Windows Operating System Course

Windows History

A Personal Computer (PC) is a computer designed for use by private individuals. The typical use of a PC has been for word processing, spreadsheets, databases, Web browsing, e-mail and computer games.

The history of personal computers began in earnest in 1977, with the introduction of the microcomputer. When the microprocessor was developed, it was possible to create computers so affordable to purchase that private individuals could buy them.

When IBM (International Business Machines) began producing a Personal Computer in 1980 it created a need for an operating system for this new computer. IBM approached Microsoft with a request. Microsoft was not developing operating systems at this time, but since the mid-1970s had been a leader in the development of tools for the programming language, BASIC. Microsoft acquired an operating system by purchasing it from Seattle Computer Products, and then made changes to this system so that it was suited for PCs. Microsoft called the operating system MS-DOS.

MS-DOS

The new operating system got the name MS-DOS 1.0 DOS = Disk Operating System MS-DOS was an operating system based on a simple communication between user and computer. The user entered commands on the screen using the keyboard, as a mouse was used to a limited extent at this point.

MS-DOS was the most common operating system for PCs before Windows, and was the base operating system in the first versions of Windows. MS-DOS therefore continued to live long after the introduction of Windows.

Microsoft has made many versions of MS-DOS, with MS-DOS 8.0 being the latest version, which was launched in the year 2000.

The First Versions of Windows

The development of operating systems with a graphical user interface started in the 1980s, which was when Microsoft decided to give MS-DOS a graphical user interface. Microsoft created a graphical program for this purpose called Windows. At first, Windows was not a separate operating system, but instead a graphical application that used MS-DOS as operating system.

Windows 1.0 was the first version and came in 1983, though the first versions of Windows (1.0 and 2.0) were not a success. The reason for this was that there was little software for Windows, while the existing software was unstable and simple. It was not until Windows 3.0 and then Windows 3.1 that Windows became widely taken into use.

Version	Release	About the version
Windows 3.0	1990	Ten million copies sold.
Windows 3.1	1991	Windows becomes widespread.
Windows 95	1995	New and improved version.
Windows 98	1998	Integrating the Internet.
Windows Millennium	2000	Focus on multimedia.

The operating systems Windows 95, Windows 98 and Windows Millennium were quite similar, so they were therefore called Windows 9x.

Windows 95

Windows 95 was a major improvement from earlier versions of Windows, central to this being an enhanced usability and better networking capabilities. The new features in Windows 95 were multitasking and the automatic detection and configuration of equipment (Plug and Play).

Windows 98

Windows 98 was an upgrade and improvement of Windows 95, as Microsoft wanted to implement the Internet in Windows at this time. As a result, Windows 98 contained Internet Explorer and other programs for the Internet.

Windows Millennium

Windows Millennium was the last release in the series based on the Windows 9x platform, and was aimed at the domestic market with a focus on multimedia.

Windows NT

Computers acquired more and more memory, a higher processor speed and more disk space. MS-DOS could not handle a lot of memory, and could not run multiple applications simultaneously, so there was a need for a new operating system. This led to the developing of Windows NT, in which NT stands for New Technology.

Microsoft released the first version of Windows NT in 1993 and called it Windows NT 3.1, because it came at the time when Windows 3.1 was in use. Windows NT 3.1 had the same appearance and user interface as Windows 3.1, but they were completely different operating systems.

Windows NT 4.0 came in 1996, with the two basic versions of Windows NT 4.0 being:

• Windows NT Server

• Windows NT Workstation

Windows NT 4.0 Server was a network operating system designed to be used on servers in local networks. Windows NT 4.0 Workstation was designed for use on both home computers and workstations, but was primarily used by companies as workstations in local networks.

Windows NT 4.0 was an advanced 32-bit operating system designed to be secure, stable and flexible, thus making it possible to use multiple processors on the same computer. Windows NT 4.0 could utilize a large memory and large hard drives, which meant that the operating system was well scalable.

Windows NT introduced users as a part of the system's security model, so in order to use a workstation in a modern Windows system you must be a registered user. One can define multiple users on a workstation, and each user has certain rights to files and to access system resources in general.

