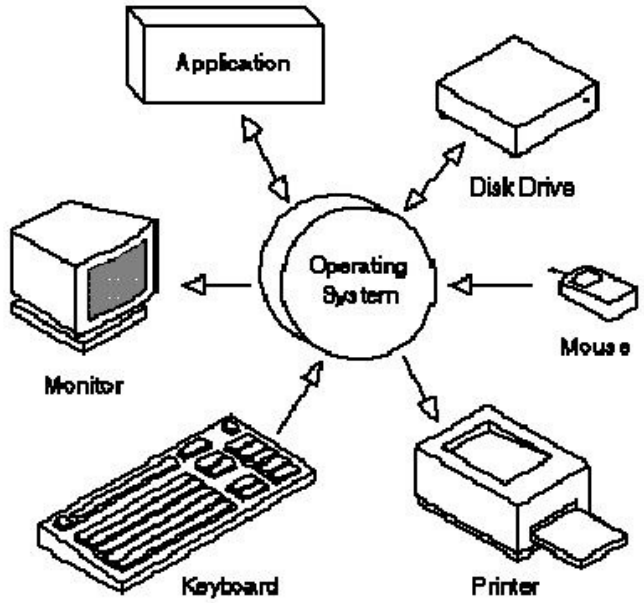
An **operating system** (**OS**) is software that manages computer hardware and software resources and provides common services forcomputer programs. The operating system is an essential component of the system software in a computer system. Application programs usually require an operating system to function.

Examples of popular modern operating systems include Android, BSD, iOS, Linux, OS X, QNX, Microsoft Windows, Windows Phone, and IBM z/OS. The first six of these examples share roots in UNIX.

# Types of operating systems




## *Classification of Operating systems*

- **Multi-user:** Allows two or more users to run programs at the same time. Some operating systems permit hundreds or even thousands of concurrent users.
- **Multiprocessing :** Supports running a program on more than one CPU.
- **Multitasking :** Allows more than one program to run concurrently.
- **Multithreading :** Allows different parts of a single program to run concurrently.
- **Real time:** Responds to input instantly. General-purpose operating systems, such as DOS and UNIX, are not real-time.

### Single- and multi-tasking

A single-tasking system can only run one program at a time, while a multi-tasking operating system allows more than one program to be running in concurrency. This is achieved by time-sharing, dividing the available processor time between multiple processes which are each interrupted repeatedly in time-slices by a task scheduling subsystem of the operating system. Multi-tasking may be characterized in pre-emptive and co-operative types. In pre-emptive multitasking, the operating system slices the CPU time and dedicates a slot to each of the programs. Cooperative multitasking is achieved by relying on each process to provide time to the other processes in a defined manner.

### Single- and multi-user

Single-user operating systems have no facilities to distinguish users, but may allow multiple programs to run at the same time. A multi-user operating system extends the basic concept of multi-tasking with facilities that identify processes and resources, such as disk space, belonging to multiple users, and the system permits multiple users to interact with the system at the same time. Time-sharing operating systems schedule tasks for efficient use of the system and may also include accounting software for cost allocation of processor time, mass storage, printing, and other resources to multiple users.

### Distributed

A distributed operating system manages a group of distinct computers and makes them appear to be a single computer. The development of networked computers that could be linked and communicate with each other gave rise to distributed computing. Distributed computations are carried out on more than one machine. When computers in a group work in cooperation, they form a distributed system

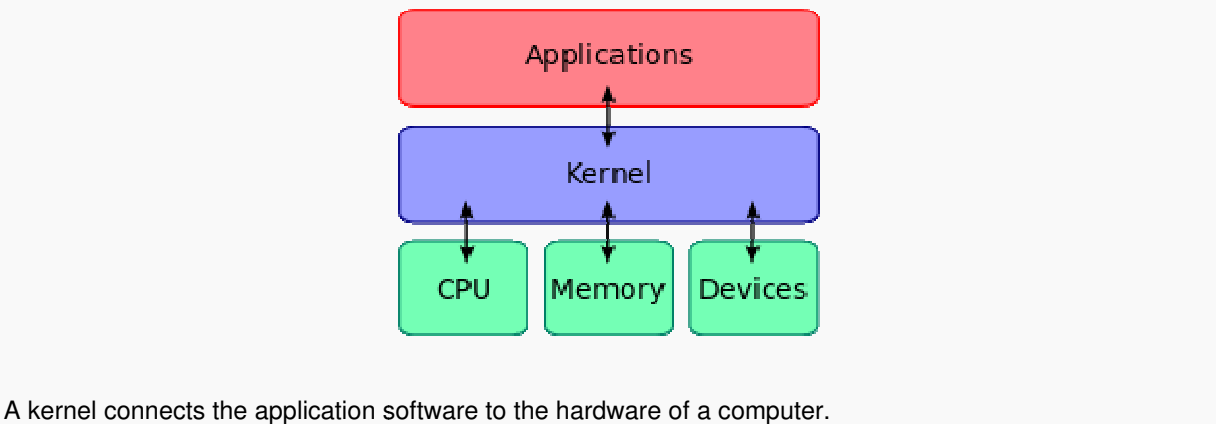
### Real-time

A real-time operating system is an operating system that guaranties to process events or data within a certain short amount of time. A real-time operating system may be single- or multi-tasking, but when multitasking, it uses specialized scheduling algorithms so that a deterministic nature of behavior is achieved. An event-driven system switches between tasks based on their priorities or external events while time-sharing operating systems switch tasks based on clock interrupts.

## Components

The components of an operating system all exist in order to make the different parts of a computer work together. All user software needs to go through the operating system in order to use any of the hardware, whether it be as simple as a mouse or keyboard or as complex as an Internet component.

### Kernel




A kernel connects the application software to the hardware of a computer.

#### Program execution

The operating system provides an interface between an application program and the computer hardware, so that an application program can interact with the hardware only by obeying rules and procedures programmed into the operating system. The operating system is also a set of

services which simplify development and execution of application programs. Executing an application program involves the creation of a process by the operating system kernel which assigns memory space and other resources, establishes a priority for the process in multi-tasking systems, loads program binary code into memory, and initiates execution of the application program which then interacts with the user and with hardware devices.

**Interrupts**

Interrupts are central to operating systems, as they provide an efficient way for the operating system to interact with and react to its environment. The alternative — having the operating system "watch" the various sources of input for events (polling) that require action — can be found in older systems with very small stacks (50 or 60 bytes) but is unusual in modern systems with large stacks. Interrupt-based programming is directly supported by most modern CPUs. Interrupts provide a computer with a way of automatically saving local register contexts, and running specific code in response to events. Even very basic computers support hardware interrupts, and allow the programmer to specify code which may be run when that event takes place.

**Memory management**

Among other things, a multiprogramming operating system kernel must be responsible for managing all system memory which is currently in use by programs. This ensures that a program does not interfere with memory already in use by another program. Since programs time share, each program must have independent access to memory.

Cooperative memory management, used by many early operating systems, assumes that all programs make voluntary use of the kernel's memory manager, and do not exceed their allocated memory. This system of memory management is almost never seen any more, since programs often contain bugs which can cause them to exceed their allocated memory. If a program fails, it may cause memory used by one or more other programs to be affected or overwritten. Malicious programs or viruses may purposefully alter another program's memory, or may affect the operation of the operating system itself. With cooperative memory management, it takes only one misbehaved program to crash the system.

Memory protection enables the kernel to limit a process' access to the computer's memory. Various methods of memory protection exist, including memory segmentation andpaging. All methods require some level of hardware support (such as the 80286 MMU), which doesn't exist in all computers.

In both segmentation and paging, certain protected mode registers specify to the CPU what memory address it should allow a running program to access. Attempts to access other addresses trigger an interrupt which cause the CPU to re-enter supervisor mode, placing the kernel in charge. This is called a segmentation violation or Seg-V for short, and since it is both difficult to assign a meaningful result to such an operation, and because it is usually a sign of a misbehaving program, the kernel generally resorts to terminating the offending program, and reports the error.

Windows versions 3.1 through ME had some level of memory protection, but programs could easily circumvent the need to use it. A general protection fault would be produced, indicating a segmentation violation had occurred; however, the system would often crash anyway.

**Multitasking**

Multitasking refers to the running of multiple independent computer programs on the same computer; giving the appearance that it is performing the tasks at the same time. Since most

computers can do at most one or two things at one time, this is generally done via time-sharing, which means that each program uses a share of the computer's time to execute.

**Disk access and file systems**

Access to data stored on disks is a central feature of all operating systems. Computers store data on disks using files, which are structured in specific ways in order to allow for faster access, higher reliability, and to make better use out of the drive's available space. The specific way in which files are stored on a disk is called a file system, and enables files to have names and attributes. It also allows them to be stored in a hierarchy of directories or folders arranged in a directory tree.

## Networking

Currently most operating systems support a variety of networking protocols, hardware, and applications for using them. This means that computers running dissimilar operating systems can participate in a common network for sharing resources such as computing, files, printers, and scanners using either wired or wireless connections. Networks can essentially allow a computer's operating system to access the resources of a remote computer to support the same functions as it could if those resources were connected directly to the local computer. This includes everything from simple communication, to using networked file systems or even sharing another computer's graphics or sound hardware. Some network services allow the resources of a computer to be accessed transparently, such as SSH which allows networked users direct access to a computer's command line interface.

## Security

A computer being secure depends on a number of technologies working properly. A modern operating system provides access to a number of resources, which are available to software running on the system, and to external devices like networks via the kernel.

The operating system must be capable of distinguishing between requests which should be allowed to be processed, and others which should not be processed. While some systems may simply distinguish between "privileged" and "non-privileged", systems commonly have a form of requester *identity*, such as a user name. To establish identity there may be a process of *authentication*. Often a username must be quoted, and each username may have a password. Other methods of authentication, such as magnetic cards or biometric data, might be used instead. In some cases, especially connections from the network, resources may be accessed with no authentication at all (such as reading files over a network share). Also covered by the concept of requester **identity** is *authorization*; the particular services and resources accessible by the requester once logged into a system are tied to either the requester's user account or to the variously configured groups of users to which the requester belongs.

## User interface

Every computer that is to be operated by an individual requires a user interface. The user interface is usually referred to as a shelland is essential if human interaction is to be supported. The user interface views the directory structure and requests services from the operating system that will acquire data from input hardware devices, such as a keyboard, mouse or credit card reader, and requests operating system services to display prompts, status messages and such on output hardware devices, such as a video monitor or printer. The two most common forms of a user interface have historically been the command-line interface, where computer commands are typed out line-by-line, and the graphical user interface, where a visual environment (most commonly aWIMP) is present.

**Graphical user interfaces**

Most of the modern computer systems support graphical user interfaces (GUI), and often include them. In some computer systems, such as the original implementation ofMac OS, the GUI is integrated into the kernel.

While technically a graphical user interface is not an operating system service, incorporating support for one into the operating system kernel can allow the GUI to be more responsive by reducing the number of context switches required for the GUI to perform its output functions. Other operating systems are modular, separating the graphics subsystem from the kernel and the Operating System. In the 1980s UNIX, VMS and many others had operating systems that were built this way. Linux and Mac OS X are also built this way. Modern releases of Microsoft Windows such as Windows Vista implement a graphics subsystem that is mostly in user-space; however the graphics drawing routines of versions between Windows NT 4.0 and Windows Server 2003 exist mostly in kernel space. Windows 9x had very little distinction between the interface and the kernel.

# Defragmentation

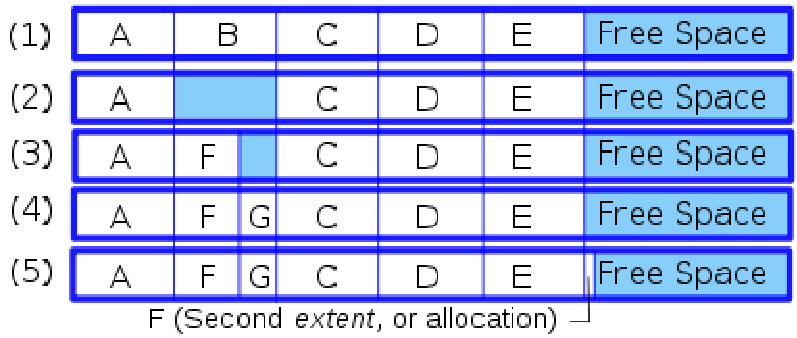
In the maintenance of file systems, **defragmentation** is a process that reduces the amount of fragmentation. It does this by physically organizing the contents of the mass storage device used to store files into the smallest number of contiguous regions (fragments). It also attempts to create larger regions of free space using compaction to impede the return of fragmentation. Some defragmentation utilities try to keep smaller files within a single directory together, as they are often accessed in sequence.

Defragmentation is advantageous and relevant to file systems on electromechanical disk drives. The movement of the hard drive's read/write heads over different areas of the disk when accessing fragmented files is slower, compared to accessing the entire contents of a non-fragmented file sequentially without moving the read/write heads to seek other fragments.

## Causes of fragmentation

Fragmentation occurs when the file system cannot or will not allocate enough contiguous space to store a complete file as a unit, but instead puts parts of it in gaps between existing files (usually those gaps exist because they formerly held a file that the operating system has subsequently deleted or because the file system allocated excess space for the file in the first place). Larger files and greater numbers of files also contribute to fragmentation and consequent performance loss. Defragmentation attempts to alleviate these problems.

### Example




Consider the following scenario, as shown by the image:

An otherwise blank disk has five files, A through E, each using 10 blocks of space (for this section, a *block* is an allocation unit of the filesystem; the block size is set when the disk is formatted and can be any size supported by the filesystem). On a blank disk, all of these files would be allocated one after the other (see example 1 in the image). If file B were to be deleted, there would be two options: mark the space for file B as empty to be used again later, or move all the files after B so that the empty space is at the end. Since moving the files could be time consuming if there were many files which need to be moved, usually the empty space is simply left there, marked in a table as available for new files (see example 2 in the image). When a new file, F, is allocated requiring 6 blocks of space, it could be placed into the first 6 blocks of the space that formerly held file B, and the 4 blocks following it will remain available (see example 3 in the image). If another new file, G, is added and needs only 4 blocks, it could then occupy the space after F and before C (example 4 in the image). However, if file F needs to be expanded, there are three options, since the space immediately following it is no longer available:

1. Move the file F to where it can be created as one contiguous file of the new, larger size. This would not be possible if the file is larger than the largest contiguous space available. The file could also be so large that the operation would take an undesirably long period of time.
2. Move all the files after F until one opens enough space to make it contiguous again. Same problem as in the previous example, if there are a small number of files or not much data to move, it's not a big problem. If there are thousands, or tens of thousands, there isn't enough time to move all those files.
3. Add a new block somewhere else, and indicate that F has a second *extent* (see example 5 in the image). Repeat this hundreds of times and the filesystem will have a number of small free segments scattered in many places, and some files will have multiple extents. When a file has many extents like this, access time for that file may become excessively long because of all the random seeking the disk will have to do when reading it.

