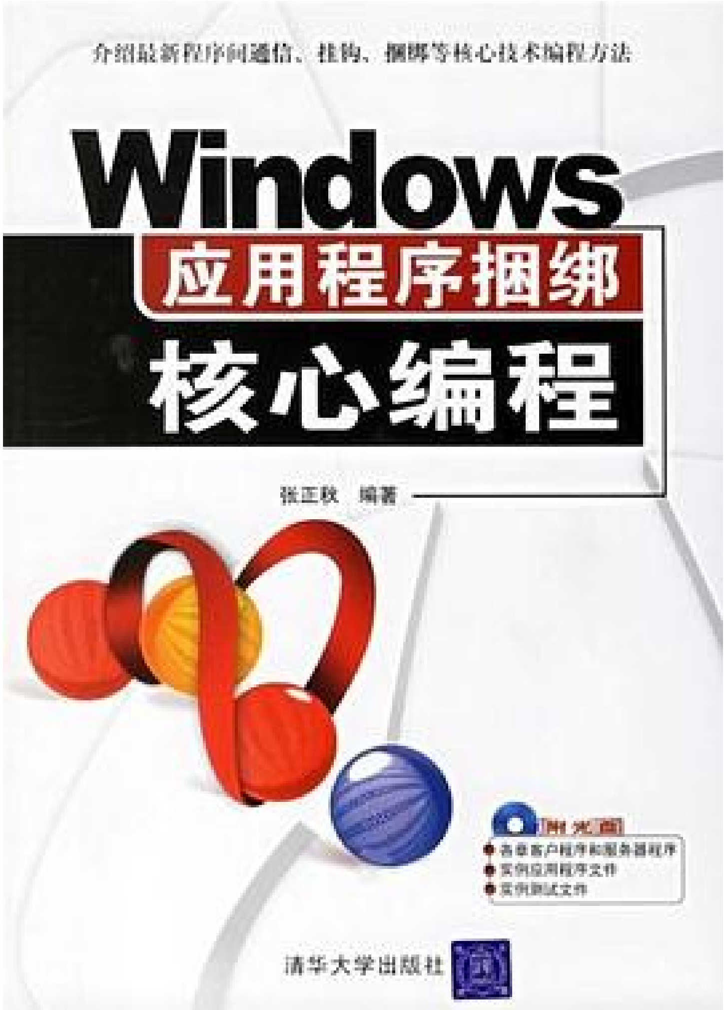
Windows应用程序捆绑核心编程



Windows应用程序捆绑核心编程_下载链接1_

著者:张正秋

出版者:清华大学出版社

出版时间:2006-12

装帧:

isbn:9787302140887

《Windows应用程序捆绑核心编程》所介绍的内容与计算机防护技术相关。《Windows

应用程序捆绑核心编程》基于作者在计算机编程方面的多年实践经验，对当今国际上最新的应用程序间的通信、挂钩、捆绑技术作了较为具体、系统的归纳和总结，并给出了大量的实例。《Windows应用程序捆绑核心编程》中很多的技术还没有公开，属于底层热门技术，所给出的很多程序代码可以直接用于商业软件的制作。

作者介绍:

张正秋
现在中国气象科学研究院工作，获北京大学物理学院理学博士学位，长期从事数值模式研究和计算机软件开发工作。对应用程序间的通信、挂钩和捆绑技术的编程有较丰富的实践经验。

