Broadview
WWW.BROADVIEW.COM.CN

Microsoft

包含
高级诊断
技巧和
崩溃分析

4

Fourth Edition

深入解析 Windows 操作系统，第4版

——Microsoft Windows Server 2003/ Windows XP/Windows 2000技术内幕

Microsoft Windows Internals, Fourth Edition:Microsoft Windows Server 2003, Windows XP, and Windows 2000

Jim Allchin 作序
David N. Cutler 题写"Windows NT的历史全景"

[美] Mark E. Russinovich
David A. Solomon 著

潘爱民 译

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

深入解析 Windows 操作系统

第 4 版

——Microsoft Windows Server 2003/Windows XP/Windows 2000 技术内幕

Microsoft Windows Internals

Fourth Edition:

Microsoft Windows Server 2003, Windows XP, and Windows 2000

[美] Mark E. Russinovich 著
David A. Solomon
潘爱民 译

電子工業出版社

Publishing House of Electronics Industry

北京 • BEIJING

内 容 简 介

本书是著名的操作系统内核专家 Mark Russinovich 和 David Solomon 撰写的 Windows 操作系统原理的最新版著作，全面和深入地阐述了 Windows 操作系统的整体结构以及内部工作细节。本书针对 Windows Server 2003、Windows XP 和 Windows 2000 做了全面更新，通过许多练习实验让你直接感受到 Windows 的内部行为。另外，本书还介绍了一些高级诊断技术，以便使你的系统运行得更加平稳和高效。无论你是开发人员还是系统管理员，你都可以在本书中找到一些关键的、有关体系结构方面的知识，通过这些知识你可以更好地做系统设计、调试，以及性能优化。

全书内容丰富、信息全面，主要包括的 Windows 操作系统深度知识有：理解 Windows 的关键机制，包括系统服务分发和调度机制、启动和停机，以及注册表；挖掘 Windows 的安全模型，包括访问控制、特权和审计；利用内核调试器和其他的工具来检查内部系统结构；检查与进程、线程和作业相关的数据结构和算法；观察 Windows 如何管理虚拟内存和物理内存；理解 NTFS 的操作和格式，诊断文件系统访问问题；从上往下查看 Windows 的网络栈，包括映射、API、名称解析和协议驱动程序；诊断引导问题，执行崩溃分析。

本书适合广大 Windows 平台开发人员、IT 专业从业人员等参考使用。

版权贸易合同登记号　图字：01-2005-0907

图书在版编目（CIP）数据

深入解析 Windows 操作系统：第 4 版：Microsoft Windows Server 2003/Windows XP/Windows 2000 技术内幕 /（美）罗斯（Russinovich,M.E.），（美）所罗门（Solomon,D.A.）著；潘爱民译.
—北京：电子工业出版社，2007.4
书名原文:Microsoft Windows Internals，Fourth Edition: Microsoft Windows Server 2003，Windows XP，and Windows 2000
ISBN 978-7-121-03969-0

I. 深… II.①罗…②所…③潘… III.服务器－操作系统（软件），Windows IV.TP316.86

中国版本图书馆 CIP 数据核字（2007）第 031620 号

策划编辑：方　舟
责任编辑：方　舟　陈元玉
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：61.75　　字数：1 000 千字
印　　次：2007 年 4 月第 1 次印刷
定　　价：99.00 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，联系电话：（010）68279077；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。

译 序

这是一本随Windows NT一起发展和成长起来的经典图书。我在1995年的时候阅读过这本书的第1版中文版，通过该书了解到了Windows NT设计的诸多考虑。它对于我理解Windows曾经起到了重要的作用。除了这本书以外，另外一套讲述Windows SDK开发指南的图书（记得有四卷）也深刻地影响了我对于Windows的理解。虽然第4版与早期的版本有了很大的变化（原作者也不相同，请参考引言部分关于本书历史的介绍），但由于Windows NT的内核结构一直沿袭下来了，无疑本书新的版本更趋成熟，而且新版作者们编写的许多工具更是使本书增色不少。

