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

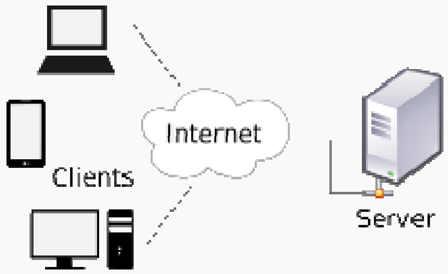
A virtual private network (VPN) is an overlay network in which some of the links between nodes are carried by open connections or virtual circuits in some larger network (e.g., the Internet) instead of by physical wires. The data link layer protocols of the virtual network are said to be tunneled through 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

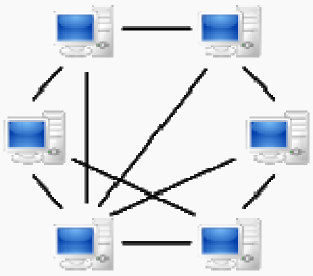


A computer network diagram of clients communicating with a server via the Internet.

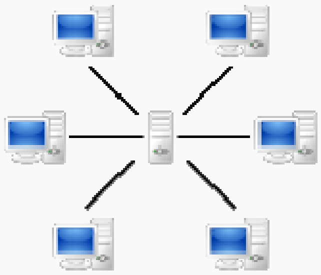
The **client–server model** of computing is a distributed application structure that partitions tasks or workloads between the providers of a resource or service, called servers, and service requesters, called clients.[1] Often clients and servers communicate over acomputer network on separate hardware, 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.

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.

Hoax

A hoax is a deliberately fabricated falsehood made to masquerade as truth. It is distinguishable from errors in observation or judgment, or rumors, urban legends, pseudosciences or April Fools' Day events that are passed along in good faith by believers or as jokes.

Definition

Robert Nares defined the word hoax as meaning "to cheat", dating from Thomas Ady's 1656 book A candle in the dark, or a treatise on the nature of witches and witchcraft.

The term hoax is occasionally used in reference to urban legends and rumors, but the folklorist Jan Harold Brunvand argues that most of them lack evidence of deliberate creations of falsehood and are passed along in good faith by believers or as jokes, so the term should be used for only those with a probable conscious attempt to deceive. As for the closely related terms *practical joke* and prank, Brunvand states that although there are instances where they overlap, hoax tends to indicate "relatively complex and large-scale fabrications" and includes deceptions that go beyond the merely playful and "cause material loss or harm to the victim" According to Professor Lynda Walsh of the University of Nevada, Reno, some hoaxes—such as the Great Stock Exchange Fraud of 1814, labeled as a hoax by contemporary commentators—are financial in nature, and successful hoaxers—such as P. T. Barnum, whose Fiji mermaid contributed to his wealth—often acquire monetary gain or fame through their fabrications, so the distinction between hoax and*fraud* is not necessarily clear. Alex Boese, the creator of the Museum of Hoaxes, states that the only distinction between them is the reaction of the public, because a fraud can be classified as a hoax when its method of acquiring financial gain creates a broad public impact or captures the imagination of the masses.

One of the earliest recorded media hoaxes is a fake almanac published by Jonathan Swift under the pseudonym of Isaac Bickerstaff in 1708. Swift predicted the death of John Partridge, one of the leading astrologers in England at that time, in the almanac and later issued an elegy on the day Partridge was supposed to have died. Partridge's reputation was damaged as a result and his astrological almanac was not published for the next six years.

It is possible to perpetrate a hoax by making only true statements using unfamiliar wording or context, such as in the Dihydrogen monoxide hoax. Political hoaxes are sometimes motivated by the desire to ridicule or besmirch opposing politicians or political institutions, often before elections.

A hoax differs from a magic trick or from fiction (books, movies, theatre, radio, television, etc.) in that the audience is unaware of being deceived, whereas in watching a magician perform an illusion the audience expects to be tricked.

A hoax is often intended as a practical joke or to cause embarrassment, or to provoke social or political change by raising people's awareness of something. It can also emerge from a marketing or advertising purpose. For example, to market a romantic comedy movie, a director staged a phony "incident" during a supposed wedding, which showed a bride and preacher getting knocked into a pool by a clumsy fall from a best man. A resulting

video clip of Chloe and Keith's Wedding was uploaded
to YouTube and was viewed by over 30 million people and the
couple was interviewed by numerous talk shows. Viewers were
deluded into thinking that it was an authentic clip of a real accident
at a real wedding; but a story in *USA Today*in 2009 revealed it was a
hoax.

A borderline case between fiction and hoax is a 1938 radio broadcast
by Orson Welles describing a Martian invasion of earth. Many people
who tuned in without hearing the introduction of the program as
fiction were concerned that the invasion was real. It has been
suggested that Welles knew the schedule of a popular program on
another channel, and scheduled the first report of the invasion to
coincide with a commercial break in the other program so that
people switching stations would be tricked.

Governments sometimes spread false information to assist them with
aims such as going to war; the "Iraq dossier" is an example of this;
these often come under the heading of black propaganda. There is
often a mixture of outright hoax and suppression and management of
information to give the desired impression. In wartime and times of
international tension rumours abound, some of which may be
deliberate hoaxes.

Examples of politics-related hoaxes:

Belgium is a country with a Flemish-speaking region and a Frenchspeaking region. In 2006 French-speaking television channel RTBF interrupted programming with a spoof report claiming that the country had split in two and the royal family had fled. On Saturday 13 March 2010 the Imedi television stationin Georgia broadcast a false announcement that Russia had invaded Georgia.

Psychologist Peter Hancock has identified six steps which
characterise a truly successful hoax: Identify a constituency- a person or group of people who, for reasons such as piety or patriotism, or greed, will truly care about your creation. Identify a particular dream which will make your hoax appeal to your constituency. Create an appealing but "under-specified" hoax, with ambiguities Have your creation discovered. Find at least one champion who will actively support your hoax. Make people care, either positively or negatively – the ambiguities encourage interest and debate

Email spam

Email spam, also known as junk email or unsolicited bulk email (UBE), is a subset of electronic spam involving nearly identical messages sent to numerous recipients by email. Clicking on links in spam email may send users to phishing web sites or sites that are hosting malware. Spam email may also include malware as scripts or other executable file attachments. Definitions of spam usually include the aspects that email is unsolicited and sent in bulk. One subset of UBE is UCE(unsolicited commercial email). The opposite of "spam", email which one wants, is called "ham", usually when referring to a message's automated analysis (such as Bayesian filtering). Like other forms of unwanted bulk messaging, it is named for Spam luncheon meat by way of a Monty Python sketch in which Spam is depicted as ubiquitous and unavoidable.

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.

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.

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 apropprietary 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.