Broadview
www.broadview.com.cn

安全技术大系

看雪软件安全
http://www.pediy.com

GOOD
畅销书升级版

加密与解密

第三版

段钢 编著

揭示软件加密与解密最核心
看雪安全技术团队全力支持

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

安全技术大系

看雪软件安全
http://www.pediy.com

加密与解密

第三版

段钢 编著

電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

内 容 简 介

本书以加密与解密为切入点，讲述了软件安全领域许多基础知识和技能，如调试技能、逆向分析、加密保护、外壳开发、虚拟机设计等。读者在掌握本书的内容时，很容易在漏洞分析、安全编程、病毒分析、软件保护等领域扩展，这些知识点都是相互的，彼此联系。国内高校对软件安全这块领域教育重视程度还不够，许多方面还是空白，而近年来社会和企业对软件安全技术人才需求逐年上升。从就业角度来说，掌握这方面技术，可以提高自身的职场竞争能力；从个人成长角度来说，研究软件安全技术有助于掌握许多系统底层知识，是提升职业技能的重要途径。作为一名合格的程序员，除了掌握需求分析、设计模式等外，如能掌握一些系统底层知识，熟悉整个系统的底层结构，对自己的工作必将获益良多。

本书可以作为大中专学校或培训机构的软件安全辅助教材，是安全技术爱好者、调试人员、程序开发人员不可多得的一本好书。

图书在版编目（CIP）数据

加密与解密 / 段钢编著. —3 版. —北京：电子工业出版社，2008.7
（安全技术大系）
ISBN 978-7-121-06644-3

I. 加… II. 段… III. 电子计算机－密码术 IV. TP309.7

中国版本图书馆 CIP 数据核字（2008）第 064470 号

策划编辑：郭 立
责任编辑：葛 娜
印 刷：北京智力达印刷有限公司
装 订：北京中新伟业印刷有限公司
出版发行：电子工业出版社
北京市海淀区万寿路 173 信箱 邮编 100036
开 本：880×1230 1/16 印张：35.5 字数：1018 千字
印 次：2008 年 7 月第 1 次印刷
印 数：6000 册 定价：59.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

作 者 简 介

本书由看雪软件安全网站（看雪学院）站长段钢主持编著。在本书的编写过程中，参与创作的每位作者倾力将各自擅长的专业技术毫无保留地奉献给广大读者，使得本书展现出了极具价值的丰富内容。如果读者在阅读本书后，能够感受到管窥技术奥秘带来的内心的喜悦，并愿意与大家分享这份感受，这是作者最大的愿望。

主 编：段 钢

编 委：（按章节顺序排列）

Blowfish，沈晓斌，丁益青，单海波，王勇，赵勇，唐植明，softworm，afanty，李江涛，林子深，印豪，冯典，罗翼，林小华，郭春杨

编委档案

Blowfish

看雪首席版主。经验丰富的大龄程序员。1992 年上大学始接触电脑，1997 年读研期间接触网络并自学加密与解密技术，一发不可收拾，其时常在教育网 BBS 灌水。喜多方涉猎，亦能抓住一点深入钻研，对逆向分析技术尤为痴迷。多年来常在看雪论坛灌水，见证了论坛的风风雨雨，也结识了一些不错的朋友。

参与章节：第 5 章　5.1 序列号保护方式

第 14 章　14.5 软件保护的若干忠告

沈晓斌

看雪核心专家团队成员。看雪论坛 ID 为 cnbragon，现攻读密码学专业硕士学位。最初的爱好是网络安全，进而研究软件的逆向工程，对密码学的兴趣由此而发。对密码学的各个方面都有所涉猎，尤其擅长密码学在软件保护中的应用研究。独立完成了一个加密算法库 CryptoFBC。译作有《程序员密码学》。

个人主页：www.cnbragon.cn

参与章节：第 6 章　加密算法

丁益青

看雪技术专家。看雪论坛 ID 为 cyclotron，复旦大学在读硕士研究生，复旦大学日月光华 BBS 黑客与系统安全版版主，致力于 Windows 环境下可执行文件的加密解密与逆向工程研究。主要作品有 EmbedPE、IDT Protector、PEunLOCK 等。

个人主页：cyclotron.yculblog.com

参与章节：第 8 章　8.3 伪编译

单海波

看雪核心专家团队成员。看雪论坛 ID 为 tankaiha，生于六朝古都南京，硕士研究生毕业，现任某研究

所工程师，工作之余好与计算机为伴。2002 年接触汇编并热衷于病毒技术学习，后偶遇看雪学院，遂终日游戏于程序加密与解密，不可自拔。2006 年与 kanxue 及坛中数位好友成立.net 安全小组 DST（Dotnet Reverse Team），共同探讨.net 平台下的软件安全技术。

