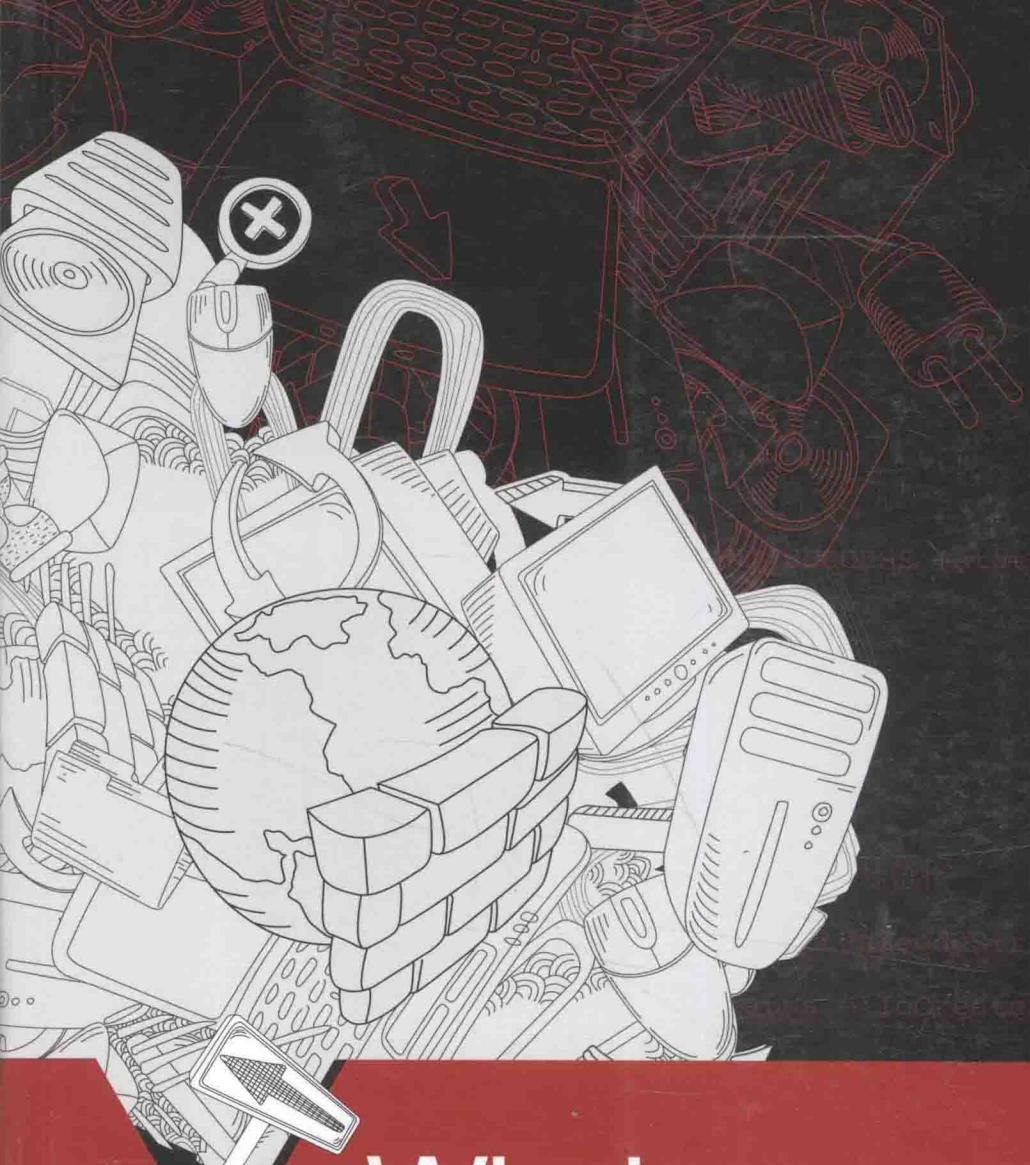
Broadview
www.broadview.com.cn



Windows内核安全与驱动开发

谭文 陈铭霖 等著

中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

Windows内核安全与驱动开发

谭文 陈铭霖 等著

電子工業出版社
Publishing House of Electronics Industry

内 容 简 介

本书的前身是《天书夜读——从汇编语言到 Windows 内核编程》和《寒江独钓——Windows 内核安全编程》。与 Windows 客户端安全软件开发相关的驱动程序开发是本书的主题。书中的程序使用环境从 32 位到 64 位，从 Windows XP 到 Windows 8 都有涉及，大部分程序不经过修改即可在 Windows 10 上运行。同时本书也深入浅出地介绍了进行内核安全编程所需要的操作系统、汇编等基础知识。

