CHAPTER 2
COMPUTER NETWORKS AND SECURITY

2.1 COMPUTER NETWORKS

A Computer network is a group of interconnected computers as illustrated in Figure 2.1. It involves connecting two or more computers together primarily with the aim of sharing resources. Before two or more computers can be said to be on a network, they have to be connected. The physical connection involves the use of a medium of communication which could be wired or wireless. For there to be a network, there must be at least two computer devices, called workstations, with each being a Microcomputer (laptop, desktop, smart phones, palmtop etc) or Supercomputer. When computers are connected together to form a network in the same local area, the main aim is to allow the sharing of resources. Resources can be in two main folds:

- **Software (Application and System Software)**
- **Hardware (Printers, Scanners, Peripherals etc.)**

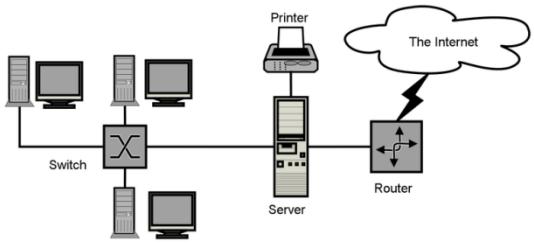

Fig. 2.1 Graphical Illustration of Computer Network

2.2 CLASSIFICATION OF COMPUTER NETWORKS

Computer Networks may be classified according to a wide variety of parameters. Typical parameters for classifying networks include: Transmission medium, functional relationship (network architecture), Network topology and the geographical area they cover (geographical scalability).

2.2.1 Transmission Medium Classification of Computer Networks

Computer networks can be classified according to the hardware technology (medium of transmission) that is used to connect the individual devices in the network. Two major categories exist: wired and wireless networks. Wired transmission media include Optical fibre and Ethernet (twisted pair and co-axial) connection cables. A wired network uses physical wiring to connect devices and is often deployed with devices such as hubs, switches, bridges and routers. Wireless networks are designed to connect devices to hubs, switches and routers without any visible cables. In wireless transmission, various types of electromagnetic waves are used to transmit signals. Radio transmissions, satellite transmissions, visible light, infrared light, X-rays, and gamma rays are all examples of electromagnetic waves or electromagnetic radiation. In general, electromagnetic radiation is energy propagated through space and, indirectly through solid objects in form of advancing disturbance of electric & magnetic fields.

2.2.2 Functional Relationships Classification of Computer Networks

Computer Networks can be classified according to the functional relationships which exist among the elements of the network. Network types in this category include: Client-Server Networks and Peer-to-Peer Networks. In the client-server model, the server is a centralized system which connects several clients. The more simultaneous clients a server has, the more resources it needs. In a peer-to-peer network, two or more computers (called peers) pool their resources and communicate in a decentralized system. Peers are co-equal nodes in a non-hierarchical network.

2.2.3 Topology Classification of Computer Networks

Network topology is the study of the arrangement or mapping of the elements (links and nodes) of a network, especially the physical (real) and logical (virtual) interconnections between nodes. Computer

networks can be classified according to their local network topology. The basic network types are Bus, Star and Ring Topologies. Figure 2.2 gives a graphical illustration of these network types.

- **Bus Topology – Here, local computers share the same single bus or communication channel. The bus is simply a linear coaxial cable into which multiple devices or workstations tap. Connecting to the cable requires a simple device called a tap which is a passive device, as it does not alter the signal and does not require electricity to operate. On the workstation end of the cable is a network interface card. The network interface card (NIC) is an electronic device that allows the workstation to send and receive data on the network. When a device transmits on the bus, all other attached devices receive the transmission.**
- **Star Topology – End user computers in this network are tied to a central computer typically called the server which controlled the transmissions of all the other workstations.**
- **Ring Topology – In this topology, local computers are tied together in a ring and transmit data on an equal basis using tokens. This topology is capable of supporting only one channel of information which flows in one direction around the ring, moving from workstation to workstation. Because the ring is a closed loop of wire, it is important to remove any circling piece of data from the ring; otherwise, the piece of data will keep circling. The device that removes the data is the workstation that originally transmitted the data.**

