Windows 7

Report

Class: DMAJ0920

Subject: Technology

Group B: Martin Hvizdak, Hubert Mariusz Kijowski, Matej Adamkovic, Adrian Tadeusz Maciejewski

Supervisor: Karsten Jeppesen

Contents

Introduction

The windows 7 is an operating system by Microsoft, that joined the marked on 22nd of October 2009.

After replacing windows vista, which was not a well-received operating system, it has become a great success and received a critical acclaim by the users.

For the improvements it had better performance, more intuitive interface (for example better taskbar), and many other.

It was so popular, that it was the most used operating system until the January of 2018, when it was surpassed by windows 10.

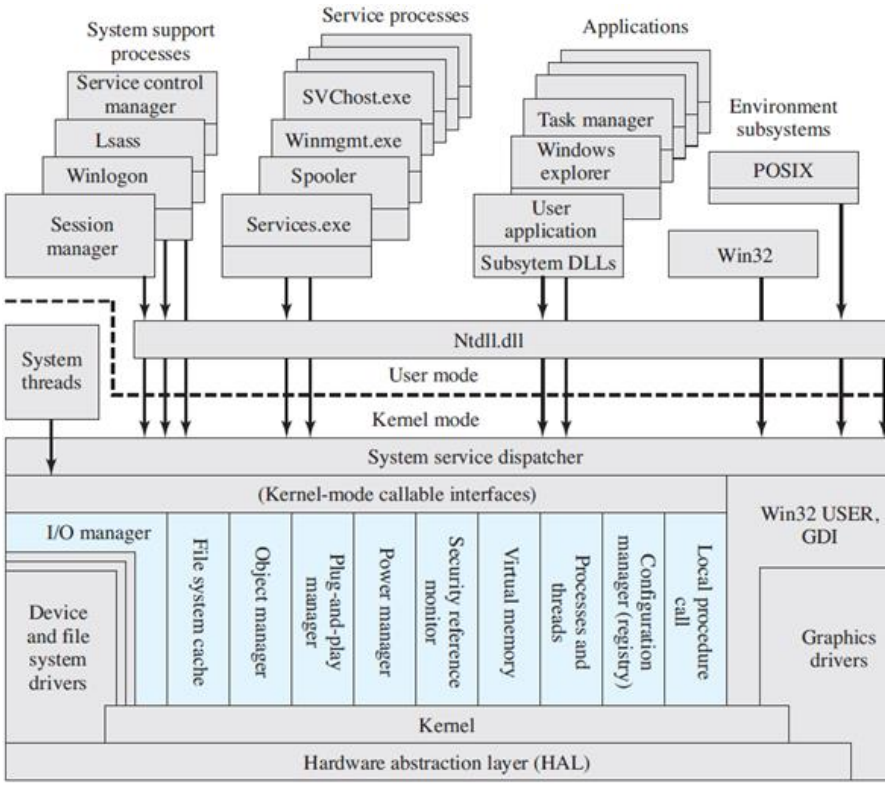
Architecture with building blocks

Windows NT

Windows NT (New Technology) is a family of operating system versions produced by Microsoft, the first version of which was released on July 27, 1993. Systems like Windows XP, Vista, 7, 8, 10 are based on Windows NT architecture. The architecture of Windows NT, is a layered design that consists of two main components, user mode and kernel mode. It is a pre-emptive , re-entrant multitasking operating system. Despite visible changes made from windows XP to windows 10, all transitional operating systems have similar architecture thanks to being based on Windows NT architecture.

Windows separates application-oriented software from the core OS software. The latter, which includes the Executive, the Kernel, device drivers, and the hardware abstraction layer, runs in kernel mode. Kernel mode software has access to system data and to the hardware. The remaining software, running in user mode, has limited access to system data. The user mode is made up of subsystems which can pass I/O requests to the appropriate kernel mode drivers via the I/O manager

Windows NT/ Windows 7 architecture



User layer

User mode is built out of various system-defined processes and Dynamic Linked Libraries.

The interface between user mode applications and kernel functions is an "environment subsystem." There are two main environment subsystems: the Win32 subsystem and POSIX subsystem.[2]. This mechanism was designed to support applications written for many different types of operating systems.

