CHAPTER 7

INTERNET

For first stage

Written by

Assist. Prof. Dr. Abdullah A. Abdullah

2015-2016

Chapter VII

The internet: (INTER national NET work)

Is a network of computers around the world linked by Telecommunication network, the user can get a large amount of information about one subject

Fig: Internet World

The Internet is a global system of interconnected computer networks that use the standard Internet protocol suite (TCP/IP) to serve several billion users worldwide. It is a network of networks that consists of millions of private, public, academic, business, and government networks, of local to global scope, that are 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 of the World Wide Web (WWW), the infrastructure to support email, and peer-to-peer networks.

How to Connect to the Internet?

The Connect to the Internet wizard will guide you through the steps of setting up an Internet connection.

Open the Connect to the Internet wizard by clicking the Start button Picture of the Start button, clicking Control Panel, clicking Network and Internet, clicking Network and Sharing Center, clicking Set up a connection or network, and then clicking Connect to the Internet.

Note:
If you are connected to a local area network, you might already be connected to the Internet. To find out, open your web browser and try accessing a website.

What are you needed to connect to the Internet?

1. Personal computer
2. Modem
3. Telephone line
4. Internet & E – mail software
5. E – mail address
6. Account with the Internet service provider (ISP)

{{*You need an Internet service provider (ISP) and some hardware to connect to the Internet:*
ISP. An ISP provides access to the Internet. You sign up for an account with an ISP just as you do for telephone service or utilities.
Hardware. For a broadband connection such as Digital Subscriber Line (DSL) or cable, you need a DSL or cable modem. This is usually included as part of the start-up hardware from your ISP when you sign up for a broadband account. For a dial-up connection, you need a dial-up modem. Many computers come with this type of modem already installed.}}
Note:

An Internet Service Provider (ISP) is a company that provides you with access to the Internet, usually for a fee. The most common ways to connect to an ISP are by using a phone line (dial-up) or broadband connection (cable or DSL). Many ISPs provide additional services such as e‑mail accounts, web browsers, and space for you to create a website.
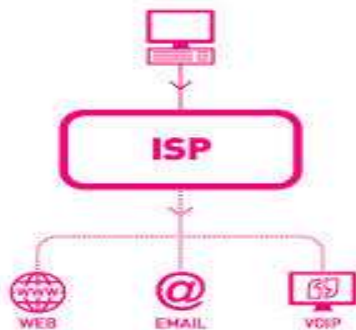

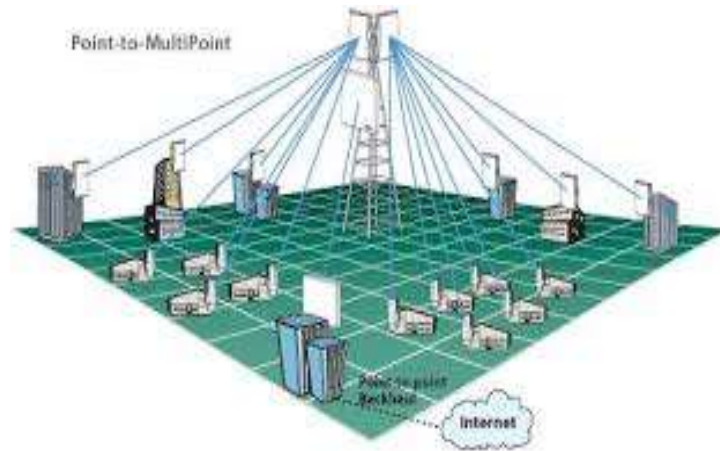
fig: (ISP) Internet Service Provider

Fig: Wireless (ISP).

Internet services:

1. **Search engines**: different programs with different methods that help you to find information on the Internet in seconds (Yahoo, Google, AltaVista). A web search engine is a software system that is designed to search for information on the World Wide Web. The search results are generally presented in a line of results often referred to as search engine results pages (SERPs). The information may be a specialist in web pages, images, information and other types of files.

Fig: Different kind of search engines.