个人主页：http://vxer.cn/blog

参与章节：第 9 章　.Net 平台加解密

王　勇

看雪技术专家。毕业于石油大学（华东）计算机科学与技术专业。擅长 C/C++、ASM 和驱动程序开发。对面向对象程序设计和 Windows 系统底层的研究有丰富的经验。很高兴这次能与各位高手一起合作，也希望能与编程爱好者及加密解密爱好者更多的交流。

主页：http://www.w-yong.com

参与章节：第 10 章　10.15 编写 PE 分析工具

赵　勇

看雪技术专家。来自江苏江阴，计算机业余爱好者，兴趣爱好广泛。

参与章节：第 13 章　13.6 附加数据

唐植明

看雪技术核心权威。看雪论坛 ID 为 DiKeN，2002 年毕业于兰州大学，计算机科学与技术专业。爱好逆向工程，iPB（inside Pandora's Box）组织创始人（在这儿更是要感谢组织的兄弟姐妹们，大家团结友好，互相学习，为 iPB 的成功做出了巨大努力），曾在 2002 年编写过《加密与解密实战攻略》算法部分。

参与章节：第 13 章　13.10 静态脱壳

softworm

看雪技术天才。70 后一代，非计算机专业的业余爱好者。1998 年开始接触逆向与破解，迄今已近 10 年，终于达到了“知道自己不知道”的境界。感兴趣的方向包括壳、虚拟机保护、病毒引擎、Rootkit。后两项还处于只知道名字的水平，愿与有共同爱好的朋友们一起学习。

E-mail：softworm2003@hotmail.com

参与章节：第 13 章　13.9.2 Thmedia 的 SDK 分析

afanty

看雪技术专家。多年专业研究软件加/解密技术。

参与章节：第 14 章　14.1 防范算法求逆

李江涛

看雪技术核心权威。看雪论坛 ID 为 ljtt，喜欢学习编程技术，常用编程语言为 VC/MASM。对 PB、VFP 的反编译有深入的研究，写过 DePB、FoxSpy 等程序。平时大多数时间都在电脑上耕作，最大的希望是能够领悟到编程的精髓，写一个自己比较满意的作品。

E-mail：shellfan@163.com

参与章节：第 14 章　14.2.2 SMC 技术实现

林子深

看雪技术导师。看雪论坛 ID 为 forgot，1989 年生，看雪论坛外壳开发小组组长。熟悉 Win32 平台和 80x86 汇编，擅长代码的逆向，对壳的研究比较多。

E-mail：forgot@live.com

参与章节：第 12 章　12.4.1 虚拟机介绍

第 14 章　14.2.4 简单的多态变形技术

第 15 章　反跟踪技术

印　豪

看雪资深技术权威。看雪论坛 ID 为 Hying，擅长加壳技术，拥有独立创作的加密利器。

E-mail：newhying001@163.com

参与章节：第 16 章　外壳编写基础

冯　典

看雪技术天才。看雪论坛 ID 为 bughoho，1990 年生，来自四川，看雪论坛虚拟机开发小组组长，目前工作主要是从事逆向研究。

个人自述：记得 14 岁时家里买了台电脑，使我对编程有了极大的兴趣。16 岁上高一时已对读书彻底不感兴趣，于是退学（现在的我才发现，我并不是对读书感兴趣，而是对教育制度的反感）。后来听了家人的意见，转读四川新华电脑学校，感受颇多，一月之后便退学，至于为什么我就不说了。17 岁时，一个偶然的机会，使我对逆向有了浓厚的兴趣，并接触到看雪论坛，也认识到了 kanxue。承蒙 kanxue 抬举，让我执笔虚拟机这一章，由于我并不是一个才高八斗的人，所以写得也没有那么的妙笔生花、鬼斧神工了。

参与章节：第 17 章　虚拟机的设计

罗　翼

看雪技术专家。资深程序员，由加/解密知识起接触编程，对 Windows 底层机制有多年的研究经验。后由于工作需要，接触 C++/ATL/COM 等技术。现致力于研究各种 Moder C++的元素的应用范围及其对降低程序复杂度所起的作用，热切关注 ISO C++以及分布式计算相关内容的进展。

参与章节：第 18 章　18.2.1 跨进程内存存取机制

18.2.2 Debug API 机制

18.2.3 利用调试寄存器机制

林小华

看雪资深版主。看雪论坛 ID 为 linhansh，武汉大学电力系统及其自动化专业，『工具分区』区版主，对论坛的工具版块发展做出了重大贡献。

个人主页：http://blog.csdn.net/linhanshi

参与章节：第 18 章　18.4 补丁工具

郭春杨

看雪技术专家。看雪论坛 ID 为 Yonsm，软件工程师，从事视频编解码和多媒体软件设计工作。对 Windows 和 Windows Mobile 系统有比较深入的了解。

