Unit 8: Multimedia and Computer Security

Introduction to Multimedia:

- Newspaper and television are the common medium of mass communication. However, they differ in the way they present information to the user.
- The information in a newspaper is presented as a combination of text, image, and graphics. This has a different impact on the user than the information presented on the television as a combination of image, photo, video, sound and music.
- Similarly, talking over a telephone (using sound) has a different impact on the user, than, talking using the Internet telephone with a web camera (sound and photo) attached to it.
- In other words, the same information when presented using different media has a different impact on the user. Or, we can say that the media used for presenting the information affects the way the user perceives and understands the information.
- Multimedia is a combination of graphics, audio, text, animation, and video using the computer.

Multimedia-Definition:

- The word multimedia consists of two words—multi and media. The word multi means many and the word media (plural of medium) are the means through which information is shared.
- Multimedia is the field concerned with the computer-controlled integration of text, graphics, drawings, still and moving images (Video), animation, audio, and any other media where every type of information can be represented, stored, transmitted and processed digitally.
- A Multimedia Application is an Application which uses a collection of multiple media sources e.g. text, graphics, images, sound/audio, animation and/or video.
- Newspaper, radio, television and films are some of the earliest and traditional means of mass communication that use mass media.
- In these traditional means of communication, the communication is one-way—from the media to the mass users. The user simply reads the newspaper, listens to the radio, and watches the television and films, and, cannot in any way manipulate the media. Mass media is used by the user in a sequence, linearly. For example, a text book consists of a sequence of combination of text, graphics, and images. The text book is meant to be read linearly from the start to the end. With mass media, the user is in a passive state (receiving whatever is communicated).
- Multimedia is delivered through the computer and microprocessor-based devices, thereby introducing the elements of interactivity, which differentiates it from the traditional forms of media (also called mass media).
- Multimedia or Interactive multimedia allows the user and the multimedia application to respond to each other. The user is able to control the elements of the multimedia application in terms of what elements will be delivered and when. Since multimedia systems are integrated with computers, they are also referred to as the digital multimedia system.

Characteristics of Multimedia System

A multimedia system has four basic characteristics:

- Computer is an intrinsic part of the multimedia system. As a result, multimedia has become interactive. In multimedia, computer allows the user to interact with the media and thus manipulate it by controlling what is to be communicated and when. Multimedia has resulted in the creation of many new possibilities—(1) the computational power of computer is utilized for multimedia applications, (2) the telecommunication network (Internet, WWW) along with the computer enables transmission and distribution of information, and, (3) the use of computer facilitates design and creation of a variety of new applications.

- The different elements of multimedia are combined and integrated into a single multimedia system. Special software is required for the integration of different media element files.
- The use of computer in multimedia requires all elements of multimedia to be in digital format. In a digital multimedia system, the media streams are digital and are produced, processed, stored, represented and transmitted using computers. The digital nature of multimedia requires special treatment of the multimedia elements. The hardware and software are needed to convert multimedia elements from analog to digital format and vice versa. There is a need to decide about the resolution versus quality of output required, during storing of data in the computer. Storing multimedia files on computer hard disk takes large amount of disk space, so compression technologies and file formats for storing the different media elements is required. Moreover, special programs are required to play the compressed files. Similarly, special software is required to edit the different media element files, and to combine and integrate the different elements of the multimedia into a single multimedia system.
- Multimedia system is interactive. The user is active and can manipulate whatever is being communicated. Multimedia allows two-way communication. The user can use devices like keyboard, trackball or joystick to interact with the multimedia system. Interactive multimedia is non-linear. The user is able to follow the links and jump from one part of the document to the other. Hypermedia enables a user to gain or provide access to text, audio and video, and computer graphics using links in a non-linear way, using computers. World Wide Web (WWW) is an example of hypermedia application. The user is able to respond and control what to see or hear and when to do it.

Elements of Multimedia

A multimedia system consists of several elements like—text, graphics, sound, video, and animation. The data streams of these different elements of the multimedia system are of two kinds—time-dependent, and time-independent. Media like text, graphics, and image are time independent. The information is not dependent on the timing of the data stream when using these media. However, media like audio, video, and animation are time-dependent. In time-dependent media, the data streams must appear at regular time intervals for the purposes of continuity.

The different media elements are described briefly in the following subsections.

Text

- Text is an important element of multimedia. The purpose of using text is to write titles, to define menus, to navigate, and to write the content.
- The text in multimedia is different from the traditional text written using paper and pen. Multimedia text is combined with other elements like graphics and pictures to deliver a powerful effect. Multimedia text can be written in a way that the user needs to jump back and forth, written in multiple channels like pictures, sound, animation, and colored text.

- The text must be short and relevant wherever used. Text is often mixed with art resulting in a much greater impact on the user. Text can also be animated. Text has evolved from being displayed in one size and one color under MS-DOS, to being specified using fonts and color on a color monitor having Windows, to the vector-based text by Adobe which uses graphics-based fonts and creates images.
- Text Font—The text can be written in different fonts: A font is composed of three things—typeface, style and size. Arial, Courier, Times are typefaces. Bold and italics are styles. Size is the length of the character (from top to bottom). Arial 11-point italic is a font.
- Text effects allow special effects to be added to text fonts by adding depth and visual impact (2D and 3D effects). Text effects can be created using MS-Word's WordArt. In WordArt, text is treated as a drawing object, i.e. text can be manipulated like an object. WordArt provides special effects to the text like, depth, direction, shape, color, and texture.
- Text animation can be used to make the text move, change or flash. MS-WORD and MS-Power-Point can be used for text animation.

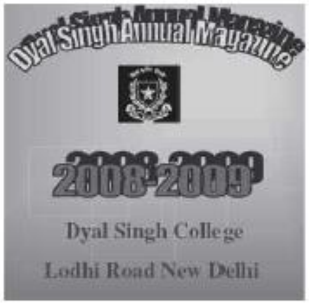

Figure 13.3 Using different text fonts

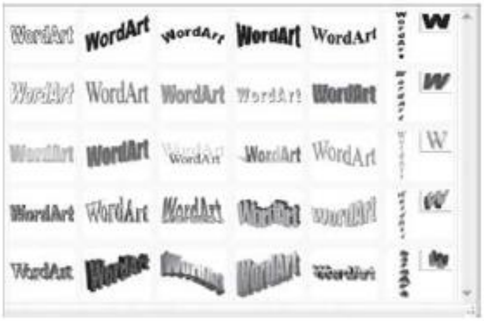

Figure 13.4 WordArt in MS-Word 2007

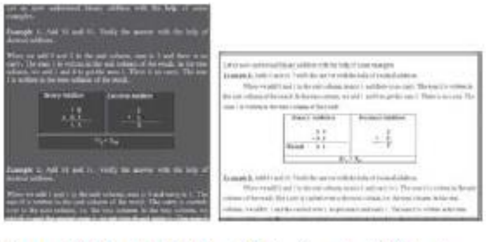

Figure 13.5 Text with different font colour, text effects etc.

