SAHYADRI
COLLEGE OF ENGINEERING & MANAGEMENT
An Autonomous Institution
MANGALURU

Department of Information Science & Engineering

CRYPTOGRAPHY AND NETWORK SECURITY

21CS653

By
Prof. Prajna U R
Assistant Professor
Department of Information Science & Engineering
Sahyadri College of Engineering and Management, Adyar Mangaluru
Email:prajnau.is@sahyadri.edu.in
Mob:8495971075

COURSE OUTCOMES (COs)

CO1	**Understand the fundamentals of networks security, security architecture, threats and vulnerabilities**	**1**	**CL2**
CO2	Apply the different cryptographic operations of symmetric cryptographic algorithms.	2	CL3
CO3	Apply the different cryptographic operations of public key cryptography	3	CL3
CO4	Apply the various Authentication schemes to simulate different applications.	4	CL3
CO5	Understand various Security practices and System security standards.	5	CL 4

Text Book List

TB1.	**AtulKahate, Cryptography and Network Security, 4th Edition,2019**
TB2.	William Stallings, Cryptography and Network Security: Principles and Practices, 7th Edition,2019.
TB3.	Nina Godbole and SunitBelapure, Cyber Security, 1st Edition, 2019.

MODULE-1

Introduction to Network Security

What is a Network?

- A network consists of two or more computers that are linked in order to share resources exchange files, or allow electronic communications.
- The computers on a network may be linked through cables, telephone lines, radio waves, satellites, or infrared light beams.
- <u>The Three Types of Area Networks are:</u>

  1. LAN (Local Area Network)
  2. MAN (Metropolitan Area Network)
  3. WAN (Wide Area Network)

What is a Network Security?

- Network security is any activity designed to protect the usability and integrity of our network and data.
- It includes both hardware and software technologies.
- It targets a variety of viruses and threats.
- It stops them from entering or spreading on our network.
- Effective network security manages access to the network.

What is Computer network?

A computer network is a group of computers that use a set of common communication protocols over digital interconnections for the purpose of sharing recourses located on or provided by the network nodes.

What is Network Security?

Is described as the implementation of technologies, processes and protocols designed to safeguard an individual or organizations communications and information

WHY DO WE NEED SECURITY?

- Protect vital information while still allowing access to those who need it
  - Trade secrets, medical records, etc.
- Provide authentication and access control for resources
  - Ex: AFS
- Guarantee availability of resources


The Internet
ISP
User
www.nesobank.com

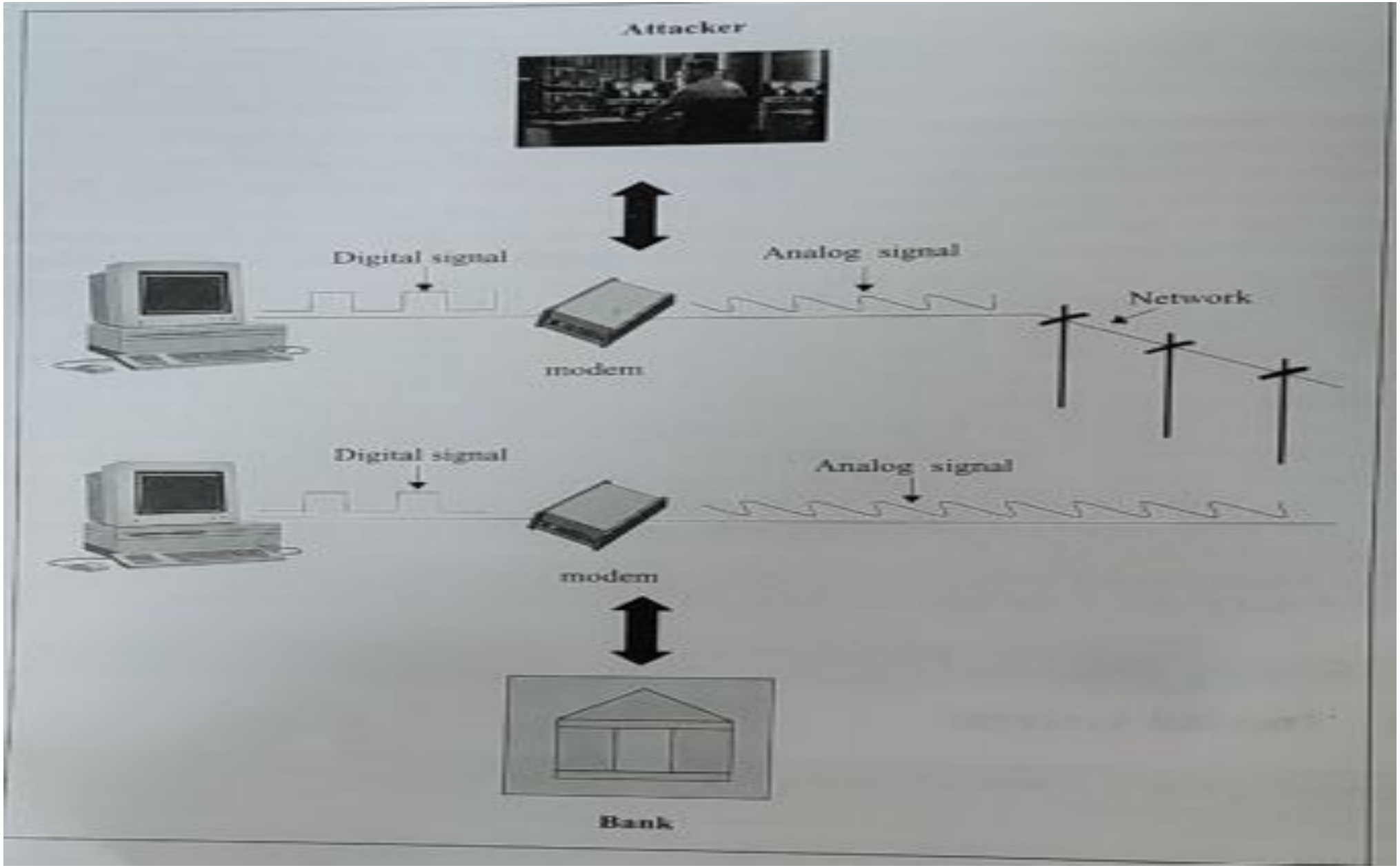

The Internet
ISP
User
Bogus Server

Computer Security

The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

Security Approaches

- **Prevention**- Prevent the treat by identifying underlying causes before they occur.
- **Protection**- Treats are ready to occur and eliminating the threat
- **Resilience**-Treat is already occurred- Need to adopt some mechanism through which we have to solve the threat


Attacker
Digital signal
Analog signal
Network
modem
Digital signal
Analog signal
modem
Bank

