Designed for Microsoft® Windows NT® Windows™ 95

Microsoft 编程系列

Includes prerelease information about Windows NT 5.0

Windows NT® 技术内幕 第二版

关于 Microsoft 的首要操作系统的体系结构和内部机制的正式指南

[美] David A. Solomon 著
北京博彦科技发展有限公司 译

清华大学出版社
http://www.tup.tsinghua.edu.cn

Microsoft® Press

Windows NT 技术内幕

(第二版)

[美] David A. Solomon 著

北京博彦科技发展有限公司 译

清 华 大 学 出 版 社

（京）新登字 158 号

Windows NT 技术内幕（第二版）

Inside Windows NT, 2nd Edition

David A. Solomon

图书在版编目（CIP）数据

Windows NT 技术内幕：第 2 版/（美）索罗门（Solomon,D.A.）著；北京博彦科技发展有限公司译.
—北京：清华大学出版社，1999.2
ISBN 7-302-03356-0

Ⅰ. W…　Ⅱ. ① 索…　② 北…　Ⅲ. 计算机网络—操作系统（软件），Windows NT　Ⅳ. TP393

中国版本图书馆 CIP 数据核字（1999）第 04455 号

出 版 者：清华大学出版社(北京清华大学校内，邮编 100084)
http：// www. tup. tsinghua. edu. cn
责任编辑：石磊(E-mail：shl@tup. tsinghua. edu. cn)
印 刷 者：清华大学印刷厂
发 行 者：新华书店总店北京发行所
开　　本：787×960 1/16　印张：28　字数：608 千字
版　　次：1999 年 7 月第 1 版　1999 年 9 月第 2 次印刷
书　　号：ISBN 7-302-03356-0/TP・1811
印　　数：5001～9000
定　　价：50. 00 元

译者序

Windows NT 4.0 是微软公司的一个非常成功的操作系统，《Windows NT 技术内幕（第二版）》就是根据 Microsoft Windows NT 4.0 Service Pack 3 编写而成的，供高级计算机专业人员使用。

在《Windows NT 技术内幕（第一版）》出版以后，其中的一些材料被 Windows NT 的开发者视为宝典，但随着 Windows NT 的新版本的推出，尤其是即将发布的 Windows NT 5.0（现已更名为 Windows 2000），其中的很多内容已经发生了变化，这就需要对原书进行修订，增加这些新的内容，让读者能系统地学习并掌握这些新的变化。

《Windows NT 技术内幕》的作者本人对 Windows NT 有很深的理解，在他写作的同时又得到了许多专家的支持和帮助，他们中的有些人参与了 Windows NT 的设计，因此这本书非常有权威性，这也是我们把它推荐给读者的一个主要原因。与它的第一版相比，本书的内容更丰富和全面。通过对本书的学习，程序开发者在设计 Windows NT 平台的应用程序时将能更好地领会在程序运行背后的基本原理，从而帮助他们解决在调试当中的一些复杂的问题；系统管理者在处理故障时也能从这些信息中得到帮助，从而使故障诊断更加容易。

另外，在书中有大量的实验，其中介绍了许多 Windows NT 标准工具和 Windows NT 的相关工具包中的工具，读者可以尝试使用这些工具去了解和体会 Windows NT 的内部是怎样工作的，通过这些实验来加深学习的印象。同时，本书对在 Windows NT 5.0 中的变更作了标记，并在书中的最后一章对它们进行了简要介绍，这样读者就能在学习的同时了解在 Windows NT 5.0 中的新变化。

参加本书翻译工作的人员主要有乔龙巴特、李旭源、李巍、张淑艳等，他们在经过数月的艰苦工作之后将这本书奉献给了广大读者。此外，还要感谢清华大学出版社的石磊先生，正是他一丝不苟的审校，才使这本书得以顺利出版。

