



华中科技大学

HUAZHONG UNIVERSITY OF SCIENCE AND TECHNOLOGY

网络空间安全学院



2.2 系统引导与控制权

网络空间安全学院 慕冬亮

Email : dzm91@hust.edu.cn

2.2 系统引导与控制权

- 系统引导与恶意软件有何关系？

恶意软件如何再次获得控制权？

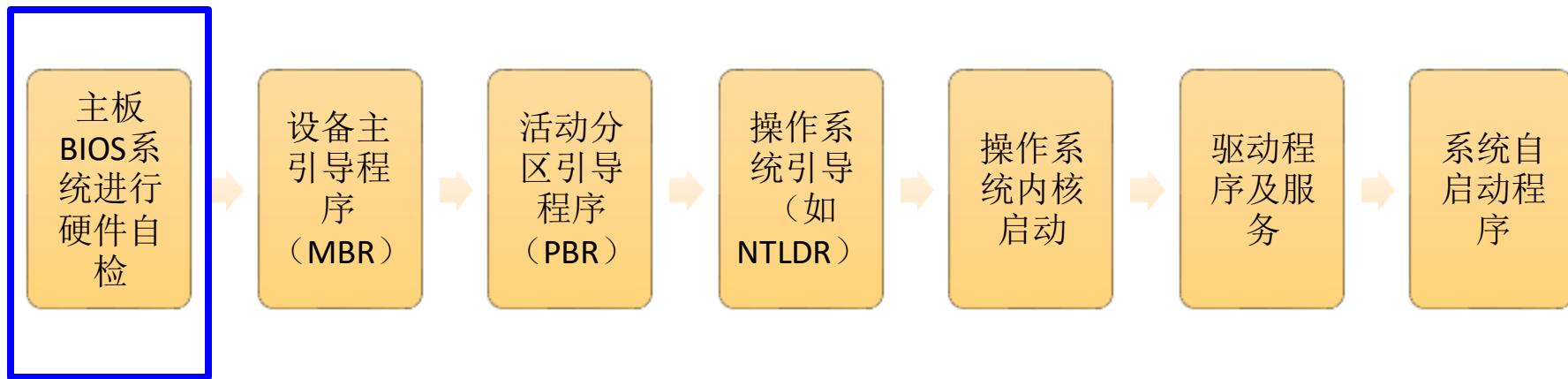
自身被结
束之后

操作系统
重启之后

操作系统
重装之后

硬盘更换
之后。。。

2.2 计算机系统引导过程



BIOS(Basic Input/Output System): 基本输入输出系统

MBR(Master Boot Record): 主启动记录

PBR(Partition Boot Record): 分区引导程序

NTLDR(NT Loader): Windows NT启动引导程序

BIOS: Basic Input and Output System

- “基本输入输出系统”，存储在主板BIOS Flash（或ROM）芯片。
- 为计算机提供最底层的、最直接的硬件设置和控制。



BIOS的自检与初始化工作

- 任务：检测系统中的一些关键设备（如内存和显卡等）是否存在和能否正常工作，进行初始化，并将控制权交给后续引导程序。
 - 显卡及其他相关设备初始化。
 - 显示系统BIOS启动画面，其中包括有系统BIOS的类型、序列号和版本号等内容。
 - 检测CPU的类型和工作频率，内存容量、并将检测结果显示在屏幕上。
 - 检测系统中安装的一些标准硬件设备及即插即用设备，这些设备包括：硬盘、CD-ROM、软驱、串行接口和并行接口等。
 - 根据用户指定的启动顺序从软盘、硬盘或光驱启动。
 - 如果从硬盘启动，则将控制权交给硬盘主引导程序。

系统自检



硬盘主引导程序

- 所在位置：
 - MBR（Master Boot Record）硬盘第一个扇区。
- 主要功能：
 - 通过主分区表中定位活动分区
 - 装载活动分区的引导程序，并移交控制权。