Security Models

- No security
- Security through obscurity
- Host security
- Network security

Security management practices

- Security policy

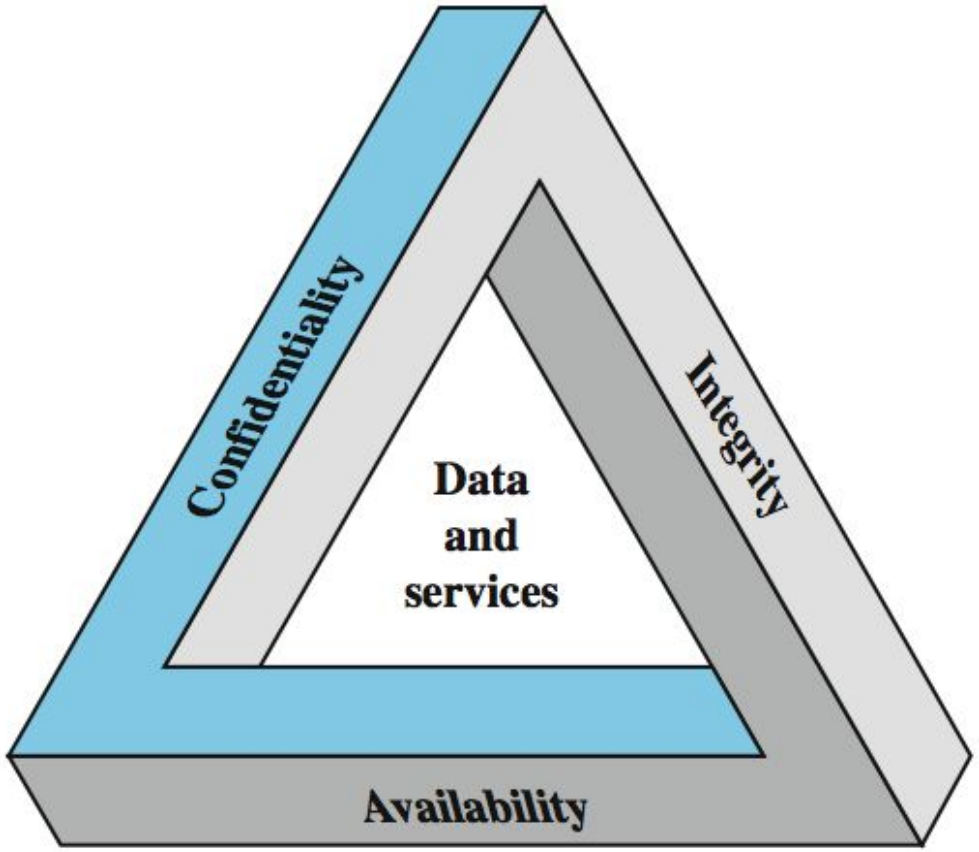
Key aspects

- Affordability
- Functionality
- Cultural Issues
- Legality

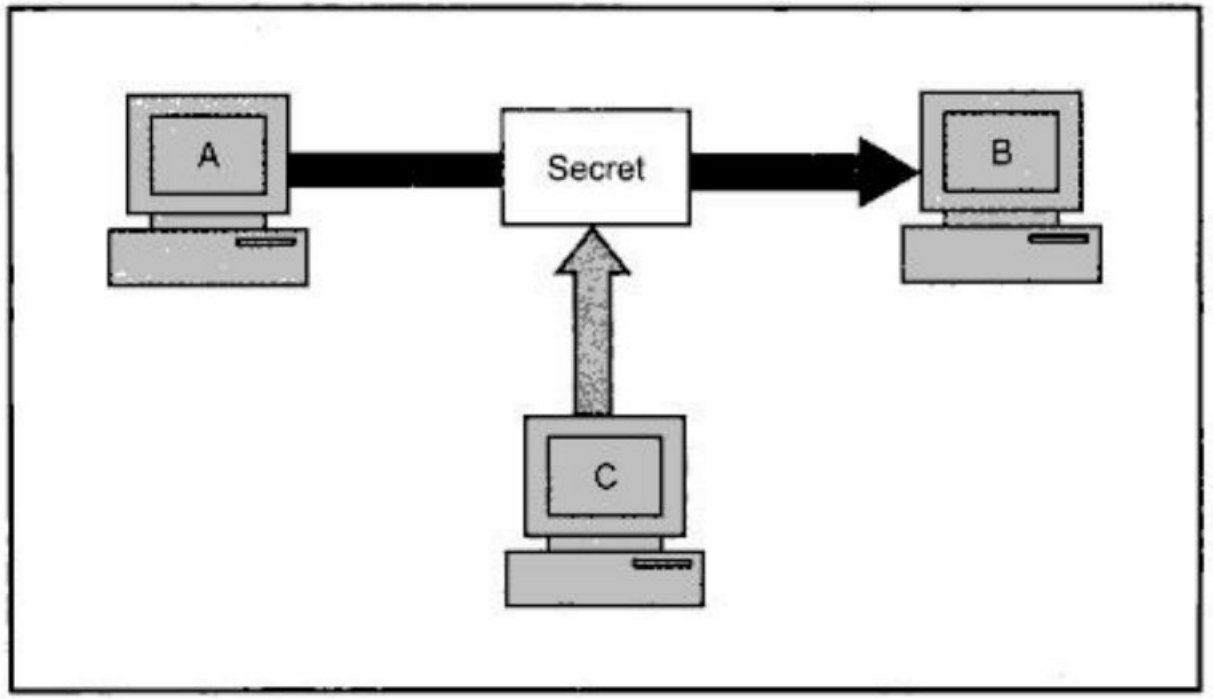
Principles of Security

CIA triad

- Non repudiation
- Access control
- Availability



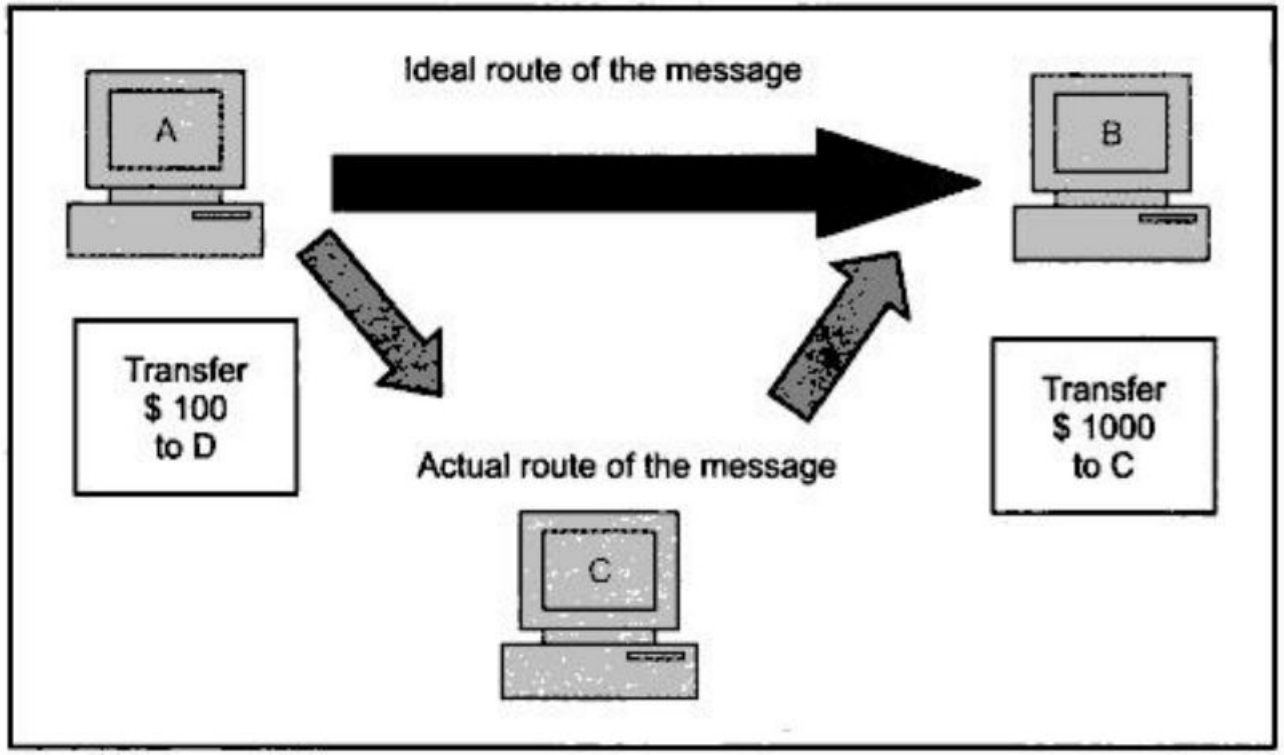
Confidentiality



- Type of attack- Interception
- Interception Causes loss of message confidentiality

- Confidentiality: (Account Information)
  - Data confidentiality: Assures confidential information is not made available or disclosed to unauthorized individuals.
  - Privacy: Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

