

TURING 图灵程序设计丛书

Microsoft

Windows Internals

Part 1 **Sixth Edition**

深入解析 Windows操作系统

卷1 (英文版·第6版)

[美] Mark Russinovich
David Solomon 著
[加] Alex Ionescu

- 微软官方权威著作最新版
- 深入剖析Windows技术内幕
- 大幅更新，涵盖Windows内核最新特性

 人民邮电出版社
POSTS & TELECOM PRESS

“在微软，我们一直用本书培训新员工……本书是深入理解Windows的绝佳入门书。”

——Windows之父Jim Allchin

“每一位操作系统开发人员都应该拥有本书。”

——微软技术院士、Windows NT首席设计师David Cutler

“我想不出还有哪一本书比本书更具权威性。”

——微软公司副总裁Ben Fathi

自20年前的第一版出版以来，本书就成为了Windows系统管理员和开发人员探究Windows核心部件运作机理和各种技术细节的权威著作。书中深入透彻地阐述了Windows底层的方方面面，包括系统架构，各种系统机制和管理机制，进程、线程和作业，安全，I/O系统，存储管理、内存管理和缓存管理，文件系统，联网，启动与停机，崩溃转储分析等内容，Windows的内幕在微软技术专家的笔下被解析得一目了然。

第6版分为卷1和卷2，仍由第5版的三位作者操刀，针对Windows 7和Windows Server 2008 R2进行了全面的更新，书中相应示例也都做了更新。卷1主要内容如下：

- 核心系统和管理机制工作原理，包括对象管理、同步、Wow64、Hyper-V和注册
- 数据结构以及进程、线程和作业的具体动作
- Windows安全模型
- Windows联网栈，包括API、BranchCache、协议和NDIS驱动器、分层服务
- 如何利用内核调试器、性能监视器等工具探究内核

延伸阅读

深入解析Windows操作系统，卷2（英文版·第6版）即将出版。

Microsoft

图灵社区：www.ituring.com.cn

新浪微博：@图灵教育 @图灵社区

反馈/投稿/推荐信箱：contact@turingbook.com

热线：(010)51095186转604



分类建议 计算机/操作系统/Windows

人民邮电出版社网址：www.ptpress.com.cn

ISBN 978-7-115-29090-8



9 787115 290908 >

ISBN 978-7-115-29090-8

定价：99.00元



Microsoft
Press

深入解析 操作系统

Windows

卷1

(英文版·第6版)

[美] Mark Russinovich
[美] David Solomon
[加] Alex Ionescu
著

人民邮电出版社



TURING 图灵程序设计丛书

Windows Internals

Part 1 Sixth Edition

深入解析 Windows操作系统 卷1 (英文版·第6版)

[美] Mark Russinovich
David Solomon 著
[加] Alex Ionescu

人民邮电出版社
北京

版权声明

Copyright © 2012 Posts & Telecom Press.

Authorized the English edition of *Windows Internals: Sixth Edition, Part 1* © David Solomon and Mark Russinovich. This English edition is published and sold by permission of O'Reilly Media, Inc., which owns or controls of all rights to publish and sell the same.

本书英文影印版由O'Reilly Media Inc.授权人民邮电出版社独家出版，未经出版者书面允许，不得以任何方式复制或抄袭本书。

版权所有，侵权必究。

站在巨人的肩上
Standing on Shoulders of Giants



www.ituring.com.cn

站在巨人的肩上
Standing on Shoulders of Giants



www.ituring.com.cn

图书在版编目 (CIP) 数据

深入解析Windows操作系统：第6版. 卷1 = Windows Internals: Sixth Edition. Part 1: 英文 / (美) 拉希诺维奇 (Russinovich, M.), (美) 所罗门 (Solomon, D.), (加) 艾欧内斯库 (Ionescu, A.) 著. — 北京: 人民邮电出版社, 2012. 9

(图灵程序设计丛书)

