NIS

Network and Information Security

&

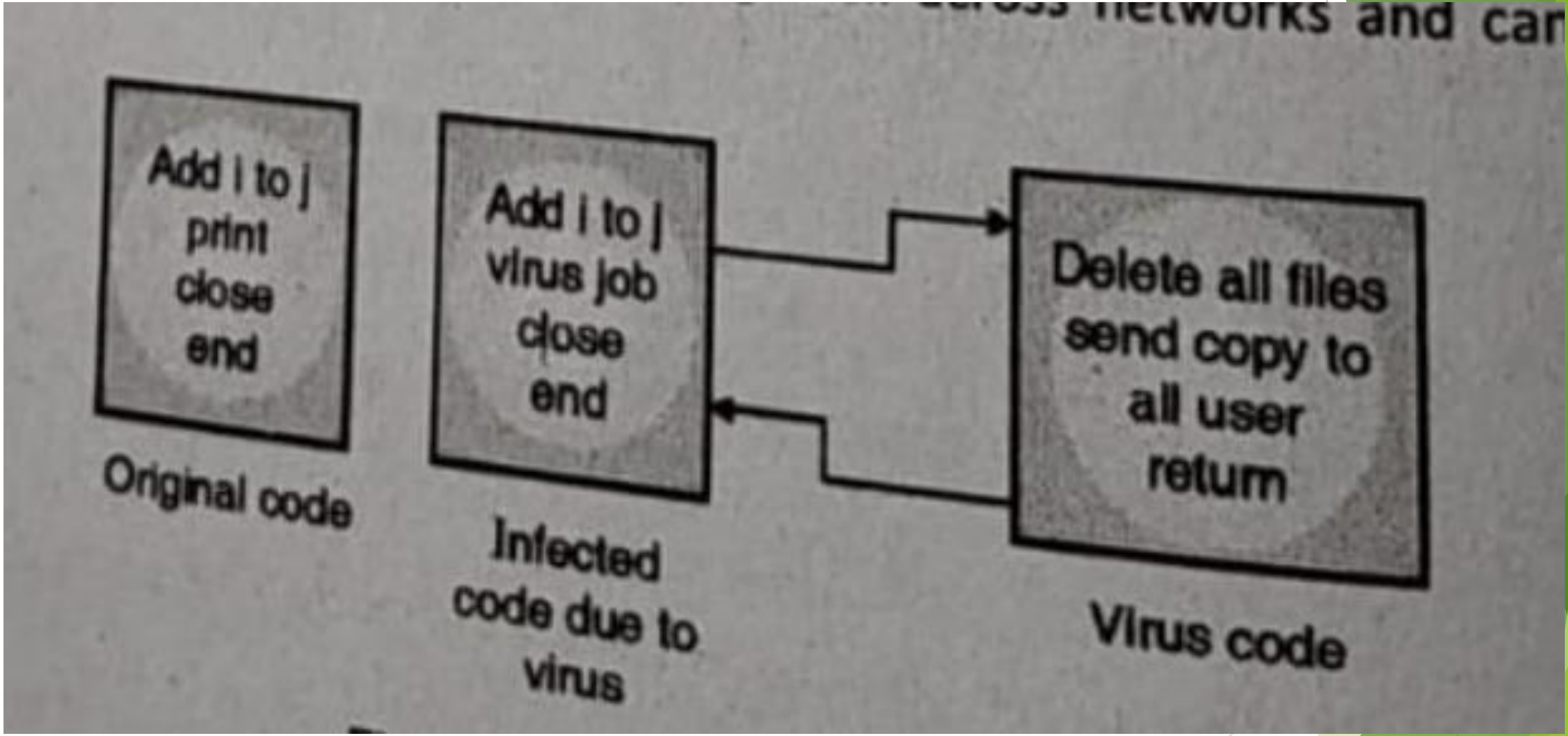
SIC

Security in Computing

Virus

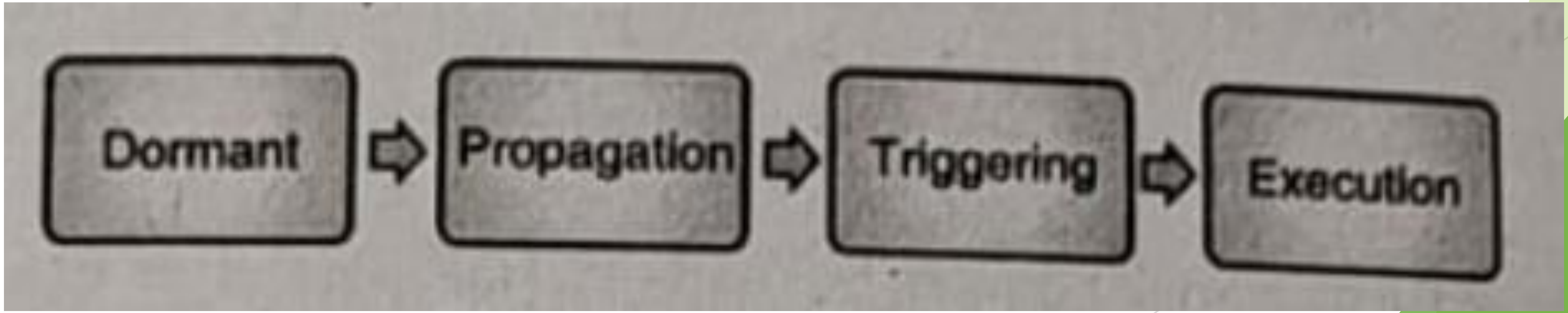
- A virus is a code that attaches itself to another code which causes damage to the computer system
- It is a piece of code which is loaded onto the computer without individuals knowledge and runs against their wishes.
- It can replicate them
- Any simple virus can be dangerous because it will quickly use all available memory space and bring the system to an halt.
- Whereas, dangerous viruses are capable of transmitting itself across networks and can be able to avoid security systems.

Virus


networks and car
Add i to j
print
close
end
Original code
Add i to j
virus job
close
end
Infected code due to virus
Delete all files
send copy to
all user
return
Virus code

Phases of Viruses

- During its lifetime, a typical virus goes through the following four phases:-
  - **Dormant Phase:-** The virus is idle and eventually activated by some event
