第一图书网, tushu007.com

<<Windows内核情景分析>>

图书基本信息

书名：<<Windows内核情景分析>>

13位ISBN编号：9787121081149

10位ISBN编号：7121081148

出版时间：2009年5月

出版时间：电子工业出版社

作者：毛德操

页数：1465

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

前言

多年来，Windows垄断了中国桌面操作系统，中国学校中也开设了很多Windows课程，但令人遗憾的是，由于Windows的源代码不开放，这些课程往往只能使学生了解Windows的外特性和操作方法，却不能使学生了解和掌握Windows的内核。
有人会问：难道中国人真的需要深入到操作系统的内核，去掌握它的核心技术吗？
有人说：微软花了上千亿美元开发出Windows操作系统，中国人花1000元人民币就能买到，为什么还要自己去研究和开发呢？
一些外国咨询公司也为中国政府支招，如麦肯锡公司在2002年所做的《中国软件产业发展战略研究报告》就主张中国不必发展操作系统，而应像印度那样，主要发展面向出口的离岸外包业务。
这样的观点前些年在中国相当流行，影响了不少人。
2008年10月，有一个事件震惊了中国：微软宣称将对其认为是使用盗版Windows和Office的电脑实行了“黑屏”。
用户面对“黑屏”束手无策，这才意识到，自己的电脑被微软操控了！
中国信息安全的软肋由此暴露无遗。
事实上，在信息安全方面我国历来要求使用“自主可控”的软件和硬件，“黑屏”事件更使广大用户有了切肤之痛，认识到自主可控的重要性。
现在，世界上许多国家也有了这种共识，如俄国、欧洲和拉丁美洲的一些国家都在发展基于开源软件Linux的自主操作系统。
在这方面，目前中国的重大进展是起动了“核高基”重大专项，这是按照《国家中长期科学和技术发展规划纲要（2006－2020年）》所部署的，旨在发展“核心电子器件、高端通用芯片及基础软件产品”。
其中的“基础软件产品”中最重要的就是操作系统。
这样，持续多年的中国要不要发展自主操作系统的争议终于有了定论。
通过“核高基”专项，中国有望在今后三个五年计划内实现自主操作系统的产业化，将来中国的信息系统再不会被人“黑屏”了。

内容概要

本书通过分析ReactOS的源代码介绍了Windows内核各个方面的结构、功能、算法与具体实现。
全书从“内存管理”、“进程”、“进程间通信”、“设备驱动”等多个方面进行分析介绍，所有的分析都有ReactOS的源代码（以及部分由微软公开的源代码）作为依据，使读者能深入理解Windows内核的方方面面，也可以使读者的软件开发能力和水平得到提高。

本书可供大学有关专业的高年级学生和研究生用做教学参考，也可供广大的软件工程师，特别是从事系统软件研发的工程师用于工作参考或用做进修教材。

书籍目录

上册 第1章 概述 1.1 Windows操作系统发展简史 1.2 用户空间和系统空间 1.3 Windows内核 1.4 开源项目ReactOS及其代码 1.5 Windows内核函数的命名 第2章 系统调用 2.1 内核与系统调用 2.2 系统调用的内核入口KiSystemService() 2.3 系统调用的函数跳转 2.4 系统调用的返回 2.5 快速系统调用 2.6 从内核中发起系统调用 第3章 内存管理 3.1 内存区间的动态分配 3.2 页面异常 3.3 页面的换出 3.4 共享映射区（Section） 3.5 系统空间的缓冲区管理 第4章 对象管理 4.1 对象与对象目录 4.2 对象类型 4.3 句柄和句柄表 4.4 对象的创建 4.5 几个常用的内核函数 4.6 对象的访问控制 4.7 句柄的遗传和继承 4.8 系统调用NtDuplicateObject() 4.9 系统调用NtClose() 第5章 进程与线程 5.1 概述 5.2 Windows进程的用户空间 5.3 系统调用NtCreateProcess() 5.4 系统调用NtCreateThread() 5.5 Windows的可执行程序映像 5.6 Windows的进程创建和映像装入 5.7 Windows DLL的装入和连接 5.8 Windows的APC机制 5.9 Windows线程的调度和切换 5.10 线程和进程的优先级 5.11 线程本地存储TLS 5.12 进程挂靠 5.13 Windows的跨进程操作 5.14 Windows线程间的相互作用 第6章 进程间通信 6.1 概述 6.2 共享内存区（Section） 6.3 线程的等待/唤醒机制 6.4 信号量（Semaphore） 6.5 互斥门（Mutant） 6.6 事件（Event） 6.7 命名管道（Named Pipe）和信插（Mailslot） 6.8 本地过程调用（LPC） 6.9 视窗报文（Message） 第7章 视窗报文 7.1 视窗线程与Win32k扩充系统调用 7.2 视窗报文的接收 7.3 Win32k的用户空间回调机制 7.4 用户空间的外挂函数 7.5 视窗报文的发送 7.6 键盘输入线程 7.7 鼠标器输入线程 7.8 默认的报文处理 第8章 结构化异常处理 8.1 结构化异常处理的程序框架 8.2 系统空间的结构化异常处理 8.3 用户空间的结构化异常处理 8.4 软异常 下册 第9章 设备驱动 第10章 网络操作 第11章 文件操作 第12章 操作系统的安全性 第13章 注册表 第14章 系统管理进程与服务进程 跋 参考文献

