

# 操作系统及安全设计

《操作系统及安全》配套实验  
信安系操作系统课程组

2019年11月

1



## 操作系统设计实验系列（四） 让操作系统走进保护模式



武汉大学

2

2



## 一、实验目标

- 如何从软盘读取并加载一个Loader程序到操作系统，然后转交系统控制权
- 对应章节：第四章



武汉大学

3

3



## 二、本次实验内容


1. 向软盘镜像文件写入一个你指定的文件，手工读取在磁盘中的信息
2. 在软盘中找到指定的文件，读取其扇区信息
3. 将指定文件装入指定内存区，并执行
4. 学会在bochs中使用xxd读取反汇编信息



武汉大学

4

4



武汉大学

5

### 三、完成本次实验要回答的问题

1.FAT12格式是怎样的？

2.如何读取一张软盘的信息

3.如何在软盘中找到指定的文件

4.如何在系统引导过程中，从读取并加载一个可执行文件到内存，并转交控制权？

5.为什么需要这个Loader程序不包含dos系统调用？

5



武汉大学

6

### 四、需了解的知识

#### FAT12基本概念

- 扇区Sector、簇Cluster、分区Partition

- 引导扇区：0号，

内有BPB（BIOS Parameter Block）

2879

数据区（长度非固定）

根目录区（长度非固定，需计算）

18

FAT2

10

FAT1

9

1

0

引导扇区

扇区号

名称	偏移	长度	内容	Orange9的值
BPB_jmpBoot	0	3	一个短跳转指令	jmp LABEL_START nop
BPB_OEMName	3	8	厂商名	"ForrestY"
BPB_BytsPerSec	11	2	每扇区字节数	0x200
BPB_SecPerClus	13	1	每簇扇区数	0x1
BPB_RsvdSecCnt	14	2	Boot记录占用多少扇区	0x1
BPB_NumFATs	16	1	共有多少FAT表	0x2
BPB_RootEntCnt	17	2	根目录文件数最大值	0x80
BPB_TotSec16	19	2	扇区总数	0x240
BPB_Media	21	1	介质描述符	0xF0
BPB_FATs16	22	2	每FAT扇区数	0x9
BPB_SecPerTrk	24	2	每磁道扇区数	0x12
BPB_NumHeads	26	2	磁头数（面数）	0x2
BPB_HiddSec	28	4	隐藏扇区数	0
BPB_TotSec32	32	4	如果BPB_TotSec16是0，由这个值记录扇区数	0
BPB_DrvNum	36	1	中断13的驱动器号	0
BPB_Reserved1	37	1	未使用	0
BPB_BootSig	38	1	扩展引导标记（z9h）	0x29
BPB_VolID	39	4	卷序列号	0
BPB_VolLab	43	11	卷标	"OrangeSO.02"
BPB_FileSysType	54	8	文件系统类型	"FAT12"
引导代码及其他	62	448	引导代码、数据及其他填充字符等	引导代码（剩余空间被0填充）
结束标志	510	2	0xAA55	0xAA55

6

## 四、需了解的知识

### FAT12基本概念

- 根目录区的条目格式,32字节
  - BPB\_RootEntCnt
  - DOS文件名的8.3格式

名称	偏移	长度	描述
DIR_Name	0	0xB	文件名8字节,扩展名3字节
DIR_Attr	0xB	1	文件属性
保留位	0xC	10	保留位
DIR_WrtTime	0x16	2	最后一次写入时间
DIR_WrtDate	0x18	2	最后一次写入日期
DIR_FstClus	0x1A	2	此条目对应的开始簇号
DIR_FileSize	0x1C	4	文件大小

- 根目录区扇区计算方法

$$RootDirSectors = \frac{(BPB\_RootEntCnt \times 32) + (BPB\_BytsPerSec - 1)}{BPB\_BytsPerSec}$$



武汉大学

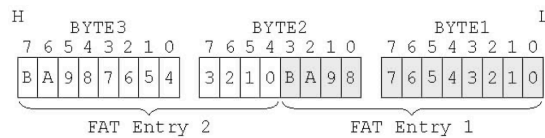
7

7

## 四、需了解的知识

### FAT12基本概念

- FAT项格式



- FAT项值指向下一个簇号
- 如果>=0xFF8,则表示末尾,如果==0xFF7,则坏簇



武汉大学

8

8