目录: 第1章 再谈计算机内存访问 11.1 引言 11.2 内存管理概述 11.2.1 虚拟内存 11.2.2 CPU工作模式 21.2.3 逻辑、线性和物理地址 31.2.4 存储器分页管理机制 31.2.5 线性地址到物理地址的转换 41.3 虚拟内存访问 51.3.1 获取系统信息 51.3.2 在应用程序中使用虚拟内存 61.3.3 获取虚存状态 71.3.4 确定虚拟地址空间的状态 81.3.5 改变内存页面保护属性 91.3.6 进行一个进程的内存读写 101.4 文件的内存映射 111.4.1 内存映射API函数 111.4.2 用内存映射在多个应用程序之间共享数据 131.4.3 用内存映射文件读取大型文件 181.5 深入认识指针的真正含义 211.5.1 指针的真正本质 211.5.2 用指针进行应用程序之间的通信 221.6 本章小结 26参考文献 27第2章 再谈PE文件结构 282.1 引言 282.2 PE文件格式概述 282.2.1 PE文件结构布局 282.2.2 PE文件内存映射 302.2.3 Big-endian和Little-endian 312.2.4 3种不同的地址 312.3 PE文件结构 322.3.1 MS-DOS头部 322.3.2 IMAGE_NT_HEADER头部 332.3.3 IMAGE_SECTION_HEADER头部 362.4 如何获取PE文件中的OEP 362.4.1 通过文件读取OEP值 372.4.2 通过内存映射读取OEP值 382.4.3 读取OEP值方法的测试 392.5 PE文件中的资源 402.5.1 查找资源在文件中的起始位置 402.5.2 确定PE文件中的资源 412.6 一个修改PE可执行文件的完整实例 432.6.1 如何获得MessageBoxA代码 432.6.2 把MessageBoxA()代码写入PE文件的完整实例 452.7 本章小结 53参考文献 53第3章 进程之间通信概述及初级技术 543.1 引言 543.2 进程通信概述 553.2.1 Windows进程间标准通信技术的发展 553.2.2 应用程序与进程 563.2.3 进程之间通信的类型 563.3 使用自定义消息通信 573.3.1 通过自定义消息实现进程间通信的方法 573.3.2 通过自定义消息实现进程间通信的实例 583.4 使用WM_COPYDATA消息通信 603.4.1 通过WM_COPYDATA消息实现进程间通信的方法 603.4.2 通过WM_COPYDATA消息实现进程间通信的实例 613.5 使用内存读写函数和内存映射文件通信 623.5.1 使用内存映射文件通信的方法 623.5.2 使用内存读写函数实现进程间通信的方法 623.5.3 使用内存读写函数实现进程间通信的实例 633.6 使用动态链接库通信 643.6.1 DLL概述 643.6.2 使用DLL通信的方法 653.6.3 使用DLL通信的实例 663.7 使用Windows剪贴板通信 673.7.1 使用剪贴板实现进程间通信的方法 683.7.2 使用剪贴板实现进程间通信的实例 683.8 使用动态数据交换（DDE）通信 703.8.1 使用DDE技术通信原理 703.8.2 如何使用DDEML编写程序 713.8.3 使用DDE通信的实例 723.9 本章小结 77参考文献 77第4章 使用消息管道、邮槽和套接字通信 784.1 引言 784.2 如何用命名管道进行进程间通信 784.2.1 命名管道函数 794.2.2 命名管道服务端与客户端之间通信的实现流程 804.2.3 命名管道服务端与客户端之间通信的实例 814.3 如何用邮槽进行进程间通信 854.3.1 用邮槽进行进程间通信的步骤 854.3.2 邮槽服务器端与客户端之间通信的实例 864.4 如何用Windows套接字进行进程间通信 904.4.1 套接字分类 904.4.2 流式套接字编程流程 914.4.3 套接字调用基本函数 924.4.4 Winsock程序设计 954.4.5 一个通用套接字类 964.4.6 套接字服务器端与客户端间通信的实例 1014.5 本章小结 106参考文献 106第5章 使用LPC和RPC通信 1075.1 引言 1075.2 接口定义语言（IDL）简介 1075.3 使用本地过程调用（LPC）通信 1085.3.1 使用LPC通信方法介绍 1085.3.2

