原创经典，威盛一线工程师倾力打造

深入驱动核心，剖析操作系统底层运行机制

通过实例引导，快速学习编译、安装、调试的方法

Broadview
www.broadview.com.cn

Windows 驱动开发技术详解

Windows Driver Development Internals

珍藏版

张 帆 史彩成 等编著

◎ 从Windows最基本的两类驱动程序的编译、安装、调试入手讲解，非常容易上手

◎ 用实例详细讲解PCI、USB、虚拟串口、虚拟摄像头、SDIO等驱动程序的开发

◎ 归纳了多种调试驱动程序的高级技巧，如用WinDbg和VMWare软件对驱动进行源码级调试

◎ 介绍了多种实用的工具软件，如BusHound、IRPTrace、DebugView等

◎ 深入Windows操作系统的底层和内核，透析Windows驱动开发的本质

CD-ROM

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

Windows
驱动开发技术详解
Windows Driver Development Internals

张 帆 史彩成 等编著

電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

内 容 简 介

本书由浅入深、循序渐进地介绍了 Windows 驱动程序的开发方法与调试技巧。本书共分 23 章，内容涵盖了 Windows 操作系统的基本原理、NT 驱动程序与 WDM 驱动程序的构造、驱动程序中的同步异步处理方法、驱动程序中即插即用功能、驱动程序的各种调试技巧等。同时，还针对流行的 PCI 驱动程序、USB 驱动程序、虚拟串口驱动程序、摄像头驱动程序、SDIO 驱动程序进行了详细的介绍，本书最大的特色在于每一节的例子都是经过精挑细选的，具有很强的针对性。力求让读者通过亲自动手实验，掌握各类 Windows 驱动程序的开发技巧，学习尽可能多的 Windows 底层知识。

本书适用于中、高级系统程序员，同时也可用做高校计算机专业操作系统实验课的补充教材。

图书在版编目（CIP）数据

Windows 驱动开发技术详解 / 张帆等编著. —北京：电子工业出版社，2008.7
ISBN 978-7-121-06846-1

I. W… II. 张… III. 窗口软件，Windows－驱动程序－程序设计 IV. TP316.7

中国版本图书馆 CIP 数据核字（2008）第 080993 号

责任编辑：高洪霞
印　　刷：北京智力达印刷有限公司
装　　订：北京中新伟业印刷有限公司
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：787×1092　1/16　印张：34.75　字数：851 千字
印　　次：2008 年 7 月第 1 次印刷
印　　数：5000 册　定价：65.00 元（含光盘 1 张）

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。

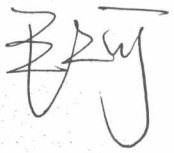
服务热线：（010）88258888。

院士推荐

目前，电子系统设计广泛采用通用操作系统，达到降低系统的设计难度和缩短研发周期。实现操作系统与硬件快速信息交换是电子系统设计的关键。

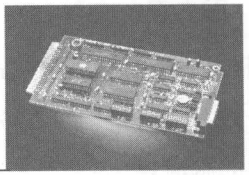
通用操作系统硬件驱动程序的开发，编写者不仅需要精通硬件设备、计算机总线，而且需要 Windows 操作系统知识以及调试技巧。学习和掌握 Windows 硬件驱动程序的开发是电子系统设计人员必备的能力。

本书是作者结合教学和科研实践经验编写而成的，不仅详细介绍了 Windows 内核原理，并且介绍了编程技巧和应用实例，兼顾了在校研究生和工程技术人员的实际需求，对教学、生产和科研有现实的指导意义，是一本值得推荐的专著。

中国工程院院士 

2008 年 5 月

自　序



写这本书，是为了圆自己一个梦！

1．你有这样的困惑吗？

你在学习 Windows 驱动程序开发的时候，有没有这样的感觉：觉得入门太难了；总有一大堆莫名其妙的术语，如“中断请求级别”、“派遣函数”、“线程上下文”、“完成例程”等；总能碰到很多诸如 PCI 总线、USB 总线等内容；还有那些无休止的死机、蓝屏等错误……

这可能让你感到很困惑。但这很正常，因为 Windows 驱动开发涉及 Windows 操作系统底层的很多知识，而且很多概念非常抽象，不容易理解。这对于入门人员，甚至有一定基础的开发者都有一定的困难。我也曾经有过和你们一样的经历，当然除了困惑之外，还有解决困惑之后的喜悦。