  - **Propagation Phase:-** The virus places are identical copy to itself into other programs or into certain system areas on the disk
  - **Triggering Phase**:- The virus is activated to pearform the function for which it was intended.
  - **Execution Phase**:- The function is performed



Types of Virus

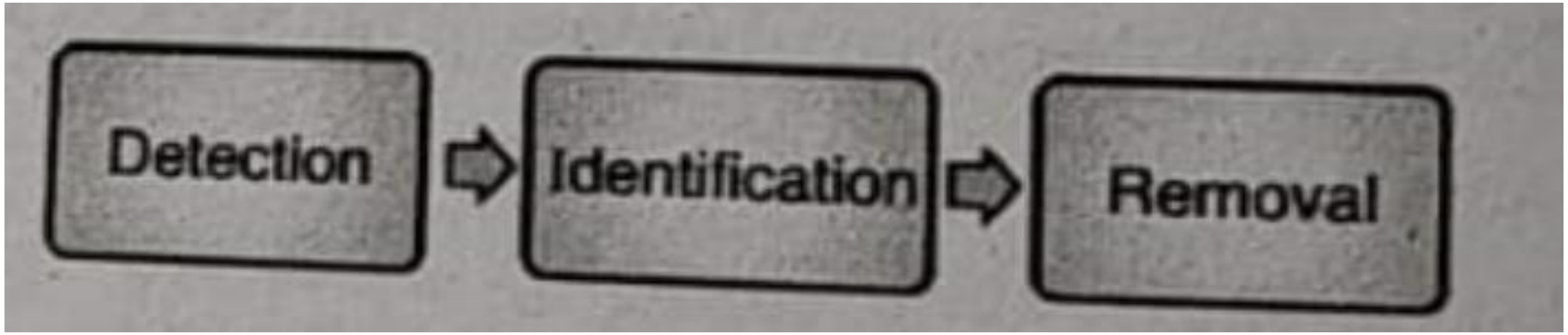
- **Parasitic Virus**:- It attaches itself to executable code and replicates itself. When the infected code is executed, it will find other executable code or program to infect.
- **Memory resident virus**:- This type of virus lives in the memory after its execution. It inserts themselves as a part of operating system or application and can manipulate any file that is executed, copied or moved.
- **Boot Sector Virus:-** This type of virus infects the boot record and spread through a system when system is booted from disk containing virus
- **Overwriting Virus:-** This type of virus overwrites the code with its own code.
- **Macro Virus:-** These viruses are not executable,it affects Microsoft Word like documents. They can spread through emails.