- Text on the Internet can be represented as hypertext. A hypertext uses documents to be connected via hyperlink. Using hypertext, different documents can be linked and different parts of the same document can be linked. Hyperlinks allow the user to navigate the document in a non-linear way.

Graphics

- Communication via pictures is easier to understand. Graphics is the most important element of multimedia.
- Multimedia presentations are predominantly graphics-based.
- Graphics elements in a multimedia system are images that could be still pictures (like photographs) converted to digital format with the help of scanners, or pictures generated on the computer. They may be 2-dimensional such as photographs, or, 3-dimensional such as objects around us. They may be either static graphic elements or animated.
- In computer graphics, an image is always a digital image.
- Image Resolution: The resolution of an image is the number of pixels in the digital image relative to the physical size of the original material. Resolution is measured in dpi (dots per inch) and is applied to the image and also to the input and output devices used to scan or print the image. Resolution of monitor is generally, 72 pixels/inch. Higher the resolution, better is the picture.
- Image Color: There are two image color models—Red, Green, and Blue (RGB) model, and, Hue, Saturation, and Lightness (HSL) model. The three colors—red, green, and blue—give us quite a large spectrum by just adding colors. In HSL, the classification of the color circle rests upon three attributes of colors, called Hue, Brightness, and Saturation.
- Image File Size: The image that has been created has to be stored on the computer. The size of a digital graphic is the size of the graphics file on the computer. The size of graphic files is dependent on three things—(i) Dimension of the graphics is the physical size (maximum height and width in pixels), (ii) Bit-depth is the amount of color information stored in each pixel, and (iii) the compression used to store the image. The quality and size of the graphics file is dependent on the amount of compression used.
- Image Compression: Usage of compression technologies is important, especially, for graphics used on the Internet, since download time goes up drastically with increasing file size. While the image is compressed, the quality of the image must not suffer. Two image compression algorithms are widely used on the Internet—Joint Photographic Experts Group (JPEG) and Graphical Interchange Format (GIF).
    - JPEG compression works well with 24-bit color images (true color). It is suited for images that contain many colors (such as photographs).
    - GIF supports 8 bits of color information (Grayscale, Color map). GIF compression is suited to images such as line drawings, for images containing text, and cartoons containing at most 256 colors. It is preferred for vector graphics over the Internet.
    - jpg (for JPEG) and .gif (for GIF) are the most common file formats in use on the web. A relatively new file format—portable network graphic (.png), improves upon some of .gif features. Web browsers require plug-ins for .png.
- Image Capture: The graphic images on the computer can either be created using editors or can be loaded from the devices that capture the graphics images. Scanner, digital camera, digital video camera, and clip art are devices used for loading images on to the computer. Scanner looks like a photocopy machine and is used to copy an image to the computer. It converts an analog picture into digital format. Digital camera stores digitized images and digital video.

There are two types of digital graphics—bitmap graphics and vector graphics.

- In bitmap graphics, computer programs store pictures as pixel maps (bit-maps or raster images). The monitor is divided into a grid of pixels (short form of picture elements). Screen area of 800 × 600 pixels is common on Windows platform. Each pixel contains value representing a particular color. When a picture is sent to the screen, a graphics driver converts the picture data to pixel values on the display.
- Vector graphics uses various mathematical tracks to create graphics. It uses mathematical equations for the representation of the location, size, color fill, pattern fill etc. Vector graphics is suited for graphic images that require frequent re-sizing (small or enlarge), and repositioning.

Audio:

- Sound consists of all possible sounds which may or may not be audible to humans. Audio consists of the sound humans can hear. For example, the sound emitted by the dog-whistle is heard by dogs but not by humans. The presence of sound enhances the effect of a graphic presentation, video or animation.
- In a multimedia project, sound can be used in many ways. It can be used to provide audio content in a multimedia system such as, narration for a clip playing on the screen; audio sound tracks in movies; short instructions; or, music to communicate as in a song. Sound can also be used in the background and for sound effects.
- Sound is produced through vibrations and pressure variations in the air. The vibrations generate a waveform repeated at regular intervals (periods).

Properties of Sound

- Amplitude measures the relative loudness or volume of the sound. It is measured in decibels.
- Frequency or pitch is the vibrations per second. If an object vibrates rapidly, it creates a high-pitched sound. A low-pitch sound is produced by an object that vibrates slowly. The unit of frequency is hertz (Hz). The human ear can hear frequencies in the range of 20Hz to 20 kHz.
- Bandwidth is the difference between the highest and the lowest frequency contained in a sound signal. A signal with frequency range of 200 Hz to 3,200 Hz, has a bandwidth of 3,000 Hz (= 3,200−200).

Digital Audio—Audio is analog in nature and is a continuous waveform. Also, acoustic instruments produce analog sounds. A computer needs to transfer the analog sound waves into its digital representation consisting of discrete numbers. Representation of a waveform in a digital way is made by an Analog-to-Digital Converter (ADC). The reverse process is called Digital-to-Analog Conversion (DAC).

Sound Hardware—Microphone and Speakers are the devices connected to the ADC and DAC, respectively. A microphone converts the sound waves into electrical signals. This signal is amplified, filtered, and sent to ADC. This information is then retrieved and edited using a computer. To convert this data into sound waves, the audio data is sent to the speakers via a DAC and a reconstruction filter. This produces the analog sound waves that human beings can hear.

Sound Sampling—is a process that converts the analog signal into a digital format. Sound sampling transfers a continuous sound wave into discrete numbers. The rate at which the continuous waveform is sampled is called the sampling rate. The rate varies from 5,000–90,000 samples/ second. Sampling rate is an important factor in determining how accurately the digitized sound represents the original analog sound. E.g. CD (Compact Disk) sampling rate is 44.1 kHz (44,100 samples/sec) and telephone quality audio is sampled at 8 kHz.