ISBN 978-7-115-29090-8

I. ①深… II. ①拉… ②所… ③艾… III. ① Windows操作系统—英文 IV. ①TP316.7

中国版本图书馆CIP数据核字(2012)第188455号

内 容 提 要

本书是操作系统内核专家 Russinovich 等人的 Windows 操作系统原理的最新版著作, 针对 Windows 7 和 Windows Server 2008 R2 进行了全面的更新, 主要讲述 Windows 的底层关键机制、Windows 的核心组件(包括进程/线程/作业、安全性、I/O 系统、存储管理、内存管理、缓存管理、文件系统和网络), 并分析了启动进程、关机进程以及缓存转储。书中提供了许多实例, 读者可以借此更好地理解 Windows 的内部行为。

本书内容丰富, 信息全面, 适合众多 Windows 平台开发人员、系统管理员阅读。

图灵程序设计丛书

深入解析Windows操作系统, 卷1 (英文版·第6版)

◆ 著 [美] Mark Russinovich David Solomon
[加] Alex Ionescu

责任编辑 朱 巍

◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街14号

邮编 100061 电子邮件 315@ptpress.com.cn

网址 <http://www.ptpress.com.cn>

北京艺辉印刷有限公司印刷

◆ 开本: 800×1000 1/16

印张: 46.5

字数: 744千字

2012年9月第1版

印数: 1-3 000册

2012年9月北京第1次印刷

著作权合同登记号 图字: 01-2012-4474 号

ISBN 978-7-115-29090-8

定价: 99.00元

读者服务热线: (010)51095186转604 印装质量热线: (010)67129223

反盗版热线: (010)67171154

Introduction

W*indows Internals, Sixth Edition* is intended for advanced computer professionals (both developers and system administrators) who want to understand how the core components of the Microsoft Windows 7 and Windows Server 2008 R2 operating systems work internally. With this knowledge, developers can better comprehend the rationale behind design choices when building applications specific to the Windows platform. Such knowledge can also help developers debug complex problems. System administrators can benefit from this information as well, because understanding how the operating system works “under the covers” facilitates understanding the performance behavior of the system and makes troubleshooting system problems much easier when things go wrong. After reading this book, you should have a better understanding of how Windows works and why it behaves as it does.

Structure of the Book

For the first time, *Windows Internals* has been divided into two parts. Updating the book for each release of Windows takes considerable time so producing it in two parts allows us to publish the first part earlier.

This book, Part 1, begins with two chapters that define key concepts, introduce the tools used in the book, and describe the overall system architecture and components. The next two chapters present key underlying system and management mechanisms. Part 1 wraps up by covering three core components of the operating system: processes, threads, and jobs; security; and networking.

Part 2, which will be available separately in fall 2012, covers the remaining core subsystems: I/O, storage, memory management, the cache manager, and file systems. Part 2 concludes with a description of the startup and shutdown processes and a description of crash-dump analysis.

History of the Book

This is the sixth edition of a book that was originally called *Inside Windows NT* (Microsoft Press, 1992), written by Helen Custer (prior to the initial release of Microsoft Windows NT 3.1). *Inside Windows NT* was the first book ever published about Windows NT and provided key insights into the architecture and design of the system. *Inside Windows NT, Second Edition* (Microsoft Press, 1998) was written by David Solomon. It updated the original book to cover Windows NT 4.0 and had a greatly increased level of technical depth.

Inside Windows 2000, Third Edition (Microsoft Press, 2000) was authored by David Solomon and Mark Russinovich. It added many new topics, such as startup and shutdown, service internals, registry internals, file-system drivers, and networking. It also covered kernel changes in Windows 2000, such as the Windows Driver Model (WDM), Plug and Play, power management, Windows Management Instrumentation (WMI), encryption, the job object, and Terminal Services. *Windows Internals, Fourth Edition* was the Windows XP and Windows Server 2003 update and added more content focused on helping IT professionals make use of their knowledge of Windows internals, such as using key tools from Windows Sysinternals (www.microsoft.com/technet/sysinternals) and analyzing crash dumps. *Windows Internals, Fifth Edition* was the update for Windows Vista and Windows Server 2008. New content included the image loader, user-mode debugging facility, and Hyper-V.

