Beijing Forest Studio
北京理工大学信息系统及安全对抗实验中心

计算机启动流程详解（传统BIOS版本）

Computer booting with BIOS

博士研究生 刘望桐

2018年05月09日

内容提要

- 背景知识
- BIOS
- MBR
- PBR、OS启动（略）
- 总结

- 基本掌握
  - 启动基本流程、问题自检
  - 磁盘工作原理
  - 硬盘分区原理
- 进阶掌握
  - BIOS原理
  - MBR结构及原理
  - 磁盘结构、磁盘分区、文件系统之间关系
  - 启动过程中的安全问题

背景知识

背景知识

- BOOT
  - Bootstrap(鞋带)-pull oneself up by one's bootstraps(拽着鞋带把自己拉起来)
  - 专指电子设备的启动、引导
- BOOT的矛盾
  - CPU只能从RAM（内存）里直接读取数据和指令，计算机启动前需要将指令和数据从磁盘中加载（拷贝）到RAM中
  - 加载指令和数据需要计算机启动后由CPU执行相应命令才能完成加载
  - 解决方法：ROM

背景知识

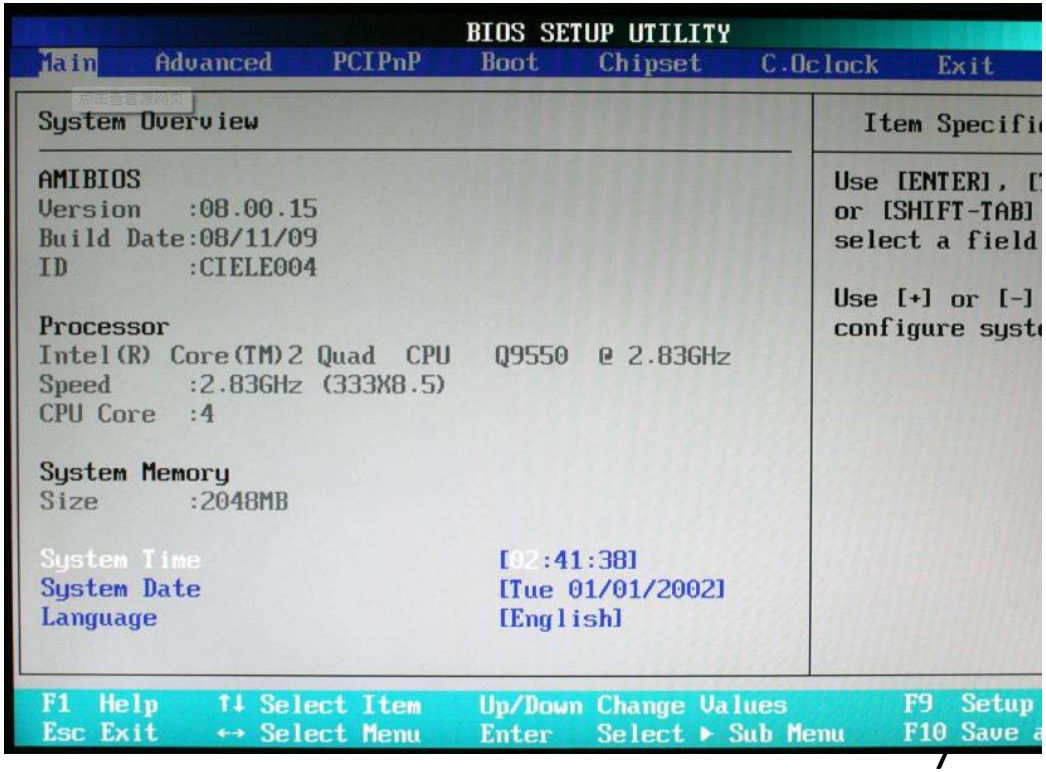
- EEPROM
  - Electrically Erasable Programmable Read-Only Memory，带电可擦可编程只读存储器
  - 被写入ROM中的程序、代码被称为“固件(Firmware)”
- 从ROM启动
  - 计算机启动时，CPU首先从ROM里读取指令和数据，由ROM里预先设置好的启动指令完成最初的启动工作
  - 第一条指令位于：0xFFFF0或0xFFFFFFF0

```
FFFFFFF0:  EA 5B E0 00 F0  jmp far ptr F000:E05B
```

