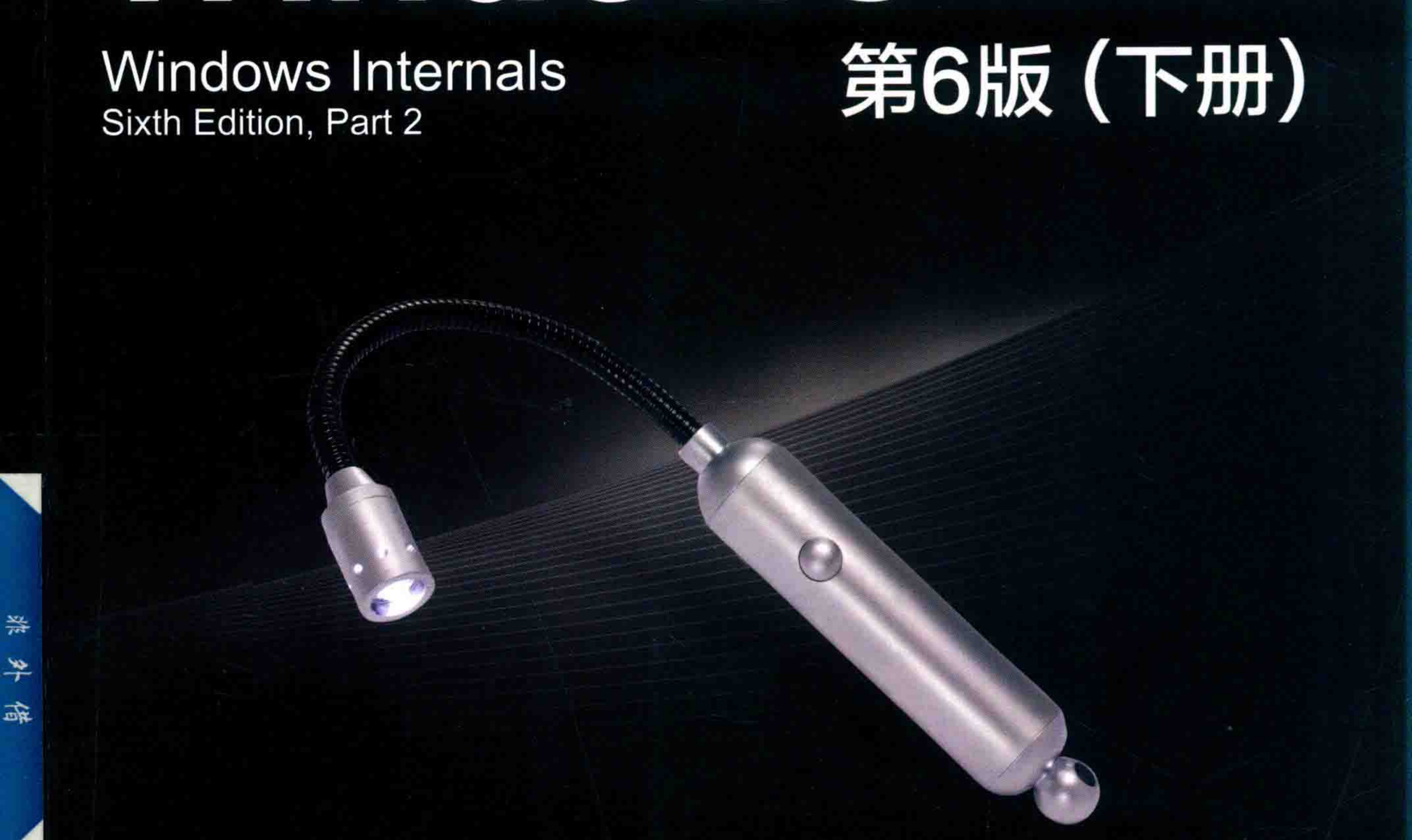
Broadview®
www.broadview.com.cn

Microsoft

深入解析 Windows 操作系统 6

Windows Internals
Sixth Edition, Part 2

第6版（下册）



[美] Mark Russinovich
David A. Solomon 著
Alex Ionescu

范德成
潘爱民 译

中国工信出版集团

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

非外借

深入解析 Windows 操作系统

第6版（下册）

Windows Internals
Sixth Edition, Part 2

Mark Russinovich
[美] David A. Solomon 著
Alex Ionescu

范德成
潘爱民 译

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

内 容 简 介

本书是关于 Windows 操作系统原理的最新著作，全面深入地阐述了 Windows 操作系统的整体结构及内部工作细节。本书针对 Windows 7、Windows Server 2008 R2 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，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，从而更好地做系统设计、调试和性能优化。