2. Electronic mail (E – mail): is a program which enables you to transmit and receive message over the Internet.

Explain the definition E-Mail: Short for electronic mail, the transmission of messages over communications networks. The messages can be notes entered from the keyboard or electronic files stored on disk. Most mainframes, minicomputers, and computer networks have an e-mail system. Some electronic-mail systems are confined to a single computer system or network, but others have gateways to other computer systems, enabling users to send electronic mail anywhere in the world. Companies that are fully computerized make extensive use of e-mail because it is fast, flexible, and reliable.

Most e-mail systems include a rudimentary text editor for composing messages, but many allow you to edit your messages using any editor you want. You then send the message to the recipient by specifying the recipient's address. You can also send the same message to several users at once. This is called broadcasting.

Sent messages are stored in electronic mailboxes until the recipient fetches them. To see if you have any mail, you may have to check your electronic mailbox periodically, although many systems alert you when mail is received. After reading your mail, you can store it in a text file, forward it to other users, or delete it. Copies of memos can be printed out on a printer if you want a paper copy.
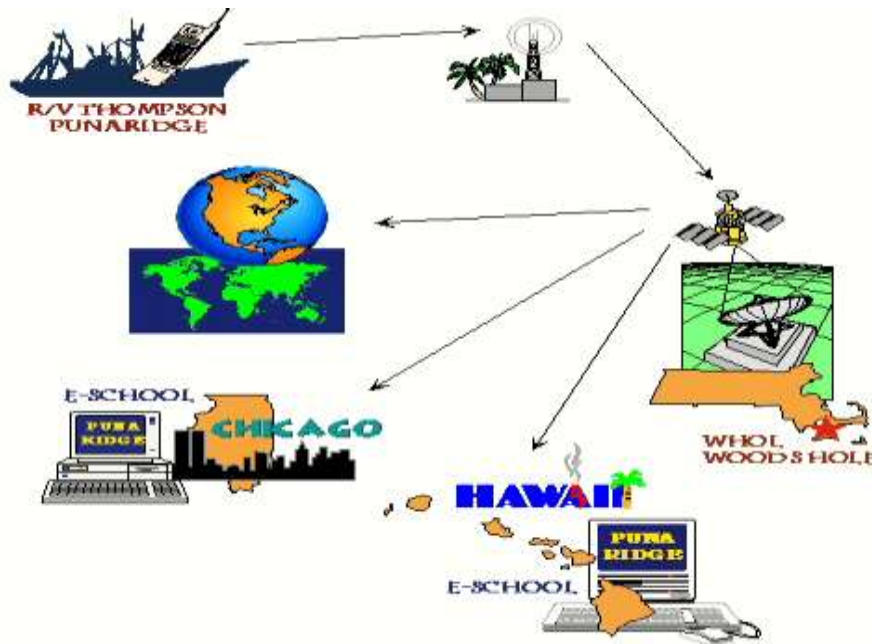
Fig show: e-mail.

Features of email
*Electronic mail or email is a means of sending messages, text, and computer files
between computers via the Internet.*
-automatic reply to messages
-auto forward and redirection of messages
-facility to send copies of a message to many people
-automatic filing and retrieval of messages
-addresses can be stored in an address book and retrieved instantly
-notification if a message cannot be delivered
-emails are automatically date and time stamped
-signatures can be attached
-files, graphics or sound can be sent as attachments, often in compressed formats
Webmail and mobile email can be used to receive and send messages while on the move
Using email
To send and receive email you must be connected to the Internet.
Dial-up users pay by the minute, so it makes sense for them to write their emails before
they connect to the Internet and to disconnect once they've received their new emails.
This saves money.
Broadband users pay a flat rate monthly subscription, the price they pay is not determined
by how long they're online.
Sending email
Open the email client, eg Microsoft Outlook, or if using webmail open a browser and
enter the webmail address, eg http://www.gmail.com and log in.
Click 'New' or 'Compose'.
Enter the intended recipient(s) email address(es) in the 'To' field.
Write a suitable subject in the 'Subject' field.
Write the message in the space below the Subject field.
Click 'Send' to send the email.
There's the option to add an attachment, eg a photo.
For security reasons, webmail users should log out once they're finished as the computer
they're using might be used by other people who, if they forgot to log out, would be able
to gain access to their email.
Receiving email
Email clients and webmail periodically check for new emails. A manual check can be
performed by clicking 'Send and Receive' in an email client or by refreshing the page
when using webmail.
Email clients download attachments automatically but webmail users must choose to
download attachments.
Email on other devices
Today email is not limited to computers. It can be sent from many other devices too, such
as:
mobile phones (using the carrier's network or a wireless hotspot).
games . TVs.
With wireless hotspots becoming increasingly common it's easier than ever to connect to
the Internet while on the move.

