参考文献

[1] Intel Inc.: Intel 64 and IA-32 Architectures Software Developer's Manual Volume 1: Basic Architecture (2006).

[2] Intel Inc.: Intel 64 and IA-32 Architectures Software Developer's Manual Volume 2: Instruction Set Reference (2006).

[3] Intel Inc.: Intel 64 and IA-32 Architectures Software Developer's Manual Volume 3: System Programming Guide, Part 1&2 (2006).

[4] [美]Andrew S. Tanenbaum, Albert S. Woodhull 著，王鹏、尤晋元、朱鹏、敖青云译: 操作系统：设计与实现（第二版）. 电子工业出版社 (2001).

[5] Abraham Silberschatz, Peter Baer Galvin, Greg Gagne, A Silberschatz: Operating System Concepts, 6th Edition.

[6] [美]William Stallings 著，魏迎梅、王涌等译: 操作系统——内核与设计原理（第四版）. 电子工业出版社 (2002).

[7] T13: Information Technology - AT Attachment with Packet Interface - 6 (ATA/ATAPI-6) (2001).

[8] Microsoft: Microsoft Extensible Firmware Initiative FAT 32 File System Specification, FAT: General Overview of On-Disk Format (2000).

[9] 杨季文等编著: 80x86 汇编语言程序设计教程. 清华大学出版社.

[10] 沈美明、温冬婵编著: IBM-PC 汇编语言程序设计. 清华大学出版社 (1996).

[11] 王士元编著: C 高级实用程序设计. 清华大学出版社 (1999).

[12] 赵炯: Linux 内核完全注释. 机械工业出版社 (2004).

[13] 骆耀祖主编: Linux 操作系统分析教程. (2004).

3.1.2　算法反汇编阅读技巧

要阅读上面那样的代码，首先把流程控制的代码与数值计算的代码分开是关键，因此前面的练习能起很大的帮助作用。得到数值计算的代码部分后，必须判断输入与输出（一般自然是被读的内部变量为输入，被写的内部变量为输出），然后把它还原成一个 C 语言的表达式。任何一段中间不加任何跳转，连续的 mov 和加减乘除的指令一般都可以还原为一个 C 表达式。当然，这可不是一个轻松的工作。

在这里顺便可以看到，二维数组 a[x][y]，处理等同于一个大小为 a[y]的结构长度为 x 的数组。所以，前面讲到的数组访问的代码非常有价值。基本的方法如下：

```
mov         eax,<我要取的数组元素的下标>
imul        eax,eax,<结构的大小>
mov         ecx,<结构数组开始的地址>
mov         eax,dword ptr [ecx+eax];取得数组元素的内容放到 eax 中
```

访问结构内部变量的时候，最后面的一个指令还会加上一个数字：

```
mov         eax,dword ptr[ecx+eax+0Ch]
```

看到这样的代码，我们应该联想到表达式中含有的数组或结构体。

《寒江独钓——Windows 内核安全编程》

电子工业出版社　预计出版日期：2009 年 6 月

【内容简介】

本书从 Windows 内核编程出发，全面介绍串口、键盘、磁盘、文件系统、网络等相关的 Windows 内核模块的编程技术，以及基于这些技术的密码保护、防毒引擎、文件加密、网络嗅探、网络防火墙的具体实现。对于驱动编程模型的选择，本书同时兼顾 WDM 与 WDF。

本书适合大专院校计算机系的学生、计算机编程爱好者、普通 Windows 程序员、Windows 内核程序员、信息安全行业的程序员使用。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。

