

《Windows 内核设计思想》

图书基本信息

书名：《Windows 内核设计思想》

13位ISBN编号：9787121253143

出版时间：2015-3

作者：陈树宝

页数：636

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：www.tushu000.com

《Windows 内核设计思想》

内容概要

《Windows 内核设计思想》主要讲述Windows 内核的设计过程，从最底层的细节使用源码一步一步分析，结合Bochs 和WinDbg 调试器进行验证。《Windows 内核设计思想》提供全部源代码和能直接编译的项目工程，集理论、架构、编码、运行和调试于一体进行讲述，从多种角度呈现内核构架的基本流程。《Windows 内核设计思想》主要包括了Windows 内核加载器（ntldr）的分析，Windows 内核调试组件的设计，实现结构化异常处理的支持，并对内存管理和对象管理进行了精心讲解，同时对基于IRP 请求包的I/O 系统进行了论述，并且介绍了如何设计文件系统，最后简单讲解了进程和线程的一些基本知识。

《Windows 内核设计思想》适合希望深入了解Windows 内核框架的程序员及对此感兴趣的读者阅读。

书籍目录

推荐序 1

推荐序 2

序言

前言

第 1 章 搭建开发和调试环境

1.1 编译环境

1.2 使用 Bochs 运行 ntos.img

1.3 使用 VMware 运行 ntos.vmdk

1.4 模拟调试运行

1.5 编程思想（等差数列求和）

1.6 函数调用约定

1.7 模块扩展约定

1.8 本章总结

第 2 章 Windows 内核加载器（SU）

2.1 主引导记录（MBR）

2.2 系统分区（Partition1）

2.3 SU 模块（startup.com）

2.3.1 原版 Windows Server 2003 系统 NTLDR startup.com 基本分析

2.3.2 根据原理重新构建新的 startup.com

2.4 检测物理内存

2.5 开启 A20 地址线

2.6 重新定位 GDT 和 IDT

2.7 保护模式

2.7.1 段描述符（Segment Descriptor）

2.7.2 特权级（privilege level）

2.7.3 段描述符表（segment descriptor table）

2.7.4 开启保护模式

2.8 加载 Loader 模块

2.9 转移控制权

2.10 导出函数

2.10.1 读写扇区

2.10.2 获取物理内存块

2.10.3 检测硬件

2.11 本章总结

第 3 章 Windows 内核调试设计

3.1 初始化调试系统

3.2 初始化模拟调试

3.3 初始化内核调试

3.3.1 中断和异常向量表

3.3.2 注册异常处理例程

3.3.3 基于栈框架的异常处理程序

3.3.4 除零错误（#DE）

3.3.5 单步异常（#DB）

3.3.6 断点异常（#BP）

3.3.7 一般保护性错误（#GP）

3.3.8 页面错误（#PF）

3.3.9 调试器服务（debugger service）

- 3.4 分发异常
- 3.5 内核调试分发
 - 3.5.1 打印字符串
 - 3.5.2 加载/卸载符号
 - 3.5.3 报告异常
- 3.6 内核调试引擎核心
 - 3.6.1 获取系统版本
 - 3.6.2 获取/设置机器信息
 - 3.6.3 读/写虚拟内存
 - 3.6.4 设置/恢复断点
- 3.7 调试通信协议
 - 3.7.1 串行端口
 - 3.7.2 COM 寄存器
 - 3.7.3 波特率
 - 3.7.4 端口初始化
 - 3.7.5 通信协议
 - 3.7.6 读端口
 - 3.7.7 写端口
 - 3.7.8 调试包
 - 3.7.9 接收调试包 (KdReceivePacket)
 - 3.7.10 发送调试包 (KdSendPacket)
- 3.8 本章总结
- 第 4 章 Windows 内核加载器 (Loader)
 - 4.1 NtProcessStartup
 - 4.2 PcMachInit
 - 4.3 初始化内存管理器
 - 4.3.1 内存描述符表
 - 4.3.2 页面查找表
 - 4.3.3 初始化堆
 - 4.4 分页机制
 - 4.4.1 页帧号 (PFN)
 - 4.4.2 页目录和页表
 - 4.4.3 开启分页机制
 - 4.4.4 虚拟地址转译物理地址
 - 4.4.5 修改页目录和页表位置
 - 4.5 Loader 读/写支持
 - 4.5.1 ARC 接口标准
 - 4.5.2 虚拟磁盘驱动 (RamDisk)
 - 4.5.3 磁盘驱动 (Hwdisk)
 - 4.5.4 文件系统驱动 (Ldfs)
 - 4.6 加载器参数块
 - 4.7 加载和启动内核
 - 4.7.1 收集硬件信息
 - 4.7.2 本地语言支持 (NLS)
 - 4.7.3 加载模块
 - 4.7.4 内存描述符链表
 - 4.7.5 处理器控制域 (PCR) 和任务状态段 (TSS)
 - 4.8 本章总结
- 第 5 章 结构化异常处理

