

UNIT - IV

GRAPHICAL USER INTERFACE

Those days cryptic commands acts as an interface between the user and the operating system Character user Interface (CUI). It was tedious for the user to remember lengthy commands.

So Later cryptic commands are connected to graphical representation Graphical user Interface (GUI) was introduced.

Advantage of GUI

- user Friendly
- More Efficient
- Windowing Technology

Windowing Technology

A single screen is divided into various partition and each partition hold different application with different size and it can be executed separately each partition is called as window. This technology is called as Windowing technology.

Components of GUI

1. Menu Bars
2. Scroll Bars
3. Controls
4. Dialog Box
5. Feedback

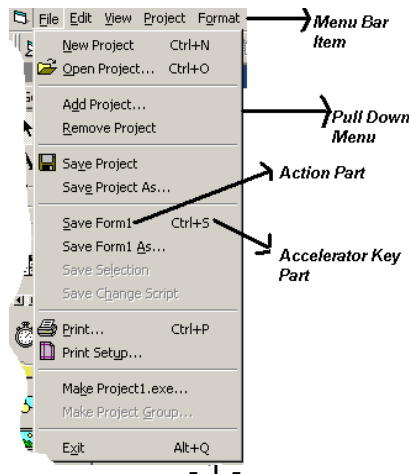
Menu Bars

A menu bar consists of Menu Bar items and a pull down menu. Menu bar items are the one that are seen without the user interaction e.g.: File, Edit, View. Pull down menu is the one that is visible after the user interaction.

A menu item has two parts

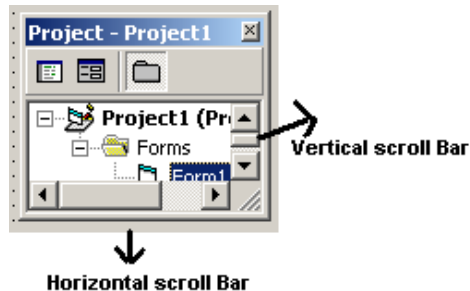
1. Action part
2. Accelerator part

The action part is on the left side and accelerator key part is on the right side (i.e. Shortcut Keys).



Scroll Bars

Scroll Bars are used to see the information that is not visible on the window. There are two types of scroll Bars they are Horizontal scroll bar and vertical scroll bar. Vertical scroll bar is used for moving upwards and downwards. Horizontal scroll bar is used for moving right to left.

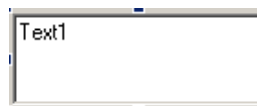


Controls

It consists of Textbox, Command Button, List Box, Combo Box, Option Button, Check Box, and Label Box.

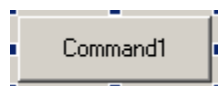
Text Box:

It is used for getting the user input.



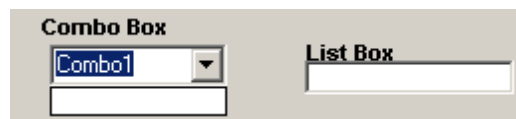
Command Button Or Push Button:

It is used for performing some events.



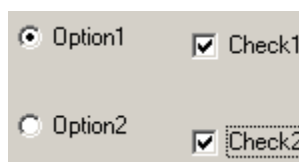
Combo Box and List Box:

Both are used for listing many items inside it. The combo box has the text area and a list area, whereas the list boxes just have only list area.



Option Button and Check Box:

Option Button is otherwise called as Radio Button. It is used for only single selection. Check Box consists of square box with items. It is used for multiple selections.



Label Box:

Label Box is used for identifying the controls.

**Dialog Box:**

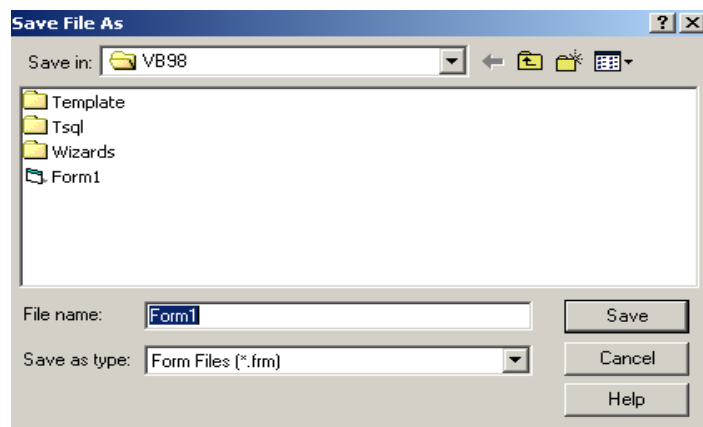
It is used to supply the user with information and it also accepts the input from the user.

There are two kinds of dialog boxes.

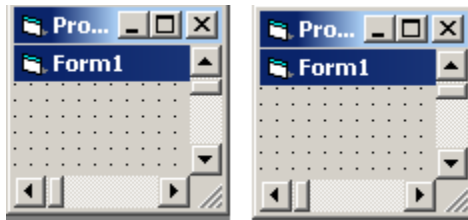
1. Modal dialog box
2. Modeless dialog box

Modal Dialog box

It expects the user to respond to it before switching on to some other window is called modal dialog box. Eg. Save, Save As Window.