Additionally, the concept of “fragmentation” is not only limited to individual files that have multiple extents on the disk. For instance, a group of files normally read in a particular sequence (like files accessed by a program when it is loading, which can include certain DLLs, various resource files, the audio/visual media files in a game) can be considered fragmented if they are not in sequential load-order on the disk, even if these individual files are *not* fragmented; the read/write heads will

have to seek these (defragmented) files randomly to access them in sequence. Some groups of files may have been originally installed in the correct sequence, but drift apart with time as certain files within the group are deleted. Updates are a common cause of this, because in order to update a file, most updaters usually delete the old file first, and then write a new, updated one in its place. However, most filesystems do not write the new file in the same physical place on the disk. This allows unrelated files to fill in the empty spaces left behind. In Windows, a good defragmenter will read the Prefetch files to identify as many of these file groups as possible and place the files within them in access sequence. Another frequently good assumption is that files in any given folder are related to each other and might be accessed together.

To defragment a disk, defragmentation software (also known as a "defragmenter") can only move files around within the free space available. This is an intensive operation and cannot be performed on a filesystem with little or no free space. During defragmentation, system performance will be degraded, and it is best to leave the computer alone during the process so that the defragmenter does not get confused by unexpected changes to the filesystem. Depending on the algorithm used it may or may not be advantageous to perform multiple passes. The reorganization involved in defragmentation does not change logical location of the files (defined as their location within the directory structure).

## Common countermeasures

**Partitioning**

A common strategy to optimize defragmentation and to reduce the impact of fragmentation is to partition the hard disk(s) in a way that separates partitions of the file system that experience many more reads than writes from the more volatile zones where files are created and deleted frequently. The directories that contain the users' profiles are modified constantly (especially with the Temp directory and web browser cache creating thousands of files that are deleted in a few days). If files from user profiles are held on a dedicated partition (as is commonly done on UNIX recommended files systems, where it is typically stored in the /var partition), the defragmenter runs better since it does not need to deal with all the static files from other directories. For partitions with relatively little write activity, defragmentation time greatly improves after the first defragmentation, since the defragmenter will need to defragment only a small number of new files in the future.

## Offline defragmentation

The presence of immovable system files, especially a swap file, can impede defragmentation. These files can be safely moved when the operating system is not in use. For example, ntfsresize moves these files to resize an NTFS partition. The tool PageDefrag could defragment Windows system files such as the swap file and the files that store theWindows registry by running at boot time before the GUI is loaded. Since Windows Vista, the feature is not fully supported and has not been updated.

In NTFS, as files are added to the disk, the Master File Table (MFT) must grow to store the information for the new files. Every time the MFT cannot be extended due to some file being in

the way, the MFT will gain a fragment. In early versions of Windows, it could not be safely defragmented while the partition was mounted, and so Microsoft wrote a hardblock in the defragmenting API. However, since Windows XP, an increasing number of defragmenters are now able to defragment the MFT, because the Windows defragmentation API has been improved and now supports that move operation. Even with the improvements, the first four clusters of the MFT remain unmovable by the Windows defragmentation API, resulting in the fact that some defragmenters will store the MFT in two fragments: The first four clusters wherever they were placed when the disk was formatted, and then the rest of the MFT at the beginning of the disk (or wherever the defragmenter's strategy deems to be the best place).

## User and performance issues

In a wide range of modern multi-user operating systems, an ordinary user cannot defragment the system disks since superuser (or "Administrator") access is required to move system files. Additionally, file systems such as NTFS are designed to decrease the likelihood of fragmentation. Improvements in modern hard drives such as RAM cache, faster platter rotation speed, command queuing (SCSI/ATA TCQ or SATA NCQ), and greater data density reduce the negative impact of fragmentation on system performance to some degree, though increases in commonly used data quantities offset those benefits. However, modern systems profit enormously from the huge disk capacities currently available, since partially filled disks fragment much less than full disks,[5] and on a high-capacity HDD, the same partition occupies a smaller range of cylinders, resulting in faster seeks. However, the average access time can never be lower than a half rotation of the platters, and platter rotation (measured in rpm) is the speed characteristic of HDDs which has experienced the slowest growth over the decades (compared to data transfer rate and seek time), so minimizing the number of seeks remains beneficial in most storage-heavy applications. Defragmentation is just that: ensuring that there is at most one seek per file, counting only the seeks to non-adjacent tracks.

When reading data from a conventional electromechanical hard disk drive, the disk controller must first position the head, relatively slowly, to the track where a given fragment resides, and then wait while the disk platter rotates until the fragment reaches the head.

Since disks based on flash memory have no moving parts, random access of a fragment does not suffer this delay, making defragmentation to optimize access speed unnecessary. Furthermore, since flash memory can be written to only a limited number of times before it fails, defragmentation is actually detrimental (except in the mitigation ofcatastrophic failure).

### Windows System Restore points may be deleted during defragmenting/optimizing

Running most defragmenters and optimizers can cause the Microsoft Shadow Copy service to delete some of the oldest restore points, even if the defragmenters/optimizers are built on Windows API. This is due to Shadow Copy keeping track of some movements of big files performed by the defragmenters/optimizers; when the total disk space used by shadow copies would exceed a specified threshold, older restore points are deleted until the limit is not exceeded.

## Defragmenting and optimizing

Besides defragmenting program files, the defragmenting tool can also reduce the time it takes to load programs and open files. For example, the Windows 9x defragmenter included the Intel Application Launch Accelerator which optimized programs on the disk by placing the defragmented program files and their dependencies next to each other, in the order of which the program loads them, to load these programs faster. At the beginning of the hard drive, the outer tracks have a higher transfer rate than the inner tracks. Placing frequently accessed files onto the outer tracks increases performance. Third party defragmenters, such as MyDefrag, will move frequently accessed files onto the outer tracks and defragment these files.

## Approach and defragmenters by file-system type

- FAT: MS-DOS 6.x and Windows 9x-systems come with a defragmentation utility called Defrag. The DOS version is a limited version of Norton SpeedDisk. The version that came with Windows 9x was licensed from Symantec Corporation, and the version that came with Windows 2000 and XP is licensed from Condusiv Technologies.
- NTFS was introduced with Windows NT 3.1, but the NTFS filesystem driver did not include any defragmentation capabilities. In Windows NT 4.0, defragmenting APIs were introduced that third-party tools could use to perform defragmentation tasks; however, no defragmentation software was included. In Windows 2000, Windows XP andWindows Server 2003, Microsoft included a defragmentation tool based on Diskeeper that made use of the defragmentation APIs and was a snap-in for Computer Management. In Windows Vista, Windows 7 and Windows 8, the tool has been greatly improved and was given a new interface with no visual diskmap and is no longer part of Computer Management. There are also a number of free and commercial third-party defragmentation products available for Microsoft Windows.
- BSD UFS and particularly FreeBSD uses an internal reallocator that seeks to reduce fragmentation right in the moment when the information is written to disk. This effectively controls system degradation after extended use.
- Linux ext2, ext3, and ext4: Much like UFS, these filesystems employ allocation techniques designed to keep fragmentation under control at all times. As a result, defragmentation is not needed in the vast majority of cases. ext2 uses an offline defragmenter called `e2defrag`, which does not work with its successor ext3. However, other programs, or filesystem-independent ones such as defragfs, may be used to defragment an ext3 filesystem. ext4 is somewhat backward compatible with ext3, and thus has generally the same amount of support from defragmentation programs. Nowadays e4defrag can be used to defragment an ext4 filesystem.
- VxFS has the `fsadm` utility that includes defrag operations.
- JFS has the `defragfs` utility on IBM operating systems.
- HFS Plus introduced with Mac OS 8.1 in 1998 a number of optimizations to the allocation algorithms in an attempt to defragment files while they are being accessed without a separate defragmenter.

- WAFL in NetApp's ONTAP 7.2 operating system has a command called `reallocate` that is designed to defragment large files.
- XFS provides an online defragmentation utility called `xfs_fsr`.
- SFS processes the defragmentation feature in almost completely stateless way (apart from the location it is working on), so defragmentation can be stopped and started instantly.
- ADFS, the file system used by RISC OS and earlier Acorn Computers, keeps file fragmentation under control without requiring manual defragmentation.

# Disk Cleanup

**Disk Cleanup** (cleanmgr.exe) is a computer maintenance utility included in Microsoft Windows designed to free up disk space on a computer's hard drive. The utility first searches and analyzes the hard drive for files that are no longer of any use, and then removes the unnecessary files. There are a number of different file categories that Disk Cleanup targets when performing the initial disk analysis:

- Compression of old files
- Temporary Internet files
- Temporary Windows files
- Downloaded program files
- Recycle Bin
- Removal of unused applications or optional Windows components
- Setup log files
- Offline web pages (cached)

The above list, however, is not exhaustive. For instance, 'Temporary Remote Desktop files' and 'Temporary Sync Files' may appear only under certain computer configurations, differences such as Windows Operating System and use of additional programs such as Remote Desktop. The option of removing hibernation data may not be ideal for some users as this may remove the hibernate option.

Aside from removing unnecessary files, users also have the option of compressing files that have not been accessed over a set period of time. This option provides a systematic compression scheme. Infrequently accessed files are compressed to free up disk space while leaving the frequently used files uncompressed for faster read/write access times. If after file compression, a user wishes to access a compressed file, the access times may be increased and vary from system to system. In addition to the categories that appear on the Disk Cleanup tab, the More Options tab offers additional options for freeing up hard drive space through removal of optional Windows components, installed programs, and all but the most recent System Restore point or Shadow Copy data in some versions of Microsoft Windows.

# Backup

In information technology, a **backup**, or the process of backing up, refers to the copying and archiving of computer data so it may be used to *restore* the original after a data lossevent. The verb form is to **back up** in two words, whereas the noun is *backup*.[1]

Backups have two distinct purposes. The primary purpose is to recover data after its loss, be it by data deletion or corruption. Data loss can be a common experience of computer users. A 2008 survey found that 66% of respondents had lost files on their home PC.[2] The secondary purpose of backups is to recover data from an earlier time, according to a user-defined data retention policy, typically configured within a backup application for how long copies of data are required. Though backups popularly represent a simple form of disaster recovery, and should be part of a disaster recovery plan, by themselves, backups should not alone be considered disaster recovery.[3] One reason for this is that not all backup systems or backup applications are able to reconstitute a computer system or other complex configurations such as a computer cluster, active directoryservers, or a database server, by restoring only data from a backup.

Since a backup system contains at least one copy of all data worth saving, the data storage requirements can be significant. Organizing this storage space and managing the backup process can be a complicated undertaking. A data repository model can be used to provide structure to the storage. Nowadays, there are many different types of data storage devices that are useful for making backups. There are also many different ways in which these devices can be arranged to provide geographic redundancy, data security, and portability.

Before data are sent to their storage locations, they are selected, extracted, and manipulated. Many different techniques have been developed to optimize the backup procedure. These include optimizations for dealing with open files and live data sources as well as compression, encryption, and de-duplication, among others. Every backup scheme should include dry runs that validate the reliability of the data being backed up. It is important to recognize the limitations and human factors involved in any backup scheme.

# Storage, the base of a backup system

## Data repository models

Any backup strategy starts with a concept of a data repository. The backup data needs to be stored, and probably should be organized to a degree. The organisation could be as simple as a sheet of paper with a list of all backup media (CDs etc.) and the dates they were produced. A more sophisticated setup could include a computerized index, catalog, or relational database. Different approaches have different advantages. Part of the model is the backup rotation scheme.

### Unstructured

An unstructured repository may simply be a stack of or CD-Rs or DVD-Rs with minimal information about what was backed up and when. This is the easiest to implement, but probably the least likely to achieve a high level of recoverability.

**Full only** / System imaging

A repository of this type contains complete system images taken at one or more specific points in time. This technology is frequently used by computer technicians to record known good configurations. Imaging is generally more useful for deploying a standard configuration to many systems rather than as a tool for making ongoing backups of diverse systems.

Incremental

An incremental style repository aims to make it more feasible to store backups from more points in time by organizing the data into increments of change between points in time. This eliminates the need to store duplicate copies of unchanged data: with full backups a lot of the data will be unchanged from what has been backed up previously. Typically, a *full* backup (of all files) is made on one occasion (or at infrequent intervals) and serves as the reference point for an incremental backup set. After that, a number of *incremental* backups are made after successive time periods. Restoring the whole system to the date of the last incremental backup would require starting from the last full backup taken before the data loss, and then applying in turn each of the incremental backups since then. Additionally, some backup systems can reorganize the repository to synthesize full backups from a series of incrementals.

Differential

Each differential backup saves the data that has changed since the last full backup. It has the advantage that only a maximum of two data sets are needed to restore the data. One disadvantage, compared to the incremental backup method, is that as time from the last full backup (and thus the accumulated changes in data) increases, so does the time to perform the differential backup. Restoring an entire system would require starting from the most recent full backup and then applying just the last differential backup since the last full backup.

Note: Vendors have standardized on the meaning of the terms "incremental backup" and "differential backup". However, there have been cases where conflicting definitions of these terms have been used. The most relevant characteristic of an incremental backup is which reference

point it uses to check for changes. By standard definition, a differential backup copies files that have been created or changed since the last full backup, regardless of whether any other differential backups have been made since then, whereas an incremental backup copies files that have been created or changed since the most recent backup of any type (full or incremental). Other variations of incremental backup include multi-level incrementals and incremental backups that compare parts of files instead of just the whole file.

**Reverse delta**

A reverse delta type repository stores a recent "mirror" of the source data and a series of differences between the mirror in its current state and its previous states. A reverse delta backup will start with a normal full backup. After the full backup is performed, the system will periodically synchronize the full backup with the live copy, while storing the data necessary to reconstruct older versions. This can either be done using hard links, or using binary diffs. This system works particularly well for large, slowly changing, data sets. Examples of programs that use this method are rdiff-backup and Time Machine.

Continuous data protection

Instead of scheduling periodic backups, the system immediately logs every change on the host system. This is generally done by saving byte or block-level differences rather than file-level differences. It differs from simple disk mirroring in that it enables a roll-back of the log and thus restoration of old image of data.

## Storage media

Regardless of the repository model that is used, the data has to be stored on some data storage medium.

Magnetic tape

Magnetic tape has long been the most commonly used medium for bulk data storage, backup, archiving, and interchange. Tape has typically had an order of magnitude better capacity/price ratio when compared to hard disk, but recently the ratios for tape and hard disk have become a lot closer. There are many formats, many of which are proprietary or specific to certain markets like mainframes or a particular brand of personal computer. Tape is a sequential access medium, so even though access times may be poor, the rate of continuously writing or reading data can actually be very fast. Some new tape drives are even faster than modern hard disks.

Hard disk

The capacity/price ratio of hard disk has been rapidly improving for many years. This is making it more competitive with magnetic tape as a bulk storage medium. The main advantages of hard disk storage are low access times, availability, capacity and ease of use.[7] External disks can be connected via local interfaces like SCSI, USB, FireWire, or eSATA, or via longer distance technologies like Ethernet, iSCSI, or Fibre Channel. Some disk-based backup systems, such as Virtual Tape Libraries, support data deduplication which can dramatically reduce the amount of disk storage capacity consumed by daily and weekly backup data. The main disadvantages of hard disk backups are that they are easily damaged, especially while being transported (e.g., for off-site backups), and that their stability over periods of years is a relative unknown.

Optical storage

Recordable CDs, DVDs, and Blu-ray Discs are commonly used with personal computers and generally have low media unit costs. However, the capacities and speeds of these and other optical discs are typically an order of magnitude lower than hard disk or tape. Many optical disk formats are WORM type, which makes them useful for archival purposes since the data cannot be changed. The use of an auto-changer or jukebox can make optical discs a feasible option for larger-scale backup systems. Some optical storage systems allow for cataloged data backups without human contact with the discs, allowing for longer data integrity.