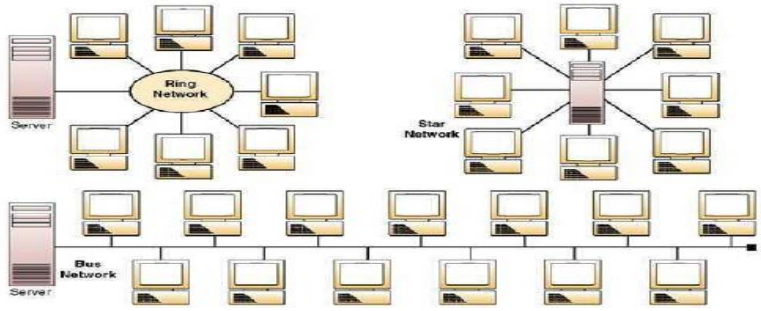

Fig. 2.2: Bus, Star and Ring Topology Networks

2.2.4 Geographical Scalability Classification of Computer Networks There are also different types of computer network in order of geographical scalability.

- **Personal Area Network - A personal area network (PAN) is a computer network used for communication among computer devices close to one person. Some examples of devices that are used in PAN are Printers, Fax machine, Telephones, PDAs (Pocket Digital Assistant) or scanners. The reach of a PAN is typically within about 20 to 30 feet (approximately 6 to 9 Metres). Personal area networks may be wired with computer buses such as USB (Universal Serial Bus) and Fire Wire. A Wireless Personal Area Network (WPAN) can be made possible with network technologies such as Infrared and Bluetooth.**
- **Local Area Network - A local area network (LAN) is a communications network that interconnects a variety of data communications devices within a small geographic area and broadcasts data at high data transfer rates. It covers a small geographic area like a home, office or building. Current LANs are typically based on the Ethernet technology. For example, a library may have a wired and a wireless LAN for users to interconnect local devices (e.g. printers and servers) and to connect to the internet. On wired LAN, PCs in the library are typically connected by some twisted pair cable (CAT 5 or CAT 6). The cables to the servers will use enhanced cable (CAT 5e or CAT 6e), which will support IEEE 802.3 standard at 1Gb/s. The wireless LAN may exist using a different IEEE protocol, 802.11b or 802.11g standard. The defining characteristics of LANs in contrast to WANs (Wide Area Networks) include their higher data transfer rates, smaller geographic range and lack of a need for leased telecommunication lines. Most LAN operates at a data rate of 10Mb/s to 100Mb/s. IEEE 802.3 LAN technologies operate at speeds up to 10Gb/s data transfer rate.**
- **Campus Area Network (CAN) - A network that connects two or more LANs but limited to a specific and contiguous geographical area such as a college campus, industrial complex or a military base is called a Campus Area Network (CAN). A CAN may be considered a type of MAN (Metropolitan Area Network), but it is generally limited to an area that is smaller than a MAN.**

- **Metropolitan Area Network (MAN) - A Metropolitan area network is network that connects two or more LANs or CANs together but does not extend beyond the boundaries of the immediate metropolis/town/city. Routers, switches and hubs are connected together to create a MAN.**
- **Wide Area Network- A Wide Area Network (WAN) is a data communication network that covers a relatively broad geographic area (i.e. one city to another and one country to another) and often uses transmission facilities provided by common carriers such as telephone companies.**

2.3 INTERNETWORK

Two or more networks or network segments connected using devices such as a router, is called an internetwork. Any interconnection among or between public, private, commercial or governmental networks may also be defined as an internetwork. In modern practice, the interconnected networks use the internet protocol. There are at least three variants of internetwork depending on who administers and who participates in them: Intranet, Extranet, and Internet. Intranet and Extranets may or may not have connections to the internet. If connected to the internet, the intranet or extranet is normally protected from being accessed from the internet without proper authorisation. The internet is not considered to be part of the intranet or extranet, although it may serve as a portal for access to portions of extranets.

2.3.1 Intranet

The Intranet is a set of interconnected networks, using the Internet Protocol (IP) and uses IP-based tools, such as web browsers and File Transfer Protocol (FTP) tools, under the control of a single administrative entity. That administrative entity closes the intranet to the rest of the world, and allows only specific users. Most commonly, an intranet is the internal network of a company or other enterprise. A large intranet will typically have its own web server to provide users with requested information.