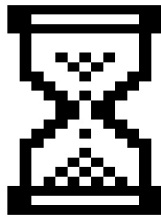
**Modeless dialog box**

It doesn't expect the user to respond is called as modeless dialog box.

**Feedback:**

Each and every GUI application should have a feedback after every action.

E.g. Hour glass pointer tells that the cpu is currently executing. The progress bar tells how much percentage is complete and how much is incomplete.



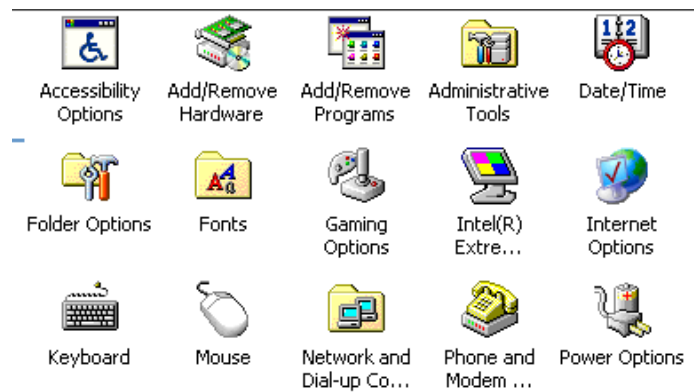
Hour Glass



Progress Bar

Icon:

An Icon is a graphical representation of an application or utility. A good icon should be able to identify and invite the user to an application. Some of the sample icons are shown below.



Comparison between MS-Dos (CUI) and MS-Windows (GUI) and MS-Windows NT (Networking Operating System)

	MS – DOS	MS-Windows	MS-Windows-NT
1.	Single Task Operating System	Multitasking Operating System	Multi User, Multitasking Operating System.
2.	CUI	GUI	GUI
3.	–	This Operating System needs at the top.	Doesn't need MS-DOS running at the top.
4.	–	–	It is a portable operating system and runs on any platform.
5.	Does not have built in networking.	Does not have built-in networking.	As a built-in networking support.
6.	Does not support Multithreading.	Does not support Multithreading.	Has a built-in Networking support.
7.	Does not allow symmetric multiprocessing.	Does not allow symmetric Multiprocessing.	Symmetric Multiprocessing is followed.
8.	Ms-Dos uses 32-bit processors.	Ms-windows uses 16-bit processors.	Ms-windows-NT uses 32-bit processors.
9.	Does not use virtual memory management technique.	Does not use virtual memory management technique.	Uses virtual memory management.
10.	Use FAT technique	Use Fat technique	NTFS (New technology File system) technique. E.g. File name up to 256 characters long.

Requirements of a Window – based GUI

Some of the basic requirements are

1. Consistency
2. Direct Manipulation
3. Flexibility
4. Explicit Destruction

Consistency:

- All applications should be within one windowing environment.
- Which means visual appearance of controls and their components should be consistent e.g.(Top right corner in window should be minimize,maximize,close button).
- Menus should be in orderly fashion. E.g. Edit → cut, copy, paste,

select all.

Direct Manipulation:

- Direct manipulation allows the user to control his action better by prompting him to select each command.
- With direct manipulation, user gets a feedback on their actions.

Flexibility:

- Users should be allowed to configure the settings and change configuration to their liking.

E.g. 1) Changing the Mouse button activity to, Right –hand for left handled person.

2) Giving different color to borders, buttons etc.

3) Multiple options for saving.

Alt+F+S, Ctrl+S.

Explicit Destruction

When an action is irreversible and has negative consequences, the user should be able to explicitly confirm it before being carried out. Such confirmation is needed when we delete a file.

AUTHENTICATION

Authentication is a process of verifying whether a person is a legitimate (valid) user or not. There are two types of authentication that are possible.

- i) Authentication in a centralized environment.
- ii) Authentication in a network or distributed environment.

i) Authentication in a centralized environment.

Authentication in this environment can be achieved in the following three ways.

- a) Password
- b) Artifact-based
- c) Human characteristics

a) Password

The password is most commonly used scheme which is easy to implement. The OS associates a password along with the username of each user, and stores it after encryption in a system file.

When the user wants to log on to the system, the Operating system demands for keys in both username and password. The OS then encrypts this keyed in password using the same encryption technique and then matches it with the one stored in the system file. It allows to login only after it gets matched.

The password scheme is easy to implement, but it is just easy to break if we know others password. In order to counter this threat, the designers of the password systems make use of number of techniques. Some of these are listed below:

Echo Suppression and Encryption

The password is normally not echoed. It is also stored in an encrypted form, so even somebody reads the password file, the password cannot be decrypted from it without knowing the key.

Choice of the password

Three methods can be used in choosing a password.

- i) The operating system itself selects the password for the user.

The system selected password may not be easy to guess for an intruder, but the problem is user himself may not remember the password.

- ii) The system administrator decides the password.

It is not particularly good idea as more than one person would know about each password.

