Beijing Forest Studio

北京理工大学信息系统及安全对抗实验中心


# 逆向分析与软件保护

硕士研究生　鲁帅

2020年05月05日

# 内容提要

- 背景简介
- 技术应用
- 分析过程
- 软件保护
- 总结

# 背景简介

- 预期收获
  - 1. 了解逆向分析的概念及应用场景
  - 2. 通过一次逆向的演示
    - 了解dbg工具的使用
    - 了解dll逆向的过程
  - 3. 了解软件开发中软件保护的方式
  - 4. 提升逆向思维和版权意识

# 背景简介

- 基本概念
  - 逆向分析：对一个事物的可能，对其进行反向分析，分解和重构，推理分析某个事物可能
- 逆向分析的对象
  - 实体物品
  - 软件系统
  - 通信协议
  - 事件
  - 科学原理

# 背景简介

- 学习网站
  - 看雪论坛 https://bbs.pediy.com/
  - 吾爱破解 https://www.52pojie.cn/
- 学习书籍
  - 《加密与解密》
  - 《C++反汇编与逆向分析技术解密》
  - 《0Day安全：软件漏洞分析技术》

# 背景简介

- 必备语言
  - C语言
  - 汇编
  - 英语
- 常用工具
  - IDA Pro
  - OllyDBG
  - PEID
  - AndroidKiller
  - APKTool Box

# 技术应用

- 学习、模仿
  - 以学习为目的
  - 以仿制为目的
- 软件破解
  - 技术交流
  - 非法盈利
  - 捆绑其他软件
  - 引流、宣传

# 技术应用

- 恶意软件（病毒、木马、僵尸程序等）分析
  - 分析恶意软件功能，评估危害等级
  - 分析关键代码和行为，提取特征用于检测与防御
  - 分析恶意软件实现机理，研发清除手段

- 软件、产品测试
  - 分析漏洞形成的位置和原因，提出修补方案；
  - 分析漏洞是否可利用、利用难度、利用成功率，评估漏洞危害性；
  - 分析同类漏洞特征、形成原因的共性特征，对该产品的其他模块或其他产品提前做出检测和修复；

# 技术应用

- 个性化DIY
  - 修改背景、图标等
  - 去除一些弹框
  - 去除某些功能
  - 汉化

# 分析过程

| | |
|---|---|
| T | 完成对软件的逆向分析和修改 |
| I | 软件安装目录下的所有文件 |
| P | 查找、替换、修改软件中的部分数据 |
| O | 修改（破解）后的软件 |

| | |
|---|---|
| P | 分析软件的结构和数据，实现对软件的修改 |
| C | 需要对软件结构、汇编语言等有较好的理解 |
| D | 调试过程较为复杂，并且存在多种保护 |
| L | 水平不一 |

# 分析过程

- 分析方法
  - 动态分析
  - 静态分析
  - 污点传播
  - 程序切片
  - 符号执行

# 分析过程

- 从使用tensorflow遇到的一个dll错误说起

```
File "<frozen importlib._bootstrap>", line 978, in _gcd_import
File "<frozen importlib._bootstrap>", line 961, in _find_and_lo
File "<frozen importlib._bootstrap>", line 950, in _find_and_lo
File "<frozen importlib._bootstrap>", line 648, in _load_unlocl
File "<frozen importlib._bootstrap>", line 560, in module_fror
File "<frozen importlib._bootstrap_external>", line 922, in cre
File "<frozen importlib._bootstrap>", line 205, in _call_with_fr
ImportError: DLL load failed: 动态链接库(DLL)初始化例程失败。
```

