<<天书夜读>>

图书基本信息

书名：<<天书夜读>>

13位ISBN编号：9787121073397

10位ISBN编号：7121073390

出版时间：2008-10

出版时间：电子工业出版社

作者：谭文，邵坚磊 著

页数：270

前言

Windows是庞大复杂的系统。
由于Windows并不公开源代码，我们在调试程序的时候，往往就调到自己未知的领域去了。
没有C代码，只能看到令人眼花缭乱的汇编指令和机器码。
我曾对它们望而生畏，敬而远之。
尤其在这个黑客、破解、病毒、木马横行的时代，如果作为安全软件的开发者，同样不能期盼病毒的作者提供可以阅读的高级语言代码。

如果那些东西，也和C语言一样亲切易懂，那多么好啊！
这样的话，即便是Windows这样庞大复杂而且封闭的系统，或者是再诡异和隐蔽的破坏技术，至少只要我愿意去探索，对我来说就不再有秘密可言。

其实这个梦想并非不切实际。
既然我们能读懂C代码，何以就不能读懂汇编呢？
很多高手眼中，机器指令和C代码一样熟悉。

这本书并没有系统地介绍Windows系统底层。
但是我尝试寻找正确的方法和手段，为读者打开Windows底层知识宝库的大门，使读者可以在其中自由阅读，自己去获取所需知识。

<<天书夜读>>

内容概要

本书从基本的Windows程序与汇编指令出发，深入浅出地讲解了Windows内核的编程、调试、阅读，以及自行探索的方法。
读者在使用C/C++开发Windows程序的基础上，将熟练掌握汇编和C语言的应用，深入了解Windows底层，并掌握阅读Windows内核的基本方法，以及Windows内核的基本编程方法。
本书适合使用C/C++在Windows上编程的读者，尤其适合希望加深自己技术功底的Windows应用程序员、计算机专业的有志于软件开发的大中院校学生；专业的Windows内核程序员，亦可从本书得到超越一般内核程序开发的启发。

作者简介

谭文：从2002年到2008年，从事信息安全类软件的Windows内核驱动的开发工作。
从2008年开始参与一个主要涉及不同架构之间二进制指令的实时翻译技术的项目的开发。
业余时间在驱动开发音（www.driverdevelop.com）以楚狂人为笔名发表了许多技术文章。

<<天书夜读>>

书籍目录

章节摘录

第10章　继续探索Windows内核　　10.1 探索Windows已有内核调用　　基础知识　　下面用本书前面介绍的知识来做一些有用的事情。
Windows从2000发展到XP后，XP DDK中出现了一些新的调用。
内核程序开发者有时会发现，这些调用非常有用（这也是这些新调用产生的原因），但是如果使用这些调用，会导致驱动在Windows 2000下无法使用。
目前Windows 2000的用户依然很多，存在这样的可移植性问题是非常遗憾的，退一步的方案是Windows 2000下限制某些功能。
在程序中动态加载系统调用，并小心地判断当前的版本。
在Windows 2000的情况下，一些功能被跳过。
这样比前者好。
但是依然不是最理想的解决方案。
有一些人开始使用未公开（Undocumented）的解决方案。
未公开的解决方案的危害就是，可能不兼容未来的操作系统。
但是由于现在这样做仅仅是针对一个过去版本的操作系统，问题就不复存在了。
在新版本的操作系统上，调用新的系统调用，而在某个已经存在而且不会再变的操作系统版本上，调用未公开的方法。
只要低版本操作系统测试无问题，以后的也不会有问题。
这里的所谓未公开的解决方案就是，在新版本的操作系统上，把新出现的功能调用进行调试，了解其实现的方法。
然后在我们自己开发的内核程序中，实现同样的或者等价的功能，同时检测当前操作系统为低版本时，调用这些特殊的代码。
下面举两个例子。
这个调用获得设备栈底的设备，这对过滤驱动非常有用。

<<天书夜读>>

编辑推荐

我作为驱动开发的老兵，深感资料缺乏的艰辛，很多信息无法在文档中找到，此时自力更生的能力更加重要。

当我们手中拿着神兵利器——WinDbg时，一切都在掌握之中。

这本书将要告诉您的不是全面的汇编知识或未公开的Windows秘密，而是怎么从这些貌似天书的汇编代码中，一探Windows底层的核心实现。

在开发中出现的问题，能不能从Windows自身找到答案?如果您正在这样思考，无疑本书是为您度身订做的。

本书授人以渔，也授人以鱼；短小精悍，读之如一缕清风，读罢则有醍醐灌顶之感。

——驱动开发网站长　　马勇（znsoft）

版权说明