工程硕士学位论文

抗逆向分析 PE 文件保护系统研究与实现

田淞煜

哈尔滨理工大学

2021 年 4 月

国内图书分类号：TP301.6

工程硕士学位论文

抗逆向分析 PE 文件保护系统研究与实现

硕士研究生： 田淞煜

导　　师： 李鹏

申请学位级别： 工程硕士

学科、专业： 计算机技术

所在单位： 计算机科学与技术学院

答辩日期： 2021 年 4 月

授予学位单位： 哈尔滨理工大学

Classified Index：TP301.6

Dissertation for the Master Degree in Engineering

Research and implementation of PE file protection system for antistress analysis

Candidate： Tian Songyu
Supervisor： Li Peng
Academic Degree Applied for： Master of Engineering
Specialty： Computer Technology
Date of Oral Examination： April, 2021
University： Harbin University of Science and Technology

哈尔滨理工大学硕士学位论文原创性声明

本人郑重声明：此处所提交的硕士学位论文《抗逆向分析 PE 文件保护系统研究与实现》，是本人在导师指导下，在哈尔滨理工大学攻读硕士学位期间独立进行研究工作所取得的成果。据本人所知，论文中除已注明部分外不包含他人已发表或撰写过的研究成果。对本文研究工作做出贡献的个人和集体，均已在文中以明确方式注明。本声明的法律结果将完全由本人承担。

作者签名：　　日期：　　年　　月　　日

哈尔滨理工大学硕士学位论文使用授权书

《抗逆向分析 PE 文件保护系统研究与实现》系本人在哈尔滨理工大学攻读硕士学位期间在导师指导下完成的硕士学位论文。本论文的研究成果归哈尔滨理工大学所有，本论文的研究内容不得以其它单位的名义发表。本人完全了解哈尔滨理工大学关于保存、使用学位论文的规定，同意学校保留并向有关部门提交论文和电子版本，允许论文被查阅和借阅。本人授权哈尔滨理工大学可以采用影印、缩印或其他复制手段保存论文，可以公布论文的全部或部分内容。

本学位论文属于

保密□，在　　年解密后适用授权书。

不保密□。

(请在以上相应方框内打 √)

作者签名：　　日期：　　年　　月　　日

导师签名：　　日期：　　年　　月　　日

抗逆向分析 PE 文件保护系统研究与实现

摘 要

在软件行业快速发展的同时，软件逆向工程技术和二进制分析技术也在快速发展和进步，使得逆向软件分析者对软件的逆向能力和分析效率大大提高，给软件安全保护工作带来极大挑战。

为应对逆向分析给 Windows 软件带来的安全威胁，本文提出并实现了一个针对 Windows 可执行程序的安全保护系统，该系统对可执行程序逆向中的静态分析和动态分析过程进行保护，有效提高了逆向分析者的分析难度。采取的主要保护措施有：一、加壳，在已有虚拟机加壳技术的基础上进行改进，提出多样化 Handler 的保护机制；二、代码混淆、通过对软件进行混淆处理，改变程序的运行时的函数块的结构并增加指令的复杂度，以此来增加逆向分析的难度。

本文以增强 PE 文件的抗逆向能力为目的，对 Windows 平台下的 PE 文件的二进制混淆技术和虚拟机加壳技术进行研究，主要工作包括：

一、PE 文件加壳技术的研究。首先对 PE 文件的加载过程和 PE 文件的文件结构进行分析，总结常见加壳方式不足，在虚拟机加壳的基础上，提出多样化 Handler 虚拟机加壳技术，对同一个 Handler 进行多样化的指令实现，使得同一个功能模块有不同的二进制指令实现，有效增加逆向分析者的分析成本。

二、PE 二进制混淆技术的研究。首先对二进制混淆技术进行分析，总结常见二进制混淆方法的不足，提出建立索引进行函数间基本块交换的混淆算法，给出了混淆算法的整体思想，给出了对 PE 文件进行基本块交换后的重构方法。

三、根据提出的 PE 文件加壳方法和混淆算法设计并实现了一个 PE 文件保护系统，系统包括 PE 文件虚拟机加密壳和 PE 文件二进制混淆器。对该系统的设计与实现进行了详细阐述，并对 PE 文件虚拟机加密壳和 PE 文件二进制混淆器进行功能的验证和性能评估。实验结果表明提出的多样化 Handler 虚拟机加壳方式和二进制代码混淆算法均有效，都有效增强了 Windows 的 PE 文件的抗逆向分析能力。

关键词 逆向工程，代码混淆，PE 文件保护，加壳，软件保护;

Windows executable virtual machine shell

Abstract

With the rapid development of the software industry, software reverse engineering technology and binary analysis technology are also developing and progressing rapidly, which greatly improves the reverse-software analysts' ability and analysis efficiency of software, and brings great challenges to software security protection.

In order to deal with the security threats brought by the reverse analysis to Windows software, this paper proposes and implements a security protection system for Windows executable program, which protects the static analysis and dynamic analysis process in the reverse of the executable program and effectively improves the difficulty of the analysis for the reverse analyst. The main protection measures adopted are as follows: 1. Packer improvement is made on the basis of the existing virtual machine packer technology, and a diversified Handler protection mechanism is proposed; 2. Second, code obfuscation. The software can be obfuscated to change the structure of the function block and increase the complexity of instructions in order to increase the difficulty of reverse analysis.

In order to enhance the anti-directional ability of PE files, this paper studies binary obfuscation technology and virtual machine shell technology of PE files under Windows platform. The main work includes:

I. Research on PE file packing technology. Of PE file loading process and the PE file structure analysis, summarizes the common packers way is not enough, on the basis of the virtual machine and shell, diversified add case Handler virtual machine technology is put forward, to achieve diversification of instruction, the same Handler has the same functional modules have different binary instructions, effectively increase the reverse analysis is the analysis of the cost.

Second, PE binary obfuscation technology research. Firstly, this paper analyzes binary confounding technology, summarizes the shortcomings of common binary

confounding methods, proposes a confounding algorithm for basic block exchange between functions by building index, gives the whole idea of the confounding algorithm, and gives a reconstruction method for PE files after basic block exchange.

A PE file protection system is designed and implemented according to the proposed PE file packing method and obfuscation algorithm, which includes a PE file virtual machine encryption shell and a PE file binary obfuscation. The design and implementation of the system are described in detail, and the PE file virtual machine encryption shell and PE file binary obfuscation are validated and the performance is evaluated. The experimental results show that the proposed multiple Handler virtual machine shell method and binary code obfuscation algorithm are both effective, which effectively enhance the anti-direction analysis ability of Windows PE file.

Keywords reverse engineering, code obfuscation, PE file protection,packing, software protection