Windows Versions Based On Windows NT

Windows NT operating system is the basis for the current versions of Windows.

Version	Release	About the version
Windows 2000	2000	Was not intended for home computers.
Windows XP	2001	Both for home computers and workstations.
Windows Vista	2006	New user interface with Windows Aero.
Windows 7	2009	Emphasis on functionality and performance.
Windows 8	2012	New graphical interface Microsoft Metro.
Windows 10	2015	Better functionality between different classes of device.

Windows NT has become a widespread operating system in the computer world, as today you can find variations of the original Windows NT on laptops, desktops, servers and Xbox consoles worldwide.

Windows 2000

Windows 2000 (Windows NT 5.0) was built on Windows NT 4.0. In addition, Windows 2000 had most of the useful qualities of Windows 98, such as support for Plug and Play. Windows 2000's operating system was available in several versions. One version was for workstations, and there were several versions for servers.

Windows XP

Launched in August 2001, Windows XP (Windows NT 5.1) has been the most popular version of Windows, based on the number of copies sold.

Windows Vista

Launched in November 2006, Windows Vista (Windows NT 6.0) contained hundreds of new and revised features.

Windows 7

Windows 7 (Windows NT 6.1) came in October 2009. Unlike previous versions of Windows, Windows 7 did not contain many new features, basically being more of an upgrade of Windows Vista. The objective of Windows 7 was an operating system that had increased functionality and performance over previous versions.

Windows 8

Windows 8 (Windows NT 6.2) came in October 2012, and contained a new graphical interface known as Metro, which is used for tablets, laptops, desktops and Windows Phone. Optimized for touch screens, Metro can also be controlled with a mouse and keyboard.

Windows 10

Windows 10 (Windows NT 10.0) came in July 2015. Windows 10 is intended as the last version as there will be no Windows 11. Instead Windows Update will update the existing Windows 10 to new versions. At this point there have been three such updates, one in November 2015 (version 1511), one in July 2016 (version 1607) and one in Mars 2017 (version 1703).

Microsoft described Windows 10 as an *operating system as a service* that would receive ongoing updates to its features and functionality. Windows 10 harmonizes the user experience and functionality between different classes of device, and addresses shortcomings in the user interface that were introduced in Windows 8.

Windows 10 has become a shared platform known as OneCore, and it runs on PCs, phones, the Xbox One game console, the HoloLens and Internet of Things (IoT) devices such as Raspberry Pi 2.

Windows Server

Microsoft has made several versions of the Windows operating system adapted to act as a server in local networks.

Microsoft's first attempt at creating an operating system with network features was Windows 3.11 (1992). Another name for Windows 3.11 is Windows for Workgroups, and this version had some additional features that gave network support:

- Network cards and cables
- Sharing directories, disks and printers
- E-mail and instant messaging functionality

However, it was with Windows NT that Microsoft began developing a network operating system intended to act as a server.

Version	Release
Windows NT 4.0 Server	1996
Windows Server 2000	2000
Windows Server 2003	2003
Windows Server 2008	2008
Windows Server 2012	2012
Windows Server 2016	2016

Windows NT 4.0 Server

It was first with Windows NT 4.0 that Microsoft got a proper network operating system adapted to the task as a server in a local area network, as the Windows NT 4.0 Server could serve many users in a network.

Windows Server 2000

The sequel to Windows NT 4.0 Server was Windows Server 2000. The main novelty in Windows Server 2000 was Active Directory, which is Microsoft's directory service for managing users and resources in a local area network.

Windows Server 2003

Built on Windows XP, Windows Server 2003 had several improvements over Windows Server 2000. New in Windows Server 2003 was the Internet Information Services (IIS) used to create web pages for servers.

Windows Server 2008

Launched in February 2008, Windows Server 2008 was an upgrade of Windows Server 2003. Windows Server 2008 had enhancements to Active Directory, Group Policy, disk management and security.

