《加密与解密》姊妹篇

揭示极具商业价值的软件加密技术

软件加密技术内幕

看雪学院　编著

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

含光盘1张

软件加密技术内幕

看雪学院　编著

電子工業出版社

Publishing House of Electronics Industry

北京 • BEIJING

内 容 简 介

本书结合实例，重点讲述了软件加密技术及其实施方案，以帮助程序员更好地保护自己的软件。书中介绍了相关系统的底层知识，例如，PE 格式深入分析，调试 API 应用，未公开技术 SEH 的深入研究等，从而使读者在了解这些底层知识后，可以应用到自己的软件保护方案如各种反跟踪技术的实现中。本书还首度公开了如何编写加壳软件，以及如何将壳与程序融合在一起等一些热门技术。

本书由加密解密技术界一流高手共同打造，读者将从本书中获得许多极具商业价值的内幕技术，是专业开发人员不可多得的一本好书。

图书在版编目（CIP）数据

软件加密技术内幕 / 看雪学院编著. —北京：电子工业出版社，2004.8
ISBN 7-121-00098-9

Ⅰ.软... Ⅱ.看... Ⅲ.软件—密码—加密 Ⅳ.TP309.7

中国版本图书馆 CIP 数据核字（2004）第 067430 号

责任编辑：郭 立 高洪霞
印 刷：北京智力达印刷有限公司
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
经 销：各地新华书店
开 本：787×1 092 1/16 印张：26.5 字数：448 千字
印 次：2004 年 8 月第 1 次印刷
印 数：6050 册 定价：45.00 元（含光盘 1 张）

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。联系电话：（010）68279077。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。

作 者 简 介

现阶段，软件开发人员必须掌握一定的加密技术，但由于现阶段软件保护资料极其缺乏，使得开发人员在软件保护上无从下手，这就是我们推出本书的目的。本书由数位在研究软件保护方面颇有心得的好手共同创作完成，每位作者都将自己擅长的技术无私奉献出来，读者将从本书中获得许多极具商业价值的内幕技术。

主编：段 钢

编委：dREAMtHEATER、王勇、印豪、罗翼、温玉杰、李江涛、于阳、Blowfish、王景泉、裴来隆、周文雄、郭春杨

主编：**段钢**

网名看雪，1994 年毕业于上海同济大学，看雪学院（http://www.pediy.com）站长，致力于软件加密与解密研究。2001 年 9 月组织推出国内第一本全面介绍 Windows 平台下软件的加密与解密技术的书籍《加密与解密——软件保护技术及完全解决方案》。2003 年 6 月出版《加密与解密》（第二版）。

参与章节：5.1 反调试技术；5.3 反加载技术；5.4 反监视技术；5.7 文件完整性校验；5.8 代码与数据结合技术。

主页：http://www.pediy.com

邮件：pediy@pediy.com

编委：dREAMtHEATER

出生于 20 世纪 70 年代初，真正学编程是从软件逆向工程开始的，有将近一年的时间都在逆向工程的世界里徘徊， 也在那个阶段打下了汇编的坚实基础。由于对汇编的至爱，曾经用很长一段时间，写成了一个对作者自身来说具有划时代意义的软件——NoteXPad。

他不只精通 ASM ，还坚持不懈地朝着 programmer 发展，无论是传统的 C 语言还是 OOP 时代的 C++/Object Pascal，用起来都得心应手，目前正在 Delphi 平台下开发新的软件。

参与章节：第 1 章 PE 文件格式的深入分析（参考 Matt Pietrek 的“An In-Depth

Look into the Win32 Portable Executable File Format”）

主页：http://dreamtheater.yeah.net

邮件：notexpad@163.com

编委：王勇

网名破解勇，现就读于石油大学（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 系统底层的研究有一定的经验，很希望能与编程爱好者及加密解密爱好者有更多的交流机会。

参与章节：第 2 章　PE 分析工具编写

QQ：65779603

邮件：pojieyong@tom.com

编委：印豪

网名 Hying，看雪论坛版主之一，擅长加壳技术，并且在壳的商业化道路上走得极为成功。

参与章节：3.1　Win32 调试 API 原理；3.2　利用调试 API 编写脱壳机；5.6　反 DUMP 技术；6.1　外壳编写基础。

邮件：h-ying@yeah.net

编委：罗翼

程序员，从学习加解密知识开始接触编程，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：3.3　利用调试 API 制作内存补丁