本书适合广大 Windows 平台开发人员、IT 专业从业人员阅读。

版权贸易合同登记号 图字：01-2013-4703

图书在版编目（CIP）数据

深入解析 Windows 操作系统：第 6 版. 下册 /（美）马克·拉希诺维奇（Mark Russinovich），（美）大卫·A. 所罗门（David A. Solomon），（美）艾力克斯·伊纳苏（Alex Ionescu）著；范德成，潘爱民译. —北京：电子工业出版社，2018.3

书名原文：Windows Internals, Part 2, 6E

ISBN 978-7-121-33643-0

Ⅰ. ①深… Ⅱ. ①马… ②大… ③艾… ④范… ⑤潘… Ⅲ. ①Windows 操作系统 Ⅳ. ①TP316.7

中国版本图书馆 CIP 数据核字(2018)第 023744 号

责任编辑：刘 皎
印 刷：三河市鑫金马印装有限公司
装 订：三河市鑫金马印装有限公司
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：37.25 字数：715 千字
版 次：2018 年 3 月第 1 版（原书第 6 版）
印 次：2018 年 3 月第 1 次印刷
定 价：128.00 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）88254888，88258888。

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。

本书咨询联系方式：010-51260888-819，faq@phei.com.cn。

译者序一

在所有介绍Windows操作系统的图书中，我相信都离不开*Windows Internals*系列提供的信息。除了公开可见到的Windows源代码以外，本书是披露Windows系统机理最为详尽的一份资料，尤其对于Windows的每一个最新版本。本书第6版专门针对Windows 7和Windows Server 2008 R2进行了大幅度更新。由于篇幅的增加，这一版本改成了上下两册来发行，由此也可见本书的“分量”。本书上册中文版已于2014年4月出版，这几年间，我经常收到读者的询问，本书下册是否出版。现在，下册中文版终于要出版了，读者们可以如愿看到本书了。

在Windows操作系统的发展历程中，Windows 7是一个具有特殊意义的版本。它可以算得上是最为复杂的单机操作系统，无论是从代码规模、代码复杂度，还是从系统适应场景的复杂程度，都超过了以前所有的版本。从某种意义上，Windows 7代表了软件工程的一个顶峰——人类可以构造出如此复杂且能稳定工作的软件系统！与此相对应，要用一本书来涵盖其中的各种机理也同样是一项艰巨的任务，本书作者基于他们过去所做的大量工作，以及对Windows的深入理解，出色地完成了这一诠释工作。

本书的权威性毋庸置疑。Mark Russinovich因在Windows内核探索方面所作出的贡献而成为Microsoft Fellow（现为Azure CTO），本书中用到的大量Sysinternals工具均出自他的手笔。David Solomon长期从事Windows NT内部机理的培训，他不仅在全球各地培训Windows系统程序员，甚至也为Microsoft的内部员工提供Windows内核培训服务，他从本书第2版开始奠定了卓有成效的叙述风格。Alex Ionescu是一名年轻的黑客型Windows专家，曾经为ReactOS（一个开源的操作系统项目，旨在兼容Windows 2000/XP/Server 2003的应用程序）编写了绝大多数内核代码。他曾经发现和报告了一些与Windows内核相关的软件漏洞，也跟David Solomon一起讲授Windows内部机理的课程。有如此强大的作者组合，再加上Microsoft的内部支持（包括提供源代码，以及Windows开发组的细致解释），本书无疑是Windows最新版本的第一手技术资料。

每一个对Windows操作系统有浓厚兴趣的读者都不应该错过这本书。本书上册介绍了Windows的系统架构、系统机制、管理机制、进程与线程、安全性和网络。下册是上册的直接延续，共有7章，分别介绍了Windows I/O、存储管理、内存管理、缓存管理器、文件系统、启动与停机，以及崩溃转储分析。每一章都是一个重要话题，读者既可以在上册的基础上继续深入钻研Windows各个子系统，也可以有选择地阅读某些章节。在阅读过程中，最好能动手做一做书中描述的实验。做这些实验的门槛并不高，但效果非常好，既可以让你直观地领会Windows内部的一些设计与实现，也可以积累一些洞察Windows内部活动的方法，这些方法