Solid state storage

Also known as flash memory, thumb drives, USB flash drives, CompactFlash, SmartMedia, Memory Stick, Secure Digital cards, etc., these devices are relatively expensive for their low capacity, but are very convenient for backing up relatively low data volumes. A solid-state drive does not contain any movable parts unlike its magnetic drive counterpart and can have huge throughput in the order of 500Mbit/s to 6Gbit/s. SSD drives are now available in the order of 500GB to TBs.

Remote backup service

As broadband Internet access becomes more widespread, remote backup services are gaining in popularity. Backing up via the Internet to a remote location can protect against some worst-case scenarios such as fires, floods, or earthquakes which would destroy any backups in the immediate vicinity along with everything else. There are, however, a number of drawbacks to remote backup services. First, Internet connections are usually slower than local data storage devices. Residential broadband is especially problematic as routine backups must use an upstream link that's usually much slower than the downstream link used only occasionally to retrieve a file from backup. This tends to limit the use of such services to relatively small amounts of high value data. Secondly, users must trust a third party service provider to maintain the privacy and integrity of their data, although confidentiality can be assured by encrypting the data before transmission to the backup service with an encryption key known only to the user. Ultimately the backup service must itself use one of the above methods so this could be seen as a more complex way of doing traditional backups.

Floppy disk

During the 1980s and early 1990s, many personal/home computer users associated backing up mostly with copying to floppy disks. However, the data capacity of floppy disks failed to catch up with growing demands, rendering them effectively obsolete.

## Managing the data repository

Regardless of the data repository model, or data storage media used for backups, a balance needs to be struck between accessibility, security and cost. These media management methods are not mutually exclusive and are frequently combined to meet the user's needs. Using on-line disks for staging data before it is sent to a near-line tape library is a common example.

On-line

On-line backup storage is typically the most accessible type of data storage, which can begin restore in milliseconds of time. A good example is an internal hard disk or a disk array (maybe connected to SAN). This type of storage is very convenient and speedy, but is relatively expensive. On-line storage is quite vulnerable to being deleted or overwritten, either by accident, by intentional malevolent action, or in the wake of a data-deleting virus payload.

Near-line

Near-line storage is typically less accessible and less expensive than on-line storage, but still useful for backup data storage. A good example would be a tape library with restore times ranging from seconds to a few minutes. A mechanical device is usually used to move media units from storage into a drive where the data can be read or written. Generally it has safety properties similar to on-line storage.

Off-line

Off-line storage requires some direct human action to provide access to the storage media: for example inserting a tape into a tape drive or plugging in a cable. Because the data are not accessible via any computer except during limited periods in which they are written or read back, they are largely immune to a whole class of on-line backup failure modes. Access time will vary depending on whether the media are on-site or off-site.

Off-site data protection

To protect against a disaster or other site-specific problem, many people choose to send backup media to an off-site vault. The vault can be as simple as a system administrator's home office or as sophisticated as a disaster-hardened, temperature-controlled, high-security bunker with facilities for backup media storage. Importantly a data replica *can* be off-site but also *on-line* (e.g., an off-site RAID mirror). Such a replica has fairly limited value as a backup, and should not be confused with an off-line backup.

Backup site **or disaster recovery center (DR center)**

In the event of a disaster, the data on backup media will not be sufficient to recover. Computer systems onto which the data can be restored and properly configured networks are necessary too. Some organizations have their own data recovery centers that are equipped for this scenario. Other organizations contract this out to a third-party recovery center. Because a DR site is itself a huge investment, backing up is very rarely considered the preferred method of moving data to a DR site. A more typical way would be remote disk mirroring, which keeps the DR data as up to date as possible.

# Selection and extraction of dat

A successful backup job starts with selecting and extracting coherent units of data. Most data on modern computer systems is stored in discrete units, known as files. These files are organized into filesystems. Files that are actively being updated can be thought of as "live" and present a challenge to back up. It is also useful to save metadata that describes the computer or the filesystem being backed up.

Deciding what to back up at any given time is a harder process than it seems. By backing up too much redundant data, the data repository will fill up too quickly. Backing up an insufficient amount of data can eventually lead to the loss of critical information.

## Files

With **file-level** approach, making copies of files is the simplest and most common way to perform a backup. A means to perform this basic function is included in all backup software and all operating systems.

### Partial file copying

Instead of copying whole files, one can limit the backup to only the blocks or bytes within a file that have changed in a given period of time. This technique can use substantially less storage space on the backup medium, but requires a high level of sophistication to reconstruct files in a restore situation. Some implementations require integration with the source file system.

## Filesystems

Instead of copying files within a file system, a copy of the whole filesystem itself in **block-level** can be made. This is also known as a *raw partition backup* and is related todisk imaging. The process usually involves unmounting the filesystem and running a program like dd (Unix). Because the disk is read sequentially and with large buffers, this type of backup can be much faster than reading every file normally, especially when the filesystem contains many small files, is highly fragmented, or is nearly full. But because this method also reads the free disk blocks that contain no useful data, this method can also be slower than conventional reading, especially when the filesystem is nearly empty. Some filesystems, such as XFS, provide a "dump" utility that reads the disk sequentially for high performance while skipping unused sections. The corresponding restore utility can selectively restore individual files or the entire volume at the operator's choice.

### Identification of changes

Some filesystems have an archive bit for each file that says it was recently changed. Some backup software looks at the date of the file and compares it with the last backup to determine whether the file was changed.

Versioning file system

A versioning filesystem keeps track of all changes to a file and makes those changes accessible to the user. Generally this gives access to any previous version, all the way back to the file's creation time. An example of this is the Wayback versioning filesystem for Linux.

## Live data

If a computer system is in use while it is being backed up, the possibility of files being open for reading or writing is real. If a file is open, the contents on disk may not correctly represent what the owner of the file intends. This is especially true for database files of all kinds. The term fuzzy backup can be used to describe a backup of live data that looks like it ran correctly, but does not represent the state of the data at any single point in time. This is because the data being backed up changed in the period of time between when the backup started and when it finished. For databases in particular, fuzzy backups are worthless.

### Snapshot **backup**

A snapshot is an instantaneous function of some storage systems that presents a copy of the file system as if it were frozen at a specific point in time, often by a copy-on-writemechanism. An effective way to back up live data is to temporarily quiesce them (e.g. close all files), take a snapshot, and then resume live operations. At this point the snapshot can be backed up through normal methods. While a snapshot is very handy for viewing a filesystem as it was at a different point in time, it is hardly an effective backup mechanism by itself.

#### Open file backup

Many backup software packages feature the ability to handle open files in backup operations. Some simply check for openness and try again later. File locking is useful for regulating access to open files.

When attempting to understand the logistics of backing up open files, one must consider that the backup process could take several minutes to back up a large file such as a database. In order to back up a file that is in use, it is vital that the entire backup represent a single-moment snapshot of the file, rather than a simple copy of a read-through. This represents a challenge when backing up a file that is constantly changing. Either the database file must be locked to prevent changes, or a method must be implemented to ensure that the original snapshot is preserved long enough to be copied, all while changes are being preserved. Backing up a file while it is being changed, in a manner that causes the first part of the backup to represent data *before* changes occur to be combined with later parts of the backup *after* the change results in a corrupted file that is unusable, as most large files contain internal references between their various parts that must remain consistent throughout the file.

#### Cold database backup

During a cold backup, the database is closed or locked and not available to users. The datafiles do not change during the backup process so the database is in a consistent state when it is returned to normal operation.

#### Hot database backup

Some database management systems offer a means to generate a backup image of the database while it is online and usable ("hot"). This usually includes an inconsistent image of the data files plus a log of changes made while the procedure is running. Upon a restore, the changes in the log files are reapplied to bring the copy of the database up-to-date (the point in time at which the initial hot backup ended).

### Metadata

Not all information stored on the computer is stored in files. Accurately recovering a complete system from scratch requires keeping track of this non-file data too.

#### System description

System specifications are needed to procure an exact replacement after a disaster.

Boot sector

The boot sector can sometimes be recreated more easily than saving it. Still, it usually isn't a normal file and the system won't boot without it.

### Partition layout

The layout of the original disk, as well as partition tables and filesystem settings, is needed to properly recreate the original system.

### File metadata

Each file's permissions, owner, group, ACLs, and any other metadata need to be backed up for a restore to properly recreate the original environment.

### System metadata

Different operating systems have different ways of storing configuration information. Microsoft Windows keeps a registry of system information that is more difficult to restore than a typical file.

## Manipulation of data and dataset optimization

It is frequently useful or required to manipulate the data being backed up to optimize the backup process. These manipulations can provide many benefits including improved backup speed, restore speed, data security, media usage and/or reduced bandwidth requirements.

### Compression

Various schemes can be employed to shrink the size of the source data to be stored so that it uses less storage space. Compression is frequently a built-in feature of tape drive hardware.

### Deduplication

When multiple similar systems are backed up to the same destination storage device, there exists the potential for much redundancy within the backed up data. For example, if 20 Windows workstations were backed up to the same data repository, they might share a common set of system files. The data repository only needs to store one copy of those files to be able to restore any one of those workstations. This technique can be applied at the file level or even on raw blocks of data, potentially resulting in a massive reduction in required storage space. Deduplication can occur on a server before any data moves to backup media, sometimes referred to as source/client side deduplication. This approach also reduces bandwidth required to send backup data to its target media. The process can also occur at the target storage device, sometimes referred to as inline or back-end deduplication.

### Duplication

Sometimes backup jobs are duplicated to a second set of storage media. This can be done to rearrange the backup images to optimize restore speed or to have a second copy at a different location or on a different storage medium.

### Encryption

High capacity removable storage media such as backup tapes present a data security risk if they are lost or stolen. Encrypting the data on these media can mitigate this problem, but presents new

problems. Encryption is a CPU intensive process that can slow down backup speeds, and the security of the encrypted backups is only as effective as the security of the key management policy.

### Multiplexing

When there are many more computers to be backed up than there are destination storage devices, the ability to use a single storage device with several simultaneous backups can be useful.

**Refactoring**

The process of rearranging the backup sets in a data repository is known as refactoring. For example, if a backup system uses a single tape each day to store the incremental backups for all the protected computers, restoring one of the computers could potentially require many tapes. Refactoring could be used to consolidate all the backups for a single computer onto a single tape. This is especially useful for backup systems that do *incrementals forever* style backups.

### Staging

Sometimes backup jobs are copied to a staging disk before being copied to tape. This process is sometimes referred to as D2D2T, an acronym for Disk to Disk to Tape. This can be useful if there is a problem matching the speed of the final destination device with the source device as is frequently faced in network-based backup systems. It can also serve as a centralized location for applying other data manipulation techniques.

# Managing the backup process

As long as new data are being created and changes are being made, backups will need to be performed at frequent intervals. Individuals and organizations with anything from one computer to thousands of computer systems all require protection of data. The scales may be very different, but the objectives and limitations are essentially the same. Those who perform backups need to know how successful the backups are, regardless of scale.

## Objectives

### Recovery point objective **(RPO)**

The point in time that the restarted infrastructure will reflect. Essentially, this is the roll-back that will be experienced as a result of the recovery. The most desirable RPO would be the point just prior to the data loss event. Making a more recent recovery point achievable requires increasing the frequency of synchronization between the source data and the backup repository.[14]

### Recovery time objective **(RTO)**

The amount of time elapsed between disaster and restoration of business functions.[15]

### Data security

In addition to preserving access to data for its owners, data must be restricted from unauthorized access. Backups must be performed in a manner that does not compromise the original owner's undertaking. This can be achieved with data encryption and proper media handling policies.

## Limitations

An effective backup scheme will take into consideration the limitations of the situation.

**Backup window**

The period of time when backups are permitted to run on a system is called the backup window. This is typically the time when the system sees the least usage and the backup process will have the least amount of interference with normal operations. The backup window is usually planned with users' convenience in mind. If a backup extends past the defined backup window, a decision is made whether it is more beneficial to abort the backup or to lengthen the backup window.

**Performance impact**

All backup schemes have some performance impact on the system being backed up. For example, for the period of time that a computer system is being backed up, the hard drive is busy reading files for the purpose of backing up, and its full bandwidth is no longer available for other tasks. Such impacts should be analyzed.

**Costs of hardware, software, labor**

All types of storage media have a finite capacity with a real cost. Matching the correct amount of storage capacity (over time) with the backup needs is an important part of the design of a backup scheme. Any backup scheme has some labor requirement, but complicated schemes have considerably higher labor requirements. The cost of commercial backup software can also be considerable.

**Network bandwidth**

Distributed backup systems can be affected by limited network bandwidth.

## Implementation

Meeting the defined objectives in the face of the above limitations can be a difficult task. The tools and concepts below can make that task more achievable.

**Scheduling**

Using a job scheduler can greatly improve the reliability and consistency of backups by removing part of the human element. Many backup software packages include this functionality.

**Authentication**

Over the course of regular operations, the user accounts and/or system agents that perform the backups need to be authenticated at some level. The power to copy all data off of or onto a system requires unrestricted access. Using an authentication mechanism is a good way to prevent the backup scheme from being used for unauthorized activity.

Chain of trust

Removable storage media are physical items and must only be handled by trusted individuals. Establishing a chain of trusted individuals (and vendors) is critical to defining the security of the data.

## Measuring the process

To ensure that the backup scheme is working as expected, key factors should be monitored and historical data maintained.

Backup validation

(also known as "backup success validation") Provides information about the backup, and proves compliance to regulatory bodies outside the organization: for example, an insurance company in the USA might be required under HIPAA to demonstrate that its client data meet records retention requirements. Disaster, data complexity, data value and increasing dependence upon ever-growing volumes of data all contribute to the anxiety around and dependence upon successful backups to ensure business continuity. Thus many organizations rely on third-party or "independent" solutions to test, validate, and optimize their backup operations (backup reporting).

**Reporting**

In larger configurations, reports are useful for monitoring media usage, device status, errors, vault coordination and other information about the backup process.

**Logging**

In addition to the history of computer generated reports, activity and change logs are useful for monitoring backup system events.

**Validation**

Many backup programs use checksums or hashes to validate that the data was accurately copied. These offer several advantages. First, they allow data integrity to be verified without reference to the original file: if the file as stored on the backup medium has the same checksum as the saved value, then it is very probably correct. Second, some backup programs can use checksums to avoid making redundant copies of files, and thus improve backup speed. This is particularly useful for the de-duplication process.

**Monitored backup**

Backup processes are monitored by a third party monitoring center, which alerts users to any errors that occur during automated backups. Monitored backup requires software capable of pinging the monitoring center's servers in the case of errors. Some monitoring services also allow collection of historical meta-data, that can be used for Storage Resource Management purposes like projection of data growth, locating redundant primary storage capacity and reclaimable backup capacity.

# BIOS

The **BIOS** (/ˈbaɪ.ɒs/, an acronym for **Basic Input/Output System** and also known as the **System BIOS**, **ROM BIOS** or **PC BIOS**) is a type of firmware used during the bootingprocess (power-on startup) on IBM PC compatible computers.[1] The BIOS firmware is built into personal computers (PCs), and it is the first software they run when powered on. The name itself originates from the Basic Input/Output System used in the CP/M operating system in 1975. Originally proprietary to the IBM PC, the BIOS has been reverse engineered by companies looking to create compatible systems and the interface of that original system serves as a *de facto* standard.