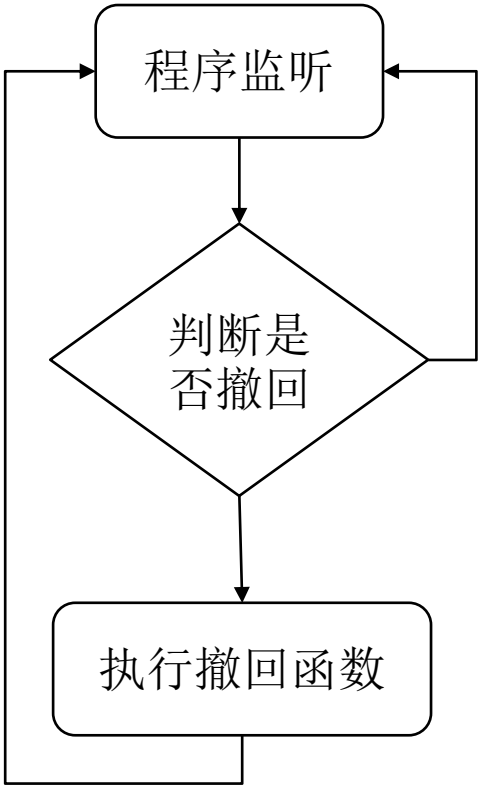
# 分析过程

- 什么是dll文件?
  - DLL(Dynamic Link Library)文件，是动态链接库文件。
- 什么是链接库?
  - 链接库可以理解为导入的库文件，包括静态库和动态库。静态库和动态库的区别是：静态库在程序的链接阶段被复制到了程序中，和程序运行的时候没有关系；动态库在链接阶段没有被复制到程序中，而是程序在运行时由系统动态加载到内存中供程序调用。使用动态库的优点是系统只需载入一次动态库，不同的程序可以得到内存中相同的动态库的副本，因此节省了很多内存。

# 分析过程

- 以微信的某dll文件为例演示一下逆向破解的过程
  - 实现微信消息防撤回

# 分析过程




破解点一：关掉接收网络指令的功能

破解点二：无法识别撤回指令

破解点三：无法执行撤回函数

# 分析过程

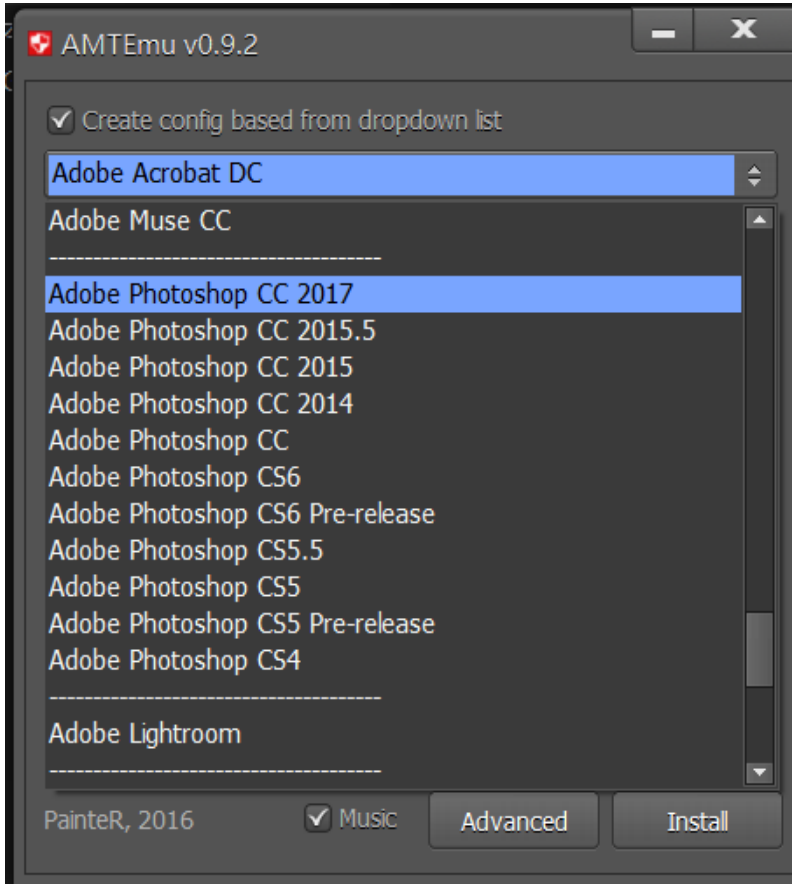
- 一般情况下软件逆向分析只对本地有效，结合密码学、web技术等可以产生较大范围的影响
- 但是逆向思维可以应用在学习、工作的方方面面，有助于快速地解决问题
- 网络上破解版本，或安装、替换文件的破解方法存在一定的风险