主页：WWW.Yonsm.NET

E-mail：Yonsm@163.com

参与章节：附录 B　在 Visual C++中使用内联汇编

前　言

软件安全是信息安全领域的重要内容，涉及到软件相关的加密、解密、逆向分析、漏洞分析、安全编程以及病毒分析等。目前，国内高校对软件安全教育重视程度不够，许多方面还是空白。随着互联网应用的普及和企业信息化程度的不断提升，社会和企业对软件安全技术人才需求逐年上升，在计算机病毒查杀、网游安全、网络安全、个人信息安全等方面人才缺口很大，相关职位待遇较高。从就业角度来看，掌握软件安全相关知识和技能，不但可以提高自身的职场竞争能力，而且有机会发挥更大的个人潜力，获得满意的薪酬；从个人成长方面来说，研究软件安全技术有助于掌握许多系统底层知识，是提升职业技能的重要途径。作为一名合格的程序员，除了掌握需求分析、设计模式等外，如能掌握一些系统底层知识，熟悉整个系统的底层结构，对自己的工作必将获益良多。

本书以软件加密与解密为切入点，讲述了软件安全领域相关基础知识和技能。读者在阅读了本书的内容后，很容易在漏洞分析、安全编程、病毒分析等领域得到扩展。这些知识点的相互关联性，将促使读者开阔思路，使所学融会贯通，领悟更多的学习方法，提升自身学习能力。

本书是《加密与解密》的第三版，此书今天能够与读者见面，完全是广大读者的热情和鼓舞带来的成果，作者深表谢意。

关于看雪学院

本书作者是软件安全主题网站——“看雪学院”的站长。看雪软件安全网站（www.pediy.com）由 kanxue（作者网名）创建于 2000 年。网站历经 8 年多的发展，脱颖而出，凭借自身实力，已经成为中国软件安全领域公认的最权威的技术站点，影响深远。

2000 年初，笔者想找一些研究软件加解密的朋友交流一下，但十分令人遗憾的是，那时国内这方面的技术资料很缺乏，不成系统，大家的交流也十分有限。因此，笔者自己建立了一个主页“看雪学院”，期望与兴趣相投的朋友共同探讨加密与解密的知识。当初这个简单的网站，就是今天看雪软件安全网站的雏形，并且是当时国内唯一从技术角度研究软件加/解密的站点。很短的时间，这个站点就获得了大家的认同，并在广大网友的支持下，健康地成长起来。随着我们的努力，网站推出的软件调试论坛逐渐成为国内知名度最高的软件安全论坛，吸引了众多高手。

本着知识共享，一切免费的建站宗旨，看雪软件安全网站汇聚了大量高水平的技术文章，至今为止原创了数千余篇精华文章，极大地推动了国内软件安全技术的发展。2007 年论坛改名为看雪软件安全论坛，论坛在保持已有的软件加密与解密研究方面外，在漏洞分析、系统底层、病毒分析、Rootkit 等技术领域进行全面扩展，逐步发展为信息安全的综合服务网站。

多年来，看雪软件安全网站一直遵循纯技术的发展策略，不但在行业中树立了令人尊敬的专业形象，更使一大批专业人士和专家聚集在这里，形成了一个技术交流的网上家园，带动了大批对软件安全感兴趣的网友加入进来，构建起了一个围绕软件安全主题的活跃的大社区，历久弥新。正是看到这种技术气氛，不少知名的公司都很关注论坛技术人才，如微软公司信息安全部门、珠海金山毒霸公司、深圳腾讯公司、

360 安全中心、启明星辰以及部分网游公司等。

为了推进软件安全技术为社会和企业服务的理念，我们正在努力提升看雪网站的社会作用和价值，从而为关注信息安全的大众，提供更好的服务和技术产品。

看雪软件安全网站，汇聚了许多志趣相投的朋友，经历了风风雨雨的 8 年，一直走到今天实属不易。作为网站站长和此书的作者，本人在此由衷地感谢所有关心和支持我们的共同事业，参与共同发展的朋友们！每到网站最困难的时候，是你们伸出无私的援助之手，才让网站渡过了一个个难关，能有今天的大好局面！在此特别鸣谢以下朋友和机构的大力支持：

海城金航网络科技有限公司阿男为网站提供网站空间

雅联网络服务有限责任公司李智勇为论坛提供独立服务器

南京慧速科技发展有限公司刘小荣为论坛提供独立服务器

感谢陈超达为服务器安全维护所做的大量工作

本书的缘起

当今的信息社会里，安全技术越来越重要了，如何普及软件安全知识是作者始终关注的一个大问题。正是为了更好地将软件安全知识普及到社会各个领域的愿望，促成了本书的问世。

依托看雪学院的技术背景，由作者主编和主导的看雪软件安全系列书籍，目前已出版发行了《加密与解密——软件保护技术及完全解决方案》（简体版，繁体版）、《加密与解密（第二版）》（简体版，繁体版）、《软件加密技术内幕》等书籍；基于电子资料的形式，历年发行的《看雪论坛精华》被众多网站转载，保守计算，其下载量已经超过数百万份，极大地推动了国内软件安全技术的发展。