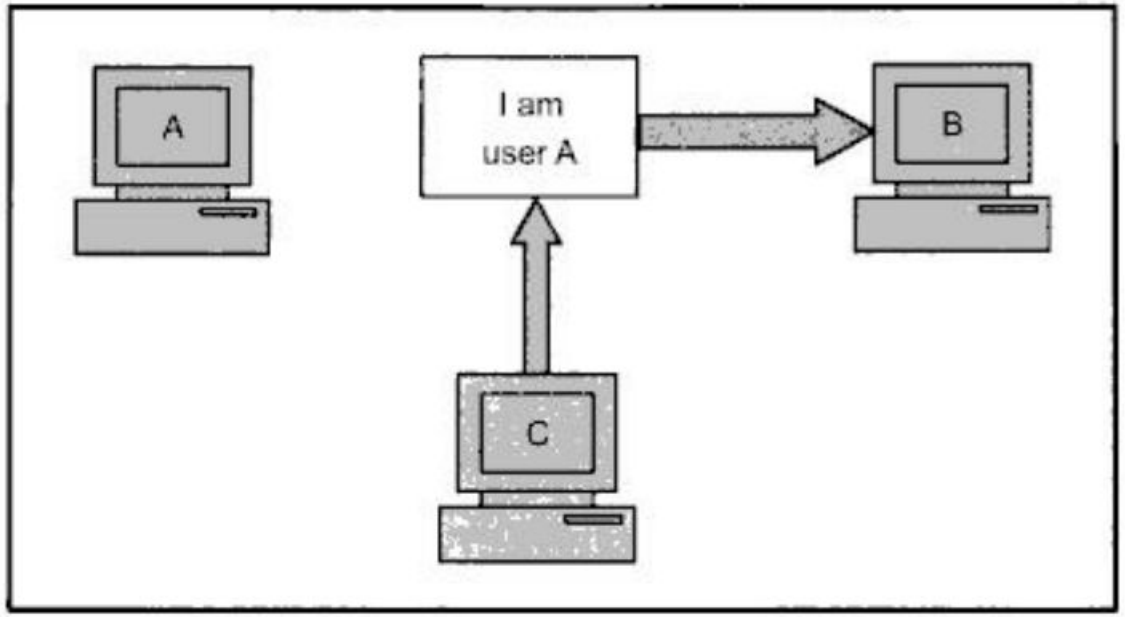
Integrity



- Type of attack- Modification
- Modification Causes loss of message Integrity.

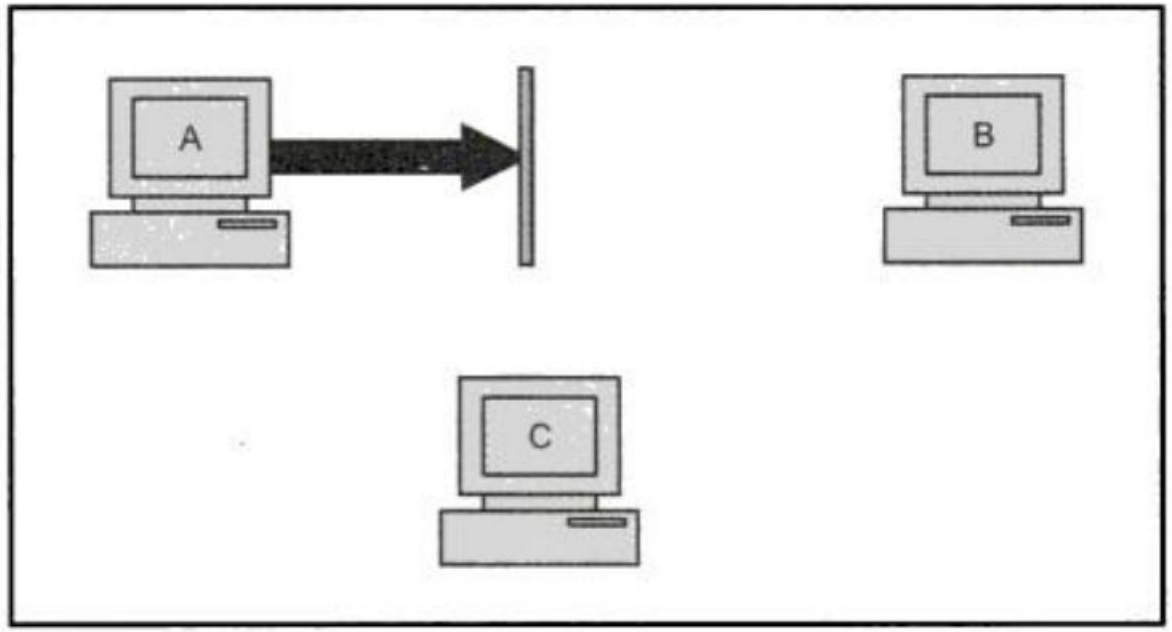
- Integrity: (Patient information)
  - Data integrity: Assures that information and programs are changed only in a specified and authorized manner.
  - System integrity: Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.
    - Any modification in message should be identified by the security system

Authentication



- Type of attack- Fabrication
- Fabrication is possible in the absence of proper authentication mechanisms.

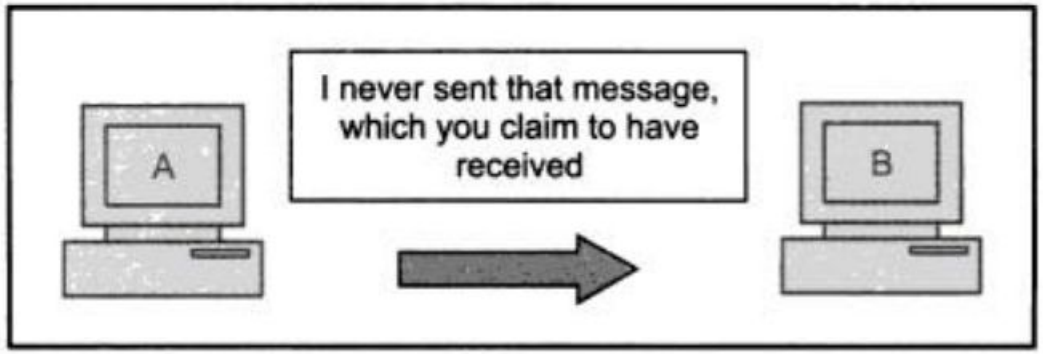
Availability



- Type of attack- Interruption
- Interruption puts the availability of recourses in danger.

- Availability: Google vs Banking sites
  - Assures that systems work promptly and service is not denied to authorized users.
- Authenticity:
  - The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator.
- Accountability:
  - truly secure systems are not yet an achievable goal, must be able to trace a security breach to a responsible party

Non Repudiation



Non repudiation does not allow the sender of a message to refute the claim of not sending that message.

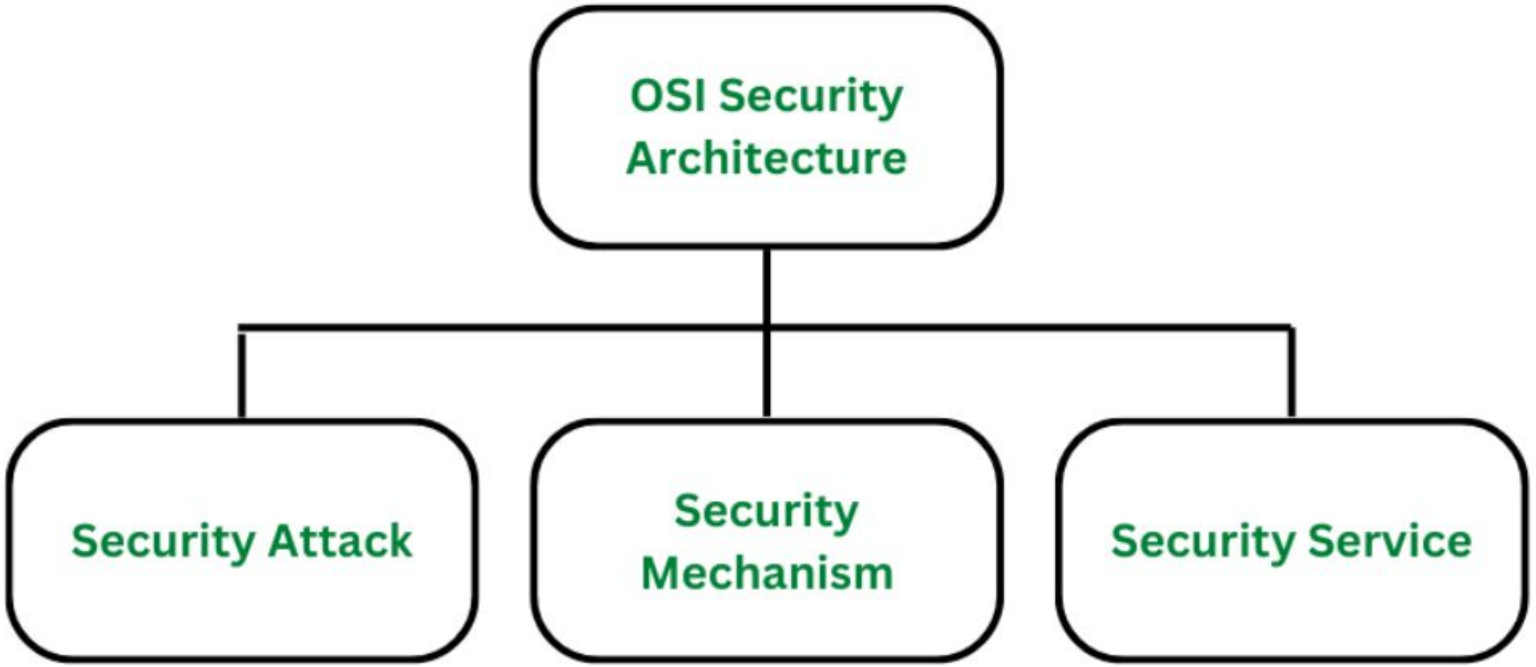
Access control

- The principle of Access control determines who should be able to access what.

