Research of a New Shell Technique

Zufeng ZHONG

Zhanjiang Normal University, Zhanjiang, China

Email: *zhongzufeng@163.com*

Abstract: Focused on the principle and process of packing or unpacking, the fusion-packing technology emerged. This article contains the technology's principle, algorithm and implementation. The software experimental results show that the method can balance in safety and performance.

Keywords: packing; disassembly; software protection; fusion-packing

一种新的加壳技术的研究

钟足峰

湛江师范学院商学院，湛江，中国，524048

Email: zhongzufeng@163.com

摘　要：基于加、解壳原理和运行流程，提出了一种融合加壳方法，包括该方法的原理、算法和具体实现。软件加壳实验表明，这种方法在安全和性能上达到了良好的平衡。

关键词：加壳；反汇编；软件保护；融合加壳

1 引言

随着科技的发展，计算机应用已经渗透到人类生活的各个方面，其中软件起着至关重要的作用。计算机软件产品有开发完成后复制成本低、复制效率高的特点,所以往往成为遭受版权侵犯的对象[1]。

常见的软件侵权行为包括[2]：未经软件著作权人许可,发表、登记、修改、翻译其软件;复制或者部分复制著作权人的软件;故意避开或者破坏著作权人为保护其软件著作权取的技术措施。

据美国商业软件联盟(BSA)和市场调查公司 IDC 在 2008 年进行的一项软件盗版调查报告显示[3]，中国软件的盗版率在 2003、2004、2005、2006 和 2007 年分别为 92%、90%、86%、82%和 82%;相应年份造成的经济损失分别为 3823、3565、3884、5429 和 6664 百万美元。

国内外对通过技术手段对软件进行保护的方法和策略研究较多。通过技术手段进行软件保护主要是防止对软件产品的非法复制和使用,以及对软件产品进行的非法修改。软件技术保护的方式主要有以下几种，序列号保护方式：该方式主要保护非法权限用户使用软件，初次安装使用需要填入正确的序列号，成为授权用户才能使用所有功能，这种方式实现比较简单，不需要额外的成本，用户购买也非常方便，在互联网上 80%的软件都是使用这种方式保护[4]。网络验证方式：客户端安装过程中需要联网到服务器端获取关键数据和信息。适合网络软件。数据加密方式：使用各种加密算法如 RSA、DES、DSA、MDS、混沌密码学等对程序和数据进行加密。硬件保护方式：加密系统依赖特定的硬件(如:加密狗、加密卡等)来实施加密，因此其成本较高。

但是这些方法都存在一个明显的缺点:比较和跳转指令过于明显,很容易用底层调试软件跟踪到比较和跳转位置,然后把地址改为程序继续执行的位置即可破解。

而为了解决该问题，提出了加壳技术。

2 传统加壳技术及其缺陷

为了保护在 PC 上运行的软件就必须给原始软件加上一层保护壳。这个壳类似于自然界植物种子外层的壳。软件的壳就是一段专门负责保护软件不被非法修改或反编译的程序。它们一般是先于程序运行，拿到控制权，然后完成它们保护软件的任务。使用外壳的好处在于可以很好地防止静态分析、文件补丁和动态跟踪[5]。这样无需做更多的事情而只需要一个简单

湛江市科技攻关项目（项目号：湛科[2009]67 号）
湛江师范学院资助科研项目（项目号：W0721）

的壳就可以实现软件的保护。加壳软件按照其加壳的目的和作用，可分为两类:一是压缩，二是保护。压缩壳的主要目的是减小程序体积;保护壳使用了各种反跟踪技术保护程序不被调试、脱壳。常用的加壳软件有 ASPack、UPS、PECompact、ASProtect 等。

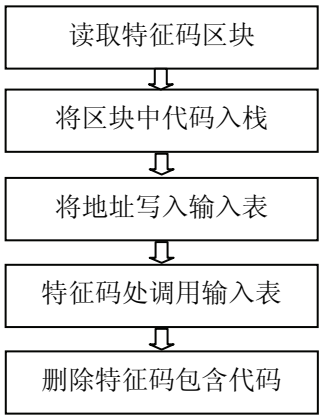
一般壳的加载过程如下：(1)首先获取壳自身所需要使用的 API 地址：加壳后输入表有了改变，而壳需要 API 函数来完成其功能。(2)解密原程序的各个区块的数据：如果加壳时用到了压缩技术，那么在解密前还要进行解压缩。(3)重定位：文件执行时将被映像到指定内存地址（基地址）中，系统不能保证每次 DLL 文件运行的基地址一样，则需要进行重定位。(4)修改输入表：壳对源程序的输入表进行修改，模仿系统填充输入表中的数据。(5)跳转到程序原入口点：把控制权交给原程序。

