Components of the Boot Process – Windows XP and Server 2003

Component	Definition
Master Boot Record (MBR)	The first sector of the hard disk: • Contains MBR code and partition table.
Partition Boot Sector (PBS)	The first sector of the partition: • Contains BIOS Parameters Block (BPB) and boot sector code.
NTLDR	Reads the boot.ini file and loads the necessary initial operating system files into system memory.
Boot.ini	Boot configuration file.
Ntdetect.com	Performs hardware detection.
Ntoskrnl.exe	The operating system's kernel image.
HAL.dll	Hardware Abstraction Layer (HAL) - hides the hardware dependencies from the operating system. The Ntoskrnl.exe and HAL.dll images are matched pairs.
Session Manager Subsystem (Smss)	Responsible for starting the user's session.
Winlogon	Interactive Logon Manager - responsible for coordinating the secure identification and authentication of the user during logon.
Services	Service Control Manager (SCM) - loads and initializes AUTO_START device drivers and services.

Boot Process – Windows XP and Server 2003

Component	Responsibility
Master Boot Record (MBR)	When power is applied to the system, by default, this sector of the hard disk is read first: • Reads the partition table for the active partition. • Reads the partition boot sector of the active partition into system memory.
Partition Boot Sector (PBS)	The first sector of the partition: • Defines the format of the partition. • Reads the boot loader (NTLDR) into system memory.

NTLDR	• Reads boot configurations from the boot.ini file into memory to determine the OS to load, or make available any pre-boot diagnostic programs (i.e. memdiag.exe).
	  ○ If only one OS is installed, loads it as the default.
	  ○ If more than one OS is installed, presents "Boot Selection Menu".
	• Checks to see if the system was hibernated:
	  ○ If yes, loads Hiberfil.sys into memory and loads resume.exe into system memory. Transfer control to resume.exe.
	  ○ If no, loads and executes the appropriate Winload.exe image for the OS to be loaded.
	• Transfers control to Ntoskrnl.exe.

Ntoskrnl.exe (Phase 0)	During this stage, processor resources are allocated and the core Executive Subsystems required early in the boot process are initialized: • Initialized the HAL, Executive, Memory Manager, Bootvid Library, and NLS tables. • Enumerates and loads BOOT_START device drivers, into system memory. • Initializes Object Manager, Process Manager, Security Reference Monitor, and Plug and Play Manager.

Component	Responsibility
Ntoskrnl.exe (Phase 1)	• Initializes Power Manager, System Time, and Auditing Structures. • Loads HKLM\SOFTWARE and HKLM\HARDWARE registry hives into memory: ○ Information collected by Ntdetect.com is used to build HARDWARE hive. • Cache manager and I/O manager are initialized. • BOOT_START device drivers are initialized. • SYSTEM_START device drivers are loaded into system memory and initialized. • Session Manager process is launched.
Smss	• Runs programs specified in BootExecute. • Processes delayed file move/rename operations. • Initializes paging. • Initialized remaining registry hives. • Starts Win32k.sys. • Starts Csrss.exe. • Starts Winlogon.exe.
Winlogon	• Loads the GINA (Msgina.dll/LogonUI.exe). • Starts the Service Control Manager (Services.exe): ○ Loads AUTO_START services and device drivers. • Starts Lsass.exe. • Winlogon then waits for an interactive logon notification.

Components of the Secure Logon Process – Windows XP and Server 2003

Component	Definition
Secure Attention Sequence (SAS)	Keystroke combination that is registered by Winlogon during system initialization: • Calls Winlogon to display security desktop.
Winlogon	Interactive Logon Manager - coordinates all user identification and authentication activities during logon.
GINA	Graphical identification and authentication - user to present the logon dialog box to the user to collect the users logon credentials.
Lsass	Local Security Authority Subsystem: • Performs user Authentication. • Creates user's security token.
Authentication Packages	Creates a hash of the password entered for comparison to the hash stored in the SAM/AD database.
Security Accounts Manager/Active Directory (SAM/AD) database	Stores the known good hash of the user's password used for authentication of the user.
Security (policy) database	Stores security policy restrictions relating to user logon.
Userinit	Userinit: • First process launched in the user's session. • Loads the user's profile. • Loads and launches the user's shell.
Shell	The process that the user's logon session executes in.

Secure Logon Process – Windows XP and Server 2003

Step	Description
SAS is entered	Calls Winlogon to present the Secure Desktop Winlogon: • Loads GINA. • GINA displays logon dialog box to collect user's credentials.
User credentials entered	GINA collects user's credentials and returns them to the winlogon process. The winlogon process then passes the entered credentials to lsass.exe via secure Advanced Local Procedure Call (ALPC) connection.

User is authenticated	Lsass passes the credentials to the appropriate Authentication Package (AP) to create a hash of the user's password.
	• The AP retrieves the users account information from the SAM/AD database (username, groups, and restrictions).
	• AP checks for restrictions that would prevent the user from logging on:
	  ○ If restrictions exist, logon process fails.
	  ○ If no restrictions exist, logon process continues.
	• AP compares hash to password hash that is stored with the user's account in the SAM/AD database:
	  ○ If the hashes are different, authentication fails and the logon process is terminated, and an error message is returned to Winlogon.exe.
	  ○ If the hashes match, the user is authenticated, and the AP creates a Locally Unique Identifier (LUID) for the logon session and the logon session itself, and the logon process proceeds.
	• Lsass checks the Security (policy) database for the user's allowed access:
	  ○ If the requested access does not match, logon fails and the process is terminated.
	  ○ If the requested access is permitted, the appropriate Security IDs are recorded for inclusion in the user token.

Step	Description
Access Token is created	The access token is created. It includes the following information: • User's account SID. • Group SIDs for those groups the user belongs to. • Restricted SIDs. • User's privilege array. • Access token is maintained within the Lsass.
Winlogon.exe	Launches Userinint.exe: • Handle to user's token is attached to this process.

Userinit.exe	Performs the following:
	• Loads the user's profile (NTUSER.dat) into the registry under Hkey_Current_User (HKCU).
	• Runs user scripts defined at: HKCU\Software\Microsoft\Windows\System\Scripts
	• Run machine scripts defined at: HKLM\Software\Microsoft\Windows\System\Scripts
	• Launches the user's shell by reading the following registry keys:
	  ○ Custom shell: HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell
	  ○ Default shell (Explorer.exe): HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell
	• Inherits copy of the handle to user's token.
	• Updates "Last Known Good" registry value: HKLM\System\Select\LastKnownGood
	• Userinit.exe exits.
	• User's shell becomes parent process for user's logon session.