二进制思维

----4k组织成员

[转]驱动程序开发—编译前传(4)

好啦，辛辛苦苦终于写完了程序，让我们编译运行吧！按下Ctrl+F5（嘿嘿，让我们先假设你习惯用VC来写程序），我等啊等……疑？怎么毫无动静的？再看看Output窗口，哇！有几百个错误啊！！不禁头大——这是怎么回事呢？

原来，WDM程序编译出来的并不是我们常见的.exe，而是.sys文件，在未经设置编译环境之前，是不能直接用VC来编译的（这就是为什么会有几百个错误了）。这种类型的文件你可以在WINNT\System32\Drivers里面找到很多。其实驱动程序也是一种PE文件，它同样由DOS MZ header开头，也有完整的DOS stub和PE header，同样拥有Import table和Export table——……那跟普通的PE文件有什么不一样呢？那么就让我们先来做个小剖析，加深对.sys文件的认识吧

首先祭出Delphi里附带的tdump.exe程序。让我们键入：

C:\WINNT\System32\Drivers>tdump ccport.sys -em -ee

参数-em是列出Import table，-ee是列出Export table。回车之后，屏幕列出一大堆东西：

```
C:\WINNT\SYSTEM32\DRIVERS>tdump ccport.sys -em -ee
Turbo Dump  Version 5.0.16.12 Copyright ? 1988, 2000 Inprise Corporation
            Display of File CCPORT.SYS

IMPORT:    NTOSKRNL.EXE={hint:011Fh}.'memcpy'
IMPORT:    NTOSKRNL.EXE={hint:003Dh}.'IoDeleteDevice'
IMPORT:    NTOSKRNL.EXE={hint:0030h}.'IoAttachDeviceToDeviceStack'
IMPORT:    NTOSKRNL.EXE={hint:008Eh}.'KeSetEvent'
IMPORT:    NTOSKRNL.EXE={hint:0068h}.'IofCallDriver'
IMPORT:    NTOSKRNL.EXE={hint:0095h}.'KeWaitForSingleObject'
IMPORT:    NTOSKRNL.EXE={hint:0074h}.'KeInitializeEvent'
IMPORT:    NTOSKRNL.EXE={hint:003Fh}.'IoDetachDevice'
IMPORT:    NTOSKRNL.EXE={hint:00D3h}.'RtlFreeUnicodeString'
IMPORT:    NTOSKRNL.EXE={hint:0077h}.'KeInitializeSpinLock'
IMPORT:    NTOSKRNL.EXE={hint:0129h}.'strcpy'
IMPORT:    NTOSKRNL.EXE={hint:0121h}.'memset'
IMPORT:    NTOSKRNL.EXE={hint:003Ch}.'IoCreateUnprotectedSymbolicLink'
IMPORT:    NTOSKRNL.EXE={hint:0038h}.'IoCreateDevice'
IMPORT:    NTOSKRNL.EXE={hint:00C2h}.'RtlAnsiStringToUnicodeString'
IMPORT:    NTOSKRNL.EXE={hint:0069h}.'IofCompleteRequest'
IMPORT:    NTOSKRNL.EXE={hint:0124h}.'sprintf'
IMPORT:    NTOSKRNL.EXE={hint:003Eh}.'IoDeleteSymbolicLink'
IMPORT:    NTOSKRNL.EXE={hint:0042h}.'IoFreeIrp'
IMPORT:    NTOSKRNL.EXE={hint:004Dh}.'IoInitializeIrp'
IMPORT:    NTOSKRNL.EXE={hint:002Dh}.'IoAllocateIrp'
IMPORT:    NTOSKRNL.EXE={hint:0027h}.'InterlockedExchange'
IMPORT:    NTOSKRNL.EXE={hint:0025h}.'InterlockedCompareExchange'
IMPORT:    NTOSKRNL.EXE={hint:0035h}.'IoCancelIrp'
IMPORT:    NTOSKRNL.EXE={hint:012Ah}.'strlen'
IMPORT:    NTOSKRNL.EXE={hint:0126h}.'strcat'
IMPORT:    NTOSKRNL.EXE={hint:0114h}.'atoi'
IMPORT:    NTOSKRNL.EXE={hint:0128h}.'strcmp'
IMPORT:    NTOSKRNL.EXE={hint:0034h}.'IoBuildSynchronousFsdRequest'
IMPORT:    NTOSKRNL.EXE={hint:00D5h}.'RtlInitAnsiString'
IMPORT:       HAL.DLL={hint:0006h}.'KfAcquireSpinLock'
IMPORT:       HAL.DLL={hint:0009h}.'KfReleaseSpinLock'

EXPORT ord:0001='Vcomm_DriverControl'
```