Types of Virus

- **Companion virus:-** This is the virus which creates a new program instead of modifying an existing file.
- **Email Virus:-** Virus gets executed when email attachment is open by recipient. Virus send itself to everyone on the mailing list of the sender.

Dealing with virus

- Preventing the virus is always a good option.
- There is no direct way to test/ find the hidden code but we can attempt to detect, identify and remove viruses.



- **Detection**:- Find out the location of virus
- **Identification** :- Identify the specific virus that has attached.
- **Removal** :- After identification, it is necessary to remove all traces of the virus and restore the affected file to the original state with the help of anti-virus

Worms

- Worm is a special type of virus that can replicate itself and use memory, but cannot attach itself to another program.
- Antivirus software and procedures can reduce the maximum portion of the threat. Generally, viruses and worms are non-discriminating threats that are released on the internet in a great fashion and are not targeted at a specific organization.
- When they are released, they are typically high visible once released, so they aren’t the best tools where the secrecy is important in highly standard attacks.

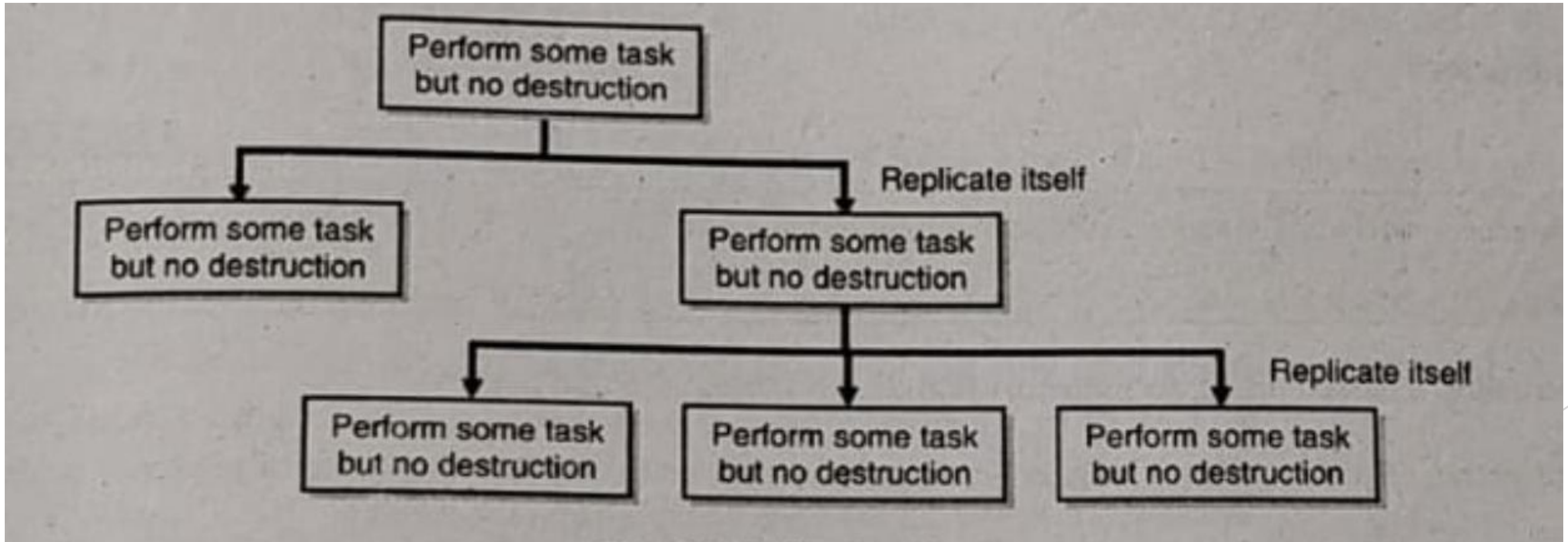

Perform some task but no destruction
Perform some task but no destruction
Replicate itself
Perform some task but no destruction
Perform some task but no destruction
Perform some task but no destruction
Replicate itself
Perform some task but no destruction