Sixth Edition Changes

This latest edition has been updated to cover the kernel changes made in Windows 7 and Windows Server 2008 R2. Hands-on experiments have been updated to reflect changes in tools.

Hands-on Experiments

Even without access to the Windows source code, you can glean much about Windows internals from tools such as the kernel debugger and tools from Sysinternals and Winsider Seminars & Solutions. When a tool can be used to expose or demonstrate some aspect of the internal behavior of Windows, the steps for trying the tool yourself are listed in “EXPERIMENT” boxes. These appear throughout the book, and we encourage you to try these as you’re reading—seeing visible proof of how Windows works internally will make much more of an impression on you than just reading about it will.

Topics Not Covered

Windows is a large and complex operating system. This book doesn't cover everything relevant to Windows internals but instead focuses on the base system components. For example, this book doesn't describe COM+, the Windows distributed object-oriented programming infrastructure, or the Microsoft .NET Framework, the foundation of managed code applications.

Because this is an internals book and not a user, programming, or system administration book, it doesn't describe how to use, program, or configure Windows.

A Warning and a Caveat

Because this book describes undocumented behavior of the internal architecture and the operation of the Windows operating system (such as internal kernel structures and functions), this content is subject to change between releases. (External interfaces, such as the Windows API, are not subject to incompatible changes.)

By "subject to change," we don't necessarily mean that details described in this book will change between releases, but you can't count on them not changing. Any software that uses these undocumented interfaces might not work on future releases of Windows. Even worse, software that runs in kernel mode (such as device drivers) and uses these undocumented interfaces might experience a system crash when running on a newer release of Windows.

Acknowledgments

First, thanks to Jamie Hanrahan and Brian Catlin of Azius, LLC for joining us on this project—the book would not have been finished without their help. They did the bulk of the updates on the "Security" and "Networking" chapters and contributed to the update of the "Management Mechanisms" and "Processes and Threads" chapters. Azius provides Windows-internals and device-driver training. See www.azius.com for more information.

We want to recognize Alex Ionescu, who for this edition is a full coauthor. This is a reflection of Alex's extensive work on the fifth edition, as well as his continuing work on this edition.

Thanks to Eric Traut and Jon DeVaan for continuing to allow David Solomon access to the Windows source code for his work on this book as well as continued development of his Windows Internals courses.

Three key reviewers were not acknowledged for their review and contributions to the fifth edition: Arun Kishan, Landy Wang, and Aaron Margosis—thanks again to them! And thanks again to Arun and Landy for their detailed review and helpful input for this edition.

This book wouldn't contain the depth of technical detail or the level of accuracy it has without the review, input, and support of key members of the Microsoft Windows development team. Therefore, we want to thank the following people, who provided technical review and input to the book:

- Greg Cottingham
- Joe Hamburg
- Jeff Lambert
- Pavel Lebedynskiy
- Joseph East
- Adi Oltean
- Alexey Pakhunov
- Valerie See

For the “Networking” chapter, a special thanks to Gianluigi Nusca and Tom Jolly, who really went beyond the call of duty: Gianluigi for his extraordinary help with the BranchCache material and the amount of suggestions (and many paragraphs of material he wrote), and Tom Jolly not only for his own review and suggestions (which were excellent), but for getting many other developers to assist with the review. Here are all those who reviewed and contributed to the “Networking” chapter:

- 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 and Dotan Elharrar were extremely helpful on NAP, and Shiva Kumar Thangapandi helped extensively with EAP.

The detailed checking Christophe Nasarre, overall technical reviewer, performed contributed greatly to the technical accuracy and consistency in the book.

We would like to again thank Ilfak Guilfanov of Hex-Rays (www.hex-rays.com) for the IDA Pro Advanced and Hex-Rays licenses they granted to Alex Ionescu so that he could speed up his reverse engineering of the Windows kernel.

