Windows 7 Boot Process

Mark E. Donaldson

1. The **MBR** at 0000h:7C00h finds and loads the **Volume Boot Sector** and the **NT Boot Sector** (8 KB in size). The NT Boot Sector has the ability to read FAT32 and NTFS.

2. The **NT Boot Sector** finds and loads **BOOTMGR.EXE** from the system32 or system32/boot directory at 2000h:0000h. **BOOTMGR.EXE** has a 16 bit header prepended to itself. This 16 bit header checks the checksum of embedded **PE.EXE** and maps it at 0x400000. Execution of **BOOTMGR.EXE** starts in 32 bits in the **BmMain** function.

3. **BOOTMGR.EXE** checks for hibernation state. If it's found, it loads **WINRESUME.EXE**.

4. **BOOTMGR.EXE** mounts and extracts basic boot information from **BCD** (Boot Configuration Data). After user selects a boot entry, it is launched using **BmLaunchBootEntry** with added switches. In 64-bit systems, the CPU switches to 64-bit mode just before jumping to **WINLOAD.EXE**.

5. **BOOTMGR.EXE** loads and passes control to **WINLOAD.EXE**.

6. **WINLOAD.EXE** then loads **NTOSKRNL.EXE**, **HAL.DLL**, dependencies, boot drivers, and the **SYSTEM** registry hive. **WINLOAD.EXE** then creates a **PsLoadedModuleList** and **LOADER_PARAMETER_BLOCK** structure which contains a memory map and options list.

7. **WINLOAD.EXE** then loads and executes **NTOSKRNL.EXE** and transfers control to the kernel using **OslArchTransferToKernel**. **NTOSKRNL.EXE** uses two phases to initialize the system.

8. **NTOSKRNL.EXE** **phase 0** initializes the kernel itself. It calls **HalInitializeBios**, initializes the display driver, start the debugger, and calls **KiInitializeKernel**. **NTOSKRNL.EXE** **phase 1** initializes the system. It calls **Phase1InitializationDiscard**, **HalInitSystem**, **ObInitSystem**, sets the time bias for ASLR, calls **PsInitialSystemProcess**, and then calls **StartFirstUserProcess SMSS.EXE**.

9. **NTOSKRNL.EXE**, after stopping the debugger, then passes control to the Session Manager **SMSS.EXE**.

10. **SMSS.EXE** loads the rest of the registry, configures the environment to run the Win32 subsystem (**WIN32K.SYS**) and its various processes.

11. **SMSS.EXE** loads the **WINLOGON.EXE** process to create the user session, and then starts the services and the rest of the non-essential device drivers and the security subsystem **LSASS.EXE**.

Windows 7 Boot Process

Mark E. Donaldson