Environment subsystems

- The Win32 environment subsystem can run 32-bit Windows applications. It contains the console as well as text window support, shutdown and hard-error handling for all other environment subsystems. It also supports Virtual DOS Machines (VDMs), which allow MS-DOS and 16-bit Windows (Win16) applications to run. It handles input events (such as from the keyboard and mouse), then passes messages to the applications that need to receive this input. Each application is responsible for drawing or refreshing its own windows and menus, in response to these messages.
- The POSIX in windows 7 has been replaced by Interix, POSIX-conformant Unix subsystem for Windows NT operating systems. Like the POSIX subsystem, Interix was an environment subsystem. It included numerous open source utility software programs and libraries.
- WoW64 (Windows 32-bit on Windows 64-bit) is a subsystem of the Windows operating system capable of running 32-bit applications on 64-bit Windows. It is included in all 64-bit Windows systems.

Ntdll.dll exports the Windows Native API. The Native API is the interface used by user-mode components of the operating system that must run without support from Win32 or other API subsystems. The large majority of Windows applications do not call NTDLL.DLL directly.

Kernel Layer

Windows NT kernel mode has full access to the hardware and system resources of the computer and runs code in a protected memory area.[8] It controls access to scheduling, thread prioritization, memory management and the interaction with hardware. The kernel mode stops user mode services and applications from accessing critical areas of the operating system that they should not have access to; user mode processes must ask the kernel mode to perform such operations on their behalf.

Executives

The Windows Executive services make up the low-level kernel-mode portion, and are contained in the file NTOSKRNL.EXE.[8] It deals with I/O, object management, security and process management. These are divided into several *subsystems*, among which are *Cache Manager*, *Configuration Manager*, *I/O Manager*, *Local Procedure Call (LPC)*, *Memory Manager*, *Object Manager*, *Process Structure* and *Security Reference Monitor (SRM)*. Grouped together, the components can be called *Executive services* (internal name *Ex*). *System Services* (internal name *Nt*), i.e., system calls, are implemented at this level, too, except very few that call directly into the kernel layer for better performance.

I/O Manager

Allows devices to communicate with user-mode subsystems. It translates user-mode read and write commands and passes them to device drivers. It accepts file system I/O requests and translates them into device specific calls, and can incorporate low-level device drivers that directly manipulate hardware to either read input or write output. It also includes a cache

manager to improve disk performance by caching read requests and write to the disk in the background.

Memory Manager

Manages virtual memory, controlling memory protection and the paging of memory in and out of physical memory to secondary storage, and implements a general-purpose allocator of physical memory.

Process Structure

Handles process and thread creation and termination, and it implements the concept of *Job*, a group of processes that can be terminated as a whole, or be placed under shared restrictions (such a total maximum of allocated memory, or CPU time).

Hardware Abstraction Layer (HAL)

Windows runs on many different configurations of the personal computer. Each configuration requires a layer of software that interacts between the hardware and the rest of the operating system. Because this layer abstracts (hides) the low-level hardware details from drivers and the operating system, it is called the hardware abstraction layer (HAL). The HAL includes hardware-specific code that controls I/O interfaces, interrupt controllers and multiple processors.

Supported CPU Architectures

Windows 7 Supports following architectures:

X86

x86 is a family of instruction set architectures initially developed by Intel based on the Intel 8086 microprocessor. The 8086 was introduced in 1978 as a fully 16-bit extension of Intel's 8-bit 8080 microprocessor. The term "x86" came into being because the names of several successors to Intel's 8086 processor end in "86", including the 80186, 80286, 80386 and 80486 processors. Later processors from XX86 family implemented 32-bit architecture what caused x86 to be commonly known as 32-bit architecture set despite its roots in 16-bit architecture.

IA-32

IA-32 is short for "Intel Architecture, 32-bit", is the 32-bit version of the instruction set architecture, designed by Intel and first implemented in the 80386 microprocessor in 1985. IA-32 is the first incarnation of x86 that supports 32-bit computing; as a result, the "IA-32" term may be used as a metonym to refer to all x86 versions that support 32-bit computing

X64

x86-64 (also known as x64, x86_64, AMD64 and Intel 64) is a 64-bit version of the x86 instruction set, first released in 1999. It introduced two new modes of operation, 64-bit mode and compatibility mode, along with a new 4-level paging mode.

