Windows Architecture

May 2020

Windows Architecture:

- Highly modular
- 2 main layers - user mode and kernel mode
- Kernel mode: unlimited access to system memory and external deives
- Can also be called a hybrid kernel kernel
- Architecture is:
    - Hybrid kernel
    - Hardware Abstraction Layer (HAL)
    - Drivers
    - Executive

Windows Architecture

- User mode applications don’t call OS system services directly
- Subsystem DLLs - translate a documented function into Windows system service calls
- Environment subsystem processes: manage client processes in their world, impose process model, and security

Kernel Mode Components: Executive

Handles:

- Base operating system services
- Memory management, process and thread management
- Security, I/O, interprocess communication
- Written almost entirely in C

Contained in file Ntoskrnl.exe

Kernel Mode Components: Kernel

- Low-level operating system functions
- Thread scheduling, interrupt and exception dispatching
- Multiprocessor synchronization
- Provides the set of routines and objects that are used by the rest of executive to implement higher level constructs
- Contained in file Ntoskrnl.exe

Kernel Mode Components: Drivers

- Interface between hardware and higher level functions

User Mode Processes

- System support processes
  - Logins, and Session Managers
- Services processes
  - Windows services: task scheduler, printer, ...
- User Applications
- Environment Subsystems
  - (Outdated ?)

Symmetric Multiprocessing (SMP)

- No master processor
  - All the processors share one memory space
  - Interrupts can serviced on any processsor
  - Any processor can cause another processor to reschedule what it's running
- Maximum Number of CPUs stored in registry (HKLM\System\CurrentControlSet\Control\Session Manager\LicensedProcessors)
- Replaced by hyperthreading

App calls subsystem

- Function entirely implemented in user mode
    - No message sent to environment subsystem process
    - No Windows executive service system is called
- Functions requiring one/more calls to Windows executive
    - Ie. Functions to read and write files
- Functions that require some work in the environment subsystem process
    - Client/Server requests, subsystem DLL waits for reply before returning to caller

Windows Subsystem: Environment Subsystem Process

- CSRSS.exe
- Console windows
- Creating and deleting processes and threads
- ...

Windows Subsystem: Kernel-mode device driver

- WIN32K.sys
- Window Manager: manages screen output
- Input from I/O devices
- User messages to applications
- Graphical Device Interface (GDI)

Windows Subsystem: Subsystem DLLs

- Such as USER32.DLL, ADVAPI32.DLL, GDI32.DLL, KERNEL32.DLL
- Translate Windows API functions into calls to NTOSKRNL.exe, and WIN32K.sys

Kernel Mode Device Drivers

- Separate loadable modules
- Defined in registry

Windows Startup Processes

- Process ID 0 (IDLE)
    - Part of the loaded system image
    - Home for idle thread(s) (not a real process nor real threads)
    - Called System Process frequently
- Process ID 2 (SYSTEM)
    - Part of the loaded system image
    - Home of kernel-defined threads (not a real process)
    - Thread 0 (routine name Phase 1 intialization)
    - launches the first “real” process, running smss.exe
    - Then becomes the zero page thread

System Startup Processes: smss.exe

- Session Manager
- First created process
- Takes parameters from \HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager
- Launches required subsystems: csrss.exe, and then winlogin

System Startup Processes: winlogon.exe

- Logon Process: Launches services.exe and lsass.exe; presents first login prompt
- When someone logs in, launches apps in \Software\Microsoft\Windows NT\WinLogon\Userinit
- Launches services.exe, and then lsass.exe (Local Security Authentication Server)

Startup Processes: services.exe

- Server Controller, for many Windows-supplied services
- Starts processes for services not part of services.exe

System Startup Processes: userinit.exe

- Started after login, starts Explorer.exe (\Software\Microsoft\Windows NT\CurrentVersion

Services in the Registry

- Defined in the registry
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
  - One key per installed
- Mandatory information kept on each service:
  - Type of service (Windows, Drivers, ..)
  - Imagename of service.exe
  - Start type (automatic, manual, or disabled)
- Additional Information:
  - Display Name, Description, Dependencies, Account and Password to run under
- Can store application-specific configuration parameters
  - Parameters subkey under service key