邮件：firingme@sina.com

编委：温玉杰

网名 Hume，酷爱计算机，对操作系统、面向对象程序设计、网络及网络安全、加密解密等较感兴趣并有较深入的研究；业余维护了一个个人汇编站点，希望能和同

样爱好计算机的朋友们交流。

参与章节：第 4 章　Windows 下的异常处理

主页：Humeasm.yeah.net

邮件：humewen@263.net

主要作品：翻译出版《Intel 汇编语言程序设计》（第四版）

编委：李江涛

网名 ljtt，喜欢学习编程技术，常用编程语言为 Visual C++/MASM；对 PB、VFP 的反编译有较深入的研究，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，创造一个自己比较满意的作品。

参与章节：5.2　断点检测技术；5.5　反静态分析技术

E-mail：shellfan@163.com

编委：于阳

网名：fisheep，酷爱软件技术，常用编程语言：Delphi，Java；对面向对象的数据库映射方法、软件测试方法和软件保护方法等较感兴趣并有较深入的研究。

参与章节：5.5.4　信息隐藏

邮件：fisheep@sohu.com

编委：Blowfish

看雪论坛软件调试论坛版主，大龄程序员，92 年上大学时开始接触电脑，97 年读研期间接触网络并自学加密解密技术；从此一发不可收拾，其时常在教育网 BBS 上灌水；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；5 年多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：5.9　软件保护的若干忠告

邮件：blowfish2000@163.com

编委：王景泉

网名 Spirng.W，毕业于山东省信息工程学校计算机技术及应用专业，擅长 Visual C++/ASM，工作地点：山东省潍坊市。1991～1995 年工作于山东潍坊华光照排公司，1995 年下海，从事 IT 业。

参与章节：6.2　加壳程序综合运用的实例

邮件：hellowjq@163.com

编委：**裴来隆**

网名 PLL621，2001 年毕业于合肥工业大学电子信息专业，性喜静，不多言，好追根究底，从事嵌入式系统设计，业余时间沉迷于编程和调试技术中，乐此不疲。

参与章节：第 7 章　如何让壳与程序融为一体

邮件：PLL621@163.com

编委：**周文雄**

网名小楼，接触电脑 5 年，学习软件加密与解密 4 年，研究 Visual Basic 6 反编译两年有余，皆业余爱好；现在喜欢编程，探索编译器的奥秘。

或问：先生何至于此？曰：无他，惟专一耳。《阴符》有云："绝利一源，用师十倍"。吾能达于此。

参与章节：第 8 章　Visual Basic 6 逆向工程

邮件：xixiaolou@hotmail.com

编委：**郭鑫杨**

网名 Yonsm，自诩是"传说中的宇宙十大杰出青年"的 Windows 程序员，毕业后一直从事图像和多媒体软件的编程工作；对写程序有十二分的兴趣，对 Windows 编程有深入的理解。

参与章节：附录 A　在 Visual C++ 中使用内联汇编

主页：www.Yonsm.com

邮件：Yonsm@163.com

前　言

作为一名软件开发人员，你是否因看到自己的软件被他人破解而痛恨？你是否因面对着猖獗的盗版而无奈？你是否正在寻找一套行之有效的软件保护方案？

如果你对上述问题的答案都是肯定的，那么本书对你而言实在是再合适不过的了。解决上述问题可以从提高用户版权意识和加强软件保护两方面入手。从目前情况来说，对软件进行加密保护是最直接有效的。但由于软件保护技术所带来的商业利益，掌握这方面技术的个人和公司都很保守，造成目前软件加密保护方面的资料比较匮乏。因此许多软件开发人员不得不自行摸索，导致在重复劳动中走了不少弯路，耗费了大量的时间和精力开发出来的保护产品在解密者眼中不堪一击，最终，他们的产品蒙受了巨大的经济损失。本书将公开许多极有商业价值的加密技术，以帮助读者更好地对软件实施加密保护。