时隔10年以后，当编辑找到我，希望我来翻译这本书的第4版时，我的第一感觉是，我不能翻译这本书，所以我直截了当地拒绝了编辑。我的顾虑在于两个方面：首先，这是一本重量级的书，更适合于操作系统领域中的资深专家来把握和诠译；其次，我担心没有足够的时间来及时地完成这本书的翻译工作。两周以后，当编辑再次找到我时，我答应找一个帮手来翻译这本书，但是，合适的帮手并不好找。最后，我决定独立翻译本书，但需要一年时间。而实际上，我花了一年半时间才完成本书的翻译工作。无奈，在质量和进度之间，我选择了前者。

这是一本独特的书，它既不像教材那样宣讲Windows操作系统的原理，也不教读者如何编写内核驱动程序或者如何更好地配置Windows系统。相反地，它按照Windows操作系统的体系结构，把内核几乎翻了个遍，目的在于帮助读者理解Windows内核的每一部分是如何工作的，并且通过各种工具让你真正能够看到Windows内部的数据结构和状态，甚至一些运行过程。阅读这本书的过程，其实也是玩转Windows的过程。经过作者们的剖析，Windows已经完完全全不再神秘。如果你想知道Windows的内部工作原理，那么，这本书对你来说再合适不过了。

Microsoft提供了很多工具（并且许多工具可直接通过Microsoft的Web站点获得），可用来观察或控制系统内核的方方面面，其中最为重要的当然非内核调试器（Windbg）莫属了。除此以外，本书作者们也提供了大量实用的工具（有的还相当好玩，见本书第14章最后一节。所有这些工具都可通过*www.sysinternals.com*下载而得到），你不仅在阅读本书的时候能使用这些工具来帮助你更好地理解书中的内容，在日常的工作或生活中也可以使用这些工具来解决一些实际问题。例如，我和同事们通过Process Explorer（在本书中我将其翻译为“进程管理器”）

发现过机器上的流氓软件的痕迹，有时候，当目录无法删除或移动设备无法卸载的时候，通过它也能查到哪个进程还在抓着不放手。对于有些工具，作者们还在书中介绍了实现原理，比如Filemon就是一个很好的例子。

这本书确实打破了Windows操作系统的神秘感，但是，更让Windows大白于天下的，当是Windows的源代码了。2006年7月，Microsoft真正开放了一份可编译的内核源代码（仅核心部分），编译得到的内核文件可以在Windows Server 2003 （SP1）上启动和运行。如果读者有资格获得这一份代码，那么，在阅读本书的时候，你甚至可以直接参考源代码。我想，在这一点上，Microsoft的确体现了诚意。有关详细的信息，请参考*http://www.microsoft.com/resources/sharedsource/Licensing/WindowsAcademic.mspx*。

说到本书的权威性，看一看David Culter（NT内核的最初设计者，奠定了Windows NT的基础）和Jim Allchin为本书写的序言就能知晓。作者之一David Solomon从事Windows NT内部机理的培训和研讨有10多年经历了，而且也在Microsoft内部对员工进行培训。我有幸参加了他2006年春天在北京的一次培训。而另一名作者Mark Russinovich呢，*www.sysinternals.com*上这么多优秀的工具皆出自他的手笔，现在已经加入Microsoft了。有兴趣的读者，可以到网站上看一看Mark的blog，一些技术文章非常有意思。

这一年多翻译本书的过程，于我也是一个学习的过程。这些知识帮助我解决了在工作中遇到的许多难题，也让我更好地理解了Windows操作系统。我经常向同事和实习生们推荐这本书，希望能帮助他们解决手头的一些技术难题，以及更好地在Windows平台上开展工作。如果你的工作也需要紧密地接触Windows，那么，不管是科研人员、开发人员，还是系统管理员，都可以从这本书中获益良多。

如何更有效地发挥本书的作用呢？以我的感觉而言，这本书的叙述并不像教材那样严谨，也不像教材那样按照学习的顺序来组织内容，它应该是一本讲述Windows系统内部机理的实用参考书。所以，如果你没有计算机科学的专业背景，我建议你配合学习一本讲述操作系统原理的书籍。有了操作系统理论的基础以后，再阅读本书无疑会有更好的效果。另外，在阅读过程中，若有条件，一定要动手做一做书中描述的实验。这些实验很容易做，你若能举一反三，则掌控Windows就不在话下了。