Windows Server 2012

Windows Server 2012, also called Windows Server 8, debuted in September 2012. New with Windows Server 2012 was better support for server virtualization and the use of the cloud (Cloud Computing). Windows Server 2012 includes a new file system (ReFS), but this file system is only used by file servers.

Windows Server 2016

With Windows Server 2016, Microsoft aims to assist customers in modernizing on premise data centers, making it easier to move workloads out to its Azure public cloud. New in Windows Server 2016 is Nano Server. Nano Server is a scaled down, purpose-built operating system designed to run modern cloud applications and act as a platform for containers.

Support for containers is another of the standout features for Windows Server 2016.

The Tasks of an Operating System

There are two types of software running on a computer: software applications and system software. A software application is a program designed for end users, while system software consists of low-level programs belonging to the operating system, compilers and utilities for managing resources.

An operating system is software that enables services for software applications to run on a computer. An important task of an operating system is taking care of the communication between the software applications and hardware devices attached to your computer. For example, a word processor communicates with devices such as a keyboard and mouse.

Operating systems are large programs consisting of thousands of functions, which provide services of various kinds. Often called by events in the system, the functions perform a service when needed. To make operating systems fast and most effective, the functions are often written in C or C++, but also low-level programming languages such as Assembly has occasionally been used.

Construction of Computers

To understand the tasks of an operating system, it is necessary to have some knowledge of computer systems. In this text, there will be no detailed description of the constructions of computers, but we will look at some key components of the computer system and show why these need to be administered by an operating system.

A processor executes the instructions that a computer program is comprised of. The processor is therefore the central unit of program execution.

Several applications are often simultaneously executed on a computer. It is therefore a task for the operating system to launch programs and allocate time for programs in one or more processors.

The applications running are loaded into a computer's memory for storage. Consequently, it is therefore necessary to keep track of where in the memory different data resides. In addition, there is a need to keep track

of which parts of the memory are available and which parts are in use. Managing computer memory is a task for the operating system.

Files are stored on a hard disk. The operating system keeps track of where files on the hard disk are situated, as well as what parts of the hard disk are in use and what parts are not in use.

Input/output means communication between software applications and screen, keyboard, mouse and similar devices. The operating system takes care of the input/output to make it easier for applications to communicate with different drivers for input/output devices.

Item	Description
Processor	A processor is the part of the computer system that is able to execute program code.
Memory	Computer memory is a temporary storage location for data and the program code. Data is lost in the memory when the power of the computer is turned off.
Hard drive	The task of hard drives is to permanently store data on a computer. The hard drives store program files, documents and data files.
Input/output devices	Equipment used for communication between the computer and a user. The most common input/output devices are the keyboard, mouse and screen.

In addition to creating services for the computer system, it is a task for an operating system to provide a user interface for the computer. Windows has a graphical user interface in which the user uses the keyboard, mouse and touch screen to interact with applications.

Central Tasks for an Operating System

We want fast and reliable computers; hence, an important task for an operating system is to utilize computer resources in the best possible way.

There are two main goals of an operating system:

• Managing applications and giving applications access to hardware.

• Manage data system resources optimally.

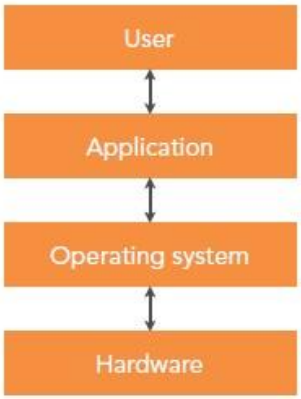
Important tasks for an operating system are to:

1. Manage applications running on the computer.
2. Take care of input and output.
3. Manage communication between software applications and hardware.
4. Manage computer memory.
5. Manage the file system.
6. Manage networking.
7. Take care of the security of the computer system.
8. Provide a user interface for the computer.

The operating system manages applications running on the computer. The operating system starts and stops applications, and provides time for applications in the processor.

An important task for an operating system is to help facilitate communication between applications and hardware, while user applications access the hardware through the operating system.