# 软件保护

- 法律层面
  - 申请专利
  - 申请软件著作权

# 软件保护

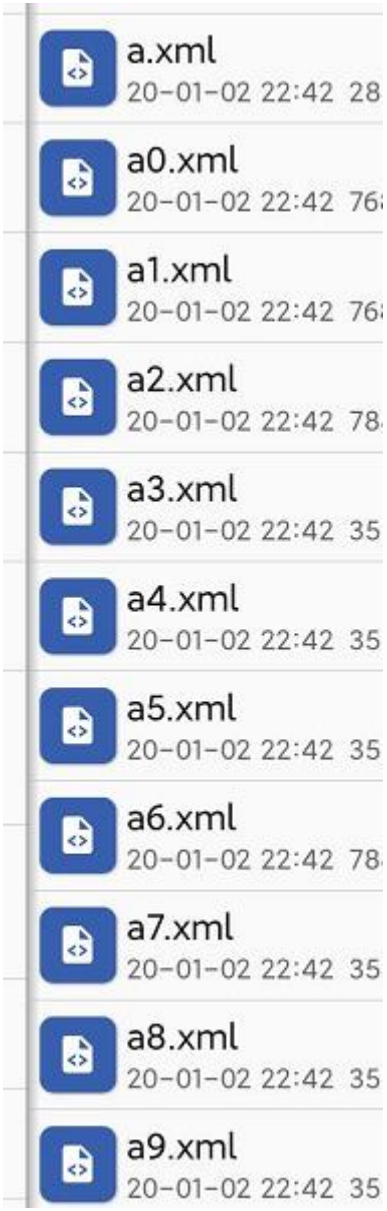
- 使用复杂的密钥算法
- 版本迭代时更换算法



# 软件保护

- 代码混淆
  - 字符代码混淆

将代码中的各种元素，如变量，函数，类的名字改写成无意义的名字。比如改写成单个字母，或是简短的无意义字母组合，甚至改写成“___”这样的符号，使得阅读的人无法根据名字猜测其用途。重写代码中的部分逻辑，将其变成功能上等价，但是更难理解的形式。比如将for循环改写成while循环，将循环改写成递归，精简中间变量，等等。打乱代码的格式。比如删除空格，将多行代码挤到一行中，或者将一行代码断成多行等等。



# 软件保护

- 代码混淆
  - 二进制代码混淆
    - 针对反汇编工具的缺陷进行设计使反汇编出错。
      - 花指令技术
    - 对代码加密混淆使静态分析无法得到真正的运行代码。
      - ASPack、UPX、Zprotect等加壳保护
    - 指令控制流混淆，增加理解、分析反汇编代码的难度。
      - VMProtect采用的虚拟化混淆技术

# 软件保护

- 虚拟机保护技术
  - 核心技术是指令虚拟化，是代码混淆技术的一种补充和延伸。使待保护程序代码变得极度复杂。
- 反调试技术
  - 反调试技术通过防止程序被调试来实现保护程序。一般的反调试技术处于Ring0或更上层，近年来结合硬件虚拟化技术提出基于硬件虚拟化的反调试软件保护技术，使反调试技术进一步深入底层，提高反调试保护的强度。

# 软件保护

- 软件加壳
  - 在二进制的程序中植入一段代码，在运行的时候优先取得程序的控制权，之后再把控制权交还给原始代码，这样做的目的是隐藏程序真正的OEP（入口点，防止被破解）。大多数病毒就是基于此原理。
  - 可执行程序资源压缩
  - 常用工具
    - UPX
    - VMP

# 软件保护

- 联网或本地验证软件及签名的完整性
  - 离线破解
  - 签名验证


# 软件保护

- 强制更新
  - 不更新就不能用
  - 适用于使用范围较小的软件
  - 软件出现能够对网络中其他用户产生较大影响的bug

# 总结

- 逆向思维很重要，快速地解决问题能力离不开较强的逆向思维
- 没有绝对安全的系统，无法从技术上完全保证软件安全
- 逆向与web等技术结合可以产生更大的影响
- 从系统设计之初就从顶层考虑安全问题
- 未来的趋势
  - 破解与反破解、调试与反调试的技术呈螺旋式对抗发展
  - 机器学习的方法来监控代码行为
  - 手工的分析调试不会被完全取代

# 参考资料


- 《编译原理》Alfred V.Aho Ravi Sethi等著 李建中 姜守旭 译
- 《软件加密技术内幕》看雪学院著
- 周祥. 低代价的软件防逆向分析方法研究与实现[D].西北大学,2017.
- Anas Alhamwieh, Said Ghoul. A Feature Based Methodology for Variable Requirements Reverse Engineering. 2019, 8(1)
- C. Basile,D. Canavese,L. Regano,P. Falcarin,B. De Sutter. A Meta-model for Software Protections and Reverse Engineering Attacks[J]. The Journal of Systems & Software,2018.

# 分享

- 只可用于交流学习，支持正版!可用于jetbrains下所有产品，测试Pycharm、Goland、IDEA均有效。

知乎

**pycharm2019永久激活，题主亲试几十次有效!**

over future

265 人赞同了该文章

再再再更更更一次次

**Licensed to https://zhile.io**
You have a perpetual fallback license for this version
Subscription is active until July 8, 2089

Runtime version: 11.0.6+8-b765.25 amd64
VM: OpenJDK 64-Bit Server VM by JetBrains s.r.o

知人者智，自知者明。胜人者有力，自胜者强。知足者富。强行者有志。不失其所者久。死而不亡者，寿。

谢谢！