本书共分三篇，基础篇囊括了驱动开发的基础知识，降低了入门的难度；开发篇介绍了在实际工作中可能遇到的各种开发需求的技术实现，包括：串口的过滤、键盘的过滤、磁盘的虚拟、磁盘的过滤、文件系统的过滤与监控、文件系统透明加密、文件系统微过滤驱动、网络传输层过滤、Windows 过滤平台、NDIS 协议驱动、NDIS 小端口驱动、NDIS 中间层驱动、IA-32 汇编基础、IA-32 体系中的内存地址、处理器权限级别切换、IA-32 体系结构中的中断和 Windows 内核挂钩；高级篇包含了汇编语言、操作系统原理、处理器体系架构相关的内容。本书是由长期从事这个行业的工程师自己写的，所以处处以实用为准。对细节的考究主要体现在对实际问题的解决，而不是知识的详尽程度上。

本书适合计算机安全软件从业人员、计算机相关专业院校学生以及有一定 C 语言和操作系统基础知识的编程爱好者阅读。

图书在版编目（CIP）数据

Windows 内核安全与驱动开发 / 谭文等著. —北京：电子工业出版社，2015.6
ISBN 978-7-121-26215-9

Ⅰ. ①W… Ⅱ. ①谭… Ⅲ. ①Windows 操作系统—程序设计 Ⅳ. ①TP316.7

中国版本图书馆 CIP 数据核字（2015）第 118552 号

策划编辑：李 冰
责任编辑：葛 娜
印 刷：北京中新伟业印刷有限公司
装 订：三河市皇庄路通装订厂
出版发行：电子工业出版社
北京市海淀区万寿路173信箱 邮编：100036
开 本：787×1092 1/16 印张：42.5 字数：1121千字
版 次：2015年6月第1版
印 次：2015年6月第1次印刷
定 价：139.00元（含光盘1张）

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至zlts@phei.com.cn，盗版侵权举报请发邮件至dbqq@phei.com.cn。

服务热线：（010）88258888。

本书的作者和贡献者

本书的内容是《天书夜读——从汇编语言到 Windows 内核编程》（以下简称《天》）和《寒江独钓——Windows 内核安全编程》（以下简称《寒》）这两本书的原版内容重新编辑整理，并新添了一些章节而成的。除了直接编写本书的作者外，《天》与《寒》两本书也有多位业内技术人士协同编写。所有的作者一并介绍如下：

谭文，网名楚狂人，长期从事客户端安全的开发工作。先后在 NEC、英特尔亚太研发有限公司、腾讯科技任职。曾经从事过企业安全软件、x86 版 Android、腾讯电脑管家等开发工作。编写了《天》与《寒》的大部分章节，并为本书重写了部分章节，添加了一些新的内容。

陈铭霖，腾讯电脑管家团队高级工程师，长期从事 Windows 系统研究，目前从事客户端安全的开发工作。编写了本书中部分新的章节，并统稿全书，重新整理和编辑了《天》和《寒》的全部内容。对本书的面世做出了巨大的贡献。

张佩，Windows 驱动开发技术专家，长期从事声卡、显卡等硬件驱动程序的开发、调试工作。目前在英特尔亚太研发有限公司平板电脑相关的部门工作。曾著有《竹林蹊径——深入浅出 Windows 驱动开发》一书。为《寒》贡献了若干个网络驱动相关的章节，这些内容大多原版整合到了本书中。

杨潇，曾为 Windows 客户端安全工程师，先后在上海贝尔和北京 Comodo 工作。后来离职创业，目前为西安一家医疗科技公司的 CEO。为《寒》一书编写了磁盘驱动相关的章节，这些章节也整合到了本书中。

