混淆 crifan.github.io

离线下载阅读

- 移动端逆向：代码混淆和反代码混淆 PDF
- 移动端逆向：代码混淆和反代码混淆 ePub
- 移动端逆向：代码混淆和反代码混淆 Mobi

版权和用途说明

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

(反)代码混淆概览

在**移动端逆向**期间，往往会涉及到：**反代码混淆**

所以在解决反代码混淆之前，也要对**代码混淆**，有足够的了解。

下面就来详细解释。

代码混淆

从正向的防护角度来说，可以用**代码混淆**去增加和保护自己的app的代码逻辑，增大逆向人员破解的难度。

通用

TODO：

- 【整理】iOS和Android安全防护相关：代码混淆
- 去除花指令 去混淆

混淆方式

代码混淆，有多种方式=手段，此处概述如下：

代码混淆手段	简称=缩写	ollvm参数	goron参数	说明
字符串加密	`sobf` = `String Obfuscation`	`-mllvm -sobf`	`-mllvm -irobf-cse`	把字符串明文加密成乱码字符串
控制流平坦化	`fla` = `Control Flow Flattening`	`-mllvm -fla`	`-mllvm -irobf-cff`	
虚假控制流	`bcf` = `Bogus Control Flow`	`-mllvm -bcf`		
指令替换	`sub` = `Instruction Substitution`	`-mllvm -sub`		
基本块分割	`split` = `Basic Block Splitting`	`-mllvm -split`		
间接跳转	`indbr` = `indirect branch`			
间接函数调用	`icall` = `indirect call`			

sobf=字符串加密

TODO：

- 【整理】代码混淆手段：String Obfuscation字符串混淆
- 【已解决】iOS逆向Apple账号：Xcode实时调试函数MGCopyAnswer的实现原理机制
- 【已解决】iOS逆向：爱思助手中和UDID相关的iPhone设备相关信息

- `sobf` = `String Obfuscation` = `字符串加密` = `字符串混淆`
  - 参数：
    - `ollvm`：`-mllvm -sobf`
    - `goron`：`-mllvm -irobf-cse`

举例

MGCopyAnswer相关key和value

- `SerialNumber` -> `VasUgeSzVyHdB27g2XpN0g`
  - 值：`FFMYRLS0JC6C`
- `ECID` = `UniqueChipID` -> `TF31PAB6aO8KAbPyNKSxKA`
  - 值：`3445358584856622`
- `WifiAddress` -> `gI6iODv8MZuiP0IA+efJCw`
  - 值：`14:9d:99:f0:b4:15`
- `BluetoothAddress` -> `k5lVWbXuiZHLA17KGiVUAA`
  - 值：`14:9d:99:eb:d8:f7`

fla=控制流平坦化

TODO：

- 【整理】代码混淆手段：Control Flow Flattening控制流平坦化

- `fla` = `Control Flow Flattening` = `控制流平坦化` = `控制流扁平化` = `控制流展开`
  - 参数：
    - `ollvm`：`-mllvm -fla`
    - `goron`：`-mllvm -irobf-cff`

bcf=虚假控制流

TODO：

- 【整理】代码混淆手段：Bogus Control Flow虚假控制流

- `bcf` = `Bogus Control Flow` = `虚假控制流` = `虚假控制流程` = `虚假块`
  - 参数：
    - `ollvm`：`-mllvm -bcf`

split=基本块分割

TODO：

- 【整理】代码混淆手段：Basic Block Splitting基本块分割

- `split` = `Basic Block Splitting` = `基本块分割`
  - 参数：
    - `ollvm`：`-mllvm -split`

sub=指令替换

TODO：

- 【整理】代码混淆手段：Instruction Substitution指令替换
- 【整理】代码混淆手段：Dead Code Injection垃圾代码注入

- `sub` = `Instruction Substitution` = `指令替换` = `指令膨胀`
  - 参数：
    - `ollvm`：`-mllvm -sub`
  - ~= `Dead Code Injection` = `垃圾代码注入` == `花指令` ?
    - 垃圾指令：`.long unknown code`

indbr=间接跳转

TODO：

- 【记录】混淆类型 indbr

- `indbr` = 间接跳转
  - 参数
    - `goron`：`-mllvm -irobf-indbr`

icall=间接函数调用

- `icall` = 间接函数调用
  - 参数
    - `goron`：`-mllvm -irobf-icall`

其他

- Opaque Constants=不透明的常量
  - 【整理】代码混淆手段：Opaque Constants不透明的常量
- Opaque Fields Access=不透明字段访问
  - 【整理】代码混淆手段：Opaque Fields Access不透明字段访问
- 间接全局变量引用
  - 参数：
    - goron：`-mllvm -irobf-indgv`
- 关于IDA
  - 故意制造堆栈不平衡 -》 使得IDA反编译异常，无法准确识别代码逻辑
  - 其他方式