Sound Digitization—is the process of assigning a discrete value to each of the sampled values. It is performed by an ADC. Recording at high sampling rates produces a more accurate capture of the high-frequency content of the sound. Along with the sampling rate, the resolution determines the accuracy with which the sound is digitized. The increase in the number of bits in a recording makes the sound playback increasingly realistic. Sound formats are standard in most audio editing software. Sampling rates of 8, 11, 22, and 44 kHz are normally used. There is no loss of quality when reproducing digital audio.

Music and Speech—Digital audio (music and speech) can be created or synthesized using the computer. Synthesized sounds are a set of instructions to the hardware audio device on how and when to produce sound.

- Musical Instrument Digital Interface (MIDI) format is the most widely used digital format for generating synthesized sound. In MIDI, the actual data is not recorded. MIDI works by recording the keys depressed, time when the key was depressed, duration for which the key was depressed, and how hard the key was struck. Almost all software that support audio can play MIDI files.
- Speech is the natural form of human communication. Speech is time-bound, dynamic, and transient. Distortion and noise are some of the speech effects.

Audio File Formats—The audio is stored on the computer as an audio file. Some commonly used audio file formats are—Resource Interleave File Format (RIFF) saved with extension (.wav), Motion Picture Experts Group (MPEG) as (mpg, mp2, mp3), or MIDI as (.mid, midi).

Audio Editors—Audio editors are used to record or manipulate audio files. The editors require a sound card to be installed on the computer. The editors allow the user to perform functions like copy and paste, and, concatenate, append, or mix two or more audio files. Sound effects can be incorporated in audio files using audio editors. Some common audio editing software for Windows are—Cool Edit, Sound Forge XP, Audacity, and Wave Flow.

Audio Compression—Compression is used to reduce the physical size of data so that it occupies less storage space and memory. Compressed audio files are easier and faster to transfer (small size), and also reduces bandwidth utilization thus providing good sound quality. Since applications exchange audio data using networks, standards like International Consultative Committee for Telephone and Telegraph (CCITT), International Standard Organization (ISO), and MPEG are used to achieve the compatibility. The most commonly used compression scheme for audio is MPEG. MPEG audio coding can compress the original audio on a CD by a factor of 12 without losing the sound quality. Audio files are often encoded in Mp3 (compression ratio is 1:10–1:12) as it is the most preferred format for PC and Internet applications.

Selecting a Quality Audio—The choice of sampling rate and compression for an audio depends upon its use. Sound that is to be embedded on a web page and downloaded over the Internet uses a low or medium sampling rate with compression. For recording a song on a CD, the highest sampling rate of 44.1 kHz is used.

Video:

Video is another element of multimedia. Video and audio are closely related, and together they are the most effective means of communication that can be a part of the multimedia system. Digital video is used in making of movies, gaming, and IT industry. The Digital Video Disk (DVD) makes it possible to distribute large videos in a compact form.

- Analog and Digital Video—Digital video allows random access within a movie; cut, paste, or edit video; and addition of special effects. It is easy to duplicate digital video without loss of quality. Digital video also allows for interactivity. The video seen on TV, cable TV, or VCR is broadcast in analog format.
- Video Editing—Digital video is easy to edit. Editing involves removing frames, inserting frames, mixing audio with video, creating special effects on video, superimposing clips, adjusting transparency, and adjusting volume of audio. Some of the software packages that support editing are Adobe Premiere, Adobe AfterEffects CS4 and Strata Avid Video.
- Digitizing Analog Video—The process of digitizing analog video is called video capture. Video is captured using plug-in cards called video capture cards. A video capture card accepts a video input from an input device such as a VCR or a video camera. The audio is sampled through a separate cable which attaches to the sound card. The software with the video card synchronizes the two channels of audio and video. With the software that comes with the video card, the video capture process is started. Digital cameras can directly store full-motion video in digital formats that can be copied onto a computer's hard disk.
- Video Compression—Digital video files are extremely large files that take a large amount of disk space, and require high data transfer rates from hard disk to screen. Compression restructures the data to reduce the size of the file. A compressed video file is decompressed when it is played. Several compression/decompression (codec) algorithms are available for compressing digital videos. Codecs may be asymmetric or symmetric; software-based, hardware-based, or both. A symmetric codec takes almost the same time to compress and decompress data. An asymmetric codec takes longer to encode video than it does to decode. Microsoft Video 1, Cinepak and Intel Indeo Video Raw are some of the Window-based codecs. Motion JPEG (MJPEG), MPEG-1, MPEG-2 are examples of the hardware-based codecs.
- Video File Formats—The digital video is saved on the disk in a video file format. The AVI format is used for the PC, and Quicktime format is used for Macintosh. The AVI format is used to play video in the Windows environment. It supports 256 colors to millions of colors, sound from 5 kHz Mono to CD quality stereo sound, and, can deliver video at rates ranging from 0.03 MB/sec to 0.3 MB/sec. Quicktime is similar to the AVI format, and can be viewed on almost every platform available.

Video on Internet

A video captured in real time from a live source is broadcasted using live camera web site. It takes video input from a video camera and compresses it to a size that can be delivered over the Internet. Streaming video and surround video are the technology that makes video on the Internet possible.

- Streaming Video—allows transmitting of real time video via the Internet, enabling a user to watch the video as it downloads. The video file takes a few seconds to load before starting the image. If the transmission slows down, the reserve of video available to the user's computer memory is used for uninterrupted viewing. VDOLive, RealVideo, Web Theater, and Stream Works are some of the streaming video products.
- Surround Video—allows the user to turn the image around in a Web page and interact with it from every angle. This is used for displaying products allowing the user to zoom in to any point and click on URL links.

Animation:

Animation is creating of an illusion of movement from a series of still drawings. To create a feeling of motion of an image (still drawing), the image is projected on the screen as frames. Generally, 30 frames per second are used to make the object appear to be in smooth motion on the screen.