Advantages of E – mail via postal mail:
Almost free
Fast, low cost communication
Message can be sent to number of people at the same time
You can correspond with friend easily & quickly
You can forward message
You can replay message
Disadvantages:
You cannot send physical material
No privacy
E – mail may have viruses within it

Advantages and disadvantages of using email(in general)

Advantages
Emails are delivered extremely fast when compared to traditional post.
Emails can be sent 24 hours a day, 365 days a year.
Webmail means emails can be sent and received from any computer, anywhere in the world, that has an Internet connection.
Cheap - when using broadband, each email sent is effectively free. Dial-up users are charged at local call rates but it only takes a few seconds (for conventional email, eg text only) to send an email.
Emails can be sent to one person or several people.
Disadvantages
The recipient needs access to the Internet to receive email.
Viruses are easily spread via email attachments (most email providers scan emails for viruses on your behalf).
Phishing - sending an email to a user falsely claiming to be a legitimate company to scam the user into providing information, such as personal information and bank account numbers on a bogus website. The details will then be used for identity theft.
No guarantee the mail will be read until the user logs on and checks their email.
Spam - unsolicited email, i.e. junk mail.

Viruses

Software programs, which are written with the intention of causing serious damage in computer system. Flies on floppies can spread viruses, across a network or   **via** e– mail and the Internet.

What is a computer virus?

Computer viruses are small software programs that are designed to spread from one computer to another and to interfere with computer operation.

What do computer viruses do?

Through the course of using the Internet and your computer, you may have come in to contact with computer viruses. Many computer viruses are stopped before they can start, but there is still an ever growing concern as to what do computer viruses do and the list of common computer virus symptoms. A computer virus might corrupt or delete data on your computer, use your email program to spread itself to other computers, or even erase everything on your hard disk.

Computer viruses are often spread by attachments in email messages or instant messaging messages. That is why it is essential that you never open email attachments unless you know who it's from and you are expecting it.

Viruses can be disguised as attachments of funny images, greeting cards, or audio and video files.

Computer viruses also spread through downloads on the Internet. They can be hidden in illicit software or other files or programs you might download.

Protection from viruses: -

It is important to keep Anti – virus software up – to – date, if there is not any up- to – date anti – virus software installed into your computer, then you should follow these guide lines: -

1. Don't use floppies from unreliable source.
2. Use only registered software.
3. Never open E – mail attachment unless it from reliable source.

To help avoid computer viruses, it's essential that you keep your computer current with the latest updates and antivirus tools, stay informed about recent threats, run your computer as a standard user (not as administrator), and that you follow a few basic rules when you surf the Internet, download files, and open attachments.

Once a virus is on your computer, its type or the method it used to get there is not as important as removing it and preventing further infection.

How to remove and avoid viruses, spyware, and other malicious software

If you suspect your computer has been infected with a virus, spyware, or other malicious software, visit the Microsoft Windows website for step-by-step instructions for removing viruses and other malware.

Fortunately, if you update your computer and use antivirus software such as Microsoft Security Essentials, you can help permanently remove unwanted software and prevent installation in the first place.

Note: In Windows 8, Windows Defender replaces Microsoft Security Essentials. Windows Defender runs in the background and notifies you when you need to take specific action. However, you can use it anytime to scan for malware if your computer isn't working properly or if you clicked a suspicious link online or in an email message.

How do I know if my computer has been infected?

If you open and run an infected program or attachment on your computer, you might not realize that you've introduced a virus until you notice something isn't quite right.