Thread model

In Windows 7 and any other Windows from NT family is Multithreading. A feature of the operating system that allows several tasks, called threads, to be performed in a single process. New tasks are sequences of instructions that are carried out independently to some extent. All threads in the same process share the same virtual address space containing the program code and its data.

Features of multithreading

- All threads execute within only one program (process) - in other words, one process has many execution instances (threads)
- Threads have been introduced to enable concurrent processing, e.g. when you need to execute multiple tasks simultaneously. It can also increase processing performance as long as sufficient hardware is used (at least multiple single-core processors or a single multi-core processor).
- All threads of a given process share the same virtual address space and use the same system resources
- Communication between threads is based on referencing the same variables and objects. Inter-process communication requires the use of IPC (InterProcess Communication) mechanisms
- sharing a virtual address space has its drawbacks - one "faulty" thread may endanger the execution of the entire process (program);

The scheduler and dispatcher

Before windows 7, the windows kernel dispatcher employed a single lock (the dispatcher lock), which has worked for 64 processors.

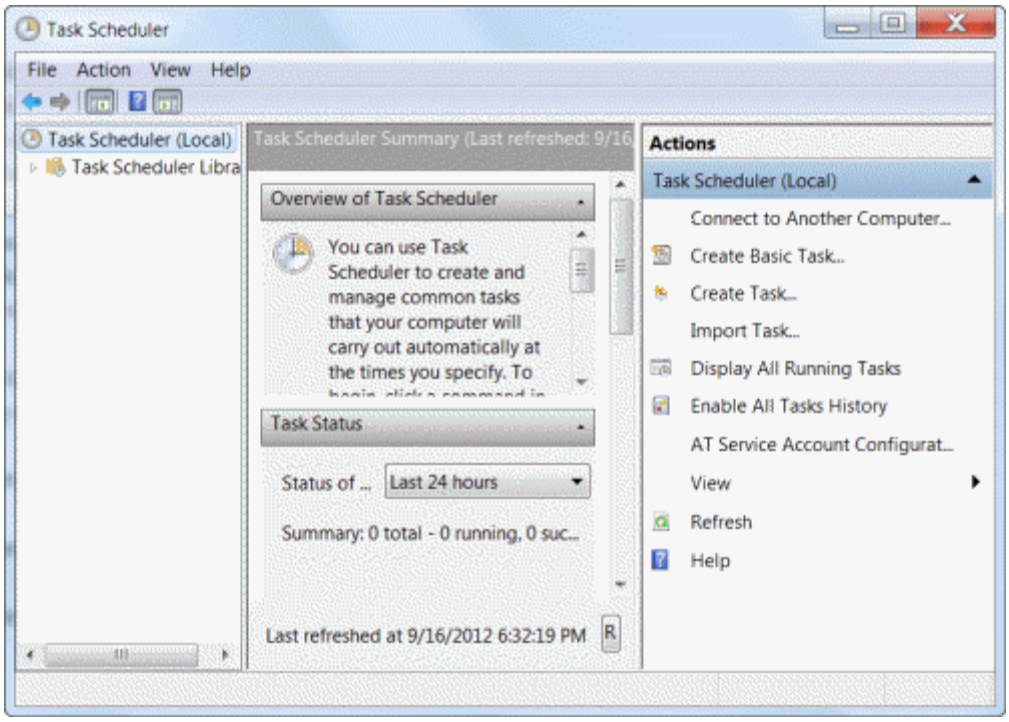
But within the time of windows 7, 64 processors were not that many.

For this, a new NT scheduler was written, so the windows 7 could scale up to 256 processors.

In addition to running tasks on scheduled times, the scheduler supported calendar and event-based triggers.

Tasks can also be idle for a set amount of time after startup.

The scheduler exposes an API consists of 42 COM (Component object model) interfaces.

