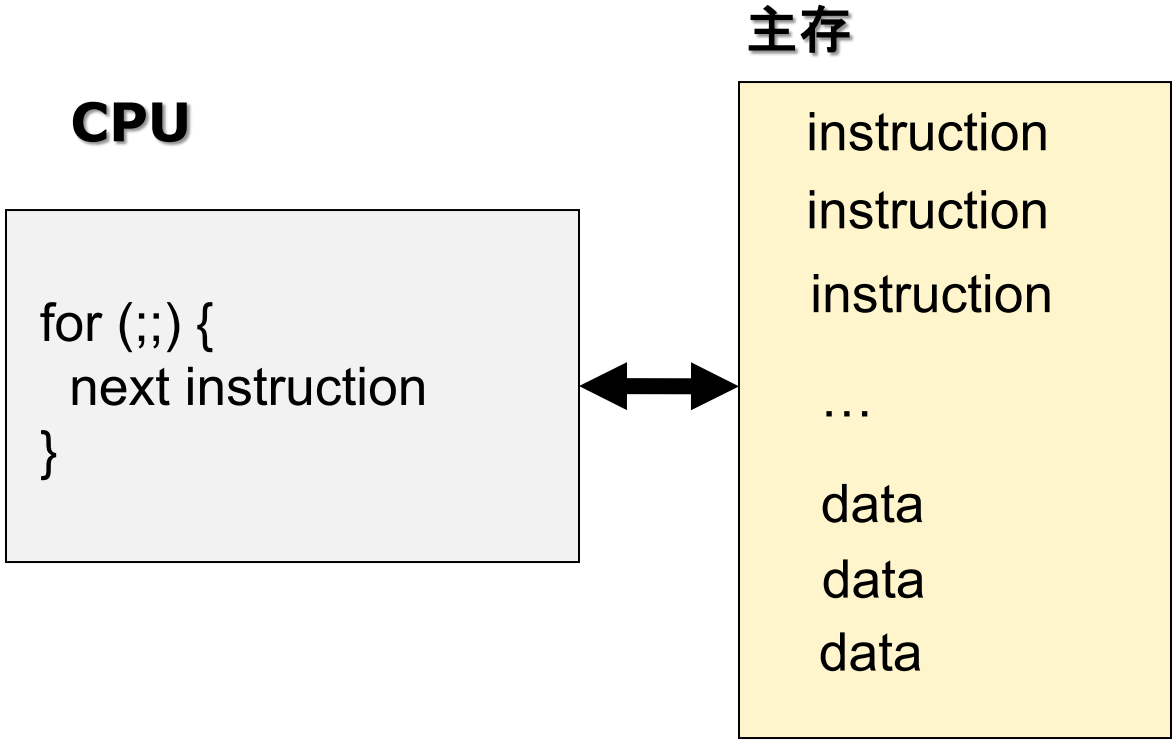
第2章 进程与线程

2.2 计算机的启动

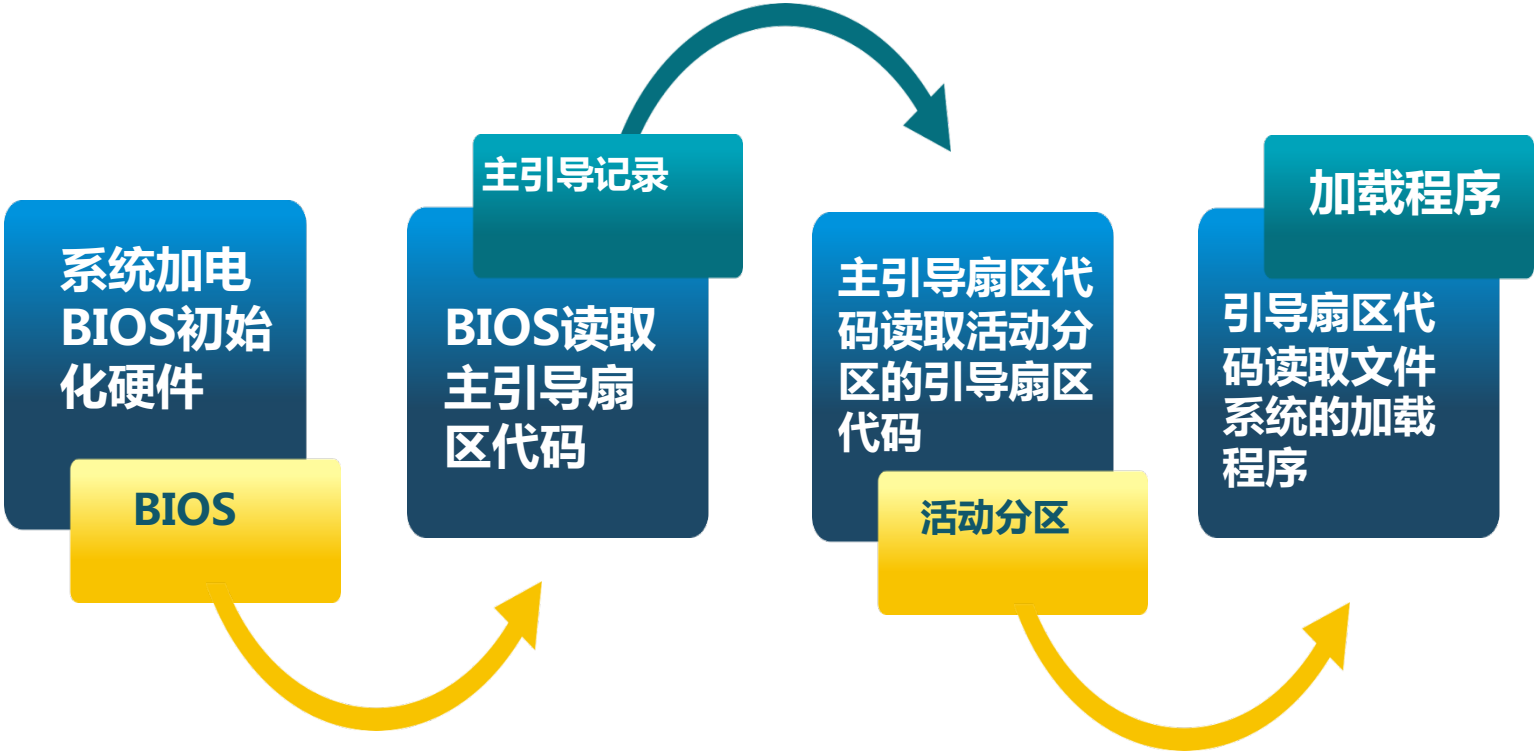
2.2 计算机的启动

- **CPU** 解释并执行指令
