1) Introduction to Computer security and security trends

Page No. 1
Date

1.1 Introduction :- The term computer security means the collective processes and mechanisms by which sensetive and valueable information and services are protected from publication, tampering or collapse by unauthourised activities or untrustworthy individuals and unplanned events respectively. The objective of computer security includes protection of information and property from theft, corruption or natural disaster.

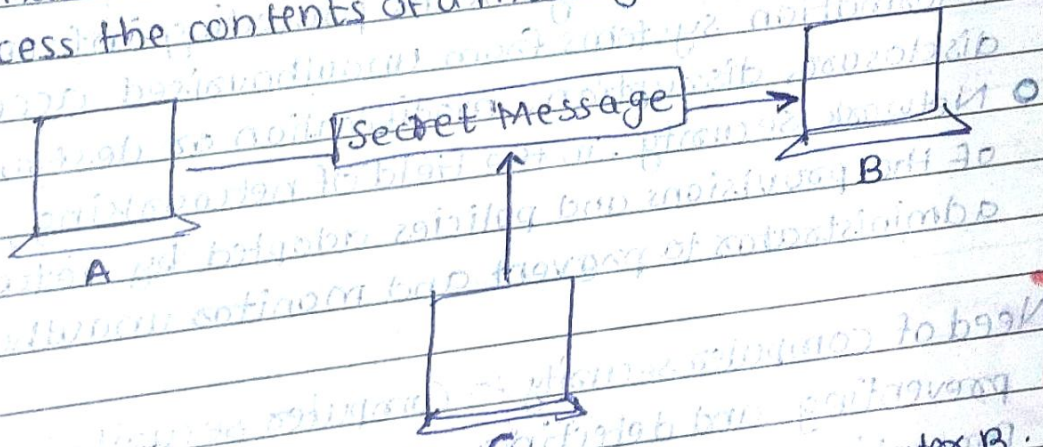
- Computer security is the protection of computers and data that the computer holds. This can be done by placing passwords and setting up firewalls.
- Data security means ensuring data which is kept safe from corruption and access to it is suitably controlled. Thus it helps us to ensure privacy.
- Information security means protecting information and information systems from unauthourised access, use, disclosure, disruption, modification or destruction.
- Network security, in the field of networking, it comprises of the provisions and policies adapted by network administrator to prevent and monitor unauthourised activities.

- Need of computer security :- Computer security is the process of preventing and detecting unauthourised use of your computer. Prevention measures help you to stop hackers from accessing any part of computer systems. Hackers do not care about your identity, often they want to gain control over your computer to launch attack on other computer security. Adding to these, hackers are always discovering vulnerabilities to exploit in computer software.

Security Basics :- Computer security objectives are described in terms of three basic overall objectives:

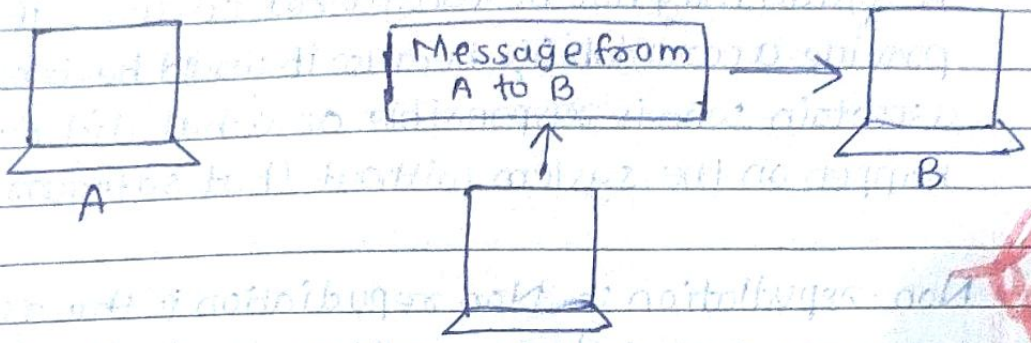
- Confidentiality, meaning that the computing system's assets can be read only by authorised parties.
- Integrity, meaning that the assets can only be modified or deleted by authorised parties in authorised ways.
- Availability, meaning that the assets are accessible to the authorised parties in a timely manner as determined by systems requirements. The failure to meet this goal is called as denial of service.

Confidentiality :- It is the concealment of information or resources. It's principle specifies that only the sender and the intended recipient(s) should be able to access the contents of a message



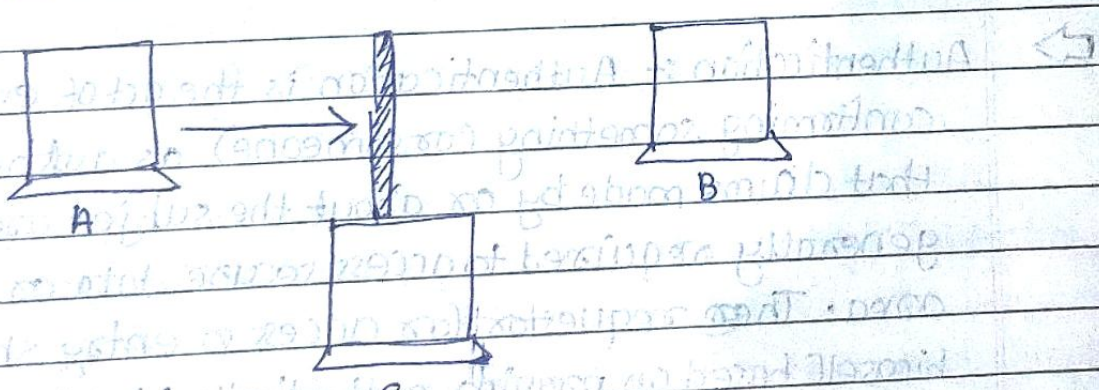
Here, computer A sends message to computer B. If C gets access to this message, it will defeat the purpose of confidentiality. This type of attack is called as interception.

⇨ Integrity :- It refers to the trustworthiness of data or resources, in terms of preventing improper or unauthorised change. It includes data integrity (the content of information) and origin integrity (the source of the data, often called authentication).



Here, computer A sends message to computer B. The contents of the message are changed by C before processing that message to B. Computer A is unaware of this change. This will defeat the purpose of integrity. This type of attack is called as modification.

⇨ Availability :- The principle of availability states that resources should be available to authorised parties at all times.



Here, computer A is sending message to computer B. Due to intentional actions of unauthorised user C, A may not be able to send data to B. This would defeat the purpose of availability. This type of attack is called as interruption.

⇨ Accountability :- It is another important feature/ principle of information security that refers to the possibility of tracing action and events back in the time to the users, systems or processes that performed them to establish responsibility for actions or omissions. A system may not be considered secure, if it does not provide accountability because it would be impossible to ascertain who is responsible or what did or did not happen on the system without that safeguard.

Read

⇨ Non-repudiation :- Non repudiation is the assurance that someone cannot deny something. Typically it refers to the ability to ensure that the party to the contract or communication cannot deny the authenticity of their signature on the document or sending of a message that they originated. One of the services of non-repudiation is digital signature. It is a cryptographic mechanism that is electronic equivalent to a written signature to authenticate a piece of data as to identify the sender.

⇨ Authentication :- Authentication is the act of establishing or confirming something (or someone) as authentic, that is that claims made by or about the subject are true. It is generally required to access secure data or enter a secure area. The requestor for access or entry shall authenticate himself based on proving authentically his identity by means of:

- What requestor individually know as a secret, such as password or Personal Identification Number (PIN)
- Requesting owner uniquely has, passport or an ID-card
- What requester is bearing individually, such as biometric data, like a ~~figer~~ finger print or face geometry.

Difference between Authentication and authorisation:-
Authentication is the process of verifying a person's identity; whereas authorisation is the process of verifying that a known person has the authority to perform certain operation.