An operating system is a layer between applications and hardware. A user interacts with an application, the application interacts with the operating system and the operating system communicates with hardware.



Hardware equipment consists of various types and uses different drivers, whereas the operating system takes care of the communication with the hardware. This makes it much easier to create computer programs since programmers do not need to consider communication with different drivers.

Modern operating systems use multitasking, which allows multiple applications to run simultaneously, thereby making it possible to perform more than one action on the computer at approximately the same time. To help achieve this, programs take turns running in the processor. An application executes in a processor for a short time before it must be out of the processor, and another application is loaded into the processor for execution.

Data security is important when using computer technology, particularly for computers attached to a network. The objective of computer security is therefore to provide information and data against unauthorized access, theft, destruction and natural disasters.

32-bit and 64-bit architecture refers to the length of the memory address used by the processor. The 64-bit version of Windows, which handles large amounts of RAM (Random Access Memory), is more effective than a 32-bit system. However, much of today's software was made during the 32-bit time. To fully benefit from a 64-bit operating system, you must have software optimized for 64-bit processing.

Device Drivers

Drivers are control programs that enable communication between hardware devices and the operating system, and are necessary for Windows to communicate with hardware.

Windows includes installation drivers that support a huge number of different hardware devices. Thousands of drivers are available through a Windows Update, and there are hundreds of new drivers every month.

Device Drivers are small programs designed to help applications at a higher level to communicate with hardware. Device Drivers are running in kernel mode, and provide an interface between the input/output manager and hardware.

There are several types of device drivers. The following provides an overview of some of them:

- Drivers for hardware devices. Using the hardware layer, these drivers take care of input/output for physical equipment.
- File system drivers are Windows drivers that take care of input/output to files.
- File system filter drivers perform tasks such as encryption or writing data to more than one disk. They also do scanning to locate viruses. File system drivers for the network transfer the file system input/output to other computers at a network.
- Protocol drivers implement a networking protocol such as TCP/IP or NetBUI.
- Software drivers are kernel modules that perform operations that can only be done in kernel mode on behalf of some user mode process.

Memory Management

Managing memory concerns in terms of how to allocate memory for programs and how to free memory that is no longer needed. How this is done will affect computer performance, which makes memory management an important task in a computer system.

The following provides an overview of some of the problems with memory management:

1. There must be space for several programs in the memory at the same time.
2. There may not be room for all programs in the memory at the same time.
3. Programs will have different addresses in the memory at different runs

Input and Output

A computer is connected to devices such as a screen, keyboard, mouse, hard disk, printer, CD/DVD, etc. An important task for an operating system is to communicate with the input/output devices connected to the computer.

Input and output have been a problem in operating systems. One reason for this is the large difference in speeds within a computer system.

In the processor and the memory, data processes very quickly, though by comparison communication with peripheral devices is very slow. To write to the screen or to a file is a slow process. A user typing on a keyboard can wait several seconds before he types a character, while for the processor, it is not a good use of time to wait for input/output devices.

Type of equipment	*Transfer speed*
Keyboard	10 bytes/second
Mouse	100 bytes/second
SAS disk	129 Mb/second
SSD disk	241 Mb/second
USB 3.1	1250 Mb/second

Another challenge with input/output is that hardware connecting to a computer is from different manufacturers. For example, there are many types of screens, and these require separate drivers. It would hence be cumbersome if programmers had to create code for each type of screen driver that might be using the program.

The operating system takes care of the communication with the screen, mouse, printers and similar equipment. Applications can therefore work on different computers with different hardware devices connected.

The operating system takes care of errors that can occur when communicating with input/ output devices. The operating system should be able to:

1. Detect errors.
2. Correct mistakes.

Many errors can occur when using input/output devices. The operating system should be able to detect whether a process tries to write to a file opened for reading, and also recognize corrupt data.

Sometimes the operating system successfully corrects errors that occur. If the operating system is able to correct a mistake, it will not normally notify the program where the error occurred.