- Access control broadly related to two areas.
- Role management-user side
- Rule management-resources side

Access control specifies and controls who can access what.

OSI SECURITY ARCHITECTURE



Classification of OSI Security Architecture

OSI SECURITY ARCHITECTURE

Security attack: Any action that compromises the security of information owned by an organization.

Security mechanism: A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.

Security service: A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

Threat v/s Attack

Threat

A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

Attack

An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

Security Services – Definition

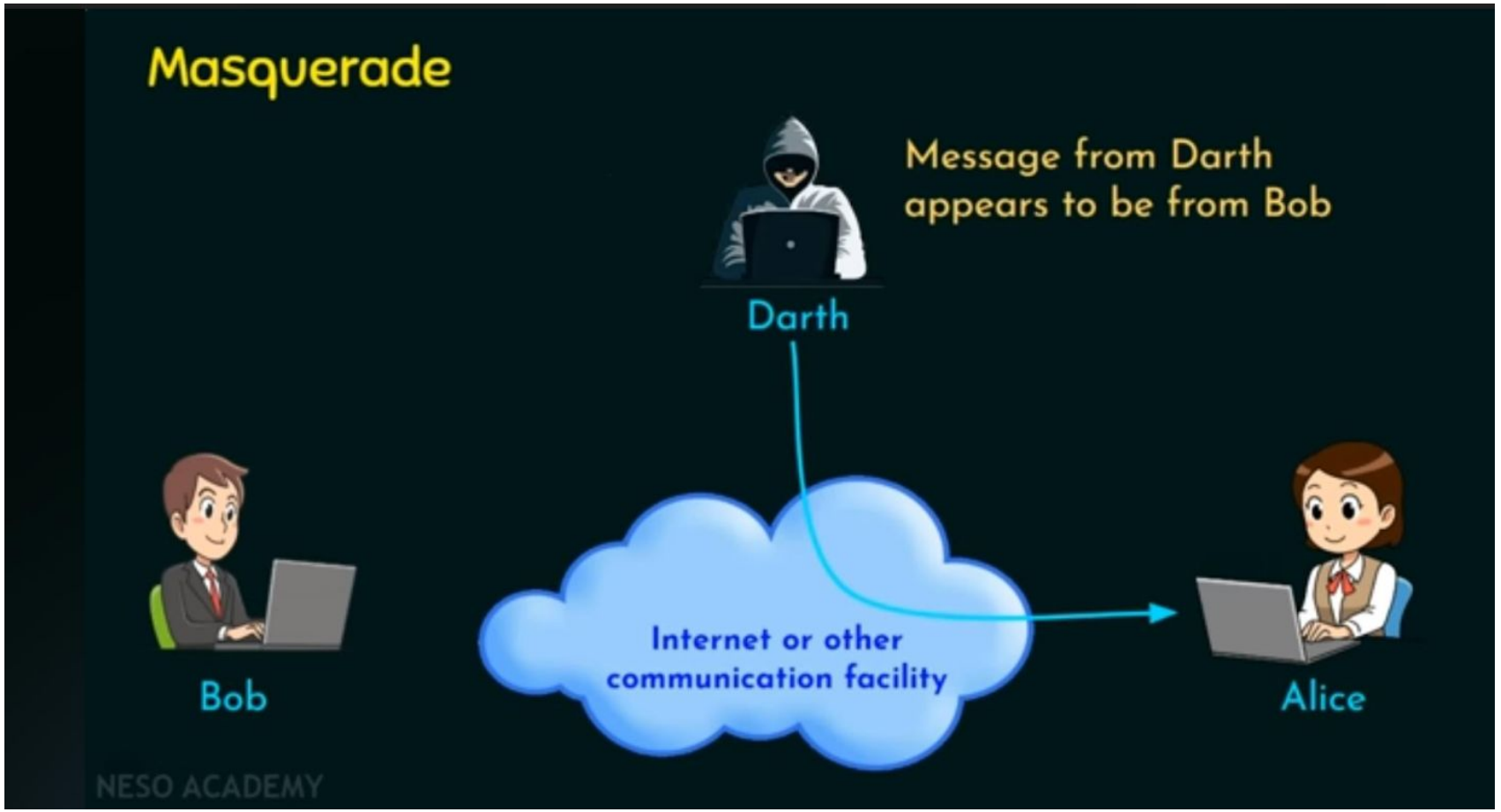
The processing or communication service that is provided by a system to give a specific kind of protection to system resources; security services implement security policies and are implemented by security mechanisms.