关于本书

本书是由“看雪学院”（http://www.pediy.com）众多高手共同打造而成的。要了解本书的写作背景，先简单谈谈本站的发展历史。

在2000年初时想找一些研究加解密的朋友交流一下，但令人十分遗憾，那时国内这方面的技术资料很缺乏，大家的交流也有限，因此就创建了主页“看雪学院”，与大家共同探讨加密与解密的知识。主页提供的论坛成了国内知名的加解密技术论坛，吸引了加解密技术界（以下简称“密界”）众多高手。当前，最新的加解密技术都可从这里接触到。

为了填补国内Windows平台加密与解密书籍的空白，作者与看雪论坛的密界一流好手合作努力，于2001年9月推出国内第一本全面介绍Windows平台下软件的加密与解密技术的书籍《加密与解密——软件保护技术及完全解决方案》。次年，在台湾发行了繁体版，深受台湾读者的欢迎。在这本书中，我们从加密和解密两方面对当今流行的软件保护技术进行分析。读过这本书后，读者能够对当今流行的软件保护技术及破解技术有所了解。这本书获得了2002年全国优秀畅销书奖（科技类）！同时还获得了2002年版权输出奖。

为了跟上技术发展的步伐，在2003年6月推出《加密与解密》（第二版）。这本书是在第一版的基础上写作而成的，补充了许多新技术，结构更加合理。这本书几乎囊括了Windows下的软件保护的绝大多数内容，是一本研究加密与解密入门的好书。

由于开发人员对当前流行的软件加密技术有进一步的需求，我们决定推出《软件

加密技术内幕》，其内容侧重软件加密技术及其具体实施方案。这本书的创作历时两年，共有十余名对加解密有心得的好手参与。

《软件加密技术内幕》与《加密与解密》的联系

《加密与解密——软件保护技术及完全解决方案》与《加密与解密》（第二版）是同一本书的不同版次，主要讲解加密与解密的相互性，比较侧重一些软件解密技巧的讲述。

《软件加密技术内幕》内容是与前一本书承接互补的，并不重复。主要讲述当前流行的软件加密保护技术。这本书对读者软件调试技巧有一定的要求，这方面的知识可以从《加密与解密》（第二版）获得。

内容导读

要研究软件加密技术必须对系统底层有一定的了解，书中首先讲解了相关系统的底层知识，如 PE 格式深入分析、调试 API 应用和未公开技术 SEH 的深入研究等。在了解这些底层知识后，就可以实现各种加密技巧。同时，本书花了较大篇幅讲解了目前很热门的技术——如何编写加壳软件，以及如何将壳与程序结合起来。

本书各章节内容如下：

第1章　PE 文件格式的深入分析

一个操作系统的可执行文件格式和数据结构揭示了藏在操作系统内部的秘密，理解 EXE 或 DLL 将有助于对操作系统的深刻理解。如果知道 EXE 和 DLL 里面的奥秘，你将成为一名知识更加渊博的程序员。

第2章　PE 分析工具编写

编写 PE 分析工具可以加深对 PE 文件格式的了解，为以后编写加壳、脱壳等工具打好基础。

第3章　Win32 调试 API

Win32 中自带了一些 API 函数，它们提供了相当于一般调试器的大多数功能。利用调试 API，可以编写自己的调试器、脱壳机、内存补丁等。

第4章　Windows 下的异常处理

Windows 下异常处理机制之一 SHE 的出现已绝非一日，但很多人可能还没有彻底了解 SEH 的工作机制；有关 SEH 的知识资料不是很多，详细资料就更少！本章将使读者对 SEH 有一个全面的了解。SEH 不仅可以简化程序错误处理，使你的程序更加健壮，还广泛应用于反跟踪及加解密中。本章对 Windows 操作系统内部提供的异常处理支持机制进行了深入探究。首先介绍最常见 SEH 的实现、原理及应用；然后，介绍 Visual C++如何封装这些内部支持，从而实现众所周知的__try{} __except{}/__finally{} 语言；最后对 Windows XP 新引进的 VEH 异常处理做了简单的介绍。