最后，借此机会，感谢两位作者写了这么一本有用的书以及一组实用工具。谢谢周筠编辑让我翻译这本书，并容许我这么久才完稿。今年4月份她说的一句话让我感动，她说“我不催你，我知道你很忙”，而实际上，原书的出版社正在催她，她是顶着压力说这句话的。谢谢微软亚洲研究院高校关系经理马歆小姐，她在过去几年中为推广Windows在国内高校的教学和科

研做了大量幕后工作，包括组织国内高校的操作系统教师编写了《Windows操作系统原理》一书，正是在跟她的接触和交流过程中，让我更加意识到了这本书有多么重要。也要谢谢本书编辑方舟和陈元玉，他们配合我的翻译进度，使得我们的工作能以流水线方式进行，他们的工作态度让我感受到了从未有过的编辑对译者的尊重。

在翻译过程中，我也尽可能地改正原著中的一些错误，但我相信这本书还远没有达到完美，尤其是，因翻译而新引入的错误更是在所难免。尽管我花了四个月的时间来复查一遍译稿，但交稿之后还是能发现一些翻译不妥之处，甚至错译的句子，请读者原谅。另外，本书正文之后列出了英汉习惯用语对照表，以方便阅读。

潘爱民

2006年12月于北京

六年前开始的等待

—出版人感言—

2000年暮秋的一个傍晚，我同时结识了蒋涛和潘老师。蒋涛那时刚过而立，白衣飘飘，一身仙气。潘老师与蒋涛同岁，略显老成，斯文和气，令我一见如故。当天，依稀记得我们一起在聊蒋涛即将创办的《程序员》杂志，聊潘老师受到读者追捧的《VC++技术内幕》（第四版），聊我要做的侯捷老师的《深入浅出MFC》（第二版）。

从那一天起，我和潘老师就成为了朋友。他这个人，微笑比较多，言语向来不多。偶然，我在网上发现他写一笔漂亮的钢笔行书，还发现他在练太极。这都是我感兴趣的，问他，他的回答依然寥寥，曰不过是一点兴趣而已，并无深入研究。我趁机向他约稿，约翻译，也约写作。他总是说：会有机会的。

每年去北京的时候，都会和潘老师约着一起喝喝茶，他偶尔兴致好，也有余暇的时候，愿意随我和一帮80后的程序员们聚会，也往往都是带着他不变的微笑听小年轻们意气风发、挥斥方遒，依然话不多。但，他看人其实是独到的，一两句话，就能点到人家的穴位，这时，一双浓眉下的眼睛会显得特别犀利明亮。我一直在想他这样的表情像谁。有一天，他和我喝茶，闲聊到他原来是徐志摩和金庸的老乡——浙江海宁人，我猛然意识到他真的有点像也是浙江人的围棋天才马晓春，呵呵，结果有朋友对我的这一发现也表示赞同。

浙江人的聪明勤奋，我已多次从合作的作译者身上见识到了。这次潘老师依然让我深刻地体会到了这一点。等待与他的合作，已经等了六年。这六年间，IT专业出版潮起潮落，而潘老师却能无视这些沉浮，安然地做着他想做的事情，几乎年年都会在出版上给读者带来惊喜。他也总是鼓励着我，鼓励我耐心做好自己的份内事，不要因追求数量而伤害品质，不要为虚名所累。

2003年春，我做了母亲，潘老师正好来武汉开会，专门来看我和还未满月的女儿。博文视点那时还在筹建中，我对未来一派迷茫，他真诚的鼓励给了我很大的信心。人的一生，太需要这样的朋友了。

2004年底，策划编辑方舟选定了这本《Windows Internals,4/e》，我问他找谁翻译为好，他说：那肯定是潘老师最合适了。我就去请潘老师，几番蹉跎后，潘老师总算首肯了。我发短信