There are many ways of authenticating user:
1] Password based authentication :- Requires the user to know some predetermined quantity (their password).
Advantages :- Easy to implement, requires no special equipment
Disadvantages :- Easy to forget password. User can tell another user its password. Password can be written down. Password can be reused.
2] Device based authentication :- Requires the user to posses some item such as a key, mag strip, card, s/key device, etc.
Advantages :- Difficult to copy. Cannot forget password. If used with a PIN is near useless if stolen.
Disadvantages :- Must have device to use service so the user might forget it at home. Easy target for theft. Still doesn't actually actively identify the user.
3] Biometric authentication :- It identifies physical characteristic of the user that cannot be seperated from their body.
- Retina scanners :-
Advantages :- Accurately identifies the user when it works
Disadvantages :- New technology that is still evolving. Not perfect yet.
- Hand scanner :-
Advantages :- Difficult to seperate from user. Accurately identifies the user.
Disadvantages :- Getting your hand stolen to break into a vault sucks a lot more than getting ID card stolen

Authorisation :- Once the system knows who the user is through authentication, authorisation is how the system decides what the user can do.

Two Factor Authentication :- When elements representing two factors are required for identification, the term two factor authentication is applied. For ex:- bank card and ~~and~~ a PIN.

Multi Factor Authentication :- It is an extension of two factor authentication only involves exactly two factors, multi factor authentication involves two or more factors. Thus every two factor authentication is multi-factor authentication but not vice versa.

□ Example of security :-

Examples of types of security breaches and threats :

1] Backdoors :- A backdoor in a computer system is a method of bypassing normal authentication, securing remote access to the computer, while remaining undetected. The backdoor may take the form of an installed program or could be a modification to an existing program or hardware device.

2] Denial of service attack :- These attacks are not used to gain unauthorised access or control of a system. Attackers can deny service to individual victims, such as by deliberately entering a wrong password three consecutive times and and thus causing the account of the victim to be blocked.

3] Direct Access attacks :- In this type of attacks hackers gain access to your computer system and install various software worms, key loggers and operating system modification. The only way to prevent this type of attack is to encrypt the storage media and store the key away from the devices.

4] Eavesdropping :- It is the act of listing to private conversation typically between hosts on a network.

5] Exploits :- An exploit is a piece of software, a chunk of data, or sequence of commands that take advantage of a software bug or glitch in order to cause unintended behaviour onto the computer system. This frequently includes such things as gaining control of a computer system or allowing previlage escalation or a denial of service attack.

6] Indirect attacks :- An indirect attack is an attack launched by third party computer. By using someone else's computer to launch an attack, it becomes far more difficult to track down the actual attacker.

☐ Challenges for security :- According to the innovative security approaches, six significant security challenges can be identified as follows:

⇨ Ecommerce requirement
⇨ Information security attacks
⇨ Immature information security market
⇨ Information security staff shortage
⇨ Government legalisation and industry regulations
⇨ Mobile workforce and wireless computing.

Model for security :- A computer security model is a scheme for specifying and enforcing security policies. Various security models deployed by industry are listed below:

1] The Biba Model or Biba Integrity Model, is a formal state transition system of computer security that describes a set of access control rules designed to ensure data integrity.

2] The Bell-LaPadula Model (BLP) is a state machine model used for accessing address control in government and military applications.

3] The Brewer and Nash Model, was constructed to provide information security access control that can change dynamically.

4] The Clark-Wilson integrity model, provides a foundation for specifying and analysing an integrity policy of a computer system.

5] Multiple levels of Security (MLS), is the application of a computer system to process information with incompatible classification.

6] Role based access control (RBAC) is an approach restricting system access to authorised users. It is sometimes referred to as role based security.

1.2 Risk and threat analysis

Assets:- The core areas in risk assesment are:

1] Scope
2] Data collection
3] Analysis of policies and procedure
4] Threat analysis
5] Vulnerability analysis
6] Correlation and assesment of Risk acceptability

Threat analysis:- Threats are described as anything that would contribute to the tampering, destruction or interruption of any service or item of value. These threats can be split into Human and Non human elements.

Human:-

- ⇨ Hackers
- ⇨ Theft (electronically and physically)
- ⇨ Non-technical staff (Financial / accounting)
- ⇨ Accidental
- ⇨ Inadequately trained IT staff
- ⇨ Backup operators
- ⇨ Technicians, Electricians

Non-Humans:

- ⇨ Floods
- ⇨ Lightning strike
- ⇨ Plumbing
- ⇨ Viruses
- ⇨ Fire
- ⇨ Electrical
- ⇨ Air (dust)
- ⇨ Heat control

□ Information security threats:

1] Corporate cracks:- Intellectual property, business plans, customer database, hospital database records, credit card numbers are important to global economy. To crack into any of the above is referred to as Corporate cracks.

2] Internet commerce - Credit card Fraud :- Emboldened by the anonymity of Internet, some criminals will seek to make a quick hit and max of the card, while others will seek to buy small charges on a card indefinitely

3] Website Defacement :- A website defacement means someone broke into network gained access to relevant file system and modified the HTML for the site's home page. In website spoofing, someone creates a fake web page and then redirects traffic to that fake page.

4] Industrial espionage :- Industrial espionage involves collecting proprietary data from private corporations i-e competitor organizations or government agencies for the benefit of other organisation. Industrial espionage can be perpetrated either by companies seeking to improve their competetive advantage or by governments seeking to aid their domestic industries.

5] Foreign Government Espionage :- In some instances, there may be threats posed by foreign government intelligence services. Foriegn Industrial espionage carried out by a government is called as ecconomic espionage. In addition to possible economic espionage, foriegn intelligence services may target unclassified systems to further their intelligence missions.

6] Information Warfare :- Hired experts and professionals are used to launch attacks that lead to information warfare.

(a) Business to business (Corporate)
Motive :- To gain business advantage

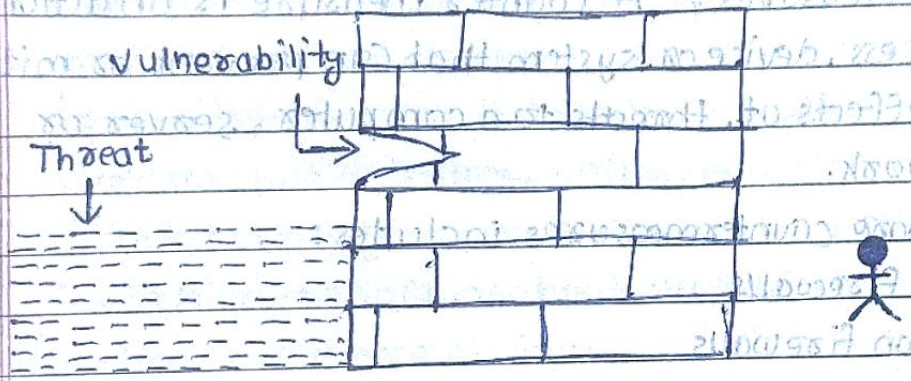
(b) Country to Country
Motives:- To leak secrets, to gain strategic advantage

7] Cyber terrorism : For some time, everything bad or perceived as bad on the internet fell into black hole known as cyber terrorism. Events such as hacking, political protests, actions by international terrorists, war time attacks on computers, denial of service attacks and trashing website come under cyber terrorism.

Attacks and Vulnerability :-

Vulnerability is a weakness in the security system; in procedures, design or implementation that might be exploited to cause loss or harm.

A Threat to a computing system is a set of circumstances that has the potential to cause loss or harm. To see a difference between threat and vulnerability, consider this figure



Here, a wall is holding water back. The water to the left of the wall is a threat to the man standing on right side of the wall. If water overflows the walls, then it will collapse, putting man's security in question. Also, if the water rises to or beyond the level of crack in wall, it will exploit vulnerability and harm the man.

A control is an action, device, procedure or technique that removes or reduces vulnerability.

Risks :-

Some security professionals describe relationship between security terms according to one of the following formulas:

Risk = Threat × Harm

Risk = Consequence × Threat × Vulnerability

Risk = Consequence × Likelihood

Risk = Consequence × Likelihood × Vulnerability

Risk of an organisation are evaluated by three distinguishing characteristics:

⇨ A loss associated with an event e.g.: disclosure of confidential data, lost time, lost revenues.

⇨ A likelihood (probability) that an event will occur.

