第一图书网, tushu007.com

<<深入解析Windows操作系统>>

图书基本信息

书名：<<深入解析Windows操作系统>>

13位ISBN编号：9787115211651

10位ISBN编号：7115211655

出版时间：2009.9

出版时间：人民邮电出版社

作者：Mark Russinovich,David A. Solomon,Alex Ionescu

页数：1232

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：http://www.tushu007.com

第一图书网, tushu007.com

前言

It's both a pleasure and an honor for me to write the foreword for this latest edition ofWindows Internals. Many significant changes have occurred in Windows since the last editionof the book, and David, Mark, and Alex have done an excellent job of updating the book toaddress them. Whether you are new to Windows internals or an old hand at kernel develop-ment, you will find lots of detailed analysis and examples to help improve your understand-ing of the core mechanisms of Windows as well as the general principles of operating systemdesign.Today, Windows enjoys unprecedented breadth and depth in the computing world. Variantsof the original Windows NT design run on everything from Xbox game consoles to desktopand laptop computers to clusters of servers with dozens of processors and petabytes of stor-age. Advances such as hypervisors, 64-bit computing, multicore and many-core processordesigns, flash-based storage, and wireless and peer-to-peer networking continue to provideplenty of interesting and innovative areas for operating system design.One such area of innovation is security. Over the past decade, the entire computing indus-try——and Microsoft in particular——has been confronted with huge new threats, and securityhas become the top issue facing many of our customers. Attacks such as Blaster and Sasserthreatened to bring the entire Internet to its knees, and Windows was at the eye of the hur-ricane. It was obvious to us that we could no longer afford to do business as usual, as manyof the usability and simplicity features designed into Windows were being used to attack itfor nefarious reasons. At first the hackers were teenagers trying to gain notoriety by breakinginto systems or adding graffiti to a corporate Web site, but pretty soon the attacks intensifiedand went underground. The hackers became more sophisticated and evaded inspection. Yourarely see headlines about viruses and worms these days, but make no mistakembotnets andidentity theft are big business today, as are industrial and government espionage throughtargeted attacks.

第一图书网, tushu007.com

<<深入解析Windows操作系统>>

内容概要

本书是操作系统内核专家Mark Russinovich和David Solomon的Windows操作系统原理的最新版著作，针对Windows Vista和Windows Server 2008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。

第一图书网, tushu007.com

作者简介

Mark E.Russlnovich 微软技术院士（Technical Fellow）。
享誉世界的Windows内核技术专家。
他也是Sysinternals的创建者之一。
开发了很多用于Windows管理和诊断的工具。

第一图书网, tushu007.com

<<深入解析Windows操作系统>>

书籍目录

1 Concepts and Tools Windows Operating System Versions Foundation Concepts and Terms Windows API Services, Functions, and Routines Processes, Threads, and Jobs Virtual Memory Kernel Mode vs User Mode Terminal Services and Multiple Sessions Objects and Handles Security Registry Unicode Digging into Windows Internals Reliability and Performance Monitor Kernel Debugging Windows Software Development Kit Windows Driver Kit Sysinternals Tools Conclusion 2 System Architecture Requirements and Design Goals Operating System Model Architecture Overview Portability Symmetric Multiprocessing Scalability Differences Between Client and Server Versions Checked Build Key System Components Environment Subsystems and Subsystem DLLs Ntdll dll Executive Kernel Hardware Abstraction Layer Device Drivers System Processes Conclusion 3 System Mechanisms Trap Dispatching Interrupt Dispatching Exception Dispatching System Service Dispatching Object Manager Executive Objects Object Structure Synchronization High-IRQL Synchronization Low-IRQL Synchronization System Worker Threads Windows Global Flags Advanced Local Procedure Calls (ALPCs) Kernel Event Tracing Wow64 Wow64 Process Address Space Layout System Calls Exception Dispatching User Callbacks File System Redirection Registry Redirection and Reflection I/O Control Requests 16-Bit Installer Applications Printing Restrictions User-Mode Debugging Kernel Support Native Support Windows Subsystem Support Image Loader Early Process Initialization Loaded Module Database Import Parsing Post Import Process Initialization Hypervisor (Hyper-V) Partitions Root Partition Child Partitions Hardware Emulation and Support Kernel Transaction Manager Hotpatch Support Kernel Patch Protection Code Integrity Conclusion 4 Management Mechanisms 5 Processes, Threads, and Jobs 6 Security 7 I/O System 8 Storage Management9 Memory Management 10 Cache Manager 11 File Systems 12 Networking 13 Startup and Shutdown 14 Crash Dump Analysis Glossary Index