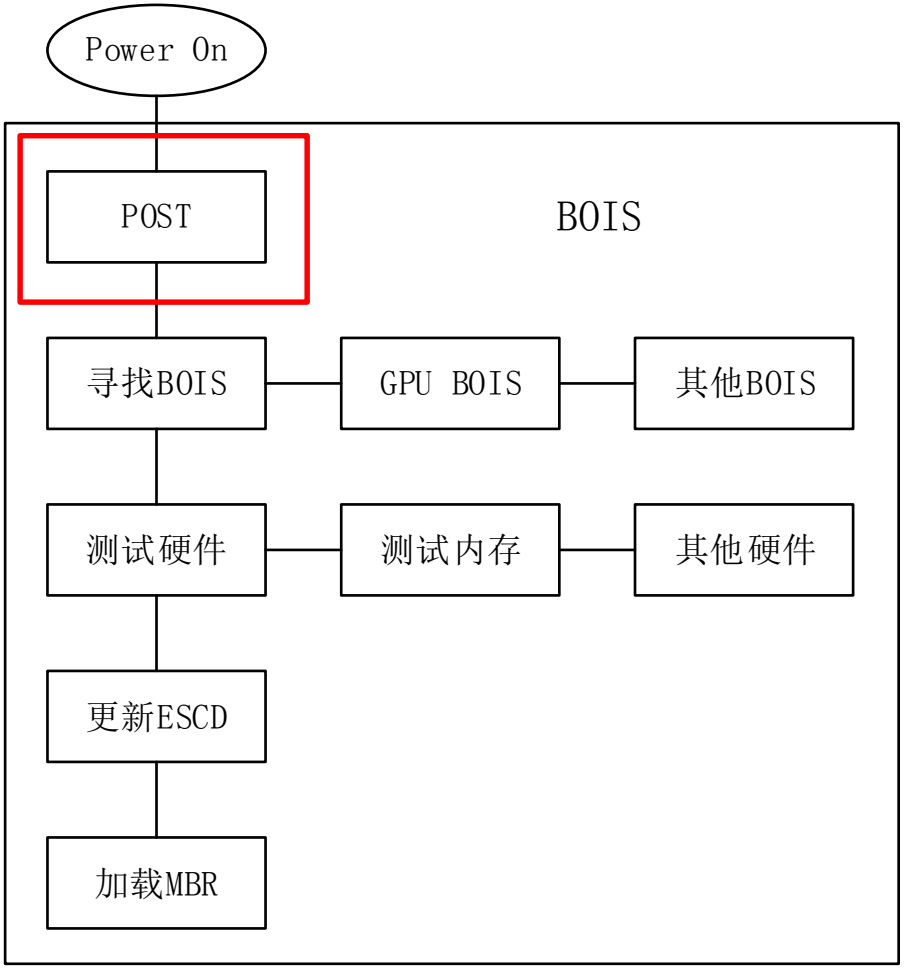
BIOS

BIOS

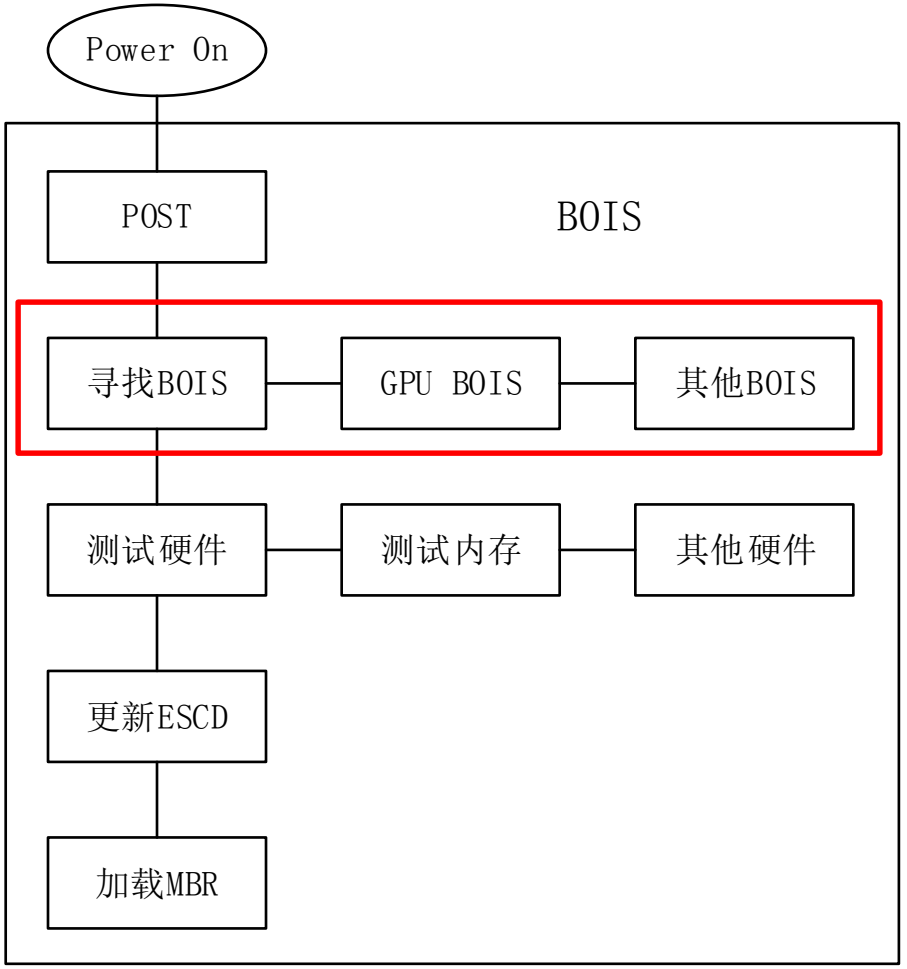
- BIOS——Basic Input/Output System，基本输入输出系统
  - 通常位于主板(Motherboard)的ROM中，负责计算机启动初期的各项管理、检查操作



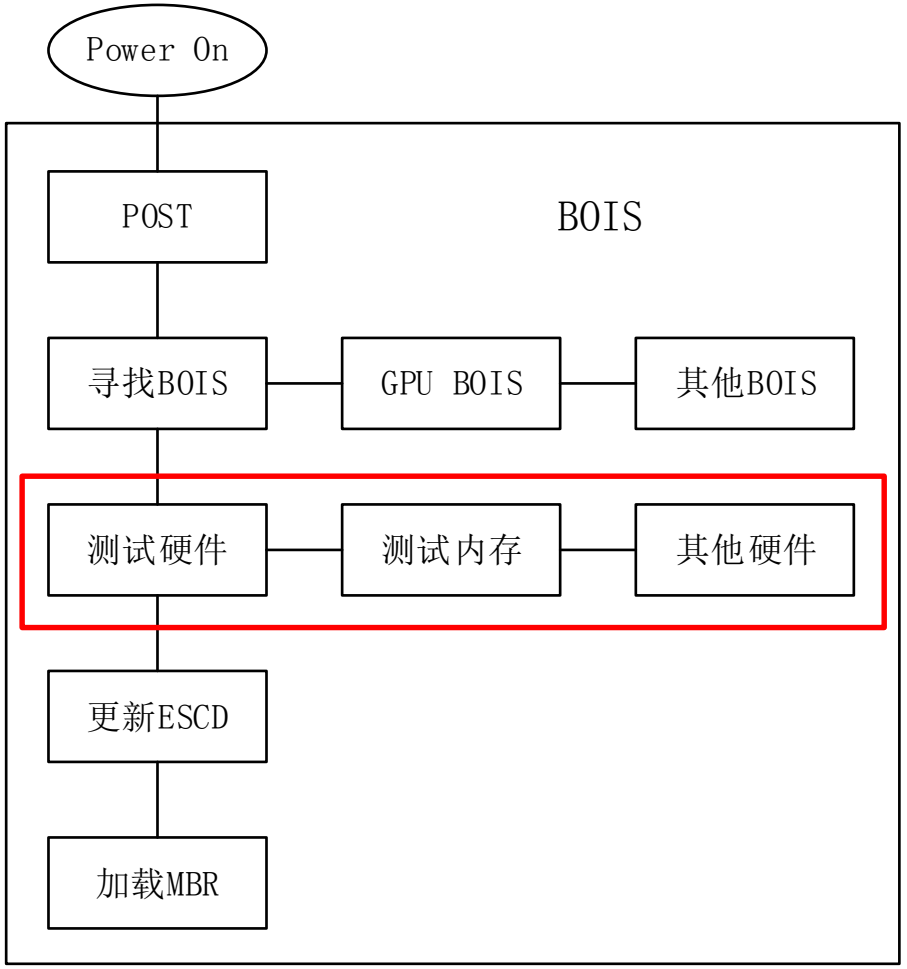
- POST
  - Power-On Self Test，加电后自检
  - 检测系统中一些关键设备是否存在和能否正常响应，例如内存和显卡等设备
  - 通过主板上的喇叭反馈检测结果



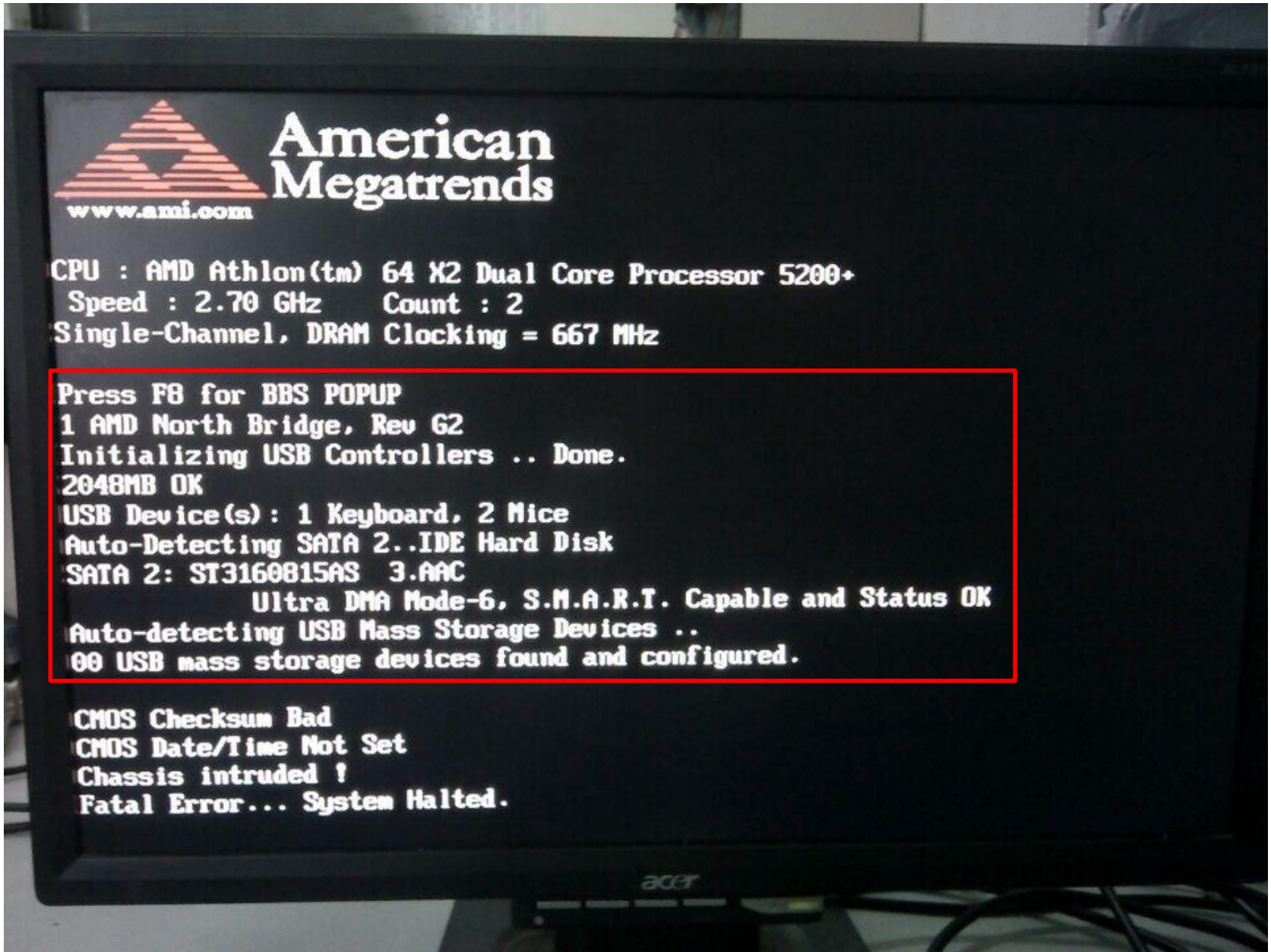
- 查找BIOS
  - 查找系统内其他硬件的BIOS并加载到内存中，完成对该硬件设备的启动初始化
  - 后续的部分工作需要调用到对应硬件设备的BIOS中的相应代码
  - 最重要的是找到显卡（GPU）的BIOS



