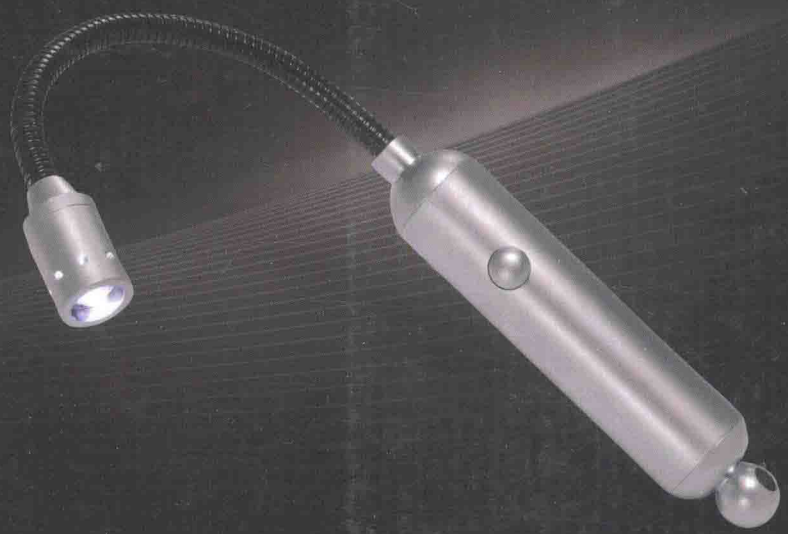
Broadview
www.broadview.com.cn

Microsoft

深入解析 Windows 6 操作系统

Windows Internals
Sixth Edition, Part 1

第6版（上册）



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

潘爱民
范德成 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 6

Windows Internals
Sixth Edition, Part 1

第6版 (上册)

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

潘爱民
范德成 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、Allen Ionescu撰写的关于Windows操作系统原理的最新版著作，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校。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，以及性能优化。

本书适合广大Windows平台开发人员、IT专业从业人员等参考阅读。

版权贸易合同登记号　图字：01-2013-4702

图书在版编目（CIP）数据

深入解析Windows操作系统：第6版. 上册/（美）拉希诺维奇（Russinovich, M. E.）等著；潘爱民，范德成译. —— 北京：电子工业出版社，2014.4

书名原文：Windows Internals 6th Edition, Part 1

ISBN 978-7-121-21956-6

Ⅰ. ①深… Ⅱ. ①拉… ②潘… ③范… Ⅲ. ①Windows操作系统 Ⅳ. ①TP316.7

中国版本图书馆CIP数据核字（2013）第276785号

责任编辑：白　涛

印　　刷：北京京师印务有限公司

装　　订：北京京师印务有限公司

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：**44　　**字　　数：**800千字

印　　次：2014年4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。

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。

译者序

在所有介绍Windows操作系统的图书中，我相信都离不开***Windows Internals***提供的信息。除公开可见到的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的每一份最新版本。本书的第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，这一版本改成上下两册来发行，由此也可见本书的“分量”。

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。它是目前最为复杂的单机操作系统，无论从代码规模、代码复杂度，到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，本书作者们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因其在Windows内核探索方面所做出的贡献而成为Microsoft Fellow，本书中用到的大量Sysinternals工具均出自他的手笔。David Solomon从事Windows NT内部机理的培训有十多年经历，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一起教授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），本书无疑成为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。那么，如何发挥本书的作用呢？首先，本书并非如教材那样循序渐进，而是全景式地讲述了Windows的系统机理。第3章和第4章介绍总体结构，尤其是系统内部的核心机制和管理机制，值得每个人认真阅读，其他后续的章节可以有选择地阅读。其次，阅读本书之前最好有操作系统的基础知识，以及一定程度的Windows编程技能，否则难以深刻领会Windows中大量的精妙设计。再次，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，可以让你直观地领会Windows内部的一些设计和实现。

我与这本书的渊源是从第4版（针对Windows XP/Server 2003）开始的，当时博文视点武汉分部的周筠老师强烈推荐我来翻译第4版。后来第5版（针对Windows Vista/Server 2008）原版出版后，又交给我来翻译。由于第5版与第6版之间时间差较短，内容更新也相对较少，在我手上又拖了太长时间，导致最后第5版中文版失去了出版时机。很抱歉，辜负了周筠老师的重托。我也要特别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。

本书的翻译工作由范德成和我共同完成，其中第1~4章由我完成，第5~7章由范德成完成。全书由我统稿。Windows的各种技术涉及大量的术语，甚至一些全新的技术术语，为此我们尽可能按照中文习惯来表达这些术语，或适当地保留一些专有名词。若在译稿中有任何不妥之处，请读者原谅。此外，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