- 5.1 异常触发
- 5.2 分发异常 (RtlDispatchException)
- 5.3 异常处理 (_except_handler3)
- 5.4 全局展开 (__global_unwind2)
- 5.5 局部展开 (__local_unwind2)
- 5.6 冒泡排序 (BubbleSort)
- 5.7 本章总结
- 第 6 章 内存管理
 - 6.1 物理内存管理概述
 - 6.2 虚拟地址空间布局
 - 6.3 初始化内存系统 (MmArmlnitSystem)
 - 6.4 初始化机器相关 (MiInitMachineDependent)
 - 6.5 初始化非分页池 (MiInitializeNonPagedPool)
 - 6.6 初始化系统 PTE (MiInitializeSystemPtes)
 - 6.7 映射页帧数据库 (MiMapPfnDatabase)
 - 6.8 初始化颜色表 (MiInitializeColorTables)
 - 6.9 初始化页帧号数据库 (MiInitializePfnDatabase)
 - 6.9.1 从页面建立页帧号数据库 (MiBuildPfnDatabaseFromPages)
 - 6.9.2 从加载块物理内存链表建立页帧号数据库 (MiBuildPfnDatabaseFromLoaderBlock)
 - 6.10 初始化池 (InitializePool)
 - 6.11 分配池页面 (MiAllocatePoolPages)
 - 6.11.1 非分页池分配
 - 6.11.2 分页池分配
 - 6.11.3 分页池页面错误处理
 - 6.12 释放池页 (MiFreePoolPages)
 - 6.12.1 释放分页池
 - 6.12.2 释放非分页池
 - 6.13 建立分页池 (MiBuildPagedPool)
 - 6.14 分配池内存 (ExAllocatePoolWithTag)
 - 6.15 释放池内存 (ExFreePoolWithTag)
 - 6.16 初始化系统空间映射 (MiInitializeSystemSpaceMap)
 - 6.17 本章总结
- 第 7 章 对象管理
 - 7.1 对象概述
 - 7.1.1 对象整体结构
 - 7.1.2 对象头 (object header)
 - 7.1.3 对象类型 (object type)
 - 7.1.4 对象类型例程模板 (object type procedure template)
 - 7.2 分配对象内存空间 (ObpAllocateObject)
 - 7.3 释放对象内存空间 (ObpDeallocateObject)
 - 7.4 初始化对象系统 (ObInitSystem)
 - 7.5 创建句柄表 (ExCreateHandleTable)
 - 7.6 创建对象类型 (ObCreateObjectType)
 - 7.7 创建目录对象 (NtCreateDirectoryObject)
 - 7.8 创建对象 (ObCreateObject)
 - 7.9 插入对象 (ObInsertObject)
 - 7.10 查找对象名 (ObpLookupObjectName)
 - 7.11 查找目录项 (ObpLookupEntryDirectory)

- 7.12 创建无名句柄 (ObpCreateUnnamedHandle)
- 7.13 分配句柄表项 (ExpAllocateHandleTableEntry)
- 7.14 解析符号链接 (ObpParseSymbolicLink)
- 7.15 Section 和 Segment
 - 7.15.1 Prototype PTE 页面异常处理
 - 7.15.2 Section 映射到系统进程
 - 7.15.3 VAD 页面错误处理
- 7.16 本章总结
- 第 8 章 I/O 系统
 - 8.1 初始化 I/O 系统 (IoInitSystem)
 - 8.2 创建驱动对象 (IoCreateDriver)
 - 8.3 创建设备对象 (IoCreateDevice)
 - 8.4 分配 I/O 请求包 (IoAllocateIrp)
 - 8.5 传递 I/O 请求包 (IoCallDriver)
 - 8.6 释放 I/O 请求包 (IoFreeIrp)
 - 8.7 解析设备 (IoParseDevice)
 - 8.8 磁盘读/写支持
 - 8.9 本章总结
- 第 9 章 文件系统设计
 - 9.1 文件系统初始化 (DriverEntry)
 - 9.2 挂载卷 (NtfsMountVolume)
 - 9.2.1 识别文件系统格式
 - 9.2.2 文件控制块 (FCB)
 - 9.2.3 上下文控制块 (CCB)
 - 9.2.4 创建流文件对象 (IoCreateStreamFileObject)
 - 9.2.5 初始化缓存映射 (CcInitializeCacheMap)
 - 9.3 打开文件 (NtfsOpenFile)
 - 9.4 读文件 (NtfsReadFile)
 - 9.5 关闭文件 (NtfsCloseFile)
 - 9.6 发起卷挂载请求
 - 9.7 加载 NTDLL
 - 9.7.1 打开 NTDLL
 - 9.7.2 检查 NTDLL 映像 (MmCheckSystemImage)
 - 9.7.3 创建 NTDLL Section
 - 9.7.4 映射 NTDLL Section 到当前进程空间
 - 9.7.5 获取用户进入点
 - 9.8 本章总结
- 第 10 章 进程和线程
 - 10.1 进程和线程初始化
 - 10.1.1 初始化进程
 - 10.1.2 初始化线程
 - 10.1.3 初始化线程上下文
 - 10.1.4 初始化进程系统 (PspInitPhase0)
 - 10.2 线程优先级 (priority)
 - 10.3 线程状态 (thread state)
 - 10.4 线程调度 (thread dispatch)
 - 10.5 分配进程虚拟内存 (NtAllocateVirtualMemory)
 - 10.6 创建用户进程 (smss.exe)
 - 10.7 本章总结

《Windows 内核设计思想》

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:www.tushu000.com