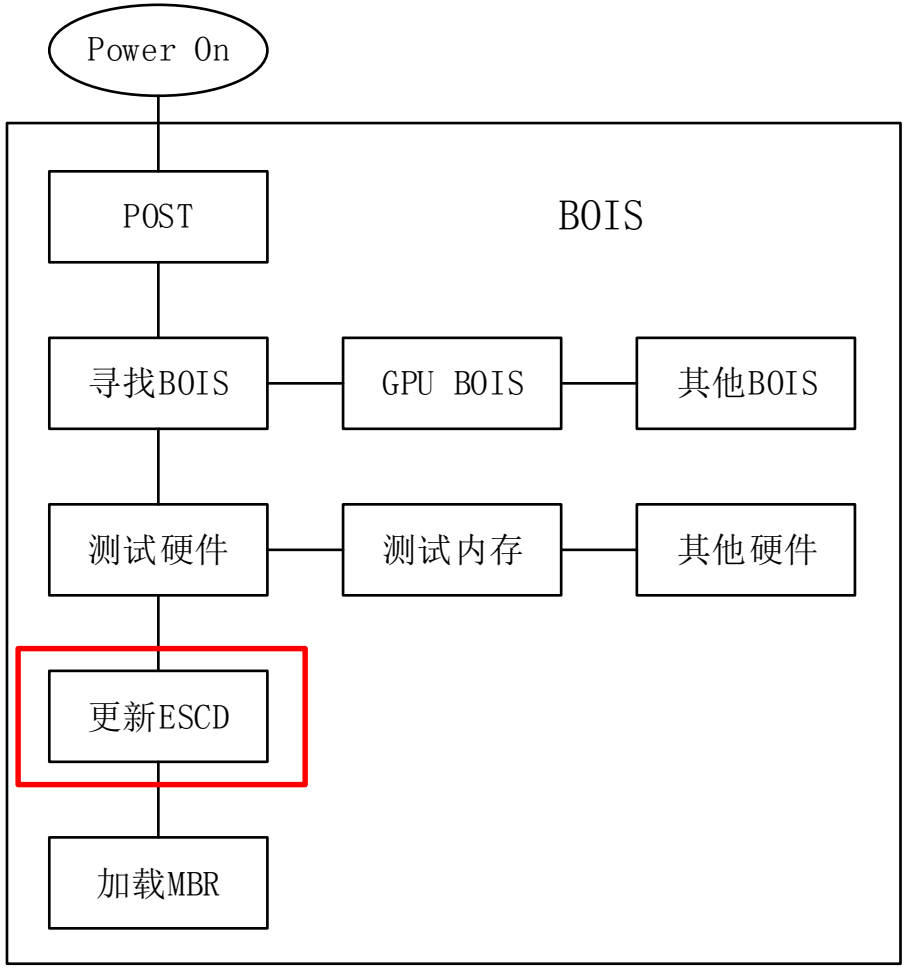
- 硬件测试
  - 测试包括内存在内的各硬件设备是否能正常工作、型号配置如何
  - 主要测试对象为内存、鼠标键盘、显示器等即插即用硬件
  - 对每个设备需要分配中断号、DMA通道、I/O端口等



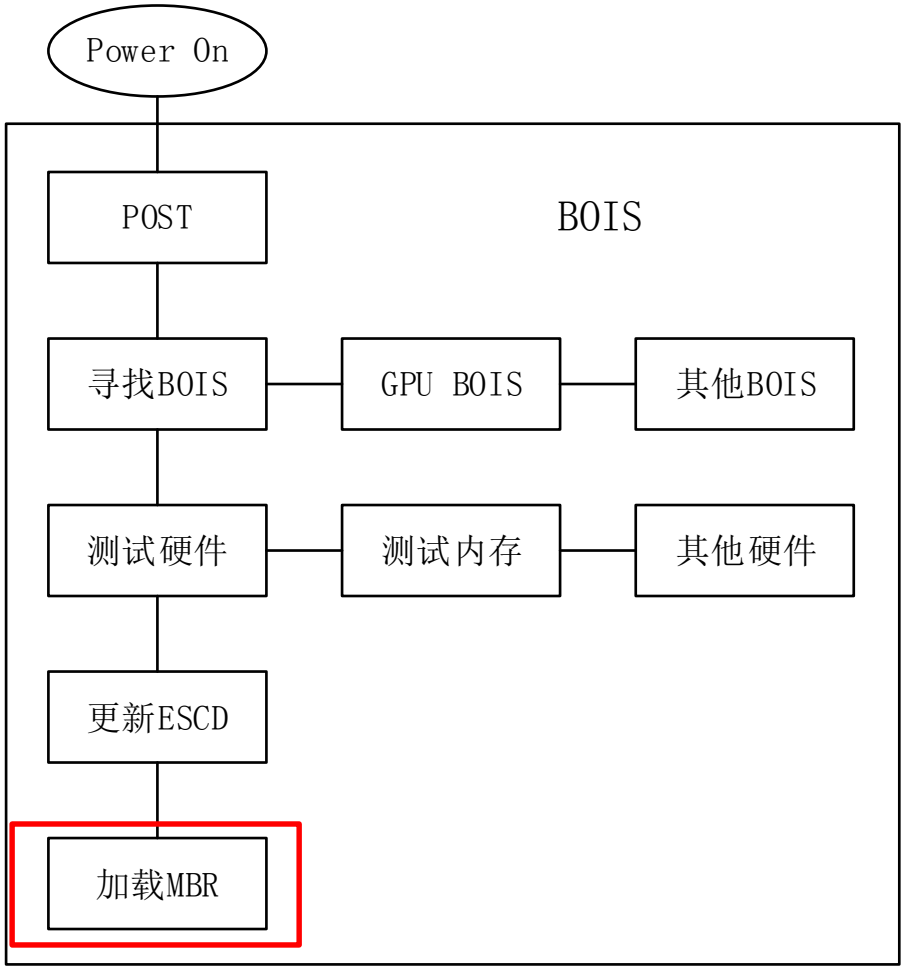
BIOS


American Megatrends
www.ami.com
CPU : AMD Athlon(tm) 64 X2 Dual Core Processor 5200+
Speed : 2.70 GHz Count : 2
Single-Channel, DRAM Clocking = 667 MHz
Press F8 for BBS POPUP
1 AMD North Bridge, Rev G2
Initializing USB Controllers .. Done.
2048MB OK
USB Device(s): 1 Keyboard, 2 Mice
Auto-Detecting SATA 2..IDE Hard Disk
SATA 2: ST3160815AS 3.AAC
Ultra DMA Mode-6, S.M.A.R.T. Capable and Status OK
Auto-detecting USB Mass Storage Devices ..
00 USB mass storage devices found and configured.
CMOS Checksum Bad
CMOS Date/Time Not Set
Chassis intruded !
Fatal Error... System Halted.
acer