- iii) The user selects the password

The user can remember it easily, it can be penetrated easily too because most of the users make use of names, family names, names of cities so an intruder can guess the possible password easily.

Password Length

The password length plays an important role in the effectiveness of the password scheme. If the password is short, it is easy to remember, but a short password is easy to break. If a password is too long it is difficult to penetrate, but it is difficult to remember by the valid users. Therefore, a tradeoff is necessary. It is normally kept 6-8 characters long.

Pass Phrases

This scheme is used if the password length is very short. Along with each password, a long but meaningful message or phrase is predetermined.

Ex:

“I AM READING A GOOD BOOK”

The OS encrypts it and stores along with the original password. When the user wants to login the user must give the original password and the long message to the system. The system applies the same encryption and compares both the passwords and then allows the user to login only if it gets match.

Advantage: It is difficult to break and does not require larger storage space.

Disadvantage: Too many characters to be keyed in by the user.

Salting

Salting is a technique suggested by Morris and Thompson to make it difficult to break somebody's password. The salting technique appends a random number n to the password before the encryption is done.

Additional password

Some Operating system asks for multiple passwords at different levels. This makes penetration more difficult. This additional password could be demanded at the very beginning or intermittently at a random frequency. It provides additional security.

Continuous Challenge

An operating system at random intervals, may ask predetermined questions to the user challenging him to prove his identity.

Ex:

Where you born?

What was the name of your maths teacher?

Computer Dial Back

The operating system maintains a list of all the legitimate users and their work telephone numbers .after a user keys the username, the operating system consults this list and dials back the telephone number automatically to ensure that it is the same user.

Force Password changes

The operating system forces the user to change the password at a regular frequency. Because even the intruder has found out a password it would not be valid for long time.

Disable Users

Many Operating systems allow a user to try a few guesses (typically 3). After these unsuccessful attempts, the operating system logs the user off. Some operating systems go to the extent of disabling the user from the system itself. If the user want to login again he must contact the system administrator.

b) Artifact-based

Some systems make user of artifacts such as machine readable badges with magnetic stripes or some kinds of electronic smart cards. Only on the supply of the correct artifact that the user possesses, he is allowed to use the system .It is popular in Automatic Teller Machines (ATMs).

c) Human Characteristics

This technique measures something human about a user, which is normally unique to him; It can be divided into two categories.

i) **Physiological**

The computer uses the scanners to capture and store a database of the bit patterns of finger prints for different users. If the user wants to login, the system compares the finger print which already stored in the database. These techniques are also called “biometric technique”.

Ex: fingerprints, hand shapes, pattern in the retina of the eye.

ii) **Behavioral**

In case of voice pattern matching, the system requires the user to speak out some thing (say password) at the time of creating a user profile for him. The system digitizes these spoken passwords and creates a database of them for future use.

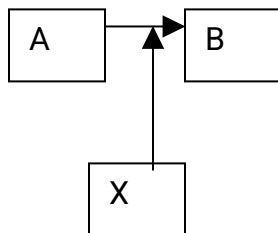
When the user wants to login, he have to speak his password the operating system match the voice pattern

Ex: voice pattern, signature analysis.

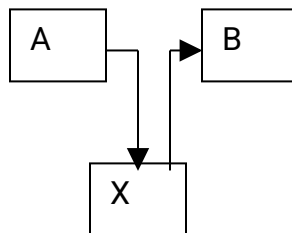
SECURITY AND PROTECTION

INTRODUCTION TO SECURITY AND PROTECTION

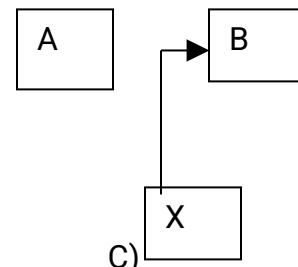
THREATS:



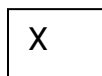
A) TAPPING/DISCLOSURE
FABRICATION



B) AMENDMENT



C)



D) DENIAL

A) Tapping:

- Unauthorized use of service
- The third party access it without the knowledge of others.

Disclosure:

- A Source party willingly or knowingly discloses it to the third party

B) Amendment:

- Unauthorized alteration or deletion of information.

C) Fabrication:

- Unauthorized Fabrication of information.

D) Denial:

- Denial of service to the authorized user.

ATTACKS ON SECURITY:

The security system can be attacked and penetrated in number of ways.

- Authentication
- Browsing
- Trapdoor
- Line tapping
- Lost line
- Line trapping
- Waste Recovery
- Electronic Data Capture
- Rogue Software
 - ❖ Trojan horse
 - ❖ Chameleon Software
 - ❖ Ordinary software Bomb
 - ❖ Timed software Bomb
 - ❖ Logical software Bomb
 - ❖ Virus
 - ❖ Worms

➤ Authentication:

Authentication means verification of access to the system resources. Some of the ways the intruder attack the authentication are.

- ❖ The intruder may guess or steal somebody else password
- ❖ An intruder may find out the password by the trial or error method.