这是一本很难写的书，因为 2000 年时，软件安全是一个全新的领域。从 Windows 95 面世以来的 6 年内，市面上没有一本这方面的书，网上也缺乏相关资料。为了填补国内 Windows 平台上加密与解密书籍的空白，作者与看雪论坛的一流好手努力合作，克服种种困难，于 2001 年 9 月推出了国内第一本全面介绍 Windows 平台下软件加密与解密技术的书籍，这就是本书的第一版《加密与解密——软件保护技术及完全解决方案》。

在第一版中，我们试图从软件加密和解密这两个方面对当今流行的软件保护技术进行分析。希望读者看过此书之后，能够对各种流行的软件保护与破解技术有所了解。

第一版一面世就得到了广大读者的喜爱和认可，获得了 2002 年全国优秀畅销书奖（科技类）！在全国很多计算机专业书店获得了名列前茅的销售业绩，而且一年来在著名的华储网销售排行中都被排在前几名内。次年，本书在台湾发行了繁体版，得到了台湾读者的热烈欢迎。


全国优秀畅销书
证 书
电子工业出版社：
你社出版的《加密与解密——软件保护技术及完全解决方案》一书，经我会评选委员会评审，被评为2002年度全国优秀畅销书（科技类）。
特发此证书。
中国书刊发行业协会
二〇〇二年十一月


获奖证书
你社出版的《 》荣获
2002年度
特颁此证

2003 年 6 月以本书第一版为基础，完成了本书的第二版《加密与解密》。

笔者从 2004 年开始第三版的更新准备工作，这个版本编写时间比较长，前后用了四年多的时间才得已完稿。这是所有参与者共同的努力，是他们把自己才华中最精彩部分展现给大家了。

现在读者看到的这本 500 多页的图书，几乎包含了当今 Windows 32 位环境下软件保护技术的绝大部分内容，从基本的跟踪调试到深层的拆解脱壳；从浅显的分析注册到中高级软件保护与分析，其跨度之广、内容之深，国内至今尚无同类出版物能与之比肩。

第三版的变化

第三版是在《加密与解密》第二版与《软件加密技术内幕》两本书的基础上完成的，删除了第二版中的过时内容，将《软件加密技术内幕》一些知识点补充融合进来，结构更加合理。

1. 讲解通俗，突出基础

本书加强了基础部分的篇幅，系统讲解软件逆向的整个基本流程，包括动态分析、静态分析，以及逆向分析的基础知识。比如重点讲解了逆向必备工具 OllyDbg 和 IDA 的用法，并详细讲述逆向分析的基础知识，初学者通过相关几章的学习，可以轻松入门。

2. 案例丰富，覆盖面广

书中提供了大量的案例分析，方便读者理论与实践相结合。通过实际操作，提高读者的调试分析能力。

3. 加强了密码学算法

密码学算法越来越多地应用在软件保护领域，调试软件必须对比较知名的密码学算法有一定的了解。“加密算法”这一章，讲解了常见密码学算法的应用。

4. 新增.Net 技术

随着微软.Net 平台的推广，越来越多的开发者开始关注.Net 程序的安全。.Net 这章向读者普及了.Net 安全的基本知识。

5. 加强脱壳基础知识的篇幅

脱壳一章的结构和内容规划，参考了大量的建议，组织更加合理，完全为脱壳新手量身定做。

6. 软件保护技术实施

相关章节详细研究了大量极具商业价值的保护技术，包括反跟踪技术、外壳编写基础、虚拟机的设计等，读者完全可以将这些技术应用到自己软件保护之中去。

7. 二次开发与补丁技术

“代码的二次开发”一章中讲解如何在没有源码的情况下，扩充程序功能，打造开发接口；“补丁技术”一章讲解如何自己编程实现内存补丁或内存注册机。

本书预备知识

在阅读本书前，读者应该对汇编语言有大致的了解。汇编语言是大学计算机的必修课，这方面的书籍品种很多，如《IBM PC 汇编语言程序设计》，虽然大多数书以 DOS 汇编为讲解平台，但对理解汇编指令功能依然有益。

读者如果熟悉和了解 C 语言，对阅读本书是很有帮助的。

建议掌握一些 Win32 编程，不论研究加密与解密，还是编程，都应该了解 Win32 编程。Win32 编程是 API 方式的 Windows 程序设计，学习 Windows API 能使读者更深入地了解 Windows 工作方式。此类书籍推荐您阅读 Charles Petzold 所著的《Windows 程序设计》，该书堪称经典之作，它以 C 语言为讲解平台。