File Systems in Windows

A file system stores and organizes the files on a hard disk, so it is desirable that it should be easy to find and retrieve files. File systems are therefore made for this purpose. To take care of files and file management, the Windows operating system uses the File Manager. The mission of the File Manager is to organize the files so that users can obtain them quickly and easily.

In the Windows operating system, there are three file systems used on hard drives: there are the NTFS file system, the older FAT and FAT32. Windows also supports file systems for CD-ROM and DVD.

FAT

FAT is an abbreviation for File Allocation Table, and is the file system used in MS-DOS and early versions of Windows. There have been several versions of FAT, including FAT12, FAT16, FAT32 and exFAT.

FAT12 was a 12-bit address system designed for floppy disks, while FAT16 was developed when PCs with hard disks were taken in use. The first versions of MS-DOS and the very first versions of Windows used FAT12 and FAT16, which are no longer in use.

The early versions of the Windows operating system were Windows 95, Windows 98 and Windows Millennium, all of which used FAT32, and which is no longer in general use. Although Windows do not use FAT any more, FAT is still in use. FAT is a useful format for solid-state memory cards and it is often used as file system on SD cards.

exFAT, which is also called FAT64, is a newer version of FAT. exFAT is designed for smaller storage devices such as USB pens, so is therefore a version of FAT still in use.

NT File System

The NT File System (NTFS) is the file system developed for Windows NT, and is the file system that current versions of Windows use. NTFS supports long file names, security, fault tolerance, encryption, disk compression and very large files and volumes.

NTFS has several advantages over FAT32 when it comes to safety, reliability, extensibility and efficiency.

Safety

Security is enhanced by the fact that users are given access to just the directories and files they need. In FAT32, all users could access all the files on a hard disk.

Reliability

NTFS keeps track of changes in the file system by keeping a journal. NTFS uses log files to keep track of all disk activity, which allows an NTFS volume to recover quickly after a disk crash.

Extensibility

Using NTFS formatted volumes can expand the storage capacity to existing volumes without having to take backup, to repartition, to reformat or to restore anything.

Efficiency

NTFS volumes will manage partitions larger than 8 GB of memory more efficiently than the old FAT32 file system.

Compression

NTFS supports the compression of files and directories. You can create a file as compressed, and then NTFS automatically compresses the contents of the file.

File names

A file name in NTFS can be up to 255 characters long. File names are in Unicode, which means that you can use file names in character sets other than Latin, e.g. Greek, Chinese, Russian, etc.

Storage Management

Storage Management defines how operating systems interact with disks and storage media. Windows provides support for many types of storage media, including hard drives, USB drives, tape drives and network storage such as SAN (Storage Area Networks) and iSCSI (Internet Small Computer System Interface).

There are different ways to organize the data storing in a computer system. A PC typically only has one volume on one hard drive. However, it may be beneficial to organize a disk by dividing it into several volumes.

Volumes used by servers will often extend across multiple hard drives, the purpose of this being to increase the reading speed and security.

Partitions

A hard drive consists of one or more partitions, which is a section of a hard drive. Each partition can then function as a separate disk. A partition is a collection of contiguous sectors on a disk. A partition table or other databases for disk management stores the starting sector and the size of the partitions.

The task of the Partition Manager is to create, delete and manage partitions, thereby ensuring that all partitions have a unique ID.

Volumes

The storage on a computer is divided into volumes designated by a letter such as C, D or E. A simple volume is only one partition, but you can organize volumes so that they consist of multiple partitions on one or more hard drives.

A simple volume uses only one hard drive, which means that if the hard disk crashes, the volume is out of use. Using multiple volumes and multiple disks avoids this, hence you can still access data even if one hard drive is not functioning.

There are two types of volumes:

1. Simple volumes representing sectors on a single partition
2. Multi-partition volumes representing sectors from multiple partitions

Advantages of multi-partition volumes are performance, reliability and the size of volumes.

Storing Data on Servers

Networked computers offer new possibilities for data storage. The organizing of data storage on servers is usually done in another way than for a single PC.

