Broadview
www.broadview.com.cn

安全技术大系

看雪软件安全
http://www.pediy.com

微软.NET程序的加密与解密

单海波 王坤峰 李晓峰 编著

本书涉及的所有实例和代码文件可以到
博文视点主页下载，文件下载：
http://www.broadview.com.cn

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

微软.NET程序的加密与解密

单海波 王坤峰 李晓峰 编著

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

内 容 简 介

本书是软件安全主题网站——看雪学院《加密与解密》软件安全系列丛书的第三本，主要介绍代码保护与加密解密技术在微软.NET 框架中的应用。全书分为基础篇、分析篇、保护篇和扩展篇四大部分，内容涉及.NET 框架基础、元数据与 MSIL、.NET 程序与内核调试、主流代码保护及其逆向技术、非托管 API 应用、64 位.NET 程序调试等。本书的层次循序渐进，难度深入浅出，且注重实例分析，是软件开发人员了解.NET 内核及加密解密技术不可多得的参考书，适合.NET 开发人员及加密与解密爱好者阅读。

图书在版编目（CIP）数据

微软.NET 程序的加密与解密 / 单海波，王坤峰，李晓峰编著. —北京：电子工业出版社，2008.11
（安全技术大系）
ISBN 978-7-121-07552-0

I. 微… II. ①单… ②王… ③李… III. 计算机网络－密码术 IV. TP393.08

中国版本图书馆 CIP 数据核字（2008）第 159538 号

责任编辑：顾慧芳
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：787×980　1/16　印张：22.25　字数：498 千字
印　　次：2008 年 11 月第 1 次印刷
印　　数：4000 册　　定价：49.00 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。

前　言

自微软 2000 年 6 月宣布其.NET 战略以来的八年时间内，.NET 技术得到了迅猛发展。越来越多的程序员选择在.NET 框架上开发程序，越来越多的企业选择.NET 作为自己产品的平台。有商业化的产品，就必然有对其进行保护的需求，于是加密与解密的战场再一次从传统的 Win32 平台扩展至.NET。可以说，.NET 发展的这几年，也是.NET 程序加密解密技术飞速成长的几年，其间出现了诸多很有特点的保护技术与逆向技术。但也许是受英语语言的限制及缺少资料的影响，国内许多企业和程序员对目前国内外最新的加密解密技术了解甚少，于是在选择适合自己产品的保护方式时往往无从下手；而加密与解密爱好者在学习.NET 逆向技术时，也感到缺乏这方面的资料。于是，我认为很有必要写一本专注于.NET 程序加密解密与内核调试的书，希望和读者互相交流，共同提高。

本书的由来

在调试程序时经常会有这种体会：分析一个保护方式的最好方法就是了解它的历史。因此，先来谈谈本书的诞生。

2004 年经朋友介绍我知道了软件安全主题网站——看雪学院，看着前辈高手们在其论坛（看雪论坛）上发表的一篇篇精华文章，实有相见恨晚之感。此时，.NET 框架诞生已近 4 年，但自己对.NET 可谓一无所知，国内对这方面的讨论也很少。偶尔的机会，接触到了.NET 程序，并在 CodeProject 网站上搜索到一篇关于去除强名称的文章，这也成了我步入该领域的入门指南。零零星星地，我开始在看雪论坛里发表一些关于.NET 程序加密解密的文章，也认识了一些有着同样兴趣的朋友。

2006 年，看雪论坛中关于.NET 的讨论渐成气候，大家明显感觉到国内在这方面与国外的差距很大，于是经看雪学院支持，将其论坛里在.NET 程序加密解密上起步较早的朋友们集合起来，组成“.NET 逆向小组”。小组成立以后，大家畅所欲言，互相交流，这段时间也成为小组每个成员成长进步最快的阶段，谈论的话题也已从简单的 MSIL 修改与编译的“高层次”深入到.NET 内核的挂钩与元数据结构的“低层次”上了。

也就是在这一年，看雪学院组织的《加密与解密》第三版的编写启动了实质性工作，并计划在其中加入一个章节讨论.NET 程序的加密与解密。正在西藏支边的我，空闲时间相对较多，于是毛遂自荐，希望负责该章节的编写。想不到看雪学院很爽快地答应下来，这