The fundamental purposes of the BIOS are to initialize and test the system hardware components, and to load a boot loader or an operating system from a mass memory device. The BIOS additionally provides an abstraction layer for the hardware, i.e. a consistent way for application programs and operating systems to interact with the keyboard, display, and other input/output (I/O) devices. Variations in the system hardware are hidden by the BIOS from programs that use BIOS services instead of directly accessing the hardware.MS-DOS (PC DOS), which was the dominant PC operating system from the early 1980s until the mid 1990s, relied on BIOS services for disk, keyboard, and text display functions. MS Windows NT, Linux, and other protected mode operating systems in general ignore the abstraction layer provided by the BIOS and do not use it after loading, instead accessing the hardware components directly.

Every BIOS implementation is specifically designed to work with a particular computer or motherboard model, by interfacing with various devices that make up the complementary system chipset. Originally, BIOS firmware was stored in a ROM chip on the PC motherboard; in modern computer systems, the BIOS contents are stored on flash memory so it can be rewritten without removing the chip from the motherboard. This allows easy updates to the BIOS firmware so new features can be added or bugs can be fixed, but it also creates a possibility for the computer to become infected with BIOS rootkits.

Unified Extensible Firmware Interface (UEFI) was designed as a successor to BIOS, aiming to address its technical shortcomings. As of 2014, new PC hardware predominantly ships with UEFI firmware.

# Operating system services

The BIOS ROM is customized to the particular manufacturer's hardware, allowing low-level services (such as reading a keystroke or writing a sector of data to diskette) to be provided in a standardized way to programs, including operating systems. For example, an IBM PC might have either a monochrome or a color display adapter (using different display memory addresses and hardware), but a single, standard, BIOS system call may be invoked to display a character at a specified position on the screen in text mode orgraphics mode.

The BIOS provides a small library of basic input/output functions to operate peripherals (such as the keyboard, rudimentary text and graphics display functions and so forth). When using MS-DOS, BIOS services could be accessed by an application program (or by MS-DOS) by executing an INT 13h interrupt instruction to access disk functions, or by executing one of a number of other documented BIOS interrupt calls to access video display, keyboard, cassette, and other device functions.

Operating systems and executive software that are designed to supersede this basic firmware functionality provide replacement software interfaces to application software. Applications can also provide these services to themselves. This began even in the 1980s under MS-DOS, when programmers observed that using the BIOS video services for graphics display was very slow. To increase the speed of screen output, many programs bypassed the BIOS and programmed the video display hardware directly. Other graphics programmers, particularly but not exclusively in the demoscene, observed that there were technical capabilities of the PC display adapters that were not supported by the IBM BIOS and could not be taken advantage of without circumventing it. Since the AT-compatible BIOS ran in Intel real mode, operating systems that ran in protected mode on 286 and later processors required hardware device drivers compatible with protected mode operation to replace BIOS services.

In modern personal computers running modern operating systems the BIOS is used only during booting and initial loading of system software. Before the operating system's first graphical screen is displayed, input and output are typically handled through BIOS. A boot menu such as the textual menu of Windows, which allows users to choose an operating system to boot, to boot into the safe mode, or to use the last known good configuration, is displayed through BIOS and receives keyboard input through BIOS.

However, it is also important to note that modern PCs can still boot and run legacy operating systems such as MS-DOS or DR-DOS that rely heavily on BIOS for their console and disk I/O. Thus, while not as central as they once were, the BIOS services are still important.

## Processor microcode updates

Intel processors have reprogrammable microcode since the P6 microarchitecture. The BIOS may contain patches to the processor microcode that fix errors in the initial processor microcode; reprogramming is not persistent, thus loading of microcode updates is performed each time the system is powered up. Without reprogrammable microcode, an expensive processor swap would be required; for example, the Pentium FDIV bug became an expensive fiasco for Intel as it required a product recall because the original Pentium processor's defective microcode could not be reprogrammed.

## Identification

Some BIOSes contain a *software licensing description table* (SLIC), a digital signature placed inside the BIOS by the original equipment manufacturer (OEM), for example Dell. The SLIC is inserted into the ACPI table and contains no active code.

Computer manufacturers that distribute OEM versions of Microsoft Windows and Microsoft application software can use the SLIC to authenticate licensing to the OEM Windows Installation disk and system recovery disc containing Windows software. Systems having a SLIC can be preactivated with an OEM product key, and they verify an XML formatted OEM certificate against the SLIC in the BIOS as a means of self-activating (see System Locked Preinstallation, SLP). If a user performs a fresh install of Windows, they will need to have possession of both the OEM key (either SLP or COA) and the digital certificate for their SLIC in order to bypass activation. This can be achieved if the user performs a restore using a pre-customised image provided by the OEM. Power users can copy the necessary certificate files from the OEM image, decode the SLP product key, then perform SLP activation manually. Cracks for non-genuine Windows distributions usually edit the SLIC or emulate it in order to bypass Windows activation.

## Overclocking

Some BIOS implementations allow overclocking, an action in which the CPU is adjusted to a higher clock rate than its manufacturer rating for guaranteed capability. Overclocking may, however, seriously compromise system reliability in insufficiently cooled computers and generally shorten component lifespan. Overclocking, when incorrectly performed, may also cause components to overheat so quickly that they mechanically destroy themselves.

## Modern use

Some operating systems, for example MS-DOS, rely on the BIOS to carry out most input/output tasks within the PC.

Because the BIOS still runs in 16-bit real mode, calling BIOS services directly is inefficient for protected-mode operating systems. BIOS services are not used by modern multitasking GUI operating systems after they initially load, so the importance of the primary part of BIOS is greatly reduced from what it was initially.

Later BIOS implementations took on more complex functions, by including interfaces such as Advanced Configuration and Power Interface (ACPI); these functions include power management, hot swapping, and thermal management. At the same time, since 2010 BIOS technology is in a transitional process toward the UEFI.

# Computer network

A **computer network** or **data network** is a telecommunications network which allows computers to exchange data. In computer networks, networked computing devices pass data to each other along network links (data connections). Data is transferred in the form of packets. The connections between nodes are established using either cable media or wireless media. The best-known computer network is the Internet.

Network computer devices that originate, route and terminate the data are called network nodes.[1] Nodes can include hosts such aspersonal computers, phones, servers as well as networking hardware. Two such devices are said to be networked together when one device is able to exchange information with the other device, whether or not they have a direct connection to each other.

Computer networks differ in the transmission media used to carry their signals, the communications protocols to organize network traffic, the network's size, topology and organizational intent. In most cases, communications protocols are layered on (i.e. work using) other more specific or more general communications protocols, except for the *physical layer* that directly deals with the transmission media.

Computer networks support applications such as access to the World Wide Web, shared use of application and storage servers,printers, and fax machines, and use of email and instant messaging applications.

# Networking cables

**Networking cables** are used to connect one network device to other network devices or to connect two or more computers to share printer, scanner etc. Different types of network cables like Coaxial cable, Optical fiber cable, Twisted Pair cables are used depending on the network's topology, protocol and size. The devices can be separated by a few meters (e.g. via Ethernet) or nearly unlimited distances (e.g. via the interconnections of the Internet).

While wireless may be the wave of the future, most computer networks today still utilize cables to transfer signals from one point to another.

## Twisted pair

*Twisted pair* cabling is a form of wiring in which pairs of wires (the forward and return conductors of a single circuit) are twisted together for the purposes of canceling outelectromagnetic interference (EMI) from other wire pairs and from external sources. This type of cable is used for home and corporate Ethernet networks.

There are two types of twisted pair cables: shielded, unshielded.

## Fiber Optic cable

An optical fiber cable consists of a center glass core surrounded by several layers of protective material. The outer insulating jacket is made of Teflon or PVC to prevent interference. It is expensive but has higher bandwidth and can transmit data over longer distances.

## Coaxial cable

Coaxial lines confine the electromagnetic wave to area inside the cable, between the center conductor and the shield. The transmission of energy in the line occurs totally through the dielectric inside the cable between the conductors. Coaxial lines can therefore be bent and twisted (subject to limits) without negative effects, and they can be strapped to conductive supports without inducing unwanted currents in them.

The most common use for coaxial cables is for television and other signals with bandwidth of multiple megahertz. Although in most homes coaxial cables have been installed for transmission of TV signals, new technologies (such as the ITU-T G.hn standard) open the possibility of using home coaxial cable for high-speed home networking applications (Ethernet over coax).

In the 20th century they carried long distance telephone connections.

## Patch cable

A *patch cable* is an electrical or optical cable used to connect one electronic or optical device to another for signal routing. Devices of different types (e.g. a switch connected to a computer, or a switch connected to a router) are connected with patch cords. It is a very fast connection speed. Patch cords are usually produced in many different colors so as to be easily distinguishable,[2] and are relatively short, perhaps no longer than two meters .

## Ethernet (crossover) cable

An **Ethernet crossover cable** is a type of Ethernet cable used to connect computing devices together directly where they would normally be connected via a network switch, hubor router, such as directly connecting two personal computers via their network adapters. Some newer Ethernet devices support the use of cross-over cables in the place of patch cables.

## Power lines

Although power wires are not designed for networking applications, new technologies like Power line communication allows these wires to also be used to interconnect home computers, peripherals or other networked consumer products. On December 2008, the ITU-T adopted Recommendation G.hn/G.9960 as the first worldwide standard for high-speed powerline communications.[3] G.hn also specifies communications over phonelines and coaxial

# Some of important hardware stuff

**Switches**

A network switch is a device that forwards and filters OSI layer 2 datagrams between ports based on the MAC addresses in the packets. A switch is distinct from a hub in that it only forwards the frames to the physical ports involved in the communication rather than all ports connected. It can be thought of as a multi-port bridge.  It learns to associate physical ports to MAC addresses by examining the source addresses of received frames. If an unknown destination is targeted, the

switch broadcasts to all ports but the source. Switches normally have numerous ports, facilitating a star topology for devices, and cascading additional switches.

Multi-layer switches are capable of routing based on layer 3 addressing or additional logical levels. The term *switch* is often used loosely to include devices such as routers and bridges, as well as devices that may distribute traffic based on load or based on application content (e.g., a Web URL identifier).

**Routers**

A router is an internetworking device that forwards packets between networks by processing the routing information included in the packet or datagram (Internet protocol information from layer 3). The routing information is often processed in conjunction with the routing table (or forwarding table). A router uses its routing table to determine where to forward packets. (A destination in a routing table can include a "null" interface, also known as the "black hole" interface because data can go into it, however, no further processing is done for said data.)

**Modems**

Modems (MOdulator-DEModulator) are used to connect network nodes via wire not originally designed for digital network traffic, or for wireless. To do this one or more carrier signals are modulated by the digital signal to produce an analog signal that can be tailored to give the required properties for transmission. Modems are commonly used for telephone lines, using a Digital Subscriber Line technology.

**Firewalls**

A firewall is a network device for controlling network security and access rules. Firewalls are typically configured to reject access requests from unrecognized sources while allowing actions from recognized ones. The vital role firewalls play in network security grows in parallel with the constant increase in cyber attacks.

# Geographic scale

A network can be characterized by its physical capacity or its organizational purpose. Use of the network, including user authorization and access rights, differ accordingly.

**Nanoscale Network**

A nanoscale communication network has key components implemented at the nanoscale including message carriers and leverages physical principles that differ from macroscale communication mechanisms. Nanoscale communication extends communication to very small sensors and actuators such as those found in biological systems and also tends to operate in environments that would be too harsh for classical communication.

**Personal area network**

A personal area network (PAN) is a computer network used for communication among computer and different information technological devices close to one person. Some examples of devices

that are used in a PAN are personal computers, printers, fax machines, telephones, PDAs, scanners, and even video game consoles. A PAN may include wired and wireless devices. The reach of a PAN typically extends to 10 meters. A wired PAN is usually constructed with USB and FireWire connections while technologies such as Bluetooth and infrared communication typically form a wireless PAN.

**Local area network**

A local area network (LAN) is a network that connects computers and devices in a limited geographical area such as a home, school, office building, or closely positioned group of buildings. Each computer or device on the network is a node. Wired LANs are most likely based on Ethernet technology. Newer standards such as ITU-T G.hn also provide a way to create a wired LAN using existing wiring, such as coaxial cables, telephone lines, and power lines.

All interconnected devices use the network layer (layer 3) to handle multiple subnets (represented by different colors). Those inside the library have 10/100 Mbit/s Ethernet connections to the user device and a Gigabit Ethernet connection to the central router. They could be called *Layer 3 switches*, because they only have Ethernet interfaces and support the Internet Protocol. It might be more correct to call them access routers, where the router at the top is a distribution router that connects to the Internet and to the academic networks' customer access routers.

The defining characteristics of a LAN, in contrast to a wide area network (WAN), include higher data transfer rates, limited geographic range, and lack of reliance on leased linesto provide connectivity. Current Ethernet or other IEEE 802.3 LAN technologies operate at data transfer rates up to 10 Gbit/s. The IEEE investigates the standardization of 40 and 100 Gbit/s rates.[19] A LAN can be connected to a WAN using a router.

**Home area network**

A home area network (HAN) is a residential LAN used for communication between digital devices typically deployed in the home, usually a small number of personal computers and accessories, such as printers and mobile computing devices. An important function is the sharing of Internet access, often a broadband service through a cable TV or digital subscriber line (DSL) provider.

**Storage area network**

A storage area network (SAN) is a dedicated network that provides access to consolidated, block level data storage. SANs are primarily used to make storage devices, such as disk arrays, tape libraries, and optical jukeboxes, accessible to servers so that the devices appear like locally attached devices to the operating system. A SAN typically has its own network of storage devices that are generally not accessible through the local area network by other devices. The cost and complexity of SANs dropped in the early 2000s to levels allowing wider adoption across both enterprise and small to medium-sized business environments.

**Campus area network**

A campus area network (CAN) is made up of an interconnection of LANs within a limited geographical area. The networking equipment (switches, routers) and transmission media (optical

fiber, copper plant, Cat5 cabling, etc.) are almost entirely owned by the campus tenant / owner (an enterprise, university, government, etc.).

For example, a university campus network is likely to link a variety of campus buildings to connect academic colleges or departments, the library, and student residence halls.

**Backbone network**

A backbone network is part of a computer network infrastructure that provides a path for the exchange of information between different LANs or sub-networks. A backbone can tie together diverse networks within the same building, across different buildings, or over a wide area.

For example, a large company might implement a backbone network to connect departments that are located around the world. The equipment that ties together the departmental networks constitutes the network backbone. When designing a network backbone, network performance and network congestion are critical factors to take into account. Normally, the backbone network's capacity is greater than that of the individual networks connected to it.

Another example of a backbone network is the Internet backbone, which is the set of wide area networks (WANs) and core routers that tie together all networks connected to theInternet.

**Metropolitan area network**

A Metropolitan area network (MAN) is a large computer network that usually spans a city or a large campus.

**Wide area network**

A wide area network (WAN) is a computer network that covers a large geographic area such as a city, country, or spans even intercontinental distances. A WAN uses a communications channel that combines many types of media such as telephone lines, cables, and air waves. A WAN often makes use of transmission facilities provided by common carriers, such as telephone companies. WAN technologies generally function at the lower three layers of the OSI reference model: the physical layer, the data link layer, and the network layer.