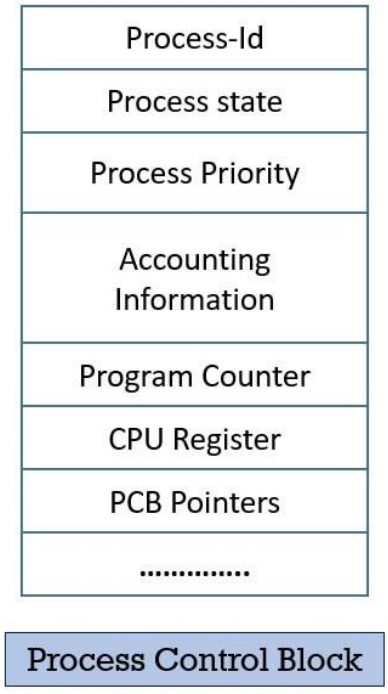


Process Control Block

Process Control Block (PCB) it is an area of operating memory, reserved by the operating system kernel for the purpose of storing many important and less important information about every currently existing and registered process in this system. PCB is the process representation in the operating system.

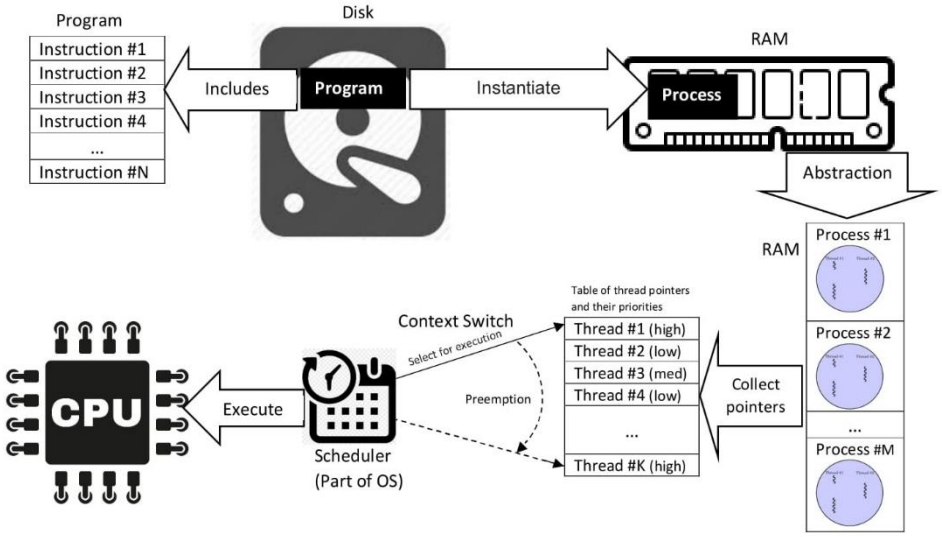
PCB implementation

1. Process identifier
2. Process State: The state of a process can be identified by the system as new, active, pending, or ready.
3. Processor registers: The number and types of processor registers depend on the architecture of the computer. There may be registers such as accumulators, index registers, stack pointers, general purpose registers, and condition registers. Information on the Command Counter and Index Registers must be kept during the interrupt event so that the process can be continued correctly afterwards.
4. CPU Allocation Planning Information: This information includes the process priority, pointers to the order scheduling queues, and other scheduling parameters.
5. Memory management information: This can be, for example, information such as: boundary register contents, page tables, or segment tables (depending on the virtual memory system used by the operating system.
6. Billing information: This category of information includes: the amount of CPU and real-time used, time constraints, account numbers, task or process numbers, etc. This information, especially in older types of commercially used computers, was mainly used to charge users for the time used. processor.
7. I / O status information: This includes information about the I / O devices assigned to the process as well as a list of open files, etc.
8. process priority
9. indicator on the PCB of the next process



Process handling

Process is a program that is currently executed. In order to execute a program some conditions must be met. Windows 7 must allocate required resources to the process, let program to share and exchange information and isolate resources from different processes so they don't interfere together.



Resource Allocation

Operating system needs to decide what resources are required by program and allocate them accordingly.

