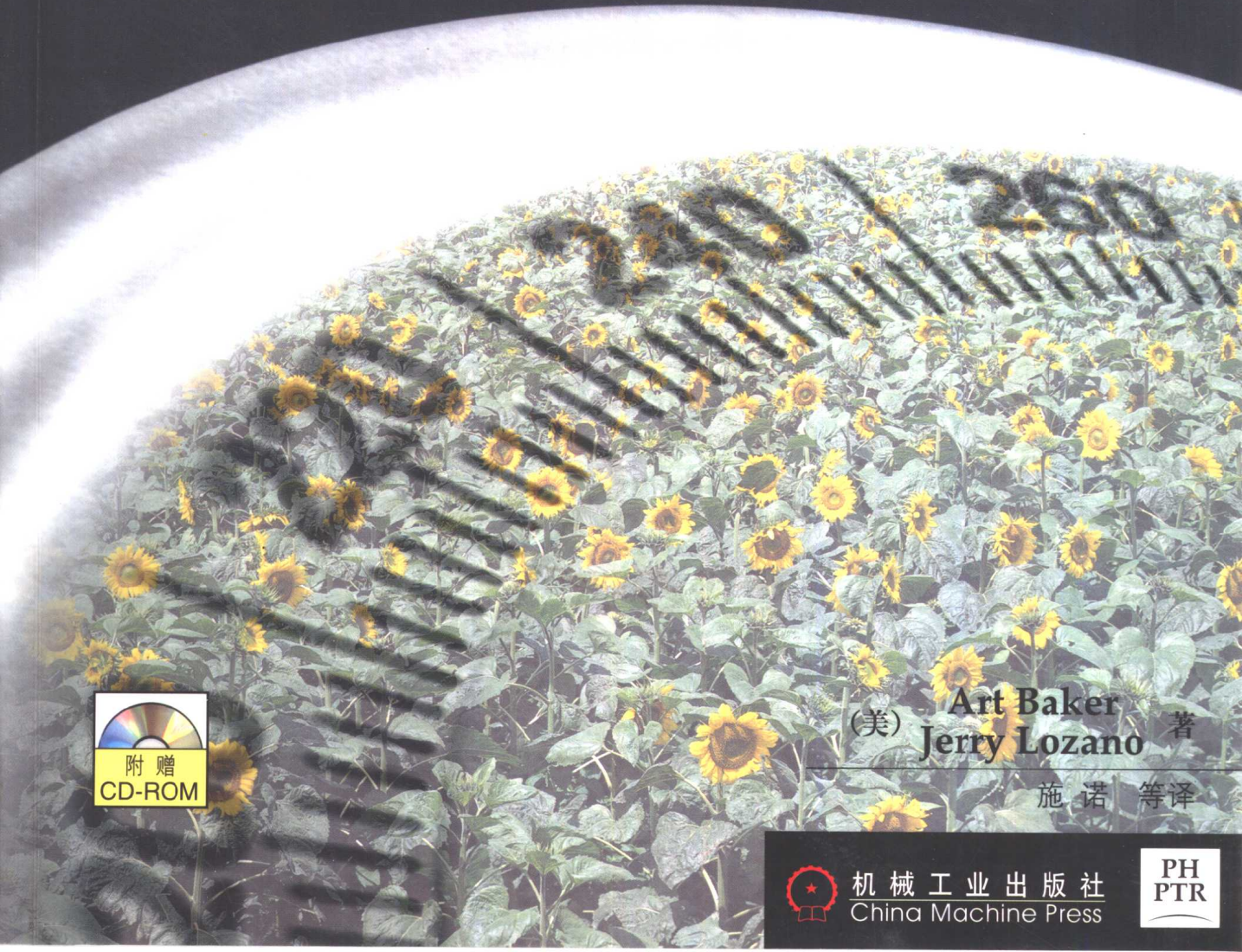
HZ BOOKS

The Windows 2000 Device Driver Book *(Second Edition)*

软件开发技术丛书

Windows 2000 设备驱动程序设计指南

（原书第2版）



附赠 CD-ROM

(美) Art Baker
Jerry Lozano 著

施诺 等译

机械工业出版社
China Machine Press

PH PTR

软件开发技术丛书

Windows 2000 设备驱动程序设计指南

（原书第2版）

（美） Art Baker
Jerry Lozano 著

施 诺 等译

机械工业出版社
China Machine Press

本书全面讲述了驱动程序模型、内核模式编程和硬件接口等方面的知识，可作为驱动程序开发的自学教材使用。全书共分17章和三个附录，第1～5章讨论编写设备驱动程序所需的基础知识。包括Windows 2000体系结构，Windows 2000 I/O管理程序等内容。第6～13章是本书的核心内容，讨论了Windows 2000驱动程序开发的所有内容。第14～15章讨论设备驱动程序构造方面的高级主题，包括使用系统线程、分层、过滤和驱动程序类别等。最后两章讨论驱动程序的安装和调试。附录部分讨论了驱动程序开发所需的参考信息，列出了Windows 2000符号文件安装、故障检验码等内容。

本书版权登记号：图字：01－2001－1115

图书在版编目(CIP)数据

Windows 2000设备驱动程序设计指南/(美)贝克(Baker, A.)，(美)洛泽诺(Lozano, J.)著；施诺等译. －北京：机械工业出版社，2001.9
(软件开发技术丛书)
书名原文：The Windows 2000 Device Driver Book: Second Edition
ISBN 7-111-09283-X

Ⅰ.W… Ⅱ.①贝… ②洛… ③施… Ⅲ.窗口软件，Windows 2000－装配程序－程序设计－指南 Ⅳ.TP316.7－62