⇨ A degree to which the risk outcome can be influenced i.e controls that will influence the event

□ Counter Measures :- A counter measure is an action, process, device or system that can prevent or mitigate the effects of, threats to a computer, server or network.

1] Software countermeasures includes:

⇨ Personal firewalls

⇨ Application firewalls

⇨ Anti-virus software

⇨ Popup blockers

⇨ Spyware detection / removal programs

2] Hardware counter measures include :-

⇨ Router, that can prevent IP address of an individual computer from being directly visible on the internet.

⇨ Biometric authentication systems

⇨ Physical restriction of access to computers and peripherals

⇨ Intrusion detectors

⇨ Alarms

3] Behavioural countermeasures include,

⇨ Frequent deletion of stored cookies & temporary files from Web browsers.

⇨ Regular scanning for viruses and other malware.

⇨ Regular installation of updates and patches for operating system

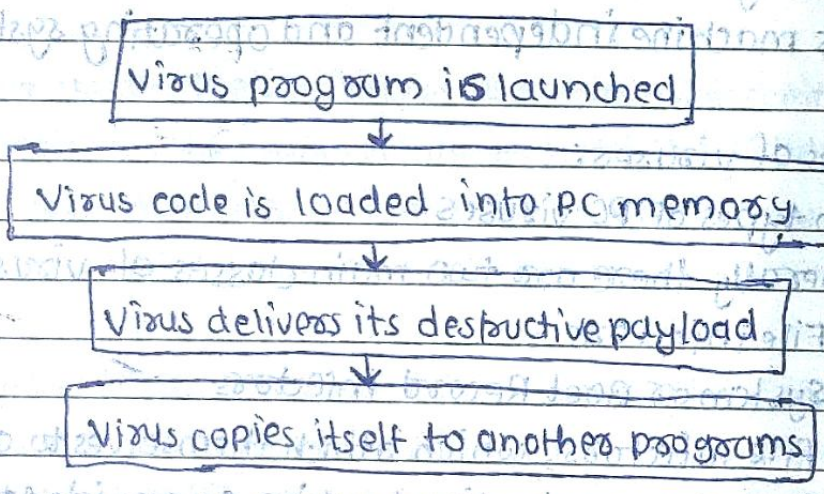
⇨ Refusing to click on links that appear within e-mail message

⇨ Refraining from opening email messages and attachments from unknown senders.
⇨ staying away from questionable websites.
⇨ Regularly backing up of data on external media.

1.8 Threats to security:

☐ Viruses and Worms:- Many web and network attacks from outside are done by adding malicious code such as viruses and worms. A computer virus attaches itself to a program or file enabling it to spread from one computer to another, leaving infections as it travels. A typical computer virus performs two functions:- First, it copies itself into previously uninfected programs or files. Second, it executes whatever instruction the virus author included in it.

Functional sequence of virus:



The functional logic of virus is as follows:
⇨ Search for a file to infect it
⇨ Open the file to see, if it is infected
⇨ If infected, search for another file to infect
⇨ Else, infect the opened file
⇨ Return control to the host program.

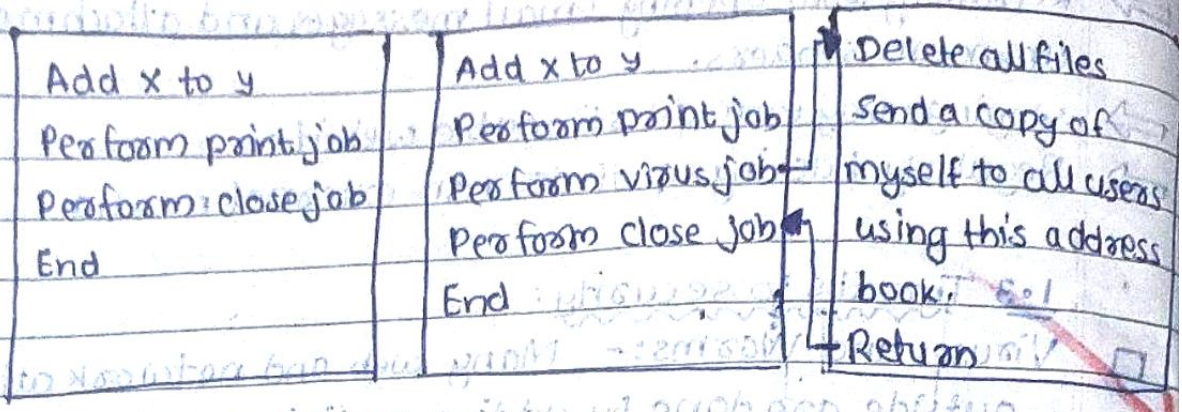


Fig:- structure of virus

⇒ Characteristics of virus

1) It is hard to detect.
2) It is not easily destroyed or deactivated.
3) It spreads infection widely
4) It can reinfect its home program or other programs
5) It is easy to create.
6) It is machine independent and operating system independent

⇒ Types of viruses:

1) Main types of PC viruses.

Generally there are two main classes of viruses

(a) File infectors
(b) System or Boot Record infectors

(a) File infectors, which attach themselves to ordinary program files. They can be direct action or resident.

* Direct Action Virus :- The main purpose of this virus is to replicate and take action when it is executed. When specific condition is met, the virus will infect the system and is in the directories that are specified in the AUTOEXEC.BAT File PATH.

* Resident virus :- A resident virus hides itself somewhere in memory, triggers itself when certain conditions are satisfied. This type of virus is permanent which dwells in RAM memory. Their functions : corrupting files & programs
Ex :- Randex, CMJ, Meve, MrKlunky, Vienna

The second category is system or boot record infectors.
Ex :- Brain, Stoned, Empire, Azusa, Michaelangelo. such viruses are resident viruses.

* Boot viruses :- These viruses infect floppy disk boot records or master boot record in hard disk. They replace boot record program, copying it elsewhere on the disk overwriting it.
Ex :- Form, Disk killer, Michaelangelo, Stone Virus

2) Stelth viruses :- These viruses use certain techniques to avoid detection. They may either redirect the disk head to read another sector instead of the one in which they reside.
Ex :- Frodo, Joshi, Whale, etc.

3) Polymorphic Virus :- A virus that can encrypt its code in different ways so that it appears differently in each infection. These viruses are difficult to detect.
Ex :- Involuntary, stimulate, Cascade, Pheonix, Evil, Proud, Virus 101

4) Fast and slow infectors :-

- Fast infector is a virus which, when it is active in memory, infects not only program when executed, but even those which are merely opened.
  Ex :- Dark Avenger, Frodo viruses
- Slow infector is used for a virus which it is active in memory, infects only file as they are modified.
  Ex :- Darth Vader virus

5) Companion virus :- A companion virus is one which, instead of modifying existing file, creates a new program (which is unknown to the user) gets executed instead of original program.
Ex :- Stator, Asimov. 1539, Terrax. 1069

6) Program viruses :- These infect executable program files, such as those which extensions like .BIN, .COM, .OVL, .DRV (driver), .SYS (system driver). The virus becomes active in memory, making copies of it and infecting files.
Ex :- Sunday, Cascade

7) Multipartite viruses :- A hybrid of Boot and Program viruses. They infect program files and when the infected program is executed, these viruses infect the boot record.
Ex :- Invader, Flip and Tequila

8) Macro viruses :- A macro virus is a type of a computer virus that infects macros within a document or template. When word processing or spreadsheet document is opened, the macro virus is activated and it infects the normal template.
ex :- Relax, Melissa-A, Bablas, 097M/Y2K, DMV, Nuclear, Word Concept.

9) Overwrite viruses :- Viruses of this kind is characterised by the fact that it deletes the information contained in the files that it infects, rendering them partially or totally useless. The only way to deal with this problem is to delete the infected file permanantly.
Ex:- Way, Tuj. Reboot, Trivial. 88. D

10) Directory virus :- It changes paths that indicate location of the file. By executing a program (with extension .EXE or .COM) which has been infected, you are unknowingly running a virus program. The original file or program has been already removed from original path where we are accessing it.