对于排查Windows平台上出现的问题往往很有帮助。

我与本书的渊源是从第4版（针对Windows XP/Server 2003）开始的，后来第5版（针对Windows Vista/Server 2008）错过了出版周期，直至这次第6版又有机会翻译。这三个版本，连同后来的第7版（针对Windows 10/Server 2016）都采用同样的叙述框架，只是针对最新的Windows版本做了更新。本书讲述的内容，虽然是针对Windows 7/Server 2008 R2，但更新幅度较大，尤其是有关64位系统的介绍，有较多新内容。即使读者已经在Windows 8或者Windows 10上工作，本书中的内容仍然对你有价值。另外，如果读者不满足于本书Windows系统机理的系列介绍，而希望进一步理解Windows操作系统的源代码实现以及内核中的各种基础算法，则推荐阅读另一本书《Windows内核原理与实现》，这是我在Windows XP/Server 2003 SP1内核代码基础上写作的一本讲解Windows内核的书，它几乎将Windows内核大白于天下。

最后，我要特别感谢范德成先生，他在我第4版译稿的基础上，更新到了第6版。也要感谢电子工业出版社的编辑刘皎，依然把第6版的翻译工作交给了我，使我有机会弥补第5版中文版未能出版之缺憾。

潘爱民

2018年1月于杭州

译者序二

微软的Windows操作系统历经三十年左右的发展，早已成为一个博大精深的桌面及服务器操作系统，并在市场上获得了很大的成功。但近十年来，以亚马逊、谷歌、Facebook等为代表的互联网企业在市场和技术两方面开疆拓土，极大地推动了移动设备、云计算、大数据和人工智能等行业的发展，显著影响了包括微软在内的各大传统软件巨头的发展态势。继2006年亚马逊提出云计算之后，微软于2008年首度公开Azure虚拟机云平台，SAP也在2012年公开其应用程序云平台。尽管各种新的技术不断涌现，但本书的定位焦点仍然在Windows操作系统本身，在我看来，这本书的价值依然很高，因为技术的本源有共通性，Windows操作系统又可谓是微软技术的中流砥柱——微软的Azure云平台的操作系统就是基于Windows开发的，其上运行的虚拟机管理器正是最早在Windows Server 2008中发布的Hyper-V。

如果你对Windows操作系统有着浓厚的兴趣，自然不应该错过本书。如果你是分布式系统架构师，也同样能从本书中受益。这是因为，分布式系统和操作系统在许多方面都有着或多或少的相似性，对操作系统设计原理的掌握自然会对分布式系统的设计有重大启发和帮助。比如，操作系统的线程调度和分布式系统的负载均衡、操作系统的磁盘缓存和分布式系统的缓存设计、操作系统的文件系统和分布式系统的文件系统、虚拟机管理器的VLAN和分布式系统的软件定义网络（SDN）、操作系统的性能监视器与分布式系统服务器的性能监视平台等之间都有不少相似性。

以事务处理为例，Windows Vista中引入了KTM（内核事务管理器，参见本书第12章），它所实现的事务的隔离级别类似于数据库的READ COMMITTED级别，是一种几乎所有SQL数据库都会实现的隔离级别；而分布式系统中的Paxos共识算法所能实现的分布式事务，其隔离级别也类似于READ COMMITTED。又以磁盘缓存为例（参见本书第11章），操作系统的磁盘缓存是强一致性的，而分布式系统缓存可以做成应用服务器内的，或者是专门的缓存层，前一种实现对负载均衡调度有特殊要求，而普通的负载均衡会大大降低缓存命中率从而导致系统性能低下，后一种实现则在网络延迟上稍差些。两种实现都要考虑是做成强一致性的还是最终一致性的，前者需要在写的同时更新缓存，后者则需要自动淘汰旧的缓存数据。缓存的粒度也很重要，粒度过小可能导致索引数据量过大，这和操作系统磁盘缓存的原理是类似的。所以，理解操作系统的知识能拓展眼界，进而对基于这些系统的设计产生正面影响。