中国版本图书馆CIP数据核字(2001)第055718号

机械工业出版社(北京市西城区百万庄大街22号 邮政编码 100037)
责任编辑：刘立卿
北京市密云县印刷厂印刷·新华书店北京发行所发行
2001年9月第1版第1次印刷
787mm×1092mm 1/16·23.5印张
印数：0 001-5 000册
定价：58.00元(附光盘)

译 者 序

众所周知，驱动程序开发是操作系统开发中最棘手、技术难度最大的一部分。设备驱动程序的优劣直接影响设备性能的发挥，尤其在 Windows 2000 的全新体系结构下，更加强调设备驱动程序必须与系统基本代码进行和谐的相互作用。

本书全面介绍了驱动程序的规划、实现、测试、调试、安装和发布，是有关 Windows 设备驱动程序创作方面最优秀的指南之一，完全更新到 Windows 2000 版本！全面介绍了新的 Windows 驱动程序模型（WDM，Windows Driver Model）、实用调试技术和交互式故障解决方法。同时，书中大多数章节都给出了一个或多个示例驱动程序，并包含在本书附带的光盘中。建议在学习过程中理论与实践相结合，动手实现每一个小程序，以取得最佳学习效果。

如果读者具备 Windows 管理方面的知识，具有 Win32 用户模式编程经验和 C 程序设计语言等方面的知识，则阅读本书能够取得更好的效果。本书可以作为一本有关驱动程序开发方面的自学教材使用，它不仅适用于那些有经验的设备驱动程序开发人员，同样也适用于那些有经验的 Windows 程序员。通过本书的学习，他们将掌握驱动程序开发的整个过程。同时，本书对于那些研究 Windows 2000 内核的人来说也是有用的，尤其是那些研究 I/O 子系统和相关组件的人。

在本书的翻译工作中，我们深深地为原著作者的教育才能所感动，仿佛自己就正在教室里听他讲课一样。在翻译过程中我们尽全力使译文忠实地体现原著的风格、内容和思想，希望读者在阅读本书中能与我们有同样的体会，这也是本书翻译过程中努力实现的目标。