给方舟道喜，方舟回复短信：那就十全十美了！

我的同事——这本书的编辑方舟、陈元玉以及市场负责人佘广均以自己耐心细致的工作赢得了潘老师由衷的称赞，我为伙伴们的工作而自豪。

六年前开始的友谊，六年后将通过彼此的合作而继续绵长。衷心盼望来自作译者和出版方的真诚合作，能带给读者美好的阅读体验。

周　筠

2007年2月于武汉

Windows NT的历史全景

我又一次发现自己真的要感谢David Solomon和Mark Russinovich了，他们提供了机会让我在他们合著的关于Windows内部机理的系列图书的最新版本中写一些话。在这一系列图书中，上一版本的出版距新版本已经有三年了，在此期间Windows已经有了两个主要的发行版本：一个是对客户系统的重大更新，另一个则是对刚刚准备就绪要发行的服务器系统的重大更新。

对于像这样一本书的作者，他们面临的两个日益显著的问题是，跟踪Microsoft Windows NT系统在实现方面的进展，以及记录下在每一个版本中哪些特性的实现发生的变化。最终，本书的作者们完成了这一杰出的工作，为全书提供了例子和解释。

（从左至右）David Solomon、David Cutler和Mark Russinovich

当我第一次碰到David Solomon时，我还在DEC（Digital Equipment Corporation）为VAX的VMS操作系统工作，当时他只有16岁。从那时起，他一直涉足于操作系统的开发和对操作系统内部机理的教学。我认识Mark Russinovich的时间要短一些，但知晓他在操作系统领域的专业特长也很有一段时间了。他曾经做出了很杰出的工作，比如可在Microsoft Windows 98上运行的NTFS文件系统，以及他的“实时”Windows内核调试器（通过该工具可以在Windows系统运行的时候探查其内部状态）。

Windows NT项目最初是从1988年10月份开始的，起初的目标是实现一个可移植的系统，能够解决OS/2兼容性、安全性、POSIX、多处理能力、集成的网络功能，以及可靠性等诸多问题。随着Windows 3.0的发行和巨大成功，这些系统目标很快也随之发生变化，变成了直接处理Windows的兼容性，而把OS/2兼容性移到一个子系统中。

我们最初认为，可以在两年多时间内完成第一个Windows NT系统。实际上，第一个发行版本花了四年半时间，到1993年夏天才完成，这一发行版本支持Intel i386、Intel i486和MIPS R4000处理器。六周以后，我们也引入了对于Digital Alpha处理器的支持。

Windows NT的第一个发行版本比预期的要大、要慢，所以，下一个重要的阶段是一个称为Daytona的项目（用Florida的一条高速公路来命名）。这一发行版本的主要目标是减小系统的尺寸，提高系统的速度，当然，也要使它更加可靠。1994年秋天我们发布了Windows NT 3.5，过了6个月，又发布了Windows NT 3.51，此更新版本包含了对于IBM PowerPC处理器的支持。

Windows NT下一个版本的目标是，更新用户界面以便与Windows 95兼容，以及将Microsoft已经开发多年的各种Cairo技术融合进来。这一系统的开发花了两年多时间，最终在1996年夏天作为Windows NT 4.0面市。

NT的下一个版本是Windows 2000，这是最后一个客户和服务器系统同时发布的系统。这一版本建立在与以前版本相同的Windows NT技术基础之上，同时也引入了一些重要的新特性，比如活动目录。花了三年半时间来开发Windows 2000，对当时的Windows NT技术作了全面的测试和调节。开发Windows 2000是过去11年来跨越4种体系结构的系统开发之巅峰。

在Windows 2000开发结束时，我们又启动了一个宏伟计划，要在新的客户和服务器系统中融入新的、增强的客户特性和改进的服务器能力。在这一计划实施过程中，有一点越来越清楚，即服务器特性的实现将会导致客户特性实现的滞后，因此，客户和服务器系统的版本被分开了。在2001年8月，Windows XP Professional和Windows XP Home Edition发布了，一年多以后，在2003年3月，Microsoft Windows Server 2003也发布了。除了对Intel x86体系结构的支持以外，这些系统还包含了对于Intel IA-64的支持，这标志着Windows NT第一次进入了64位处理的领域。

本书是有关Windows XP和Windows Server 2003的内部结构和工作机理的一部权威之作。而且，它也提供了Windows将来转移到64位计算上的大略介绍，包括AMD在2003年引入的x64体系结构（AMD64）和Intel于2004年2月份宣称的64位支持（EM64T）。完全支持x64的客户和服务器版本计划在2005年上半年发行，本书包含了有关x64系统实现细节的诸多精辟观点。