Fig. 1.3.4 : Worm code

Difference between Worm and virus

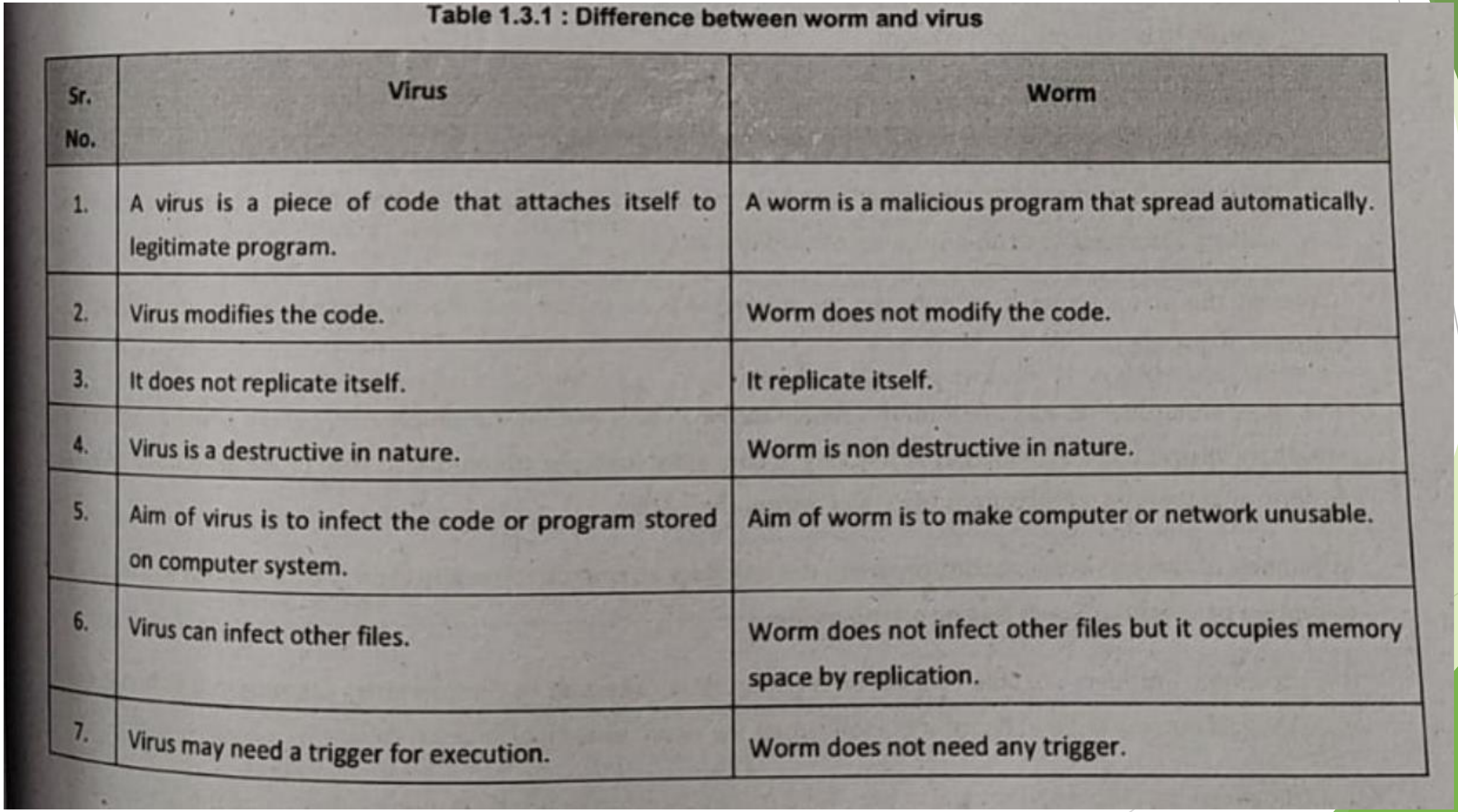


Table 1.3.1 : Difference between worm and virus

Sr. No.	Virus	Worm
1.	A virus is a piece of code that attaches itself to legitimate program.	A worm is a malicious program that spread automatically.
2.	Virus modifies the code.	Worm does not modify the code.
3.	It does not replicate itself.	It replicate itself.
4.	Virus is a destructive in nature.	Worm is non destructive in nature.
5.	Aim of virus is to infect the code or program stored on computer system.	Aim of worm is to make computer or network unusable.
6.	Virus can infect other files.	Worm does not infect other files but it occupies memory space by replication.
7.	Virus may need a trigger for execution.	Worm does not need any trigger.