本书主要由施诺组织翻译，参加本书翻译、录排、校对等工作的人员有：施惠琼、方杰、张廷辉、陈指挥、倪志红、赵朗、徐睿胤、钱建国、严俊、施晓东、盛仕辉、陈根样、王小光、龚露娜、马军、马丽、田军、田洗县、王小将等。全书最后由施平安进行统稿。

在翻译过程中，我们对本书中出现的术语都进行了仔细的推敲和研究，但由于本书的内容涉及许多有关 Windows 驱动程序开发方面的新知识，而有些方面在译者自己的开发经历中也很少遇到，加上时间仓促，译者水平有限，疏漏和争议之处在所难免，望广大读者提出宝贵的意见。

如果您在阅读中碰到了什么问题，请同我们工作室联系：qiandao@263.net。我们会尽力解决您的问题。

施 诺

2001 年 4 月

序

驱动程序的开发是操作系统开发过程中最基本的，也是技术难度最大的一部分。作为本书的读者，你应该已经意识到其中具有的复杂性。即便是对于经验非常丰富的软件工程师来讲，开发驱动程序也将是比较棘手的。编写 Windows 2000 中的设备驱动程序是 Windows 2000 学习中的一大难题。Art Baker 编写的“Windows NT Device Driver Book”是关于 Windows NT 驱动程序开发方面的最详细、最权威的指南，是当前关于 Windows NT 驱动程序开发的经典著作。我认为除了 Jerry Lozano 外，任何人都不能胜任编写 Art 的著名教程的第 2 版。Jerry 兼有十足的技术专家、优秀的作家和天才教育家的特点，而这些特色都已经在本书中得到了很好的表现。我在阅读本书的过程中，仿佛觉得就是在听 Jerry 讲课。

世界上有两种不同类型的书。一些书提供参考信息，它们读起来非常像一本百科全书，这种书适合在需要解决某个特定的问题时去查阅一下。而另一些书实际上就是自学教材，传播所需的知识和技能以解决某个问题，读者需要从头到尾地对它们进行阅读和学习。

本书与它的前一个版本一样，显然属于后一种类型的书籍。它旨在作为设备驱动程序开发者的指南。与关于该主题的其他书籍不同，本书不准备重复 DDK 内容。DDK 可作为 Windows 2000 设备驱动程序技术的权威参考，而本书提供了成功掌握 W2K 驱动程序开发的指导性内容，为开发者提供了设计、编写和调试 Windows 2000 设备驱动程序所需的知识，并且是基于 Jerry 创建的在 UCI 教学中使用的课程。根据教学过程中反馈回来的信息，作者发现，设备驱动程序和内核模式代码开发者们面临的最大问题是：缺乏关于驱动程序模型、内核模式编程和硬件接口的清楚而简明的技术资料。在本书中，Jerry 通过详细的示例和涉及各个领域的内容，成功地解决了上述难题，并且把它们论述得异常清楚。

在本书即将出版时，我清楚地认识到还有一章内容也是非常需要的，即关于 USB 和 IEEE 1394 驱动程序的细节，并向作者提出修正意见。作者愉快地接受了这一修正意见，并将这些内容包括在本书所属的网站中：www.W2KDriverBook.com。需要这些内容的读者可以访问这一站点。

Andrew Scoppa
UCI 软件技术培训主席

前　言

本书讲述如何编写、安装和调试 Windows 2000 设备驱动程序，旨在作为 Microsoft DDK 文档和软件的补充教材。

Windows 2000 与 Windows NT 的前几个版本相比，在各方面都得到了相当的改善。为 Windows 2000 设计的设备驱动程序也可以用于新的 WDM 体系结构。如果这样，驱动程序将成为与 Windows 98 相兼容的资源。本书讨论了新的 WDM 规范。

同时，本书对于那些研究 Windows 2000 内核的人来说也是有用的，尤其是那些研究 I/O 子系统和相关组件的人。

读者应具备的知识

本书的所有内容都要求读者具备一定的基础知识。首先，读者必须熟悉 Windows 2000 管理——例如，安全性和安装。因为对内核代码进行试验可能会产生与系统相关的问题；因此，读者心里应该有所准备，并能够在系统出现问题时对之进行恢复。