Finally, the authors would like to thank the great staff at Microsoft Press who have been behind turning this book into a reality. Devon Musgrave served double duty as acquisitions editor and developmental editor, while Carol Dillingham oversaw the title as its project editor. Editorial and production manager Steve Sagman, copy editor Roger LeBlanc, proofreader Audrey Marr, and indexer Christina Yeager also contributed to the quality of this book.

Last but not least, thanks to Ben Ryan, publisher of Microsoft Press, who continues to believe in the importance of providing this level of detail about Windows to their readers!

Errata & Book Support

We've made every effort to ensure the accuracy of this book. Any errors that have been reported since this book was published are listed on our Microsoft Press site at oreilly.com:

<http://go.microsoft.com/fwlink/?Linkid=245675>

If you find an error that is not already listed, you can report it to us through the same page.

If you need additional support, email Microsoft Press Book Support at mspinput@microsoft.com.

Please note that product support for Microsoft software is not offered through the addresses above.

We Want to Hear from You

At Microsoft Press, your satisfaction is our top priority, and your feedback our most valuable asset. Please tell us what you think of this book at:

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

The survey is short, and we read every one of your comments and ideas. Thanks in advance for your input!

Stay in Touch

Let's keep the conversation going! We're on Twitter: <http://twitter.com/MicrosoftPress>.

Contents

Windows Internals, Sixth Edition, Part 1

| | | |
|------------------|---|-----------|
| Chapter 1 | Concepts and Tools | 1 |
| | Windows Operating System Versions | 1 |
| | Foundation Concepts and Terms | 2 |
| | Windows API | 2 |
| | Services, Functions, and Routines | 4 |
| | Processes, Threads, and Jobs | 5 |
| | Virtual Memory | 15 |
| | Kernel Mode vs. User Mode | 17 |
| | Terminal Services and Multiple Sessions | 20 |
| | Objects and Handles | 21 |
| | Security | 22 |
| | Registry | 23 |
| | Unicode | 24 |
| | Digging into Windows Internals | 24 |
| | Performance Monitor | 25 |
| | Kernel Debugging | 26 |
| | Windows Software Development Kit | 31 |
| | Windows Driver Kit | 31 |
| | Sysinternals Tools | 32 |
| | Conclusion | 32 |
| Chapter 2 | System Architecture | 33 |
| | Requirements and Design Goals | 33 |
| | Operating System Model | 34 |
| | Architecture Overview | 35 |
| | Portability | 37 |
| | Symmetric Multiprocessing | 38 |

What do you think of this book? We want to hear from you!

Microsoft is interested in hearing your feedback so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit:

microsoft.com/learning/booksurvey

| | |
|--|-----------|
| Scalability | 40 |
| Differences Between Client and Server Versions | 41 |
| Checked Build | 45 |
| Key System Components | 46 |
| Environment Subsystems and Subsystem DLLs | 48 |
| Ntdll.dll | 53 |
| Executive | 54 |
| Kernel | 57 |
| Hardware Abstraction Layer | 60 |
| Device Drivers | 63 |
| System Processes | 68 |
| Conclusion | 78 |
| Chapter 3 System Mechanisms | 79 |
| Trap Dispatching | 79 |
| Interrupt Dispatching | 81 |
| Timer Processing | 112 |
| Exception Dispatching | 123 |
| System Service Dispatching | 132 |
| Object Manager | 140 |
| Executive Objects | 143 |
| Object Structure | 145 |
| Synchronization | 176 |
| High-IRQL Synchronization | 178 |
| Low-IRQL Synchronization | 183 |
| System Worker Threads | 205 |
| Windows Global Flags | 207 |
| Advanced Local Procedure Call | 209 |
| Connection Model | 210 |
| Message Model | 211 |
| Asynchronous Operation | 213 |
| Views, Regions, and Sections | 214 |
| Attributes | 215 |
| Blobs, Handles, and Resources | 215 |
| Security | 216 |
| Performance | 217 |
| Debugging and Tracing | 218 |