- ❖ An intruder can write a dummy login program to fool the users and steal the username and password.
- Browsing:
 - ❖ The intruder can browse the system files to get information about the unprotected files and databases.
 - ❖ Confidential information should be read or modified.
- Trap Door or Back Door:
 - ❖ The software designers may use some secret entry points (i.e.) shortcuts into a program that allows someone that is aware of back doors to gain access without going through the usual security access procedures.
- Line Tapping:
 - ❖ A special terminal is used to trap the communication line and access or even modify the data. It can be in the form of tapping, amendment or Fabrication.
- Lost Line:
 - ❖ In the networking environment a line can be lost and an intruder will gain the control and use others login
- Waste Recovery:
 - ❖ A penetrator can use some technique to recover the deleted files.
- Electronic Data Capture:
 - ❖ An intruder picks up the screens using camera and recognizes what is displayed on the screen.
- Rogue Software:
 - ❖ The variety of software program are under Rogue software.
 - o **Trojan horse:**
This is a program which appears to be harmless but has a piece of code which is very harmful.
 - o **Chameleon Software:**
It mimics by a useful and a correct program.
For eg: It can mimic a login program and Collects valid username and password.
 - o **Ordinary Software Bomb:**
This is a piece of code which “explodes” as soon as it is executed.
 - o **Timed Software Bomb**
It is the same as the ordinary software bomb but it becomes active only at a specific time.
 - o **Logical Software Bomb**
It is the same as the ordinary software bomb but it is activated only when the logical condition is satisfied.
 - o **Worms:**
These are the programs attacking the nodes on the

network and spreading to other nodes. It consumes all the resources on the network.

- o **Virus**

This is only a part of the program which gets attached to other programs and causes damages.

- o **Rabbits:**

They are similar like worms but it replicates on the disk until its capacity is exhausted, but it can be easily detected.

VIRUS

Virus attaches itself to a program and propagates (spread) copies of itself to other programs. Virus corrupts the data as well as the code. Almost all viruses are attached to an executable file, which means the virus may exist on your computer but it actually cannot infect your computer unless you run or open the malicious program. It is important to note that a virus cannot be spread without a human action, (such as running an infected program) to keep it going.

People continue the spread of a computer virus, mostly unknowingly, by sharing infecting files or sending e-mails with viruses as attachments in the e-mail.

Types of Virus

There are 2 types of virus

1. Transient Virus
2. Resident Virus

1. Transient Virus:

This virus runs when the attachment program executes and terminates when its attachment program ends.

2. Resident Virus:

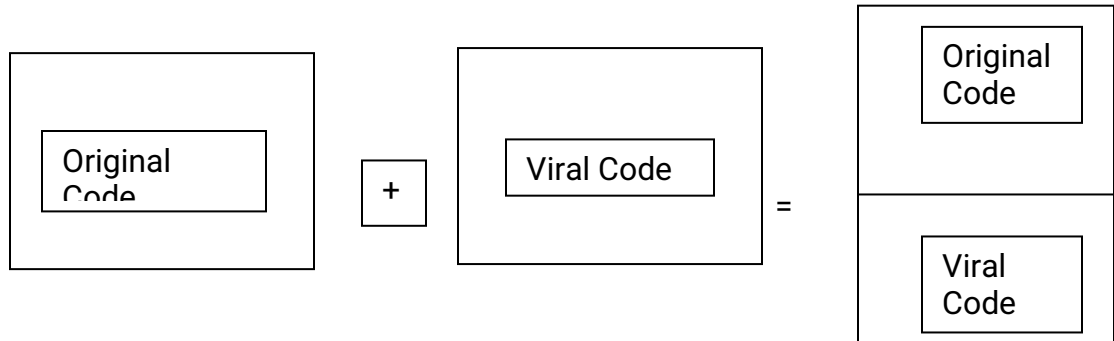
This virus resides in the memory after the attachment program is completed and it remains active.

Infection Methods of Virus

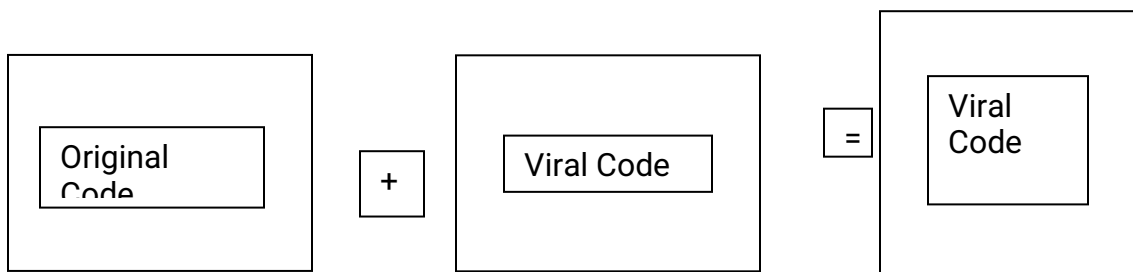
- APPEND
 - REPLACE
 - INSERT
 - DELETE
 - REDIRECT

Example:

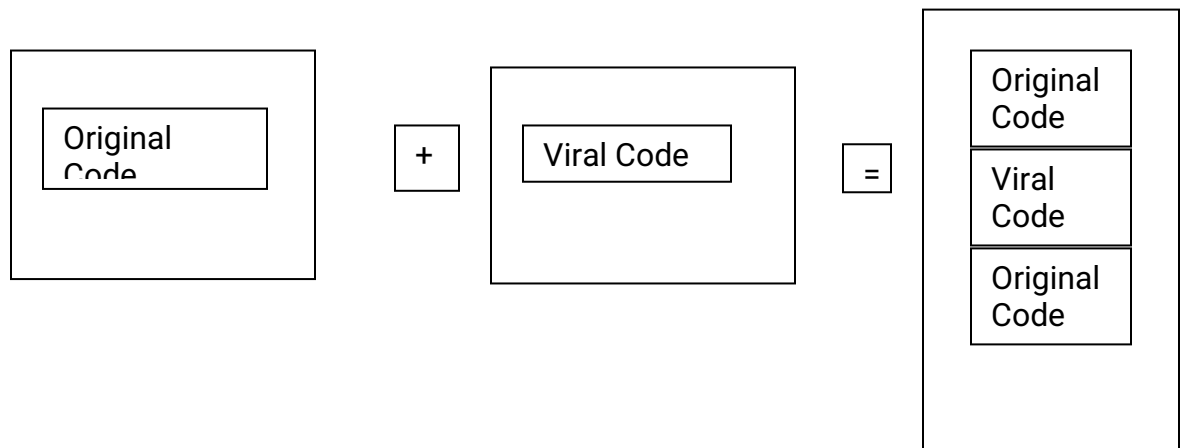
- o **APPEND** The viral code appends itself to the unaffected program.



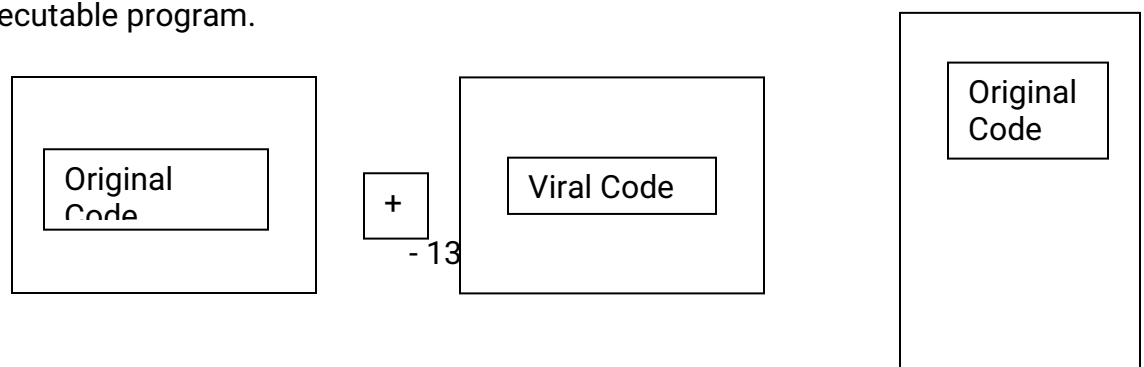
- o **REPLACE** The viral code replaces the original executed program completely or partially.



- o **INSERT** The viral code is inserted in the body of the executable code.



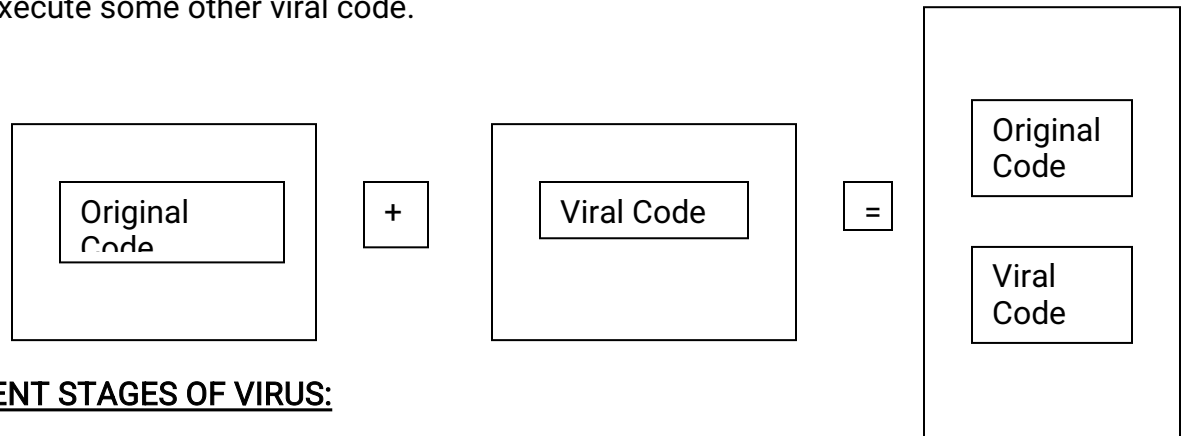
- o **DELETE** The viral code deletes some of the code from the executable program.