其次，读者应当熟悉 C 程序设计语言，并在一定程度上熟悉C++ 语言。在本书中只用到极少数的C++ 语言，并且其目的只是为了简化冗长的代码。

再次，具备 Win32 用户模式编程经验是有用的。在设计和测试设备驱动程序代码方面，知道用户模式代码如何驱动 I/O 设备是有用的。本书提供的测试代码的例子基于 Windows 的控制台子系统模型。要查阅这一主题的内容，请读者参阅“Win32 Programmers Reference”，尤其要参考关于 I/O 原语(CreateFile, ReadFile, WriteFile 和 DeviceIoControl)的内容。

最后一点，虽然不要求读者具备硬件或者设备驱动程序软件设计的经验；但是，如果读者具备某些低级设备接口方面的经验，对于阅读本书会有所帮助。例如，如果读者具备编写Unix系统设备驱动程序的知识，将有助于阅读本书。

本书内容

本书的重点在于首先解释硬件的体系结构、环境和设备驱动程序，然后详细说明如何编写代码。

本书中的各章节组织如下：

第 1 ~ 5 章：本书的前五章讨论编写设备驱动程序所需的基础知识。这些基础知识包括 Windows 2000 体系结构的范围、硬件术语和总线基础知识，以及详细探讨 Windows 2000 I/O 管理程序和相关的内容。

第 6 ~ 13 章：接下去的八章构成本书的核心内容。这几章内容几乎涉及了 Windows 2000 驱动程序开发的所有内容，包括从建立驱动程序的机制，到驱动程序特定设备的测试及记录错误和

其他事件。

第 14～15 章：这两章内容讨论设备驱动程序构造方面的更高级主题，包括使用系统线程、分层、过滤，以及使用驱动程序类别。

第 16～17 章：最后两章讨论驱动程序安装和调试所需的实践性内容。讨论了使用 Windows 2000 INF 文件进行即插即用设备的自动安装（以及遗留设备的手动安装）。详细讨论了 WinDbg 的使用，使得程序员能够进行真正的交互式调试。

附录：附录讨论驱动程序开发所需的参考信息，并列出了 Windows 2000 符号文件安装、故障检验（bugcheck）码等内容。

本书没有包含的内容

由于本书旨在讲述驱动程序“自下而上”的开发过程，因此一些特定的主题不在本书的讨论范围之内。不在本书讨论范围内的主题如下：

文件系统驱动程序：当前，构造一个完整的 Windows 2000 可安装的文件系统要求有 Microsoft IFS 设备。对于将要使用 IFS 设备的用户，本书将会为他们提供有益的帮助，因为本书涉及的内容是使用 IFS 设备所必需的前提知识。

特定设备的驱动程序信息：构造 NIC（Network Interface Card）、SCSI、视频（包括捕捉设备）、打印机和多媒体驱动程序，没有在本书中进行明确讨论。第 1 章内容讨论了这类驱动程序的结构内涵；但是，即使是专门讲述这些主题的章节，内容也是很不完整的。

虚拟 DOS 设备驱动程序：当前驱动程序的开发趋向于 32 位的 WDM 模型。遗留的 16 位 VDD 模型将不再流行。

关于示例代码

本书中大多数章节包括一个或多个示例驱动程序。所有代码均包括在本书所带的光盘中。每个章节的例子分别位于光盘上的不同子目录中，因此可以直接安装各个工程。

该光盘还包括 Microsoft Visual C++ 版本 6 的设备驱动程序应用向导。该向导配置编译环境，使得可以在 Visual Studio 中编写、编译和连接代码。