也给了我很大的鼓励。写作过程从开始到结束并不长，原因是这些年已经积累了一些.NET程序加密解密方面的资料，再加上国内外尚没有专门讨论该话题的书籍出现，因此写起来倒也算轻松。唯一遗憾的是，看雪学院只给了50页的版面，因此有许多内容被忍痛割爱、再三精简，还有一些知识点根本没有写进去。2007年，在《加密与解密》第三版一书的.NET章节——.NET平台加解密完稿交付的同时，我就决定：单独写一本讨论.NET软件加密与解密问题的书。

本书从开始编写到出版，前后共经历近两年的时间。这段时间恰是.NET保护技术飞速发展的两年，因此在写作过程中，我不断地修改内容，力争将.NET保护的最新发展囊括进来。一个人的力量总是有限的，于是我又积极地寻求小组成员的帮助，多亏他们无私地将自己的成果奉献出来，才使我得以将精力专注于书籍本身而不是无休止地进行程序分析与调试。所以，读者手中的这本书，内容全面、深浅适宜，是国内众多.NET好手智慧的结晶。

本书的特点

我对这本书的整体结构及包含的内容是下了一番工夫琢磨的。首先，我想书在难度上要由浅入深，既让初次接触.NET的读者有耐心和信心读下去，又要让熟悉.NET高层开发的读者能了解相当底层的知识，总体难度为中等偏上。其次，我非常注意可操作性，这是加密解密书籍的重要特点，读者跟着书中的示例及说明进行操作，便可更加牢固和深入掌握知识点。其三是知识点的完备性，本书基本涵盖了目前.NET程序加密与解密领域的所有知识点并能突出重点，因此既可顺序阅读，也可作为手册随时查阅。

关于加密解密的学习要注意两点：一是知识点的掌握，二是方法的掌握，且后者更重要。读者在阅读本书时，一定要注意体会书中的操作技巧，学会举一反三，方能以不变应万变。

某位大牛说过，技巧与技术是不同的。而本书介绍的都是技巧，因此如何将这些技巧转换为技术，则要靠各位读者自己不懈的努力了。

对读者的要求

本书是针对有一定Win 32和.NET编程和加密解密经验的读者而写的。其中，Win32加密解密的基础知识可以从看雪学院的《加密与解密》第三版中获得，而.NET程序设计的书籍市面上比比皆是，读者可自行选择。

.NET 是跨层次的平台，因此对读者的语言要求比较特殊。高层次平台中，读者应熟悉 C#或 VB.NET 等面向.NET 的托管程序设计语言；底层调试中，又要求读者熟悉 C++、ASM 等 Win 32 编程语言。如果有余力，可以再学习 C++/CLI，它是托管与非托管混合编程的语言，对理解.NET 平台的底层运行是非常有帮助的。

本书适合以下读者：

- 希望通过学习.NET 框架底层知识，提高自身软件开发水平的.NET 程序员；
- 希望了解.NET 加密解密基本原理，以选择合适的.NET 保护程序的程序员或公司；
- 对软件加密与解密感兴趣，并希望了解.NET 程序逆向分析技术的读者。

最后，英语虽不是必需，但在这些年的实践中，我深深感到语言的差异严重影响了知识的普及，而且很好地掌握英语会让读者在成长路上如虎添翼，因此建议每一名读者要学好计算机英语。

关于配套下载文件

本书涉及的所有实例和代码文件可以到博文视点主页下载，文件下载：http//broadview.com.cn。大部分代码均在 2.0 版.NET 框架下使用 Visual Studio 2005 编译，读者也可以选择最新的 Visual Studio 2008。代码选择的语言主要为 C++和 C#，少部分为 C++/CLI。

本书配套下载文件中还提供了部分需要使用的逆向分析工具、以前没有提供的工具以及现有工具的最新版。

致谢

感谢看雪学院的大力支持，您是我能写完本书的第一动力。

感谢博文视点的毕宁、顾慧芳两位老师为本书的写作与出版付出的辛勤劳动。

感谢看雪论坛.NET 逆向小组的所有同事，特别是 inraining、dreaman、rick、tracky、MegaX、Wickg Hu 在.NET 加密解密核心技术上的无私分享。

感谢家人对我的支持，在生活上为我分担了无数烦恼。

技术支持

虽然我已竭尽全力力求书中的内容及下载文件内容的准确性，但限于水平，错误在所难

免。因此，我会在 Blog 及看雪论坛中发布本书的更正内容，也欢迎各位读者就书中内容及.NET 逆向技术发表看法，进行讨论。本书笔者意在抛砖引玉，若能激起大家对.NET 软件安全问题的关注和交流，并借此结识更多的朋友，那么投入的时间与精力也就值了。