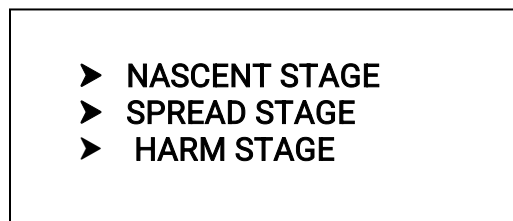
=

Viral
Code

- o **REDIRECT** The normal control flow of the program is changed to execute some other viral code.



DIFFERENT STAGES OF VIRUS:



NASCENT STAGE As long as the virus is in floppy or CD then it is called as nascent stage.

SPREAD STAGE When the virus is copied from floppy or CD to the system it is called as spread stage.

HARM STAGE When the program is executed then is harm stage.

VIRUS DEDUCTION, REMOVAL, PREVENTION:

Virus Deduction

- Virus can be deducted using checksum.
For Example:

If a program ABC has a checksum value 120 and if the checksum value is changed we can say that virus can be detected.

VIRUS REMOVAL

The pattern of the virus is known then it can be removed.

Original Code: A000B000C000

Viral Code : A***B***C***

The above example is some of the patterns of virus.

VIRUS PREVENTION

Virus can be prevented by the following methods.

1. Choosing only commercial software
2. Open attachments only when it is known to them to be safe.
3. Make backup copies of the executable system files.
4. Use virus detectors and scan regularly and update them daily.
5. Scan the floppy or CD before the activation.

WORMS:

A **worm** is similar to a virus by design and is considered to be a sub-class of a virus. Worms spread from computer to computer, but unlike a virus, it has the capability to travel without any human action.

The biggest danger with a worm is its capability to replicate itself on your system, so rather than your computer sending out a single worm, it could send out hundreds or thousands of copies of itself.

One example would be for a worm to send a copy of itself to everyone listed in your e-mail address book. Then, the worm replicates and sends itself out to everyone listed in each of the receiver's address book

MODE OF OPERATIONS OF WORMS:

It originates from CD, Floppy, Internet, and other computers. It looks at the mailing lists. (It has the information about the list of the computer connected) and spreads to them and takes control over the resources of other computers.

SAFE GUARD AGAINST WORMS:

- | |
|--|
| <ul style="list-style-type: none">❖ Prevent its creation❖ Prevent its spreading |
|--|

❖ PREVENT ITS CREATION:

By tight security and protection mechanism and by scanning the CD, Floppy disk etc., Worms can be prevented during its creation itself.

❖ PREVENT ITS SPREADING:

This can be done by introducing various checkpoints in the network. We can disallow the transfer of executable files over the network.

DESIGN PRINCIPLES IN SECURITY:

To design a secured system the following principles have to be followed

- 1) Public design
- 2) Least privilege
- 3) Explicit demand
- 4) Continuous verification
- 5) Simple design
- 6) User acceptance
- 7) Multiple condition

PUBLIC DESIGN:

The design of the security system should not be secret. The designer should assume that the penetrator know the algorithm. But the security will be still maintained because they may not know the keys.

LEAST PRIVILEGE:

Every process should be given least possible privilege that are necessary for an execution.

EXPLICIT DEMAND:

No access rights should be granted to a process as default. Each user has to demand the access rights explicitly to avoid granting rights to unauthorized user.

CONTINUOUS VERIFICATION:

The access rights should be verified frequently or continuously for each user. For e.g.-: the access rights has to be checked whenever the user is opening, reading and writing the file.

SIMPLE DESIGN:

The design of the security system should be simple and uniform security has to be built from the lowest level to the highest level.

USER ACCEPTANCE:

The design should be simple and easy to use for the users, the user should not waste time to learn how to protect the system of files.

MULTIPLE CONDITIONS:

The system should be designed to satisfy multiple condition. For e.g.-: the system could demand for two password.

ENCRYPTION:

Encryption is one of the most important tool in security, protection and authentication.

This process involves two things

1. Encryption

2. Decryption

1. Encryption

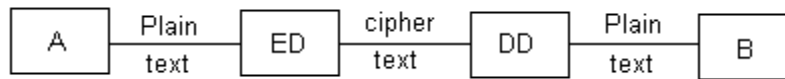
Changing the original data into different data is called as encryption.

2. Decryption

Changing the Different data into original data is called as decryption.

Note:

- The original data is called as Plaintext
- Different data is called as Cipher text.



DIFFERENT ENCRYPTION AND DECRYPTION ALGORITHM:

There are **two methods**, they are

1. Transposition cipher
2. Substitution cipher

Transposition cipher

Letters in the message are not changed but the order are changed in transposition cipher.

For E.g. 1:

Original Text: X Y Z

Cipher Text: Z X Y

For E.g. 2:

Plain text: I am fine

Cipher Text: enif ma I

Substitution cipher

The original data is changed into different set of characters and numbers in substitution cipher.