2.3.2 Extranet

An Extranet is a network or internetwork that is limited in scope to a single organisation or entity but which also has limited connections to the networks of one or more other usually, but not necessarily, trusted organizations or entities. For example, a company's clients may be given access to some of its intranet creating in this way an extranet. Nevertheless simultaneously, the customers may not be considered 'trusted' from the standpoint of security. Technically, an extranet may also be categorised as a CAN, MAN, WAN or other type of network, although by definition, an extranet cannot consist of a single LAN; it must have at least one connection with an external network.

2.3.3 Internet

The collection of all networks (LAN, MAN, WAN etc) became known as the Internet. Today's present Internet is a vast collection of thousands of networks and their attached devices. The Internet began as the the Advanced Research Projects Agency NETworks (ARPANET) developed by the U.S. Department of Defence during the 1960s. One high-speed backbone connected several university, government, and research sites. The backbone was capable of supporting 56kbps transmission speeds and eventually became financed by the National Science Foundation (NSF). To support the Internet and all its services, many protocols are necessary. A protocol is a set of rules determining the format and transmission of data. These protocols include Internet Protocol (IP), Transmission Control Protocol (TCP), Address Resolution Protocol (ARP), Dynamic Host Configuration Protocol (DHCP) and Network Address Translation (NAT). Participants in the Internet use the IP suites and addresses allocated by address registries. Service providers and large enterprises exchange information about the reachability of their address ranges through the Border Gateway Protocol (BGP).

The Internet is home to the World Wide Web (WWW). WWW is a vast collection of electronic documents that are located on many different Web servers and contain text and images that can be accessed by simply clicking links within a browser's Web page. Using a Web browser, you can download and view Web pages on a personal computer. Of all the Internet services, the World Wide Web is

probably the one that has had the most profound impact on business. Internet retail sales and service support have exploded with the use of personal computers and Web browsers. Virtually any and every imaginable product and service is now sold on the Web. Web pages are created using HyperText Markup Language (HTML), which can be generated manually with a text-based editor such as Notepad, or through using a Web page authoring tool. Once you've created your Web page, you store it on a computer that contains Web server software and has a connection to the Internet. The Web server software accepts Hypertext Transfer Protocol (HTTP) requests from Web browsers connected to the Internet, retrieves a requested Web page from storage, and returns that Web page to the requesting computer via the Internet.

2.4 BASIC HARDWARE COMPONENTS USED IN NETWORKING

All computer networks are made up of basic hardware building blocks to interconnect network nodes. Examples of such hardware components include Network Interface Cards (NICs), Bridges, Hubs, Switches, Routers etc.

2.4.1 Network Interface Cards (NICs)

A network card, network adapter or Network Interface Card (NIC) is a piece of computer hardware designed to allow computers to communicate over a computer network. It provides physical access to a networking medium and often provides a low- level addressing system through the use of MAC (Media Access Control) addresses. It allows users to connect to each other either by using cables or wireless medium.

2.4.2 Bridges

A network bridge is a network device that connects multiple network segments. Network bridging describes the action taken by network equipment to allow two or more communication networks, or two or more network segments, to create an aggregate network. Bridging is distinct from routing (which allows the networks to communicate independently as separate networks). There are four types of network-bridging technologies: simple bridging, multiport bridging, learning or transparent bridging and source route bridging.

2.4.3 Hubs

A hub contains multiple ports. A port (interface) is computer circuit consisting of the hardware and associated circuitry that links one device with another. When a data packet arrives at one port, it is copied to all the ports of the hub for transmission. When the packets are copied, the destination address in the frame does not change to a broadcast address. It does this in a rudimentary way; it simply copies the data to all of the nodes connected to the hub.

2.4.4 Switches

A switch is a device that performs switching. Specifically, it forwards and filters chunks of transmitted data based on the MAC-addresses in the packet. This is distinct from a hub in that it only forwards the packet to the ports involved in the communications rather than all the ports connected. The switch normally has numerous ports with the intention that most or the entire network be connected directly to a switch or another switch that is in turn connected to a switch.

2.4.5 Routers

Routers are networking devices that forward data packets between networks using headers and forwarding tables to determine best path to forward the packets. Routers are mainly useful in connecting network segments together. The router is connected to at least two networks, commonly two LANs/ WANs or a LAN and its ISP's (Internet Service Provider's) network.