看雪学院：http://www.pediy.com

作者 Blog：http://vxer.cn/blog

单海波

2008 年 5 月

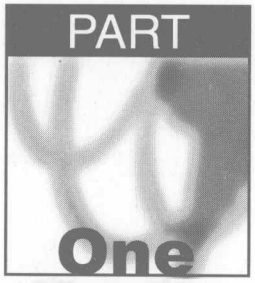
目　录

第一部分　基　础　篇

第二部分　分　析　篇

第三部分 保 护 篇

第四部分 扩 展 篇



第一部分　基础篇

CHAPTER 1

第 1 章　微软.NET 框架基本原理

了解.NET 框架的程序运行原理及代码编写方法是学习.NET 加密与解密的基础。本章不去长篇大论“什么是.NET”，因为大多数编程书籍已将这个问题解释得很清楚了，从加密与解密的角度帮助读者了解.NET 框架才是本章的核心内容。

接下来的内容将以四步走的形式介绍：通过编译第一个.NET 程序，学习 SDK 的基本使用，对.NET 程序的运行有感性认识；通过反编译，学习 ildasm 的使用，掌握.NET 逆向的初步技巧；通过修改 IL 代码并再次编译，对 MSIL 语言和元数据有初步认识；最后，在以上三步的基础上，理解.NET 框架最重要的两个概念：CLR 与 JIT。

1.1　什么是.NET

.NET 是架构于操作系统之上的平台，它是一套虚拟机，其核心功能由一系列运行在用户层（ring3 层）的 DLL 文件实现。相对于读者已经非常熟悉的 Win32 平台，或是尚未普及的 Win64 平台，.NET 是既有联系又有区别。联系是指，.NET 框架构建在 Win32/64 平台之上，它的核心程序是一系列运行于用户层的 DLL，这就决定了.NET 的内核实现仍是基于 Win32/64；区别是指，传统用户层 DLL（如 Kernel32.dll、User32.dll 等）的主要功能是提供 API，而同样是由 DLL 实现的.NET 功能要强大得多，它提供了一套完整的程序开发框架，包括新的编程语言、新的程序运行方式、新的服务等，这些都远远超过 API 涵盖的范围。从上述区别方面来说，可以将.NET 当作一个全新的平台来学习。

如果读者熟悉 Java 或者虚拟机的概念，那么理解.NET 会非常容易。如果读者是个新手，也不用担心，只要把握住以下三个.NET 最重要的特性。

（1）统一了编程语言。过去，不同编程语言间的协作总有着或多或少的兼容性问题，使用比较麻烦。.NET 则统一了编程语言：无论程序是用 C#，还是 C++，或是 VB 编写，最终都被编译为.NET 中间语言 MSIL（简称 IL）。这种统一对程序开发的贡献不言而喻，

但同时也方便了软件逆向：无须再分别为每一种语言单独编写反编译器。

（2）扩展了 PE 文件的格式。可执行文件中不再保存机器码，而是 IL 指令和元数据，部分 PE 结构被扩展用于保存.NET 的相关信息。相应地，程序的可移植性也大大提升。

（3）改变了程序的运行方式。这一点算是.NET 相比传统 Windows 程序最大的改变了：Windows 不再直接负责程序的运行，而由.NET 框架进行管理，框架中的 JIT 引擎负责在运行时将 IL 代码即时编译为本地汇编代码执行。举个简单的例子，传统 Win32 程序的错误处理机制 SEH 是依靠操作系统实现的，而在.NET 中则是由框架负责程序的错误处理。

到本书写作时为止，个人电脑上的.NET 共经历了 1.0、1.1、2.0、3.0 和 3.5 等几个主要版本，另外还有 Windows Mobile 系统上的.NET Compact Framework。Vista 之前的操作系统，.NET 是非内置的，用户在第一次运行.NET 程序时需下载并安装相应版本的运行库。Vista 问世后，.NET 已经被集成在操作系统中，普通用户将体会不到运行.NET 程序和运行 Win32/64 程序的差别。其中，最重要的属 2.0 版本，因为其后的 3.0 与 3.5 版本的框架内核与 2.0 几乎是相同的，只是在高级功能上有所增强，因此本书的大部分讨论选择基于 2.0 版本的框架。

最后，引用《Professional .NET Framework 2.0》的一幅图来结束本节内容，图 1.1 所示为.NET 框架的基本结构及其与 Windows 操作系统和底层硬件的关系，其中所有的要点都将在本书后面的章节中涉及。在 1.2 节中，将带领读者编译自己的第一个.NET 程序。