第5章　反跟踪技术

好的软件保护都要与反跟踪技术结合在一起。如果没有反跟踪技术，软件等于直接裸露在解密者的面前。本章主要讲述防调试器、防静态反汇编、防监视工具和反加载技术等内容。读者可以根据实际情况在软件中采用相关的技术和代码。

第6章　加壳软件编写

软件最终发行之前一定要将可执行程序进行加壳，使解密者无法直接修改程序。但是外面流行的加壳软件，已被广泛深入地研究，有了通用的脱壳办法，保护能力不强。因此十分有必要开发自己的加壳方法。由于外壳技术具有很大的商业价值，因此编写外壳的资料几乎没有。本章手把手地讲解如何编写自己的加壳软件，并介绍如何将前面章节介绍的反跟踪技术结合进去，打造你自己的加壳软件。

第7章　如何让壳与程序融为一体

不可能有不能脱的壳，那只是时间的问题。如果将壳与程序捆绑到一起，就会加大脱壳的难度，延长脱壳的时间，这也是壳的发展方向。本章就是讲述如何将壳与程序融合的技术和方法。

第8章　Visual Basic 6 逆向工程

现在所使用的语言无非是两种，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。解释语言的一个最大弱点就是能反编译，因此其保护的重点应放在如何防止反编译上。本章以 Visual Basic 6 为例，讲解如何对解释语言进行逆向工程，以便针对这类语言的特点研究出更好的保护方法。

附录 A　在 Visual C++ 中使用内联汇编

在编写某些加密代码时，可能要用汇编语言编写一些特定功能的代码。使用内联汇编可以在 C/C++ 代码中嵌入汇编语言指令，而且不需要额外的汇编和链接步骤。

附录 B　在 Visual Basic 中使用汇编

汇编代码不能直接插入 Visual Basic 程序，必须采用一些特殊方法。

对读者的要求

本书是针对具有一些编程经验和一定解密基础的程序员而写的。作为软件开发人员，有必要对软件保护（加密）和破解（解密）两方面同时进行研究。也就是说应该更多地从破解者的角度考虑，这样才可能比较合理地运用各种技术。这方面的知识可以从本书的姊妹篇《加密与解密》（第二版）中获得。

由于要与 Windows 的底层打交道，不可避免地要使用汇编语言，而且使用汇编语言来阐述将是最清晰直接和易于理解的，因此需要读者有一定的汇编基础。

本书适合以下读者：

- 对软件加密技术感兴趣的软件开发人员

- 进行商业软件开发的相关人员
- 对系统底层机制感兴趣的读者
- 对逆向工程感兴趣的读者

致　谢

感谢博文视点公司对本书的大力支持！

感谢 Sun Bird、Aming、Arbiter、vBin、小牧童等看雪论坛众多朋友的支持和帮助！

感谢常州师范专科学校外语系顾晓波翻译的 Brief Introduction to P-code，Mr.Silver 一文。

感谢参与写作的各位作者的技术共享的精神，是他们的无私让读者可以从本书中获得许多极有商业价值的技术。

关于配套光盘

本书所有实例均在配套光盘里提供，大部分实例是以 Masm 或 Visual C ++开发并测试的。笔者尽量使这些程序简短而完整，并将代码印刷在书里。对于那些较长的实例，需要读者阅读本书所附光盘上的那些文件。

- 请将光盘文件拷贝到硬盘，并去除只读属性后再编译和调试。
- 所有的实例程序均带源码，并且实例在光盘上都是预编译好的。
- 本书部分实例用汇编语言来描述，读者可利用内联汇编技术将汇编代码直接插入 C++，Delphi 等语言代码中去。
- 大部分实例虽采用 Visual C++来描述，但由于采用 Win32 编程，所以读者仍然可以很容易地将代码移植到其他编译语言中去。

技术支持

虽然作者竭尽全力保证书中内容及所附光盘上内容的准确性，但错误在所难免。为此，我们会在主页上提供关于本书的更正内容：

http://www.pediy.com

我们非常希望能够了解读者对本书的看法。读者可以将对本书的评论、疑问及其他意见发到我们的论坛里，我们乐意回答朋友们提出的任何合理的问题。同时，在这里你也能结识到许多兴趣相投的朋友。

段　钢

2004 年 5 月

目　录