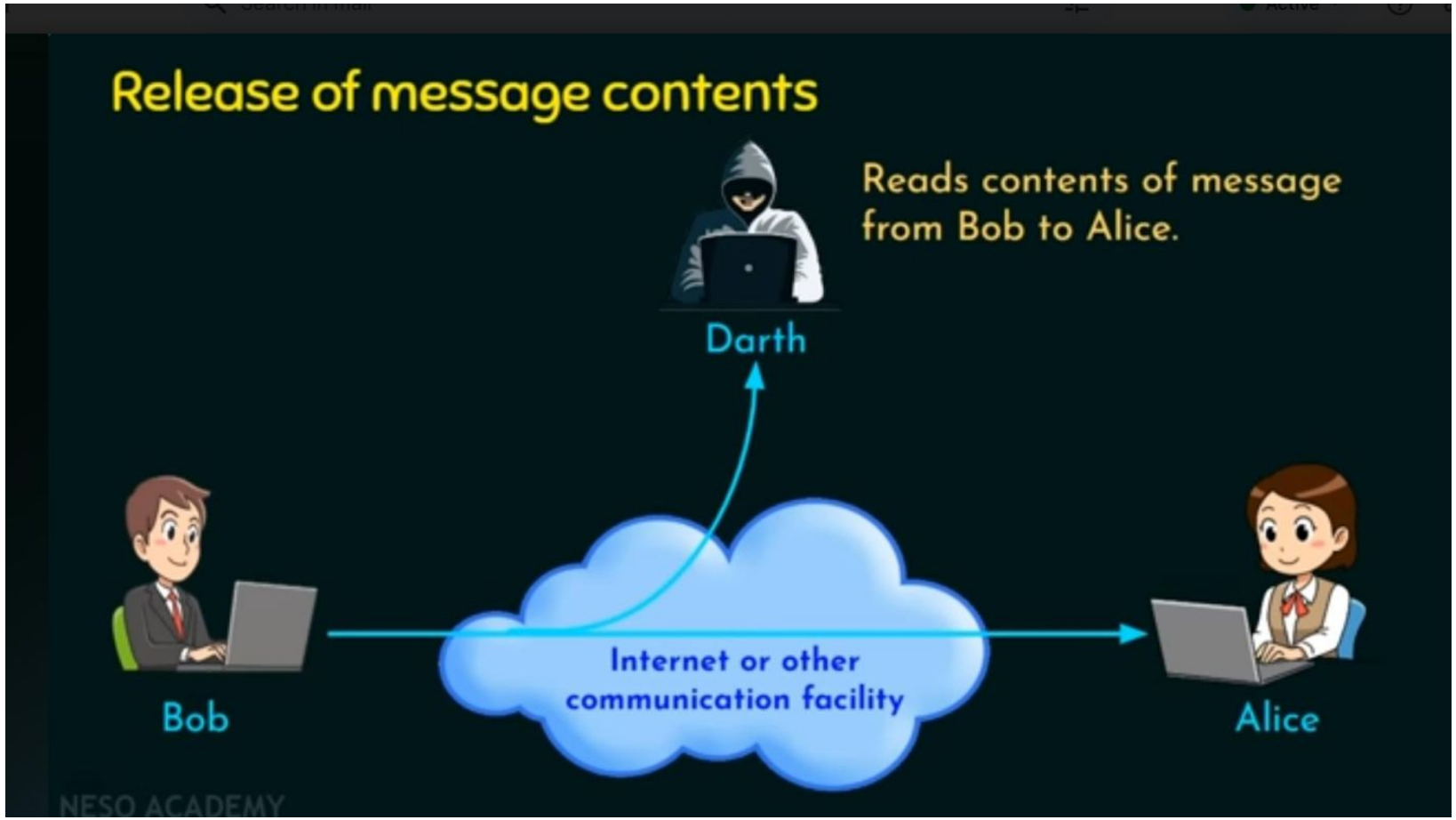
Security Services

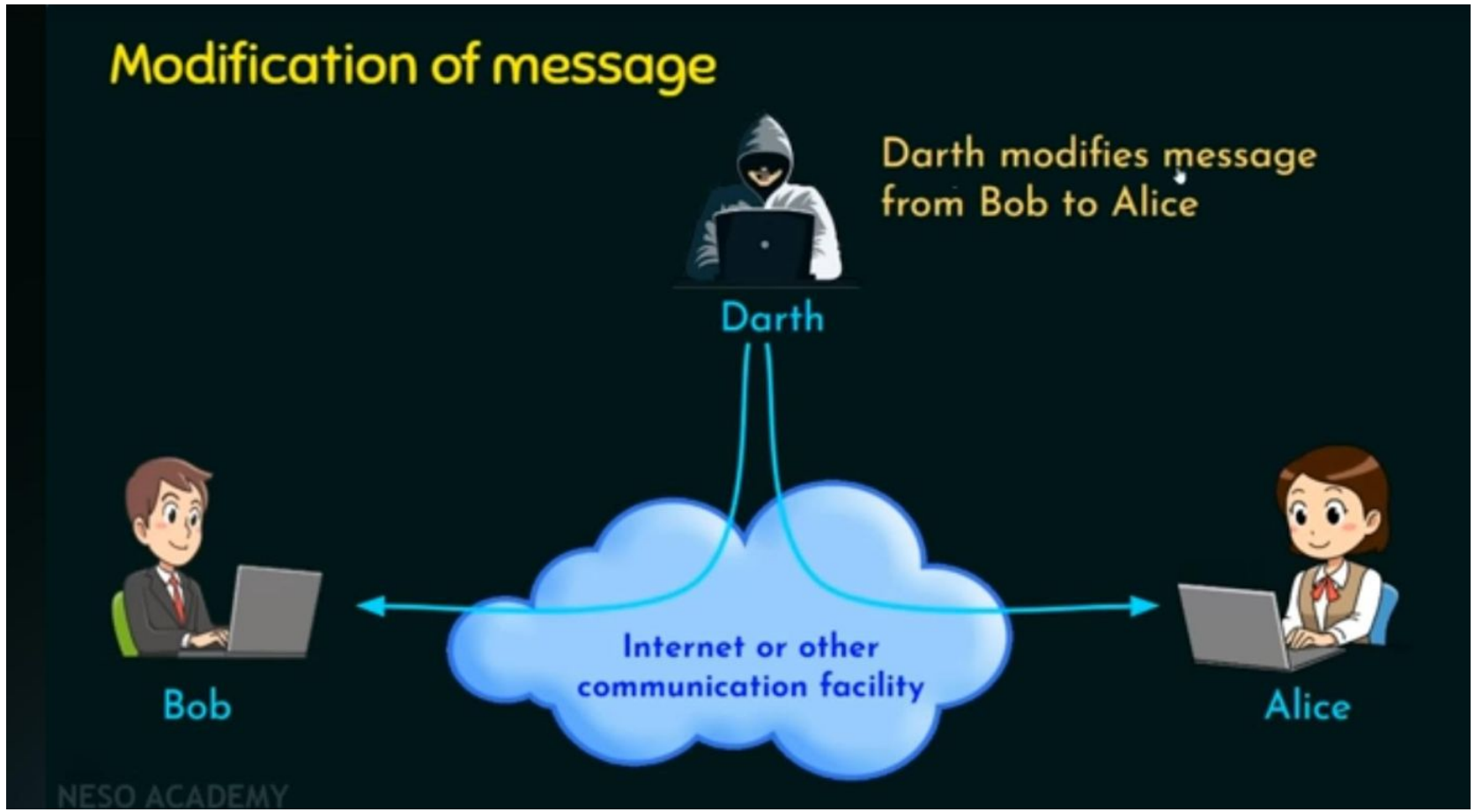
- ★ Authentication
  - ○ Peer entity authentication
  - ○ Data origin authentication
- ★ Access control
- ★ Data confidentiality
- ★ Data Integrity
- ★ Nonrepudiation