此外，理解操作系统的行为有助于设计性能更高的分布式程序。比如，了解操作系统磁盘缓存的原理，有助于设计出高性能的对象存储服务——可以想办法提高对象存储在操作系统上的缓存命中率，或者在必要时禁用操作系统缓存而改为自己实现缓存机制。又如，了解操作系统网络栈的工作模式，有助于编写做高速网络传输的程序，甚至可以深入驱动程序层

面做进一步的性能优化。

我是Windows操作系统的深度用户，学习和研究了包括Windows、Linux、FreeBSD、OpenBSD在内的多种操作系统。从1995年首次接触Windows 3.1开始，就与Windows结下了不解之缘。陆续使用过Windows 3.1、Windows 95、Windows 98、Windows ME、Windows NT 4.0、Windows 2000、Windows XP、Windows Vista、Windows 7、Windows 8、Windows 8.1和Windows 10等各个版本，还接触过Windows Server 2000、Windows Server 2003、Windows Server 2008、Windows Server 2008 R2等服务器版本，以及其上的Microsoft Virtual PC、Virtual Server和Hyper-V虚拟化技术。我会好奇它们有着怎样的功能和性能，底层是怎样工作的，为什么这样设计而不是那样设计的；正是因为这种好奇，所以*Windows Internals*一直是我十分感兴趣的一本书。在完成本书上册的翻译工作后，我写了一篇后记（http://www.fandecheng.com/personal/interests/pwindows/wi_translation_ps.pdf里面讲了很多个人的理解和感悟）。2012年，当好友高博打电话告诉我有机会参与《深入解析Windows操作系统》第6版的翻译时，我非常欣喜。在高博的引荐下，我首次见到了仰慕已久的潘爱民老师。因此我非常感谢高博的引荐和潘爱民老师的认可，感谢电子工业出版社的刘皎和白涛两位编辑，本书的出版离不开他们的策划和编辑。

范德成

2018年1月于上海浦东张江

引言

《深入解析Windows操作系统（第6版）》的读者对象是那些想要理解Microsoft Windows 7和Windows Server 2008 R2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，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，有助于理解系统的性能行为，并且在事情变糟时更容易诊断各种系统问题。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

《深入解析Windows操作系统（第6版）》第一次被分成了上下册来出版。为Windows的每一个版本更新这本书需要花相当多的时间，所以，按照上下册来组织本书内容使我们可以更快地出版上册部分。

本书上册的前两章为“概念和工具”和“系统结构”：第1章定义了关键的概念，并介绍了本书后面用到的工具；第2章讲述了总体系统结构和组件。接下来的两章展示了系统中关键的底层机制和管理机制。上册部分还覆盖了操作系统的三个核心组件：进程、线程和作业；安全性；网络。

本书下册的内容覆盖了剩余的核心子系统：I/O、存储、内存管理、缓存管理器和文件系统。下册最后部分还描述了启动和停机过程，并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6版。第1版由Helen Custer撰写（在Microsoft Windows NT 3.1最初发布之前出版）。*Inside Windows NT*是第一本关于Windows NT的书籍，它提供了有关Windows NT系统架构和设计方面的关键要点。*Inside Windows NT (Second Edition)*（Microsoft Press, 1998）由David Solomon撰写，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）由David Solomon和Mark Russinovich合著完成。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。它也覆盖了Windows 2000中内核的变化，比如Windows驱动程序模型（WDM，Windows Driver Model）、即插即用、电源管理、Windows管理设施（WMI，Windows Management Instrumentation）、加密、作业对象和终端服务。*Windows Internals (Fourth Edition)*是针对Windows XP和Windows Server 2003的更新，它加入了更多的内容，主要集中在帮助IT专业人员更好地利用Windows的内部机理的知识，比如使用Windows Sysinternals （www.microsoft.com/technet/sysinternals）的关键工具，以及分析崩溃转储。*Windows Internals (Fifth Edition)*是针对Windows Vista和Windows Server 2008的更新，它包含的新内容有：映像加载器、用户模式调试设施，以及Hyper-V。

第6版的变化

这一最新的版本在内容上做了更新，以覆盖Windows 7和Windows Server 2008 R2中所做的内核变化。练习用的实验也相应地做了更新，以反映出工具中的变化。