- 更新ESCD
  - Extended System Configuration Data，扩展系统配置数据
  - 记录计算机各类扩展配置硬件信息（例如PCI扩展槽上的设备）的数据，供操作系统启动时读取



- 将硬盘中的MBR加载到内存中，并执行其中的命令，启动流程转移到MBR阶段，BIOS阶段结束



- UEFI
  - Unified Extensible Firmware Interface，统一可扩展固件接口
  - 新型的用以统一包括传统BIOS在内的各种ROM固件的接口格式
  - 特点
    - 有图形界面
    - 主要有由C语言编写
    - 运行速度更快
    - 使用GPT分区格式
    - 支持文件系统
  - 可能需要手动开启/关闭

MBR

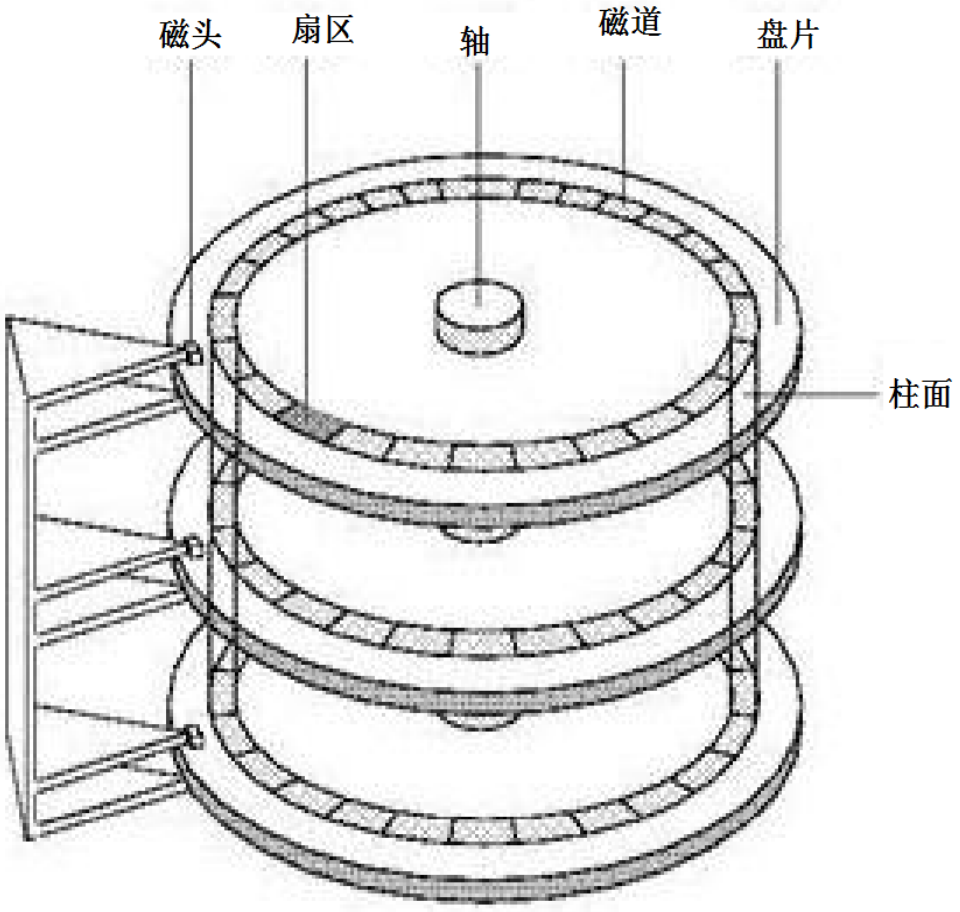
MBR

- MBR
  - Main Boot Record，主引导记录
  - 位于外部存储设备（如硬盘）的起始位置，保存着和操作系统启动相关代码
  - 一共512字节
  - 最后2字节为主引导记录签名（0x55AA）
- 从BIOS到MBR
  - BIOS检查所有存储器上的起始512字节中的最后2字节，如果是0x55AA，那么说明这个外部存储设备中有MBR，能够引导计算机启动

MBR

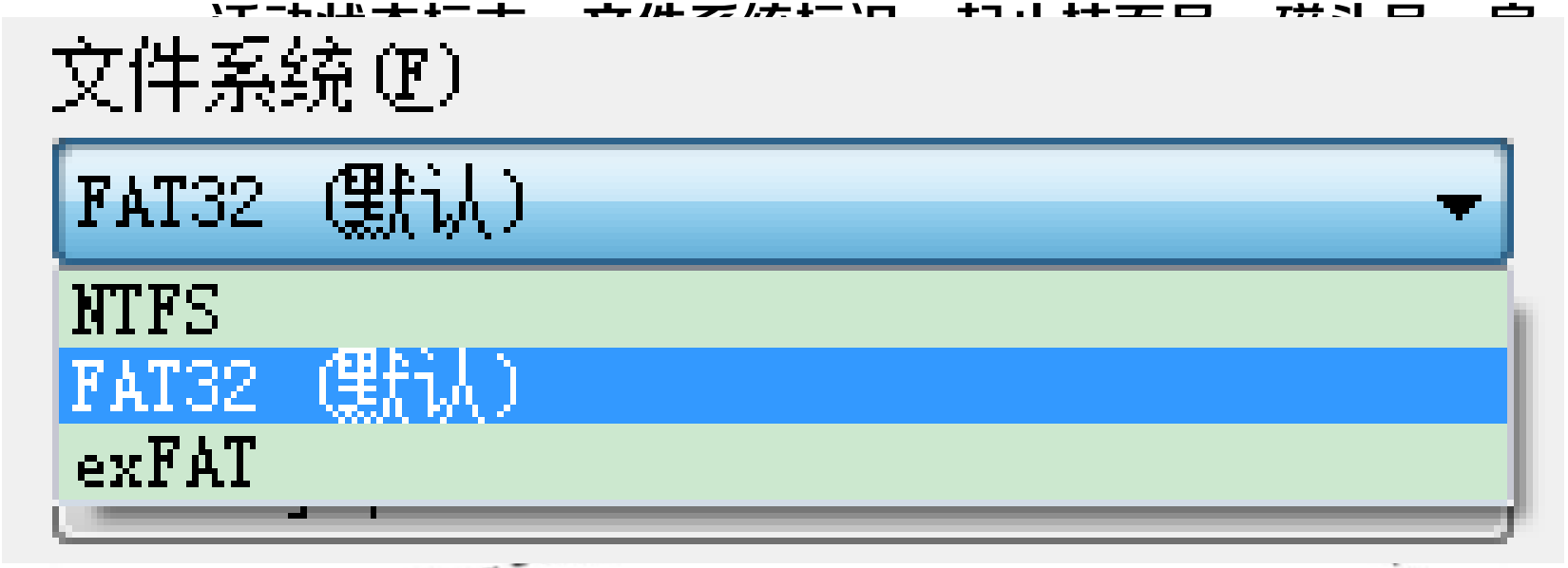
- MBR的主要工作是从自身所在存储设备上找到操作系统的位置并将其加载到内存中
  - 大部分情况下，MBR的内容就是在安装操作系统时安装程序设置的
  - 安装多系统时所需安装的“启动器”（如Grub）会替换MBR中的内容，在启动时根据用户的选择启动不同的操作系统
- MBR的另一个重要的功能是储存所在设备的分区信息
  - 后续启动流程中都需要用到分区信息
  - MBR自身功能有限，“寻找操作系统”的过程本质是“寻找操作系统所在分区”的过程