邵坚磊，网名 wowocock，业内著名的 Windows 安全技术专家。长期从事 Windows 安全相关的内核开发工作。目前在奇虎 360 任职。为《天》和《寒》都贡献了部分章节和代码实例，这些内容有一部分整合到了本书中。

卢冠豪，中国台湾人。毕业于辅仁大学资讯工程学系。长期从事 C、C++、网络与通信程序设计的工作；参与过“端点安全”、“资产管理”、“网络流量分析”等项目的开发与维护；擅长 Windows 项目开发。编写了《寒》一书中的文件系统微端口过滤一章，此章也整合到了本书中。

前　言

本书的前身是《天书夜读——从汇编语言到 Windows 内核编程》和《寒江独钓——Windows 内核安全编程》。实际上，本书相当于这两本书（重写和充实了不少章节）的合体。因为这两本书讲述的内容本来就是同一类技术，只不过各有侧重，合并成一本书之后体系更加完整了。

与 Windows 客户端安全软件开发相关的驱动程序开发是本书的主题。因为这些驱动程序都运行在 Windows 内核中，所以本书称为《Windows 内核安全与驱动开发》。这些驱动程序主要分成三大类：第一类是串口、键盘等输入/输出设备驱动程序；第二类是硬盘、文件系统驱动程序；第三类是网络驱动程序。覆盖了客户端安全的 Windows 编程中所涉及的各种驱动程序。书中的程序使用环境从 32 位到 64 位，从 Windows XP 到 Windows 8 都有涉及，大部分程序不经过修改即可在 Windows 10 上运行。同时本书也深入浅出地介绍了进行内核安全编程所需要的操作系统、汇编等基础知识。

与前身相比，本书重新排布了章节，主体上分为三个部分。第一个部分为“基础篇”，囊括了驱动开发的基础知识，降低了入门的难度；第二个部分为“开发篇”，包含了在实际工作中可能遇到的各种开发需求的技术实现；第三个部分是“高级篇”，汇编语言、操作系统原理、处理器体系架构相关的内容都放在了本篇中介绍。本篇内容对读者来说可能会感觉比较困难，但由于有前两篇的基础，相信读者不会太难以跨越。

本书是由长期从事这个行业的工程师自己写的，所以处处以实用为准。对细节的考究主要体现在对实际问题的解决，而不是知识的详尽程度上。有些读者可能会觉得这不太像一本“教科书”，在某些细节点上很有“囫囵吞枣”的嫌疑。当然，本书本来就不是教科书，但它是可以用来学习的。只是学习的方法，以实际应用为唯一的动力。

以前常有读者和我交流。我发现最常问的问题是：“我对内核编程有兴趣，请问应该如何学习呢？”

学习的方法应该根据每个人不同的需要有所不同。每个人性格不同，学习的路线也会不一样。比如有的人就擅长计划，他们会先制定周全的步骤，然后按部就班地执行。先从有经验的人那里讨教“如何学习”也是步骤之一。我曾很努力地想这样去做，但总是没有足够的毅力而失败。所以我成了一个随波逐流、随遇而安的家伙。我的学习都是迫不得已，没有计划和方法可言。所以被问到这个问题时，我只能说，我都是在解决实际问题的过程中学习的。这个风格也被带到了本书中。

在读大学的时候，我对驱动开发并无任何概念，我也不为此担心。什么时候我会需要为一个硬件去编写驱动程序呢？这不是硬件厂商的事吗？我为一家硬件厂商工作的机会本来就低，更何况几千个员工里轮到我去写驱动的概率更是低到不可思议的程度。但世事就这么难料。我刚进第一家公司，自以为 VC 6.0 用得多么熟练，准备大干一场的时候，老板说："我这里有个无盘驱动，你去做试试看……"

当时，他们需要的是一种类似"网络邻居"的共享盘。硬盘的主体在服务器上，上面有很多文件共享给所有的客户机。Windows 本身的"网络邻居"不足以满足全部需求。他们要求每个客户机对这个磁盘都有读写的权力，可以新建、修改或者删除磁盘上的文件。如果直接用 Windows 的目录共享，很快这个磁盘上的文件就会被修改得乱七八糟。所以另一个要求是，任何人都可以修改，但任何人的修改都不得影响他人。