到此为止，作者将不再假设你已经具有任何加/解密的经验了。

适合的读者

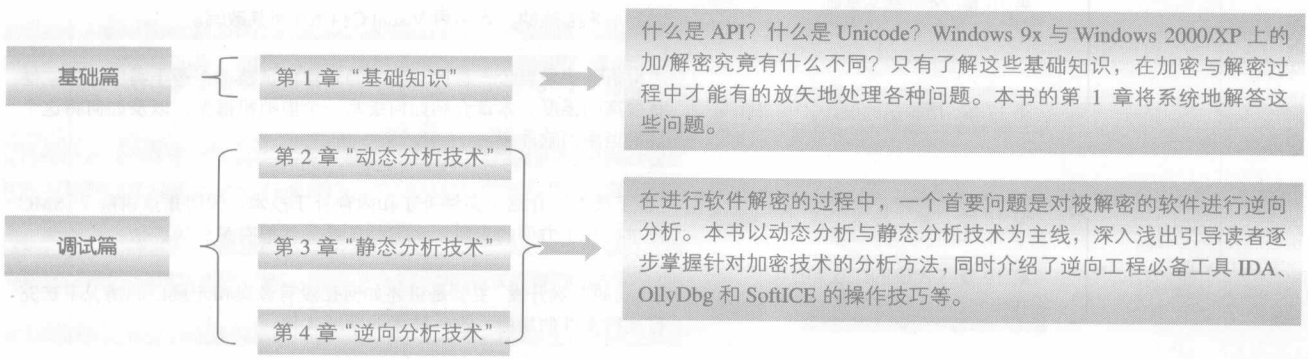
本书适合以下读者：

- 软件安全技术相关工作者：本书是软件安全研究的一本不错的技术字典；
- 对调试技术感兴趣的读者：提高读者的调试技能，增强软件的质量；
- 对软件保护感兴趣的软件开发人员：更好地保护你的作品；
- 大中专在校学生：通过本书掌握的相关知识和技能，将使你获得职场竞争的秘密武器；
- 其他：关注个人信息安全、计算机安全技术，并且想了解技术内幕的朋友，可以从中获得答案。

内容导读

大多数人可能认为软件加密与解密是一门高深的学问。造成这种认识的原因是以前这方面的技术资料缺乏，从而将“加密与解密”这一技术“神”化了。初学者一般不知从何下手，由于没方向，花费了大量时间和精力，走了不少弯路。本书给对这方面感兴趣的读者指明一个方向，提供一个捷径。

本书大部分章节既关联又彼此独立，因此读者可以根据自己情况，选择合适自己的内容阅读。



解密篇

- 第 5 章“常见的演示版保护技术”：一些软件作者对软件保护方案的策划与实施很不以为然，他们往往自以为是的保护在解密者看来其实不堪一击。希望本部分能让这些软件作者了解一些软件攻击的方法，以便更好地保护自己的作品。
- 第 6 章“加密算法”：当今时代，研究加密与解密不掌握点密码学的知识是不可思议的。本章详细讲解了 MD5、SHA、CRC、RSA、ElGamal 等知名算法在软件保护方面的应用，并提供了全部实例的源码。

语言和平台篇

- 第 7 章“Delphi 程序”
- 第 8 章“Visual Basic 程序”

读者应该了解，不论加密和解密，都需要根据软件的编译语言的特点进行，才能达到比较理想的效果。现在编程所使用的语言主要是两种运行形式：一种是解释执行的语言，另一种就是编译后才能够执行的语言。解释语言的弱点之一是容易被反编译，因此其保护的重点应放在如何防止反编译上。

- 第 9 章“.Net 平台加解密”：.Net 是微软的一个重要战略步骤，越来越多的企业已经在.Net 平台上开发自己的产品。由于.Net 的“特殊性”，对其反编译很容易获得相应的源码，因此，摆在企业和.Net 程序员面前一个迫切需要解决的问题，就是.Net 安全性！

系统篇

- 第 10 章“PE 文件格式”：PE 是 Windows 上可执行文件的格式，了解 PE 文件格式将有助于对操作系统的深刻理解。如果你知道 EXE 和 DLL 里面的奥秘，将有助于提升你个人技术的含金量。本书用大量篇幅，图文并貌地详细讲解了 PE 格式。作为初学者，PE 格式的细节部分可以暂时跳过，需要了解此部分内容时，可以随时查阅。
- 第 11 章“结构化异常处理”：SEH 的出现已非一日，但有关 SEH 的知识资料却不是很多。SEH 不仅可以简化程序的错误处理，使程序更加健壮，还被广泛应用于反跟踪和加密中。本书从调试角度讲述了 SEH 的机理，掌握这些内容后，调试 SHE 处理的程序，就会更加自如。