平台依赖：本书包括的示例代码只针对 Intel 平台，并且只在 Intel 平台上测试通过。因为最新的非 Intel 平台（Alpha）似乎不在 Windows 2000 的最新发行版本中，所以这样安排并不应该让读者感到吃惊。然而，我们必须知道，Windows 2000 本质上是一个独立于平台的操作系统，可以直接将 Windows 2000 操作系统移植到许多现代硬件设备上。编写设备驱动程序的人员应当利用 Windows 2000 的抽象设计，即允许编写的源码与非 Intel 平台兼容。

编译和运行例子：除了 Microsoft DDK（Device Driver Kit，设备驱动程序开发工具包）以外（该软件包可从 MSDN 订阅得到，当前也可以从微软的站点 www.microsoft.com/DDK 中免费下载），示例代码要求系统安装了 Microsoft Visual C++。设备驱动程序应用向导是在 *Visual Studio* 版本 6 上建立的。显然，稍加修改，这些示例代码也可以用其他软件商提供的编译器进行编译。

当然,示例代码要求已经安装了 Windows 2000 的各种版本(包括 Professional、Server 或者 Enterprise)。为了使用 WinDbg 进行交互式调试,还要求另一个主机平台。

本书历史演变

本书的第 1 版由 Art Baker 编写,书名为"Windows NT Device Driver Book"。对于将要编写 Windows NT 驱动程序的人来讲,无论如何也要阅读一下此书。Microsoft 驱动程序模型是一个不断发生变化的目标,近来推出的关于这一主题的书籍,提供了详细而最新的信息。该书修订版(第 2 版)的目标是,在用微软提供的最新信息更新本书内容的同时,推进 Art 原著的目标、风格和清晰的思路。

如果读者以前阅读过本书的原始著作,我希望你会发现这一版本同样也很有价值。我尽全力提供关于 Windows 2000 设备驱动程序这一主题的正确、简明而清晰的信息。虽然大量地依赖于 Art 的原始著作,但是本书中出现的任何过错都是由我个人造成的。

培训和咨询服务

本书的材料来源于业界不同公司所进行的培训和咨询内容。

本书的主要材料由 UCI 独家提供,以 5 天一次的讲座/实验课形式出现。这一课程的内容作为公共资料出现,或者可以从网站教室中得到。UCI 在高级编程、网站开发和管理、数据库和系统技术等方面提供全面培训。

有关这些服务的详细信息,请用下面提供的信息访问 www.ucitraining.com 网站:

UCI Corporation

,4 Constitution Way

Suite G

Woburn, MA 01801

1 - 800 - 884 - 1772

修订版的作者,Jerry Lozano 提供了关于设备驱动程序主题和相关主题的学习班和专题研讨会。有关的详细信息,请访问 www.StarJourney.com 网站。

目　录

第1章 Windows 2000驱动程序概述

本章内容：

- 总的系统体系结构
- 内核模式I/O组件
- 专用的驱动程序体系结构
- 小结

在任何操作系统上，设备驱动程序都必须与基本的系统代码进行和谐的相互作用，这一和谐的相互作用对于Windows 2000尤其重要。在介绍Windows 2000设备驱动程序的有关内容之前，本章先介绍Windows 2000的设计原理和总的体系结构。

1.1 总的系统体系结构

在计算机历史上，Windows 2000在操作系统控制方面进行了最具挑衅性的尝试。这一节概述Windows 2000的体系结构，着重讲解对于编写设备驱动程序人员极其重要的特征。

1.1.1 Windows 2000的设计目标

Microsoft的NT(New Technology，新技术)操作系统形成于1989年初。有趣的是，NT的最初概念甚至没有涉及一个Windows操作环境。然而，NT操作系统自1989年以来确实经历了一个漫长的发展过程，但是，如下所述的五个基本目标保持不变。

- 兼容性。操作系统应尽量支持已经存在的软件和硬件。
- 健壮性和可靠性。操作系统应经得起有意或无意的错误操作。用户的应用程序不应当使操作系统崩溃。
- 可移植性。操作系统应尽量能够在现有的和未来的平台上运行。
- 可扩展性。因为市场需求随时间而变化，操作系统应易于增加新功能和支持新的硬件，并且对已有代码的影响达到最小。
- 性能。操作系统应当为宿主的硬件平台的给定能力提供良好的性能。

