第一图书网, tushu007.com

<<寒江独钓>>

图书基本信息

书名：<<寒江独钓>>

13位ISBN编号：9787121087967

10位ISBN编号：7121087960

出版时间：2009年6月出版

出版时间：电子工业出版社

作者：谭文,杨潇,邵坚磊 著

页数：516

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

早在一年前，谭文就和我谈过想写一本既能深刻介绍Windows内核架构，又能结合具体Windows驱动程序开发实例的书。
在一年的时间中，谭文一直在构思酝酿。
那时候他的《天书夜读——从汇编语言到Windows内核编程》已经出版，《天书夜读》所涉及的内容很广，但就如同书名一样，它的内容不太适合刚刚涉猎Windows内核编程的程序员，反而更像一本供黑客学习的读物。
书中翔实地介绍了很多反汇编技巧的技巧，非常的精辟，但对于新手来说，容易对Windows内核编程产生畏惧感。
　　当我第一次读完《寒江独钓——Windows内核安全编程》的初稿时，我觉得本书非常适合Windows内核程序的入门。
Windows内核程序一直被认为是只有高手才能涉及的领域，很多程序员对这种开发都觉得非常神秘。
我觉得这是一种错觉，其中有一个很重要的原因就是国内很少出版这方面的书籍。
这本书很好地弥补了这方面的空白，我相信大部分读者读完后，都会觉得Windows内核开发程序不再那么神秘。
的确，微软自从Windows 2000版本以后，内核的架构变化不是很大。
当然，这并不意味着你读完本书后，你就可以对内核开发游刃有余了，这需要你对每一个细节反复研究，并且多做试验。
　　编写Windows内核程序，就意味着这个程序可以执行任意指令，可以访问计算机所有的软件、硬件资源。
因此，稍有不慎就有可能将系统变得不稳定。
Windows的设计者设计了各种驱动模型或者框架，如NT式内核驱动模型、WDM框架和新推出的WDF框架。
在这些模型框架下编程，就使内核编程变得简单，同样也降低了内核程序崩溃的机会。
其实，Windows驱动程序员和黑客都在写内核程序，唯一不同的是驱动程序员按照微软设计的模型写程序，而黑客可以不按照这些框架写。
Windows设计的这些框架，可以将操作系统的原理隐藏起来，只暴露一些接口，驱动程序员只要把这些接口写好就可以了。
从这个角度看，驱动开发并不难，尤其是读完本书后，更会觉得不难了。
但是想完成一些特殊的功能，如内核级隐藏进程等，Windows的这些框架就没什么用处了，程序员就需要对Windows内核有全面的了解，通过直接修改Windows内核来实现这些目的。
往往黑客对这种技术乐此不疲，通过修改Windows内核，你会发现你的程序几乎无所不能。
　　编写内核程序是一件很痛苦的事情，回想起这些年学习内核程序开发的经历，真是感慨万千。
就如同谭文所说：编写内核程序的人从某种程度讲是孤独的。
当一个经验并不丰富的小程序员面对庞大复杂的并且不开源的Windows框架时，那是一种怎样的无助感啊！
谭文是我比较钦佩的程序员之一，他对技术非常执着，并且精力充沛。
内核程序的知识涉及面非常广，不同类别的内核程序差别也特别大，他几乎都有所涉猎。
相信读者在读完这本书后，能对Windows内核开发有比较详细的了解，同时也能结合书中的实例写出很优秀的内核程序了。
　　张 帆　　2009年5月1日于北京本书是一本专门介绍实时扫描的防毒软件、虚拟磁盘、硬盘还原、硬盘加密、文件系统保护、文件透明加密、防火墙、密码输入保护等软件的Windows内核模块的具体实现方法的编程技术书。
本书的目的是使读者能够用C语言编写这些核心模块。
　　大学的时候，在Windows平台上我最初学的是VB，然后是Delphi。
我的感觉是，无论想实现任何功能，都早已有工具的开发者给我们准备了良好的接口和文档，让我们