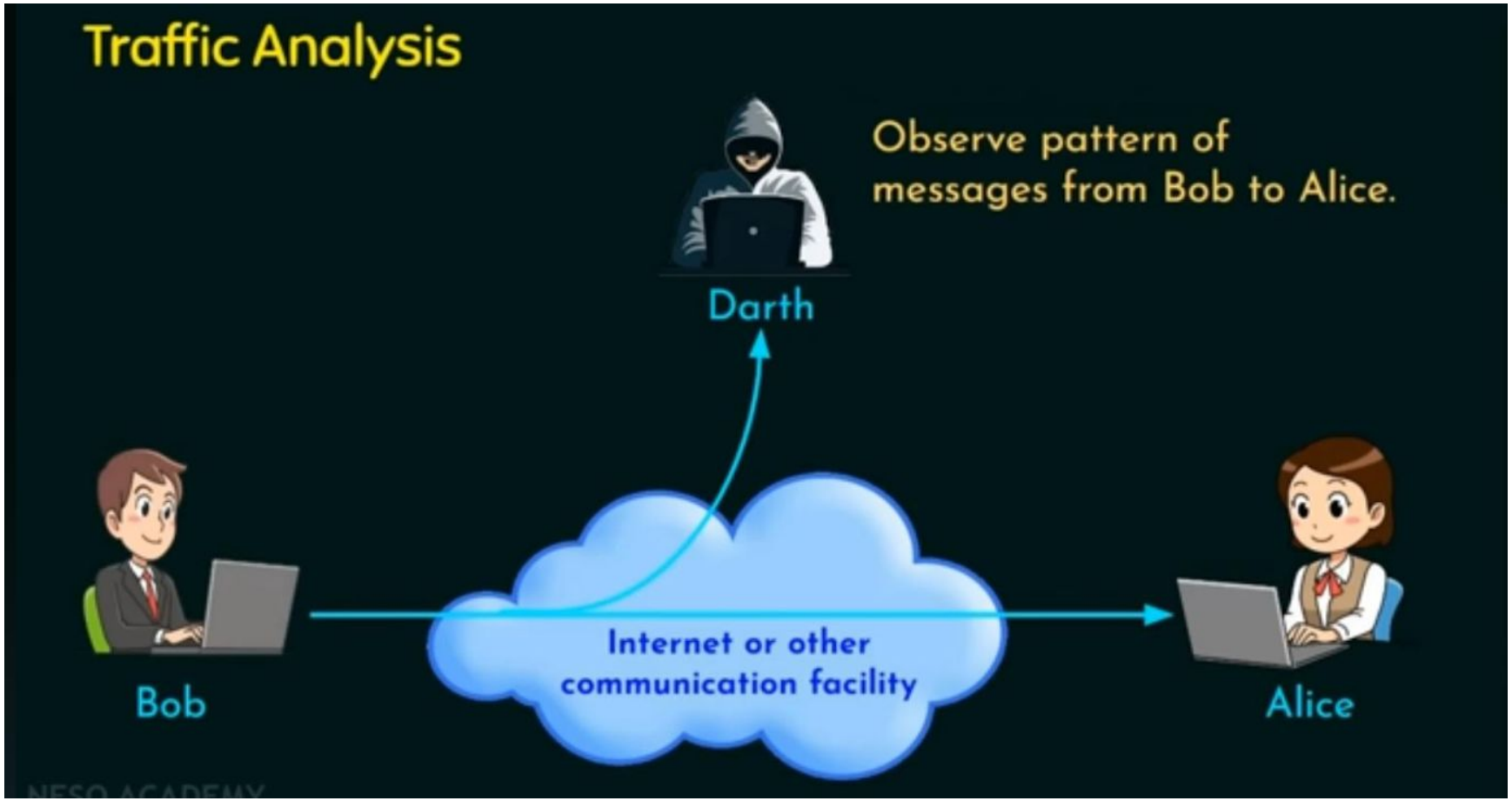
Specific Security Mechanisms

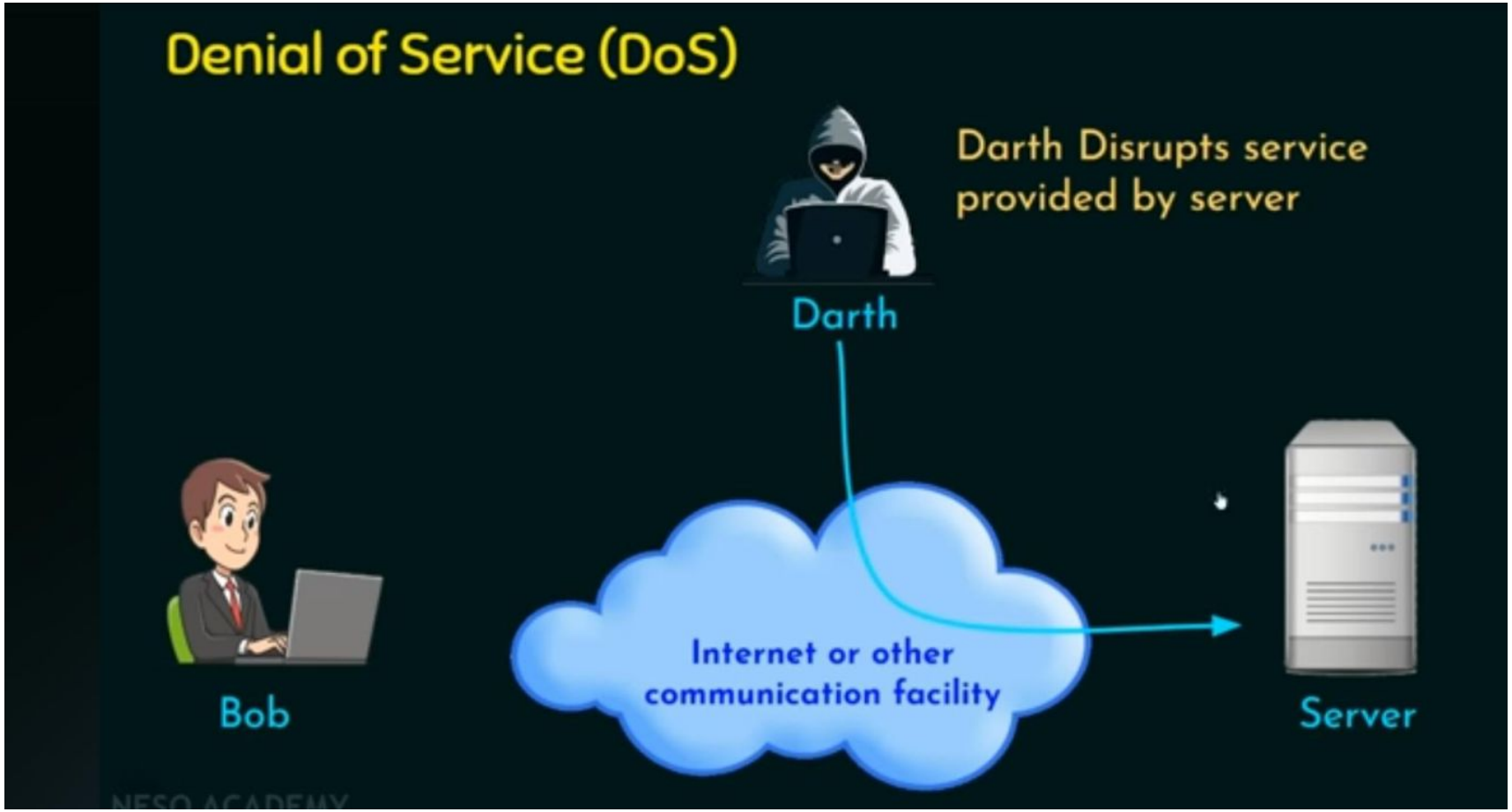
- ★ Encipherment
- ★ Digital Signature
- ★ Access Control
- ★ Data Integrity
- ★ Authentication Exchange
- ★ Traffic Padding
- ★ Routing Control
- ★ Notarization


Masquerade
Message from Darth
appears to be from Bob
Darth
Bob
Internet or other
communication facility
Alice
NESO ACADEMY


Release of message contents
Reads contents of message from Bob to Alice.
Darth
Bob
Internet or other communication facility
Alice
NESO ACADEMY

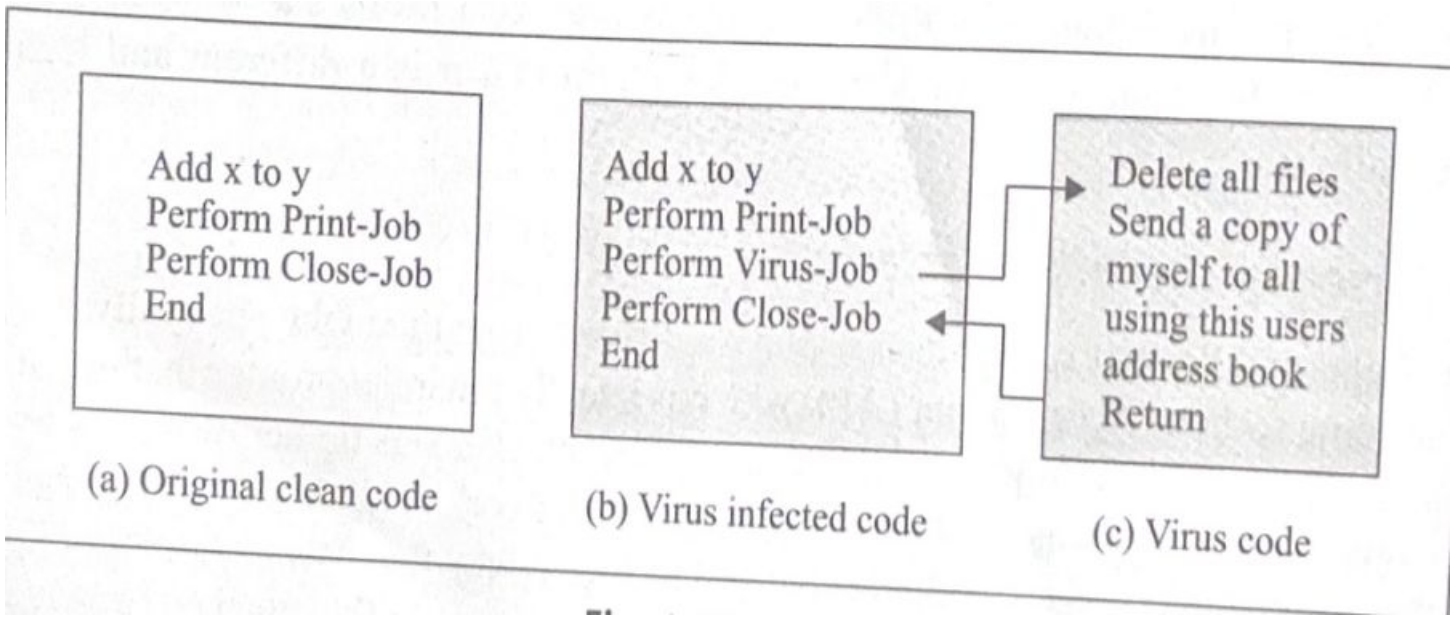

Modification of message
Darth modifies message from Bob to Alice
Darth
Internet or other communication facility
Bob
Alice
NESO ACADEMY