~~Ex:-~~

11) FAT virus :- This type of virus attack can be especially dangerous, by preventing access to certain parts of disk where important files are stored. Damage caused can result in information loss or entire directories are gone forever.

12) Worms :- A worm is a program which replicates itself. It can lead to negative effects on your system. They can be detected and eliminated by anti-viruses.
Ex:- PSW Bugbear.B, Lovgate.F, Trile.C, Sobig.D, Mapson

13) Logic bombs :- They are not considered viruses because they do not replicate. They are not programs in their own right but rather camouflaged segments of other programs. Their objective is to ~~meet~~ ~~casts~~ destroy data on the computer once certain conditions have been met. They are undetected until launched, but results are destructive.

⇨ Categories of viruses:

① Destructive viruses :- They cause
* Massive destruction i.e low level format of disk whereby any programs and data on disk is not recoverable.
* Partial destruction i.e erasing or modification of part of a disk
* Selective destruction i.e erasing or modification of specific files on the disk.
* Random havoc

② Non-destructive viruses :- They are intended to cause attention to the author or to harass the end users. Usually they display annoying messages.

⇨ Mechanism of virus infection into computer system:
A virus may enter into a system by an unsuspecting users who has been duped by the virus creator (covert entry) or it may directly enter by the creator (Overt entry).

Virus spreading mechanism:- A virus may reproduce itself by delaying its attack until it has made copies of it into other disks, (active reproduction) or it may depend entirely unsuspecting users to make copies of it and pass around (passive reproduction). It may also use combination of these methods.

Triggers of a virus attacks:- Attacks begin upon occurrence of certain event, such as
* On certain date / time of day / year
* At certain time of day
* When certain job is run
* After doning itself 'n' times
* When certain combination of keystrokes occur.
* When computer is restarted.

one way or another, the virus code must put itself into a position either when computer is turned on or specific program is run.

⇒ Components of viruses:

(1) Infector :- This is the section of the viral code, which infects some part of the system when triggered for the first time. That happens when virus enters the system first. The infector part may decide to infect a file system or system sector or an application.

(2) Replicator :- It is that section of the virus, which has the job of making the virus replicate or duplicate such that every time the viral code is triggered or executed, the virus gets chance to replicate. They are essential to decide strength of the virus.

(3) Payload :- This is a section, which can determine the amount of damage or harm a virus can cause to the system or its resources. Usually it is a direct implication of replicator. The higher the payload, the more easily the virus can overcome the system.

⇒ Virus Symptoms :-

* computer seems to be running slower than the normal.
* Floppy disk or hard disk is accessed suddenly without any reason. Program do unusual activities or do not work properly
* Files and folder disappear mysteriously or contain garbage
* System crashes often without any reason.
* Computer does not boot completely at all.
* System memory or disk space reduces without any logical reason
* Unusual error messages appear on the screen
* Programs take more time to load than normal
* Change in data/programs file sizes is observed.

⇨ Protection against viruses :- (Refer textbook for details)

* Education
* Backup and recovery procedures
* Isolate software libraries
* Implement software library management
* Develop a virus alert procedure
* Factors affecting level of protection :
  - The sensetivity of the data on your PCs
  - The number of personnel having access to your PC.
  - The security awareness of computer personnel
  - The skill levels of computer personnel
  - Attitude, Ethics and morales of computing personnel.

⇨ Golden rules for virus prevention :

* Always keep backup of your data / programs.
* Keep floppies write protected.
* Do not copy anything in your system from any unknown source
* Restrict the use of machines to only authorised users.
* Never download mail attachments, unknown content from internet.
* Even after using these precautions, if the virus creeps into your system, it can be detected in various ways apart from using a virus scanner for it.

- Worms :- The first widespread internet worm appeared in 1988. A graduate student at Cornell University, Robert Morris, created a worm program that exploited several vulnerabilities and released it to the internet. It impaired over 6000 internet connected computers and caused hundreds of thousands of dollars as clean up cost.

In 2001, "Code Red" worm spread to over 300000 machines in just 14 hours. According to computer economics, the damage associated with this worm came to $3.72 billions.