**Enterprise private network**

An enterprise private network is a network that a single organization builds to interconnect its office locations (e.g., production sites, head offices, remote offices, shops) so they can share computer resources.

**Virtual private network**

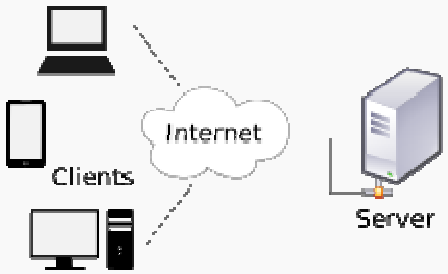
A virtual private network (VPN) is an overlay network in which some of the links between nodes are carried by open connections or virtual circuits in some larger network (e.g., the Internet) instead of by physical wires. The data link layer protocols of the virtual network are said to be tunneled through the larger network when this is the case. One common application is secure communications through the public Internet, but a VPN need not have explicit security features, such as authentication or content encryption. VPNs, for example, can be used to separate the traffic of different user communities over an underlying network with strong security features.

VPN may have best-effort performance, or may have a defined service level agreement (SLA) between the VPN customer and the VPN service provider. Generally, a VPN has a topology more complex than point-to-point.

**Global area network**

A global area network (GAN) is a network used for supporting mobile across an arbitrary number of wireless LANs, satellite coverage areas, etc. The key challenge in mobile communications is handing off user communications from one local coverage area to the next. In IEEE Project 802, this involves a succession of terrestrial wireless LANs.

# Client–server model

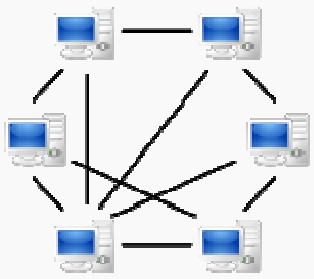



A computer network diagram of clients communicating with a server via the Internet.

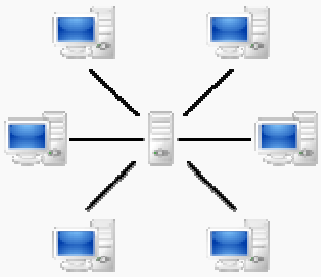
The **client–server model** of computing is a distributed application structure that partitions tasks or workloads between the providers of a resource or service, called servers, and service requesters, called clients.[1] Often clients and servers communicate over acomputer network on separate hardware, but both client and server may reside in the same system. A server host runs one or more server programs which share their resources with clients. A client does not share any of its resources, but requests a server's content or service function. Clients therefore initiate communication sessions with servers which await incoming requests.

Examples of computer applications that use the client–server model are Email, network printing, and the World Wide Web.

# Peer-to-peer



A **peer-to-peer (P2P) network**in which interconnected nodes ("peers") share resources amongst each other without the use of a centralized administrative system



A network based on the **client-server model**, where individual*clients* request services and resources from centralized servers

**Peer-to-peer** (**P2P**) computing or networking is a distributed application architecture that partitions tasks or work loads between peers. Peers are equally privileged, equipotent participants in the application. They are said to form a peer-to-peer network of nodes.

Peers make a portion of their resources, such as processing power, disk storage or network bandwidth, directly available to other network participants, without the need for central coordination by servers or stable hosts.Peers are both suppliers and consumers of resources, in contrast to the traditional client-server model in which the consumption and supply of resources is divided. Emerging collaborative P2P systems are going beyond the era of peers doing similar things while sharing resources, and are looking for diverse peers that can bring in unique resources and capabilities to a virtual community thereby empowering it to engage in greater tasks beyond those that can be accomplished by individual peers, yet that are beneficial to all the peers.

While P2P systems had previously been used in many application domains, the architecture was popularized by the file sharing systemNapster, originally released in 1999. The concept has inspired new structures and philosophies in many areas of human interaction. In such social contexts, peer-to-peer as a meme refers to the egalitarian social networking that has emerged throughout society, enabled by Internettechnologies in general.

## Internet Protocol Suite

The Internet Protocol Suite, also called TCP/IP, is the foundation of all modern networking. It offers connection-less as well as connection-oriented services over an inherently unreliable network traversed by data-gram transmission at the Internet protocol (IP) level. At its core, the protocol suite defines the addressing, identification, and routing specifications for Internet Protocol Version 4 (IPv4) and for IPv6, the next generation of the protocol with a much enlarged addressing capability.

# Internet

The **Internet** is a global system of interconnected computer networks that use the standard Internet protocol suite (TCP/IP) to link several billion devices worldwide. It is a *network of networks*[1] that consists of millions of private, public, academic, business, and government networks of local to global scope, linked by a broad array of electronic, wireless, and optical networking technologies. The Internet carries an extensive range of information resources and services, such as the inter-linked hypertext documents andapplications of the World Wide

Web (WWW), the infrastructure to support email, and peer-to-peer networks for file sharing andtelephony.

# World Wide Web

The **World Wide Web** (**www**, **W3**) is an information system of interlinked hypertext documents that are accessed via the Internet and built on top of the Domain Name System. It has also commonly become known simply as *the Web*. Individual document pages on the World Wide Web are called web pages and are accessed with a software application running on the user's computer, commonly called a web browser. Web pages may contain text, images, videos, and other multimedia components, as well as web navigationfeatures consisting of hyperlinks.

Tim Berners-Lee, a British computer scientist and former CERN employee, is the inventor of the Web. On 12 March 1989,[3] Berners-Lee wrote a proposal for what would eventually become the World Wide Web.[4] The 1989 proposal was meant for a more effective CERN communication system but Berners-Lee also realised the concept could be implemented throughout the world. Berners-Lee and Belgian computer scientist Robert Cailliau proposed in 1990 to use hypertext "to link and access information of various kinds as a web of nodes in which the user can browse at will",[ and Berners-Lee finished the first website in December of that year. The first test was completed around 20 December 1990 and Berners-Lee reported about the project on the newsgroup *alt.hypertext* on 7 August 1991.

# Uniform resource locator

A **uniform resource locator (URL)** is a reference to a resource that specifies the location of the resource on a computer network and a mechanism for retrieving it. A URL is a specific type of uniform resource identifier (URI). although many people use the two terms interchangeably.[ A URL implies the means to access an indicated resource, which is not true of every URI. URLs occur most commonly to reference web pages (http), but are also used for file transfer (ftp), email (mailto), database access (JDBC), and many other applications.

Most web browsers display the URL of a web page above the page in an address bar. A typical URL has the form*http://www.example.com/index.html*, which indicates the protocol type (*http*), the domain name, (*www.example.com*), and the specific web page (*index.html*).

# IP address

An **Internet Protocol address** (**IP address**) is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication.[1] An IP address serves two principal functions: host or network interface identification and location addressing. Its role has been characterized as follows: "A name indicates what we seek. An address indicates where it is. A route indicates how to get there."[2]

The designers of the Internet Protocol defined an IP address as a 32-bit number[1] and this system, known as Internet Protocol Version 4 (IPv4), is still in use today. However, because of the growth of the Internet and the predicted depletion of available addresses, a new version of IP (IPv6), using 128 bits for the address, was developed in 1995.[3]IPv6 was standardized as RFC 2460 in 1998,[4] and its deployment has been ongoing since the mid-2000s.

IP addresses are usually written and displayed in human-readable notations, such as 172.16.254.1 (IPv4), and 2001:db8:0:1234:0:567:8:1 (IPv6).

The Internet Assigned Numbers Authority (IANA) manages the IP address space allocations globally and delegates five regional Internet registries (RIRs) to allocate IP address blocks to local Internet registries (Internet service providers) and other entities.

# Internet Protocol

The **Internet Protocol** (**IP**) is the principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries. Its routing function enables internetworking, and essentially establishes the Internet.

IP has the task of delivering packets from the source host to the destination host solely based on the IP addresses in the packetheaders. For this purpose, IP defines packet structures that encapsulate the data to be delivered. It also defines addressing methods that are used to label the datagram with source and destination information.

Historically, IP was the connectionless datagram service in the original *Transmission Control Program* introduced by Vint Cerf andBob Kahn in 1974; the other being the connection-oriented Transmission Control Protocol (TCP). The Internet protocol suite is therefore often referred to as TCP/IP.

The first major version of IP, Internet Protocol Version 4 (IPv4), is the dominant protocol of the Internet. Its successor is Internet Protocol Version 6 (IPv6).

# MAC address

A **media access control address** (**MAC address**) is a unique identifier assigned to network interfaces for communications on the physical network segment. MAC addresses are used as a network address for most IEEE 802 network technologies, including Ethernet and WiFi. Logically, MAC addresses are used in the media access control protocol sublayer of the OSI reference model.

MAC addresses are most often assigned by the manufacturer of a network interface controller (NIC) and are stored in its hardware, such as the card's read-only memory or some other firmware mechanism. If assigned by the manufacturer, a MAC address usually encodes the manufacturer's registered identification number and may be referred to as the **burned-in address** (**BIA**). It may also be known as an **Ethernet hardware address** (**EHA**), **hardware address** or **physical address**. This can be contrasted to a programmed address, where the host device issues commands to the NIC to use an arbitrary address.

A network node may have multiple NICs and each NIC must have a unique MAC address.

MAC addresses are formed according to the rules of one of three numbering name spaces managed by the Institute of Electrical and Electronics Engineers (IEEE): MAC-48, EUI-48, and EUI-64. The IEEE claims trademarks on the names EUI-48[1] and EUI-64,[2] in which EUI is an abbreviation for *Extended Unique Identifier*.

# Domain Name System

The **Domain Name System** (**DNS**) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most prominently, it translates domain names, which can be easily memorized by humans, to the numerical IP addresses needed for the purpose of computer services and devices worldwide. The Domain Name System is an essential component of the functionality of most Internet services because it is the Internet's primary directory service.

The Domain Name System distributes the responsibility of assigning domain names and mapping those names to IP addresses by designating authoritative name servers for each domain. Authoritative name servers are assigned to be responsible for their supported domains, and may delegate authority over sub-domains to other name servers. This mechanism provides distributed and fault tolerant service and was designed to avoid the need for a single central database.

The Domain Name System also specifies the technical functionality of the database service which is at its core. It defines the DNS protocol, a detailed specification of the data structures and data communication exchanges used in DNS, as part of the Internet Protocol Suite. Historically, other directory services preceding DNS were not scalable to large or global directories as they were

originally based on text files, prominently the HOSTS.TXT resolver. DNS has been in wide use since the 1980s.

The Internet maintains two principal namespaces, the domain name hierarchy and the Internet Protocol (IP) address spaces. The Domain Name System maintains the domain name hierarchy and provides translation services between it and the address spaces. Internet name servers and a communication protocol implement the Domain Name System. A DNS name server is a server that stores the DNS records for a domain name; a DNS name server responds with answers to queries against its database.

The most common types of records stored in the DNS database are those dealing with a DNS zone's authority authority (SOA), IP addresses (A and AAAA), SMTP mail exchangers (MX), name servers (NS), pointers for reverse DNS lookups (PTR), and domain name aliases (CNAME). Although not intended to be a general purpose database, DNS can store records for other types of data for either automatic machine lookups for things like DNSSEC records, or for human queries like responsible person (RP) records. For a complete list of DNS record types, see the List of DNS record types. As a general purpose database, DNS has also seen use in combating unsolicited email (spam) by using a real-time blackhole list stored in a DNS database. Whether for Internet naming or for general purpose uses, the DNS database is traditionally stored in a structured zone file.

# File Transfer Protocol

The **File Transfer Protocol** (**FTP**) is a standard network protocol used to transfer computer files from one host to another host over a TCP-based network, such as the Internet.

FTP is built on a client-server architecture and uses separate control and data connections between the client and the server. FTP users may authenticate themselves using aclear-text sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it. For secure transmission that protects the username and password, and encrypts the content, FTP is often secured with SSL/TLS (FTPS). SSH File Transfer Protocol (SFTP) is sometimes also used instead, but is technologically different.

The first FTP client applications were command-line applications developed before operating systems had graphical user interfaces, and are still shipped with most Windows,Unix, and Linux operating systems. Many FTP clients and automation utilities have since been developed for desktops, servers, mobile devices, and hardware, and FTP has been incorporated into productivity applications, such as Web page editors.

# Simple Mail Transfer Protocol

**Simple Mail Transfer Protocol** (**SMTP**) is an Internet standard for electronic mail (e-mail) transmission. First defined by RFC 821in 1982, it was last updated in 2008 with the Extended SMTP additions by RFC 5321 - which is the protocol in widespread use today.

SMTP by default uses TCP port 25. The protocol for mail submission is the same, but uses port 587. SMTP connections secured bySSL, known as SMTPS, default to port 465 (nonstandard, but sometimes used for legacy reasons).

Although electronic mail servers and other mail transfer agents use SMTP to send and receive mail messages, user-level client mail applications typically use SMTP only for sending messages to a mail server for relaying. For receiving messages, client applications usually use either POP3 or IMAP.

Although proprietary systems (such as Microsoft Exchange and Lotus Notes/Domino) and webmail systems (such as Hotmail, Gmailand Yahoo! Mail) use their own non-standard protocols to access mail box accounts on their own mail servers, all use SMTP when sending or receiving email from outside their own systems.

# Computer crime

**Computer crime,** or **cybercrime**, is any crime that involves a computer and a network. (also known as hacking) The computer may have been used in the commission of a crime, or it may be the target. **Netcrime** is criminal exploitation of the Internet, inherently a cybercrime. Dr. Debarati Halder and Dr. K. Jaishankar (2011) define Cybercrimes as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)".Such crimes may threaten a nation's security and financial health. Issues surrounding these types of crimes have become high-profile, particularly those surrounding hacking, copyright infringement, child pornography, and child grooming. There are also problems of privacy when confidential information is intercepted or disclosed, lawfully or otherwise. Dr.Debarati Halder and Dr.K.Jaishankar(2011) further define cybercrime from the perspective of gender and defined 'cybercrime against women' as "“Crimes targeted against women with a motive to intentionally harm the victim psychologically and physically, using modern telecommunication networks such as internet and mobile phones”.[4]

An Australian nationwide survey conducted in 2006 found that two in three convicted cybercriminals were between the ages of 15 and 26.

Internationally, both governmental and non-state actors engage in cybercrimes, including espionage, financial theft, and other cross-border crimes. Activity crossing international borders and involving the interests of at least one nation state is sometimes referred to as cyberwarfare. The international legal system is attempting to hold actors accountable for their actions through the International Criminal Court.

A report (sponsored by McAfee) estimates the annual damage to the global economy at $445 billion;[7] however, a Microsoft report shows that such survey-based estimates are "hopelessly flawed" and exaggerate the true losses by orders of magnitude.Approximately $1.5 billion was lost in 2012 to online credit and debit card fraud in the US.

# Classification

## Fraud and financial crimes

Computer fraud is any dishonest misrepresentation of fact intended to let another to do or refrain from doing something which causes loss. In this context, the fraud will result in obtaining a benefit by:

- Altering in an unauthorized way. This requires little technical expertise and is common form of theft by employees altering the data before entry or entering false data, or by entering unauthorized instructions or using unauthorized processes;
- Altering, destroying, suppressing, or stealing output, usually to conceal unauthorized transactions. This is difficult to detect;
- Altering or deleting stored data;

Other forms of fraud may be facilitated using computer systems, including bank fraud, identity theft, extortion, and theft of classified information.