学习和使用都非常的方便。
因此觉得自己已经学到了终点。
如果仅从“能实现功能”的角度讲，我没有必要再学习了，剩下的事情，只是去很舒适地使用那些接口就可以了。
那又何必再学习Windows编程呢？
　　工作之后遇到了障碍。
我的第一个任务是实现一个网络的虚拟磁盘。
我虽然自以为无所不能，但是也找不到在Windows系统里增加一个虚拟磁盘的API在哪里。
我每天都在使用虚拟光驱、杀毒软件、防火墙，但是我从未想过它们如何实现。
不是因为我懂，而是因为我自以为任何功能的实现一定是简单而舒适的，等需要的时候再去研究，绝不会有什么困难。
　　但是实际编码的时候才明白：良好的接口、舒适的编码过程，绝对不是天生之道。
天地万物自混沌而起，那些美好的表面，不过是在残酷的现实上重重包裹的包装纸罢了。
　　一辆新车的表面自然光彩照人，操作接口也人性而美好。
但是一旦需要打开车身去修理内部某根漏油的管子，就没有那么容易和舒适了。
造成这种情况，绝不是Windows的底层开发者们天生没有美学观念。
那些多年积累和维护着并不断改进的无数行代码，已经是人类工程史上的奇迹了。
如今要打开它的外壳去肆意修理，当然不是一件轻松的事情。
　　但这正是Windows内核编程的魅力所在。
　　只有极少的程序员会需要参与微软的Windows内核开发，也只有极少的读者会自己试图从头开发一个类Windows的操作系统内核（有这方面兴趣的读者，建议参考开源项目ReactOS）。
单纯地讲解Windows内核编程对大多数读者都没有意义。
但是，信息安全类的软件是内核编程的极好的应用实例。
病毒实时监控、防火墙、入侵检测、数据保护还原、数据即时备份、数据加密、数据防止泄密、反外挂等，都不同程度地涉及到内核编程；或者，内核编程可以让它们工作得更好。
这些就是本书的内容，因此本书的副标题为“Windows内核安全编程”。
“寒江独钓”则表明了这个领域的寒冷与寂寥。
　　本书和《天书夜读——从汇编语言到Windows内核编程》的不同之处在于：《天书夜读》一书介绍的是自己调试Windows内核、获取知识、解决问题的技巧。
因此《天书夜读》一书介绍的内容大部分是没有文档可循的，容易走火入魔。
　　本书则基本上介绍的是正统的内核编程技术，是微软在内核编程中给信息安全软件开发者提供的相关接口的大集合，是名门正派的技术，不沾邪气。
一个好的内核程序员，“正邪兼修”是有必要的。
　　本书既适合于有志于成为软件程序员的学生使用，也适合于希望加强自己的技术实力的Windows程序员阅读，同时更适合于从事信息安全行业的Windows软件的开发者作为手头参考。
　　本书对改善病毒横行的网络现状也有一定益处。
虽然无助于劝说那些孜孜不倦的病毒开发者们弃恶从善，但是至少有助于他们提高技术素养，学会更认真地编写程序，以免总是写出导致程序崩溃和系统蓝屏的代码，影响无辜者的正常工作。
　　本书假定读者了解C语言，能理解C语言的基本语法，并且学习过操作系统、计算机网络和数据结构的基础知识。
一般来说，如果读者听说过“进程”、“文件系统”、“中断”、“TCP协议”、“以太网包”、“链表”、“哈希表”、“加密算法”这些名词，则足够阅读此书了。
　　有些读者可能会关心作为一个程序员的就业前景。
这也是我非常关心的一个问题。
我曾经在杭州的核新软件公司为证券营业部开发防火墙和虚拟磁盘，一共3年的时间；后来在日电卓越软件（北京）的上海分公司开发部信息安全开发课工作了3年。
我认识的业界朋友们，大多在赛门铁克、趋势、瑞星、EMC、华赛这样的公司就职。

现在是我工作的第7个年头了，我在Intel在上海的紫竹中心参与动态二进制翻译项目。
最有价值的是，我参与的每一个项目都让我学习到更多的知识，面对许多前所未有的考验，每一步都让人充满了精神上的成就感。
　　本书的读者未来很可能会从事底层编码的工作，而不是一个上层的设计和管理人员。
从事底层编码的程序员，常常被同事称为“牛人”。
这个牛人不是“牛皮哄哄的人”的意思，而是“像牛一样辛苦工作的人”的意思。
想从事这个行业的读者，我抄我的前同事钱铮最喜欢的一首古诗《代牛言》献给您：　　渴饮颍水流，饿喘吴门月。
黄金如可种，我力终不竭。
　　谭 文　　2009年1月1日

