

WINDOWS VISTA VS XP BOOT PROCESS

Mark E. Donaldson

Windows Vista boot-up process is slightly different than windows XP, and to have an understanding on how windows vista boot process differ from windows XP, we should start by reviewing the XP process, follow by vista boot process, then we shall review the changes after that.

Windows XP boot up process:

1. System is powered on
2. The CMOS loads the BIOS and then runs POST
3. Looks for the MBR on the bootable device, and loads NTLDR
4. The BIOS/CMOS transfers control to the NTLDR
5. NTLDR first looks for Hiberfil.sys (if present, the system resumes from where it was hibernated)
6. If the hiberfil.sys is not present, NTLDR looks for boot.ini
7. If you have more than one operating system installed on your computer, Boot.ini will give you the option to choose the operating system to boot from.
8. The selected operating system then boots, in windows XP involves the loading of the kernel
9. After system services and user required DLLs are loaded, finally msgina.dll brings up the login screen.
10. When the user logs on, the system checks for the user's credentials in the SAM, if the credentials are correct, the user profile is loaded from documents and settings folder.
11. This brings up the desktop and at that point, the ControlSets are copied to the CurrentControlSet in the registry. Now, the system is considered booted.

Windows Vista boot-up process:

1. System is powered on
2. The CMOS loads the BIOS and then runs POST
3. Looks for the MBR on the bootable device
4. Through the MBR the boot sector is located and the BOOTMGR is loaded
5. BOOTMGR looks for active partition
6. BOOTMGR reads the BCD file from the \boot directory on the active partition
7. The BCD (boot configuration database) contains various configuration parameters(this information was previously stored in the boot.ini)

WINDOWS VISTA VS XP BOOT PROCESS

Mark E. Donaldson

8. When windows vista is selected, BOOTMGR transfer control to the Windows Loader (winload.exe) or winresume.exe in case the system was hibernated.
9. Winloader loads drivers that are set to start at boot and then transfers the control to the windows kernel.
10. There is not msgina.dll in windows vista (the shell draws the login screen)

OK. Now that we have the two boot-up processes on the board, we should examine what is different on windows vista boot up process. As we can see the difference starts at the MBR.

In windows vista, NTLDR was replaced by three new boot loader components, supposedly designed to load windows quicker and more securely. Those components are;

Windows Boot Manager (Bootmgr.exe)
Windows OS Loader (Winload.exe)
Windows Resume Loader (Winresume.exe)

Windows Boot Manager reads the boot configuration data (BCD) and display an operating system selection menu to the user

Windows OS loader is the operating system boot loader. It is invoked by the windows boot manager in order to load the operating system kernel (ntoskrnl.exe) and boot-class device drivers.

Notice the Boot Configuration Data (BCD) This new data store serves essentially the same purpose as boot.ini. However, BCD abstracts the underlying firmware and provides a common programming interface to manipulate the boot environment for all Windows-supported computer platforms) Boot Configuration Data allows for third party integration so anyone can implement tools like diagnostics or recovery options

Windows Resume loader replaces the Hiberfil.sys.

Another change that is worth noting is the msgina.dll file, I guess Microsoft sensed that was being abused too much and integrated the logon screen into the shell. Msgina.dll was used on windows XP to change custom login screens.