75-08 Sistemas Operativos
Lic. Ing. Osvaldo Clúa
2010

Facultad de Ingeniería
Universidad de Buenos Aires

Windows Boot Process

Resumen

Componente	*Ejecución (Procesador)*	*Propósito*
Master Boot Record (MBR)	16-bit *real mode*	Lee y carga *partition boot sectors.*
Boot sector	16-bit *real mode*	Lee el directorio "/" para cargar Ntldr
Ntldr	16-bit *real mode* y 32-bit or 64-bit *protected*	Lee Boot.ini, presenta el *boot menu,* carga Ntoskrnl.exe, Bootvid.dll, Hal.dll, y los drivers de boot-start. Conmuta a *32-bit protected mode* o a *64-bit long mode* según la instalación
Ntdetect.com	16-bit *real mode*	Detecta el hardware para Ntldr.
Ntbootdd.sys	*Protected mode*	Device driver usado para I/O sobre SCSI y Advanced Technology Attachment (ATA
Ntoskrnl.exe	*Protected mode* con paginado	Inicializa los *executive subsystems* y los *boot y system-start device drivers.* Prepara els sitema para correr aplicaciones nativas Carga Smss.exe.
Hal.dl	*Protected mode* con paginado	*Kernel-mode DLL* que sirve de interface entre Ntoksnrl y los drivers con el hardware
Smss	Aplicación Nativa	Carga *Windows subsystem,* incluyendo *Win32k.sys* y *Csrss.exe,* lanza *Winlogon*
Winlogon	Aplicación Nativa	Lanza al *Service Control Manager* (SCM), al *Local Security Subsystem* (LSASS), y presenta la caja de diálogo de *logon.*
Service control manager (SCM)	Aplicación Nativa	Carga e inicializa los *auto-start device drivers* y los *Windows Services.*

Proceso de boot - Windows XP

- Se carga el MBR del disco.
- Se cargan 512 Bytes de la primer partición marcada como activa. Contiene un mini file system driver.
- Se carga el archivo NTLDR (oculto en el directorio \).
  - Pasa al procesador a modo protegido
  - Inicializa las tablas de paginado.
  - Si existe *hiberfil.sys*, lo carga y recupera al sistema que está hibernando.
- Si no ....

NTLDR (XP)

- Si existe, carga *Boot.ini* y envia un prompt al usuario.
  - Si no existe, trata de cargar el S.O. de C:\.
  - Si se oprime F8 se lanza un menú con opciones.
- Lanza *ntdetect.com* para obtener datos de la configuración.
  - Si hay mas de un perfil, envía un *prompt* al usuario para determinar cual activar.
- Muestra una *splash screen* (logo)
  - Carga *ntoskrnl.*

Win Vista/7

- Se carga el Windows Boot Manager (bootmgr.efi)
  - Desde la Partición EFI
  - Desde el \boot\efi
- Lee el Boot Configuration Data (BCD) y despliega el menú de opciones
  - El BCD (reemplaza a boot.ini) se crea al instalar o reparar (bootrec) del DVD de instalación.

Win Vista/7

  - El BCD también se puede modificar usando bcdedit o EasyBCD

- Finalmente invoca a winload.exe para que cargue el kernel.
  - El proceso sigue como en XP
- Estas dos etapas (bootmgr y winload) reemplazan a NTldr

ntoskrnl.exe

- Phase 0 (Interrupciones inhabilitadas)
  - Carga la Hardware Abstraction Layer Hal.dll
  - Carga los drivers de boot-time (pero no los inicializa) y guarda esa información en la clave del registry HKLM\SYSTEM.
    - Se guardan varios conjuntos de esta clave del registry, permitiendo acceso a "Last Known Good Configuration".
  - Se inicializa el Process Manager
    - Se crean las estructuras para el Proceso de la Phase 1 y para el Idle Process

Ntoskrnl Phase 1

- Se habilitan las interrupciones.
  - El *idle process* se interrumpe y entonces
  - Se llama a HAL para preparar el Controlador de Interrupciones de los dispositivos.
  - Se inicializan los servicios:
    - Object Manager, Executive, Microkernel, Security Reference Monitor, Memory Manager, Cache Manager,LPCS, I/O Manager y Process Manager.
      - En XP y 2003, esto se hace en forma asincrónica.
- El control pasa al Session Manager (smss)

smss.exe

- El Session Manager es una aplicación nativa (no usa las Windows API) y confiable (puede crear *security tokens*).
  - Hace un *autocheck* (*chkdsk*) si es necesario.
  - Carga las variables de ambiente (HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Environment)
  - Lanza el kernel mode del subsistema Win32 (win32k.sys) y pasa a modo gráfico.

smss.exe

- Lanza el modo usuario de Win32 Client Server Runtime Server Subsystem (csrss.exe)
  - Permite a las aplicaciones acceder a la Win32 API.
- Carga las DLLs conocidas.
- Termina de inicializar al *Registry* y los *Page files*.
- Finalmente lanza el Windows Logon Manager (winlogon.exe)

Autenticación de usuario

- Winlogon carga a la GINA (Graphical Identification And Authentication).
  - En Vista se la reemplazó por Credential Providers.
  - Permite otros métodos de identificación.
- Winlogon verifica la autenticidad de Windows.
- Espera el ingreso de un usuario para pasar a la fase de Logon.
  - Una vez exitoso el logon, crea un nuevo "Last Known Good Configuration"

Problemas durante el boot (XP)

Causa	*Síntoma*	*Tratamiento*
MBR Corrupto	"Invalid Partition Table," "Error Loading Operating System," "Missing Operating System."	Recovery Console → *fixmbr* (no recupera la Partiton Table)
Boot Sector Corrupto	"A disk read error occurred" "NTLDR is missing," "NTLDR is compressed"	Recovery Console → *fixmboot*
Boot.ini desconfigurado (o borrado)	"Windows could not start because of a computer disk hardware configuration problem," Could not read from selected boot disk," "Check boot path and disk hardware.	Recovery Console → *bootcfg /rebuild* (Explora las particiones y reconstruye el *boot.ini)*
Archivo del sistema corrupto	*"Windows could not start because the following file is missing or* corrupt," "STOP: 0xC0000135 {Unable to Locate Component}."	Recovery Console → *chckdsk* Buscar copia del archivo en \Windows\System32\DllCache
Registry corrupto	"Windows could not start because the following file is missing or corrupt: \WINDOWS\SYSTEM32\CONFIG\SYSTEM"	Recovery Console → *chckdsk* usar *ChkReg (bajar de Microsoft)* *NO CheckReg (es un troyano)* *Usar un ASR Backup*
Post-Splash Screen (cuelgue o caída)		Rebootear con F8 a LKG (Last Known Good)

Hay otras herramientas como un live cd para recuperar las particiones.
Es conveniente mantener un ASR backup (Auto System Recovery) del Sistema.
En Win 7 estan las facilidades de WINRE