- Process of Animation—requires four steps—(1) Story board layout defines the outline of the action and the motion sequence as a set of basic events, (2) Definition of objects defines the movement for each object, (3) Key frame specifications gives the detailed drawing of the scene of animation at a particular time, and (4) Generation of in-between frames defines the number of intermediate frames between key frames.
- Creation of Animation—Creation and usage of animation using the computer includes processes like looping, morphing, and rendering, which are briefly discussed below:
- Looping is the process of playing the animation continuously. It is used if the animation requires a basic few frames to be created. For example, a hop by a rabbit in 2–3 frames when put in a loop appears as if the rabbit is walking a long distance.
- Morphing means changing of shape. Morphing is the transformation of one image to another. Morphing requires two elements—the shape to be changed and the shape after change. Morphing is used to make the object appear as if it is physically changing its shape. Morphing is used to make an object appear to move, run, dance, expand, contract etc, giving a smooth transformation of the image from one state to another. Morphing with lines, and Point morphing are some processes of morphing.
- Rendering is the process to create an image from a data file. An animation requires about 30 renderings per second. Generally, a whole scene cannot be drawn by the 3-D graphics program inclusive of colors, shading etc. So, what is done is—a rough representation of the position of the object at each point in motion is provided to the rendering package. The rendering package generates the 30 frames required for the rendering which will result in the real motion of the object and thus animation. The rendering time is an important consideration in all 3-D animation.
- Hardware and Software for Animation—The hardware platforms used for animation are—SGI, PC, Macintosh, and Amiga. The SGI platform is used to broadcast quality computer animation productions. PCs use 3D Studio and Animator Studio applications for making animations. Some of the most popular software packages used for animation are—3D Studio Max, Light Wave 3D, Adobe Photoshop, Adobe Premiere, and Animator Studio.
- Animation File Formats—Animation can be in any of the following formats—Flic format (FLI/FLC), MPEG (.mpg), and Quicktime Movie. Flic format is used by 3D Studio and DOSbased graphics software packages. MPEG format is used on the Internet since it allows for a much faster file transfer because of its reduced file size. The file size is 40 times smaller than a Flic format file. The Quicktime Movie format is the standard Macintosh animation format, which allows for compression and can contain audio tracks.

Multimedia System:

The multimedia system includes the hardware and software components that are required to be used for multimedia. The hardware and software components required for a multimedia system are as follows:

- Input Devices—Keyboard and OCR for text; Digital cameras, Scanners and CD-ROM for graphics, MIDI keyboards, CD-ROM and microphones for sound; Video cameras, CD-ROM and frame grabbers for video; Mice, trackballs, joy sticks, virtual reality gloves and wands for spatial data; and mouse, touch screen, trackball, tablet, voice recognition system, infrared remotes, magnetic card encoder and reader, 3D input devices, and virtual reality devices.
- Output Devices—CD-quality speakers, Hi-resolution monitors, color printers, specialized helmets, and immersive devices displays for virtual reality, and video devices.
- Storage Devices—Hard disks, CD-ROM drive, Zip drive, DVD drive.
- Communication Network—Ethernet, Token Ring, Intranets, and Internets.
- Communication Devices—Modem, Network Interface Card.
- Computer System—Multimedia Desktop machine, Workstation, MPEG/VIDEO hardware
- Software—Some of the familiar tools for multimedia software are—Word Processor (MS-WORD, WordPerfect), Spreadsheet (MS-Excel), Database, and, Presentation Tools (MS-PowerPoint). Some of the software tools used for different elements of multimedia are as follows:
    - Music Sequencing and Notation—Cakewalk, Cubase, Macromedia Sound Edit
    - Digital Audio—Cool Edit, Sound Forge, Pro Tools
    - Image Editing—Adobe Illustrator, Adobe Photoshop, Macromedia Fireworks
    - Video Editing—Adobe Premiere, Windows Movie Maker, iMovie
    - Animation—3D Studio Max
- Multimedia Authoring Tools are programs that help the user in writing multimedia applications.

Desirable Features of Multimedia System

The hardware and software components used for a multimedia system have a minimum configuration to be used for multimedia. A multimedia system should have the following desirable features:

- Very high processing power—more than 500 MHz of processing speed.
- Large storage units (50 GB or more) and large memory (512 MB or more).
- Multimedia Capable File System to deliver real-time media e.g. video/audio streaming.
- File Formats that allow for compression/decompression in real-time.
- Efficient and fast I/O to allow for real-time recording and playback of data.
- Special operating system that supports direct transfer to disk, real-time scheduling, fast interrupt processing, and I/O streaming.
- Network Support for Internet.
- Software Tools to handle and deliver media, and, design and develop applications.

Multimedia Applications:

- Multimedia applications have found their way into different areas of our life.
- We are interacting with multimedia applications in the area of education where students and teachers use graphics, animation or video clips. PowerPoint presentations, drawings, laboratory works, resource sharing, e-learning etc. are some more applications.
- Multimedia for entertainment includes sports, laser shows, video games, or animation movies.
- Multimedia applications have found their way in business—may it be for advertising, marketing, video meetings, result presentations or customer feedbacks. Meetings are conducted using

multimedia applications like PowerPoint Presentations. Reports are generated along with graphics and images. Moreover, businesses use multimedia to market their products and to enlighten people about their products through the use of animations and videos. A CD giving details of the product is used. Car manufacturers, white-good manufacturers like television, microwave, refrigerators and washing machines, cell phone manufacturers etc., rely heavily on multimedia to display their product, market them, and to enhance sales of their product. Multimedia is also used by business organizations to train their people, for marketing and advertising, for creating visual and sound effects that are appealing to people, and thus making their product more saleable. Since the information inclusive of all sound and visual effects can be stored on a CD and distributed, it is considered as an inexpensive means of advertising and business promotion.

- Nowadays, training is also imparted using multimedia applications like simulations and 3D designs. Entertainment parks like Disneyland use virtual reality and multimedia, innovatively design, create, and improve; their games and rides.
- Virtual Reality is created using multimedia. Virtual reality is a special environment that is created using multimedia, where the users feel as if they are in a three-dimensional world. It gives the feeling to the users as if they are participating in the scenario.

Introduction to Computer Security:

- Computer security, also known as cybersecurity or IT security, is the protection of information systems from theft or damage to the hardware, the software, and to the information on them, as well as from disruption or misdirection of the services they provide.
- Computer security is needed to protect the computing system and to protect the data that they store and access. Transmission of data using network (Internet) and communication links has necessitated the need to protect the data during transmission over the network.
- Computer security focuses on the security attacks, security mechanisms and security services.
- Security attacks are the reasons for breach of security. Security attacks comprise of all actions that breaches the computer security.
- Security mechanisms are the tools that include the algorithms, protocols or devices, that are designed to detect, prevent, or recover from a security attack.
- Security services are the services that are provided by a system for a specific kind of protection to the system resources.
- The purpose of computer security is to provide reliable security services in the environments suffering security attacks, by using security mechanisms. The security services use one or more security mechanism(s).

Security Threat and Security Attack:

- A threat is a potential violation of security and causes harm. A threat can be a malicious program, a natural disaster or a thief.
- Vulnerability is a weakness of system that is left unprotected. Systems that are vulnerable are exposed to threats.