Here are a few indicators that your computer might be infected:

-Your computer runs more slowly than normal

-Your computer stops responding or freezes often

-Your computer crashes and restarts every few minutes

-Your computer restarts on its own and then fails to run normally

-Applications on your computer don't work correctly

-Disks or disk drives are inaccessible

-You can't print correctly

-You see unusual error messages

-You see distorted menus and dialog boxes

These are common signs of infection—but they might also indicate hardware or software problems that have nothing to do with a virus. If you suspect that your computer has a virus, run the Microsoft Safety Scanner and install industry-standard, up-to-date antivirus software on your computer.

Tip: Beware of messages warning you that you've sent email that contained a virus. This can indicate that the virus has listed your email address as the sender of tainted email. This does not necessarily mean you have a virus. Some viruses have the ability to forge email addresses. In addition, there is a category of malware called rogue security software that works by causing fake virus alerts to pop up on your computer.

How do I install updates and antivirus software if I can't use my computer?
It might be difficult to download tools or update your computer if your computer has a virus. In this case, you can try one of the following options:

Use another computer to download the tools to a disk.

Get help through Microsoft support.

Try the Virus and Security Solution Center.

How can I prevent infection by computer viruses, spyware, and other malicious software?

Nothing can guarantee the security of your computer, but there's a lot you can do to help lower the chances that your computer will become infected.

Use a firewall

Using a firewall is like locking the front door to your house—it helps keep intruders (in this case, hackers and malicious software,) from getting in. Windows Firewall is included in Windows and is turned on by default.

Update your software

Microsoft releases security updates on the second Tuesday of every month. Visit Microsoft Update to confirm that you have automatic updating turned on and that you've downloaded and installed all the latest critical and security updates.

Adjust Internet Explorer security settings

You can adjust the security settings in your Internet Explorer web browser to specify how much—or how little—information you want to accept from a website.

Microsoft recommends that you set the security settings for the Internet zone to Medium or higher. (If you use Windows 8, Windows 7, Windows Vista, or Windows XP Service Pack 2 and you use Internet Explorer to browse the web, your browser security settings for the Internet zone are set to Medium by default.)

Internet Explorer also includes a number of features to help protect against viruses, spyware, and many other kinds of malicious, deceptive, or unwanted software.

Download and install antivirus software

Microsoft Security Essentials helps protects your computer from viruses, spyware, and other unwanted software. It's available as a no-cost download for Windows XP SP2 and higher, Windows Vista, and Windows 7.
Note: In Windows 8, Windows Defender replaces Microsoft Security Essentials. Windows Defender runs in the background and notifies you when you need to take specific action. However, you can use it anytime to scan for malware if your computer isn't working properly or if you clicked a suspicious link online or in an email message.

Surf and download more safely

The best defense against spyware and other unwanted software is not to download it in the first place. Here are a few helpful tips that can help you avoid downloading software that you don't want:

Only download programs from websites you trust. If you're not sure whether to trust a program you are considering downloading, enter the name of the program into your favorite search engine to see if anyone else has reported that it contains spyware.

Read all security warnings, license agreements, and privacy statements associated with any software you download.

Never click "Agree" or "OK" to close a window. Instead, click the red "x" in the corner of the window or press Alt + F4 on your keyboard to close a window.

Be wary of popular "free" music and movie file-sharing programs, and be sure you understand all of the software that is packaged with those programs.

Use a standard user account instead of an administrator account. For more information, see Why use a standard account instead of an administrator account?

It's crucial that you keep your antivirus software current with the latest updates (usually called definition files). These help the tool identify and remove the latest threats.

Type of Viruses:
There are six broad categories or types of computer viruses:
1. Boot Sector Virus
2. File Infection Virus
3. Multipartite Virus
4. Network Virus
5. E-mail Virus
6. Macro Virus

Boot Sector Viruses

Viruses that aim at the boot sector of a hard drive are infecting a very crucial component of the boot process. The boot sector holds critical information that controls the hard drive and also the part of the operating program that is in charge of the whole boot process. These types of computer viruses go a long way toward the assurance they will be successful in their mission by absolutely loading into the system memory while the boot cycle is starting.

Unlike other viruses the boot virus does not affect files, instead it goes after the drive itself on which the virus is saved and this is part of the reason that it is no longer as big a threat as it used to be. Since the advent of CD and DVD and the drives that carry them it is not possible to infect the programs that they carry. In the days of floppy drives the virus could spread quite quickly from computer to computer via the disks but since it is not possible to infect a CD or DVD this virus has become almost a non-threat. Another reason this types of computer viruses have become less common is that now operating systems stand guard over the boot sector and that makes it very hard for the virus to have any effect.