Life of a Service

- Install time
  - Setup application tells service
  - Controller about the service
- System boot/initialization
  - SCM reads registry, starts services as directed
- Management/maintenance
  - Control panel can start and stop services and change startup parameters

Service Processes

- A process created and managed by the Service Control Manager (SCM) (Services.exe)
  - Similar in concept to Unix daemon processes
  - Typically configured to start at boot time and do not interact with the desktop
- Service control tools:
  - net start/stop local system only
  - Sc.exe, psservice (sysinternals) - similar to SC
  - Other resources

Windows Security and Access Control: Basics

Important Components:

- Security Reference Model (SRM)
- Local Security Authority (LSA)
- Security Account Manager (SAM)
- Active Directory (AD)
- Authentication Packages
- WinLogon and NetLogon

Security Reference Monitor (SRM)

- Performs access (permission) checks
- Generates audit log entries
- Manipulate user rights (privileges)

Local Security Authority (LSA)

- Resides in user-mode process lsass.exe
- Enforces local security policy including:
  - Password policy (complexities, and expiration)
  - Auditing policy (which operations on what objects to audit)
  - Privilege settings (which accounts on a computer can perform privileged operations)
- Issues security tokens to accounts as they log into the system

Security Account Manager (SAM)

- Database storing account data and relevant security information about local users, and groups
- When user logs into the computer using a local account, the SAM process (SamSrv) takes logon information, and performs lookup on SAM DB, which resides in Windows\System32\config directory
- SAM file is a binary and is locked (can not be read) during a local session, password are stored as hashes

Active Directory (AD)

- Clients communicate with AD to perform security operations, like account login
- Clients are authenticated using AD when they attempt to login to a domain account rather than a local account
- Users credential information is sent securely across the network, and verified by AD, before the user is logged in.
- Credentials might be username and password, or private and public key

Local vs Domain

- Networked Windows Computer is either domain joined or in a workgroup
- Domain joined: users gain access to that computer using domain accounts, which are centrally managed in Active Directory. They can also log on using a local, but it might not have access to domain resources
- Computer in a workgroup: Only local accounts can be used, held in SAM.

Workgroup

- A collection or group of computers connected to one another using a network
- Machines in the workgroup use only local accounts
- Difference between a workgroup and a domain:
  - A workgroup has no domain controllers
  - Authentication is performed on each computer
  - (Domain authenticates accounts at domain controllers running AD)

Domain Example: User logging into the system

Domain Admin:

- Adds the users account to system
- Grants group membership, and additional Privileges

Windows creates an account in the domain controller's active directory

- Assigns a unique Security ID (SID)

New User:

- logins in, and is authenticated by AD
- 2 Login Formats:
- SAM Format: DOMAIN\Username
- User Principal Name (UPN): user@domain.company.com

SIDs Format:

S-X-Y-ZZ-AAA-BBB-CCC-RRR

- S for SID
- X - SID version number
- Y - identifier authority (ie. SECURITY_NT_AUTHORITY)
- ZZ - 21 = not unique,
- AAA-BBB-CCC - uniques number representing domain
- RRR - relative ID (RID) - RID increments by 1 for every new account.

Workgroup: Login

- User enters their username and password
  - A token is created by the OS, which includes the user's SID, SIDs for all the groups they are part of, and their privileges

- Domain-joined computer local login, use the "." domain, .\Username will log the user in locally.

Access Control Lists (ACL)

- Windows has 2 forms of ACL
- Discretionary ACL (DACL)
  - Grants or denies access to protected resources in Windows such as files, shared memory, named pipes, etc
- System ACL
  - Used for auditing, and enforces mandatory integrity policy

DACL

- Objects are assigned a DACL
  - Includes the SID of the object owner, and Access Control Entries (ACEs)
  - Each ACE includes SID and access mask
  - Access masks are type specific (different for different file types)

The data structure that contains the object owner, DACL, and SACL is called the object;s security descriptor (SD)

Access Checks

- User attempts to access a protected object, Windows performs an access check
- It compares the user and group information in the user's token, and the ACE in the object's ACL
- If all requested operations are present in the ACL the user is granted access, otherwise they are denied access