A variety of internet scams, many based on phishing and social engineering, target consumers and businesses.

## Cyberterrorism

Government officials and Information Technology security specialists have documented a significant increase in Internet problems and server scans since early 2001. But there is a growing concern among federal officials that such intrusions are part of an organized effort by cyberterrorists, foreign intelligence services, or other groups to map potential security holes in critical systems. A cyberterrorist is someone who intimidates or coerces a government or organization to advance his or her political or social objectives by launching a computer-based attack against computers, networks, or the information stored on them.

Cyberterrorism in general, can be defined as an act of terrorism committed through the use of cyberspace or computer resources (Parker 1983). As such, a simple propaganda in the Internet,

that there will be bomb attacks during the holidays can be considered cyberterrorism. As well there are also hacking activities directed towards individuals, families, organized by groups within networks, tending to cause fear among people, demonstrate power, collecting information relevant for ruining peoples' lives, robberies, blackmailing etc.

## Cyberwarfare

The U.S. Department of Defense (DoD) notes that the cyberspace has emerged as a national-level concern through several recent events of geo-strategic significance. Among those are included, the attack on Estonia's infrastructure in 2007, allegedly by Russian hackers. "In August 2008, Russia again allegedly conducted cyberattacks, this time in a coordinated and synchronized kinetic and non-kinetic campaign against the country of Georgia. Fearing that such attacks may become the norm in future warfare among nation-states, the concept of cyberspace operations impacts and will be adapted by warfighting military commanders in the future.

## Computer as a target

These crimes are committed by a selected group of criminals. Unlike crimes using the computer as a tool, these crimes requires the technical knowledge of the perpetrators. These crimes are relatively new, having been in existence for only as long as computers have - which explains how unprepared society and the world in general is towards combating these crimes. There are numerous crimes of this nature committed daily on the internet:

Crimes that primarily target computer networks or devices include:

- Computer viruses
- Denial-of-service attacks
- Malware (malicious code)

## Computer as a tool

When the individual is the main target of cybercrime, the computer can be considered as the tool rather than the target. These crimes generally involve less technical expertise. Human weaknesses are generally exploited. The damage dealt is largely psychological and intangible, making legal action against the variants more difficult. These are the crimes which have existed for centuries in the offline world. Scams, theft, and the likes have existed even before the development in high-tech equipment. The same criminal has simply been given a tool which increases his potential pool of victims and makes him all the harder to trace and apprehend.[13]

Crimes that use computer networks or devices to advance other ends include:

- Fraud and identity theft (although this increasingly uses malware, hacking and/or phishing, making it an example of both "computer as target" and "computer as tool" crime)
- Information warfare
- Phishing scams
- Spam
- Propagation of illegal obscene or offensive content, including harassment and threats

The unsolicited sending of bulk email for commercial purposes (spam) is unlawful in some jurisdictions.

Phishing is mostly propagated via email. Phishing emails may contain links to other websites that are affected by malware.[14] Or, they may contain links to fake online banking or other websites used to steal private account information.

### Obscene or offensive content

The content of websites and other electronic communications may be distasteful, obscene or offensive for a variety of reasons. In some instances these communications may be legal.

Over 25 jurisdictions within the USA place limits on certain speech and ban racist, blasphemous, politically subversive, libelous or slanderous, seditious, or inflammatory material that tends to incite hate crimes.

The extent to which these communications are unlawful varies greatly between countries, and even within nations. It is a sensitive area in which the courts can become involved in arbitrating between groups with strong beliefs.

One area of Internet pornography that has been the target of the strongest efforts at curtailment is child pornography.

**Harassment**

Whereas content may be offensive in a non-specific way, harassment directs obscenities and derogatory comments at specific individuals focusing for example on gender, race, religion, nationality, sexual orientation. This often occurs in chat rooms, through newsgroups, and by sending hate e-mail to interested parties (see cyberbullying, cyberstalking,hate crime, online predator, and stalking). Any comment that may be found derogatory or offensive is considered harassment. Harassment targeting women and children in the internet also includes revenge pornography. Dr.Debarati Halder and Dr.K.Jaishankar (2013) defined online revenge pornography as "an act whereby the perpetrator satisfies his anger and frustration for a broken relationship through publicising false, sexually provocative portrayal of his/her victim, by misusing the information that he may have known naturally, and that he may have stored in his personal computer, or may have been conveyed to his electronic device by the victim herself, or may have been stored in the device with the consent of the victim herself; and which may essentially have been done to publicly defame the victim.".

There are instances where committing a crime, which involves the use of a computer, can lead to an enhanced sentence. For example, in the case of United States v. Neil Scott Kramer, Kramer was served an enhanced sentence according to the U.S. Sentencing Guidelines Manual §2G1.3(b)(3) for his use of a cell phone to “persuade, induce, entice, coerce, or facilitate the travel of, the minor to engage in prohibited sexual conduct.” Kramer argued that this claim was insufficient because his charge included persuading through a computer device and his cellular phone technically is not a computer. Although Kramer tried to argue this point, U.S. Sentencing Guidelines Manual states that the term computer "means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

Connecticut was the first state to pass a statute making it a criminal offense to harass someone by computer. Michigan, Arizona, and Virginia and South Carolina have also passed laws banning harassment by electronic means.

Harassment as defined in the U.S. computer statutes is typically distinct from cyberbullying, in that the former usually relates to a person's "use a computer or computer network to communicate obscene, vulgar, profane, lewd, lascivious, or indecent language, or make any suggestion or proposal of an obscene nature, or threaten any illegal or immoral act," while the latter need not involve anything of a sexual nature.

**Threats**

Although freedom of speech is protected by law in most democratic societies (in the US this is done by the First Amendment), it does not include all types of speech. In fact spoken or written "true threat" speech/text is criminalized because of "intent to harm or intimidate", that also applies for online or any type of network related threats in written text or speech. The US Supreme Court definition of "true threat" is "statements where the speaker means to communicate a serious expression of an intent to commit an act of unlawful violence to a particular individual or group".

**Drug trafficking**

"Drug traffickers are increasingly taking advantage of the Internet" according to cyber authorities and personnel." to sell their illegal substances through encrypted e-mail and other Internet Technology. Some drug traffickers arrange deals at internet cafes, use courier Web sites to track illegal packages of pills, and swap recipes for amphetamines in restricted-access chat rooms. The deep web site Silk Road was a major online marketplace for drugs

before it was shut down by law enforcement (then reopened under new management, and then shut down by law enforcement again).

The rise in Internet drug trades could also be attributed to the lack of face-to-face communication. These virtual exchanges allow more intimidated individuals to more comfortably purchase illegal drugs. The sketchy effects that are often associated with drug trades are severely minimized and the filtering process that comes with physical interaction fades away.

# Combating computer crime

## Diffusion of Cybercrime

The broad diffusion of cybercriminal activities is an issue in computer crimes detection and prosecution. According to Jean-Loup Richet (Research Fellow at ESSEC ISIS), technical expertise and accessibility no longer act as barriers to entry into cybercrime. Indeed, hacking is much less complex than it was a few years ago, as hacking communities have greatly diffused their knowledge through the Internet. Blogs and communities have hugely contributed to information sharing: beginners could benefit from older hackers' knowledge and advice. Furthermore, Hacking is cheaper than ever: before the cloud computing era, in order to spam one needed a dedicated server, skills in server management, network configuration and maintenance, knowledge of Internet service provider standards, etc. By comparison, a mail software-as-a-service is a scalable, inexpensive, bulk, and transactional e-mail-sending service for marketing purposes and could be easily set up for spam. Jean-Loup Richet explains that cloud computing could be helpful for a cybercriminal as a way to leverage his attack - brute-forcing a password, improve the reach of a botnet, or facilitating a spamming campaign.

## Investigation

A computer can be a source of evidence (see digital forensics). Even where a computer is not directly used for criminal purposes, it may contain records of value to criminal investigators in the form of a logfile. In most countries Internet Service Providers are required, by law, to keep their logfiles for a predetermined amount of time. For example; a European wide directive (applicable to all EU member states) states that all E-mail traffic should be retained for a minimum of 12 months.

## Legislation

Due to easily exploitable laws, cybercriminals use developing countries in order to evade detection and prosecution from law enforcement. In developing countries, such as the Philippines, laws against cybercrime are weak or sometimes nonexistent. These weak laws allow cybercriminals to strike from international borders and remain undetected. Even when identified, these criminals avoid being punished or extradited to a country, such as the United States, that has developed laws that allow for prosecution. While this proves difficult in some cases, agencies, such as the FBI, have uses deception and subterfuge to catch criminals. For example, two Russian hackers had been evading the FBI for some time. The FBI set up a fake computing company based in Seattle, Washington. They proceeded to lure the two Russian men into the United States by offering them work with this company. Upon completion of the interview, the suspects were arrested outside of the building. Clever tricks like this are sometimes a necessary part of catching cybercriminals when weak legislation makes it impossible otherwise.

President Barack Obama released in an executive order in April 2015 to combat cybercrime. The executive order allows the United States to freeze assets of convicted cybercriminals and block their economic activity within the United States. This is some of the first solid legislation that combats cybercrime in this way.

## Penalties

Penalties for computer related crimes in New York State can range from a fine and a short period of jail time for a Class A misdemeanor such as unauthorized use of a computer up to

computer tampering in the first degree which is a Class C felony and can carry 3 to 15 years in prison.

However, some hackers have been hired as information security experts by private companies due to their inside knowledge of computer crime, a phenomenon which theoretically could create perverse incentives. A possible counter to this is for courts to ban convicted hackers from using the internet or computers, even after they have been released from prison – though as computers and the internet become more and more central to everyday life, this type of punishment may be viewed as more and more harsh and draconian. However, nuanced approaches have been developed that manage cyberoffender behavior without resorting to total computer and/or Internet bans.[ These approaches involve restricting individuals to specific devices which are subject to computer monitoring and/or computer searches by probation and/or parole officers.

# Computer virus

A **computer virus** is a malware program that, when executed, replicates by inserting copies of itself (possibly modified) into othercomputer programs, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be "infected".[1][2][3][4] Viruses often perform some type of harmful activity on infected hosts, such as stealing hard disk space or CPU time, accessing private information, corrupting data, displaying political or humorous messages on the user's screen, spamming their contacts,logging their keystrokes, or even rendering the computer useless. However, not all viruses carry a destructive payload or attempt to hide themselves—the defining characteristic of viruses is that they are self-replicating computer programs which install themselves without user consent.

Virus writers use social engineering and exploit detailed knowledge of security vulnerabilities to gain access to their hosts' computing resources. The vast majority of viruses target systems running Microsoft Windows, employing a variety of mechanisms to infect new hosts, and often using complex anti-detection/stealth strategies to evade antivirus software. Motives for creating viruses can include seeking profit, desire to send a political message, personal amusement, to demonstrate that a vulnerability exists in software, forsabotage and denial of service, or simply because they wish to explore artificial life and evolutionary algorithms.

Computer viruses currently cause billions of dollars' worth of economic damage each year due to causing systems failure, wasting computer resources, corrupting data, increasing maintenance costs, etc. In response, free, open-source antivirus tools have been developed, and a multi-billion dollar industry of antivirus software vendors has cropped up, selling virus protection to users of various operating systems of which Windows is often the most victimized, partially due to its extreme popularity. No currently existing antivirus software is able to catch all computer viruses (especially new ones); computer security researchers are actively searching for new ways to enable antivirus solutions to more effectively detect emerging viruses, before they have already become widely distributed.

## Infection targets and replication techniques

Computer viruses infect a variety of different subsystems on their hosts. One manner of classifying viruses is to analyze whether they reside in binary executables (such as.EXE or .COM files), data files (such as Microsoft Word documents or PDF files), or in the boot sector of the host's hard drive (or some combination of all of these).

### Resident vs. non-resident viruses

A *memory-resident virus* (or simply "resident virus") installs itself as part of the operating system when executed, after which it remains in RAM from the time the computer is booted up to when it is shut down. Resident viruses overwrite interrupt handling code or other functions, and when the operating system attempts to access the target file or disk sector, the virus code intercepts the request and redirects the control flow to the replication module, infecting the target. In contrast, a *non-memory-resident virus* (or "non-resident virus"), when executed, scans the disk for targets, infects them, and then exits (i.e. it does not remain in memory after it is done executing).

### Macro viruses

Many common applications, such as Microsoft Outlook and Microsoft Word, allow macro programs to be embedded in documents or emails, so that the programs may be run automatically when the document is opened. A *macro virus* (or "document virus") is a virus that is written in a macro language, and embedded into these documents so that when users open the file, the virus code is executed, and can infect the user's computer. This is one of the reasons that it is dangerous to open unexpected attachments in e-mails.

### Boot sector viruses

*Boot sector viruses* specifically target the boot sector/Master Boot Record (MBR) of the host's hard drive or removable storage media (flash drives, floppy disks, etc.).

## Stealth strategies

In order to avoid detection by users, some viruses employ different kinds of deception. Some old viruses, especially on the MS-DOS platform, make sure that the "last modified" date of a host file stays the same when the file is infected by the virus. This approach does not fool antivirus software, however, especially those which maintain and date cyclic redundancy checks on file changes.

Some viruses can infect files without increasing their sizes or damaging the files. They accomplish this by overwriting unused areas of executable files. These are called *cavity viruses*. For example, the CIH virus, or Chernobyl Virus, infects Portable Executable files. Because those files have many empty gaps, the virus, which was 1 KB in length, did not add to the size of the file.

Some viruses try to avoid detection by killing the tasks associated with antivirus software before it can detect them (for example, Conficker).

As computers and operating systems grow larger and more complex, old hiding techniques need to be updated or replaced. Defending a computer against viruses may demand that a file system migrate towards detailed and explicit permission for every kind of file access.

## Countermeasures

### Antivirus software

Many users install antivirus software that can detect and eliminate known viruses when the computer attempts to download or run the executable (which may be distributed as an email attachment, or on USB flash drives, for example). Some antivirus software blocks known malicious web sites that attempt to install malware. Antivirus software does not change the underlying capability of hosts to transmit viruses. Users must update their software regularly to patch security vulnerabilities ("holes"). Antivirus software also needs to be regularly updated in order to recognize the latest threats. The German AV-TEST Institute publishes evaluations of antivirus software for Windows and Android.

Examples of Microsoft Windows anti virus and anti-malware software include the optional Microsoft Security Essentials (for Windows XP, Vista and Windows 7) for real-time protection, the Windows Malicious Software Removal Tool (now included with Windows (Security) Updates on "Patch Tuesday", the second Tuesday of each month), and Windows Defender (an optional download in the case of Windows XP). Additionally, several capable antivirus software programs are available for free download from the Internet (usually restricted to non-commercial use). Some such free programs are almost as good as commercial competitors. Common security vulnerabilities are assigned CVE IDs and listed in the US National Vulnerability Database. Secunia PSI is an example of software, free for personal use, that will check a PC for vulnerable out-of-date software, and attempt to update it. Ransomware and phishing scam alerts appear as press releases on the Internet Crime Complaint Center noticeboard.

Other commonly used preventative measures include timely operating system updates, software updates, careful Internet browsing, and installation of only trusted software. Certain browsers flag

sites that have been reported to Google and that have been confirmed as hosting malware by Google.