第一图书网, tushu007.com

章节摘录

插图：Because the flag responsible for special kernel APC delivery disabling （and the guardedregion functionality） was not added until Windows Server 2003, most drivers do not yettake advantage of guarded mutexes. Doing so would raise compatibility issues with earlierversions of Windows, which require a recompiled driver making use only of fast mutexes.Internally, however, the Windows kernel has replaced almost all uses of fast mutexes withguarded mutexes, as the two have identical semantics and can be easily interchanged.Another problem related to the guarded mutex was the kernel function KeAreApcsDisabled.Prior to Windows Server 2003, this function indicated whether normal APCs were disabled bychecking if the code was running inside a critical section. In Windows Server 2003, this func-tion was changed to indicate whether the code was in a critical, or guarded, region, changingthe functionality to also return TRUE if special kernel APCs are also disabled.Because there are certain operations that drivers should not perform when special ker-nel APCs are disabled, it makes sense to call KeGetCurrentlrql to check whether the IRQLis APC level or not, which is the only way special kernel APCs could have been disabled.However, because the memory manager makes use of guarded mutexes instead, thischeck fails because guarded mutexes do not raise IRQL. Drivers should therefore callKeAreAIIApcsDisabled for this purpose. This function checks whether special kernel APCs aredisabed and/or whether the IRQL is APC level-the sure-fire way to detect both guardedmutexes and fast mutexes.

第一图书网, tushu007.com

媒体关注与评论

“在微软，我们一直用本书培训新员工……如果你和我一样，想要深入理解Windows。本书将是一个绝佳的起点。”
——Windows之父Jim AIIchin“每一位真正的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WDavid Cutler“我想不出还有哪一本书能比本书更具权威性。”
——微软公司副总裁Ben Fathi

第一图书网, tushu007.com

<<深入解析Windows操作系统>>

编辑推荐

《深入解析Windows操作系统(第5版.英文版)》：近20年来，无论是开发人员还是系统管理员。
如果想探究Windows核心部件的运作机理或者各种技术细节，都会求助于这部毋庸置疑的权威著作。
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，使Windows的内幕一目了然。
《深入解析Windows操作系统(第5版.英文版)》作者阵容空前强大，除了Russinovich币llSolomon两位大师之外，还新增了年轻一代最具实力的Windows内核专家lonescu。
与上一版相比，本版修订篇幅超过25%，除针对Windows Visla和Windows Server 2008新特性《PatchGuard、Hyper-V支持、内核事务管理器、I／O优先级等)进行了全面更新外。
作者也对之前未涉及或者阐述不够的既有技术进行了挖掘，包括映像加载程序、用户态调试框架、64位调用表和压缩等。
更充分运用了自己编写的流行工具Process Explorer和Process Monitor更新了大量实验和示例。
这一切都使《深入解析Windows操作系统(第5版.英文版)》更趋完美。
Windows之父Allchin，Windows NT首席设计师Cutler，微软公司副总裁Fathi联袂推荐。
微软官方Windows权威著作最新版，深入剖析Windows技术内幕，大幅更新，涵盖Windows内核新特性。

第一图书网, tushu007.com

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:http://www.tushu007.com