File Virus

File viruses are coded so that they will attach themselves to exe files, compressed files like zip files and driver files. The can be set into actions when the program they are attached to is started. Then after the virus is set into motion it will attach itself to other programs and system files and start along it's intended path for which it was written. So you see it is a two prong approach. First depending on the types of computer viruses it will duplicate and then go about its intended mission. The virus will search through the programs in the system and find places to infect with the code and then it will activate when that program is run next time. It will continue to duplicate

until it is all over the computer and probably any computer that is attached to the original system.

Often these viruses will harbor special code that causes them to be activated when certain events take place. The event often is a date or some other trigger event that is easily defined on any computer system you may have.

Multipartite Viruses

That which has been termed the multipartite virus are the types of computer viruses that are both a file virus and a boot sector virus. They enter the computer via various sorts of media and then embed themselves in the system memory. They then go into the hard drive and infect the boot sector. Once installed in the boot sector these types of computer viruses infect executable files and spread them in the system.

This is another virus that has past its prime for various reasons but in times past these types of computer viruses were responsible for many infections because they combined characteristics of two different viruses into one.

Network Viruses

A virus that is especially made for networks is uniquely created to quickly spread throughout the local area network and generally across the internet as well. Most of the time is moves within shared resources like drives and folders. Once it finds entry into a system it will search for vulnerable computers in the network and likewise infect that system and do the same again and again always on the hunt for new vulnerable systems.

E-Mail Viruses

Most of the time a e-mail virus is one of those types of computer viruses that is generally a macro virus and it will multiply itself by seeking out the other contacts in a e-mail address book and then send itself to those addresses in hopes that they will activate the virus too. Thus it spreads over and over again exponentially. There are even times an email virus can spread by only previewing it in the mail client. One that was very successful in spreading worldwide was the ILOVEYOU virus and it was destructive too.

14

Macro Viruses

Macro viruses as the name implies, will infect files of programs that use macros in the program itself. The most common of these are the Microsoft Office files created in Excel spreadsheets, Word documents, Access databases, Power point presentations and these type of files from AmiPro and Corel Draw and others.

These types of computer viruses are programmed using the language that the application understands and not in the language of the operating system thus they are operating in a way that is independent of the operating system so it can infect any kind of system be it Mac, PC or even Linux just as long as the computer is running the application that understands the macro virus. As the macro language has become more and more powerful the threat of these types of computer viruses has graduated to more critical types of computer viruses. These viruses have been around since 1995 and the first was found to infect Microsoft Word but now have moved to other programs and they number in the thousands.

One should always be on the lookout for these types of computer viruses and should take every precaution to avoid them. Be ever watchful of every file you open or else you may be looking for my next hub on how to remove these types of computer viruses.
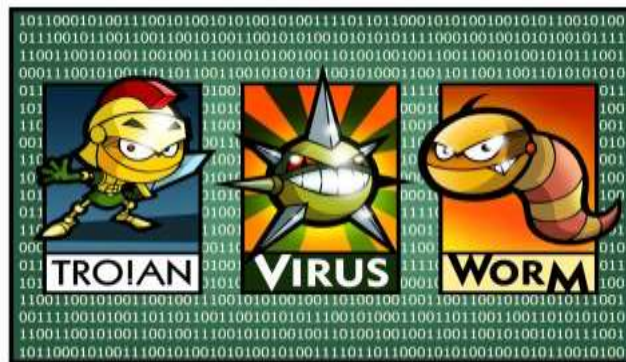

Fig: show the famous kind of virus.

General concept:

World Wide Web (WWW):
Is a collection of Web pages and related resources which are linked together across the internet?
Web site:
Computer storage area that contains one or more Web pages
Hypertext:
It is a piece of text that can perform an action when the user clicks on it
Home page:
It is the main page of a Web with links to other related page
Start page:
The first Web page you see when you start internet Explorer
Hypertext transfer protocol (HTTP):
A protocol that allows text with links to be transmitted from computer to computer.
Hypertext Markup Language (HTML):
A set of formatting commands that you place around a text or pictures to create a Web page
File transfer protocol (FTP):
Is an Internet software tool for transferring files form one computer to another.