脱壳篇

- 第 12 章“专用加密软件”：市场虽有大量现成的保护方案可选用，如基于软件的加密壳保护和基于硬件的加密锁保护产品。这些优秀的保护方案由于太流行，造成大家对其研究的深入和核心技术的公开化，反而容易被破解。因此，有必要自己实现部分保护方法，提高软件产品安全性。
- 第 13 章“脱壳技术”：现在越来越多的软件都采用了加壳保护。在对一款软件分析和汉化过程中，脱壳是必不可少的一步，本章详细介绍了各种壳的脱壳技巧。

保护篇

- 第 14 章“软件保护技术”：这部分介绍一些实用的软件保护与反跟踪技术，读者可以将这些技术直接移植运用到自己的软件中。
- 第 15 章“反跟踪技术”：深入浅出的讲解，将看似杂乱的知识点巧妙地串联起来，使读者对当前各种反调试技术有一个全新的认识。
- 第 16 章“外壳编写基础”：本章取材自《软件加密技术内幕》，原作者是印豪。原文章外壳部分是以汇编来描述的，本书用 Visual C++ 6.0 将其改写。
- 第 17 章“虚拟机的设计”：虚拟机保护是当今一种比较热门的软件保护技术，基于其保护的软件有很高的强度。本章介绍如何编写一个虚拟机框架，以及如何将这个技术运用到软件中。

PEDIY 篇

- 第 18 章“补丁技术”：“补丁技术”介绍了文件补丁和内存补丁技术，同时重点讲解了 SMC 技术在补丁方面的应用。学习补丁是一件很有意思的事情。
- 第 19 章“代码的二次开发”：“代码的二次开发”主要是讲述如何在没有源码和无接口的情况下扩充可执行文件的功能，这一技术非常的实用。

特别致谢

首先真诚感谢我的父母、妻子、女儿对我的大力支持，使得我顺利完成此书的编写！我所有的荣耀都属于你们。

谨此对电子工业出版社博文视点公司所有相关人员致以真诚的谢意！

特别感谢电子工业出版社博文视点公司总经理郭立所做的大量工作！

特别感谢上海盛大网络发展有限公司徐海侠、王峰、刘庆民、蒋渭华、李明、张子雁、史昕峰、彭伟、张静盛等对本书的大力支持！

特别感谢微软公司大中华区首席安全官江明灶和微软的战略安全架构专家裔云天对本书的支持！

特别感谢珠海金山毒霸事业部陈勇、赵闽的技术支持！

特别感谢看雪软件安全论坛核心管理团队 CCDebuger、Ivanov、riijj、michael 的支持！

特别感谢看雪软件安全论坛各版主及各技术小组成员，对本书的大力支持！他们是：

（1）北极星 2003、笨雄、rackabcer、nbragon、inhanshi、LOVE、monkeycz、逍遥风、小虾、zmworm

（2）软件调试小组：aker、hawking、elance、theOcrat

（3）虚拟机技术小组：bughoho、linxer、wangdell、Isaiah

（4）外壳开发小组：forgot、dummy、bithaha

（5）工具开发小组：doskey、netsowell、freecat、wak、menting

（6）编程技术小组：北极星 2003、没有风、CCDeath、Combojiang、Sislcb

（7）PTG 翻译小组：arhat、thinkSJ、kkbing、aalloverred、月中人、alpsdew、jdxyw、Jhlqb、mjahuolong

（8）.Net 小组：tankaiha、backer、dreaman、inraining、kkbing、lccracker、oep1、rick、slan、tracky、菩提！、MegaX