内容概要

本书从Windows内核编程出发，全面系统地介绍了串口、键盘、磁盘、文件系统、网络等相关的Windows内核模块的编程技术，以及基于这些技术实现的输入密码保护、防毒引擎、文件加密、网络嗅探、网络防火墙等信息安全软件的核心组件的具体编程。
主要知识重点包括：Windows串口与键盘过滤驱动、Windows虚拟存储设备与存储设备过滤驱动、Windows文件系统过滤驱动、文件系统透明加密/解密驱动、Windows各类网络驱动（包括TDI过滤驱动及3类NDIS驱动），以及最新的WDF驱动开发模型。
有助于读者熟悉Windows内核驱动的体系结构，并精通信息安全类的内核编程技术。
本书的大部分代码具有广泛的兼容性，适合从Windows 2000一直到目前最新的Windows 7 Beta版。
　　本书适合大专院校计算机系的学生、普通Windows程序员、Windows内核程序员、信息安全行业的程序员，以及希望了解Windows系统底层知识的计算机编程爱好者使用。
阅读本书，需要读者有C语言、数据结构、操作系统和计算机网络的基础知识。

作者简介

邵坚磊，前执业医生，现C、汇编程序员。
1976年生于上海，毕业于上海交通大学计算
机系，具有临床医学和计算机专业的双学位。
长期致力于x86体系架构与Windows系统底
层技术的研究与相关开发工作；目前在上海某公司主持信息防泄密软件的Windows内核
驱动的开发工作。
是著名的反rootkit工具DarkSpy的作者之一。
曾与谭文合著《天书夜
读——从汇编语言到Windows内核编程》。
爱好网游。
编写本书的第4章。

张佩，C程序员，1982年生于江苏扬中，毕业于苏州大学。
近三四年来，一直从事底层
软件开发，乐此不疲。
因偶然的机会参与了本书的写作，非常开心。
现从事于一项音视
频软件方面的项目。
此人好读书，好写文章，好交朋友。
为人善，与人交善，诚善人
也。
受邀编写本书的第13章。

书籍目录

第1章 内核上机指导 1.1 下载和使用WDK 1.1.1 下载安装WDK 1.1.2 编写第一个C文件 1.1.3 编译一个工程 1.2 安装与运行 1.2.1 下载一个安装工具 1.2.2 运行与查看输出信息 1.2.3 在虚拟机中运行 1.3 调试内核模块 1.3.1 下载和安装WinDbg 1.3.2 设置Windows XP调试执行 1.3.3 设置Vista调试执行 1.3.4 设置VMWare的管道虚拟串口 1.3.5 设置Windows内核符号表 1.3.6 实战调试first 练习题 第2章 内核编程环境及其特殊性 2.1 内核编程的环境 隔离的应用程序 2.1.2 共享的内核空间 2.1.3 无处不在的内核模块 2.2 数据类型 2.2.1 基本数据类型 2.2.2 返回状态 2.2.3 字符串 2.3 重要的数据结构 2.3.1 驱动对象 2.3.2 设备对象 2.3.3 请求 2.4 函数调用 2.4.1 查阅帮助 2.4.2 帮助中有的几类函数 2.4.3 帮助没有的函数 2.5 Windows的驱动开发模型 2.6 WDK编程中的特殊点 2.6.1 内核编程的主要调用源 2.6.2 函数的多线程安全性 2.6.3 代码的中断级 2.6.4 WDK中出现的特殊代码 练习题 第3章 串口的过滤 3.1 过滤的概念 3.1.1 设备绑定的内核API之一 3.1.2 设备绑定的内核API之二 3.1.3 生成过滤设备并绑定 3.1.4 从名字获得设备对象 3.1.5 绑定所有串口 3.2 获得实数据 3.2.1 请求的区分 3.2.2 请求的结局 3.2.3 写请求的数据 3.3 完整的代码 3.3.1 整的分发函数 3.3.2 如何动态卸载 3.3.3 完整的代码 本章的示例代码 练习题 第4章 键盘过滤第5章 磁盘的虚拟 第6章 磁盘过滤 第7章 文件系统的过滤与监控 第8章 文件系统透明加密 第9章 件系统微过滤驱动第10章 网络传输层过滤 第11章 NDIS协议驱动 第12章 NDIS小端口驱动 第13章 NDIS中间层驱动附录A 如何使用本书的源码光盘

编辑推荐

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