Note: -

- Down loading: the process of transferring a file from a network computer to your local computer.
- Up loading: the process of transferring a file from your local computer to a network computer.
- Web Browser: computer programs which allow people to access information, view images, hear sounds and watch video on the WWW. Microsoft internet Explorer & Netscape Navigator is Browsers.

Starting internet explorer:

  The internet explorer is the application that displays the Web pages from the internet, we can started in many ways: -

- Click the internet explorer icon on the desktop Window

Or: {Start > programs > internet explorer}.

The components of internet explorer: -

1. *Title Bar*: appears at the top of the screen contains the name of the current Web page or file.
2. *Menu Bar*: contains a series of menus that you can use to control the way Internet Explorer works.
3. *Tool Bar*: it is a group of buttons you can click to run frequently used commands.

Web address:

  Every page has its own unique address, known as Uniform Resource Location URL, as shown in the figure:
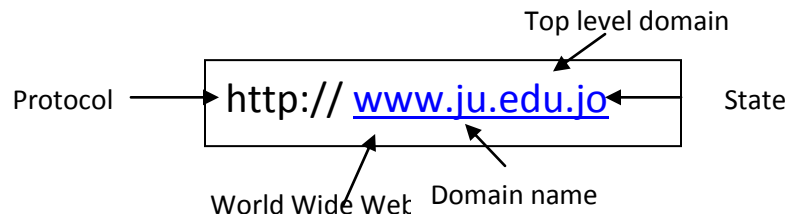
URL is made up of four components: -

1. http: Hypertext transfer protocol, is used to access the Internet and the other text Documents.
2. WWW: World Wide Web.
3. Domain Name: location or area where the pages are stored.

4. Top level Domain:
    a. ***Three – Letter code of a URL that indicates whether the address is***:

Top level domain name	Extension
Commercial	.com
Organization	.org
Network	.net
Government	.gov
Military	.mil
Education	.edu

    b. ***Two – letter code represent the state.***

- **access a Web site by typing its address:**
1. Click the address box, so that the current address is highlighted.
2. Type New address.
3. Press the Enter key.

Security system:

 Security: is a system of safe guards for protecting information Technology against disasters, system failure, or unauthorized access that can result in damage or loss.

Computer security (Also known as cyber security or *IT* Security) is information security as applied to computers and networks.
The field covers all the processes and mechanisms by which computer-based equipment, information and services are protected from unintended or unauthorized access, change or destruction. Computer security also includes protection from unplanned events and natural disasters.