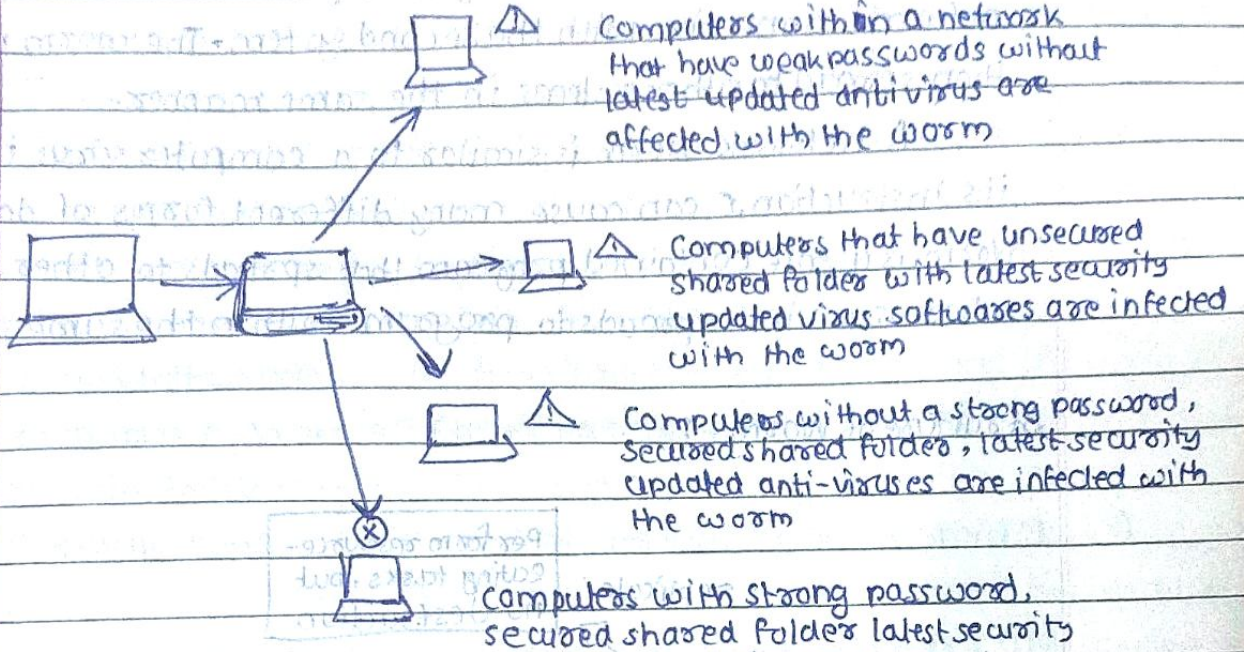


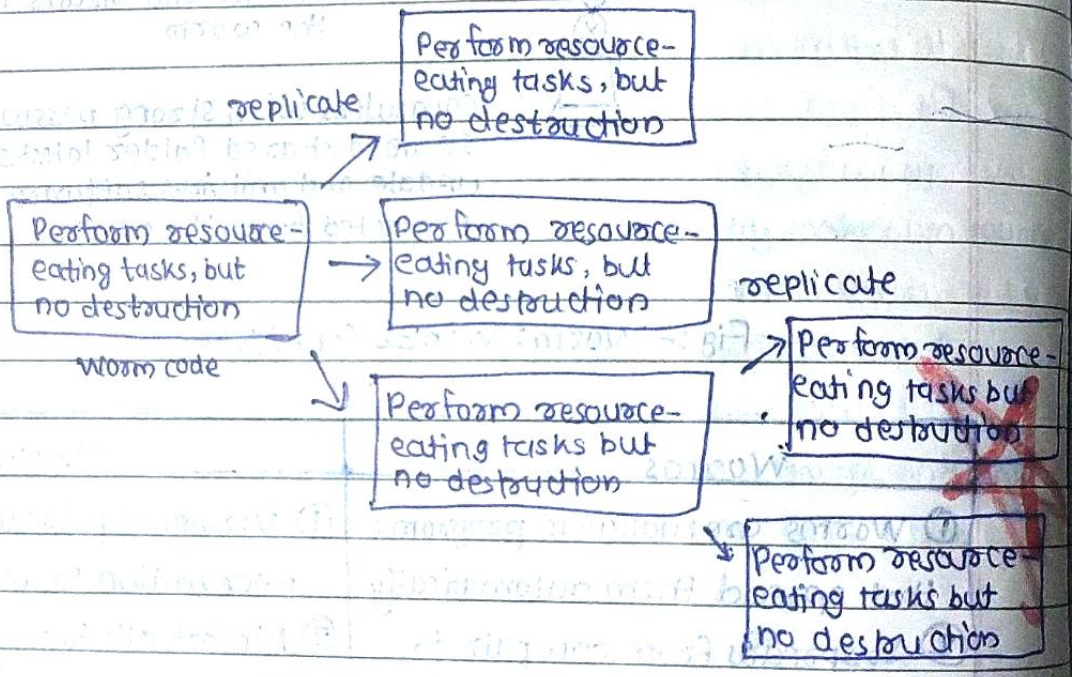
Fig :- Worm: Win32 Conficker

Worms	Viruses
① Worms are malicious programs that spread them automatically	① Viruses require some human intervention to spread.
② It spreads from computer to computer, but it has the capabability to travel without any human intervention.	② Almost all viruses are attached to an executable file, means virus resides in computer and activates when malicious program is opened.
③ Worms spread faster than viruses	③ Viruses slowly affect the system.
④ Worm doesnt need a host file to move from system to system	④ Virus does need host file to move from system to system
⑤ Code Red, Nimda, Worm32. Mydoom AXEMM	⑤ Ninja, Predator, Angelina, Iloveyou, etc.

Network worm:- A name for a program or command file that uses a computer network as a means for causing damage to the computer systems. From one system, a network worm may attack a second system by first establishing a network connection with the second system. The worm may then spread to other systems in the same manner.

A network worm is similar to a computer virus in that its instructions can cause many different forms of damage. Worm is a self contained program that spreads to other systems whereas a virus spreads to programs within the same system.

Structure of Worms:



Structure of worm

Worms have three main parts:

① Attack Mechanism :- Worms exploit one or more specific vulnerabilities in a computer system. Buffer overflow vulnerabilities compose of majority of vulnerabilities that worms exploit.

(2) Payload :- The payload is the part of the worm code that performs malicious actions against the compromised host. Some worms have no payloads, so they simply spread themselves and drain resources. The payload may also search the computer for data such as confidential data and sends it to main server so that the worm's authour may collect it.

(3) New Target selection :- Once worm's code is executed on an attacked system, it attempts to spread again. To do this, worms must locate target computers that are vulnerable to its attack mechanisms. The mechanism used varies in sophistication

Examples of Worms: (refer textbook for details)

* Code Red Worm
* Mobile code

☐ Types of attackers:

* Insiders
* Intruders
* Computer criminals
* Cyber terrorists
* Hired professionals

* Insider :- Insider is a person who belongs to the said organisation and launches security threats and attacks from inside.

- Motives : side business, anger, revenge, favours, obligation
- Opportunity : Definitely, being insider knows configuration, cyan passwords, authentication and access control policies and mechanisms.
- Methods : salami attacks, information leakage, Trapdoor etc.
- Control : It is difficult to detect an inside attack. The controls typically applied are Repine, an IDS to check the system and user behaviour also maintaining transaction logs and audit trails help in tracking who did what, when and from where.

* Intruders :- The person who is not belonging to the organisation (an outsider) who tries to intrude and launch security threat and attacks from outside.
  - Motives :- Money, Hired, Fun, Psychic
  - Opportunity :- Less, but uses spying and wiretapping to gain information and access.
  - Methods :- Any suitable interception, interruption, modification or fabrication method.

Intruders are of three types :-

1. Masquerader :- A user who does not have authority to use computer, but penetrates into a system to access a legimate users' account is called as masquerador. It is generally an external user.
2. Misfeasor :- There are two possible cases for an internal user to be called as misfeasor :
   1. A legimate user, who does not have access to some applications, data or resources, access them
   2. A legimate user, who has access to some applications, data or resources, misuses these privilages.
3. Clandestine user :- An internal or external user, who tries to work using previlages of a supervisor user to avoid auditing information being captured and recorded is called as a clandestine user.

Intruders	Insider
1. Extremely patient as time consuming	1. More dangerous than outsiders
2. Outsiders	2. Insiders
3. Keep trying attacks till success	3. Cause immidiate damage to organisation
4. Individual or small group of attackers	4. More in numbers who are directly or indirectly access to the organisation.

(5) Next level of this group is script writers i.e elite hackers. There are three types: (a) Masquerader (b) Misfeasor (c) Clandestine user are misuse of access given by insiders.	(5) They may give remote access to organisation

* Computer Criminals :- Convicted computer criminals are people who are caught and convicted of computer crimes such as breaking into computers or computer networks. Some of the characteristics of them are:
  - Amateurs :- They are normal computer professionals who happen to take advantage of some opportunity or weakness and so getting involved into the computer crimes as side activity.
  - Hackers & crackers :- They are specialist in hacking and cracking the password. They are hired by the organisation itself and are said to be doing ethical hacking. They can also be hired by computer criminals or competitors.
  - Career criminals :- They are those who perform computer crimes as their main activity or business. They earn their living by performing computer crimes.

* Cyber Terrorists :- The person or organisation that involves itself in terrorising through computer ~~and~~ networks and internet are known as cyber terrorists. The ideology of spreading terror and launching attacks through cyber space is called as cyber terrorism.
  - Motives :- Ideology, spread and terror.

* Hired professionals :- Hired experts and professionals are used to launch attacks that lead to information warfare.
  - Motive :- To gain business edge (profitability), to leak secrets and to gain strategic advantage.

☐ Information warfare Avenues of attack :-
Today many nations have developed the capability to conduct information warfare. It is a warfare conducted against information and information processing equipment used by an adversary. It falls into the highly structured threat category. In information warfare, the key targets include the military forces and the various infrastructures that a nation relies on for its daily existance.

Avenues of attack : A computer system can be targeted by the attacker, or it can be the opportunistic target.
① An attacker can target a computer system for political reason.
② An attack against a target of opportunity is conducted against a site that has hardware or software vulnerable to a specific exploit.
③ Targeted attacks are more difficult and take more time than attacks on target of opportunities.

The steps in an attack :- The steps an attacker takes in attempting to penetrate a targeted network are similar to the ones that a security consultant performing a penetration test would have take.

① The attacker will need to gather as much as information about the organisation as possible.
② The first step in an technical part of an attack is often to determine what target systems are available and active.
③ An attacker can search for known vulnerabilities and tools that exploit them, download the information and tools, and use them against a site.
④ There are many different ways a system can be attacked, generally gathering information about the target and exploits based on the information about the system.

Minimizing possible avenues of attack:
① The administration should ensure that all patches for the operating system and the applications are installed to minimize possible attacks.
② The administrator must limit the services running on the system.
③ The administrator must provide as little information about the organisation and its computing resources as possible.

☐ The steps in an attack:
(This can be referred by considering same topic on pg-26)

☐ Types of Attacks:
① Attacks on specific software: These system are generally possible because of either an oversight in the code or because of a flaw or bug in the code.
② Attacks on a specific service or protocol: These are attempts to either take advantage of a specific feature of the service/protocol or the use the service/protocol in a manner for which it was not intended.

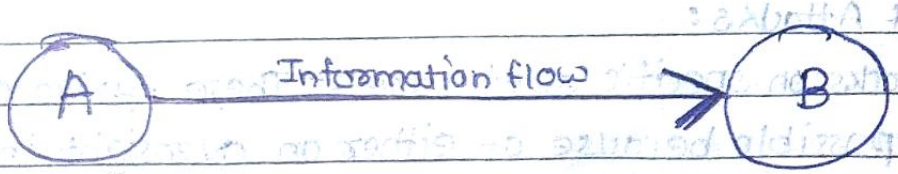
Exploits :- An exploit is a piece of software, a chunk of data, or sequence of commands that takes advantage of a bug, unanticipated behaviour to occurs on computer software, hardware. This also includes gaining control of computer software, hardware. This also includes gaining control of computer system or denial of service attacks.