For E.g. 1:

Original Text: X Y Z

Cipher Text: 1 2 3

For E.g. 2:

Plain text: I am fine

Cipher Text: j bn gjof

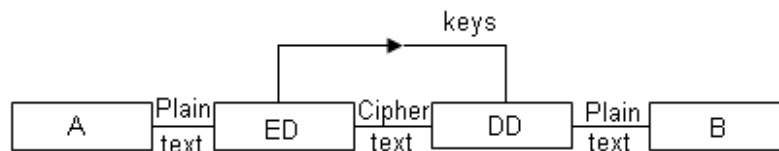
Methods of Encryption:

There are two methods of encryption

1. Conventional encryption
2. Public Key encryption

1. Conventional Encryption:

There is only one key that is known to A and B and not known to anybody else. This method also called key distribution method.



ADVANTAGE:

Authentication is possible in conventional encryption.

DISADVANTAGE:

The two parties each time has to decide upon a common key and then initializing the communication.

2. Public Key encryption:

There are two types of keys

1. Public Key
2. Private Key

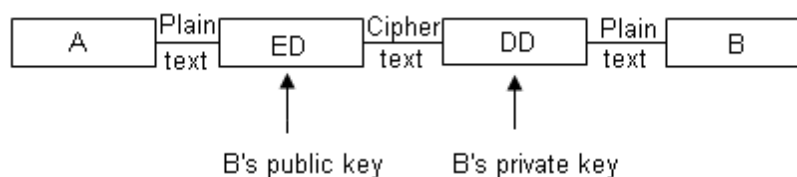
Public Key:

If the key is known to all the nodes connected in the system then it is called as public key.

Private Key:

If the key is known only to a particular node then it is called as private key.

The public key encryption when A wants to send the data to B, A encrypts the message using B's public key and produces the cipher text. The cipher text is now transferred to B, now B decrypts the message using B's private key.



The protection in this key very good, because B can only decrypt that cipher text message and no body else can do it.

DISADVANTAGE:

B could not confirm that the message is originated from A .That is no

authentication is possible because the public key is known to every one. Anybody could have send this message instead of A.

SECURITY IN DISTRIBUTED ENVIRONMENT:

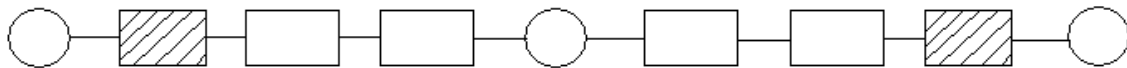
- Security is more important in network environment, because an intruder can tap the message to a network and the data may be lost.
- Twisted pair cable, coaxial cable and optic fiber cable are used as the communication medium between the nodes in which optical fiber cable is good communication medium where tapping is almost impossible.

Location of Encryption devices:

There are basically two forms of encryption.

1. End to End encryption.
2. Link encryption.

Eg:



The shaded boxes represent end to end encryption and the empty boxes represent link encryption.

The end to end encryption needs less number of Encryption/Decryption devices.

The linked encryption needs more number of Encryption/Decryption devices.

As per the above example, there are two encryption/decryption devices for end to end encryption and four encryption/decryption devices for linked encryption.

Key distribution:

If two parties want to communicate with one and another in the distributed environment we need a key. They are of two types.

1. Permanent key.
2. Session key.

1. Permanent key:

A key is pre determined permanently between the two parties and then used for all the communication.

2. Session key:

For every session a separate key is agreed upon the two parties.

Authentication Server & Distribution Server: (A.S & D.S):

- Authentication server is responsible for allowing or disallowing the parties to communicate.
- Distribution server is responsible for key distribution.
- When X wants to communicate with Y. X applies to authentication server for the permission to communicate with Y.
- Authentication server checks for the permission. If the permission is yes, then authentication server makes a request to the distribution server to generate a key and then it distributes to X and Y. Both X and Y receives the key from the distribution server over the network.
- From this status onwards X and Y can communicate with one and another with that key.

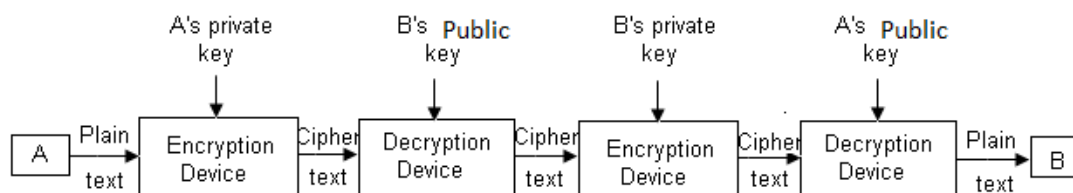
DIGITAL SIGNATURE:

Digital signature is used to achieve both protection and authentication.

It is like any other human signature on a plain text of paper. Let us assume that a person A sends a signed letter to person B with acknowledgement. This serves us with two purposes.

1. A cannot tell that it has not send a letter to B (B can produce its proof).
2. B cannot refuse that it has not got it because A would have an acknowledgment.

This concept is implemented in digital signature.



A digital signature maintains both protection and authentication. Authentication is done with A's private key and decrypts with A's public key. From this statement we can assure that the message could have been sent only by A. Assuming that A has not leaked out its private key.

Protection is accomplished by adding two private keys and two public keys.

Protection Mechanism:

Protection is used to protect the systems, Resources, hardware or software.

The main aim of protection is to protect the files, devices, databases and

processes from unauthorized users.