因为本书涉及的知识和技术是如此精深，所以尽管我们为此付出了很多努力，但限于水平，书中难免还存在一些翻译不当之处，欢迎广大读者批评指正。

北京博彦科技发展有限公司

1998 年 12 月

前　言

很多人经常问我什么时候更新《Windows NT 技术内幕（第一版）》。很明显，在Windows NT 的三个主要版本之后，有很多内容已经发生了变化，这就很有必要修订版本。例如，Windows NT 4.0 完全重做了用于图形引擎的客户/服务器模型，把大部分的 USER 和 GDI 组件移入了核心态。而作为高性能 I/O 应用程序基础的完成端口，在本书的第一版发行时还不存在。系统还做了许多其他小的增强，例如分散/集中 I/O、为了更好的可伸缩性而在调度程序和内存管理程序中所做的变化、在调度算法中的变化和对新的 API 的支持。尽管这些变化使 Windows NT 成为更稳固更强大的操作系统（尽管我个人认为，没有任何核心组件需要进行重大更改的事实是初始设计进行得十分细致的很好证明），但这也意味着《Windows NT 技术内幕（第一版）》中的一些材料（虽然这些材料被 Windows NT 开发者视为宝典）已经多少有些过时并且需要扩充。

大约在一年以前，David Solomon 先生同意从事编写《Windows NT 技术内幕（第二版）》的工作。像大多数人一样，他大大低估了撰写这本书所需要的时间。即便如此，他还是在 Windows NT 5.0 出版之前完成了它！当我听说 David 先生被提名修订这本重要的书籍时，我就知道这本书一定会和它的第一版一样成功。

我初次见到 David 先生是我们共同在 Digital Equipment Corporation 工作的时候。在那个时候，他就对 Windows NT 很感兴趣。当 Microsoft 宣布要召开第一次 Windows NT Professional Developers Conference （PDC）后，David 先生就打电话给我，询问我是否认为通过召开研讨会来帮助客户由 VAX/VMX 转向 Windows NT 将会是一项可以获得成功的计划。怀着对 Windows NT 及 David 先生的信心，我告诉他，去做吧！在 PDC 上，David 先生已经致力于一本用 VAX/VMS 术语描述 Windows NT 的书，并列出了很多要向我以及他能找到的任何人请教的问题。

David 先生完成了一项令人吃惊的工作，他解释了操作系统的各个部分相互作用的方式，并描述了管理内核及核心态构造的规则和策略。除更新了反映 Windows NT 4.0 的内容外，David 先生还深入到数据结构和内部组件的更深层次的内容中，并且指出了如何使用在系统中分布的和 Windows NT 资源工具包中的工具，检查内部系统结构和了解内部系统结构间的关系。他还合并了有关 Windows NT 文件系统（NTFS）的内容，这些内容起初是一个单独出版物，但现在 David 先生把它写成了有关高速缓存管理程序的完整一章。

很奇怪，Windows NT 4.0 版本作为本书的基础，实际上是 Windows NT 的第四个版本。我说“奇怪”是因为软件版本的版本号很少和零售市场上软件已发布的次数相联系。Windows NT 的第一版发布于 1993 年 7 月，版本号是 3.1。版本号的挑选并不

是要让人们相信他们获得了更成熟的产品，也就是说，我们不是说不要购买任何版本号小于 3.0 的版本。当然，选择 3.1 是为了保持与现有的应用程序兼容。应用程序通常要使用操作系统的某些特性。要确认存在那些特性，应用程序将询问操作系统的版本号。如果版本号不够高，就不能安装应用程序。版本号的检查本身是一种魔术。在设计 Windows NT 时，我们试着通过提供简单的 API 使版本号检查变得更加简单。伴随着每个新版本的发布，您将会发现一些应用程序不能正确安装在更高版本的系统中，这是因为它们的版本检查不正确。（大多数应用程序采用的测试等式是，如果版本不是 4.0，那么它一定就是 3.51。）

因为 Windows NT 的第一版与 Windows 3.1 兼容，所以“获得版本号”将返回 3.1。因此，我们本应该把这个产品称为 Windows NT 1.0 版，并将 3.1 返回给应用程序。而应用程序的编写者已经很担忧了，并且这个技巧只会增加他们的不解。经过反复讨论，我们决定把它称为 3.1，与 16 位 Windows 一样。