混淆工具

TODO：

- 【整理】代码混淆相关工具和技术

ollvm

TODO：

- 【整理】代码混淆工具：ollvm=obfuscator-llvm
- ollvm分析及反混淆

- `ollvm`
  - Github
    - https://github.com/obfuscator-llvm/obfuscator
  - Wiki
    - Home · obfuscator-llvm/obfuscator Wiki
      - Installation · obfuscator-llvm/obfuscator Wiki
  - 当前版本
    - obfuscator-llvm/obfuscator at llvm-4.0

goron

- goron
  - Github
    - https://github.com/amimo/goron
      - Yet another llvm based obfuscator
  - 支持特性
    - 混淆过程间相关
    - 间接跳转,并加密跳转目标(`-mllvm -irobf-indbr`)
    - 间接函数调用,并加密目标函数地址(`-mllvm -irobf-icall`)
    - 间接全局变量引用,并加密变量地址(`-mllvm -irobf-indgv`)
    - 字符串(c string)加密功能(`-mllvm -irobf-cse`)
    - 过程相关控制流平坦混淆(`-mllvm -irobf-cff`)
  - 示例
    - goron/examples at master · amimo/goron

Armariris

TODO：

- 【整理】代码混淆工具：Armariris孤挺花

- Armariris
  - Github
    - https://github.com/GoSSIP-SJTU/Armariris
      - 孤挺花（Armariris） -- 由上海交通大学密码与计算机安全实验室维护的LLVM混淆框架
  - 目前开放功能
    - 字符串加密 `sobf`
    - 控制流扁平化 `fla`
    - 指令替换 `sub`

O-MVLL

TODO：

- 【整理】代码混淆工具：O-MVLL

- O-MVLL
  - logo
    - 

  - 概述
    - O-MVLL (in reference to O-LLVM) is a LLVM-based obfuscator driven by Python and the LLVM pass manager
  - 官网
    - https://obfuscator.re/omvll/
      - Getting started | O-MVLL Documentation
  - Github
    - https://github.com/open-obfuscator/o-mvll
      - open-obfuscator/o-mvll: :electron: O-MVLL is a code obfuscator based on LLVM for native code (Android & iOS)
  - 下载
    - https://github.com/open-obfuscator/o-mvll/releases/

Hikari

TODO：

- 【整理】代码混淆工具：Hikari光

- Hikari
  - Github
    - https://github.com/HikariObfuscator/Hikari
      - LLVM Obfuscator
  - 说明
    - 20230129 已停止维护
  - 其他fork
    - https://github.com/61bcdefg/Hikari-LLVM15
      - 61bcdefg/Hikari-LLVM15: A fork of Hikari Obfuscator [WIP]
        - 说明：20241001 已停止维护

Tigress

TODO：

- 【整理】代码混淆工具：Tigress
- Tigress混淆器安装与使用指南-CSDN博客

- Tigress
  - Github
    - https://github.com/JonathanSalwan/Tigress_protection
  - 官网
    - 新
      - https://tigress.wtf/index.html
    - 旧
      - http://tigress.cs.arizona.edu/

iOS

TODO：

- 【整理】iOS逆向相关：代码混淆
- iOS 安全探索：字符串加密 - 掘金 (juejin.cn)

混淆工具

ios-class-guard

- ios-class-guard
  - Github
    - https://github.com/Polidea/ios-class-guard
      - Polidea/ios-class-guard: Simple Objective-C obfuscator for Mach-O executables. (github.com)

Android

TODO：

- 安卓apk混淆：np管理器
- 【未解决】安卓逆向：.datadiv_decode
- 安卓 App安全

Proguard

- Proguard
  - 概述：安卓中的代码混淆工具=库
  - Github
    - https://github.com/Guardsquare/proguard
      - Guardsquare/proguard: ProGuard, Java optimizer and obfuscator
  - 相关公司
    - guardsquare
      - https://www.guardsquare.com/proguard
        - Java Obfuscator and Android App Optimizer | ProGuard
          - Use ProGuard®, Guardsquare’s open-source shrinker for Java bytecode, to enhance and optimize your code.
      - 其他其他产品
        - DexGuard
          - https://www.guardsquare.com/dexguard
            - Full-spectrum protection for Android apps & SDKs
              - With DexGuard, achieve the most comprehensive Android app protection, featuring multiple layers of code hardening, built-in malware defense, and automated runtime application self-protection (RASP) in less than a day.
  - 注意：
    - Android Gradle plugin 3.4.0+，不再用ProGuard
    - 最新的用：R8
      - R8 configuration files
  - 安卓相关
    - Shrink, obfuscate, and optimize your app | Android Studio | Android Developers

dProtect

- dProtect
  - 概述：安卓中的代码混淆工具，基于 `Proguard`
    - an Android bytecode obfuscator based on Proguard
  - 官网
    - https://obfuscator.re/dprotect/