SAN

A SAN (Storage Area Network) is a storage medium that is available to servers via a network so that it looks as if the storage media is located locally on the server.

iSCSI

iSCSI (Internet Small Computer System Interface) is a network standard based on IP (Internet Protocol) to access a storage device via a network. The purpose of iSCSI is to help facilitate data transmission over the network and manage the storage of data over long distances.

Data Storage in a Cloud

Data can be stored in a Cloud. You can store your data on servers that are located at remote server parks connected to the Internet. Instead of having your own storage system in a LAN, you can rent storage space on a server via the Internet.

Networking Features in Windows

The first of Microsoft's operating systems had little network support, although Windows NT was developed to function in a network. In today's Windows, there is broad support for network tasks in the input/output system and the Windows API.

The common task for a network application is to take a request from an application on one computer and send it to another computer. The remote computer then performs the request and sends back the result.

An operating system hence needs services that enable communication between computers. A Windows operating system has networking software just for this purpose.

There are four types of networking software in Windows:

- Network services
- Network APIs
- Protocols
- Drivers

Network services

Windows has several network services based on the API components. Two of these are Remote Access and Active Directory.

Remote Access

Remote Access allows clients to associate a connection to servers so that they can obtain resources via a network connection. This may be resources on a server such as files, printers and network services. Windows allows two types of remote access, which are a dial-up connection and a Virtual Private Network (VPN).

A dial-up connection allows clients to connect to a server via telephone lines or a similar infrastructure. Dial-up is a temporary physical or virtual connection between a client and a server.

Remote Access with VPN establishes a connection to a server over an IP network such as the Internet. You can log on with VPN to a server in local network from anywhere in the world via the Internet.

Active Directory

Active Directory is a tool used to manage a local network using a Windows Server operating system, and is a directory that provides an overview of all users and all devices in the network. With Active Directory, a network administrator organizes users and computers in groups.

In large networks, it is necessary for group users and computers to maintain an overview of the network. Active Directory makes it possible to manage very large networks with up to millions of users.

Network APIs

Network APIs are network functions in Windows API. Windows has several network APIs that provide support for software, and applications can use these to communicate with programs on other computers.

Some network APIs include Windows Sockets, Remote Procedure Call, Named Pipes and Mailslot's.

Windows Sockets

Windows Sockets API, also called Winsock, is a technical specification that defines how Windows network software should cooperate with network services such as TCP/IP. Windows Sockets provides an interface between a Windows TCP/IP client program and the underlying TCP/IP protocol.

Windows Sockets makes it possible for developers to create advanced network of applications for both the Internet and intranet using Microsoft Windows networking functions, regardless of the network protocol used.

Remote Procedure Call

Remote Procedure Call (RPC) is a type of process communication that allows a computer to execute code on another computer over a network, without the programmer having to code the details of the communication. In other words, the programmer writes about the same code, whether the code is executed on the local computer or

on a remotely located computer. RPC therefore makes the communication process as simple as a function call, operating between processes at different computers in a network.

Named Pipes

Named Pipes is a programming API for communication between processes, which takes place between a named pipe server and a named pipe client. A named pipe server is a program that creates a named pipe that clients can use, as data is transferred via a buffer. A process writes data to a buffer so that another process can read the data from the buffer.

In Windows, Named Pipes is a client/server communication that works quite similarly to Sockets.

Mailslot

Mailslot is a broadcast mechanism for one-way communication that allows communication between processes, both locally and over a network. The messages are usually sent via a local network or an Internet network. A process that creates a mailslot is called a mailslot server.

Other processes (clients) can send messages to a mailslot server that has a name. Mailslot´s provides a simple way of sending short messages.

Drivers

Network API drivers take API requests and translate them into network protocol requests, so that it is possible to send them via a network. API drivers use transport protocol drivers to do this translation.

In 1989, 3Com and Microsoft developed NDIS (Network Driver Interface Specification), which allows protocol drivers to communicate with network adapter drivers. NDIS is independent of the type of equipment used by a computer. Network adapter drivers that use NDIS are called NDIS drivers or NDIS miniport drivers.