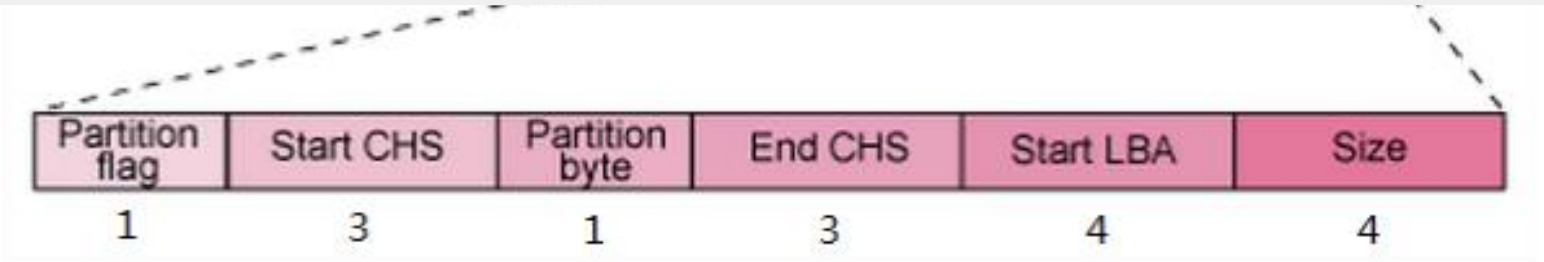
- 磁盘的存储结构
  - 单位：扇区，512字节
    - 新型号磁盘一个扇区有4K甚至更多
  - 一次磁盘读取操作至少读取一个扇区
  - 定位一个扇区可以通过“柱面(Cylinder)+磁头(Heads)+扇区(Sector)”的CHS编号，或通过线性的LBA(Logical Block Address)逻辑扇区号
  - 其他类型的硬盘（固态硬盘）也兼容了这一编号方式



MBR

- MBR的512字节中，除了初始的446字节的引导代码外，还包含了对MBR所在磁盘的分区表（partition table）
  - 分区表中的信息包括：



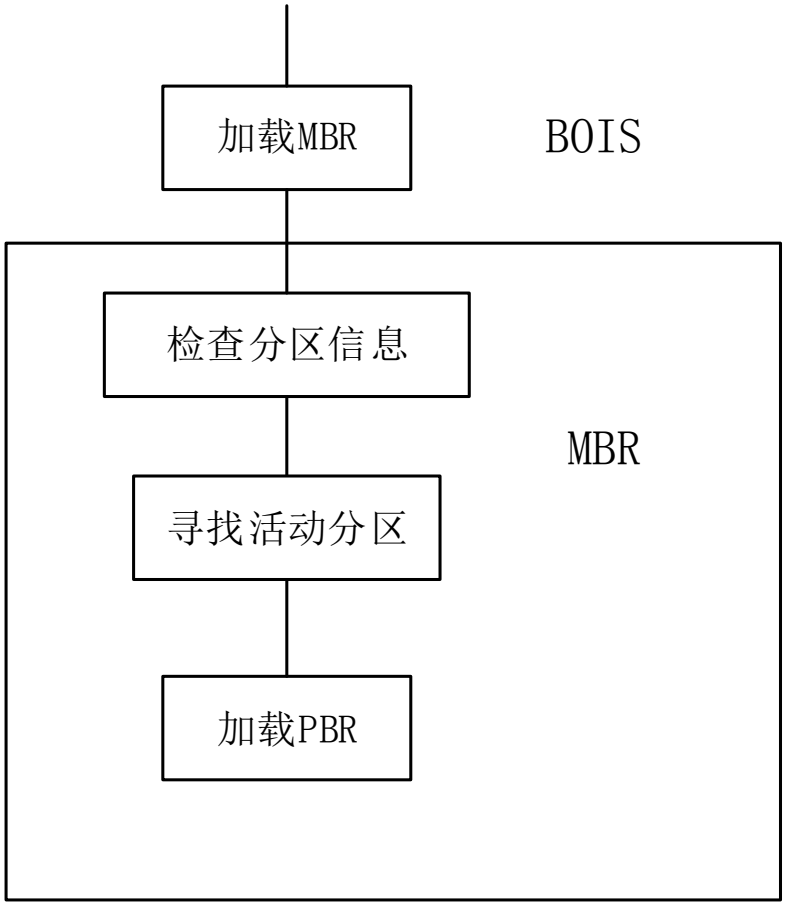


MBR

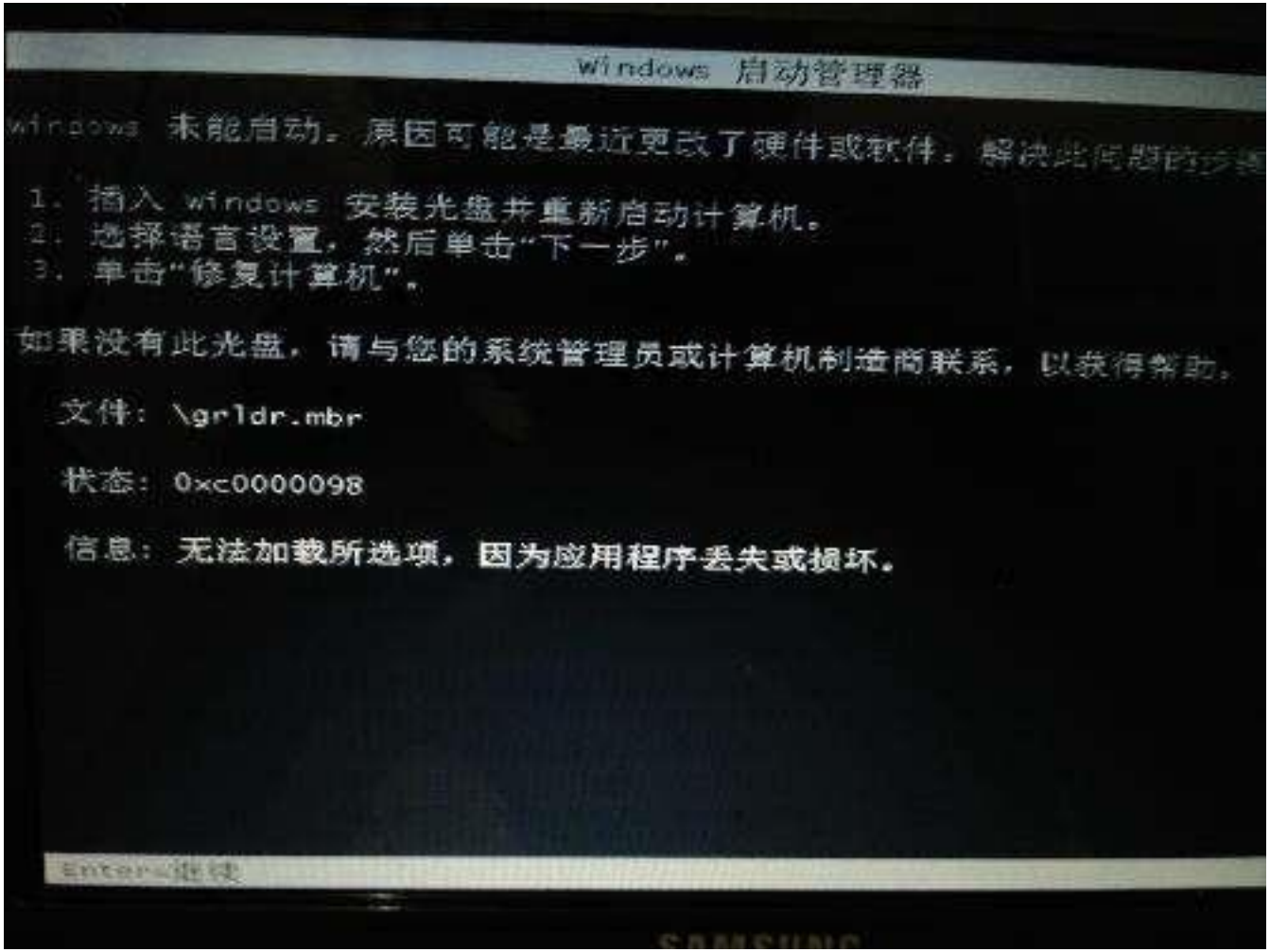
- MBR的分区表格式带来如下特性
  - 只有能4个分区
  - 单个分区内空间连续，分区首尾相接
  - 由于StartLBA和SIZE都只有4字节(32bit)，因此每个分区以及整个磁盘最多512*2^32=2^41=2T字节
- 扩展分区+逻辑分区
  - 解决只有4个分区的问题
- GTP分区表
  - 和MBR分区表不同的全新的分区表结构
  - 最大支持2^32个分区
  - 最大支持8EB硬盘和分区大小（TB->PB->EB）