章节摘录

插图：上册第2章系统调用2.1内核与系统调用对于应用程序的运行即应用进程而言，操作系统内核的作用体现在一组可以供其调用的函数，称为“系统调用（System Call）”，正是这些系统调用加上一些辅助的手段构成了应用软件的运行环境，即日常所说的“运行平台”。
从应用软件的角度看，这些系统调用都是操作系统为其提供的服务，所以也称“系统服务（System Service）”。
在本书中，“系统调用”与“系统服务”是可以互换的同义词。
从程序运行的角度看，进程是主动的、“活性（Active）”的，是发出调用请求的一方；而内核是被动（Passive）的，只是应进程的要求而提供服务。
但是，从整个系统的角度看，则内核也有活性的一面，诸多应用进程就是在内核的调度下运行，所以内核有其两面性。
离开进程调度，内核就只剩下了被动的一面，那就类似于一个运行时程序库了。
而系统调用即系统服务，就体现了内核被动的一面。
内核活性的一面即进程调度，对于应用程序而言是无形的，其目的就在于为应用软件创造一种似乎独占着CPU的假象；相比之下内核被动的一面即系统调用则是有形的，要不然应用程序就无法调用这些服务。
系统调用所提供的服务是在内核中，一般是在“系统空间”实现的，而应用软件则都在用户空间运行，二者之间有着空间的间隔，实质上是CPU运行模式的不同。
所以，在应用软件与内核之间必定存在着一个明确定义的“系统调用界面”。
不过要由应用软件直接按规定的形式进行系统调用是不方便的，所以一般都要在外面包上一层，提供一套便于调用的（用户空间）库函数作为中介。
在UNIX/Linux系统及后来的POSIX标准中，这就是c语言运行库的一部分。
就调用的参数、返回值、作用而言，由标准C语言运行库提供的“系统调用”函数与实际的系统调用一一对应并基本相同。
例如，read（）是个系统调用，而用户程序引用的read（）实际上是库函数，二者是对应的，并且参数的数量、类型、次序等基本相同，功能则完全相同。
标准C语言运行库也提供一些建立在系统调用基础上功能有所扩充的高层库函数，例如fread0是建立在read（）基础上的，但是用起来更加方便，可是那就不叫系统调用。

编辑推荐

名人推荐

操作系统是最基础、最核心的计算机软件。
长期处于技术垄断地位的Windows操作系统，其源程序代码是不公开的，可看成一个“黑盒子”。
毛德操先生这本书，通过分析ReactOS的源程序代码，介绍了Windows操作系统内核的结构及其各种机制，使读者能深入理解Windows操作系统内核这个“黑盒子”的各个方面，这对于打破Windows的技术垄断，开发具有自主知识产权的新型操作系统，实现Windows与Linux操作系统的高度互操作，具有重大的实际价值。
毛德操先生在剖析Windows、Linux等操作系统内核的结构与机制方面，走在了国际学术界的前列。
——中国开源软件推进联盟主席 陆首群　　虽然当前以Linux为代表的开源软件为中国发展自主操作系统提供了很好的支撑，但学习和借鉴Windows也有重要价值。
在这个时候，毛德操先生所著的《Windows 内核情景分析》出版了，它为广大读者打开了通向Windows内核的大门。
与其说本书是一部单纯的学术著作，不如说这更是一篇实践经验的总结。
本书正是毛德操先生近年来领导开发“兼容内核（Unified Kernel）”项目的一篇经验总结。
早在2004年毛先生就提出了开发“兼容内核”的倡议，他提出开发一个既能支持Linux应用软件运行、也能支持Windows应用软件运行的内核，这与开源项目Wine有异曲同工之妙。
——中国工程院院士 倪光南

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