加壳软件的脱壳方法通常如下：首先使用 PEID[6]、FI、PE-SCAN 等查壳软件通过特征码对比查找出壳的类型。根据壳代码到原始代码区段中间的大跳转来确定 OEP。当跟踪到 OEP 时进行抓取内存映像文件，对内存数据进行优化处理后再写入磁盘。最后修复输入表和重建可编辑资源。

虽然各种加壳技术十分复杂，但通过以上方法还是能进行脱壳。针对这类脱壳方法，本文提出一种融合加壳方法，它能够有效防止这类脱壳。

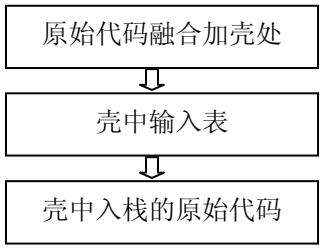
3 基融合加壳技术原理

融合加壳技术就是将原始程序中的关键代码和壳进行结合，即将原始程序中代码剪切到壳中，如果软件破坏者进行脱壳，则壳中所包含的原始代码也将被脱去，导致原始程序将不完整，甚至不能运行。加壳算法步骤如下：



在原始程序中关键代码处插入特征码组（成对包含一段关键代码），加壳时搜索该特征码组，将特征码组包含的汇编代码入栈，将壳中保存的代码地址写入输入表，并和特征码处代码对应，将原始程序中的代码删除。

当程序运行时调用算法如下：



当原始代码执行到该段代码时，根据输入表找到壳中的代码保存的栈中，进行调用。如果破解者通过脱壳技术将壳脱掉，则保存在壳中的原始代码也将被脱掉，则原始软件将不能运行，起到保护的作用。

4 融合加壳实现

系统使用 VC++进行实现。系统包括如下功能：

判断文件格式：程序处理的加密对象是 PE-EXE 文件，所以在对文件进行处理前必须先判断目标文件是否为正确的 PE-EXE 文件。先检验文件头部第一个字的值是否等于 IMAGE_DOS_ SIGNATURE，其次校验比较 PE header 的第一个字的值是否等于 IMAGE_NT_SIGNATURE。最后在验证是 EXE 还是 DLL 文件。

文件基本数据的读入：利用 GetfileSize 函数取得待处理文件的大小，然后申请一块同样大小的内存，再一次性读入整个文件。

文件压缩：为了保持原始程序文件的结构，PE 文件的压缩按区块进行，方便程序的载入与还原。还有一些区块如资源块(.rsrc)、输出块(.edata)和只读数据块(.rdata)等要进行处理后才能压缩。

资源区块的处理：资源区块需要进行处理后才能压缩，处理流程如下：先找到资源区块的起点地址，通过地址移动到资源区块位置，将其中不能压缩的写入文件，其他的压缩后写入文件。

输入表的处理：把外壳中的一段程序代码写入输入表，然后在通过这段程序代码转接到真正的原始程序代码执行。

融合壳技术实现：通过特征码找到需要融合的代

978-1-935068-10-5 © 2010 SciRes.

码，将其写入壳中，并将原始程序中的代码删除，修改成连接壳中代码段。

外壳程序实现：主要实现还原和初始化原始程序，其中包括一些自保护功能，如反跟踪和反调试代码，程序完整性检查等。

4 总结

通过与传统加壳软件对比实验表明，该加壳方法虽然在效率方面有所降低，但将大大提高程序的安全性，而随着现今硬件的发展，程序运行效率的一点降低完全能够容忍。同时，软件的安全性是一个系统的工程，网络传输、加密算法、加壳保护等各方面都需要加强。

致　谢

本文的完成感谢各位同事的帮助和协助。没有这些支持，本文很难继续，无限感激。

References (参考文献)

[1] TanMao, ChenYi .Study on software copyright protection technology [J]. computer applications and software.2007, 1: 54-56.
谭貌，陈义，软件版权保护技术的研究与分析[J]，计算机应用与软件，2007, 1: 54–56.

[2] MIKai, Shi Shangyuan. The Intellectual Property Research of Open Source Software[J]. Journal of Modem Information. 2009, 9: 4–6.
糜凯，史尚元，开源软件的知识产权研究[J]，现代情报，2009, 9: 4–6.

[3] Fifth ANNUAL BSA and IDC Global Software Piracy Study. http://www.bsa.org.cn/.2008.

[4] Duan gang. Encryption and Decryption[M]. Beijing: publishing house of electronics industry. 2003. 160–197.
段钢，加密与解密(第 2 版)[M]，北京:电子工业出版社， 2003. 160–197.

[5] Lei fanggui, Software's Encryption and Decryption[M]. Changsha: publishing house of central south university.1995, 23–28.
雷方桂，软件加密解密技术及应用，长沙，中南工业大学出版社，1995, 23–28.

[6] Li lu. Design and Analysis the Key Technologies of Packing Using by Object Code Obfuscation [D]. Suzhou:Soochow university, 2009.
李露，目标代码混淆加壳技术[D]，苏州，苏州大学，2009.