使用LPC通信的实例 1105.4 使用远程过程调用（RPC）通信 1175.4.1 RPC运行机制
1175.4.2 RPC 绑定模式和属性 1185.4.3 RPC传输（Transport） 1185.4.4
如何编写RPC应用程序 1195.4.5 使用RPC通信的实例 1205.5 本章小结 128参考文献
128第6章 使用组件模型通信 1296.1 引言 1296.2 COM/DCOM模型概述 1296.2.1
COM/DCOM的特点 1296.2.2 COM/DCOM组件模型分类 1306.3
使用组件对象模型（COM/DCOM）通信 1316.3.1 使用COM/DCOM通信方法介绍
1316.3.2 基于DCOM实现远程会话的实例 1366.4 本章小结 147参考文献 147第7章
进程的创建、控制和隐藏 1487.1 引言 1487.2 常见的几种创建进程的方法 1487.2.1
使用WinExec() 函数 1487.2.2 使用ShellExecute()和ShellExecuteEx()函数 1497.2.3
使用CreateProcess()函数 1517.2.4 使用OLE激活服务程序 1547.3 如何获得进程句柄
1557.3.1 获得一个进程的句柄 1557.3.2 提升进程权限级别 1567.4
如何实现当前进程的枚举 1587.4.1 通过系统快照实现当前进程的枚举 1587.4.2
通过psapi.dll提供的API函数实现当前进程的枚举 1607.4.3
通过wtsapi32.dll提供的API函数实现当前进程的枚举 1627.4.4
通过ntdll.dll提供的API函数实现当前进程的枚举 1637.5 如何终止进程 1647.5.1
如何终止本进程 1657.5.2 如何终止外部进程 1657.5.3 终止进程的实例 1657.6
如何隐藏进程（注入代码） 1667.6.1 基本原理 1667.6.2
使用CreateRemoteThread()隐藏DLL 1677.6.3
使用CreateRemoteThread()直接注入API函数代码 1737.6.4
使用Windows内存映射文件注入代码 1747.6.5 使用特洛伊DLL注入代码 1747.6.6
使用注册表注入DLL 1757.6.7 使用程序挂钩的方法注入代码 1757.7 本章小结
175参考文献 176第8章 应用程序的静态挂钩 1778.1 引言 1778.2
使用C/C++语言提取可执行程序代码 1778.2.1 在C/C++中使用内联汇编 1778.2.2
如何使用C/C++语言提取可执行程序代码 1798.3 如何对PE文件加壳 1828.3.1
PE文件的加壳方法 1828.3.2 向PE文件中静态注入代码的完整实例 1838.4
如何实现文件脱壳 1918.5 本章小结 192参考文献 192第9章 应用程序的动态挂钩 1939.1
动态挂钩概述 1939.2 使用Windows钩子函数挂钩 1949.2.1 Windows钩子函数 1949.2.2
具体实例 1959.3 替换原API函数入口挂钩 1989.3.1 如何替换原API函数入口实现挂钩
1989.3.2 通用的替换原API函数入口挂钩类 1999.3.3 使用JMP法编写的挂钩实例 2019.4
替换IAT中的函数地址进行挂钩 2029.4.1 如何替换IAT中的函数地址实现挂钩 2029.4.2
通用的替换IAT中的函数地址挂钩类 2039.4.3 使用IAT法编写的挂钩实例 2079.5
替换Windows消息处理函数实现挂钩 2089.5.1 Windows消息处理函数及其替换 2099.5.2
替换Windows消息处理函数实现挂钩的实例 2109.6 钩子DLL文件的装载 2149.7
本章小结 216参考文献 216第10章 数据的编码和解码实例 21710.1 引言 21710.2
游程编码 21810.2.1 CX游程压缩方法 21810.2.2 BI_RLE8压缩方法 21810.2.3
BI_RLE压缩方法 21810.2.4 缩位压缩方法（Packbits） 21910.3 Huffman编码 21910.3.1
Huffman编码原理 21910.3.2 Huffman编码过程 22010.4 算术编码 22110.4.1
算术编码算法 22110.4.2 算术解码算法 22210.5 LZW压缩算法 22210.5.1
LZW压缩算法原理 22310.5.2 用VC++实现LZW压缩算法 22510.6 Base64编码 23610.6.1
Base64算法原理 23610.6.2 Base64算法的实现 23810.7 本章小结 241参考文献
242第11章 可执行文件的捆绑和分离 24311.1 引言 24311.2 捆绑方式分类 24311.2.1
结合式捆绑 24311.2.2 功能式捆绑 24511.3 文件捆绑相关技术 24511.3.1
文件捆绑工具及实现 24511.3.2 木马程序与捆绑 24611.3.3 文件自身操作特点分析
24611.4 文件属性的获取和伪装 24811.4.1 文件属性的获取和更改 24811.4.2
一个获取文件基本属性类 24911.4.3 可执行程序自删除的实现 25111.4.4
如何获取其他应用程序的图标 25411.4.5 如何改变窗口的图标 25511.5
被捆绑文件分离后的运行及自分解文件原理 25611.5.1 异步执行分解法的实现 25611.5.2
同步执行分解法的实现 25611.5.3 自动分解法的实现 25711.6
一个捆绑机（BindHider）软件的设计 25811.6.1 BindHider的设计 25811.6.2
BindHider的源代码 25911.7 一种制作自分解文件的方法 26311.7.1 母体程序的制作
26411.7.2 自分解文件的制作 26611.8 本章小结 267参考文献 268第12章
可执行文件的分割和合并 26912.1 引言 26912.2 文件分割方式 26912.2.1
考虑文件格式的分割 26912.2.2 设置子文件大小的分割 27012.2.3
具有自合并功能的文件分割 27112.2.4 依赖文件存放位置的分割 27112.2.5