反代码混淆

通用

TODO：

- 安卓 逆向 脱壳 砸壳
- 【整理】Frida调试hook安卓：Ollvm反混淆 字符串解密 init_array

反混淆方式

TODO：

- 反混淆：模拟执行 、符号执行
- 【整理】iOS和Android逆向相关：代码反混淆Code Deobfuscation
- 【未解决】iOS逆向：如何反代码混淆反混淆去混淆
- 【整理】代码反混淆：反控制流平坦化
- 【整理】代码反混淆：反指令替换
- 【整理】代码反混淆：structure recovering结构体恢复
- 【整理】代码反混淆：String Deobfuscation字符串反混淆

反混淆工具

Unicorn

TODO：

- python unicorn 去混淆 ollvm

详见：

CPU模拟利器：Unicorn

Frida的Stalker

TODO：

- 【整理】Frida的Stalker的作用和大概逻辑

- Frida的Stalker
  - 概述：可以用Frida的Stalker去动态调试代码逻辑，实现指令级的动态调试，常用于高级的反代码混淆
  - 详见
    - Frida的Stalker · 逆向调试利器：Frida
    - Stalker · Frida逆向实例和工具函数

Triton

TODO：

- 【整理】反混淆工具：DSE框架：Triton

QSynthesis

TODO：

- 【整理】代码反混淆工具：QSynthesis

QBDI

TODO：

- 【整理】DBI框架：QBDI

iOS

TODO：

- 【记录】给抖音的libmetasec_ml.so去做反代码混淆
- 【未解决】尝试给.datadiv_decode字符串反混淆：Armariris_string_obfuscation_bypass
- 【整理】iOS逆向：MGCopyAnswer中key原属性名和混淆后属性名的映射表
- 【未解决】iOS反破解：字符串加密隐藏路径
- 【未解决】iOS逆向：IDA中F5反编译代码中的JUMPOUT
- 反混淆：恢复被OLLVM保护的程序 - h2z - 博客园 (cnblogs.com)
- [原创]Unicorn反混淆：恢复被OLLVM保护的程序(一)-茶余饭后-看雪-安全社区|安全招聘|kanxue.com

---

Android

TODO：

- 【已解决】Xposed如何hook混淆后的安卓应用中的类名和函数名
- 【记录】给安卓的jadx反编译后的混淆后的java代码优化：给类、变量、属性去重命名
- 【整理】安卓反代码混淆间接跳转相关资料
- 【已解决】安卓保活逆向360Wallpaper：用frida去hook混淆后的安卓java类x6的e.java
- 【记录】J.N中libsscronet.so的字符串混淆后的native函数的原始函数定义和内容
- 【已解决】安卓保活逆向360Wallpaper：去使用m1.e.i去解密已混淆加密字符串得到原始字符串
- 【未解决】安卓保活逆向360Wallpaper：自己新建m1.e的实例调用i解密函数得到解密后字符串
- 【已解决】如何反混淆即还原反编译后混淆的安卓代码 – 在路上

反混淆工具

JEB

TODO：

- 【记录】新音爆安卓apk：用JEB反编译反混淆
- 【记录】Mac用JEB反混淆新音爆安卓apk：单个文件的反混淆反编译
- 【记录】Mac用JEB反混淆新音爆安卓apk：全部文件的反编译
- 【整理】JEB相关内容
- 【整理】安卓逆向：JEB功能介绍

---

jadx

TODO：

- 反混淆 · 安卓反编译利器：jadx (crifan.org)
- 【未解决】新音爆的安卓apk：用工具反混淆
- 【记录】新音爆安卓apk：用Jadx反编译反混淆
- 【记录】用jadx开启反混淆去反编译360Wallpaper安卓apk
- 【记录】Mac中用jadx反编译抖音源码

---

simplify

TODO：

- 【记录】新音爆安卓apk：用simplify反混淆

附录

下面列出相关参考资料。

参考资料

-