- Threat is a possible danger that might exploit vulnerability; the actions that cause it to occur are the security attacks.
- For example, if we leave the house lock open—it is vulnerable to theft; an intruder in our locality (might exploit the open lock) is a security threat; the intruder comes to know of the open lock and gets inside the house—This is a security attack.
- A security attack may be a passive attack or an active attack.
- The aim of a passive attack is to get information from the system but it does not affect the system resources. Passive attacks are similar to eavesdropping. Passive attacks may analyze the traffic to find the nature of communication that is taking place, or, release the contents of the message to a person other than the intended receiver of the message. Passive attacks are difficult to detect because they do not involve any alteration of the data. Thus, the emphasis in dealing with passive attacks is on prevention rather than detection.
- An active attack tries to alter the system resources or affect its operations. Active attack may modify the data or create a false data. An active attack may be a masquerade (an entity pretends to be someone else), replay (capture events and replay them), modification of messages, and denial of service. Active attacks are difficult to prevent. However, an attempt is made to detect an active attack and recover from them.

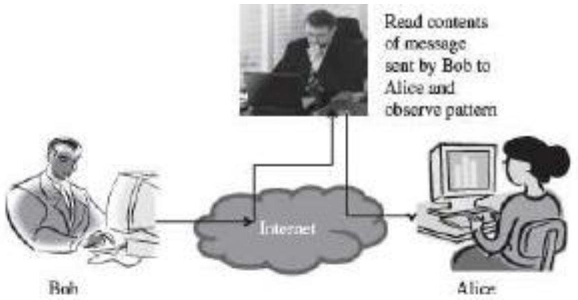
Read contents of message sent by Bob to Alice and observe pattern
Internet
Bob
Alice

Figure 14.1 Passive attack

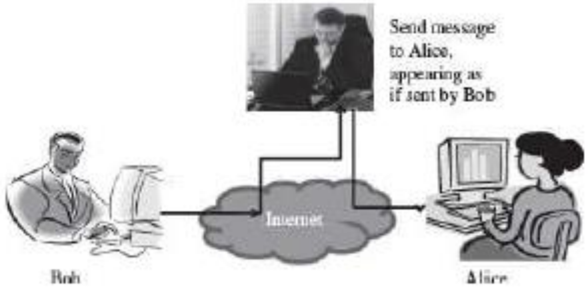

Figure 14.2 Active attack (masquerade)

- Security attacks can be on users, computer hardware and computer software.
- Attacks on users could be to the identity of user and to the privacy of user. Identity attacks result in someone else acting on your behalf by using personal information like password, PIN number in an ATM, credit card number, social security number etc. Attacks on the privacy of user involve tracking of user’s habits and actions—the website user visits, the buying habit of the user etc. Cookies and spam mails are used for attacking the privacy of users.
- Attacks on computer hardware could be due to a natural calamity like floods or earthquakes; due to power related problems like power fluctuations etc.; or by destructive actions of a burglar.

- Software attacks harm the data stored in the computer. Software attacks may be due to malicious software, or, due to hacking. Malicious software or malware is a software code included into the system with a purpose to harm the system. Hacking is intruding into another computer or network to perform an illegal act.

Malicious Software:

Malicious users use different methods to break into the systems. The software that is intentionally included into a system with the intention to harm the system is called malicious software. Viruses, Trojan horse, and Worms are examples of malicious programs.

Virus

Virus is a software program that is destructive in nature. Virus programs have the following properties:

- It can attach itself to other healthy programs.
- It can replicate itself and thus can spread across a network.
- It is difficult to trace a virus after it has spread across a network.
- Viruses harm the computer in many ways—
    - corrupt or delete data or files on the computer,
    - change the functionality of software applications,
    - use e-mail program to spread itself to other computers,
    - erase everything on the hard disk, or,
    - degrade performance of the system by utilizing resources such as memory or disk space.
- Virus infects an executable file or program. The virus executes when a program infected with virus is executed or you start a computer from a disk that has infected system files.
- Once a virus is active, it loads into the computer's memory and may save itself to the hard drive or copies itself to applications or system files on the disk.
- However, viruses cannot infect write protected disks or infect written documents. Viruses do not infect an already compressed file. Viruses also do not infect computer hardware; they only infect software.
- Viruses are most easily spread by attachments in e-mail messages. Viruses also spread through download on the Internet.

Worms

- Worm is self-replicating software that uses network and security holes to replicate itself.
- A copy of the worm scans the network for another machine that has a specific security hole.
- It copies itself to the new machine using the security hole, and then starts replicating from there, as well. A worm is however different from a virus.
- A worm does not modify a program like a virus, however, it replicates so much that it consumes the resources of the computer and makes it slow.

Trojan Horse

- Trojan horse is destructive programs that masquerade as useful programs.
- The name "Trojan horse" is given because of the Greek soldiers who reached the city of Troy by hiding themselves inside a large wooden horse. The people of the city of Troy themselves pulled

the horse inside their city, unaware of the fact that the Greek soldiers were hiding inside the horse.

- Similarly, users install Trojan horses thinking that it will serve a useful purpose such as a game or provide entertainment.
- However, Trojan horses contain programs that corrupt the data or damage the files. Trojan horses can corrupt software applications. They can also damage files and can contain viruses that destroy and corrupt data and programs. Trojan horse does not replicate themselves like viruses.

Security Services:

The security services provide specific kind of protection to system resources. Security services ensure Confidentiality, Integrity, Authentication, and Non-Repudiation of data or message stored on the computer, or when transmitted over the network. Additionally, it provides assurance for access control and availability of resources to its authorized users.

- Confidentiality—The confidentiality aspect specifies availability of information to only authorized users. In other words, it is the protection of data from unauthorized disclosure. It requires ensuring the privacy of data stored on a server or transmitted via a network, from being intercepted or stolen by unauthorized users. Data encryption stores or transmits data, in a form that unauthorized users cannot understand. Data encryption is used for ensuring confidentiality.
- Integrity—It assures that the received data is exactly as sent by the sender, i.e. the data has not been modified, duplicated, reordered, inserted or deleted before reaching the intended recipient. The data received is the one actually sent and is not modified in transit.
- Authentication—Authentication is the process of ensuring and confirming the identity of the user before revealing any information to the user. Authentication provides confidence in the identity of the user or the entity connected. It also assures that the source of the received data is as claimed. Authentication is facilitated by the use of username and password, smart cards, biometric methods like retina scanning and fingerprints.
- Non-Repudiation prevents either sender or receiver from denying a transmitted message. For a message that is transmitted, proofs are available that the message was sent by the alleged sender and the message was received by the intended recipient. For example, if a sender places an order for a certain product to be purchased in a particular quantity, the receiver knows that it came from a specified sender. Non-repudiation deals with signatures.
- Access Control—It is the prevention of unauthorized use of a resource. This specifies the users who can have access to the resource, and what are the users permitted to do once access is allowed.
- Availability—It assures that the data and resources requested by authorized users are available to them when requested.