There are two main allocation techniques

- Resource partitioning approach
- Pool based approach

Resource partitioning approach - Resources are divided into partitions, for example - 10MB of memory, printer and some reserved cpu power

This approach is easy to implement, however lacks flexibility as new resources cannot be assigned and the ones that are not used are wasted.

Pool based approach – Common pool of resources is used. Whenever a program makes request for a resource operating system checks if the resource is free and allocates it to a program.

The main advantage is that no resources are wasted

Handling deadlocks

Deadlock detection

Deadlock detection monitors the driver's use of resources which need to be locked.

It is supported from windows XP and included later versions.

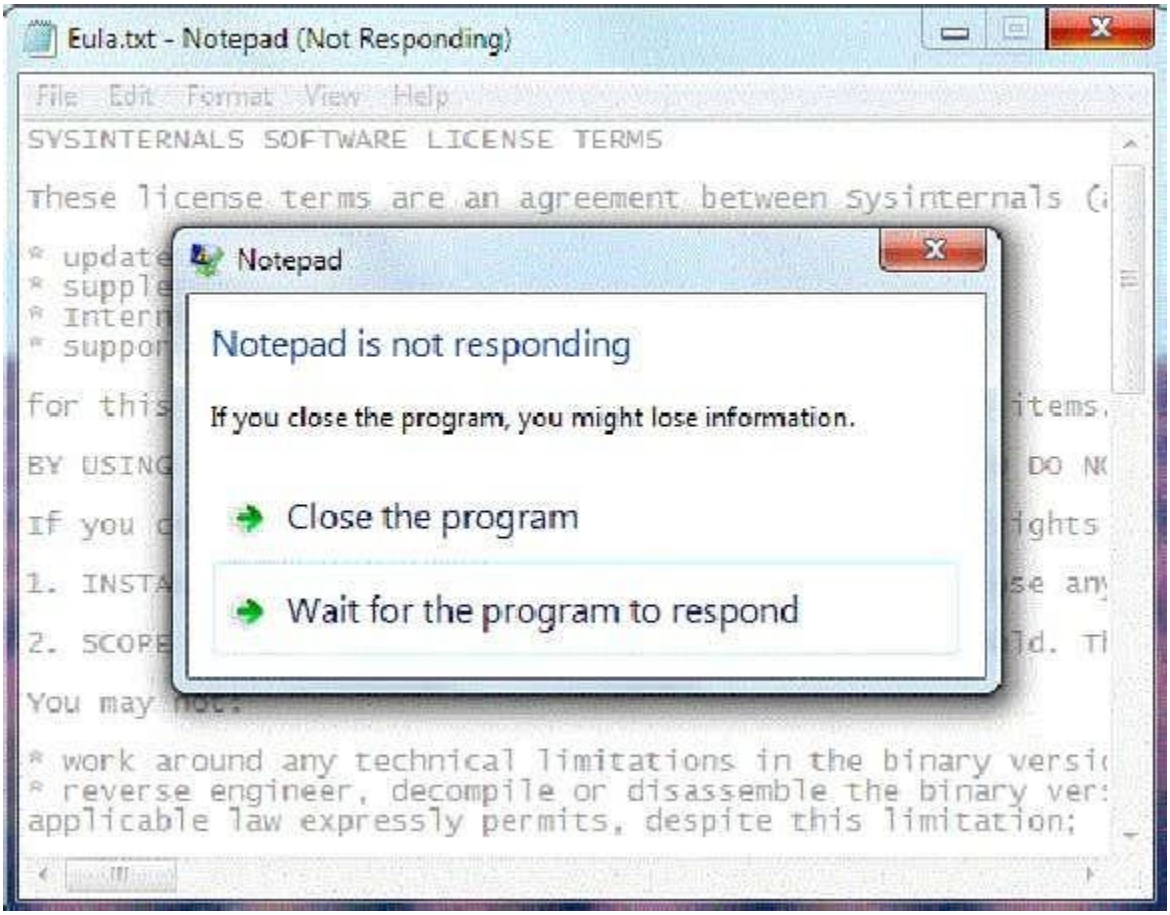
When a thread creates a window on the desktop, it enters a contract with the Desktop Window Manager(later DWM).