依赖磁盘大小的分割 27112.3 如何使用多线程 27212.3.1 线程的创建和终止 27212.3.2 线程的控制函数 27312.3.3 线程的通信 27312.4 文件的简单分割与合并 27412.4.1 文件的简单分割 27412.4.2 文件的简单合并 27512.5 用多线程进行文件的分割与合并的实例 27712.5.1 文件的分割与合并方案设计 27712.5.2 用多线程进行文件分割 27912.5.3 用多线程进行文件合并 28212.6 分割后文件自动合并的方案设计 28612.6.1 控制程序的制作 28612.6.2 用于文件自合并的控制程序的制作 28712.6.3 一种生成自合并文件的分割软件制作 28912.7 本章小结 292参考文献 292第13章 多线程下载和断点续传 29313.1 引言 29313.2 使用FTP进行多线程下载和断点续传 29313.2.1 FTP协议简介 29313.2.2 FTP的工作模式 29513.2.3 FTP协议多线程下载和断点续传的实现 29513.2.4 实例 30613.3 使用HTTP进行多线程下载和断点续传 30713.3.1 HTTP协议简介 30713.3.2 HTTP协议的内部操作过程 30813.3.3 HTTP协议多线程下载和断点续传的实现 31113.3.4 实例 32113.4 BT下载简介 32313.4.1 BT下载与一般下载的区别 32313.4.2 BT种子 32413.4.3 BT的下载过程 32413.5 本章小结 324参考文献 325第14章 带附件的电子邮件发送剖析 32614.1 引言 32614.2 电子邮件的发送方法 32614.3 用WinSock实现SMTP协议 32714.3.1 SMTP协议 32714.3.2 SMTP的实现 32814.4 邮件格式化 33514.4.1 邮件主体格式化 33514.4.2 邮件附件格式化 33814.4.3 邮件格式化 34114.5 发送电子邮件实例 34614.6 本章小结 347参考文献 347第15章 特洛伊木马与反木马技术 34815.1 引言 34815.2 常见的木马种类 34915.3 木马的载入方式 35015.4 木马采用的伪装方法 35115.5 Windows 2K/XP中无法删除文件的常用解决办法 35215.6 一种木马病毒的检测技术 35315.7 本章小结 358参考文献 359
· · · · · ·(收起)

Windows应用程序捆绑核心编程_下载链接1_

标签

Windows编程

编程

计算机技术

黑客技术

windows

有点想买

应用编程-windows

mark

评论

这会课程设计就参考这本书了，做个EXE文件捆绑器//
这本书其实很不错，是启发你来理解编程本质的，尤其是windows下编程//
仔细看了后感觉作者功力还是不行，PE文件那章讲得不知所云，还是罗云彬功力深厚啊！这本书还是只看看目录和例子就够了，启发一下也就ok了。

木马 钩子

先看看也不错，用的时候再看也不迟

入门书，当故事会看吧

烂书！！都是抄的东西。

Windows应用程序捆绑核心编程_下载链接1_

书评

Windows应用程序捆绑核心编程_下载链接1_