Network Security System Architecture
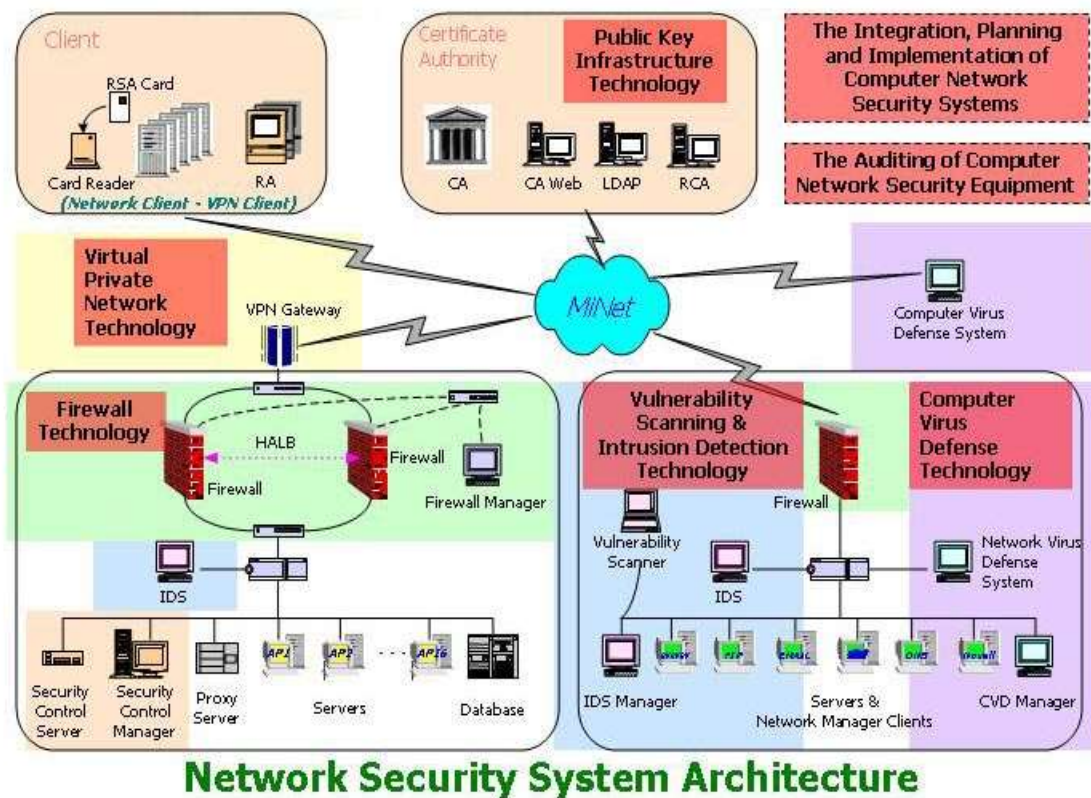
- *To protect your system you need to:*
    1. Use password.
    2. Use Authentication Techniques.
    3. Use authorization process.
    4. Use several standard Encryption & Decryption code.
    5. Change the password frequently.
    6. Make backup of files.
    7. Save storage media in a save place.
    8. Use Anti – Viruses programs.

Password: is a secret word or string of characters used for user authentication to prove identity or access approval to gain access to a resource (example: an access code is a type of password), which should be kept secret from those not allowed access.

The PC Tools Password Generator allows you to create random passwords that are highly secure and extremely difficult to crack or guess due to an

optional combination of lower and upper case letters, numbers and punctuation symbols.

Authentication:

This might involve confirming the identity of a person or software program, tracing the origins of an artifact, or ensuring that a product is what its packaging and labeling claims to be. Authentication often involves verifying the validity of at least one form of identification.
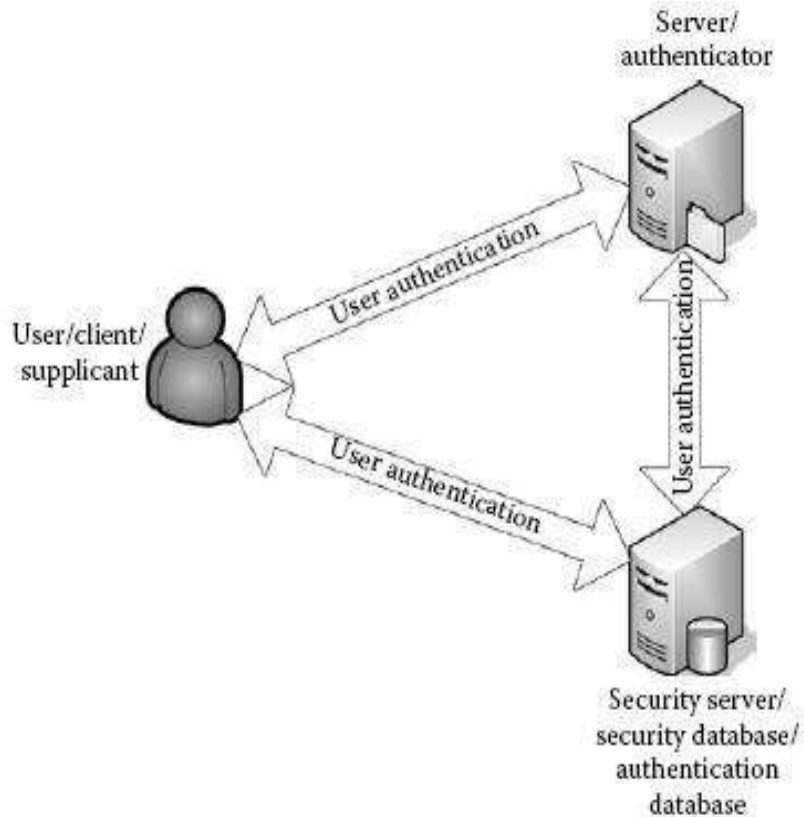
Authorization:

Authorization is the process of determining whether an already identified and authenticated user is allowed to access information resources in a specific way. Authorization is often the responsibility of the service providing access to a resource.