1.2　编写第一个.NET 程序

本节将带领读者动手编译一个.NET 程序，涉及的内容包括.NET 开发环境的建立、代码的编译以及程序的运行，最后引出.NET 下非常重要的两个概念：CLR 与 JIT。通过运行自己编写的程序，读者可以对.NET 有感性的认识。

1.2.1　.NET 开发环境

构建.NET 开发环境最简单的方法就是安装微软 Visual Studio .NET 2005（以下简称 VS2005）。VS2005 中包含了软件开发的三个基本要素：2.0 版的.NET 框架软件开发工具包（.NET Framework SDK）、高效强大的集成开发环境（IDE）、MSDN 文档。读者也可选择安装 VS2008，其支持的.NET 版本已升级至 3.5。

在安装之前先回答两个问题。一、可以安装 Visual Studio 2003 吗？答案是不推荐，因为它只附带了.NET 1.1 版本，这是一个过渡版本的框架，其内核与 2.0 版的相差较大，现在使用已经不多；二、可以只安装 SDK 而不安装 IDE 吗？可以，不过 SDK 只具备编译和

反编译.NET 程序的最基本工具，而 IDE 会让调试与分析过程更加轻松。

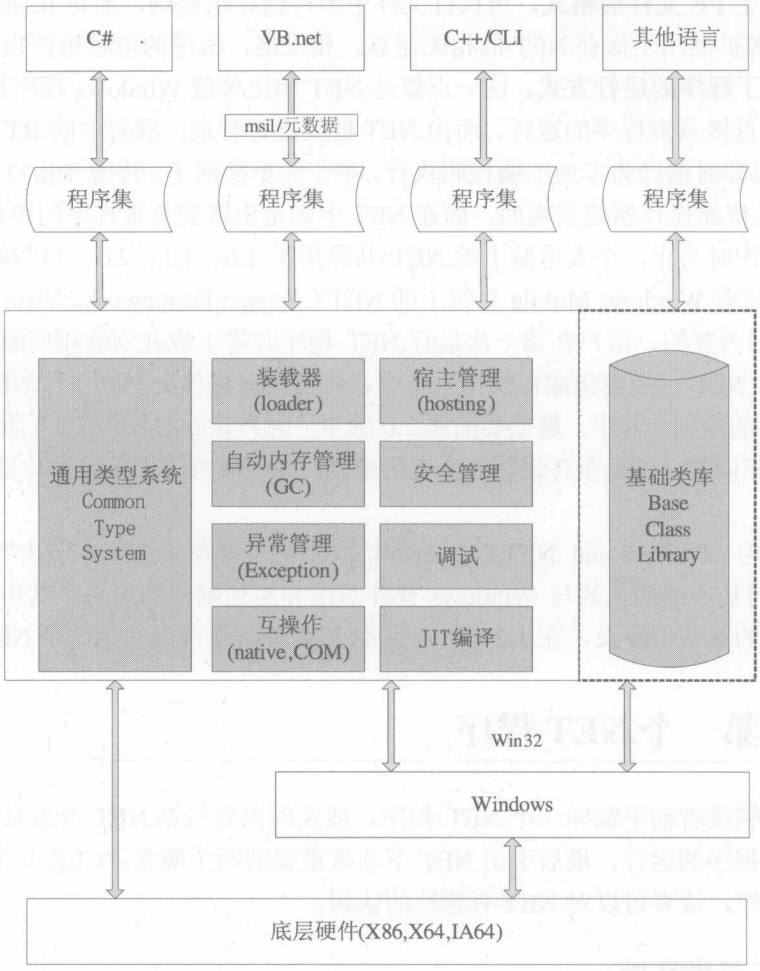


图 1.1　.NET 框架基本结构

这里安装 VS2005 并非完全出于软件开发的目的，而是进行.NET 加密与解密的学习，所以在可选项的确定上有些特殊要求。图 1.2 给出了必须安装的选项，包括三种最常见的开发语言：C#、VB.NET、VC++.NET 和框架 SDK。而混淆器 Dotfuscator 及程序发布工具 Tools for Redistributing Applications 是可选项。其他如 Visual J#、Visual Web Developer、水晶报表和 SQL 不是必需的功能，读者可自行决定。确定安装选项和路径后，一路 next 便可完成.NET 开发环境的构建。