Trojan Horse

- Trojan horse is a hidden piece of code, it allows an attacker to obtain confidential data.
- Main purpose of Trojan Horse is to reveal confidential information to an attacker.
- For example:- Trojan Horse can hide in code for login screen. When the user enters the user id and password, the trojan horse captures the details and transfer it to the hacker without knowledge of authorized user.
- The attacker then can use the information to gain the access to the system.

Intruders

- An intruder is a person who enters the territory that does not belongs to that person
- The objective of the intruder is to gain access to a system or to increase the range of privileges accessible on a system.
- This is one of the most publicated threats to security. There are three classes of intruders:-
  - **Masquerader**:- An individual who is not authorized to use the computer and who enters a systems access controls to use a legal user's account
  - **Misfeasor**:- A legitimate user who accesses data, programs or resources for whom these access is not authorized , or who is authorized for such access but misuse his or her privilege
  - **Clandestine/ Secret User**:- An individual who hold managerial control of the system and uses this control to avoid auditing and access controls or to suppress audit collections
- Generally, the masquerader is an outsider, Misfeasor is an insider and Secret User can either be insider or outsider.

Insider

- Insiders have the access and necessary knowledge to cause immediate damage to an organization. Hence, Insiders is more dangerous than outside intruders.
- Many securities are designed to protect the organization against outside intruders and so they lies at the boundary between the organization and the rest of the world.
- Insiders may already have all the access to carry out criminal activity like fraud. Also frequently the insiders have knowledge of the security systems in place and will be better able to avoid detection.
- Employees are not the only insiders within the organization but there are number of other individuals who have physical access to facilites like contractors or partners, may not have physical access to the organizations facilities but may also have access to computer systems and networks