练习实验

即使没有访问Windows源代码，你也可以通过一些工具（比如内核调试器，以及来自Sysinternals和Winsider Seminars & Solutions的工具）获得许多有关Windows内部机理的知识。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印象要深刻得多。

本书没有覆盖的话题

Windows是一个大而复杂的操作系统。本书并没有覆盖与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Microsoft .NET框架（托管代码应用程序的基础）。

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发行版本之间有所变化。（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”，我们并不是指本书所讲述的细节将在不同发行版本之间一定有所变化，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的Windows版本上无法正常工作。更糟的是，在内核模式下运行并且用到了这些未文档化接口的软件（比如设备驱动程序）在新的Windows发行版本上运行时可能会导致系统崩溃。

致谢

首先，感谢Azius LLC的Jamie Hanrahan和BrianCatlin加入这一项目——没有他们的帮助，本书将无法完成。他们对“安全性”和“网络”这两章做了大量的更新，也为“管理机制”和“进程和线程”这两章的更新做出了很多贡献。Azius提供了Windows内部机理和设备驱动程序的训练。更多信息参见www.azius.com。

我们想要感谢Alex Ionescu，在这一版本中他是一名完全的联合作者。这包含了Alex在本书第5版所做的大量工作，以及在这一版本中持续做的工作。

同时感谢Daniel Pearson，他更新了“崩溃转储分析”一章。他多年来的转储分析经验，使得本章内容更加贴近真实场景。

感谢Eric Traut和Jon DeVaan，继续让David Solomon可以为了写作本书而访问Windows源代码，以及继续开发他的*Windows Internals*课程。

有三个关键的评审者尚未因为他们对第5版的评审和贡献而被致以感谢，他们是：Arun Kishan、Landy Wang和Aaron Margosis。再次感谢他们！再次感谢Arun和Landy为这一版本所做的详细审查和极有帮助的见地。

若没有来自Microsoft Windows开发组关键成员的审查、建议和支持，这本书不会拥有现在这样的技术细节深度和精确度。因此，我们感谢下面的人员，他们为本书提供了技术审查和建议：Greg Cottingham、Joe Hamburg、Jeff Lambert、Pavel Lebedinsky、Joseph East、Adi Oltean、Alexey Pakhunov、Valerie See。

同时感谢Scott Lee、Tim Shoultz和Eric Kratzer在编写“崩溃转储分析”这章时所提供的协助。

对于“网络”这一章，特别感谢Gianluigi Nusca和Tom Jolly，他们所做的远远超出了他们的责任范围：Gianluigi在BranchCache的材料方面提供了特别有用的帮助，以及大量的建议（他还写了许多段落材料）；Tom Jolly不仅提供了优秀的审查意见和建议，而且让许多其他的开发人员帮忙做技术审查。下面是所有对“网络”这一章做了审查和贡献的人员：Roopesh Battepati、Molly Brown、Greg Cottingham、Dotan Elharrar、Eric Hanson、Tom Jolly、Manoj Kadam、Greg Kramer、David Kruse、Jeff Lambert、Darene Lewis、Dan Lovinger、Gianluigi Nusca、Amos Ortal、Ivan Pashov、Ganesh Prasad、Paul Swan、Shiva Kumar Thangapandi。

Amos Ortal和Dotan Elharrar对NAP的内容提供了帮助，Shiva Kumar Thangapandi对EAP部

分提供了大量帮助。

感谢Gerard Murphy为本书审阅Windows 7停机机制的内容，并清楚地解释了不同组策略下的行为。

感谢Microsoft电源管理组的Tristan Brown，有好几天他在办公室陪Alex一起加班到深夜，仔细解释处理器核心的停运算法和行为。他还提供了一幅珍贵的插图。

感谢Apurva Doshi给Alex发了一份详细解释了缓存管理器在Windows 7中改变的文档，本书中所介绍的一些新的行为和改变正是由于该文档的帮助才研究清楚的。

感谢Matthieu Suiche，是他提供的内核符号文件数据库让Alex能发现最核心的内核数据结构中新增和去除的字段，并由此引发了他对底层功能变化的探索和发现。

感谢Cenk Ergan、Michael Fortin和Mehmet Iyigun对Superfetch细节部分的审查和建议。

Christophe Nasarre作为总体技术评审人，他所做的详细检查极大地提高了本书的技术精确度和一致性。

我们也要再次感谢Hex-Rays（www.hex-rays.com）的Ilfak Guilfanov，因为他们为Alex Ionescu提供了IDA Pro Advanced and Hex Rays许可，所以Alex可以加快对Windows内核的逆向工程。