【书　摘】

5.4.4　如何处理发往设备的请求

在设备被创建好了之后，如何处理所有可能发送给设备的请求是需要考虑的下一个问题。在以往的 WDM 开发中，常用的方式是设置这个设备各个请求的分发函数为自己实现的回调函数，并且将特殊的处理放置在这些函数中。例如在这个例子里，可以将所有的读/写请求都实现为去读写内存，这就是最简单的内存盘。上面的处理方式说起来很简单，但是实现时还是需要一些技巧的，一种常用的方式是建立一个或多个队列，将所有发送到这个设备的请求都插入队列中，由另一个线程去处理队列。这是一个典型的生产者—消费者模型，这样做的好处是有了一个小小的缓冲，同时还不用担心由于缓冲带来的同步问题，因为所有的请求都被队列排队了。无独有偶的是，在 WDF 驱动框架中，微软直接提供了这种处理队列，这样就不用开发人员自己去操心如何建立队列，如何设置同步事件，如何在正确的时间销毁队列，这可真是一个造福大众的做法。

为了实现为驱动制作一个处理队列这一目标，在 WDF 驱动框架中需要初始化一个队列配置变量 ioQueueConfig，这个变量会说明队列的各种属性。一种简单的初始化方法是将这个配置变量初始化为默认状态，之后再对一些具有特殊属性的请求注册回调函数，例如为读请求注册回调函数等。在这样的初始化之后再为指定设备建立这个队列，WDF 驱动框架会自动将所有发往这个指定设备的请求都放入这个队列中处理，同时当请求符合感兴趣的属性（例如读写操作）时会调用之前注册过的处理函数去处理。对每个设备可以建立多个队列，但是在本例中不会讨论多个处理队列的情况。另外，在队列中也具有和设备类似的扩展，下面也会使用到。

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

Broadview®
www.broadview.com.cn

《Orange'S：一个操作系统的实现》读者交流区

尊敬的读者：

感谢您选择我们出版的图书，您的支持与信任是我们持续上升的动力。为了使您能通过本书更透彻地了解相关领域，更深入的学习相关技术，我们将特别为您提供一系列后续的服务，包括：

1. 提供本书的修订和升级内容、相关配套资料；

2. 本书作者的见面会信息或网络视频的沟通活动；

3. 相关领域的培训优惠等。

请您抽出宝贵的时间将您的个人信息和需求反馈给我们，以便我们及时与您取得联系。

您可以任意选择以下三种方式与我们联系，我们都将记录和保存您的信息，并给您提供不定期的信息反馈。

1. 短信

您只需编写如下短信： B08442+您的需求+您的建议

发送到1066 6666 789（本服务免费，短信资费按照相应电信运营商正常标准收取，无其他信息收费）

为保证我们对您的服务质量，如果您在发送短信24小时后，尚未收到我们的回复信息，请直接拨打电话（010）88254369。

2. 电子邮件

您可以发邮件至jsj@phei.com.cn或editor@broadview.com.cn。

3. 信件

您可以写信至如下地址：北京万寿路173信箱博文视点，邮编：100036。

如果您选择第2种或第3种方式，您还可以告诉我们更多有关您个人的情况，及您对本书的意见、评论等，内容可以包括：

（1）您的姓名、职业、您关注的领域、您的电话、E-mail地址或通信地址；

（2）您了解新书信息的途径、影响您购买图书的因素；

（3）您对本书的意见、您读过的同领域的图书、您还希望增加的图书、您希望参加的培训等。

如果您在后期想退出读者俱乐部，停止接收后续资讯，只需发送“B08442+退订”至10666666789即可，或者编写邮件“B08442+退订+手机号码+需退订的邮箱地址”发送至邮箱：market@broadview.com.cn 亦可取消该项服务。

同时，我们非常欢迎您为本书撰写书评，将您的切身感受变成文字与广大书友共享。我们将挑选特别优秀的作品转载在我们的网站（www.broadview.com.cn）上，或推荐至CSDN.NET等专业网站上发表，被发表的书评的作者将获得价值50元的博文视点图书奖励。

我们期待您的消息！

博文视点愿与所有爱书的人一起，共同学习，共同进步！

通信地址：北京万寿路 173 信箱　博文视点（100036）　　电话：010-51260888

E-mail：jsj@phei.com.cn，editor@broadview.com.cn

www.phei.com.cn
www.broadview.com.cn

反侵权盗版声明