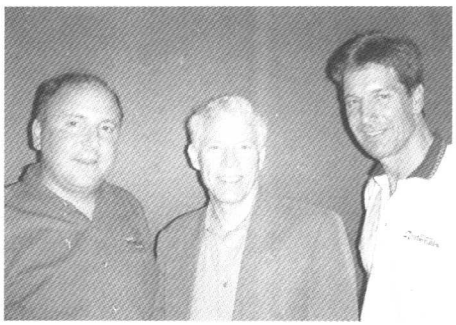
当x86体系结构开始显现出旧时代征兆之时，x64体系结构即是Windows NT的新时代的开始。这一体系结构提供了32位x86兼容性，以保护过去的软件投资，同时它也提供了64位寻址能力以便满足新应用程序更大的空间需求。这既保护了32位软件的投资，同时也为Windows NT

进入下一个10年或走得更远而提供了必不可少的支撑。

尽管在过去几年中，Windows NT系统经历了几次名称上的变化，但是，它仍然完全建立在最初的Windows NT代码基（code base）的基础之上。随着时间的推移和各种发明创造的诞生，许多内部特性的实现发生了重大的变化。本书作者已经做了令人赞不绝口的工作来诠释Windows NT代码基的细节，及其在不同版本之间和不同平台之间的实现上的差异，同时他们也开发了一些例子和工具来帮助读者理解Windows NT内部是如何工作的。每一个认真的操作系统开发人员都应该在自己的案头有这本书。

David N. Cutler
Senior Distinguished Engineer
Microsoft Corporation

序　言



Microsoft Windows成为我生活中的核心部分已经有14年了。在这段时间中，随着发行版本的不断推出，此操作系统已经在广度和深度上前进了很多。今天，推出Windows无疑是全球最重要和最复杂的项目之一。差不多有5 000名工程师在为Windows而工作。Windows的用户几乎跨越了所有的文化，从最关键的业务人员到年轻的小孩子，构成了完整的用户图谱。使用Windows的客户们几乎在各个方面都有不断增强的需求——从能够运行最大的服务器，到足够易用以便于学龄前儿童也能够使用。Windows有各种形态和大小，从嵌入式版本到媒体中心版本，再到数据中心版本。所有这些版本都使用同样的Windows核心，此核心会随着每一个发行版本而发展和增强。

本书是有关Windows内部机理核心的权威之作。如果你想要知道Windows内部是如何工作的，那么，这就是你想要的书。理解如此庞大产品的每一个细节是一项艰巨的任务。但是，如果你从系统的核心概念开始深入钻研，那么，把这些谜题拼接起来相对要容易得多。正如Windows本身已经有了长足的进步一样，本书的涵盖面也在不断拓宽，现在本书已经到了第4版。近些年来，我们使用这本书以前的版本来培训新加入Microsoft的员工，对于这一版本，也必然如此。

如果你跟我一样，那么你也喜欢弄清楚事情是如何真正工作的。阅读“如何使用…”或者“…经验和技巧” 之类的书籍是从来不能让我满足的。如果你理解了事情的内部工作原理，那么，你就会知道如何更好地使用它，使性能和安全性尽可能地最大化，以及如何诊断失败。诚然，也一定会有更多的乐趣。如果你跟我一样，想要“深入浅出”地看一看Windows，那么，这本书正好是你的一个起点。

David和Mark已经做了突出的工作，他们详细地讲述了Windows内部的技术故事。他们强调的这些工具是一份很好的资源，有助于直接的实验训练和诊断工作。当你阅读了这本书以后，你一定会更好地理解Windows操作系统是如何组织起来的，系统中有哪些最新的改进，以及如何更好地发挥这些新的技术进展的作用。