Transport Driver Interface (TDI) is an interface developed by Microsoft to make it easier for drivers to communicate with various network transport protocols. The advantage of using TDI is that services are independent of different protocols for transport in networks.

TDI transports, also called transports and NDIS protocol drivers, are drivers in kernel mode. They receive packets from TDI and send them further. NDIS miniport drivers are drivers in kernel mode, which provides an interface for TDI transports to network adapters.

Security in Windows

In a computer system, there is often sensitive data, to which it is not desirable that there should be public access. The operating system must be able to protect files, memory and setup data so that unauthorized persons cannot read or modify the data.

There are four groups of security for computer systems.

1. Data Confidentiality
2. Data Integrity
3. Access to the system
4. Attacks from outside

Data Confidentiality concerns how to prevent unauthorized access to data on computers. This is important for protecting documents to prevent unauthorized persons from gaining access to- or reading them. This applies not only to secret documents, but also personal data that could be sensitive.

Data Integrity is about preventing unauthorized changes to data in files. This applies not only to a change of data, but also to remove or to add false data. An example of this is a student who will attempt to get into the school's computer system to change his/her grade.

Access to the system revolves around nobody being allowed to disturb the system or to put it out of operation.

Attacks from outside concerns the preventing of attacks via the Internet, as hackers may attempt to gain control of computers via the Internet. One way to do this is by the use of a virus. By gaining control of a computer, hackers can use the computer for illegal activities or to send e-mails (spam).

With Windows NT came the following security in the Windows operating system:

- Secure login
- Access control for files
- Privileged access control
- Address space defense for each process
- Clearance of pages in memory
- Auditing of computer systems

Secure login means that all users use a password to login. Ctrl + Alt + Delete has been used to login, the purpose of the Ctrl + Alt + Delete being that no one should be able to add fake login windows to capture users' passwords.

Access control to files allows a user who owns a file to decide who else can access the file. Privileged access control means that the administrator has the right to determine access to files if needed, i.e. the administrator can change users' rights.

Address space defense for each process means that each process has protected addresses that unauthorized processes cannot access.

The clearance of pages in a memory means that new pages loaded into the memory will not be able to find information left behind by the previous pages. This makes it difficult for spyware to snoop into memory.

Auditing means that the system writes events in a network that may affect safety to a log file. The administrator will then be able to get information about what is happening on the system by reading the log files. The administrator can decide which events to monitor, and such events can be:

- Someone tries to do something on the system that is not allowed.
- Someone attempts to log on several times because the login fails.

Security Mechanisms in Windows

Microsoft has put a lot of resources into making the Windows operating system more secure. The reason is that in recent years there have been more and more attacks against computer systems around the world, and some of these attacks have been successful. Such attacks have managed to put the computer systems of entire countries or large businesses, which can cost society billions of dollars.

The Windows operating system therefore has a highly developed security system, which is based on access control and integrity levels. We will now look at how security system protects Windows processes and data.

Security ID

There is a need to identify devices such as threads, which can perform operations on the system. Instead of using names to identify such devices, the Windows operating system uses a SID (Security ID). A SID is a number, and each SID is unique in the world.

A SID can be assigned to either a user or group of users in a network. When a process starts, the process and the threads run under the user's SID. Other threads will not be able to access the process unless they have a SID with special authorization to do so.

Security Descriptor

Each process has information about its reliability that tells what privileges the user and the process have. Each process has a Security Descriptor attached that a Security Descriptor points to for controlling lists. These checklists contain access information that can deny access for users or groups of users.

Access to Objects

Central to the security of the Windows operating system is the protection of objects. Windows has a comprehensive security model that prevents unauthorized access to objects, which requires that before a thread can have access to an object, it must first specify what actions it will perform on the object.

Objects protected in the Windows operating system include files, hardware devices, mailslot's, pipes, processes, threads, events, Mutex's, semaphores, shared memory, input/output ports, timers, volumes, network shares, services, printers, etc.