Security Mechanisms:

Security mechanisms deal with prevention, detection, and recovery from a security attack. Prevention involves mechanisms to prevent the computer from being damaged. Detection requires mechanisms that allow detection of when, how, and by whom an attacked occurred. Recovery involves mechanism to stop the attack, assess the damage done, and then repair the damage.

Security mechanisms are built using personnel and technology.

- Personnel are used to frame security policy and procedures, and for training and awareness.
- Security mechanisms use technologies like cryptography, digital signature, firewall, user identification and authentication, and other measures like intrusion detection, virus protection, and, data and information backup, as countermeasures for security attack.

Cryptography:

Cryptography is the science of writing information in a “hidden” or “secret” form and is an ancient art. Cryptography is necessary when communicating data over any network, particularly the Internet. It protects the data in transit and also the data stored on the disk. Some terms commonly used in cryptography are:

- Plaintext is the original message that is an input, i.e. unencrypted data.
- Cipher and Code—Cipher is a bit-by-bit or character-by-character transformation without regard to the meaning of the message. Code replaces one word with another word or symbol. Codes are not used any more.
- Cipher text—It is the coded message or the encrypted data.
- Encryption—It is the process of converting plaintext to cipher text, using an encryption algorithm.
- Decryption—It is the reverse of encryption, i.e. converting cipher text to plaintext, using a decryption algorithm.

Cryptography uses different schemes for the encryption of data. These schemes constitute a pair of algorithms which creates the encryption and decryption, and a key.

Key is a secret parameter (string of bits) for a specific message exchange context. Keys are important, as algorithms without keys are not useful. The encrypted data cannot be accessed without the appropriate key. The size of key is also important. The larger the key, the harder it is to crack a block of encrypted data. The algorithms differ based on the number of keys that are used for encryption and decryption. The three cryptographic schemes are as follows:

- Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption,
- Public Key Cryptography (PKC): Uses one key for encryption and another for decryption,
- Hash Functions: Uses a mathematical transformation to irreversibly encrypt information.

<u>Secret Key Cryptography</u>

- Secret key cryptography uses a single key for both encryption and decryption. The sender uses the key to encrypt the plaintext and sends the cipher text to the receiver. The receiver applies the same key to decrypt the message and recover the plaintext. Since a single key is used for encryption and decryption, secret key cryptography is also called symmetric encryption.

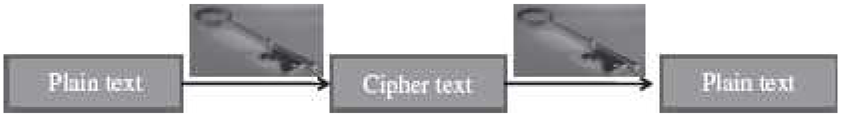

Fig: Secret key cryptography (uses a single key for both encryption and decryption)

- Secret key cryptography scheme is generally categorized as stream ciphers or block ciphers.
- Stream ciphers operate on a single bit (byte or computer word) at a time and implement some form of feedback mechanism so that the key is constantly changing.
- Block cipher encrypts one block of data at a time using the same key on each block. In general, the same plaintext block will always encrypt to the same cipher text when using a same key in a block cipher.
- Secret key cryptography requires that the key must be known to both the sender and the receiver. The drawback of using this approach is the distribution of the key. Any person who has the key can use it to decrypt a message. So, the key must be sent securely to the receiver, which is a problem if the receiver and the sender are at different physical locations.
- Data Encryption Standard (DES) and Advanced Encryption Standard (AES) are some of the secret key cryptography algorithms that are in use nowadays.

Public-Key Cryptography

- Public-key cryptography facilitates secure communication over a non-secure communication channel without having to share a secret key.
- Public-key cryptography uses two keys—one public key and one private key.
- The public key can be shared freely and may be known publicly.
- The private key is never revealed to anyone and is kept secret.
- The two keys are mathematically related although knowledge of one key does not allow someone to easily determine the other key.

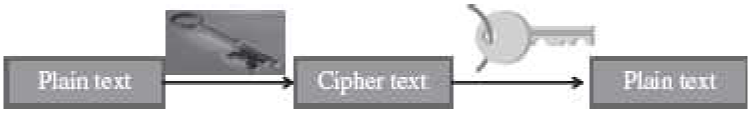

Fig: Public key cryptography (uses two keys—one for encryption and other for decryption)

- The plaintext can be encrypted using the public key and decrypted with the private key and conversely the plaintext can be encrypted with the private key and decrypted with the public key. Both keys are required for the process to work. Because a pair of keys is required for encryption and decryption; public-key cryptography is also called asymmetric encryption.
- Rivest, Shamir, Adleman (RSA) is the first and the most common public-key cryptography algorithm in use today. It is used in several software products for key exchange, digital signatures, or encryption of small blocks of data.
- The Digital Signature Algorithm (DSA) is used to provide digital signature capability for the authentication of messages.

Hash Functions

- Hash functions are one-way encryption algorithms that, in some sense, use no key. This scheme computes a fixed-length hash value based upon the plaintext. Once a hash function is used, it is difficult to recover the contents or length of the plaintext.

Hash function
Plain text
Cipher text

Fig: Hash function (have no key since plain text is not recoverable from cipher text)

- Hash functions are generally used to ensure that the file has not been altered by an intruder or virus. Any change made to the contents of a message will result in the receiver calculating a different hash value than the one placed in the transmission by the sender.
- Hash functions are commonly employed by many operating systems to encrypt passwords.
- Message Digest (MD) algorithm and Secure Hash Algorithm (SHA) are some of the commonly used hash algorithms.

The different cryptographic schemes are often used in combination for a secure transmission. Cryptography is used in applications like, security of ATM cards, computer passwords, and electronic commerce. Cryptography is used to protect data from theft or alteration, and also for user authentication.

Certification Authorities (CA) are necessary for widespread use of cryptography for e-commerce applications. CAs are trusted third parties that issue digital certificates for use by other parties. A CA issues digital certificates which contains a public key, a name, an expiration date, the name of authority that issued the certificate, a serial number, any policies describing how the certificate was issued, how the certificate may be used, the digital signature of the certificate issuer, and any other information.