Eavesdropping :- It is the act of listening private conversation. Even machines which have no contact to the outside world can be used for it via maintaining faint electromagnetic transmissions generated by hardware such as TEMPEST

1.4 Security Attacks :- security attack is any action that compromises the security of information owned by an organisation. Attacks on security of computer can be characterised best by viewing how the computer functions when sending and receiving information.

There are four types of security threats to consider:

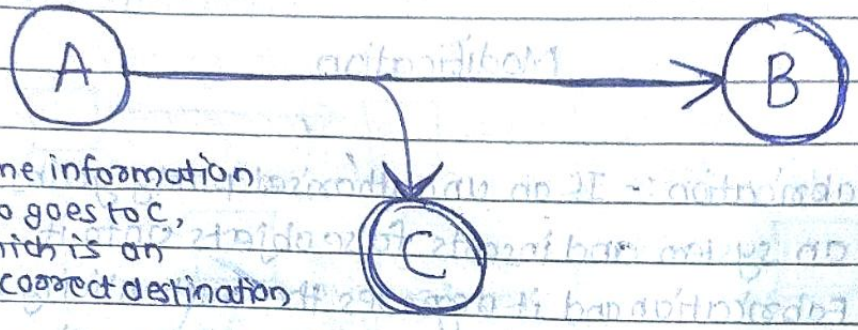
1. Interception
2. Interruption
3. Modification
4. Fabrication



Information source — Information destination

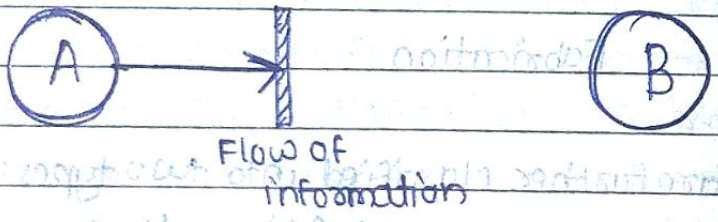
Normal flow

① Interception :- Interception occurs when any unauthorised unit gains access to an asset. That attack means that there is no privacy, therefore it is an attack on confidientiality. The unauthorised unit or party could be an individual, a program or even another computer. The figure below shows the nature of interception.



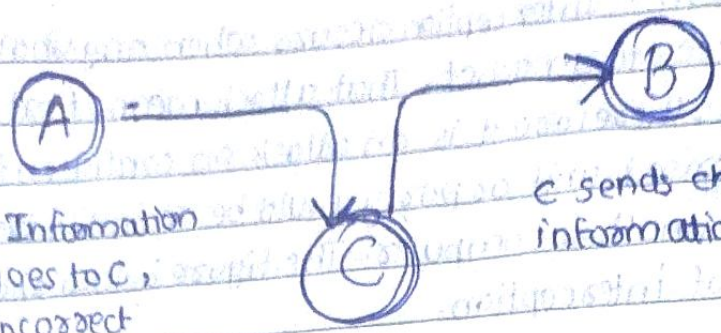
Interception

② Interruption :- In an interruption, an asset of a system becomes lost, destroyed, unavailable or unusable. This is an attack on availability of a system. The below figure shows how an interruption can occur.

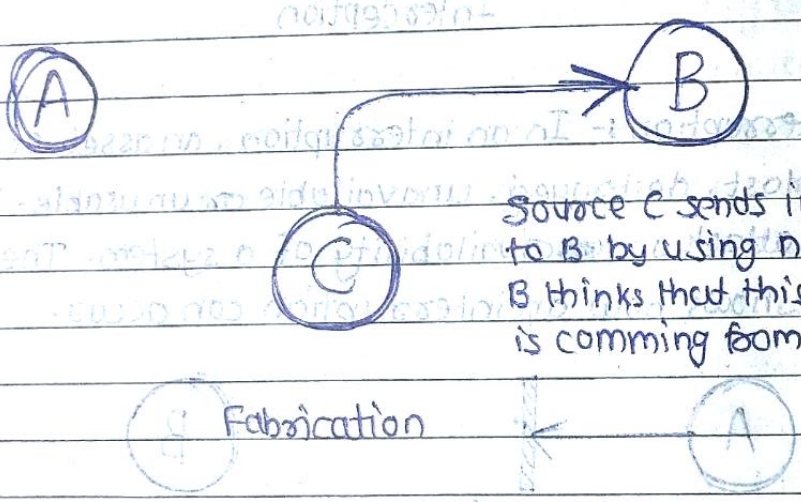


Interruption.

③ Modification :- If an unauthorised party gains access to the system and makes some changes to it, then this tampering is known as modification. This modification is an attack on the integrity of the system or the organisation. The figure on next page depicts this attack.

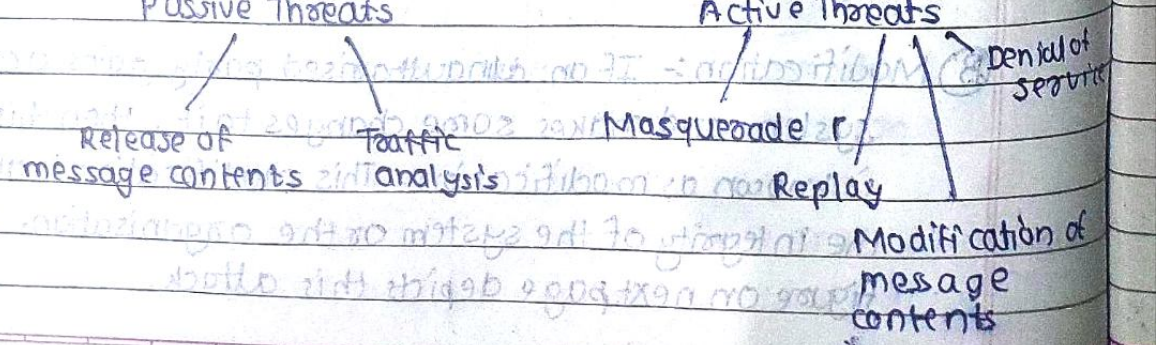


④ Fabrication :- If an unauthorised party gains access to an system and inserts false objects onto it, this is Fabrication and it degrades the authenticity of the system. The below figure reflects this information.



These attacks are further classified into two types:

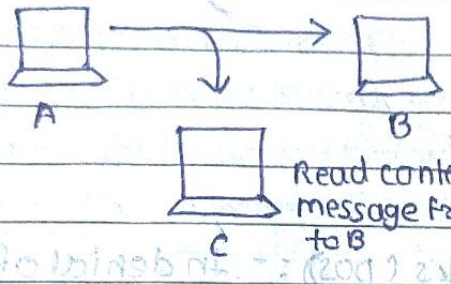
* Passive Attacks
* Active attacks



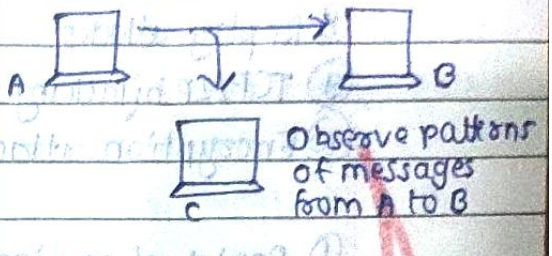
Read

Passive attacks :- Passive attacks are those wherein the attacker indulges in eavesdropping or monitoring of data transmission. The goal of attacker is to obtain information that is being transmitted. These are harder to detect as attacker does not perform any modification of data.

- Release of message contents :- Outsider learns content of transmission.