Windows NT 第二版的代号为 Daytona，发布于 1994 年 9 月。这个版本引起争议的地方是称它为 3.2 还是 3.5。这个版本主要是大小和性能的优化。

Windows NT 的第三版发布于 1995 年 5 月。该版本主要是特性集的微小改进、对 Power PC 的支持和大量的性能优化。因为特性集在很大程度上与 3.5 版一样，所以其版本号是 3.51。该版本号表明这个版本只是对 3.5 版本进行了很小的特性修改，企业对该版本进行升级不会引起很大的操作争议。

Windows NT 的第四版即 Windows NT 4.0，在 1996 年 7 月发布。该版本代号为 SUR（即 Shell Update Release，外壳更新版本），它与 Windows 95 有着相同的外观和感觉。但是 Windows NT 4.0 的变化并不仅仅是表面上的。例如，它包含了许多新的特性，通过把图形引擎（USER、GDI 和视频驱动程序）从用户态进程（CSRSS）移入核心态，使图形子系统的性能得到很大的提高。在 Windows NT 以前的版本中，图形引擎是一个单独的进程，并且使用本地过程调用机制发布请求。把图形引擎移入到核心态中会消除在多个进程之间保持数据共享能力时进程描述表切换的系统开销——数据在内核地址空间内共享，而不是在用户态进程内共享。

本书这一版的变化之一是不包括任何有关工程师或其他人做了什么工作和为什么这样做的讨论。自一小群人在一起共同设计 Windows NT 的整个核心体系结构起，已经差不多有 10 年了。自那以后，致力于 Windows NT 工作的人数已经大大增加了，同时，我也很难做到准确说出他们的名字而不会冒犯另外一些人。既然这样，就让我告诉您在 1988 年 11 月我们开始设计如今的 Windows NT 系统时，就已经加入此行列的那些人的姓名，他们是：Dave Cutler，Darryl Havens，Gary Kimura，Mark Lucovsky，Steve Wood 和我。从那以后，Windows NT “小组”就逐渐发展为拥有 200 多名专职工程师的队伍。他们从事着核心组件（内核、图形、驱动程序、文件系统、网络、目

录服务、安全、安装、管理、外壳、OLE 和 RPC 等等）的研究工作。同时还有更多的人从事着辅助产品（例如 Internet Explorer、NetMeeting、语言运行时库和一些实用程序）的研究。

我非常愿意向每一位对 Windows NT 内部工作感兴趣的人推荐《Windows NT 技术内幕（第二版）》。读完此书以后，您将会对如何调整系统，如何分析 Windows NT 系统的性能和功能，以及 Windows NT 的各部分是如何组合起来的有更深入的了解。虽然从 Windows NT 刚刚出现时，我就一直从事核心态代码的研究，但我仍然觉得读 David 先生的书是一种享受。我相信您一定也会喜欢它！

Lou Perazzoli
Windows NT 核心操作系统主管
Microsoft Corporation

致　谢

出于对操作系统内幕的兴趣和爱好，我很想写一本关于 Windows NT 内幕的书，在 1993 年我开始教授有关这方面课题的课程时，就有了这个想法。在 Frank Artale（微软公司 Windows NT 计划管理的主管）与我接触之前，我就在打算写书的草稿。我在 TechEd 96 上做了有关 Windows NT 内幕的演讲之后，Frank Artale 问我是否有兴趣写《Windows NT 技术内幕（第二版）》。怀着对《Windows NT 技术内幕（第一版）》极大的崇敬——同时带着如何对它进行提高的明确目的——我同意了；几个月后，我们签了一份合同。经过一年多的努力工作，这本书终于完成了。尽管它并不如我所预想的那样全面，但它的下一版会更好一些……