The DWM posts messages into the thread-specific message queue. The thread retrieves and dispatches those messages via its message queue. If the thread does not service the queue by calling the GetMessage() function, messages are not processed, and the window "hangs"(is in a state of deadlock). The operating system detects this state by attaching a timer to pending messages in the message queue. If a message has not been retrieved within 5 seconds, the DWM declares the window to be in a state of deadlock.

Deadlock solution

When the operating system detects a deadlock, it enters a state when the user cannot even terminate the application. The message from close button would be stuck in the message queue like any other message. The DWM assists by hiding and then replacing the window in a deadlock state with a “ghost” copy, displaying a bitmap of the original window’s UI and adding “Not Responding” to the title bar. If the original thread does not retrieve messages, the DWM manages both windows and lets user to interact with the ghost copy.

With this, the user can decide to send debugging data to Microsoft, which can help with future development.



File storage system

Description

File system defines how data can be stored and accessed. Without it we would not be able to tell exactly where the data we are looking for is located. There are many different types of file systems and they all have different advantages and disadvantages. For example, some of them can be designed to be fast while not being very secure, but other are much more secure while being slower.

Windows 7 is using two default file systems – **NTFS, FAT32.**

NTFS: it stands for NT file system and can store and retrieve data on Windows NT operating systems. It provides better recovery and data protection with many improvements in terms of security, performance and extendibility compared to FAT.

It is very popular thanks to the big maximum file size, that does not limit the normal user.

FAT was founded in 1977 for use on floppy disks. Increases in disk drive capacity required three major variants – FAT12, FAT16 and FAT32. It is no longer default file system for Windows computers. The main disadvantage was maximum size of 4GB per one file on the device and maximum of 2TB total device capacity. On the other hand, since it is so old the combability is almost guaranteed, meaning that you can plug it in any console, device or computer and it is going to work.

Architecture

File system is based on two or three layers. They sometimes work combined and sometimes are separated. Files can have three types of attributes:

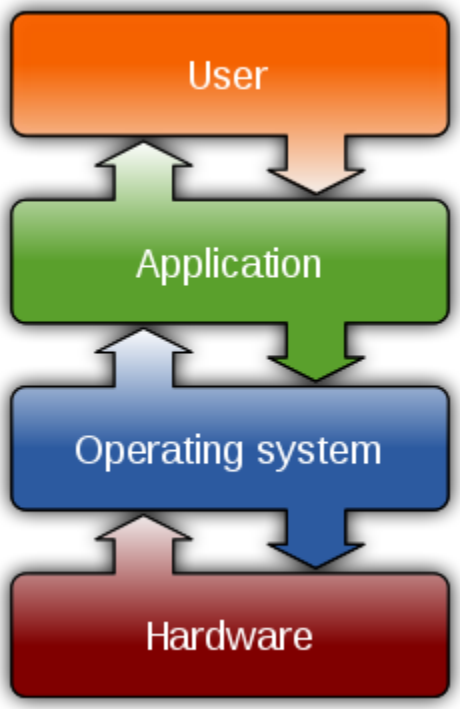
Read – User is only able to open and read the file, he cannot write any new information to the file without taking ownership over the file.

Write – User is able to write and read the file

Hidden - User cannot see the file, but the files are there

The three layers mentioned above are following:

- **Logical file system** is the level of the file system at which users can request file operations by system call.
- **Virtual file system** allows support for multiple concurrent instances of physical file systems, each of which is called a file system implementation
- **Physical file system** contains actual data stored on the system



File access methods

File access determines the way files are accessed and read into memory. Some systems support many access methods and choosing the right one is major design problem. There are three methods to access information: Sequential, direct and index sequential access method

Sequential access: most of the operating systems access file sequentially. Records are accessed in a pre-defined sequence. This is the most popular access method.

- Data is accessed in order one after one
- After a read operation, the pointer moves to the next file
- After a write operation, pointer moves to the end of file
- This access method is good for a tape for example.

Direct access: mostly used in case of database systems. Each block has its own address and can be accessed directly for reading and writing

Index access: is built on top of sequential access.