当然，目标不是现实，并且随着时间的推移，一个目标的严重折衷使得有必要实现另一个目标。NT是一个操作系统，既然如此，它也有影响所有系统的同类的折衷问题。本节接下去的内容描述关于这一折衷的巧妙的平衡方案，Microsoft操作系统设计者通过这一平衡方案来实现他们的目标。

1.1.2 Windows 2000中的硬件特权层

为了实现健壮性和可靠性目标，NT的设计者为它的核心实现部分选择了客户－服务器体

系结构。用户应用程序作为 OS 服务器的一个客户在操作系统上运行。

用户应用程序以一种特殊的硬件模式进行运行,通常称为用户模式。在这个模式中,代码局限于无害操作。例如,通过虚拟内存映射的方法,代码不能触及其他应用程序的内存(除非与另一个应用程序互相协作)。硬件 I/O 指令不能被执行。确实,整个 CPU 指令级(指定为 privileged 特权)不能被执行,诸如 CPU Halt 等。如果应用程序要求使用这些被禁止执行的操作中的任何一个,应用程序必须向操作系统进行请求。一种由硬件提供的陷阱机制用来处理这些请求。

操作系统代码以一种称为内核模式的硬件模式进行运行。内核模式代码可以执行任何有效的 CPU 指令,尤其包括 I/O 操作。任何应用程序的内存都暴露给内核模式代码,当然,假设应用程序内存没有溢出到磁盘。

当前的所有处理器都执行各种形式的特权与非特权模式。内核模式在特权环境中执行,而用户模式在非特权环境中执行。因为不同的处理器和不同平台对于执行特权模式是不同的,加上为了帮助实现可移植性的目标,OS 设计者为用户和内核模式提供了一个抽象概念。OS 代码总是使用抽象概念来执行特权环境切换,因而只有抽象代码自身需要被移植到一个新的平台上。在一个 Intel 平台上,使用指令集中的 Ring 3 执行用户模式,而使用 Ring 0 执行内核模式。

这一讨论对于编写设备驱动程序的人员来说是有用的,因为内核模式在一个特权环境中执行。因此,编写拙劣的设备驱动程序代码确实能够损害 Windows 2000 操作系统的整体性能。驱动程序作者必须充分注意所有边界条件,保证代码不至于影响整个操作系统的性能。

1.1.3 可移植性

为了实现可移植性的目标,NT 设计者选用了为软件分层的体系结构,如图 1-1 所示。

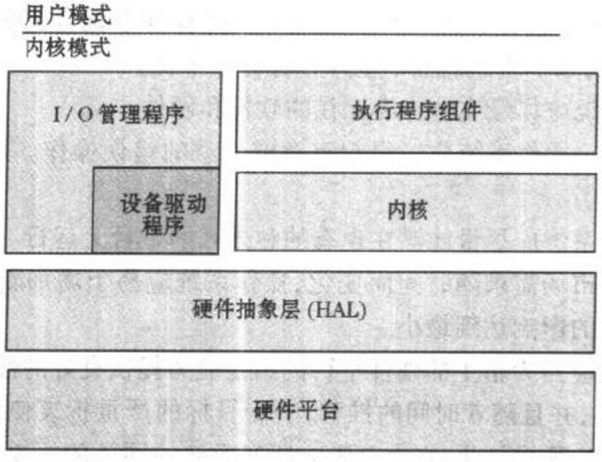


图 1-1 Windows 2000 操作系统的分层

硬件抽象层(HAL)将处理器和平台依赖与 OS 和设备驱动程序代码分开。通常,在设备驱动程序代码被移植到一个新的平台上时,只要进行重新编译即可。既然设备驱动程序代码本质上是设备、处理器和平台特有的,这一移植过程又是如何进行的呢?显然,设备驱动程序代码必