这是一次技术之旅——尚在行进之中的技术旅行。开始阅读本书吧，深入地挖掘迄今最为激动人心的操作系统。

Jim Allchin
Group Vice President, Platforms
Microsoft Corporation

致　谢

首先，要特别感谢以下人员。

- **Dave Cutler,** 高级杰出工程师（Senior Distinguished Engineer），Microsoft Windows NT的第一任架构师。Dave最初同意David Solomon访问Windows的源代码，并且支持他的工作，通过他的培训业务与“Inside Windows NT（Second Edition）”和“Inside Microsoft Windows 2000（Third Edition）”的写作来解释Windows NT的内部机理。Dave除了审阅本书中关于进程和线程这一章以外，还回答了许多关于Windows系统的内核体系结构方面的问题，以及为这一版本写了“Windows NT的历史全景”。
- **Jim Allchin**, 我们的执行赞助人，为本书写了前言，支持我们在Microsoft内部的课程。
- **Rob Short**, 副总裁，保证我们能够得到所需要的资源，以及能够访问相关的人员。

我们也要感谢Windows部门中的两位开发人员，他们编写的新内容也被合并到这一版本中，他们是：

- **Adrian Marinescu,** 在内存管理一章中，他写了可扩展堆管理器这一部分；
- **Samer Arafeh,** 他描述了Wow64。

感谢我们的老朋友Jeffrey Richter，他写了第1章中“关于.NET和WinFX”的辅助内容，并且在许多次一起吃晚饭时不断地提醒我们，按照他的看法人们会如何看待我们在书中所谈到的内容。

如果没有Microsoft Windows开发组的关键成员的审阅、建议和支持，本书的技术细节不可能有现在这样的深度，也不可能有这样的精确度，因此，我们感谢以下人员，他们为本书做了技术审阅并提出了建议。

Murali Brahmadesam	Pat Hoffer	Daniel Pravat
Molly Brown	Anthony Jones	Dragos Sambotin
Duncan Bryce	Tom Jones	Jon Schwartz
Daniel Bucherer	Joseph Joy	Rob Short
Neal Christian	Shreeniwas Kelkar	Paul Sliwowicz
Neill Clift	Connie La Chasse	Chittur Subbaraman
Mike Danseglio	Mike Lai	Cristian Teodorescu
Joseph Davies	Paul Leach	Andre Vachon
Cenk Ergan	Gerald Maffeo	Landy Wang

Tom Fout	Aaron Margosis	Richard Ward
Nar Ganapathy	Iain McDonald	Brad Waters
David Golds	Kamen Moutafov	Bruce Worthington
Robert Gu	Adi Oltean	Mark Zbikowsk
Jeff Hamblin	Vince Orgovan	Khawar Zuberi

其他一些人也为本书作出了贡献，他们或者在走廊和自助餐厅回答我们的问题，或者提供了技术资料——如果我们漏掉了你，请原谅！

也要感谢Azius开发人员培训公司（Azius Developer Training, *www.azius.com*）的Jamie Hanrahan，他与David合著了最初的Windows Internal Architecture课程的教材，本书第2版建立在此基础之上。Jamie真正懂得如何把复杂的概念用简单和实际的方式解释出来，他编写了一些概念说明，并设计了一些结构图表。

感谢Dave Probert，他提供了共享环境，使得审阅草稿得以发布给Microsoft的内部审阅者们。

还要感谢AMD的Jonathan Sloves，他安排了AMD64测试系统，并且将测试系统发送给我们以帮助我们编写64位的内容，以及把Sysinternals的一些工具移植到x64上。

最后，我们要感谢Microsoft Press的下列人员，感谢他们为本书作出的贡献。

- Robin van Steenburgh，策划编辑（acquisitions editor），谢谢他与我们一起耐心地工作，直到完成这一项目。
- Sally Stickney，曾经一度继续作为我们的项目编辑，但后来卷入到管理事务中。这次我们失去了跟他一起工作的机会！
- Valerie Woolley，接替了Sally作为我们的项目编辑。他很棒（不像Sally在上两个版本中那样总是将就我们）！
- Roger LeBlanc，辛勤地统编了所有章节的文字，找到了不一致的地方，总而言之，使本书的书稿达到了Microsoft Press的高标准。