2.5 COMPUTER NETWORK SECURITY

Security in this context is the state of well being of information and infrastructure in which the possibility of successful yet undetected theft, tampering, and disruption of information and services is kept low or tolerable. Computer security can also be simply defined by some as the protection of computing systems and the data that they store or access. The principles of computer security thus arise from the kinds of threats intruders can impose. Some basic security threats in existing systems and protection mechanisms and techniques for ensuring security of a computer system will be discussed in this section.

The objective of network security includes protection of information and property from theft, corruption, or natural disaster, while allowing the information and property to remain accessible and productive to its intended users. Network security starts from authenticating any user, commonly (one factor authentication) with a username and a password. With two factors authentication, something you have is also used; e.g. a security token or 'dongle', an ATM card, or your mobile phone is added for extra security. Three factors authentication utilises something on your body; e.g. a fingerprint or retinal scan. Security management for networks might differ depending on the situation. A small home or an office would only require basic security while large businesses will require high maintenance and advance software/ hardware to prevent malicious attacks from hackers/ spammers.

Three basic security concepts important to information are confidentiality, integrity, and availability while concepts relating to the people who use that information are authentication, authorization, and non-repudiation. When information is read or copied by someone not authorized to do so, the result is known as loss of confidentiality. For some types of information, it is very important for there to be confidentiality. Examples include research data, medical and insurance records, new product specifications, corporate investment strategies etc. In some locations, there may be a legal obligation to protect the privacy of individuals. This is particularly true for banks and loan companies, debt collectors, businesses that extend credit to their customers or issue credit cards, hospitals, doctors, offices, medical testing laboratories, individuals or agencies that offer psychological counselling or drug treatment and agencies that collect taxes. Information can be corrupted when it is available on an insecure network. When information is modified in unexpected ways, the result is known as loss of integrity. This means that unauthorized changes are made to information, whether by human error or intentional tampering. Integrity is particularly important for critical safety and financial data used for activities such as electronic funds transfers, air traffic control and financial accounting.

2.6 Computer Viruses and Other Destructive Programs

Viruses and malwares are names given to all forms of destructive programs on computer systems.

2.6.1 Malware

Malware is a general name for all programs that are harmful to the computer system. These include viruses, Trojans, worms, and spyware. They are very important threats that must never be overlooked.

2.6.2 Computer Viruses

A Computer virus is a program which attaches itself to, overwrite or otherwise replace another program in order to reproduce itself without the knowledge of a PC user. Computer viruses can be categorised based on two distinct parameters: how they infect a PC and what they infect in a PC. All computer virus types have one thing in common; any virus has to be executed in order to operate. Most viruses are pretty harmless. The user might not even notice the virus for years. Sometimes viruses might cause random damage to data files and over a long period they might destroy files and disks.

2.6.3 Trojan Horses

This is a destructive program that has been disguised (or concealed in) an innocuous piece of software. Indeed, worm and virus programs may be concealed within a Trojan horse. Trojan horses are not viruses because they do not reproduce themselves and spread as viruses do. The name, Trojan horse, was coined from the Greek mythology of the Trojan War.

Trying to find a way into the city of Troy, the great warrior Odysseus ordered his men to build a massive wooden horse, one big enough for several Greek soldiers to fit in. Once the structure was finished, he and several other warriors climbed inside, while the rest of the Greek sailed away from Troy. One of the soldiers however stayed behind in order to deceive the Trojans (as the people of Troy were known), convincing them that his fellow Greeks had betrayed and fled from the city. The wooden horse, he told the Trojans, was safe and would bring them good luck. After some discussion over the matter, the Trojans agreed to wheel the horse through their gates, unknowingly giving the Greek enemy access to the city. After proclaiming victory and partying all night, citizens of troy went to sleep. It was then that Odysseus and his men crept out of the Trojan horse and wreaked havoc on the city.

The Trojan horse software works on the same principle. A program may seem both attractive and innocent inviting the computer user to copy (or download) the software and run it. Trojan horses may be games or some other software that the victim will be tempted to try.

Fig. 2.3 Graphical illustration of Trojan Horse

Trojan horses are common but dangerous programs that hide within other seemingly harmless programs. They work the same way the ancient Trojan horse did: Once they are installed, the program will infect other files throughout the system and potentially wreck havoc on that computer. They can even send important information from the computer over the internet to the developer of the virus. The developer can then essentially control that computer, slowing down its activities or causing it to crash.