看到了吗？它主要调用了NTOSKRNL.EXE和HAL.DLL文件（实际上你会发现，几乎所有的WDM驱动程序都会调用NTOSKRNL.EXE文件，从它的名字你可以看出为什么了吧？），并且输出了一个函数“Vcomm_DriverControl”。这表明，其实.sys跟.exe文件一样，都是一种PE文件来的。不同的是，.sys文件Import的通常是NTOSKRNL.EXE，而.exe文件Import的通常是KERNEL32.DLL和USER32.DLL。

知道了这些有什么用呢？实际上，由于.sys通常不调用KERNEL32.DLL和USER32.DLL，所以你是不能在设备驱动程序里面调用任何C、C++和Win32函数的，而且也不能用C++关键字new和delete等（可以用malloc和free来代

替），而必须使用大量的内核函数。另外，你应该也能看到她调用了像IoDeleteDevice、IoAttachDeviceToDeviceStack等等函数，这些你以前可能没有见过的函数都是些内核函数。为了读者的方便，下面我列出一些常见的驱动程序可用的内核函数：

Ex… 执行支持
Hal… 硬件抽象层（仅NT/Windows 2000）
Io… I/O管理器（包括即插即用函数）
Ke… 内核
Ks… 内核流IRP管理函数
Mm… 内存管理器
Ob… 对象管理器
Po… 电源管理
Ps… 进程结构
Rtl… 运行时库
Se… 安全引用监视
Zw… 其他函数

最后让我们再来看看，写设备驱动程序时必须注意的一些问题：

1、内核宏

如果查看DDK头文件，会发现有几个内核函数是以宏的方式实现的。这种宏中有几个宏的定义是相当糟糕的。例如，我们看到RemoveHeadList的定义如下：

```
#define RemoveHeadList(ListHead)
    (ListHead)->Flink;
    {RemoveEntryList((ListHead)->Flink)}
```

如果以以下方式调用RemoveHeadList，则将编译错误的代码：

```
if(SomethingInList)
    Entry = RemoveHeadList(list);
```

使这个调用安全的唯一方法是使用花括号：

```
if(SomethingInList)
  {
    Entry = RemoveHeadList(list);
  }
```

所以我们切勿为了贪图一时的方便，而使用不太规范的写法，最好是在所有的if、for和while等语句中使用花括号。

2、驱动程序函数名称

跟C/C++的main()函数一样，设备驱动程序也有一个必须存在，而且只能以DriverEntry()为名称的入口函数。然而，除此之外，我们可以使用任何名字来给其他函数命名——只要你自己记得就行了，当然，最好符合某些特定的规范啦，例如匈牙利命名法……

3、安装时的问题

·在Windows98中驱动程序可执行文件必须是8.3文件名。（别问我为什么，我也不知道，我只能建议你去问比尔该死）

·如果INF文件中含有非法节的详细资料，Windows将不使用这个INF文件。

本节罗罗嗦嗦讲了一大堆，跟实际的编程却并没有太大的关系，前传嘛！就是这样的啦！

posted on 2007-11-14 17:04 咖啡猪 阅读(185) 评论(0) 编辑 收藏 所属分类: C++驱动开发

验证码 * 
看不清,换一张 [登录]
[注册]

内容(请不要发表任何与政治相关的内容)

Remember Me?

提交 登录 使用高级评论 新用户注册 返回页首 恢复上次提交

[使用Ctrl+Enter键可以直接提交]

相关文章:
编译调试CSLA .NET Framework v1.5
Castle 开发系列文章
asp.net控件开发基础(1)
驱动程序开发流程 (初学者适用)
编译第一个驱动程序笔记
“在系统启动时至少有一个服务或驱动程序产生错误”解决办法

相关链接:
程序员的网上家园
Java程序员如何轻松留学美国
这里有程序员必听的音乐100首
一个连英语都不会的.NET程序员能走多远?
想知道博客园有多少美女程序员吗?
移山之道-VSTS软件开发指南
道不远人-解析ASP.NET 2.0 控件开发

所属分类的其他文章:
[转]驱动开程序发—安装(6)
[转]驱动程序开发—编译正传(5)
[转]驱动程序开发—Hello Word(3)
[转]驱动程序开发—工具篇(2)
[转]驱动程序开发－概述(1)

最新IT新闻:
谷歌在企业版Google Apps中整合视频共享功能
联想ThinkPad X61存在严重散热问题
雅虎拟于9月29日关闭旗下社交网站Mash
2008年9月2日科技博客精选
Myspace推出新手机版欧洲社交网站

博客园新闻频道 博客园首页 社区