

2021/04/21_Windows32位内核_第1课_运行模式、驱动程序的编写

笔记本: Windows32位内核
创建时间: 2021/4/21 星期三 15:18
作者: ileemi
标签: 运行模式以及驱动程序的编写

- [保护模式](#)
- [驱动程序的编写](#)

保护模式

1. **实模式** (Dos、Windows NT3.1) : 8086 CPU (16位) , 单任务系统 (没有线程的概念, 系统一次只能运行一个应用程序) 。操作系统以及应用程序操作硬件 (CPU、内存、硬盘等) 没有限制, 都可以对其进行访问。操作系统和应用程序在同一个等级, 权限一致。**存在安全问题**: 恶意应用程序存在不小心修改操作系统的代码的安全问题。

- **保护模式** (32位CPU才开始有, 比如80386) : 为操作系统, 应用程序设置权限, 主要为了保护硬件, 保护模式 (为硬件划分等级) 是由CPU提供的功能、由操作系统和硬件共同完成。除了操作系统, 别的应用程序无法操控硬件。之前的CPU没有保护模式的概念, 现在CPU有保护模式的概念。

Inter CPU 权限一般有4级 (不同的CPU有不同的等级定义) : ring0~ring3, 最低级 (ring3) 的给应用程序, 剩下的给操作系统。操作系统负责资源的分配, CPU负责权限的检测。

操作系统向应用程序提供一个接口 (系统调用 system call) , 硬件厂家通过接口去实现硬件对应的驱动 (操作硬件的代码) 。应用程序通过接口向操作系统进行请求操作 (操作系统进行判断并执行相应的操作) 。

保护模式主要解决的问题:

- 权限问题
- 程序内存隔离问题 (硬件和操作系统共同完成)
- 允许多任务 (在以前由操作系统进行切换, 效率低)
- **虚拟8086模式**: 可以在保护模式下模拟运行**实模式**的代码 (在保护模式下运行16位的代码) , 主要来兼容老程序。

Rootkit: 通过加载特殊的驱动, 修改系统内核, 进而达到隐藏信息的目的。

软件开发者可以通过驱动开发进入内核。后来的操作系统 (安卓、ios) 改为静态链接驱动代码。

驱动程序的编写

DDK (Driver Developer Kit) : 驱动开发包

WDK (Windows Driver Kit) : 是一种完全集成的驱动程序开发系统, 它包含 Windows Driver Development Kit (DDK), 用于测试 Windows 驱动器的可靠性和稳定性。

[WDK 微软官方文档](#)

[Kernel 微软官方文档](#)

驱动文件通过 "makefile" 和 "sources" 两个配置文件来决定编译对应类型的驱动文件, 写换到工程对应的目录下, 打开命令行输入 `build` 即可, 会生成对应的 `.sys` 文件。之后在对应版本的操作系统中通过驱动加载工具将驱动进行安装。驱动安装后, 可以随时的启动和停止。安全模式启动操作系统, 操作系统只会加载系统的驱动。驱动中一般没有 UI 操作。

代码示例:

```
// 硬件驱动 wdm.h、内核驱动 ntddk.h
#include <ntddk.h>

// 卸载驱动
void DriverUnload(struct _DRIVER_OBJECT* DriverObject) {
    DbgPrint("[51asm] Unload");
}

// 驱动入口函数
NTSTATUS DriverEntry(struct _DRIVER_OBJECT* DriverObject,
PUNICODE_STRING RegistryPath) {
    // 代码拥有 ring0 权限

    //char* p = NULL;
    DbgPrint("[51asm] DriverEntry Hello WDK");
    DbgPrint("[51asm] DriverEntry DriverObject:%p", DriverObject);
    // *p = 1; // 会导致加载该驱动的操作系统出现蓝屏

    // 注册卸载函数
    DriverObject->DriverUnload = DriverUnload;

    // 按约定, 成功返回 STATUS_SUCCESS
    return STATUS_SUCCESS;
}

// sources 文件
TARGETNAME=Hello
TARGETTYPE=DRIVER
SOURCES=hello.c
```







操作如下图所示：

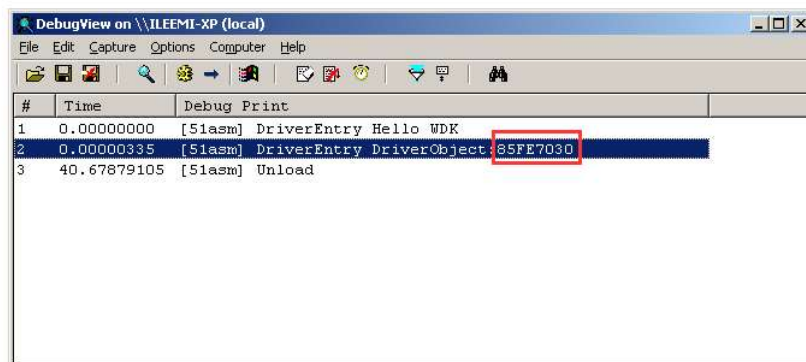
```
管理员: Windows XP x86 Checked Build Environment

C:\Users\ileemi\Desktop\Works\Kerner32>build
BUILD: Compile and Link for x86
BUILD: Loading c:\winddk\7600.16385.1\build.dat...
BUILD: Computing Include file dependencies:
BUILD: Start time: Thu Apr 22 11:15:53 2021
BUILD: Examining c:\users\ileemi\desktop\works\kerner32 directory for files to c
ompile.
      c:\users\ileemi\desktop\works\kerner32 Invalidating OACR warning log for 'ro
ot:x86chk'
BUILD: Saving c:\winddk\7600.16385.1\build.dat...
BUILD: Compiling and Linking c:\users\ileemi\desktop\works\kerner32 directory
Configuring OACR for 'root:x86chk' - <OACR on>
_NT_TARGET_VERSION SET TO WINXP
Compiling - hello.c
Linking Executable - objchk_wxp_x86\i386\hello.sys
BUILD: Finish time: Thu Apr 22 11:15:54 2021
BUILD: Done

3 files compiled - 1 Warning
1 executable built
```

在Win XP中加载驱动：

	_objects.mac	MAC 文件	1 KB
	hello.obj	OBJ 文件	17 KB
	hello.obj.oacr.root.x86chk.pft.xml	XML 文档	1 KB
	Hello.pdb	PDB 文件	123 KB
	Hello.sys	系统文件	3 KB
	vc90.pdb	PDB 文件	100 KB



内核驱动必须通过一个三环的程序调用API进行安装、启动、停止、卸载。
硬件驱动的安装可以通过脚本文件进行安装