MBR

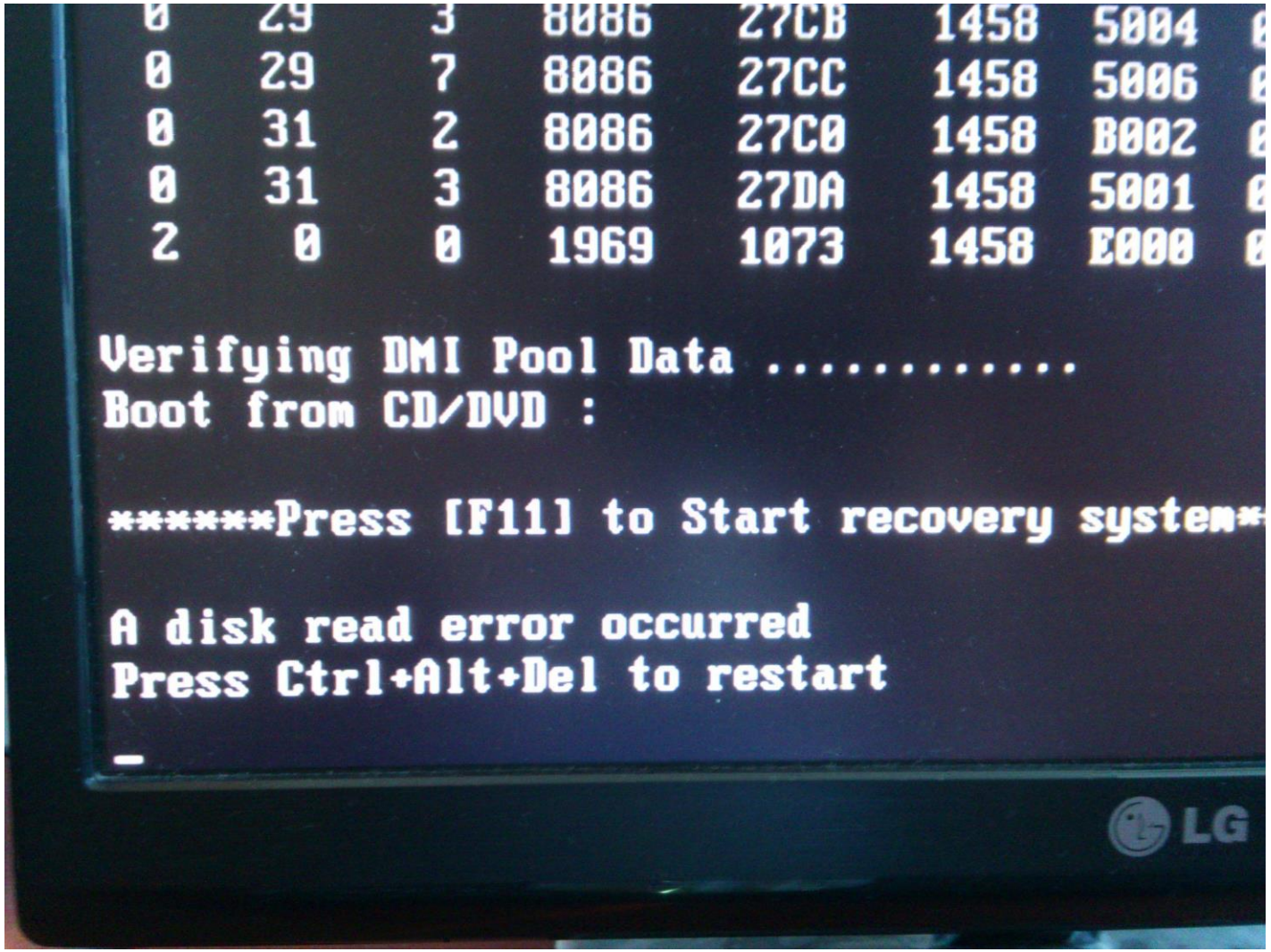
- MBR程序段的主要功能如下：
  - 检查硬盘分区表是否完好
  - 在分区表中寻找可引导的“活动”分区
  - 加载该分区第一个扇区内的内容——PBR，分区引导记录，MBR阶段结束，进入PBR阶段