感谢 CCDebuger 对“第 2 章　动态分析技术”和“第 13 章　脱壳技术”校对！

感谢 gzgzlxg 对“第 3 章　静态分析技术”提出的修正和补充意见！

感谢 zmworm 对工具 IDA 使用的补充建议！

感谢 Intel 公司中国企业应用技术支持部的段夕华对“第 4 章 逆向分析技术”提出的宝贵修正意见！

感谢 WiNrOOt 翻译的 www.datarescue.com 提供的 IDA 简易教程，IDA 部分参考了一下！

感谢 riijj 为“5.6 网络验证”一节提供的实例！

感谢 cnbragon 参与的“第 6 章　加密算法”！

感谢 cyclotron 参与的“8.3 伪编译”！

感谢 tankaiha 参与的“第 9 章　.Net 平台加解密”！

感谢 Hume 对“第 11 章　结构化异常处理”提供的技术支持！

感谢 DiKeN 参与的“13.10 静态脱壳”！

感谢 softworm 参与的“13.9.2 Themidia 的 SDK 分析”！

感谢 forgot 参与的“14.2.4 简单的多态变形技术”、“第 15 章　反跟踪技术”！

感谢 Hying 参与的“第 16 章　外壳编写基础”！

感谢 bughoho 参与的“第 17 章　虚拟机的设计”！

感谢 afanty 参与的“14.1 防范算法求逆”！

感谢并参考老罗（www.luocong.com）“矛与盾的较量——CRC 实践篇”！

感谢 Lenus 在内存 Dump 和内存断点方面给予的技术支持！

感谢 TiANWEi 翻译的 SoftICE 手册！

感谢 wynney 签名制作的帮助！

感谢 skylly 为脱壳一章提供的脚本制作的技术支持！

感谢 hnhuqiong 提供的 ODbgScript 脚本教学！

感谢 linhansh 在工具方面提供的帮助！

感谢 VolX 为本书配套光盘映像文件提供的 Aspr2.XX_unpacker.osc 脚本！

感谢 CoDe_Inject 对“18.2.4 DLL 劫持技术”一节提供的帮助！

感谢武汉科锐软件培训中心（www.51asm.com）Backer 为“18.2.4 DLL 劫持技术”提供 lpk.cpp！

感谢 frozenrain、jero、mocha、NWMonster、petnt、sudami、tankaiha、wynney、XPoy、王清、小虾等朋友为术语表所做的工作！

感谢 Sun Bird、JoJo、kvllz 等人对本书的大力支持！

感谢 fonge 等诸多看雪论坛会员持续一年多来的发帖签名支持新书！

同时，也要感谢那些共同参与《加密与解密》（第一、二版）、《软件加密技术内幕》组稿的看雪软件安全论坛的众多一流好手，是他们的参与和奉献才让此书得以顺利完成。

这次的第三版改动较大，参考引用了如下朋友在《加密与解密》（第一、二版）中的文章：

（1）Blowfish 在第一版参与的“第 5 章　软件保护技术”；

（2）Fisheep 参与的“浮点指令小结”和“信息隐藏技术”；

（3）吴朝相（http://www.souxin.com）参与的“认识壳”；

（4）mr.wei 参与的“DeDe 用法”；

（5）感谢 pll621 在扩展 PE 功能开拓性的研究；

（6）娃娃（王凌迪）提供的“MD5 算法”资料。

参考并引用了如下朋友在《软件加密技术内幕》中的文章：

（1）Hying 的 Anti_Dump；

（2）Hume 的“第 4 章　Windows 下的异常处理”；

（3）王勇的“编写 PE 分析工具”；

（4）罗翼的“3.3 利用调试 API 制作内存补丁”；

（5）郭春杨的“在 Visual C++中使用内联汇编”；

（6）Ljtt 参与的“花指令”、“SMC 技术实现”、“壳的加载过程”；

（7）dREAMtHEATER 翻译的 Matt Pietrek　An In-Depth Look into the Win32 Portable Executable File Format。

在此，还要感谢看雪软件安全论坛其他朋友的支持和帮助！是你们提供的帮助，才使得我能够完成此书。如果以上未提及对您的谢意，在此，我表示由衷的感谢！

关于本书配套光盘映像文件

本书不提供配套光盘，光盘映像文件可以到本站主页下载。

由于版权问题，光盘映像文件仅提供书中提到的免费软件或共享软件。如果从学习角度需要使用那些有版权的软件，建议读者通过搜索引擎查找。

光盘映像文件提供的软件经过多方面检查测试，绝无病毒。但一些加/解密工具采用了某些病毒技术，因此部分代码与某些病毒的特征码类似，会造成查毒软件的误报。请自行决定使用。