活动分区引导程序

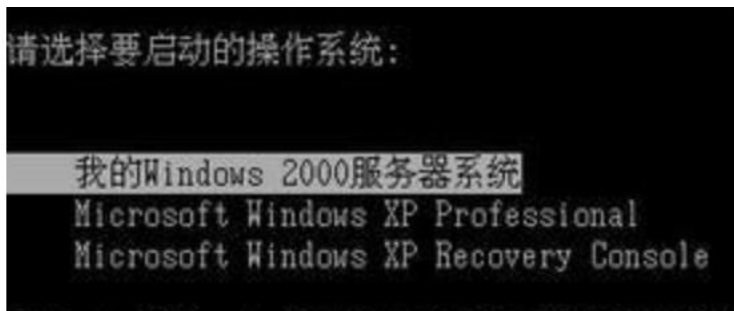
- 所在位置：
 - DBR（DOS Boot Record），或称OBR（OS Boot Record），或称分区引导记录（PBR，Partition Boot Record）
 - 分区的第一个扇区
- 功能：
 - 加载操作系统引导程序
 - 如Windows XP系统的NTLDR



```
NTLDR is missing
Press Ctrl+Alt+Del to restart
-
```


操作系统引导—以Windows NTLDR为例

- 将处理器从16位内存模式拓展为32位（64位）内存模式
- 启动小型文件系统驱动，以识别FAT32和NTFS文件系统
- 读取boot.ini，进行多操作系统选择（或hiberfil.sys恢复休眠）
- 检测和配置硬件（NT或XP系统，则运行NTDETECT.COM，其将硬件信息提交给NTLDR，写入“HKEY_LOCAL_MACHINE”中的Hardware中）



系统内核加载

- NTLDR加载内核程序NTOSKRNL.EXE以及硬件抽象层HAL.dll等。
- 读取并加载HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet 下指定的驱动程序。
- NTLDR将把控制权传递给NTOSKRNL.EXE，至此引导过程将结束。

Windows系统装载

1. 创建系统环境变量
2. 启动win32.sys（Windows子系统的内核模式部分）。
3. 启动csrss.exe（Windows子系统的用户模式部分）。
4. 启动winlogon.exe等

屏幕显示：Windows logo 界面和进度条



Windows系统装载—登陆阶段

1. 启动需要自动启动的Windows服务
2. 启动本地安全认证Lsass.exe
3. 显示登录界面等



Windows登陆之后

- 系统启动当前用户环境下的自启动项程序
 - 注册表特定键值
 - 特定目录（如startup）等
- 用户触发和执行各类应用程序
 - 如IE、QQ、Office等

Windows系统引导过程

1. 加电，主板BIOS自检程序开始运行
2. 硬盘主引导记录被装入内存，主引导程序开始执行
3. 活动分区的引导扇区被装入内存并执行，NTLDR从引导扇区被装入并初始化
4. NTLDR将处理器的从16位实模式改为32位平滑内存模式
5. NTLDR加载小文件系统驱动程序。
6. NTLDR读boot.ini文件，用户选择操作系统。
7. NTLDR装载所选操作系统
8. Ntldr.com 搜索计算机硬件并将列表传送给NTLDR，以便将这些信息写进\HKEY_LOCAL_MACHINE \HARDWARE中。
9. NTLDR装载Ntoskrnl.exe, Hal.dll和系统信息集合。
10. Ntldr搜索系统信息集合，并装载设备驱动。
11. Ntldr把控制权交给Ntoskrnl.exe，这时，启动引导程序结束
12. Windows开始装载
13. 执行驱动程序及服务
14. 系统执行自启动程序
15. 用户触发执行程序

系统引导与恶意软件的关联

- 系统引导与恶意软件有何关系？
 - 恶意软件在植入系统之后，如何再次获得控制权？
 - 在计算机系统引导阶段获得控制权
 - Bootkit: BIOS木马、MBR木马等，可用于长期驻留在系统；早期的DOS引导区病毒等。
 - CIH病毒
 - 在操作系统启动阶段获得控制权
 - 最常见的恶意软件启动方法，多见于独立的恶意软件程序。
 - 在应用程序执行阶段获得控制权
 - 最常见的文件感染型病毒启动方法。