There are two common methods that an antivirus software application uses to detect viruses, as described in the antivirus software article. The first, and by far the most common method of virus detection is using a list of virus signature definitions. This works by examining the content of the computer's memory (its RAM, and boot sectors) and the files stored on fixed or removable drives (hard drives, floppy drives, or USB flash drives), and comparing those files against a database of known virus "signatures". Virus signatures are just strings of code that are used to identify individual viruses; for each virus, the antivirus designer tries to choose a unique signature string that will not be found in a legitimate program. Different antivirus programs use different "signatures" to identify viruses. The disadvantage of this detection method is that users are only protected from viruses that are detected by signatures in their most recent virus definition update, and not protected from new viruses (see "zero-day attack").

A second method to find viruses is to use a heuristic algorithm based on common virus behaviors. This method has the ability to detect new viruses for which antivirus security firms have yet to define a "signature", but it also gives rise to more false positives than using signatures. False positives can be disruptive, especially in a commercial environment.

## Recovery strategies and methods

One can also reduce the damage done by viruses by making regular backups of data (and the operating systems) on different media, that are either kept unconnected to the system (most of the time), read-only or not accessible for other reasons, such as using different file systems. This way, if data is lost through a virus, one can start again using the backup (which will hopefully be recent).

If a backup session on optical media like CD and DVD is closed, it becomes read-only and can no longer be affected by a virus (so long as a virus or infected file was not copied onto the CD/DVD). Likewise, an operating system on a bootable CD can be used to start the computer if the installed operating systems become unusable. Backups on removable media must be carefully inspected before restoration. The Gammima virus, for example, propagates via removable flash drives.

### Virus removal

Many websites run by antivirus software companies provide free online virus scanning, with limited cleaning facilities (the purpose of the sites is to sell antivirus products). Some websites—like Google subsidiary VirusTotal.com—allow users to upload one or more suspicious files to be scanned and checked by one or more antivirus programs in one operation. Additionally, several capable antivirus software programs are available for free download from the Internet (usually restricted to non-commercial use).[61] Microsoft offers an optional free antivirus utility called Microsoft Security Essentials, a Windows Malicious Software Removal Tool that is updated as part of the regular Windows update regime, and an older optional anti-malware (malware removal) tool Windows Defender that has been upgraded to an antivirus product in Windows 8.

Some viruses disable System Restore and other important Windows tools such as Task Manager and CMD. An example of a virus that does this is CiaDoor. Many such viruses can be removed by rebooting the computer, entering Windows safe mode with networking, and then using system tools or Microsoft Safety Scanner.[ System Restore onWindows Me, Windows XP, Windows Vista and Windows 7 can restore the registry and critical system files to a previous checkpoint. Often a virus will cause a system to hang, and a subsequent hard reboot will render a system restore point from the same day corrupt. Restore points from previous days should work provided the virus is not designed to corrupt the restore files and does not exist in previous restore points.

### Operating system reinstallation

Microsoft's System File Checker (improved in Windows 7 and later) can be used to check for, and repair, corrupted system files.

Restoring an earlier "clean" (virus-free) copy of the entire partition from a cloned disk, a disk image, or a backup copy is one solution—restoring an earlier backup disk image is relatively simple to do, usually removes any malware, and may be faster than disinfecting the computer—or

reinstalling and reconfiguring the operating system and programs from scratch, as described below, then restoring user preferences.

Reinstalling the operating system is another approach to virus removal. It may be possible to recover copies of essential user data by booting from a live CD, or connecting the hard drive to another computer and booting from the second computer's operating system, taking great care not to infect that computer by executing any infected programs on the original drive. The original hard drive can then be reformatted and the OS and all programs installed from original media. Once the system has been restored, precautions must be taken to avoid reinfection from any restored executable files.

# Historical development

## Viruses and the Internet

Before computer networks became widespread, most viruses spread on removable media, particularly floppy disks. In the early days of the personal computer, many users regularly exchanged information and programs on floppies. Some viruses spread by infecting programs stored on these disks, while others installed themselves into the disk boot sector, ensuring that they would be run when the user booted the computer from the disk, usually inadvertently. Personal computers of the era would attempt to boot first from a floppy if one had been left in the drive. Until floppy disks fell out of use, this was the most successful infection strategy and boot sector viruses were the most common in the wild for many years.

Traditional computer viruses emerged in the 1980s, driven by the spread of personal computers and the resultant increase in BBS, modem use, and software sharing. Bulletin board–driven software sharing contributed directly to the spread of Trojan horse programs, and viruses were written to infect popularly traded software. Shareware and bootlegsoftware were equally common vectors for viruses on BBSs. Viruses can increase their chances of spreading to other computers by infecting files on a network file system or a file system that is accessed by other computers.

Macro viruses have become common since the mid-1990s. Most of these viruses are written in the scripting languages for Microsoft programs such as Word and Excel and spread throughout Microsoft Office by infecting documents and spreadsheets. Since Word and Excel were also available for Mac OS, most could also spread to Macintosh computers. Although most of these viruses did not have the ability to send infected email messages, those viruses which did take advantage of the Microsoft Outlook COMinterface.

Some old versions of Microsoft Word allow macros to replicate themselves with additional blank lines. If two macro viruses simultaneously infect a document, the combination of the two, if also self-replicating, can appear as a "mating" of the two and would likely be detected as a virus unique from the "parents".[

A virus may also send a web address link as an instant message to all the contacts on an infected machine. If the recipient, thinking the link is from a friend (a trusted source) follows the link to the website, the virus hosted at the site may be able to infect this new computer and continue propagating.[

Viruses that spread using cross-site scripting were first reported in 2002, and were academically demonstrated in 2005. There have been multiple instances of the cross-site scripting viruses in the wild, exploiting websites such as MySpace and Yahoo!.

# Phishing

**Phishing** is the illegal attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication. The word is a neologism created as a homophone of *fishing* due to the similarity of using fake bait in an attempt to catch a victim. Communications purporting to be from popular social web sites, auction sites, banks, online payment processors or IT administrators are commonly used to lure

unsuspecting public. Phishing emails may contain links to websites that are infected with malware. Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users, and exploits the poor usability of current web security technologies.[7] Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures. Many websites have now created secondary tools for applications, like maps for games, but they should be clearly marked as to who wrote them, and users should not use the same passwords anywhere on the internet.

Phishing is a continual threat that keeps growing to this day. The risk grows even larger in social media such as Facebook, Twitter, Myspace etc. Hackers commonly use these sites to attack persons using these media sites in their workplace, homes, or public in order to take personal and security information that can affect the user and the company (if in a workplace environment). Phishing is used to portray trust in the user since the user may not be able to tell that the site being visited or program being used is not real, and when this occurs is when the hacker has the chance to access the personal information such as passwords, usernames, security codes, and credit card numbers among other things.

# Pharming

**Pharming** is a cyber attack intended to redirect a website's traffic to another, fake site. Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in DNS server software. DNS servers are computers responsible for resolving Internet names into their real IP addresses. Compromised DNS servers are sometimes referred to as "poisoned". Pharming requires unprotected access to target a computer, such as altering a customer's home computer, rather than a corporate business server.

The term "pharming" is a neologism based on the words "farming" and "phishing". Phishing is a type of social-engineering attack to obtain access credentials, such as user names and passwords. In recent years, both pharming and phishing have been used to gain information for online identity theft. Pharming has become of major concern to businesses hosting ecommerce and online banking websites. Sophisticated measures known as anti-pharming are required to protect against this serious threat. Antivirus software and spyware removal software cannot protect against pharming.

# Trojan horse (computing)

A **Trojan horse**, or **Trojan**, in computing is generally a non-self-replicating type of malware program containing malicious code that, when executed, carries out actions determined by the nature of the Trojan, typically causing loss or theft of data, and possible system harm. The term is derived from the Ancient Greek story of the large wooden horse used to trick defenders of Troy into taking warriors concealed in the horse into their city in ancient Anatolia. The use of this name references how computer Trojans often employ a form of social engineering, presenting themselves as routine, useful, or interesting in order to persuade victims to install them on their computers.

A Trojan often acts as a backdoor, contacting a controller which can then have unauthorized access to the affected computer While Trojans and backdoors are not easily detectable by themselves, computers may appear to run slower due to heavy processor or network usage. Malicious programs are classified as Trojans if they do not attempt to inject themselves into other files (computer virus) or otherwise propagate themselves (worm). A computer may host a Trojan via a malicious program that a user is duped into executing (often an e-mail attachment disguised to be unsuspicious, e.g., a routine form to be filled in), or by drive-by download.

# Etiquette in technology

**Etiquette in technology** governs what conduct is socially acceptable in an online or digital situation. While etiquette is ingrained into culture, etiquette in technology is a fairly recent concept. The rules of etiquette that apply when communicating over the Internet or social networks or devices are different from those applying when communicating in person or by audio (such as telephone) or videophone (such as Skype video). It is a social code of network communication.

Communicating with others via the Internet without misunderstandings in the heat of the moment can be challenging, mainly because facial expressions and body languagecannot be interpreted on cyberspace. Therefore, several recommendations to attempt to safeguard against these misunderstandings have been proposed.

# Netiquette

*Netiquette*, a colloquial portmanteau of *network etiquette* or *Internet etiquette*, is a set of social conventions that facilitate interaction over networks, ranging from Usenet andmailing lists to blogs and forums.

Like the network itself, these developing norms remain in a state of flux and vary from community to community. The points most strongly emphasized about Usenet netiquette often include using simple electronic signatures, and avoiding multiposting, cross-posting, off-topic posting, hijacking a discussion thread, and other techniques used to minimize the effort required to read a post or a thread. Similarly, some Usenet guidelines call for use of unabbreviated English while users of instant messaging protocols like SMSoccasionally encourage just the opposite, bolstering use of SMS language. However, many online communities frown upon this practice.

Common rules for e-mail[ and Usenet such as avoiding flamewars and spam are constant across most mediums and communities. Another rule is to avoid typing in all caps or grossly enlarging script for emphasis, which is considered to be the equivalent of shouting or yelling. Other commonly shared points, such as remembering that one's posts are (or can easily be made) public, are generally intuitively understood by publishers of Web pages and posters to Usenet, although this rule is somewhat flexible depending on the environment. On more private protocols, however, such as e-mail and SMS, some users take the privacy of their posts for granted. One-on-one communications, such as private messages on chat forums and direct SMSs, may be considered more private than other such protocols, but infamous breaches surround even these relatively private media. For example, Paris Hilton's Sidekick PDA was cracked in 2005, resulting in the publication of her private photos, SMS history, address book, etc.

A group e-mail sent by Cerner CEO Neal Patterson to managers of a facility in Kansas City concerning "Cerner's declining work ethic" read, in part, "The parking lot is sparsely used at 8 A.M.; likewise at 5 P.M. As managers—you either do not know what your EMPLOYEES are doing; or YOU do not CARE ... In either case, you have a problem and you will fix it or I will replace you."[6] After the e-mail was forwarded to hundreds of other employees, it quickly leaked to the public. On the day that the e-mail was posted to Yahoo!, Cerner's stock price fell by over 22%[7] from a high market capitalization of US$1.5 billion.

Beyond matters of basic courtesy and privacy, e-mail syntax (defined by RFC 2822) allows for different types of recipients. The primary recipient, defined by the To: line, can reasonably be expected to respond, but recipients of carbon copies cannot be, although they still might.[ Likewise, misuse of the CC: functions in lieu of traditional mailing listscan result in serious technical issues. In late 2007, employees of the United States Department of Homeland Security used large CC: lists in place of a mailing list to broadcast messages to several hundred users. Misuse of the "reply to all" caused the number of responses to that message to quickly expand to some two million messages, bringing down their mail server. In cases like this, rules of netiquette have more to do with efficient sharing of resources—ensuring that the associated technology continues to function—rather than more basic etiquette. On Usenet, cross-posting, in which a single copy of a message is posted to multiple groups is intended to prevent this from happening, but many newsgroups frown on the practice, as it means users must sometimes read many copies of a message in multiple groups.

"When someone makes a mistake – whether it's a spelling error or a spelling flame, a stupid question or an unnecessarily long answer – be kind about it. If it's a minor error, you may not

need to say anything. Even if you feel strongly about it, think twice before reacting. Having good manners yourself doesn't give you license to correct everyone else. If you do decide to inform someone of a mistake, point it out politely, and preferably by private email rather than in public. Give people the benefit of the doubt; assume they just don't know any better. And never be arrogant or self-righteous about it. Just as it's a law of nature that spelling flames always contain spelling errors, notes pointing out Netiquette violations are often examples of poor Netiquette."

Due to the large variation between what is considered acceptable behavior in various professional environments and between professional and social networks, codified internalmanuals of style can help clarify acceptable limits and boundaries for user behavior. For instance, failure to publish such a guide for e-mail style was cited among the reasons for a NZ$17,000 wrongful dismissal finding against a firm that fired a woman for misuse of all caps in company-wide e-mail traffic.

### Online etiquette

*Digital citizenship* is a term that describes how a person should act while using digital technology online and has also been defined as "the ability to participate in society online". The term is often mentioned in relation to Internet safety and netiquette.

The term has been used as early as 1998 and has gone through several changes in description as newer technological advances have changed the method and frequency of how people interact with one another online. Classes on digital citizenship have been taught in some public education systems and some argue that the term can be "measured in terms of economic and political activities online".

## Cell phone etiquette

The issue of mobile communication and etiquette has also become an issue of academic interest. The rapid adoption of the device has resulted in the intrusion of telephony into situations where it was previously not used. This has exposed the implicit rules of courtesy and opened them to reevaluation.

### Cell phone etiquette in the education system

Most schools in the United States and Europe and Canada have prohibited mobile phones in the classroom, citing class disruptions and the potential for cheating via text messaging. In the UK, possession of a mobile phone in an examination can result in immediate disqualification from that subject or from all that student's subjects. This still applies even if the mobile phone was not turned on at the time. In New York City, students are banned from taking cell phones to school. This has been a debate for several years, but finally passed legislature in 2008.

“Most schools allow students to have cell phones for safety purposes”—a reaction to the Littleton, Colorado, high school shooting incident of 1999 (Lipscomb 2007: 50). Apart from emergency situations, most schools don’t officially allow students to use cell phones during class time.

### Cell phone etiquette in the public sphere

Talking or texting on a cell phone in public may seem a distraction for many individuals. When in public there are two times when one uses a phone. The first is when someone is alone and the other is when he/she is in a group. The main issue for most people is when they are in a group, and the cell phone becomes a distraction or a barrier for successful socialization among family and friends. In the past few years, society has become less tolerant of cell phone use in public areas for example, public transportation, restaurants and much more. This is exemplified by the widespread recognition of campaigns such as Stop Phubbing, which prompted global discussion as to how mobile phones should be used in the presence of others. “Some have suggested that mobile phones ‘affect every aspect of our personal and professional lives either directly or indirectly’” (Humphrey). Every culture's tolerance of cell phone usage varies, for instance in Western society cell phones are permissible during free time at schools, whereas in the eastern countries, cell phones are strictly prohibited on school property.