- 内存同时保存指令和数据



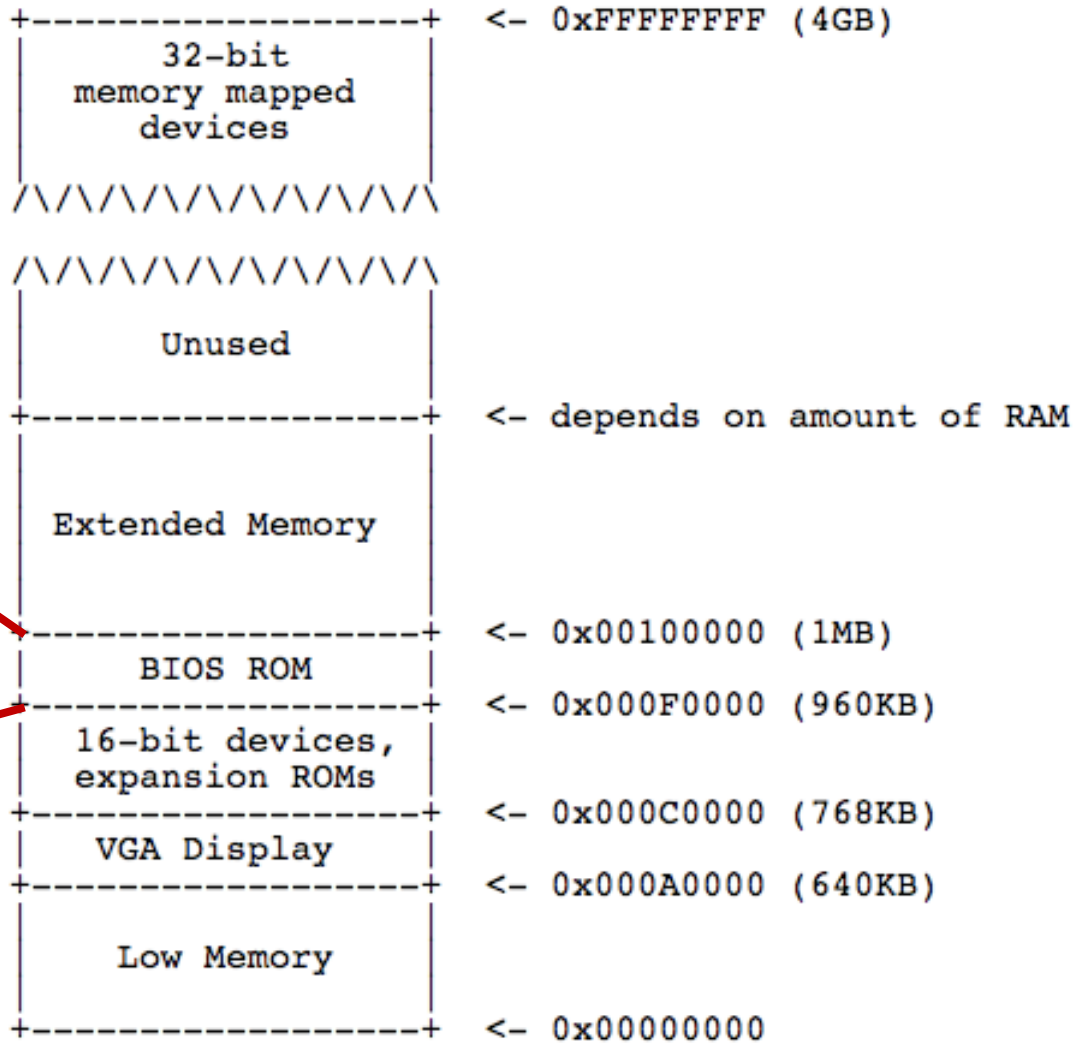
计算机是如何将硬件交于操作系统管理的？

传统启动过程：从BIOS到主引导区



启动时计算机内存布局

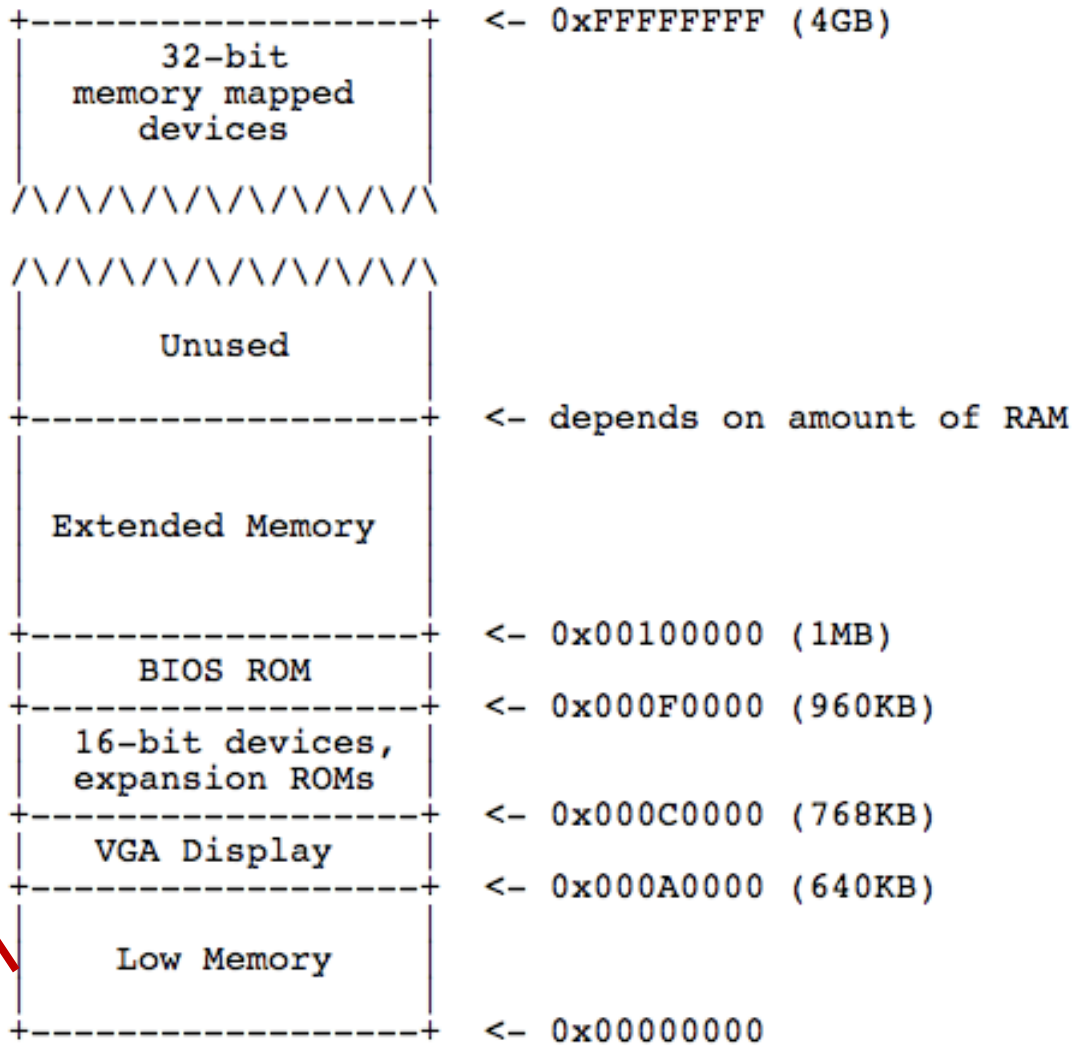
- CS: 0xF000, IP: 0xFFF0
- （CS：代码段寄存器；IP：指令指针寄存器）
- 系统处于实模式
- PC = 16*CS+IP
- EIP：0xFFFF0，指向最后的16个字节
- 20位地址空间：1MB



- 基本输入输出的程序
- 系统设置信息
- 开机后自检程序
- 系统自启动程序等

启动时计算机内存布局

- 主引导扇区：512字节，以”55AA”结尾
- BIOS自检完成后，将引导扇区的程序(bootloader)从主引导扇区加载到 **0x7c00**
- 跳转到0x7c00 处