For example, if a user tries to access a file that resides on a file server, it will be the responsibility of the file service to determine whether the user will be allowed this type of access. Authorization can provide for granular control and may distinguish between operations such as reading or writing to a file, deleting a file, launching an executable file, etc.

Before authorization takes place, the user must be identified and authenticated. Authorization relies on identification information to maintain access control lists for each service.

Accounting:

Accounting is the process of maintaining an audit trail for user actions on the system. Accounting may be useful from a security perspective to determine authorized or unauthorized actions; it may also provide information for successful and unsuccessful authentication to the system.

FIG: Authentication, Authorization, Accounting.

Encryption :is the process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot read it, but that authorized parties can In an encryption scheme, the message or information (referred to as plaintext) is encrypted using an encryption algorithm, turning it into an unreadable cipher text . This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any adversary that can see the cipher text should not be able to determine anything about the original message. An authorized party, however, is able to decode the cipher text using a decryption algorithm, that usually requires a secret decryption key, that adversaries do not have access to. For technical reasons, an encryption scheme usually needs a key-generation algorithm to randomly produce keys

Decryption: The process of decoding data that has been encrypted into a secret format. Decryption requires a secret key or password.
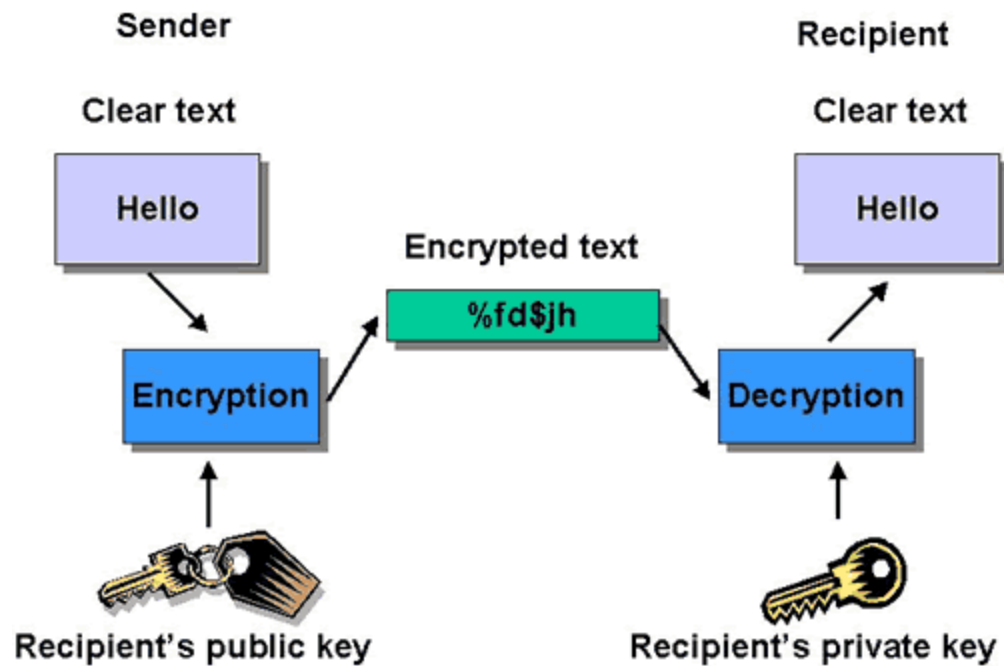
.

Fig show: Encryption& Decryption code

-

- **Computer are good for: -**
a. Repetitive tasks.
b. High speed tasks.
c. Accuracy & calculation.
d. Combining, storing & retrieving Data.
- **People are good in tasks that require: -**
    a. Creativity and imagination.
    b. Instruction cannot be written.
    c. Non – repetitive tasks.
    d. For tasks that need feeling.

Computer Hardware   Human Hardware