## Cell phone etiquette within social relationships

When critically assessing the family structure, it is important to examine the parent/child negotiations which occur in the household, in relation to the increased use of cell phones. Teenagers use their cell phones as a way to negotiate spatial boundaries with their parents (Williams 2005:316). This includes extending curfews in the public space and allowing more freedom for the teenagers when they are outside of the home (Williams 2005:318). More importantly, cell phone etiquette relates to kinship groups and the family as an institution. This is because cell phones act as a threat due to the rapid disconnect within families. Children are often so closely affiliated with their technological gadgets, and they tend to interact with their friends constantly and this has a negative impact on their relationship with their parents (Williams 2005:326). Teenagers see themselves as gaining a sense of empowerment from the mobile phone. Cell phone etiquette in the household from an anthropological perspective has shown an evolution in the institution of family. The mobile phone has now been integrated into family practices and perpetuated a wider concern which is the fracture between parent and child relationships. We are able to see the traditional values disappearing however, reflexive monitoring is occurring (Williams 2005:320). Through this, parents are becoming friendlier with their children and critics emphasize that this change is problematic because children should be subjected to social control. One way of social control is limiting the time spent interacting with friends, which is difficult to do in today's society because of the rapid use of cell phones.

# Netiquette vs. cell phone etiquette

Cell phone etiquette is largely dependent on the cultural context and what is deemed to be socially acceptable. For instance, in certain cultures using your hand held devices while interacting in a group environment is considered bad manners, whereas, in other cultures around the world it may be viewed differently. In addition, cell phone etiquette also encompasses the various types of activities which are occurring and the nature of the messages which are being sent. More importantly, messages of an inappropriate nature can be sent to an individual and this could potentially orchestrate problems such as verbal/ cyber abuse.

## New technology and behaviors

Perhaps the biggest obstacle to communication in online settings is the lack of emotional cues. Facial cues dictate the mood and corresponding diction of two people in a conversation. During phone conversations, tone of voice communicates the emotions of the person on the other line. But with chat rooms, instant messaging apps and texting, any signals that would indicate the tone of a person's words or their state of emotion are absent. Because of this, there have been some interesting accommodations. Perhaps the two most prevalent compensating behaviors are the use of emoticons and abbreviations. Emoticons use punctuation marks to illustrate common symbols that pertain to facial cues. For example, one would combine a colon and parenthesis to recreate the symbol of the smiley face indicating the happiness or satisfaction of the other person. To symbolize laughter, the abbreviation "LOL" standing for "laughing out loud" developed. Along with these, countless other symbols and abbreviations have developed including, "BRB" ("be right back"), "TTYL" (talk to you later) and specific designs incorporated by apps of a laughing face, sad face, crying face, angry face etc. The newest in the line of these symbols include Facebook's stickers, which are illustrations that one can send over Facebook's messaging app and described by Facebook as "a great way to share how you're feeling and add personality to your chats."

Now, as newer modes of communication are becoming more common, the rules of communication must adapt as fast as the technology. For example, one of the most popular new apps, Snapchat, is growing to have its own rules and etiquette. This app lets users send pictures or videos to friends that disappear after a couple seconds of viewing it. Initially, the thought that occurs to people when confronted by this app is its implications for sexting. Although it's entirely possible to make use of Snapchat for that purpose, what the app has developed into is a form of communication that shares funny or interesting moments. Originally compared to Instagram [33] by way of the app's ability to broadcast pictures to many people, it has now become standard to communicate through Snapchat by sending pictures back and forth and using the caption bar for messages. The reply option on Snapchat specifically promotes this behavior, but Snapchat etiquette is not set in stone. It is becoming clear that Snaps personalized for the receiver expect a reply, but where ends this obligation? Some people use Snapchat specifically for the purpose of

communication, while some use it to simply provide a visual update of their day. The newest update of Snapchat, an instant messaging add-on, seems to be catered to those who use the app to send messages back and forth. This new messaging add-on, along with the video chat feature will warrant new forms of social construct and expectations of behavior in accordance with this application.

# Legal aspects of computing

The first one, historically, was **information technology law** (or **IT law**). *("IT law" should not be confused with the IT aspects of law itself, although there are overlapping issues.)* **IT law** consists of the law (statutes, regulations, and caselaw) which governs the digitaldissemination of both (digitalized) information and software itself (see history of free and open-source software), and legal aspects ofinformation technology more broadly. IT law covers mainly the digital information (including information security and electronic commerce) aspects and it has been described as "paper laws" for a "paperless environment".

**Cyberlaw** or **Internet law** is a term that encapsulates the legal issues related to use of the Internet. It is less a distinct field of law than intellectual property or contract law, as it is a domain covering many areas of law and regulation. Some leading topics include internet access and usage, privacy, freedom of expression, and jurisdiction.

**"Computer law"** is a third term which tends to relate to issues including both Internet law and the patent and copyright aspects of computer technology and software.

# Software license

A **software license** is a legal instrument (usually by way of contract law, with or without printed material) governing the use or redistribution of software. Under United States copyright law all software is copyright protected, except material in the public domain. A typical software license grants an end-user permission to use one or more copies of software in ways where such a use would otherwise potentially constitute copyright infringement of the software owner's exclusive rights under copyright law.

In addition to granting rights and imposing restrictions on the use of software, software licenses typically contain provisions which allocate liability and responsibility between the parties entering into the license agreement. In enterprise and commercial software transactions these terms often include limitations of liability, warranties and warranty disclaimers, and indemnity if the software infringes intellectual property rights of others.

Software licenses can generally be fit into the following categories: proprietary licenses and free and open source. The significant feature that distinguishes them are the terms under which the end-users may further distribute or copy the software.

## Software licenses and copyright law

In the United States, Section 117 of the Copyright Act gives the owner of a particular copy of software the explicit right to use the software with a computer, even if use of the software with a computer requires the making of incidental copies or adaptations (acts which could otherwise potentially constitute copyright infringement). Therefore, the owner of a copy of computer software is legally entitled to use that copy of software. Hence, if the end-user of software is the owner of the respective copy, then the end-user may legally use the software without a license from the software publisher.

## Proprietary software licenses

The hallmark of proprietary software licenses is that the software publisher grants the use of one or more copies of software under the end-user license agreement (EULA), but ownership of those copies remains with the software publisher (hence use of the term "proprietary"). This feature of proprietary software licenses means that certain rights regarding the software are reserved by the

software publisher. Therefore, it is typical of EULAs to include terms which define the uses of the software, such as the number of installations allowed or the terms of distribution.

The most significant effect of this form of licensing is that, if ownership of the software remains with the software publisher, then the end-user *must* accept the software license. In other words, without acceptance of the license, the end-user may not use the software at all. One example of such a proprietary software license is the license for Microsoft Windows. As is usually the case with proprietary software licenses, this license contains an extensive list of activities which are restricted, such as: reverse engineering, simultaneous use of the software by multiple users, and publication of benchmarks or performance tests.

The most common licensing models is per single user (named user, client, node) or per user in the appropriate volume discount level, while some manufacturers accumulate existing licenses. These open volume license programs are typically called Open License Program (OLP), Transactional License Program (TLP), Volume License Program (VLP) etc. and are contrary to the Contractual License Program (CLP), where the customer commits to purchase a certain amount of licenses over a fixed period (mostly two years). Licensing per concurrent/floating user also occurs, where all users in a network have access to the program, but only a specific number at the same time. Another license model is licensing per dongle which allows the owner of the dongle to use the program on any computer. Licensing per server, CPU or points, regardless the number of users, is common practice as well as Site or Company Licenses. Sometimes one can choose between perpetual (permanent) and annual license. For perpetual licenses one year of maintenance is often required, but maintenance (subscription) renewals are discounted. For annual licenses, there is no Renewal, a new license must be purchased after expiration. Licensing can be Host/Client (or Guest), Mailbox, IP-Address, Domain etc., depending on how the program is used. Additional users are inter alia licensed per Extension Pack (e.g. up to 99 users) which includes the Base Pack (e.g. 5 users). Some programs are modular, so one will have to buy a base product before they can use other modules.[4]

Software licensing also includes maintenance. This, usually with a term of one year, is either included or optional, but must often be bought with the software. The maintenance agreement (contract) contains Minor Updates (V.1.1 => 1.2), sometimes Major Updates (V.1.2 => 2.0) and is called e.g. Update Insurance, Upgrade Assurance. For a Major Update the customer has to buy an Upgrade, if not included in the maintenance. For a maintenance renewal some manufacturers charge a Reinstatement (Reinstallment) Fee retroactively per month, in case the current maintenance has expired. Maintenance normally doesn't include technical support. Here one can differentiate between e-mail and tel. support, also availability (e.g. 5x8, 5 days a week, 8 hours a day) and reaction time (e.g. three hours) can play a role. This is commonly named Gold, Silver and Bronze Support. Support is also licensed per incident as Incident Pack (e.g. five support incidents per year).

Many manufacturers offer special conditions for schools and government agencies (EDU/GOV License). Migration from another product (Crossgrade), even from a different manufacturer (Competitive Upgrade) is offered.

## Free and open-source software licenses

Free and open-source licenses generally fall under two categories: Those with the aim to have minimal requirements about how the software can be redistributed (permissive licenses), and those that aim to preserve the freedoms that are given to the users by ensuring that all subsequent users receive those rights (copyleft Licenses).

An example of a copyleft free software license is the GNU General Public License (GPL). This license is aimed at giving all user unlimited freedom to use, study, and privately modify the software, and if the user adheres to the terms and conditions of GPL, freedom to redistribute the software or any modifications to it. For instance, any modifications made and redistributed by the end-user must include the source code for these, and the license of any derivative work must not put any additional restrictions beyond what GPL allows.

Examples of permissive free software licenses are the BSD license and the MIT license, which give unlimited permission to use, study, and privately modify the software, and includes only

minimal requirements on redistribution. This gives a user the permission to take the code and use it as part of closed-source software or software released under aproprietary software license.

Free Software Foundation, the group that maintains The Free Software Definition, maintains a non-exhaustive list of free software licenses. The list distinguishes between free software licenses that are compatible or incompatible with the FSF license of choice, the GNU General Public License, which is a copyleft license. The list also contains licenses which the FSF considers non-free for various reasons, but which are sometimes mistaken as being free.

# Common computer-induced medical problems

There are three main notable medical problems that can arise from using computers. They are Carpal Tunnel Syndrome, Computer Vision Syndrome and Musculoskeletal problems.

## Carpal Tunnel Syndrome

The medical problem associated with computer-related work is carpal tunnel syndrome (CTS). CTS is a stress-related injury caused by repetitive movement of joints, especially the wrist, and can lead to numerous musculoskeletal problems. It has become very common among Computer professionals due to poorly placed computer components and extensive typing over a long period of time. Studies conducted show that one in eight computer professionals suffer from CTS.[ This study was conducted over 21 companies and the majority of sufferers said that they experienced acute and in some cases severe pain due to CTS. The main cause of CTS seems to be debatable, however, with many sources saying that the syndrome is predominantly caused by the acute positioning of the wrist while typing and this problem is exacerbated by the need for the user to be crouching towards the screen while typing. Different research conducted cites the mouse as being the main cause of CTS as it was found that among the fingers the right thumb was revealed to be more susceptible to CTS due to the acute position of the thumb while using the mouse. CTS, although prevalent, seems to be very difficult to ameliorate or cure due to the consistency in the design of computer components such as the mouse and the keyboard, but some companies are leading the way with technologies such as touch screen monitors which will reduce stress on the hand and wrist. Employers in major companies are also taking measures to ameliorate CTS by implementing frequent work breaks and work rotation procedures to ensure that employees aren't working on a single computer for hours on end "a higher level of intensity of computer work results in higher risk for CTS."[ which causes severe stress on the joints and thus can lead to CTS

Cumulative trauma disorders are caused by "people who sit at PC workstations or visual display terminals in fast-paced, repetitive keystroke jobs. Their fingers, wrists, arms, necks, and back may become so weak and painful that they cannot work," Many people do not think about this when they look at their computer while using it. It is important to note that everything down to the keyboard has a design process behind it focusing on user interface.

## Computer vision syndrome

In many cases, frequent computer users suffer from computer vision syndrome, which is a degenerative eye problem which can result in severely reduced eyesight (Myopia), blurred vision, overall eye tiredness and even Glaucoma. Computer Eye Syndrome is an umbrella term for many problems but the causes of these problems can be easily identified. When using a computer due to the size and setup of the monitor and components it is necessary for the user to be within at least two feet of the monitor when performing any type of computational work. This presents many problems especially in older monitors due to an elevated amount of monitor glare, poor display quality and insufficient picture display refresh rates. Although these problems are more evident in older computers the newer models are not free from these problems either. Studies have been conducted into the correlation between computers and eye problems and it was found that the Ionizing radiation given off by monitors has severe detrimental effects on the eye and eyesight on a whole. They also state "Treatment requires a multidirectional approach combining ocular therapy with adjustment of the workstation" which shows these problems are quite easily solved with minimal investment from computer manufacturers through producing higher quality monitors with better resolution and refresh rates. The most common form of Computer Vision Syndrome is a condition termed Dry Eye, which results in itchy, sore and even the illusion that

something is stuck in your eye. This condition is often caused by extensively long period looking at a computer screen.

Video screens have a design process for user interface. Video screens can cause eyestrain from prolonged viewing. Cathode ray tubes are what are used to display the information on your computer. These send off radiation. This is a concern that has been taken into account when designing better computer screens for user interface.

### Musculoskeletal problems

Another medical issue caused by the use of computers is back and posture problems. These problems relate to musculoskeletal disorders caused by the need for the user to be crouched and hunched towards the monitors and computer components due to the design and positioning of these particular computer peripherals. This hunching forward of the user causes posture and back problems but is also the cause of severe and acute pain in the upper back, particularly pain in the neck and or shoulders. A study was conducted where 2146 technical assistants installed a computer program to monitor the musculoskeletal pain they suffered and answered questionnaires on the location and severity of the pain. The study showed interesting results, as it detailed how in the majority of cases any pain suffered was aggravated and exacerbated by the use of computer peripherals like the mouse and keyboard but overall the pain did not originate from using computers. "Moreover, there seems to be no relationship between computer use and prolonged and chronic neck and shoulder pain" This is a positive study for computer manufacturers but although the pain may not originate from computer peripherals there is no doubt that the pain is exacerbated by their use and this revelation alone should lead computer manufacturers to pioneer new technologies that reduce the risk of posture or musculoskeletal problems aggravated by the use of poorly designed and linearly designed computer peripherals.

In another study, It was found that women are at a greater risk than men to suffer from musculoskeletal problems then men. Two explanations given were that "women appear to consistently report more neck and upper extremity symptoms than men.", and that women may assume more taxing positions while working than men do due to differences in anthropometrics.

## Possible ameliorations

Overall it is clear to see that there are many medical problems that can arise from using computers and damaged eyesight, CTS and musculoskeletal problems are only the tip of the iceberg. But it is also important to note that changes are currently being made to ensure that all these problems are ameliorated to the best standard that employers and computer users currently have the technology to implement. By taking measures like ensuring our computer peripherals are situated to ensure maximum comfort while working and taking frequent breaks from computational work can go a long way to ensuring that many medical conditions arising from computers are avoided. These are small measures but they go a long way to ensuring that computer users maintain their health, As with many modern and marvellous technologies in the world today there is always a downside and the major downside of computers is the medical problems that can arise from their prolonged use. Thus it is the duty of computer users and employers everywhere to ensure that the downside is kept to a minimum.

## Treatment

Modern medical treatment for computer-induced medical problems like carpal tunnel syndrome include splints, surgery, corticosteroids, and physiotherapy therapy. Alternative medicine for computer-induced medical problems has also been shown to be effective, notably acupuncture.