最后，作者们要感谢Microsoft Press的同事们，他们在背后做了很多工作，将这本书变成现实。Devon Musgrave作为本书的策划编辑，承担了双重职责：既要考虑成本，也要考虑本书的发展；Carol Dillingham是本书的项目编辑。编辑和产品经理Steve Sagman、版权编辑Roger LeBanc、校对编辑Audrey Marr和索引编辑Christina Yeager都为本书的质量做出了贡献。

最后，感谢Microsoft Press的发行人Ben Ryan，他始终相信为读者提供如此详细程度的Windows知识是极其重要的！

勘误和本书支持

我们做了各种努力来确保本书的精确性。自本书出版以来已经报告的任何错误都将在http://go.microsoft.com/FWLink/?Linkid=245675上列出。

如果你遇到了尚未列出的错误，你可以通过以上页面将错误报告给我们。

如果你需要额外的支持，请发送电子邮件给Microsoft Press Book Support：mspinput@microsoft.com。

请注意，通过上述地址并不会提供有关Microsoft软件产品的支持。

倾听你的声音

让你满意是我们最高优先级的工作，你的反馈也是我们最有价值的财富。

注册博文视点社区（www.broadview.com.cn）用户，即享受以下服务：

- 提勘误赚积分：可在【提交勘误】处提交对内容的修改意见，若被采纳将获赠博文视点社区积分（可用来抵扣购买电子书的相应金额）。
- 交流学习：在页面下方【读者评论】处留下您的疑问或观点，与作译者和其他读者共同交流。

页面入口：http://www.broadview.com.cn/33643。

保持联系

让我们保持热线联系，我们在Twitter上的地址是：http://twitter.com/MicrosoftPress。

Contents

目录

第 8 章 I/O 系统 1

8.1 I/O 系统组件 1

I/O 管理器 3

典型的 I/O 处理过程 4

8.2 设备驱动程序 5

设备驱动程序的类型 5

WDM 驱动程序 6

分层的驱动程序 7

实验：查看已加载的驱动程序列表 9

驱动程序的结构 11

驱动程序对象和设备对象 13

实验：看一看设备对象 15

实验：显示驱动程序和设备对象 17

打开设备 18

实验：查看设备句柄 21

实验：查看 Windows 设备名称之间的映射 23

8.3 I/O 处理 24

I/O 类型 24

同步 I/O 和异步 I/O 24

快速 I/O 25

实验：查看一个驱动程序登记的快速 I/O 例程 25

映射文件 I/O 和文件缓存 26

分散/聚集 I/O 27

I/O 请求包 27

IRP 栈单元 28

实验：查看驱动程序的分发例程 29

实验：查看一个线程的未完成 IRP 29

IRP 缓冲区管理 30

针对单层驱动程序的 I/O 请求 32

为一个中断提供服务 33

完成一个 I/O 请求 34
同步 36
针对分层的驱动程序的 I/O 请求 38
实验：查看一个设备栈 39
实验：查看 IRP 40
线程无关 I/O 45
I/O 取消 45
用户发起的 I/O 取消 46
线程终止时的 I/O 取消 47
实验：调试一个无法被杀死的进程 48
I/O 完成端口 49
IoCompletion 对象 50
使用完成端口 50
I/O 完成端口操作 52
I/O 优先级支持 54
I/O 优先级 54
优先化策略 55
I/O 优先级反转的避免（I/O 优先级继承） 57
I/O 优先级提升和撞升 57
实验：“非常低”和“正常”I/O 吞吐量的对比 58
实验：I/O 优先级提升/撞升的性能分析 59
带宽预留（计划的文件 I/O） 60
容器通知 60
驱动程序检验器（Driver Verifier） 61
8.4 内核模式驱动程序框架（KMDF） 63
KMDF 驱动程序的结构和操作 64
实验：显示 KMDF 驱动程序 65
KMDF 数据模型 66
KMDF 的 I/O 模型 69
8.5 用户模式驱动程序框架（UMDF） 72
8.6 即插即用（PnP）管理器 76
即插即用支持的级别 77
驱动程序对于即插即用的支持 77
驱动程序加载、初始化和安装 79
Start 值 80
设备列举 81
实验：将设备树转储出来 84
设备栈 85
设备栈的驱动程序加载 86
实验：在设备管理器中查看详细的 devnode 信息 88
驱动程序安装 90

