

<<Delphi下深入Windows核心编程>>

图书基本信息

书名：<<Delphi下深入Windows核心编程>>

13位ISBN编号：9787505384026

10位ISBN编号：7505384023

出版时间：2003-1-1

出版时间：电子工业出版社

作者：王树伟,王蒙

页数：525

字数：857600

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>

<<Delphi下深入Windows核心编程>>

内容概要

本书是一本介绍Windows核心技术及高级技巧的专著。

从系统内核编程出发，使用大量的例子帮助读者理解这些编程技术，讲述了线程同步及隐藏、系统钩子深入分析、读写物理磁盘的关键技术、读写物理内存和其他进程内存的核心技术、Windows 9x下调用16位实模式和保护模式代码的核心技术、直接读写端口技术、可执行文件加壳的技巧、PE结构分析、Ring0的实现、Windows API截取技术、屏幕取词技术等方面的内容。

全书对热点源代码进行了深入剖析和讲解，同时本书汇聚了作者利用Soft-ICE跟踪调试经验，作者多年的编程心得和技巧一览无遗。

随书附送的光盘提供了书中涉及的程序源代码。

本书可对Windows核心编程感兴趣者提供帮助，亦可供广大编程人员及各大专院校师生参考。

书籍目录

| | | | | | | | | | |
|----------------------|-----|----------------------------|-----|---------------------------------|-----|------------------------------|-----|----------------------|-----|
| 第1章 DLL与数据共享 | 1 | 1.1 关于DLL | 1 | 1.1.1 DLL的结构 | 1 | 1.1.2 DLL数据作用范围 | 4 | 1.2 内存映像 | |
| 1.2.1 创建映像文件 | 5 | 1.2.2 打开映像文件 | 5 | 1.2.3 映射到本进程中 | 6 | 1.2.4 关闭内存映射 | 6 | 1.2.5 两个EXE文件共享内存数据块 | 8 |
| 1.2.6 两个DLL文件共享内存数据块 | 13 | 1.3 16位和32位进程间传送消息 | 17 | 1.3.1 全局原子实现数据共享 | 17 | 1.3.2 WM_COPYDATA消息实现进程间数据共享 | 20 | 第2章 钩子原理 | 23 |
| 2.1 钩子原理 | 23 | 2.1.1 挂钩函数 | 23 | 2.1.2 钩子链 | 24 | 2.1.3 脱钩 | 25 | 2.2 消息及DLL的注入 | 25 |
| 2.2.1 自消息截取 | 25 | 2.2.2 文件或串口读写监视钩子 | 27 | 2.3 Shell钩子 | 38 | 2.3.1 实现钩子 | 39 | 2.3.2 注册钩子 | |
| 2.3.3 实现步骤 | 41 | 2.3.4 完整代码 | 42 | 2.4 鼠标键盘钩子 | 45 | 第3章 系统内核 | 71 | 3.1 内核对象 | 71 |
| 3.2 进程隐藏深入剖析 | 99 | 3.4 线程 | 117 | 3.5 Windows NT/2000的性能数据库 | 134 | 第4章 低层操作 | 149 | 4.1 断 | 149 |
| 4.2 内嵌汇编 | 150 | 4.3 Ring0特权及端口直接IO | 156 | 4.4 端口读写驱动PortTalk | 162 | 4.5 Thunk机制 | | 第5章 磁盘读写 | 191 |
| 5.1 磁盘读写技术荟萃 | 191 | 5.2 枚举磁盘中已打开的文件列表 | 232 | 第6章 回收站和IE | 237 | 6.1 回收站 | 237 | 6.2 IE编程 | 255 |
| 第7章 高级应用 | 281 | 7.1 DDE | 281 | 7.2 密码相关程序 | 286 | 7.3 视 | 296 | 7.4 剪贴板监视 | 300 |
| 7.5 消息机制 | 302 | 7.6 模拟按键及鼠标双击 | 306 | 7.7 热键 | 311 | 7.8 程序运行 | | 7.9 只运行一个实例的两种方法 | 315 |
| 7.10 移动正在使用的文件 | 317 | 7.11 类型转换与存储转换 | 322 | 7.12 加壳原理 | 325 | 第8章 PE结构分析 | 341 | 8.1 PE文件结构 | 341 |
| 8.2 PEDump实例 | 355 | 第9章 内存管理 | 411 | 9.1 内存结构 | 411 | 9.2 内存堆列举 | 411 | 9.3 修改虚拟内存保护属性 | 416 |
| 9.4 读写其他进程内存的技巧 | 423 | 9.5 Windows 9x下读写物理内存的核心技术 | 429 | 9.6 Windows NT/2000下读写物理内存的核心技术 | 447 | 第10章 API Hook及屏幕取词 | 457 | 10.1 API Hook必读 | 457 |
| 10.2 屏幕取词 | 468 | 附录A Delphi编译指令说明 | 511 | A.1 使用编译设置对话框 | 511 | A.2 使用编译指令 | 512 | A.3 使用条件编译指令 | 513 |
| 附录B Delphi编译错误信息对照表 | 515 | | | | | | | | |

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>