Defense Against to Malwares

Windows Defender, also known as Microsoft Anti Spyware, is a program from Microsoft that has the function to prevent, remove and isolate spyware in Microsoft Windows. Windows Defender uses two mechanisms to detect spyware:

1. Scanning
2. Real Time protection

Windows Defender scans your computer and control programs against a database of information about spyware. Windows Defender is malware protection that helps identify and remove viruses, spyware, and other malicious software. Windows Defender runs in the background and notifies you when you need to take specific action. However, you can use it anytime to scan for malware if your computer isn't working properly or if you clicked a suspicious link online or in an email message.

Real Time Protection is a process that runs in the background and is looking for spyware that tries to install itself or run on your computer.

Windows Defender can also remove ActiveX applications and block programs that start automatically at Windows startup. Windows Defender is included in Windows Vista, Windows 7, Windows 8 and Windows 10.

A firewall is a part of a computer system or network designed to block unauthorized access and to allow authorized access. Both hardware and software can implement firewalls.

The purpose of a firewall is to prevent unauthorized Internet users from accessing local network connected to the Internet, especially intranets. The firewall will investigate all messages entering or leaving the intranet through the firewall, and will also block messages if the safety criteria do not hold.

The firewall in Windows filters both incoming and outgoing packets. All incoming packets to your computer are blocked unless they are a response to a request from your computer, while all outgoing packets from your computer are permitted unless they violate a set rule.

Windows Firewall was first introduced as part of Windows XP Service Pack 2, and later versions of Windows have improved the Firewall.

Updating Windows

An important part of keeping a computer system safe is to obtain the latest upgrades to the operating system. Microsoft is constantly working on new upgrades; this may be updated drivers or improvements of code that have contained faults.

Many upgrades just give improvements in performance and functionality, but some are also security updates to the system. Windows include Windows Update, which is a program that updates the Windows operating system for computers all over the world once a month. Using automatic updates, a Windows operating system upgrades itself over the Internet without having to use a browser. The upgrade is usually the second Tuesday of the month. However, critical upgrades can take place more often if necessary.

Windows Crashes

Many conditions can cause Windows to crash. If there is a system crash, Windows stops and displays the blue screen.

The Blue Screen

The blue screen (The Blue Screen of Death) will appear in Windows when it has encountered a critical system failure. The system then goes down to prevent the occurrence of serious faults that could damage the system.

According to Microsoft, the reason Windows shows the blue screen is poorly programmed drivers or hardware that is not working properly. The blue screen can also be a result of memory error, power failure, overheated components or hardware used in an improper way.

Often, the blue screen appears when you install new software or new hardware. For example, if you have installed a new driver and tried to reboot, you can get the blue screen. You will then have the opportunity to undo the installation and get back the old configuration.

A question is why errors cause Windows to crash. Why does the system not ignore the error and just continue? The reason is that the error that causes windows to crash is often part of a larger problem. To let Windows continue will lead to more and more serious errors. The blue screen has been in all versions of Windows since Windows 3.11 (1993).

Reasons that Windows Can Crash

Windows may crash for various reasons. A detailed description of all circumstances that may cause Windows to crash will be very extensive. In the following, we shall therefore only look at a few reasons:

Storage failure

The most common reason that Windows crashes is storage failure (Pool Corruption). Pool corruption can occur when a driver runs into problems because a buffer cannot accommodate all the data it receives. Pool corruption can also occur if a driver writes to a storage place that it had before, but has given up.

Page Fault in memory

An error on a page in memory (Page Fault) can lead to system crash.

Poor or no power supply

A driver or a function associated with the operating system will not work without power. Poor power or a lack of power can thus cause Windows to crash.

Access Violation

An access violation occurs if there is an attempt to write to a page into a memory that is only allowed to read, or if the system tries to read an address that does not exist.

Error in memory

If the Memory Manager detects that a data structure in a memory is corrupt, this can cause a system crash.

Hardware

Errors in hardware can cause system crashes. This includes errors on a disk when the memory manager attempts to read data.

USB pen

If an error occurs while performing an operation on a USB pen, this can lead to a system crash.

Error in the file system

A fatal error in the file system can lead to system crash.