这听起来有点怪，其实很简单。大家共享一台服务器的磁盘上的所有文件，但各自对这些文件的修改都保存到本地。虽然听起来是很合理、简洁的一个需求，但是对我来说却完全摸不着头脑。我写过很多程序，但还从未写过一个东西能让计算机的硬盘的行为发生改变。这是因为我一直只会写用户软件，从没动过操作系统。

操作系统非常努力地提供了完善的功能，来应付各种用户的需求。但用户的需求真是取之不尽、用之不竭的，仅仅一家开发操作系统的公司，永远也无法满足用户的需求。是否允许第三方拥有操作系统的权限来满足这些需求呢？这就形成了两种截然不同的应对方案：Windows 是允许的，任何第三方都可以通过开发驱动程序的形式来改变系统内核的行为；而像苹果的 iOS 这种操作系统是完全禁止的。

为了证明我的价值足够保底薪水，我不得不开始研究这个东西怎么实现。它肯定不是我以前实现过的任何一类工程。当时还是 Windows 9x 的时代，资料奇缺，甚至连开发用的工具包都不知道去哪里找。具体的过程我已经记不太清了，侯捷翻译后又免费放出电子版的一本专门讲 VXD 的书起了很大的作用。

最后我把这个东西做了出来。那时，我每天加班到晚上，早晨一睁眼就想往公司里赶。我敢保证任何人换了是我也会一样：第一次参加工作，到手的第一个任务，谁都想证实自己的价值。我不记得有多少知识被我"囫囵吞枣"了，但我确实满足了用户的需求。离奇的是，那时我还根本不会用 WinDbg，整个过程只靠"蓝屏试验"，压根就没像样地调试过。这根本无须任何学习方法。在有如此强烈需求的境况下，一切的不合理都会顺理成章。

开发驱动程序类似于为普通的软件开发一个"组件"。与别人约定好调用的接口，你就可以和别人协同合作，开发一个"dll"之类的组件去给别人使用。对操作系统内核也是如此，只不过这个接口由操作系统硬性规定，容不得协商。

在那个项目中我们写了种种功能来"愚弄"操作系统。这听起来像是一个磁盘相关的驱动，实际上却是一个文件系统过滤驱动。它过滤文件系统的行为，比如：读取文件时，我们让操作系统以为在操作普通的本地文件系统，其实却是去网络上取文件内容；而修改文件时，我们也让操作系统以为修改成功了，实际上数据并没有写入到网络上的服务器中，而是写到本地了。这是我第一次接触这类驱动程序。

有了这些项目的经验，后来就有了《天书夜读——从汇编语言到 Windows 内核编程》《寒江独钓——Windows 内核安全编程》之类的书，也有了本书。虽然这个跨度有点长，一晃七八年过去了，但这和我的拖拖拉拉有很大的关系。《寒江独钓——Windows 内核安全编程》绝版之

后，编辑一直催促我修改出新的版本。但我继续磨蹭，直到我到了腾讯电脑管家的团队，这里遇到的优秀同事愿意帮我整理已经乱七八糟的稿子，并填充最新的章节，最后耐心地审校和完善代码，本书才能最终得以面世。至于如何学习，我已经说了自己的糟糕的例子。我可以大概总结如下：

有计划和毅力是最好的。耐心地读完本书，调通上边所有的例子。虽然工作中不一定真会用到，但里面的东西都是别人实际用到过的。

没有必要害怕接受自己不熟悉的工作任务。泰山压顶的工作压力也是学习最好的动力——好吧，因为我没有前面一条，所以这一条就成了我唯一的动力了。碰到急需完成的任务，本书上有时也有可以参考的现成代码，不妨翻一翻看看。懂不懂没关系，先用了再说。

理想是美好的，可以创造一些令人意外的东西。但最后还是要着眼于实际。

写代码是一件很爽快的事，但调代码会很烦。读者如果买了本书并且打算从事这方面的工作，希望不要为调试的各种困难而烦躁，因为以后这就是工作的主要部分了。我因为第一个任务的缘故，一不小心就陷入十多年。开头几年里大多数时间我都很烦躁，常常被 BUG 逼得感觉走投无路。现在好多了，差不多有七分自信能将事做成。当然，剩下三分还是要靠天意的。

谭文

2015 年 5 月

目　录

基　础　篇

开 发 篇

高 级 篇

基础篇