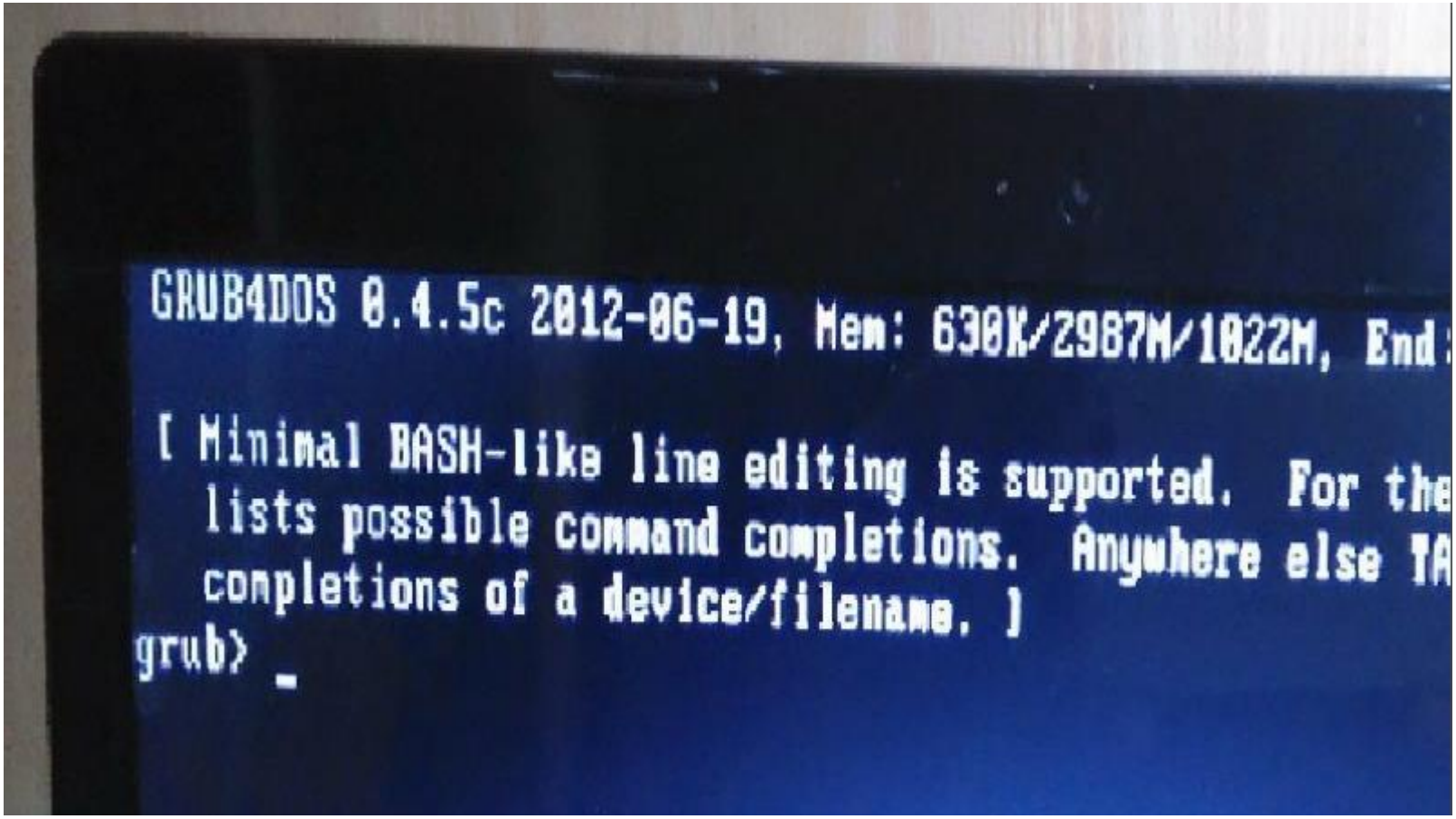
MBR损坏


Windows 启动管理器
Windows 未能启动。原因可能是最近更改了硬件或软件。解决此问题的步骤
1. 插入 Windows 安装光盘并重新启动计算机。
2. 选择语言设置，然后单击“下一步”。
3. 单击“修复计算机”。
如果没有此光盘，请与您的系统管理员或计算机制造商联系，以获得帮助。
文件: \grldr.mbr
状态: 0xc0000098
信息: 无法加载所选项，因为应用程序丢失或损坏。
SAMSUNG

MBR损坏

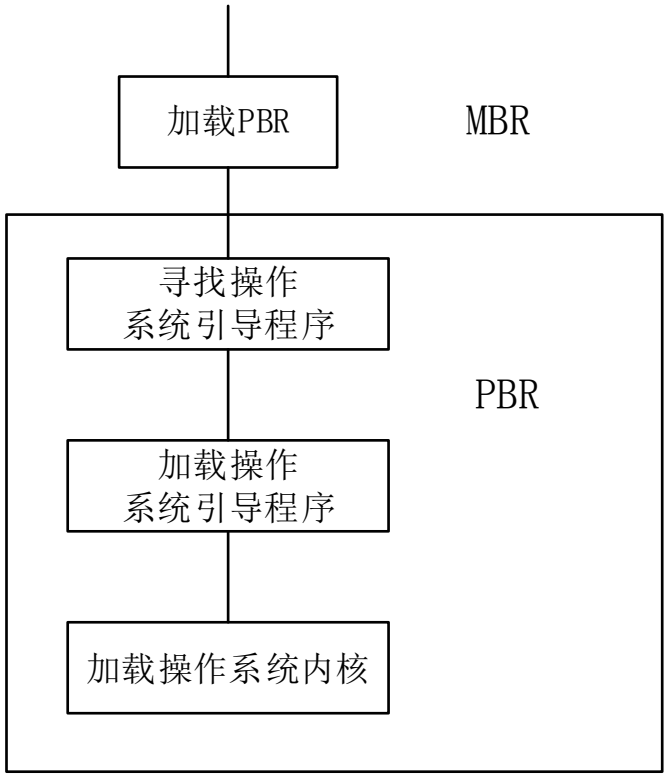

0 29 3 8086 27CB 1458 5004
0 29 7 8086 27CC 1458 5006
0 31 2 8086 27C0 1458 B002
0 31 3 8086 27DA 1458 5001
2 0 0 1969 1073 1458 E000
Verifying DMI Pool Data .....
Boot from CD/DVD :
******Press [F11] to Start recovery system**
A disk read error occurred
Press Ctrl+Alt+Del to restart
LG

MBR损坏


GRUB4DOS 0.4.5c 2012-06-19, Mem: 630K/2987M/1022M, End
[Minimal BASH-like line editing is supported. For the
lists possible command completions. Anywhere else TA
completions of a device/filename.]
grub>

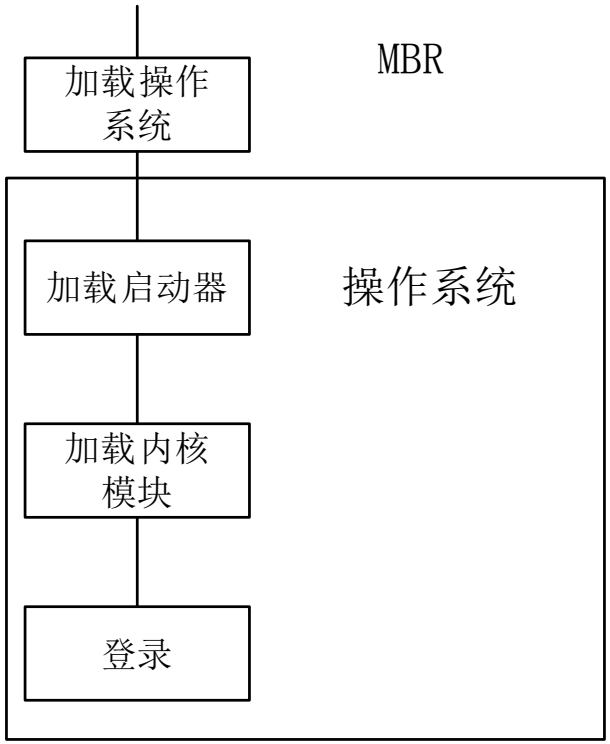
PBR、操作系统

- PBR
  - 分区引导记录，也被称为VBR、卷引导记录
  - 起始于所在分区的第一个扇区，但大小没有限制
- PBR的作用
  - PBR负责寻找并加载操作系统引导程序，最终启动整个操作系统
  - 操作系统引导程序和操作系统本身可以不在一个分区
  - 引导程序包括：
    - NTLDR（XP）
    - bootmgr（Win7以上）
    - grldr（Grub）