2012年12月，于北京西二旗

Introduction

引言

Windows Internals, 6th Edition的读者对象是那些想要理解Microsoft Windows 7和Windows Server 2008 R2操作系统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，有助于理解系统的性能行为，并且当事情变糟时更易于诊断各种系统问题。在阅读了本书以后，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

Windows Internals这本书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；以及网络。

本书下册预计将在2012年秋季单独出版，内容覆盖剩余的核心子系统：I/O、存储、内存管理、缓存管理器和文件系统。下册最后部分还将描述启动和停机过程，并且介绍崩溃转储分析。

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版是由Helen Custer所著（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系统的体系架构和设计方面的关键要点。***Inside Windows NT, 2nd Edition***

（Microsoft Press，1998）是由David Solomon所著。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, 3rd 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。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, 4th 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, 5th 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

即使不访问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）来获得许多有关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，而是把焦点集中在了基本的系统组件上。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（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，本书中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加入到这一项目上——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。这包括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。

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 Lebedynskiy
- Joseph East
- Adi Oltean

- Alexey Pakhunov
- Valerie See

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。

Christophe Nasarre作为总体技术评审人，他所做的详细的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IIfak Guilfanov，因为他们为Alex Ionescu提供了IDA Pro Advanced和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列在oreilly.com的Microsoft Press站点上：

http://go.microsoft.com/FWLink/?Linkid=245675

如果您遇到了尚未列出的错误，可以通过同样的页面将错误报告给我们。

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

请注意，上述地址并不会提供有关Microsoft软件产品的支持。

倾听您的声音

在Microsoft Press，让您满意是我们最高优先级的工作，您的反馈也是我们最有价值的财富。请告诉我们您对这本书的看法：

http://www.microsoft.com/learning/booksurvey

这份调查非常简短，我们会阅读您的每一条评论和想法。感谢您提供宝贵意见。

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*。

关于本书

《深入解析Windows操作系统》是一本旨在对Windows操作系统内核进行全面揭秘的传奇之作，在技术图书的出版史上独一无二。它不仅对于Windows系统管理员和开发测试工程师而言是无价之宝，更为当代操作系统的架构设计和运行原理的细节提供了绝佳的研究实证材料。本书作者团队成员皆为微软公司最资深的架构师，而Windows 7和Windows 2008 R2所共同拥有的也是“最后一代PC血统纯正的Windows NT内核”（潘爱民语），毫无疑问这是一个时代的集大成之作，对每个有志于在操作系统方面有所作为的工程师和研究者而言都不可错过！

本书上册对Windows系统最为核心的部分，包括系统机制、进程管理、安全性等内容做了全面阐述，而下册则将沿着这条道路，进一步介绍许多关键的Windows系统组件，包括与设备相关的系统输入输出及驱动程序、与外部存储技术相关的存储管理与文件系统、与物理内存和虚拟内存相关的内存管理与缓存管理器、讲述系统引导之后和断电之前所经历的关键过程，即启动与停机过程等内容。

本书下册内容详实，对每个重要的系统组件都给出了细致的分析，并包含了一些有趣的、能揭示系统内核原理的实验。比如，第10章“内存管理”中讲到，x86/x64版Windows的内存管理是基于英特尔80386及更高级别的CPU设计的，书中详细介绍了这一架构下内存管理的特点，包括段页式寻址、线性地址等概念，并在此基础上介绍了Windows本身的物理内存及虚拟内存的布局结构。又如，在Windows系统上编程时，如果需要在程序间共享数据，你也许会想到利用内存映射文件技术。那么，在内存中映射了文件的一部分之后，文件的长度能不能被修改？映射内容的修改是何时写入磁盘的？如果一个文件的同一部分被多个程序映射，各程序能否使用各自的虚拟内存地址？是否能不使用磁盘上的文件而在程序间共享内存？这些问题都能在下册中找到答案。

再者，现在的网络安全问题层出不穷，对于运行着诸多网络服务和应用程序的Windows系统来说，如何确保安全性也是很重要的问题。为了减少缓冲区溢出漏洞带来的安全隐患，Windows实现了一系列的技术，如DEP、ASLR、stack cookie等。这些技术是如何发挥作用的呢？在本书下册，你也能找到答案。

本书译者团队十分重视内容的技术准确性和行文可读性，不仅亲自动手重做了书中的每一个实验，还仔细审阅了每一张图表，在术语统一上下了不少功夫。希望这些努力能够为读者带来愉悦的阅读体验，尽可能地避免技术谬误。

下册将于年内推出，敬请期待！

第8章　I/O系统组件

第9章　存储管理

第10章　内存管理

第11章　缓存管理器

第12章　文件系统

第13章　启动与停机

第14章　崩溃转储分析

Contents

目录