我要感谢下面这些人对这个项目的支持和帮助，没有他们，这本书就不能和读者见面：

- 首先要感谢 Helen Custer，她写了本书的第一版，并为本书建立了非常好的声誉。
- Frank Artale，是他首次与我谈到写这本书。
- Lou Perazzoli，Windows NT 核心操作系统小组的主管，感谢他对此项目的大力支持以及他在内存管理器方面的专业知识。
- Stacey Lemire，Lou 的上级行政主管，在我多次访问 Redmond 时，他容忍了我对临时办公地点和证件的经常性的请求。
- Dave Cutler，Windows NT 的设计者，是他允许我访问源代码，这样 Jamie Hanrahan 和我就能对构成本书基础的问题进行讨论。
- Landy Wang，内存管理器的主要开发人员，感谢他细心地检查了各个章节并附以简短的评论，同时他还花费了大量的时间来解释那些令人生畏的复杂的系统组件。
- David Fields，有关 Windows NT Workstation 性能的主角，他仔细检查了对工作集修整的描述。
- Tom Miller，高速缓冲管理器的领导，是他在长途旅行之前审阅了高速缓冲管理器一章。
- Brian Andrew，他回顾了最初的 NTFS 书籍，然后和我一起在自助餐厅中对他的注释进行了润色，并预览了计划中的 NTFS 5.0 扩充。

- Ken Hiatt，Windows NT 编译研究室的领导，他经常及时地响应我对服务器、专用编译和源代码树进行访问的各种各样的请求。
- Eric Stroo，微软出版社的经理，这个项目的前前后后都是他在领导我，并给我以鼓励和批评。Eric 的电话是最让我害怕的。
- Sally Stickney，她是我在微软出版社中的编辑，她对我在整个写作过程中的疑问作了详细的讲解。即使在进度很慢时，Sally 仍对我非常友好，并给我以鼓励。她的电话仅次于 Eric，排在“最可怕”电话号码清单的第二位。
- Jim Fuchs，我的技术编辑，他解决了在原稿中与技术细节有关的问题（因为我给他们的图是错的，他重做了书中所有的图）。
- Jeffrey Richter，他检查了本书的许多章节，在此书的最后几个星期中，他让我呆在他的家中，他总是怀疑我能否按时完成这个项目。
- Jamie Hanrahan，我们 Windows NT 内部研讨会的合作者，感谢他允许我使用他开发的一些图形。
- Compaq 公司的 Trevor Porter 和 Richard Mouser，为了这个项目，他们把带有高速双 Pentium Pro 处理器的 Compaq Professional Workstation 5000 借给了我。我使用这台计算机做了内核调试和搜索 Windows NT 源代码。
- 感谢我的可靠和值得信赖的办公室工作人员 Mark Stevens 和 Ronie Diaz，是他们尽量不让我分心以便专心工作（他们整天都在问我：“您在做什么？”）。
- 最后，但相当重要，我要感谢我的妻子 Shelly 和三个孩子 Daniel，Rebecca 和 Sarah，感谢他们容忍了我的缺席，感谢他们对我耐心的鼓励，让我能专心地工作（即使是我拖延了工作的时候），感谢当我回家时的美好的聚会。感谢那个气球！噢！

David Solomon

1998 年 3 月

简　介

《Windows NT 技术内幕（第二版）》是供高级计算机专业人员（包括开发者和系统管理者）使用的参考书。这些专业人员希望了解 Microsoft Windows NT 操作系统中核心组件的内部工作方式。凭借对 Windows NT 内部的了解，在建立运行于 Windows NT 平台的应用程序时，程序开发者可以更好地领会在设计选择背后的基本原理。类似这样的知识可以帮助他们解决在调试当中的一些复杂问题。因为了解操作系统内部的工作方式有助于理解系统的运作方式，而且在处理故障时也会使系统问题的故障诊断更加容易，所以系统管理者也可以从这些信息得到帮助。在读过此书以后，您将会更好地理解 Windows NT 如何工作和为什么会这样工作。

本书是根据 Windows NT 4.0 Service Pack 3 编写而成的。在正文中以说明的形式引用了在 Windows NT 5.0 中的变更，并在后面加上“（Windows NT 5.0）”以示标记，如下所示：