Interesting facts

New features

- **Action Center** - New module that groups all common tasks related to various aspects of Windows work. You don't have to search the Control Panel or search for a solution to a problem in system help like in vista. Action Center will solve practically any computer problem for you. In a way, it is an extension of the idea of the Security Center module known from Vista or Windows XP. All popular options are grouped here, in the form of two categories: Security and Maintenance - a place where you can find all the tasks related to the stable operation of the system and its maintenance. The solution looks much better than the chaotic reporting system in Vista.
- **AppLocker** - New feature designed to prevent unauthorized programs from running, which can be a source of infection and data leakage. The service is included in the Windows 7 security and control section of the system. For security, Microsoft recommends that companies run utilities as a normal user, without privileges. However, if for some reason (e.g. compatibility with hardware) the IT department has to assign such rights to the user, AppLocker can protect the system from running unwanted programs. The service allows administrators to indicate which applications can be launched by an employee, blocking potentially dangerous software and allowing the required applications to start at the same time.
- **Windows Multi-Touch** - Multi-Touch is a new technology embedded in Windows 7. The solution will enable full interaction with the computer using hands, mainly in mobile devices.

Fixed features

1. **Battery performance** - To extend the battery life of laptops, Windows 7 offers more intelligent power management for peripherals and running applications compared to Vista. The system shuts down more processes and suspends more applications when idle. In addition, it automatically lowers the display brightness at times when the computer is not used.
   Windows 7 also turns off the power to network ports when there are no cables connected to them. A more efficient video decoder reduces power consumption when playing DVD movies. New, clearer battery status indicators and appropriate tools allow users to fine-tune computer performance.
2. **Device Management -** Windows 7 groups all external devices together for easier management and use. Device drivers are automatically downloaded when needed, so you don't have to intervene when installing new hardware.
   Microsoft has also devoted a lot of effort to improving the kernel code, which translates into faster boot and shutdown operations. In addition, applications start faster, while the taskbar and Start menu respond much faster. Individual improvements have little impact on the operation of the system separately. However, taking all of them into account, it turns out that Windows 7 is faster and more stable than Vista.
   Windows 7 also offers improvements to the backup and restore functions (the process is way easier comparing to vista). Users can also back up a PC running Windows 7 using the network, thus eliminating the need to connect an external hard drive. Other features of Windows 7 include a new "error tolerance" tool that should significantly reduce application crashes. In addition, Microsoft has released a new feature called Process Reflection, which clones suspended processes into memory, where then "seven" tries to restore them and diagnose why they failed**.**

Other trivia

1. **Forbidden Names –** There is not possibility to create a folder named CON anywhere. Well, you just can't. Even if you try and confirm your choice of one name and no other, you will find that the computer will not accept your choice. A similar problem has been observed with names such as PRN, AUX, CLOCK $, NUL, COM1, COM2, COM3, COM4, COM5, COM6, COM7, COM8, COM9, LPT1, LPT2, LPT3, LPT4, LPT5, LPT6, LPT7, LPT8 and LPT9
2. **Origin of name -** Windows 2000 was Windows 5.0 Windows XP was Windows 5.1. Next version was Windows Vista which was codenamed Windows 6.0. Since Windows 7 is the next Windows version, Microsoft decided to call it Windows 7 for easy and better understanding. And codename of Windows 7 is Windows 6.1.

Resources

"Operating Systems" - William Stallings

"Operating Systems 9th edition" Abraham Silberschatz

https://docs.microsoft.com/en-us/windows-hardware/drivers/devtest/deadlock-detection

https://www.itprotoday.com/compute-engines/inside-windows-nt-scheduler-part-1

https://www.scribd.com/document/234675311/Deadlock-Management-of-Win-7

https://docs.microsoft.com/en-us/windows-hardware/drivers/kernel/windows-kernel-mode-hal-library

https://en.wikipedia.org/wiki/Interix

https://en.wikipedia.org/wiki/Architecture_of_Windows_NT#:~:text=The%20Win32%20environment%20subsystem%20can,for%20all%20other%20environment%20subsystems.

https://en.wikipedia.org/wiki/IA-32

https://en.wikipedia.org/wiki/X86

https://en.wikipedia.org/wiki/X86-64

https://en.wikipedia.org/wiki/Windows_NT