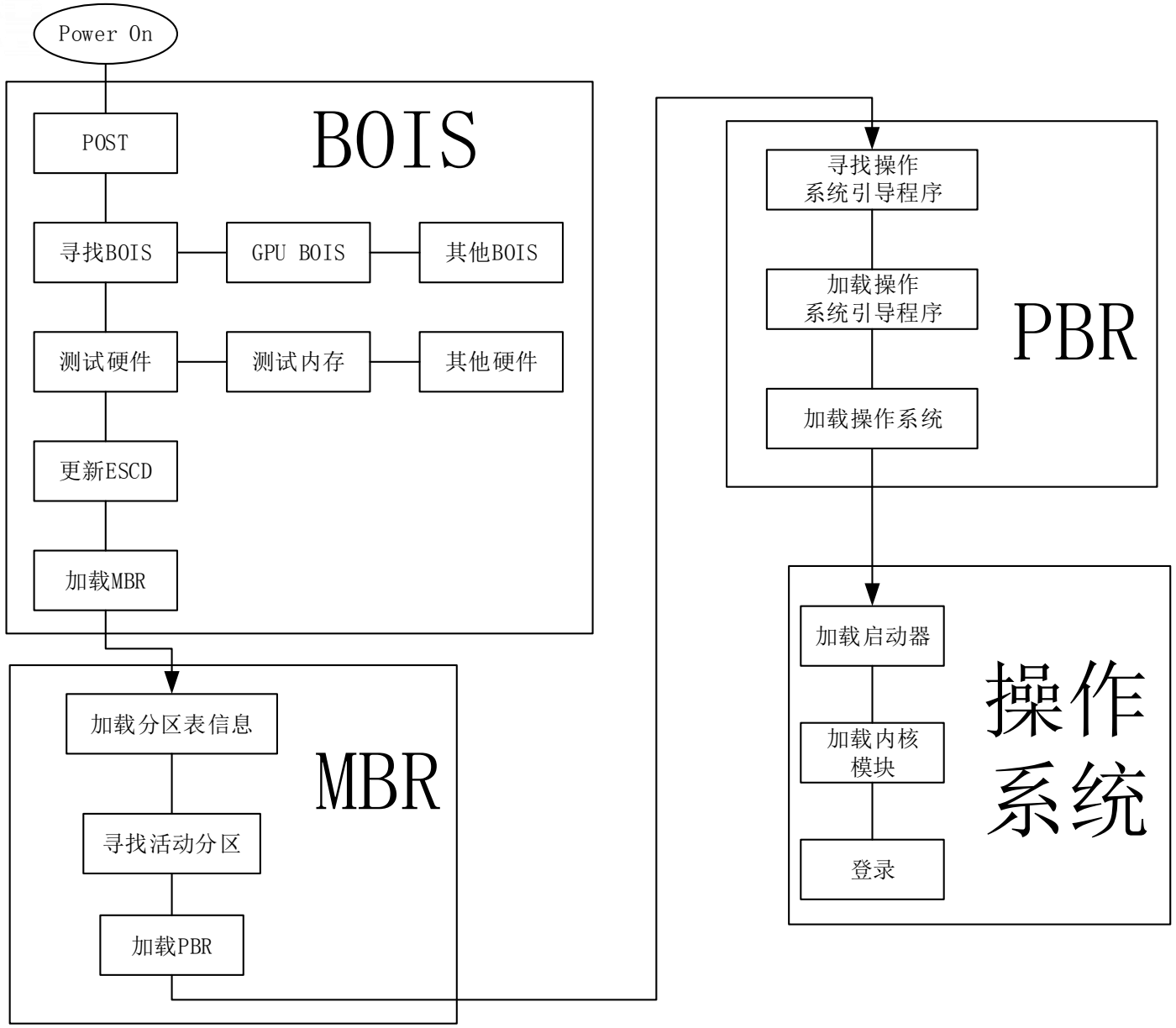
操作系统

- 操作系统的启动过程大部分情况下对用户是透明的
  - 看不见、无法干预
  - Linux系统启动时能够看到详细的启动过程
- 如果操作系统本身出现故障，会通过各种方式进行提示
  - 蓝屏（Windows内核崩溃）
  - 错误日志

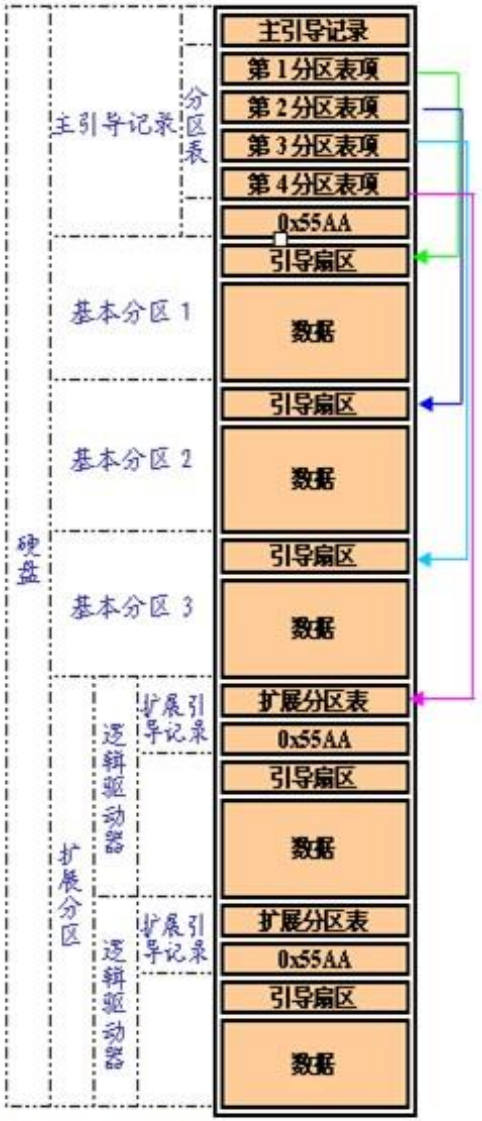


总结

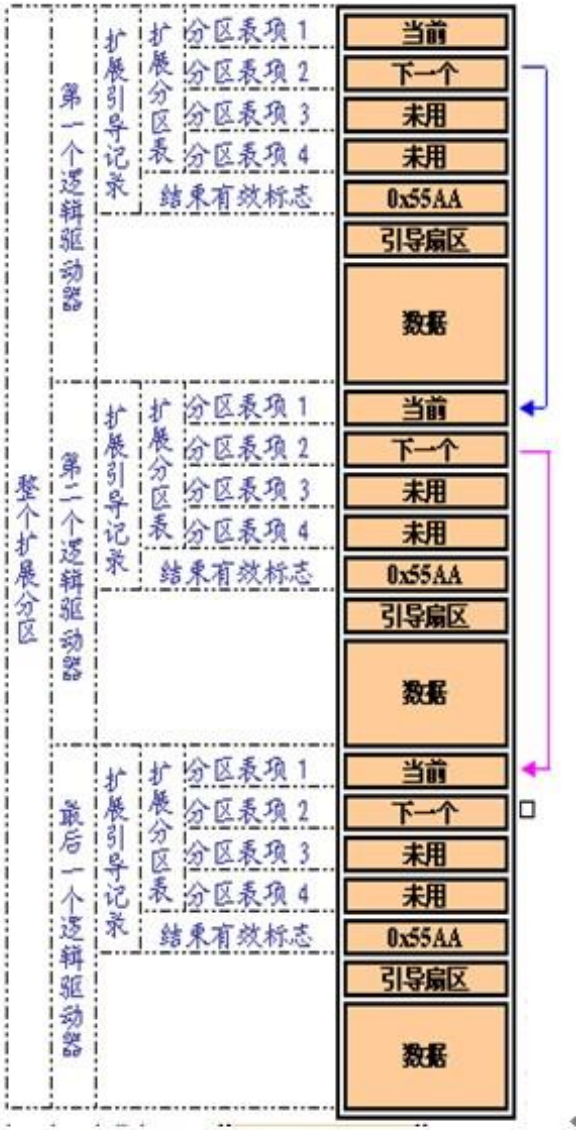
总结


Power On
BOIS
POST
寻找BOIS
GPU BOIS
其他BOIS
测试硬件
测试内存
其他硬件
更新ESCD
加载MBR
MBR
加载分区表信息
寻找活动分区
加载PBR
PBR
寻找操作
系统引导程序
加载操作
系统引导程序
加载操作系统
操作
系统
加载启动器
加载内核
模块
登录

扩展分区、逻辑分区



图表 3 分区结构图



图表 4 扩展分区表

Bootkit

- Bootkit
  - 通过感染以MBR为代表的计算机启动中使用到的数据信息，从而篡改计算机启动流程，在操作系统、杀毒软件启动前完成自身的破坏、隐蔽工作
  - 感染对象：
    - 操作系统Boot文件，硬盘中，直接可读写，易保护
    - MBR，硬盘中，直接可读写，不易保护
    - BIOS、UEFI，ROM中，不易直接读写，基本无法保护
  - 难点
    - 攻击方：不同操作系统启动流程差异较大，Bootkit兼容性差，破坏容易隐蔽难
    - 防御方：感染对象不易保护，感染后查杀困难

参考资料

- http://www.360doc.com/content/17/0107/03/18268484_620651307.shtml
- https://www.cnblogs.com/hopeworld/archive/2011/03/27/1997298.html
- http://www.blogfshare.com/mbr-dpt-ebr.html
- https://www.disktool.cn/jiaocheng/basic-partition.html

谢谢！

大成若缺，其用不弊。大盈若冲，其用不穷。大直若屈。大巧若拙。大辩若讷。静胜躁，寒胜热。清静为天下正。