David Solomon和Mark Russinovich
2004年9月

引 言

《深入解析Windows操作系统，第4版》的读者对象是那些想要理解Microsoft Windows 2000、Windows XP和Microsoft Windows Server 2003操作系统的核心组件内部工作机理的高级计算机专业人员（包括开发人员和系统管理员）。开发人员利用这些知识，可以在构建Windows平台上的应用程序时更好地理解各种设计决策背后的基本原理。这样的知识也可以帮助开发人员调试复杂的问题。系统管理员也可以从这些信息中获益，因为理解了操作系统背后的工作原理，可以有助于理解系统的性能行为，以及当事情变糟时更易于诊断各种系统问题。在阅读了这本书以后，你应该可以更好地理解Windows是如何工作的，以及它为什么有这样那样的表现。

本书的结构

前两章（“概念和工具”和“系统结构”）奠定了本书后面用到的术语和概念的基础。接下去的三章——“系统机制”、“管理机制”以及“启动和停机”——讲述了系统中关键的底层机制。接下来的八章解释了操作系统的核心组件：进程、线程和作业、内存管理、安全性、I/O系统、存储管理、缓存管理器、文件系统，以及网络，最后一章介绍了崩溃转储分析。

本书的历史

本书以前的名称是*Inside Windows NT*（Microsoft Press，1992，中文版的名称是《Windows NT技术内幕》），现在是第4版。第1版是由Helen Custer著的（在Microsoft Windows NT 3.1的最初发布以前出版）。*Inside Windows NT*是第一本关于Windows NT的书籍，它提供了有关Windows NT系统的体系结构和设计方面的关键要点。*Inside Windows NT, Second Edition*（Microsoft Press，1998）是由David Solomon著的。该书在内容上做了更新，涵盖了Windows NT 4.0，并且大大地提高了技术深度的层次。*Inside Windows 2000, Third Edition*（Microsoft Press，2000）是由David Solomon和Mark Russinovich合著的。第3版增加了许多新的话题，比如启动和停机、Windows服务的内部机理、注册表的内部机理、文件系统驱动程序、网络，以及Windows 2000中内核的变化，其中，关于Windows 2000中内核的变化，包含了Windows驱动程序模型（WDM，Windows Driver Model）、即插即用、电源管理、Windows管理规范（WMI，Windows Management Instrumentation）、加密、作业对象和终端服务。

第4版的变化

这一最新的版本，现在称为“*Microsoft Windows Internals*（*Fourth Edition*）”，在内容上做了更新，以覆盖Windows XP和Windows Server 2003中所做的内核变化，包括对于64位系统的支持。练习用的实验也相应地做了更新，以反映出工具中的变化；新增加的实验用到了一些在第3版写作时尚未可用的新工具。

由于从Windows 2000到后续版本之间的内核变化相对较小（与“Windows NT 4.0和Windows 2000之间的变化”相比较而言），所以，本书中绝大部分内容适用于Windows 2000、Windows XP和Windows Server 2003。因此，除非特别声明，否则一切内容都适用于这三个版本。

练习实验

即使没有访问源代码，你也可以通过一些工具（比如内核调试器）来获得许多有关Windows内部机理的知识。每当可以通过一个工具来揭示或演示Windows内部行为的某一方面时，本书中的“实验”辅助章节就会列出让你自己试用该工具时遵从的步骤。这样的实验遍布全书，我们鼓励你在阅读本书时试一试这些实验——看一看Windows内部是如何工作的，这比你仅仅读一遍本书所得到的印象要深刻得多。

本书没有涵盖的话题

Windows是一个大而复杂的操作系统。本书并没有涵盖与Windows内部机理相关的一切内容，而是把焦点集中在基本的系统组件上。例如，本书没有讲述COM+（Windows分布式面向对象编程基础设施），也没有讲述.NET框架（下一代托管代码的应用程序的基础）。

因为这是一本讲述内部机理的书籍，不是一本用户指南、程序设计或系统管理类型的书籍，所以，本书没有描述如何使用、编程或配置Windows。

提醒和告诫

因为本书讲述的是Windows操作系统中未文档化的内部结构和内部操作的行为（比如内核结构和函数），所以，这些内容有可能会在不同的发行版本中有所变化（外部的接口，比如Windows API，则不会受到不兼容变化的影响）。

说到“受版本变化的影响”，我们并不是指，本书讲述的细节会在不同发行版本中一定有所变化，但是你不能认为它们不会改变。任何使用了这些未文档化接口的软件都有可能在将来