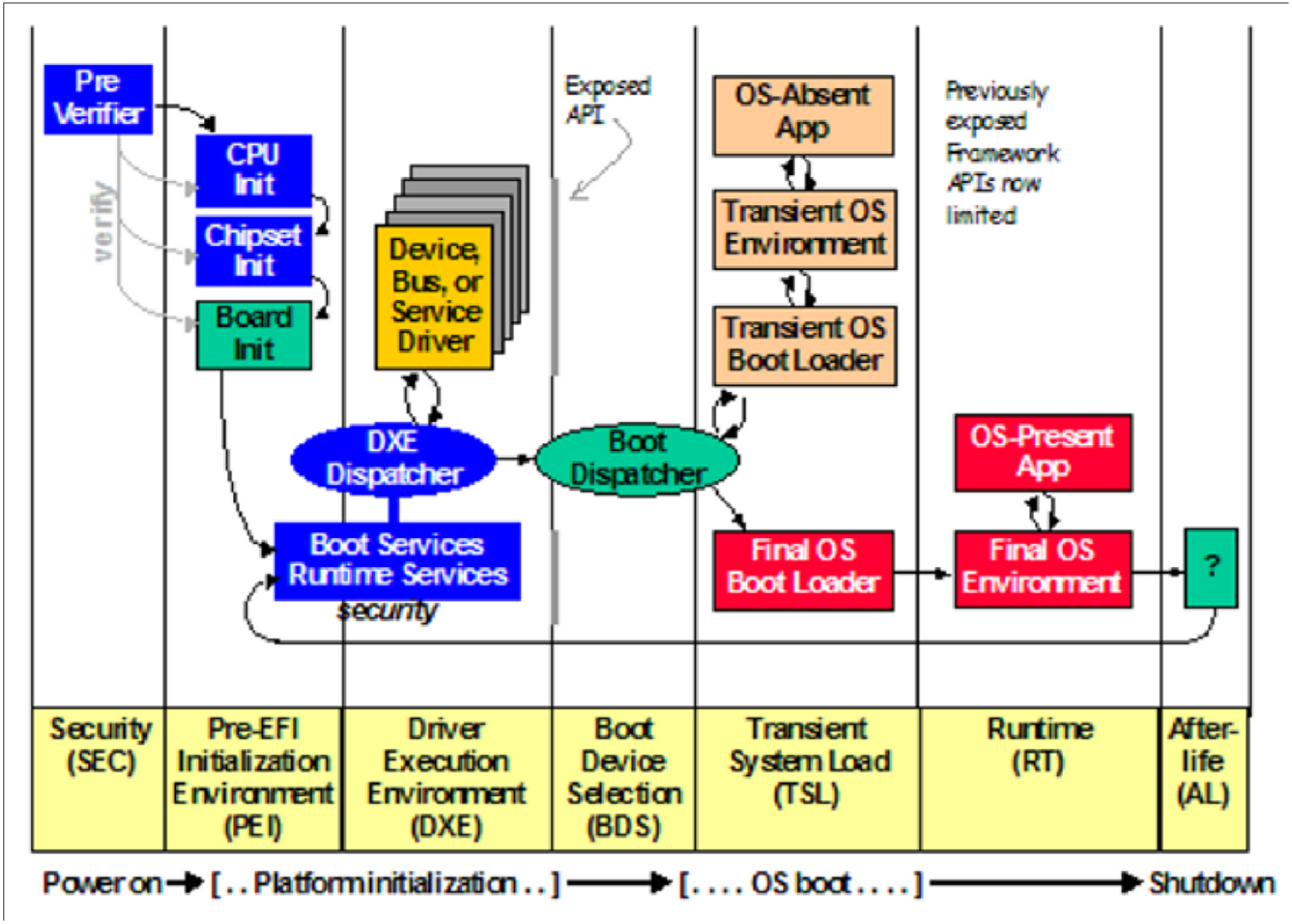
传统启动过程：OS加载

- Bootloader完成系统初始化
- OS内核的加载

现行两类启动规范

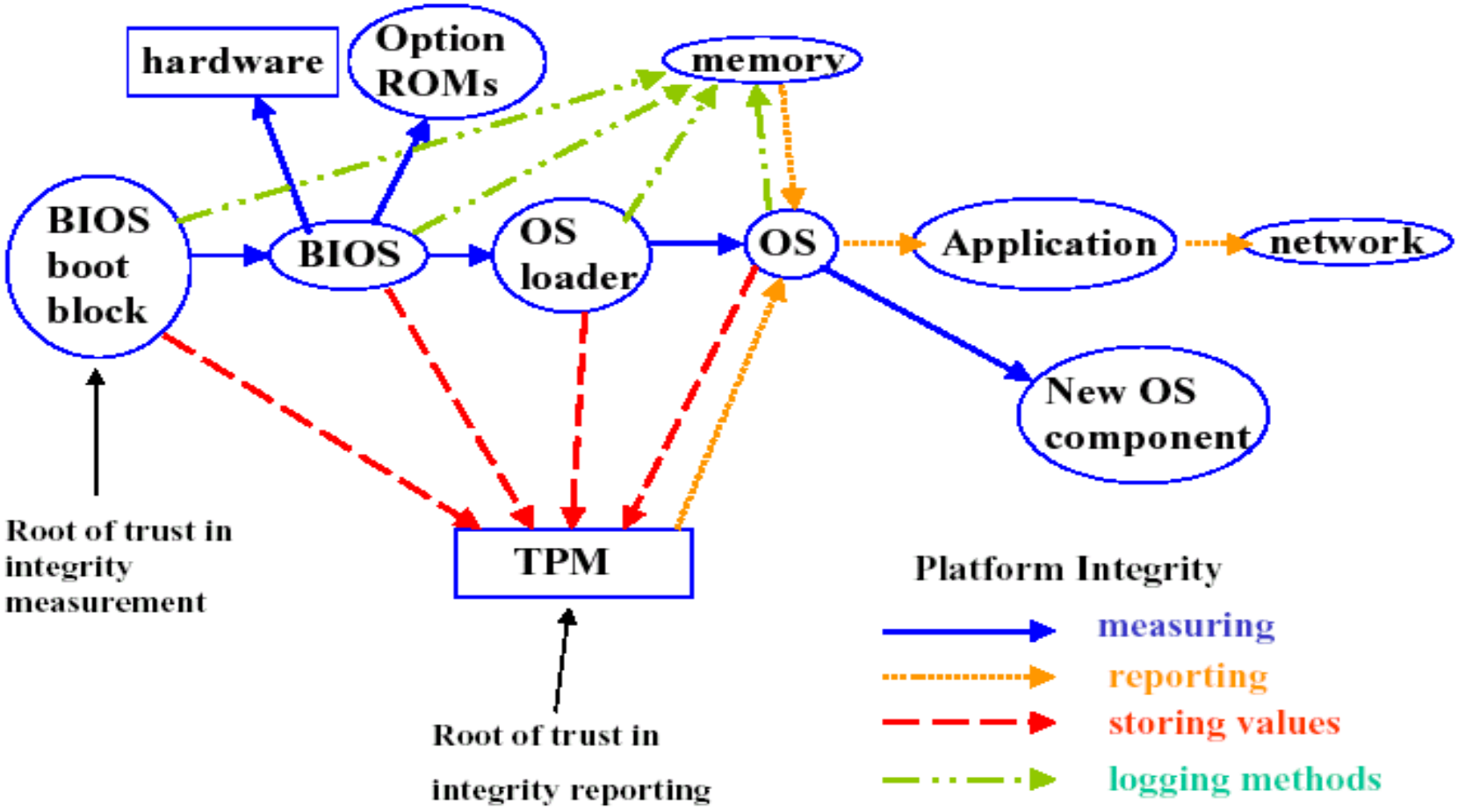
- 系统启动规范
  - Legacy BIOS
    - 固化到计算机主板上的程序
    - 包括系统设置、自检程序和系统自启动程序
  - UEFI(Unified Extensible Firmware Interface)
    - 传统BIOS弊端：赶不上硬件发展，如不支持2TB硬盘
    - 统一可扩展固件接口
    - 在所有平台上提供一致的操作系统启动服务

UEFI启动


Pre Verifier
verify
CPU Init
Chipset Init
Board Init
Device, Bus, or Service Driver
Exposed API
DXE Dispatcher
Boot Dispatcher
Boot Services
Runtime Services
security
OS-Absent App
Transient OS Environment
Transient OS Boot Loader
Final OS Boot Loader
Previously exposed Framework APIs now limited
OS-Present App
Final OS Environment
?
Security (SEC)
Pre-EFI Initialization Environment (PEI)
Driver Execution Environment (DXE)
Boot Device Selection (BDS)
Transient System Load (TSL)
Runtime (RT)
After-life (AL)
Power on
[..Platform initialization..]
[....OS boot....]
Shutdown

可信计算的启动信任链

可信PC信任链体系图



讨论问题

- 大家是否曾经了解过UEFI模式，你的机器是采用什么方式启动的？
- 对于启动过程，大家分析一下，可能存在哪些攻击方法？