Release of message contents



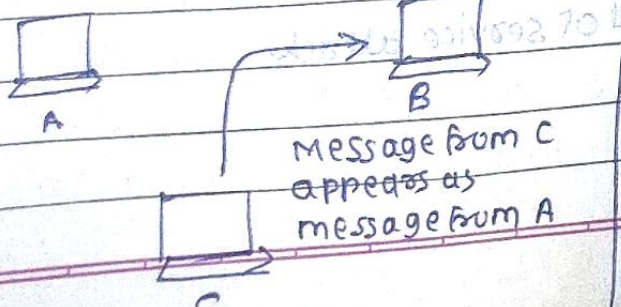
Traffic Analysis

- Traffic analysis :- By monitoring frequency and lengths of message, even encrypted, nature of communication can be guessed.

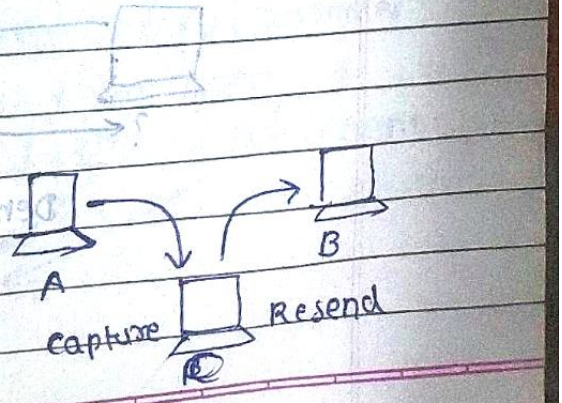
Read

Active attacks :- In ~~atta~~ active attacks, the contents of original message are modified in some way or create a false message. These attacks cannot be prevented easily.

- Masquerade :- Pretending to be a different entity
- Replay :- Capture of data unit and retransmission for an unauthorised effect
- Modification of messages
- Denial of service



Masquerade

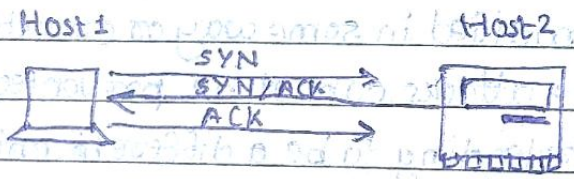


Replay

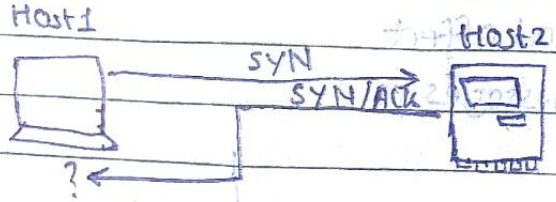
Now we will discuss some more attacks in detail:

1. Denial of service attacks (DOS)
2. Distributed Denial of service attacks (DDOS)
3. Backdoors
4. Trapdoors
5. Sniffing
6. Spoofing attack
7. Man-in-the-middle attack
8. Replay attacks
9. TCP/IP hijacking
10. Encryption attacks.

① Denial of service attacks (DOS) :- In denial of service attacks, the user sends several authentication requests to the server filling it up. All requests have false return addresses, so the server can't find the user when it tries to send authentication approval. The server waits for some time before closing the connection. When it closes the connection the attacker sends new batch of forged request and same process repeats.



Connection established



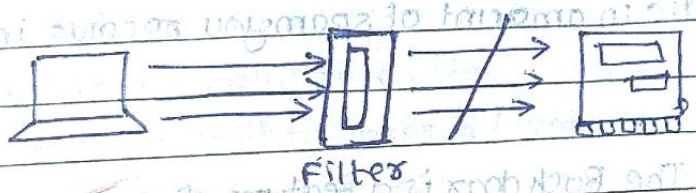
Denial of service attack.

Read all the attacks

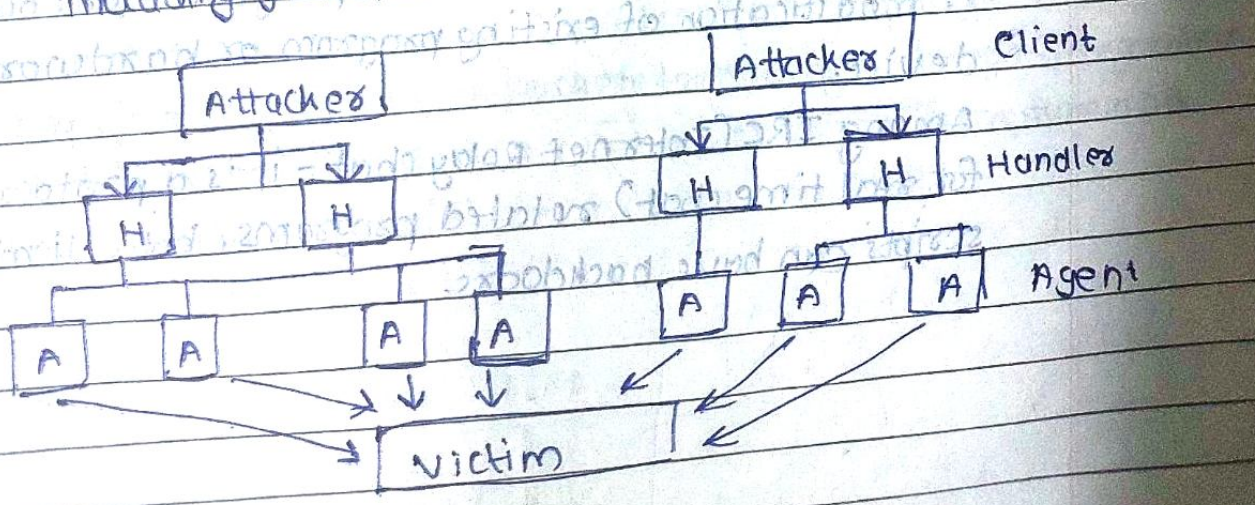
Example of DOS attack:

* SYN flooding is an example of DOS attack that take advantage of the way TCP/IP networks were designed to function. SYN flooding utilizes the TCP three way handshakes that are used for establishing a connection between two systems.

How to block a denial of service attack :- One of the ways to block DOS attack is to use a "sniffer", on a network before a stream of information reaches a site's Web servers. The filter can look for suspicious patterns in message stream. If it continues to be suspicious, filter blocks messages.



(2) Distributed Denial of service attacks:- It is the distributed version of DoS attacks. In DDOS, an attacker may use your computer to attack another computer. By taking advantage of security vulnerabilities or weakness, an attacker can take control of your computer. This attack is distributed because, attacker uses multiple computers, including yours, to launch the DOS attack.

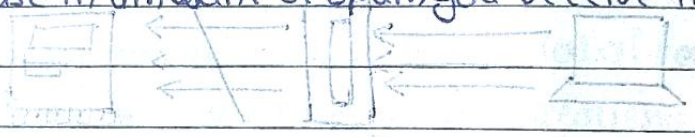


How do you avoid being part of the problem?

* Install and maintain anti-virus software
* Install a firewall, and configure it to restrict traffic comming into and leaving your computer
* Applying email filters may help you to manage unwanted traffic

How do you know if the attack is happening?

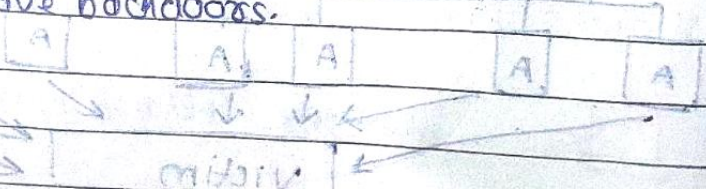
* Unusually slow network performance
* unavailability of a particular website
* inability to access any website
* Dramatic increase in amount of spam you receive in your account



③ Backdoors :- The Backdoor is a feature of a program that can be used to make it act in some way that the person who is running it did not intend.

A backdoor in a computer system is a method of bypassing normal authentication, securing remote access to a computer, obtaining access to plain text, and so on, while remaining undetected. The backdoor may take form of the installed program, or it could be a modification of existing program or hardware device.

Among IRC (Internet Relay chat - it is a protocol designed for real time chat) related programs, bots, clients and scripts can have backdoors.