Digital Signature:

- A signature on a legal, financial or any other document authenticates the document. A photocopy of that document does not count.
- For computerized documents, the conditions that a signed document must hold are—
  (1) The receiver is able to verify the sender (as claimed),
  (2) The sender cannot later repudiate the contents of the message,
  (3) The receiver cannot generate the message himself.
- A digital signature is used to sign a computerized document. The properties of a digital signature are same as that of ordinary signature on a paper. Digital signatures are easy for a user to produce, but difficult for anyone else to forge.
- Digital signatures can be permanently tied to the content of the message being signed and then cannot be moved from one document to another, as such an attempt will be detectable.
- Digital signature scheme is a type of asymmetric cryptography. Digital signatures use the public key cryptography, which employs two keys—private key and public key.
- The digital signature scheme typically consists of three algorithms:
  - Key generation algorithm—The algorithm outputs private key and a corresponding public key.
  - Signing algorithm—It takes, message + private key, as input, and, outputs a digital signature.
  - Signature verifying algorithm—It takes, message + public key + digital signature, as input, and, accepts or rejects digital signature.
- The use of digital signatures typically consists of two processes—Digital signature creation and Digital signature verification.

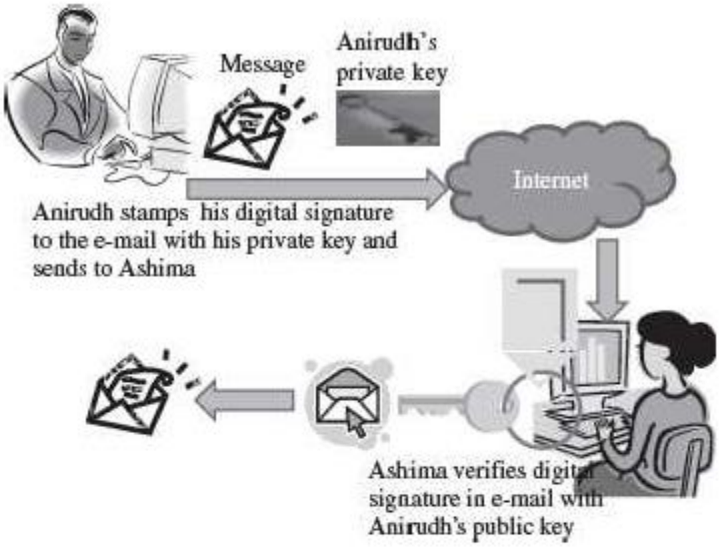
Message
Anirudh's private key
Internet
Anirudh stamps his digital signature to the e-mail with his private key and sends to Ashima
Ashima verifies digital signature in e-mail with Anirudh's public key

Fig: Digital signature

Firewall:

- A firewall is a security mechanism to protect a local network from the threats it may face while interacting with other networks (Internet).
- A firewall can be a hardware component, a software component, or a combination of both. It prevents computers in one network domain from communicating directly with other network domains. All communication takes place through the firewall, which examines all incoming data before allowing it to enter the local network.

<u>Functions of Firewall</u>

The main purpose of firewall is to protect computers of an organization (local network) from unauthorized access. Some of the basic functions of firewall are:

- Firewalls provide security by examining the incoming data packets and allowing them to enter the local network only if the conditions are met.
- Firewalls provide user authentication by verifying the username and password. This ensures that only authorized users have access to the local network.
- Firewalls can be used for hiding the structure and contents of a local network from external users..

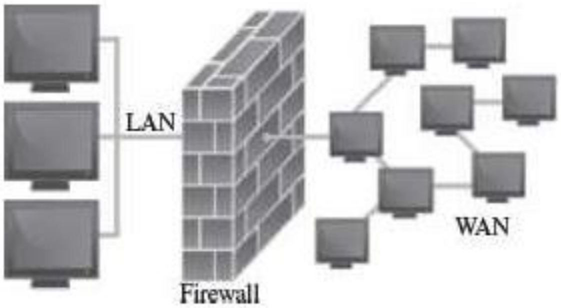

Fig: Firewall

Working of Firewall—The working of firewall is based on a filtering mechanism. The filtering mechanism keeps track of source address of data, destination address of data and contents of data. The filtering mechanism allows information to be passed to the Internet from a local network without any authentication. It makes sure that the downloading of information from the Internet to a local network happens based only on a request by an authorized user.

Firewall Related Terminology:

- Gateway—The computer that helps to establish a connection between two networks is called gateway. A firewall gateway is used for exchanging information between a local network and the Internet.
- Proxy Server—A proxy server masks the local network's IP address with the proxy server IP address, thus concealing the identity of local network from the external network. Web proxy and application-level gateway are some examples of proxy servers. A firewall can be deployed with the proxy for protecting the local network from external network.
- Screening Routers—They are special types of router with filters, which are used along with the various firewalls. Screening routers check the incoming and outgoing traffic based on the IP address, and ports.

Types of Firewall

All the data that enter a local network must come through a firewall. The type of firewall used varies from network to network. The following are the various types of firewalls generally used:

- Packet filter Firewall
- Circuit Filter Firewall
- Proxy server or Application-level Gateway

Packet Filter Firewall: Packet Filter Firewall is usually deployed on the routers. It is the simplest kind of mechanism used in firewall protection. The IP packet header is checked for the source and the destination IP addresses and the port combinations. After checking, the filtering rules are applied to the data packets for filtering. The filtering rules are set by an organization based on its security policies. If the packet is found valid, then it is allowed to enter or exit the local network. Packet filtering is fast, easy to use, simple and cost effective.

Circuit Filter Firewall: Circuit filter firewalls provide more protection than packet filter firewalls. Circuit filter firewall is also known as a "stateful inspection" firewall. It prevents transfer of suspected packets by checking them at the network layer. It checks for all the connections made to the local network, in contrast, to the packet filter firewall which makes a filtering decision based on individual packets. It takes its decision by checking all the packets that are passed through the network layer and using this information to generate a decision table. The circuit level filter uses these decisions tables to keep track of the connections that go through the firewall.

Application-Level Gateway: An application-level gateway or a proxy server protects all the client applications running on a local network from the Internet by using the firewall itself as the gateway. A proxy server creates a virtual connection between the source and the destination hosts. A proxy firewall operates on the application layer. The proxy ensures that a direct connection from an external computer to local network never takes place. The proxy automatically segregates all the packets depending upon the protocols used for them. A proxy server must support various protocols. It checks each application or service, like Telnet or e-mail, when they are passed through it. Application level gateways or proxy server tend to be more secure than packet filters. Instead of checking the TCP and IP combinations that are to be allowed, it checks the allowable applications.