Traffic Analysis
Observe pattern of
messages from Bob to Alice.
Darth
Bob
Internet or other
communication facility
Alice

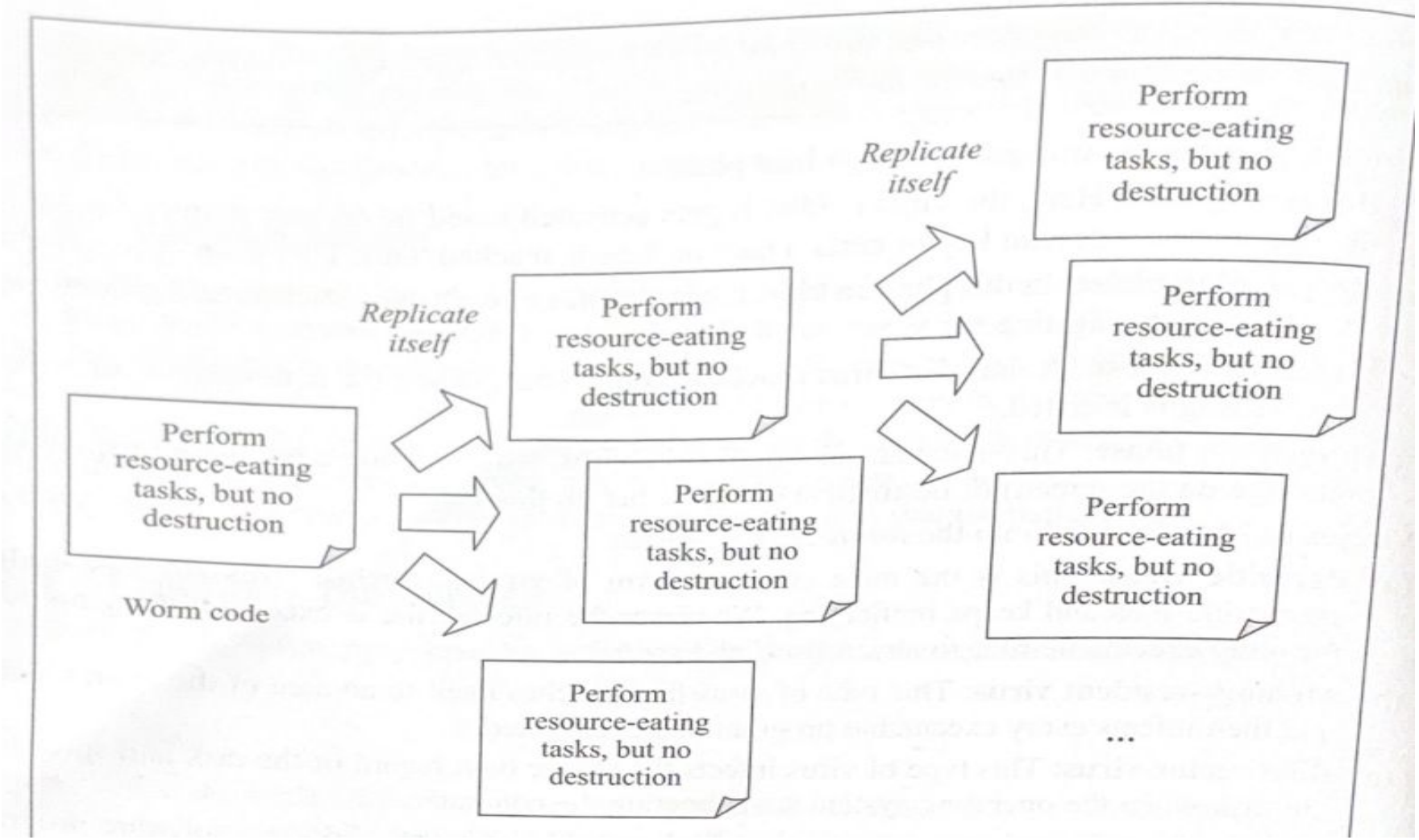

Denial of Service (DoS)
Darth Disrupts service provided by server
Darth
Bob
Internet or other communication facility
Server