2．我的经历

当我第一次接触 Windows 驱动开发时，就觉得非常吃力。那是在研究生一年级的时候，实验室在开发一个 PCI 总线视频采集卡，需要编写驱动程序来读取 PCI 卡上的数据。由于不熟悉 Windows 驱动程序，编译、安装等很简单的问题都困惑我很长时间。通过长时间的摸索，当我第一次用自己编写的驱动程序采集到 PCI 卡上的数据时，我感到非常兴奋。虽然几秒钟后，Windows 无情地蓝屏重启了，但我依然感觉很有成就感。那时候最喜欢做的事情，就是叫周围的同学“欣赏”设备管理器中我编写的设备。又经过很长时间，我才最终将蓝屏死机的原因找出，让驱动程序稳定地运行。

后来，我又开发了很多驱动程序，有 PCI 驱动、USB 驱动、摄像头驱动、SDIO 驱动。渐渐地，我发现驱动程序开发并没有想象中的那么困难。只要对驱动程序开发“入门”后，它就不再是一个神秘的事情了。

我还编写过一些 Linux 驱动程序，结果发现 Linux 设备驱动程序和 Windows 设备驱动程序有很多类似的地方。相比而言，Linux 驱动模型比较简单，加之 Linux 内核的源码是开放的，所以很多地方可以对照 Linux 内核源码进行学习。而 Windows 驱动程序模型比较复杂，其内核也没有提供源码，所以 Windows 驱动程序的编写相对困难一些。

3. 圆自己一个梦

回想当初自己学习 Windows 驱动开发的情景，感想颇多。各种各样的困难，完成一个驱动开发后的喜悦，为了找一本好的学习资料几乎翻遍了图书馆……这些至今都还深深地印在我的脑海里。

随着开发经验的积累和技术水平的提升，越来越想写本 Windows 驱动开发的书，以便向更多的人介绍 Windows 驱动程序的开发经验，使那些初学者快速入门，少走弯路，也能让已经有一定基础的人有所借鉴。这也算是圆我自己的一个梦吧。

当我把这个计划告诉我的老师史彩成时，他非常支持我，而且也愿意和我一起来完成这本书的写作。经过一年多的努力，我们终于完成了这个“大工程”，心中也自然非常喜悦。这无论是对我们，还是对渴望学习 Windows 驱动开发的人，都算是有了一个“交代”。

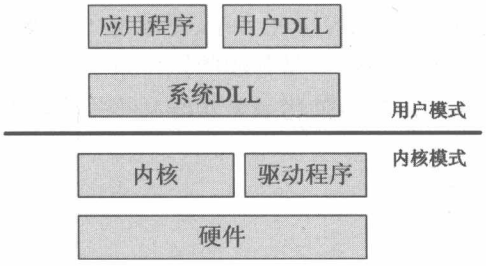
但愿这本书能够成为想致力于 Windows 驱动开发人员的良师益友，让你有所获益。我也相信，当你读完本书后应该已经能够编写大部分的 Windows 设备驱动程序了。

张　帆

前　言

PREFACE

你是否想知道 USB 移动硬盘插入 PC 后，Windows 是如何识别的？
你是否想知道 Windows 是如何得到显卡中的数据的？
你是否想知道什么导致了系统蓝屏死机？
你是否被老板或者导师逼着写一个 PCI、USB 等驱动程序，正感到无从下手？
你是否对 Windows 内核怀着强烈的好奇心？
如果你的回答为“是”，那么阅读本书将是最佳的选择！



上图是 Windows 操作系统的一个示意图。一般的 Windows 程序员都是编写应用程序或者用户 DLL，而不会对 Windows 底层有更深入的了解。而驱动程序位于操作系统的底层，它和内核紧密联系。另外，驱动程序直接操作硬件设备，但究竟如何操作，大部分程序员都不能清楚地讲出来。这些都使得驱动程序开发变得很神秘，仿佛都应该是编程高手的事情。