Trojan Horses are usually more subtle, especially when they are used for embezzlement or industrial espionage. They can be programmed to self-destruct, leaving no evidence other than the damage they have caused. A Trojan horse is particularly effective for the common banking before any data could be damaged. When trying to access whether a computer system has fallen victim to a virus, logic bomb, worm or Trojan horse, the key factor is whether the maverick program has the ability to reproduce. Only viruses can make copies of them and attach the copy to new files.

2.6.4 Logic Bombs

Writing a logic bomb program is similar to creating a Trojan horse. Both also have about the same ability to damage data. Logic bombs include a timing device so it will go off at a particular date and time. The Michelangelo virus for example was embedded in a logic bomb. Other virus programs often include coding similar to that used in logic bombs, but the bombs can be very destructive on their own, even if they lack the ability of the virus to reproduce. Logic bombs are usually timed to do maximum damage. That means the logic bomb is a favoured device for revenge by disgruntled former employees who can set it to activate after they have left the company. One common trigger occurs when the dismissed employee's name is deleted from payroll records. Logic bombs can also be insurance for suppliers or consultants who set up a computer system, causing data to be destroyed if their bills are not paid.

2.6.5 Spyware

Spywares are a category of computer programs that attach themselves to the operating system in nefarious ways. They can suck the life out of a computer's processing power. They are designed to track a user's internet habits, nag the user with unwanted sales offers or generate traffic for their host Websites. According to some estimates, more than 80 percent of all personal computers are infected with some kind of spyware. Some people mistake spywares for a computer virus. A computer virus is a piece of code designed to replicate itself as many times as possible, spreading from one host computer to any other computer connected to it.

Fig. 2.4 Graphical illustration of Spyware

Spywares are usually not designed to damage the infected computer. They get into computers without the users permission and hide in the background while they make unwanted changes to the user's experience. Their main mission in computer systems is to serve users with targeted advertisements or make their browsers display certain sites or search results.

2.6.6 Worms

A worm is a program which spreads usually over network connections. Unlike a virus which attaches itself to a host program, worms always need a host program to spread. In practice, worms are not normally associated with one person computer systems. They are mostly found in multi-user systems.

2.7 COUNTER MEASURES FOR PREVENTING NETWORK THREATS

The following are possible strategies for preventing threats to Computer networks.

2.7.1 FIREWALL

A component or a set of components that restricts access between protected network and the Internet or between other sets of networks is called a Firewall. Firewalls can be used to protect computer networks from offensive websites and potential hackers. Fig 2.5 below illustrates the concept of firewall.

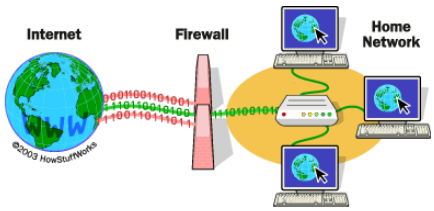

Fig. 2.5 Graphical illustration of Firewall

Basically, a firewall is a barrier to keep destructive forces away. That is why it is called a firewall. Its job is similar to a physical firewall that keeps a fire from spreading from one area to the next. Firewalls come in both hardware and software varieties.

2.7.2 ANTI-VIRUS

To guard and protect a computer from known viruses and other destructive programs, antivirus software must be installed and made to run actively on it. The software must also be updated from time to time. New viruses are discovered almost daily. Running antivirus software that has not been updated in a month or more is equivalent to not running antivirus software at all. The antivirus vendors analyze new malicious code threats as they are discovered. They look for pertinent information that makes the threat unique such as size of the file, specific text in the file, message body or subject line and specific ways the file works. They then create a signature or footprint that will identify this threat. These signatures are included in the update files put out by the antivirus vendors. Most vendors update their virus definitions at least weekly. There are many products available on the market to help protect computers from viruses. McAfee ViruScan from Network Associates and Norton Antivirus from Symantec are two of the most recognised names in antivirus software. There are plenty of other options though such as Sophos or F-Secure as well as free options such as Avira, Antivir, AVG for those who want to protect their computers on a tight or non-existent budget.