Comparison Between Intruders and Insiders

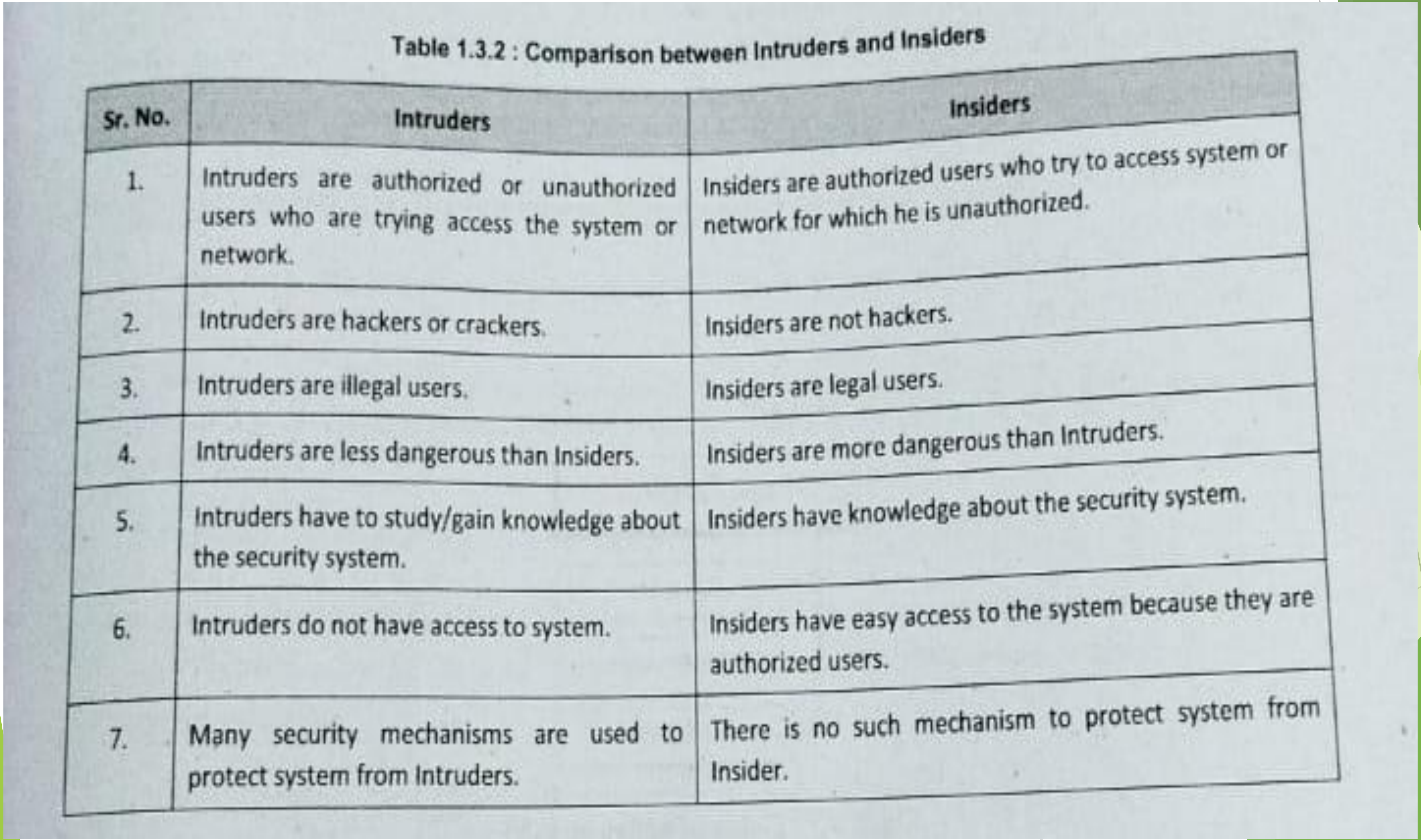
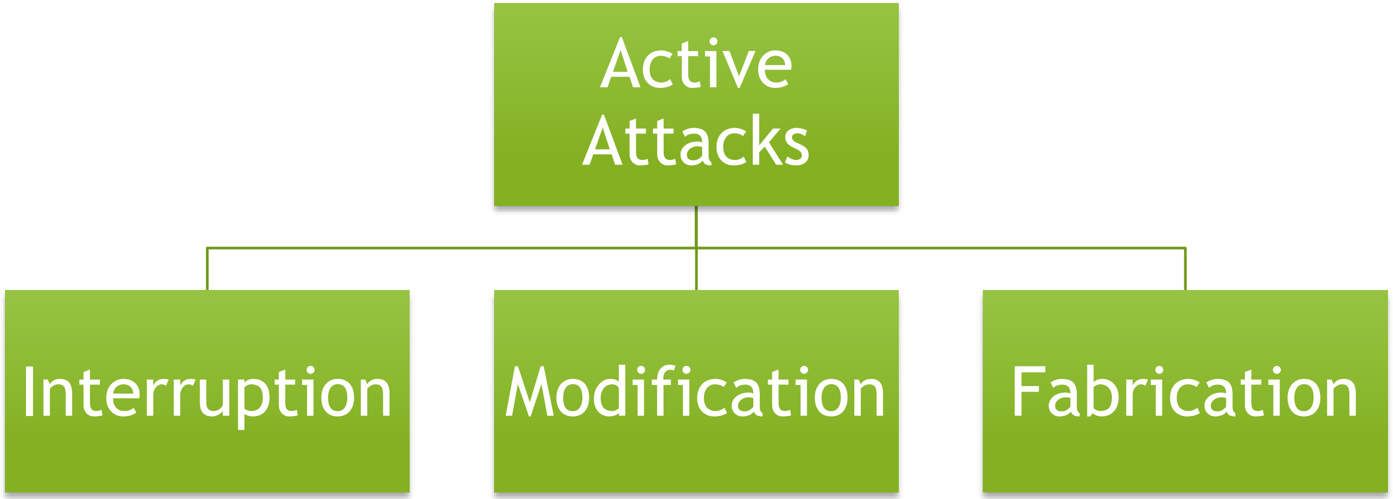


Table 1.3.2 : Comparison between Intruders and Insiders

Sr. No.	Intruders	Insiders
1.	Intruders are authorized or unauthorized users who are trying access the system or network.	Insiders are authorized users who try to access system or network for which he is unauthorized.
2.	Intruders are hackers or crackers.	Insiders are not hackers.
3.	Intruders are illegal users.	Insiders are legal users.
4.	Intruders are less dangerous than Insiders.	Insiders are more dangerous than Intruders.
5.	Intruders have to study/gain knowledge about the security system.	Insiders have knowledge about the security system.
6.	Intruders do not have access to system.	Insiders have easy access to the system because they are authorized users.
7.	Many security mechanisms are used to protect system from Intruders.	There is no such mechanism to protect system from Insider.