The various protection mechanism are given below,

1. Access rights
2. Domain and domain switching.
3. Access hierarchy
4. Blocked structure language.
5. Access control list and capability list.

1. Access rights:

- The user is called as subjects and the files, databases, devices that is currently working is called as objects.
- The operating system allows different access rights or different objects and subjects.

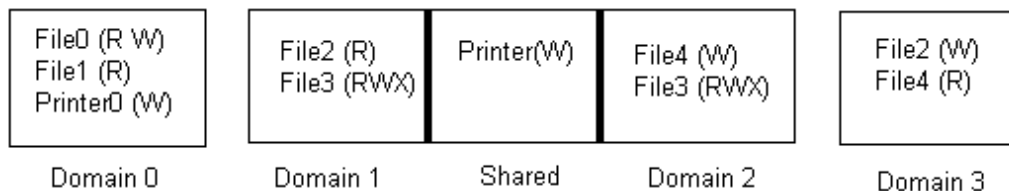
The list of access rights that can be granted is shown below.

S.No.	Access right	Code
1	No Access	N
2	Execute only	E
3	Read only	R
4	Append only	A
5	Update	U
6	Modify protection	M
7	Delete	D

For example, if a process is allowed to delete a file (D) then it is allowed for all the above access rights (M, U, A, R, E). Similarly if a process is allowed to read a file(R) then it is allowed for Read and Execute. (R,E)

2. Domain and Domain Switching:

- The operating system defines another concept called domain which is a combination of the objects and set of different access rights for each of the object.
- A subject can be put under a particular domain.



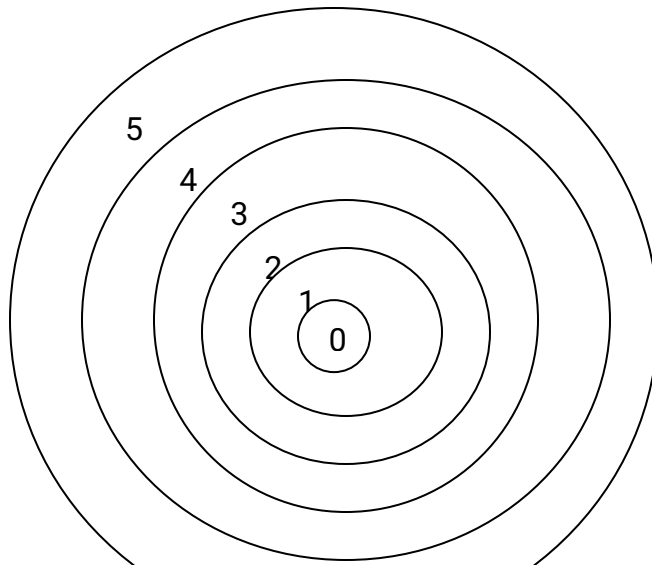
For example, the user processor executing the domain 0 as an access rights to read from file 0 and write from file 0, read from file 1 and write from

printer 0.

- Similarly domain 1, 2, 3 can be defined. Domain1 and Domain2 intersects with each other which means printer1 belongs to Domain1 and Domain2.
- Switching from one domain to another domain is called as switching domain.

3. Access hierarchy:

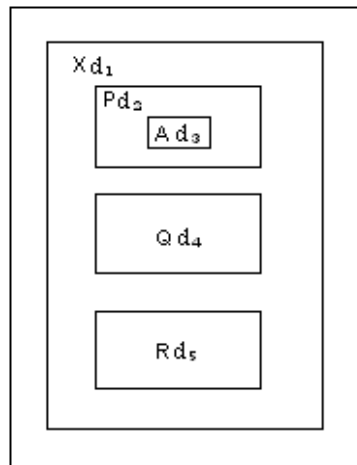
(PROTECTION RING)



- The variation of the domain switching scheme could be organized these domain into number of access hierarchy,. The number of domains is divided into number of protection raise.
- The entire protection based is divided into n domains (0 to n-1). Such a way the domain 0 as the maximum access hierarchy and domain n-1 as the least access hierarchy.
- A subject which is executing in a specific ring can access all the objects within that ring.
- A domain switch to an outer domain is easily possible because it has less privilege than the inner ring. But domain switch to an inner domain requires strike permission.

4. Block structure language:

- A block structure language such as 'C' or PASCAL gives a very important concepts for access hierarchy and it is explained as follows.



- Here X, P, Q, R, A are called as functions are of different scope and the functions have different variable inside such as d1,d2,d3,d4,d5.
- The d1 can be accessed in X, P, A, Q, R where as d4 can be accessed only in Q but not in X, P, A and R.

5. Access control list: (ACL)

	File 1	File 2		File 10
User 1	R W			
User 2			R W X	
User 3		W		X

- To have a protection mechanism information are stored inside a list called as access control list. It consists of two options users and files. According to the above example user1 has a read access and write access over files.

6. Capability list:

S.No.	Objects	Access rights	Address of file
0	File 2	W	-
1	File 5	R	-
2	File 10	X	-

- If an access control is divided by row then it becomes capability list. The above table tells about the capability list for users. This tables tells that user 3 can access file 2, file 5, file10 with W, R, X respectively.