Programs that attack computer system

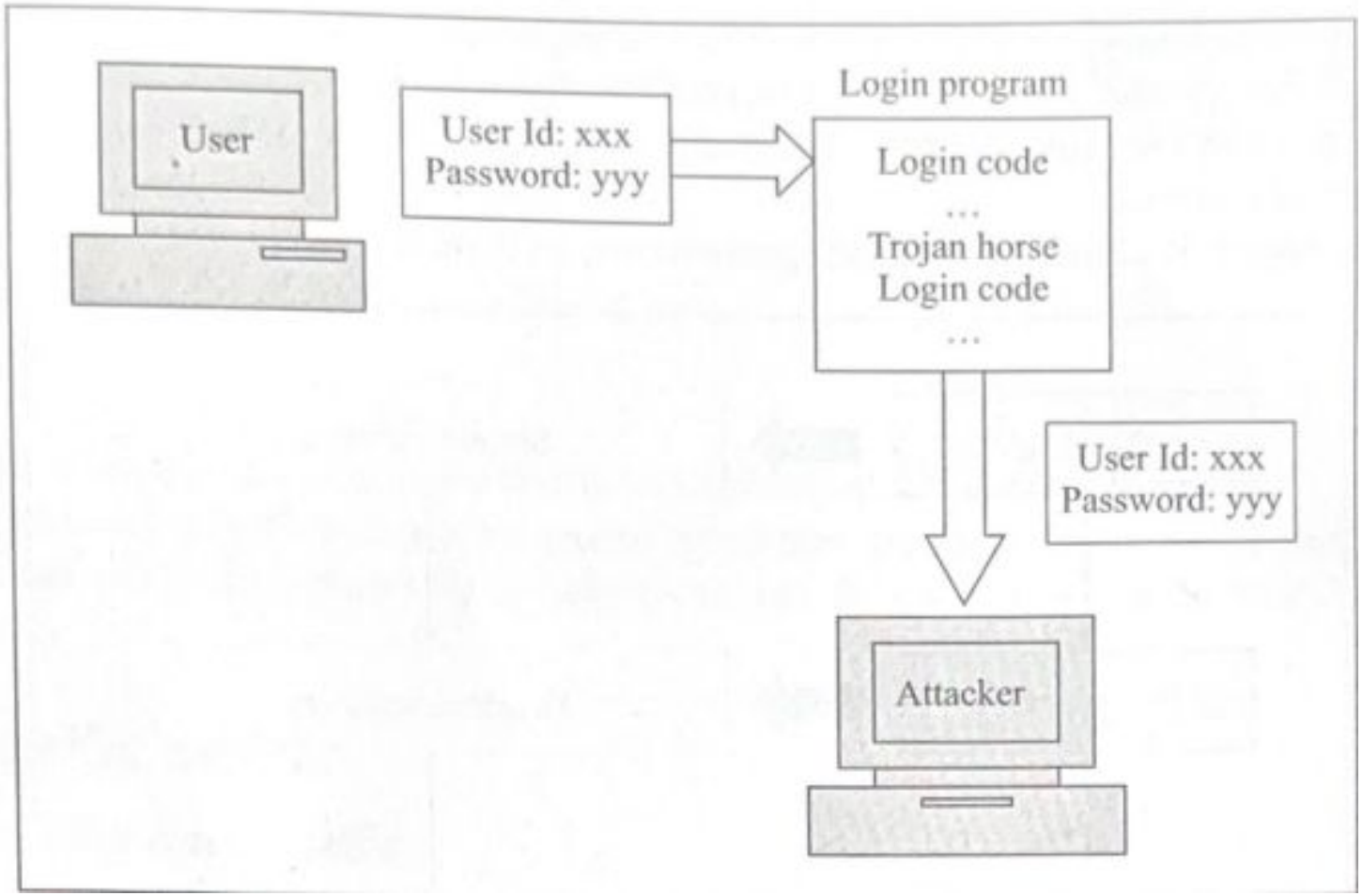
- 1. Virus



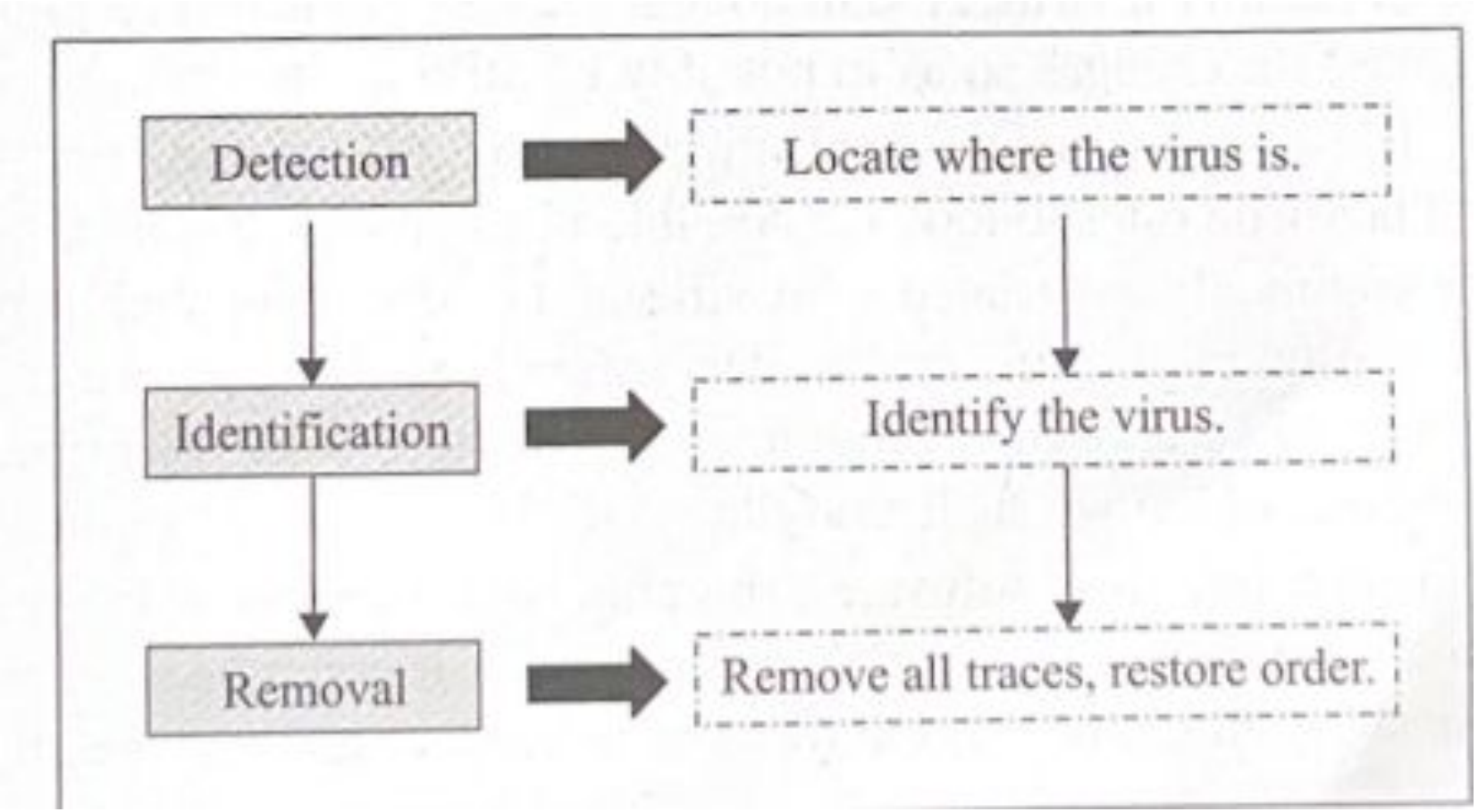
2. Worm


Perform resource-eating tasks, but no destruction
Worm code
Replicate itself
Perform resource-eating tasks, but no destruction
Perform resource-eating tasks, but no destruction
Perform resource-eating tasks, but no destruction
Replicate itself
Perform resource-eating tasks, but no destruction
Perform resource-eating tasks, but no destruction
Perform resource-eating tasks, but no destruction
...

3. Trojan Horse

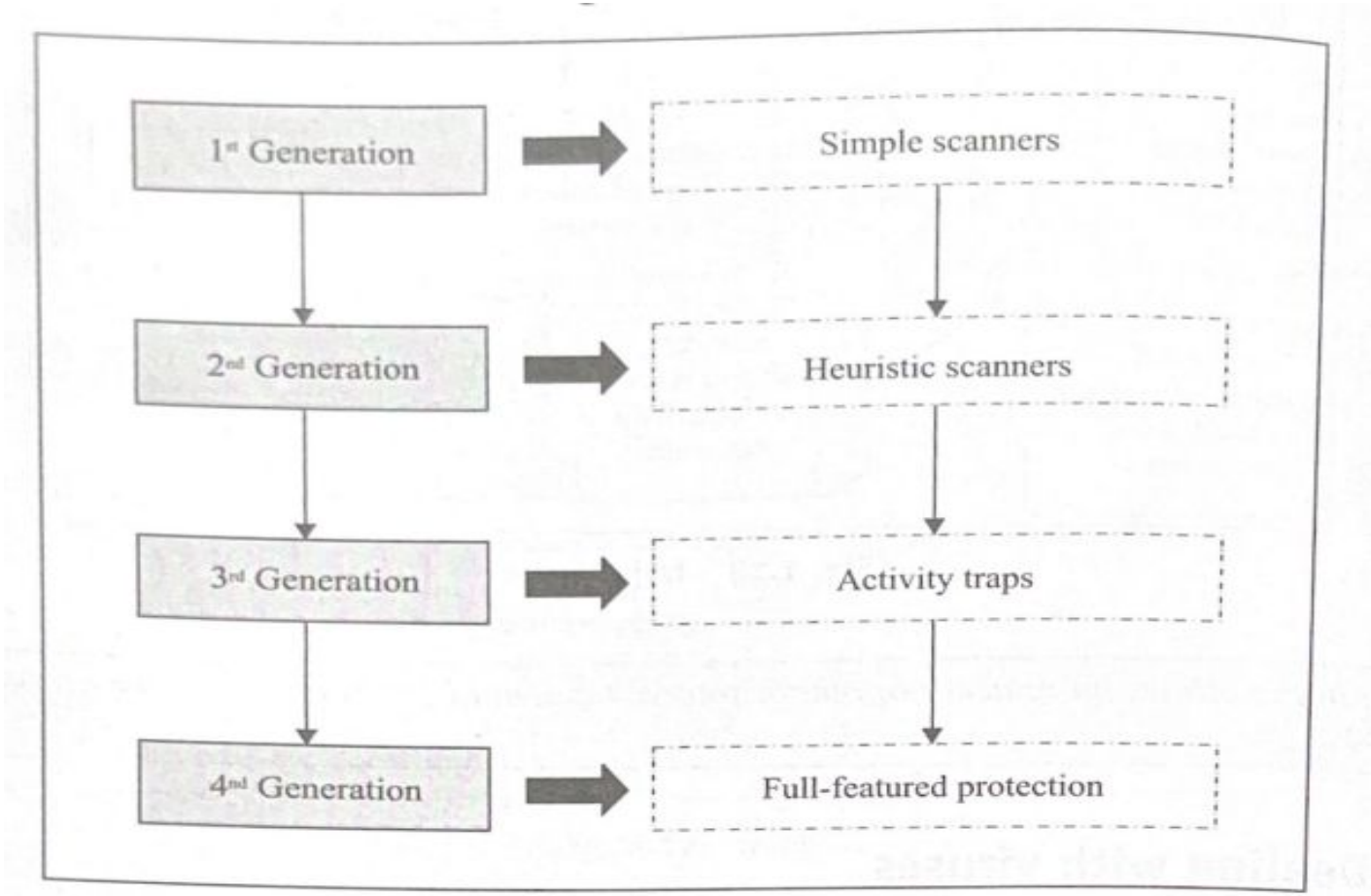


Dealing with viruses



Virus elimination steps

Generations of anti-virus software



Specific attacks

1. Sniffing and Spoofing

    Two forms

    1. packet Sniffing(IP sniffing)
    2. Packet Spoofing (IP Spoofing)

2.Phishing

3.Pharming(DNS Spoofing)