建议将光盘映像中的文件拷贝到硬盘，并去除只读属性再调试，以免出现一些无法解释的错误。

光盘映像文件下载：http://book.pediy.com

反馈信息

我们非常希望能够了解读者对本书的看法。如果您有什么问题或自己的学习心得，欢迎发到看雪软件安全网站——看雪学院。

技术支持：http://www.pediy.com

邮件地址：kanxue@pediy.com

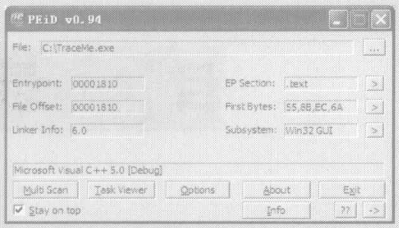
段　钢

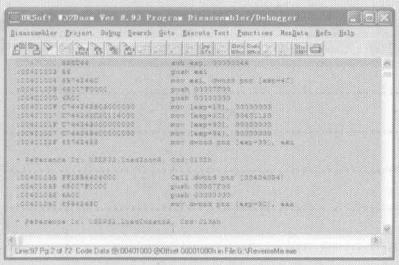
2008.5.1 于上海

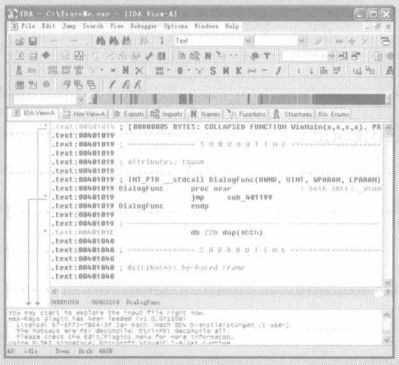
目　录

第一篇　基础篇

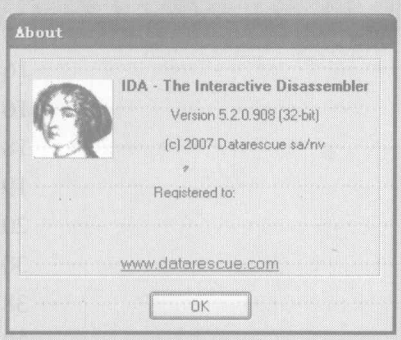
第二篇　调试篇

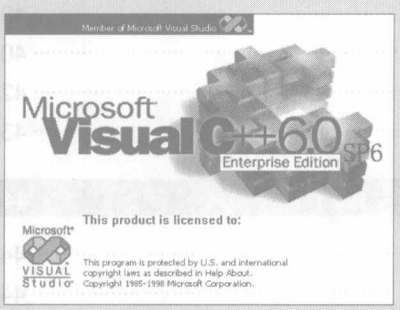


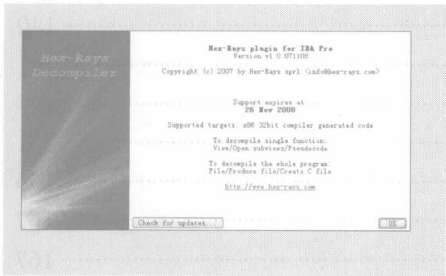




第 4 章 逆向分析技术 71

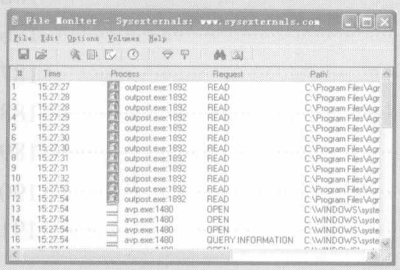


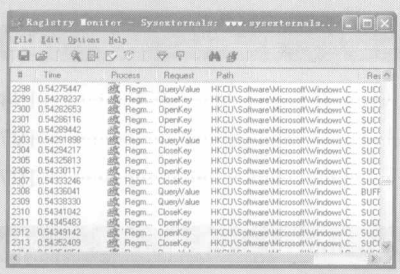


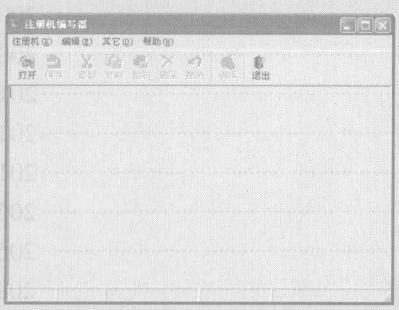


第三篇 解密篇

第 5 章 常见的演示版保护技术 102

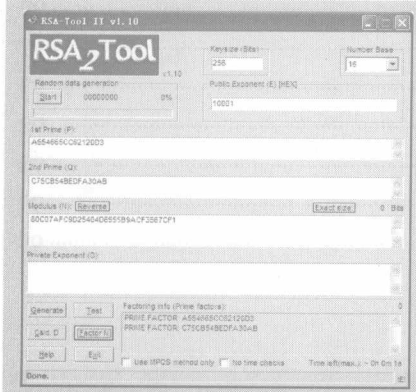




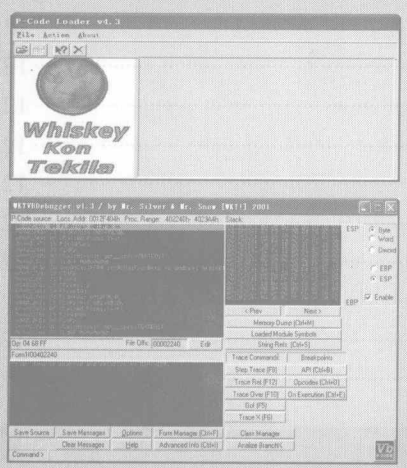


第 6 章 加密算法 131

即使这些算法的强度很高，但是使用方法也要得当，否则效果就和普通的四则运算效果没有什么两样



第四篇 语言和平台篇



由于对.Net 的反编译很容易获得其源码，摆在企业和.Net 程序员面前一个迫切需要解决的问题，就是.Net 安全性！