说明（Windows NT 5.0）：此类说明描述了计划在 Windows NT 5.0 中变更的内容。在这本书的正文当中您将会发现许多这样的说明。

第二版中的差异

《Windows NT 技术内幕（第二版）》中包含了在第一版中的所有主题，并增添了高速缓存管理程序、Windows NT 文件系统（NTFS）和预览在 Windows NT 5.0 即将出现的更改。第二版与第一版相比，内容更加详尽。例如本书包含了关键系统功能的代码流程，也更加详细地描述了关键的内部数据结构与系统全局变量。本书的这些信息主要来源于对 Windows NT 4.0 源代码的阅读，也来源于同主要的 Windows NT 开发人员及设计人员的切磋。（在此衷心感谢 Microsoft 的大力支持！）

此修订版的另一个主要新特性是其中的实验。尽管我是根据源代码来汇集此版本的信息的，但是通过使用一些标准工具（例如内核调试程序和性能监视器）以及在 Windows NT 资源工具包、Win32 软件开发工具包（SDK）和 Windows NT 设备驱动程序工具包（DDK）中的一些其他工具，您将可以学习或演绎许多有关 Windows NT 内部的情况。当您需要使用某些工具来揭示或显示 Windows NT 内部行为的某些方面时，在“实验”框中还将列出使用工具时所要执行的必要步骤。我建议您在阅读本书的同

时，尝试着去使用这些工具，实际观察并体会 Windows NT 的内部是怎样工作的，这样会使您对所读内容有更深刻的印象。

本书没有包含的主题

Windows NT 是一个庞大而复杂的操作系统。本书并未包含所有与 Windows NT 内部有关的内容，而是着重于基本的系统组件。唯一在第一版中出现而在这个版本中没有涉及的主题是网络。Windows NT 网络已经发展成为系统的极其重要的组成部分，可以单独编写成书。我希望有一天有人能写这样的一本书。

本书没有探讨的系统的另一个重要领域是 COM（Component Object Model）。COM（和 DCOM——分布式的 COM）是 Windows 分布式面向对象程序设计的构造基础。在微软出版社出版的其他几本书中，详细讲述了有关 COM 的内容，其中一本是由 Dale Rogerson 写的《Inside COM》。

最后，因为本书是介绍 Windows NT 内部情况的书，而不是有关用户、程序设计和系统管理的书，因此本书并不介绍 Windows NT 的使用、程序设计以及配置的方法。

本书的结构

除了前面三章（分别是“概念和工具”、“系统体系结构”和“系统机制”）覆盖了在整本书中要用到的基本术语和概念以外，您可以按任意顺序读其他章节，例如进程和线程、内存管理、安全、I/O 系统、高速缓存管理程序、Windows NT 文件系统（NTFS）、Windows NT 5.0 及以后版本。如果按顺序阅读本书，您将会获得更多的知识。

通知和警告

因为本书描述了 Windows NT 的内部构造和操作，所以在不同版本间某些信息会有所变化（尽管外部接口，例如 Win32 API，没有经过不兼容的修改）。例如，我参考了内部 Windows NT 系统例程、数据结构和变量以及在内部使用的用来确定资源大小和相关性能的算法和数值。这些细节根据定义在不同版本间会有所变化。

说“可能会有变动”，并不是说在本书中的详细描述在不同的版本间“一定会”改变——但是您不要以为它们不会改变。任何使用了这些非文档化的接口的软件在将来发行的 Windows NT 中可能不会工作。更糟糕的是，当升级新版本的 Windows NT 时，运行在核心态的软件（例如设备驱动程序）如果使用了这些非文档化的接口，可能会导致系统崩溃。

更新信息和勘误表

这本书并不完美。毫无疑问，它会存在一些不太准确的地方，或者可能遗漏了一些应该涉及的内容。如果您发现了您认为不正确的内容或是应该涉及而没有涉及到的内容，请把电子邮件发到 daves@solsem.com。如果在这个修订版中存在任何重大错误，我准备在微软出版社技术支持知识库（Knowledge Base）中以知识库文章来发表它们。您可以进入 http://mspress.microsoft.com/support/support.htm 中查询“Knowledge Base”。

目 录