实验：检查一个驱动程序的 INF 文件 92
实验：查看目录（catalog）文件 93
8.7 电源管理器 94
电源管理器的操作 96
驱动程序的电源操作 97
实验：查看一个驱动程序的电源映射关系 97
实验：查看系统的电源能力和策略 98
驱动程序和应用程序对于设备电源的控制 100
电源可用性请求 100
实验：在调试器中查看一个电源可用性请求 101
实验：利用 Powercfg 查看电源可用性请求 103
处理器电源管理（PPM） 103
核心停运的策略 104
利用率函数 105
实验：查看利用率和频率的信息 106
实验：查看利用率和频率的历史 107
算法覆盖 108
增加/减少动作 108
各种阈值和策略的设置 109
实验：查看当前的核心停运策略 111
“性能检查”算法 112
实验：查看当前的 PPM 检查信息 116
8.8 本章总结 118

第 9 章 存储管理 119

9.1 有关存储的术语 119
9.2 磁盘设备 120
旋转磁盘 120
磁盘的扇区格式 120
固态硬盘 122
NAND 型闪存 122
文件的删除和 irim 命令 124
9.3 磁盘驱动程序 125
Winload 125
磁盘类、端口和小端口驱动程序 126
iSCSI 驱动程序 127
多路径 I/O（MPIO）驱动程序 128
实验：观察物理磁盘 I/O 130
磁盘设备对象 130
分区管理器 131

9.4 卷的管理 132
基本磁盘 133
MBR 风格的分区 133
GPT（GUID 分区表）分区方案 133
基本磁盘卷管理器 134
动态磁盘 135
LDM 数据库 135
实验：使用 LDMDump 来查看 LDM 数据库 137
LDM 和 GPT 或 MBR 风格的分区方案 139
动态磁盘的卷管理器 140
多分区卷的管理 140
跨距卷 141
条带卷 142
实验：观察镜像卷的 I/O 操作 143
RAID-5 卷 145
卷名字空间 145
挂载管理器 146
挂载点 147
卷的挂载 148
实验：查看 VPB 149
卷的 I/O 操作 152
虚拟磁盘服务 153
9.5 虚拟硬盘（VHD 文件）支持 155
附载 VHD 的操作 156
嵌套的文件系统 156
9.6 BitLocker 驱动器加密 157
加密密钥 159
可信平台模块（TPM） 161
BitLocker 引导过程 163
BitLocker 密钥的恢复 165
全卷加密驱动程序 166
BitLocker 的管理 167
BitLocker To Go 168
9.7 卷影像（shadow）拷贝服务 170
影像拷贝 170
“克隆”影像拷贝 170
“写时复制”影像拷贝 170
VSS 的架构 170
VSS 的操作 171
影像拷贝提供者 172
实验：查看 Microsoft 影像拷贝提供者的过滤型设备对象 173

Windows 中的用途 174
备份 174
实验：查看影像卷的设备对象 174
“之前的版本”和系统还原 175
实验：导航到“之前的版本” 176
实验：映射卷影像设备对象 177
9.8 本章总结 178
第 10 章 内存管理 179
10.1 内存管理器简介 179
内存管理器组件 180
内部同步 181
检查内存的使用情况 182
实验：查看系统内存信息 182
10.2 内存管理器提供的服务 184
大页面和小页面 185
保留页面和提交页面 187
实验：保留的页面对比提交的页面 188
提交限额 190
锁住内存 190
分配粒度 191
共享内存和映射文件 192
实验：查看内存映射文件 193
保护内存 194
“不可执行”页面保护 196
实验：查看进程上的 DEP 保护 199
软件的数据执行保护 200
写时复制 201
地址窗口扩展 203
10.3 内核模式堆（系统内存池） 204
内存池的大小 205
实验：确定最大的池大小值 206
监视内存池的使用 208
实验：诊断内存池泄漏 210
快查表（Look-Aside List） 211
实验：查看系统的快查表 212
10.4 堆管理器 212
堆的类型 213
堆管理器结构 214
堆同步 215