对于驱动程序开发，书店里很少能见到这方面的书籍。笔者在学习的时候尝到了各种苦头。为了帮助大家快速掌握驱动程序开发，笔者萌生了写一本书的想法。

本书的特点

1．快速上手：为了让读者快速上手，笔者先给出两个驱动程序的例子。这两个例子分别代表 Windows 两类最基本的驱动程序，NT 式驱动程序和 WDM 式驱动程序。笔者非常详细地介绍了驱动程序编译、安装、调试的方法。编译驱动程序一般使用 build 工具，但是考虑到很多读者都是 VC 程序员，笔者特意介绍了如何用 VC 编译器编译驱动程序。

2．内容翔实，实例丰富：本书详细地介绍了 PCI 驱动程序、USB 驱动程序、虚拟串口程序、虚拟摄像头程序、SDIO 驱动程序的开发，并辅以大量实例，使读者可以边学技术，边进行实践。

3．介绍多种调试技巧：驱动程序由于运行在内核模式下，很难像普通应用程序那样可以方便地调试。尤其对于 VC 程序员来说，以前的那些调试技巧，很多都不能用了。另外，莫名其妙的“蓝屏死机”也会成为驱动程序开发人员的梦魇。笔者结合自己开发驱动

程序多年的经验，归纳了多种调试驱动程序的高级技巧。这些包括用 WinDbg 和 VMWare 软件对驱动进行源码级调试、用 WinDbg 调试蓝屏后的 Dump 文件等。

4．灵活地使用一些工具：工欲善其事，必先利其器。很多工具软件会帮助我们更好地了解驱动程序内部的运行情况。本书将介绍很多实用的工具软件，如调试 USB 驱动程序的 BusHound 软件、查看 IRP 的 IRPTrace 软件、查看调试信息的 DebugView 软件、加载 NT 式驱动的 DriverMoniter 软件、加载 WDM 式驱动的 EzDriverInstaller 及查看设备对象的 DeviceTree 工具等。

5．分析本质：本书对驱动程序的讨论不是仅停留在“表面”，更多地方是带领读者深入到操作系统的底层。本书对驱动程序涉及的操作系统中各个组件都有深入的介绍。另外，本书详细地介绍了驱动程序中的同步处理和异步处理。正确处理同步与异步，会使驱动程序更稳定，运行效率更高。

6．探讨 Windows 内核：驱动程序和 Windows 的内核紧密相连。本书讲述了很多 Windows 内核的原理。由于 Windows 不是开源的操作系统，所以很少有书籍涉及 Windows 内核的原理。深入理解 Windows 内核的构造与原理，将更好地帮助程序员写出稳定的驱动程序。

本书的内容

本书由 23 章组成，内容分布如下：

入门篇	编译、安装方法（1）	介绍 NT 式、WDM 式驱动程序的编译、安装方法
	驱动程序开发的基本方法（2~7）	介绍驱动程序的基本概念、基本数据结构。介绍驱动程序中经常用到的内核函数。介绍驱动程序的入口函数、卸载函数、IRP 处理函数等
进阶篇	同步和异步处理（8~9）	介绍驱动程序内部对同步操作请求和异步操作请求的处理。介绍如何编写同步和异步的 IRP 处理函数
	定时器（10）	介绍两种内核模式下的定时器使用方法，另外还介绍了 4 种在内核模式下等待的方法
	驱动程序之间的调用（11~12）	介绍驱动程序之间的调用方法
	即插即用和电源管理（13~14）	介绍驱动程序中即插即用和电源管理功能。这些都是 WDM 驱动程序的重点内容
实用篇	各类硬件设备或者模拟设备的驱动程序（15~20）	介绍几类硬件设备或者模拟设备的驱动程序。包括 USB 设备驱动、PCI 设备驱动、虚拟串口驱动、虚拟摄像头驱动、SDIO 设备驱动等。
提高篇	再论 IRP（21）	讨论一些高级的 IRP 处理方法
	过滤驱动程序（22）	介绍如何编写过滤驱动程序
	高级调试技巧（23）	介绍一些高级的驱动程序调试技巧

目 录 Contents

第 1 篇 入门篇

第 1 章 从两个最简单的驱动谈起 2

本章向读者呈现两个最简单的 Windows 驱动程序，一个是 NT 式的驱动程序，另一个是 WDM 式的驱动程序。这两个驱动程序没有操作具体的硬件设备，只是在系统里创建了虚拟设备。在随后的章节中，它们会作为基本驱动程序框架，被本书其他章节的驱动程序开发所复用。笔者将带领读者编写代码、编译、安装和调试程序。