Types of Attack

- Attack is a path or way by which attacker can gain the access to your computer system without your knowledge
- Attacks are grouped into two types:- Active or Passive
- **Active Attack** :- In Active Attack, the contents of the original message are modified in some way. These attacks cannot be prevented easily



Active Attacks

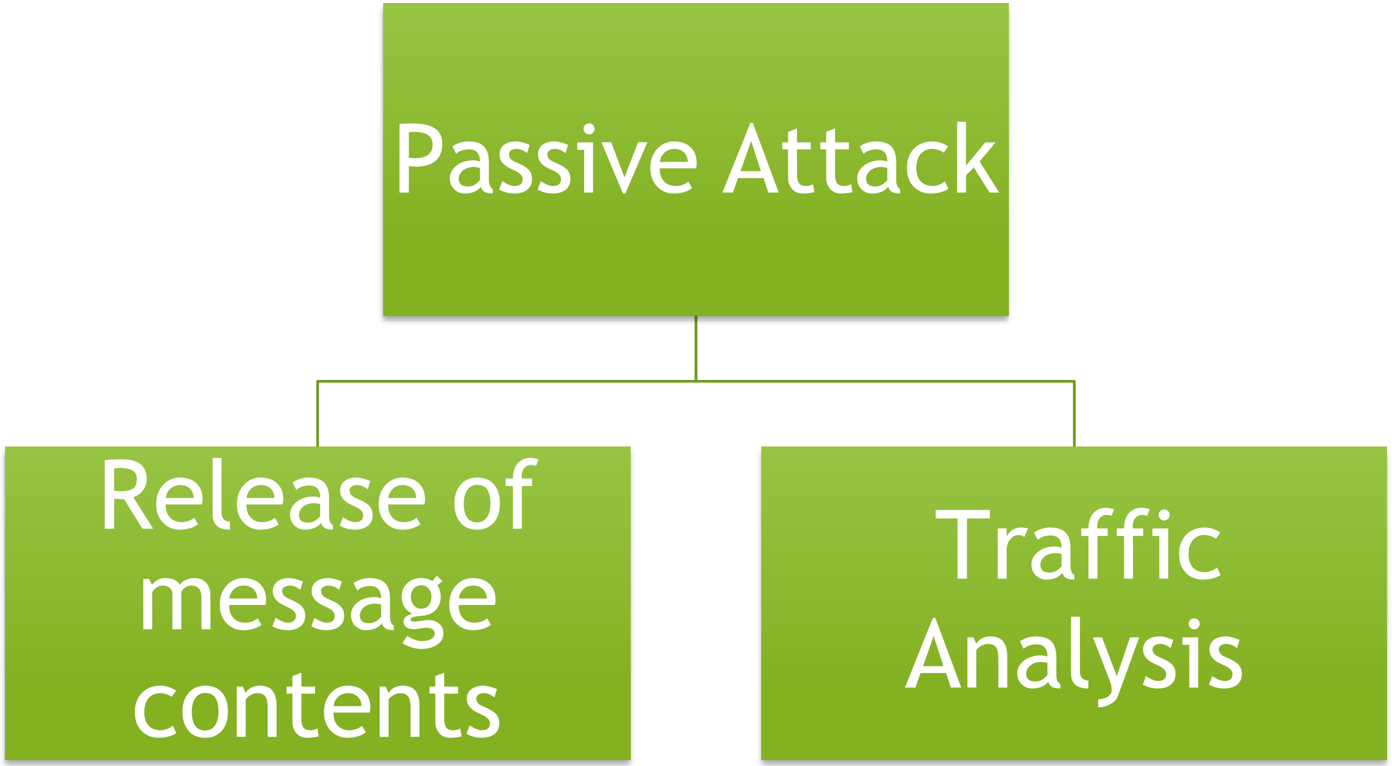
Interruption

Modification

Fabrication

Types of Attack

- **Passive Attack** :- Passive attacks are those where attackers aims to obtain the information that is in transit. In passive attack, attacker does not involve any modification to the contents of an original message.



Passive Attack

Release of message contents

Traffic Analysis

Thank you so much for hearing with Patience