④ Trapdoors :- A trap door is a secret entry point in a program that allows someone that is aware of the trap door to gain access without going through usual security access procedure. Trap doors have been used legimately by programmers to debug and test progoams, some of the legimate reasons for trap doors are:

- Intentionally leaves them for testing, and makes testing easier.
- Intentionally leaver them for covert means of access
- Intentionally leaves them for fixing bugs.

Trap doors can be almost impassible to remove in a reliable manner. Often reformatting the system is the only sure way.

⑤ Sniffing :- A network sniffer is a software or hardware device that is used to observe traffic as it passes through a network on shared broadcast media.

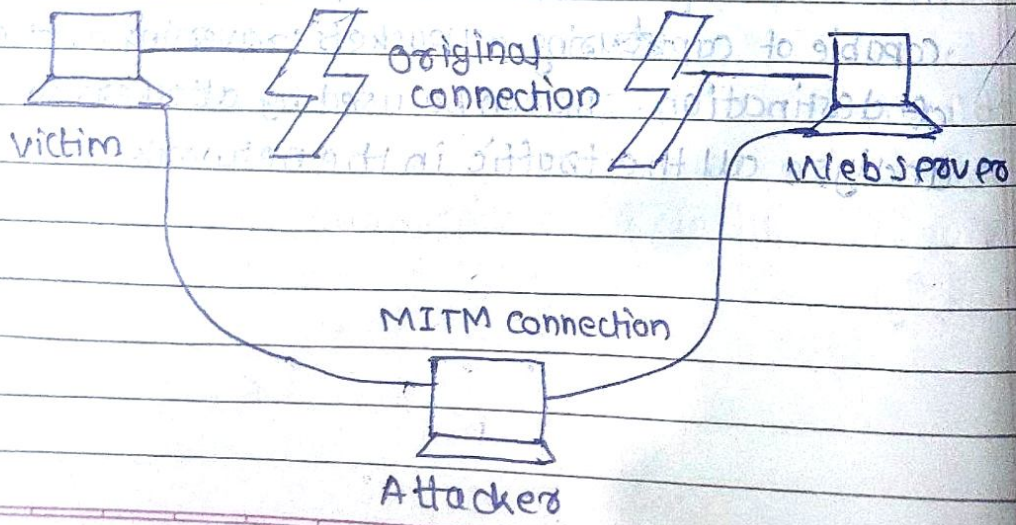
* Network sniffers can observe traffic and can also modify it. They can be used by attackers to gather information that can be used in penetration attempts.
* A packet sniffer, sometimes referred to as a network monitor or network analyser, can be used legimately by a network or system administrator to monitor and troubleshoot network traffic. Typically, it only captures the packets that were intended for the machine only. However when placed into promiscous mode, it is capable of capturing all packets traversing a network, regardless of destination. This can be used by attackers to capture and analyse all the traffic in the network.

⑥ Spoofing attack :- A spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage. The attacker must monitor the packets sent from sender to receiver and then guess sequence number of packets. Then the attacker knocks out sender with a SYN attack and injects his own packets, claiming to have address of sender.

Types of spoofing :- (Refer textbook for details)

* URL spoofing and phising
* Referrer spoofing
* Spoofing of file sharing networks
* Caller ID spoofing
* Email address spoofing
* Login spoofing

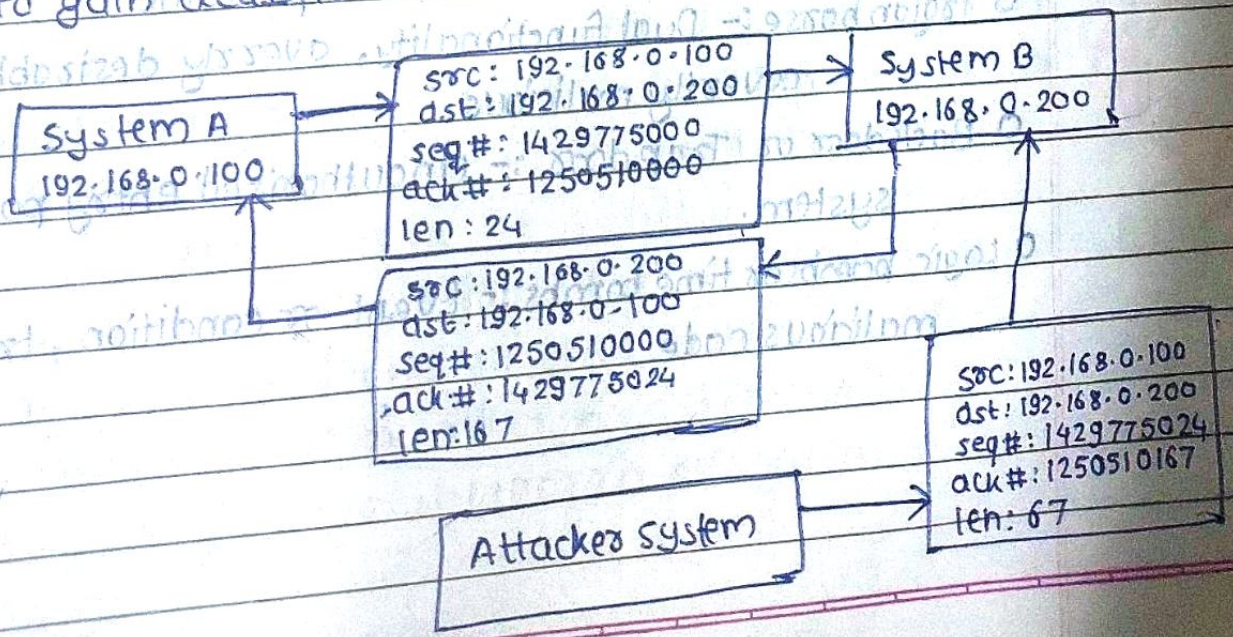
⑦ Man-in-the-middle attack :- The man-in-the-middle attack is a form of active eavesdropping in which attackers make independent connections with the two victims, making them believe they are talking to each other privately. In fact the conversation is controlled by hacker itself. It is abbreviated as MITM.



MIIM attack is also known as :
* Bucket-brigade attack
* Fire brigade attack
* Monkey-in-the-middle attack
* session hijacking
* TCP hijacking
* TCP session hijacking

(8) Replay attacks :- A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudently repeated or delayed. This is carried out either or by an adversary who intercepts the data and retransmits it, possibly as a part of a masquerade attack by IP packet substitution.

(9) TCP/IP hijacking :- TCP/IP hijacking and session hijacking are terms used to refer to the process of taking control of an already existing session between a client and a server. TCP session hacking is when a hacker takes over a TCP session between two machines. Since most authentications only occur at the start of TCP session, this allows the hacker to gain access to the machine.



(10) Encryption attacks :- Encryption is the process of transforming plaintext into an unreadable format known as cipher text using a specific technique or algorithm. Cryptographic attacks are designed to subvert the security of cryptographic algorithms, and they are used to attempt to decrypt data without prior access to the key. They are part of cryptanalysis, which is the art of deciphering encrypted data.

1.5 : Malware :- Malware or malicious code is defined as the piece of program code that causes loss or harm to the computing system, degrading and disputing the functionality of services provided by the system.

It may include computer viruses, worms, Trojan horses, spyware, dishonest ad ware, crime ware, most rootkits and other malicious and unwanted softwares.

The malware can be classified as follows :

- Virus : Infectious, Parasitic
  1) Transient
  2) Resident
- Worm :- Infectious, standalone, Non-parasitic
- Trojan horse :- Dual functionality, overtly desirable, covertly malicious
- Backdoor or Trapdoor :- Unauthorised entry point in the system.
- Logic bombs or time bombs :- Event or condition, triggered malicious code

Q

A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. For example, a programmer may hide a piece of code that starts deleting files, should they ever be terminated from the company.

Logic bombs, unlike viruses or Trojans, are type of malicious softwares that is deliberately installed, generally by an authorised user. A logic bomb is a piece of code that sits dormant for the period of time until some event invokes its malicious payload.

Logic bombs are difficult to detect because they are often installed by authorised users, and in particular, have been installed by administrators who are also often responsible for the security. This demonstrates the need of seperation of duties and a periodic review of all programs and services that are running.

THE END