Users Identification and Authentication:

- Identification is the process whereby a system recognizes a valid user's identity. Authentication is the process of verifying the claimed identity of a user.
- For example, a system uses user password for identification. The user enters his password for identification. Authentication is the system which verifies that the password is correct, and thus the user is a valid user.
- Before granting access to a system, the user's identity needs to be authenticated. If users are not properly authenticated then the system is potentially vulnerable to access by unauthorized users.
- If strong identification and authentication mechanisms are used, then the risk that unauthorized users will gain access to a system is significantly decreased.
- Authentication is done using one or more combinations of—what you have (like smartcards), what you know (Password), and what you are (Biometrics like Fingerprints, retina scans).

These are some authentication mechanisms:

- User name and password
- Smart Card
- Biometrics—Fingerprints, Iris/retina scan

Once the user is authenticated, the access controls for the user are also defined. Access controls is what the user can access once he is authenticated.

User Name and Password

The combination of username and password is the most common method of user identification and authentication. The systems that use password authentication first require the user to have a username and a password. Next time, when the user uses the system, user enters their username and password. The system checks the username and password by comparing it to the stored password for that username. If it matches, the user is authenticated and is granted access to the system.

Smart Card

A smart card is in a pocket-sized card with embedded integrated circuits which can process data. With an embedded microcontroller, smart cards have the unique ability to store large amounts of data, carry out their own on-card functions (e.g. encryption and mutual authentication) and interact intelligently with a smart card reader. A smart card inserted into a smart card reader makes a direct connection to a conductive contact plate on the surface of the card (typically gold plated). Transmission of commands, data, and card status takes place over these physical contact points. Smart cards are used in secure identity applications like employee-ID badges, citizen-ID documents, electronic passports, driver license and online authentication devices.

Biometric Techniques

Biometrics is the science and technology of measuring and statistically analyzing biological data. In information technology, biometrics refers to technologies that measures and analyzes human traits for authentication. This can include fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements, for authentication purposes.

For example, many mobile phones nowadays include a fingerprint scanner where you could place your index finger. The mobile device analyzes the fingerprint to determine your identity and authenticate you. Biometric systems are relatively costly and are used in environments requiring high-level security.

Intrusion Detection Systems

- An Intrusion Detection System (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. It is a software application that scans a network or a system for harmful activity or policy breaching.
- They complement firewalls to detect if internal assets are being hacked or exploited.
- Intrusion Detection Systems are classified into two major types: Network Based and Host Based Intrusion Detection System.
- Network Intrusion Detection System (NIDS): Network intrusion detection systems (NIDS) are set up at a planned point within the network to examine traffic from all devices on the network. It performs an observation of passing traffic on the entire subnet and matches the traffic that is passed on the subnets to the collection of known attacks. Once an attack is identified or abnormal behavior is observed, the alert can be sent to the administrator.
- Host Intrusion Detection System (HIDS): Host intrusion detection systems (HIDS) run on independent hosts or devices on the network. A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected. It takes a snapshot of existing system files and compares it with the previous snapshot. If the analytical system files were edited or deleted, an alert is sent to the administrator to investigate.

Security Awareness

- The aim of the security awareness is to enhance the security of the organization's resources by improving the awareness of the need to secure the system resources. Staff members play a critical role in protecting the integrity, confidentiality, and availability of IT systems and networks.
- It is necessary for an organization to train their staff for security awareness and accepted computer practices. Security of resources can be ensured when the people using it are aware of the need to secure their resources.
- Security awareness of staff includes the knowledge of practices that must be adhered to, for ensuring the security and the possible consequences of not using those security practices.
- For example, not disclosing your password to unauthorized users is a security practice, but if the users are not aware of the possible consequences of disclosing the password, they may disclose their password to other users, unintentionally, thus making their systems prone to security attack.
- In order to make the users and people in an organization aware of the security practices to be followed, regular training programs are conducted in organizations. Awareness is also promoted by regular security awareness sessions, videotapes, newsletters, posters, and flyers.

sec·U·R·I·T·y
You wouldn't share your toothbrush...
Don't share your PASSWORD!
YOU ARE IT!
THE UNIVERSITY OF ARIZONA, INFORMATION SECURITY OFFICE
security.arizona.edu

Fig: A security Awareness Poster

Security Policy

- A security policy is a formal statement that embodies the organization’s overall security expectations, goals, and objectives with regard to the organization’s technology, system and information.
- To be practical and implementable, policies must be defined by standards, guidelines, and procedures. Standards, guidelines, and procedures provide specific interpretation of policies and instruct users, customers, technicians, management, and others on how to implement the policies.
- The security policy states what is allowed, and what is not allowed. A security policy must be comprehensive, up-to-date, complete, delivered effectively, and available to all staff.
- A security policy must also be enforceable. To accomplish this, the security policy can mention that strict action will be taken against employees who violate it, like disclosing a password.
- Generally, security policies are included within a security plan. A security plan details how the rules put forward by the security policy will be implemented. The statements within a security plan can ensure that each employee knows the boundaries and the penalties of overstepping those boundaries. For example, some rules could be included in the security policy of an organization, such as, to log off the system before leaving the workstation, or not to share the password with other users.
- The security policy also includes physical security of the computers. Some of the measures taken to ensure the physical security of a computer are—taking regular backups to prevent data loss

from natural calamity, virus attack or theft, securing the backup media, keeping valuable hardware resources in locked room (like servers), to avoid theft of systems and storage media.

Steps in formulating a Security Policy:

- Analyzing Current Security Policies
- Identifying IT assets that need to be secure
- Identifying security threats and likely security attacks
- Defining Proactive (pre-attack) and Reactive (post-attack) security strategies

Importance of Security in Business:

- For many organizations, system and information is their most important asset, so protecting it is crucial.
- Security is “the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of system and information”.
- Information security performs four important roles:
    - Protects the organization’s ability to function.
    - Enables the safe operation of applications implemented on the organization’s IT systems.
    - Protects the data the organization collects and uses.
    - Safeguards the technology the organization uses.
- Implementing information security in an organization can protect the technology and information assets it uses by preventing, detecting and responding to threats, both internal and external.
- To support the information security strategy, it’s important to improve staff awareness of information security issues through training and initiatives. Organizations also need to enforce their information security policies and review them regularly in order to meet security requirements.
- A robust workplace security environment improves the efficiency and productivity of the company, which directly impact on the customer satisfaction and consequently the customer retention. This helps to increase the business revenue.