Hafez Barghouthi

NETWORK SECURITY

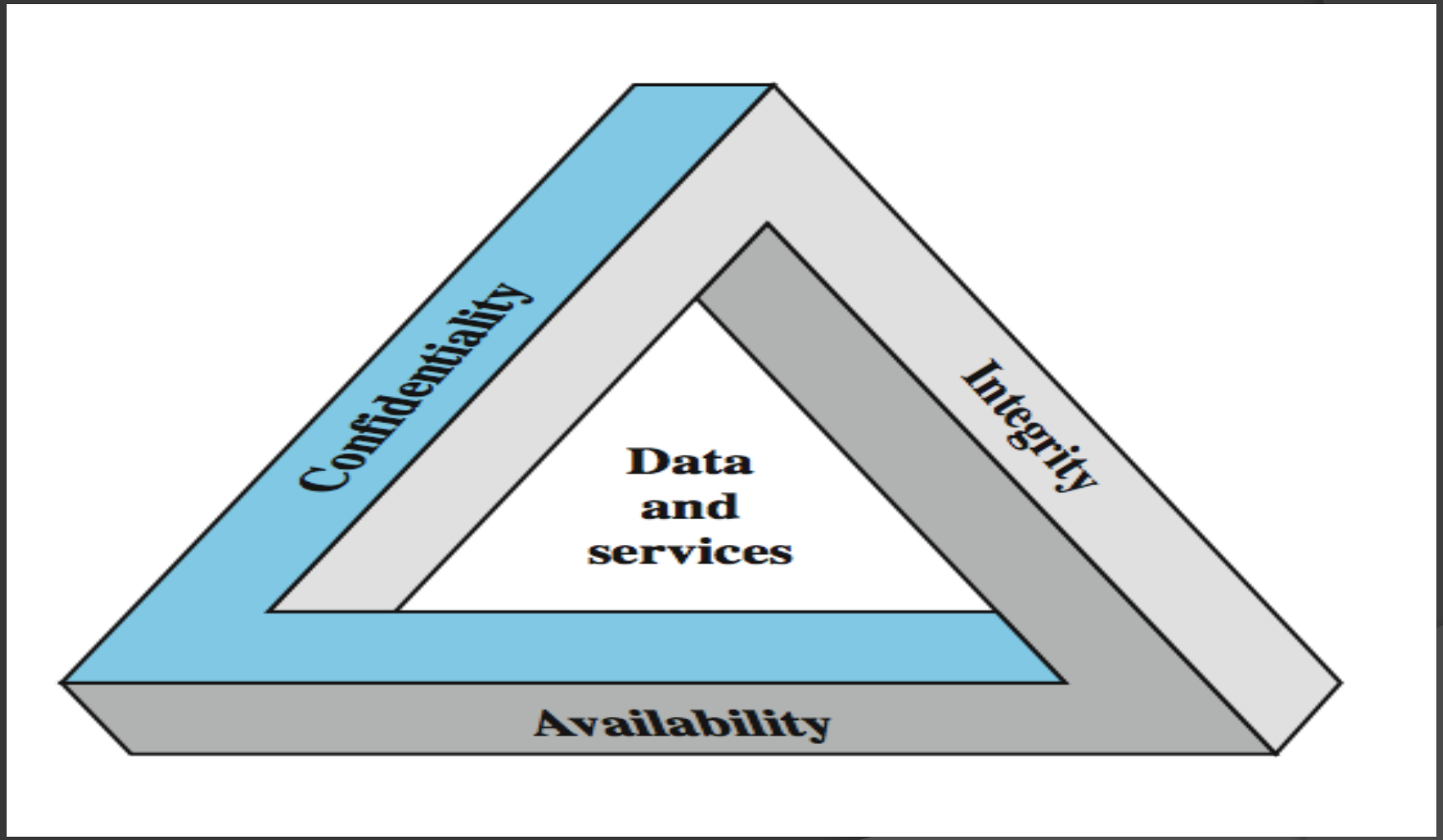
Redefine for computer security

- 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)

This definition include

- computer use requires automated tools to protect files and other stored data
- use of networks and communications links requires measures to protect data during transmission

And also again CIA



Examples of Security Requirements

- confidentiality –student grades
- integrity – patient information
- availability – authentication service

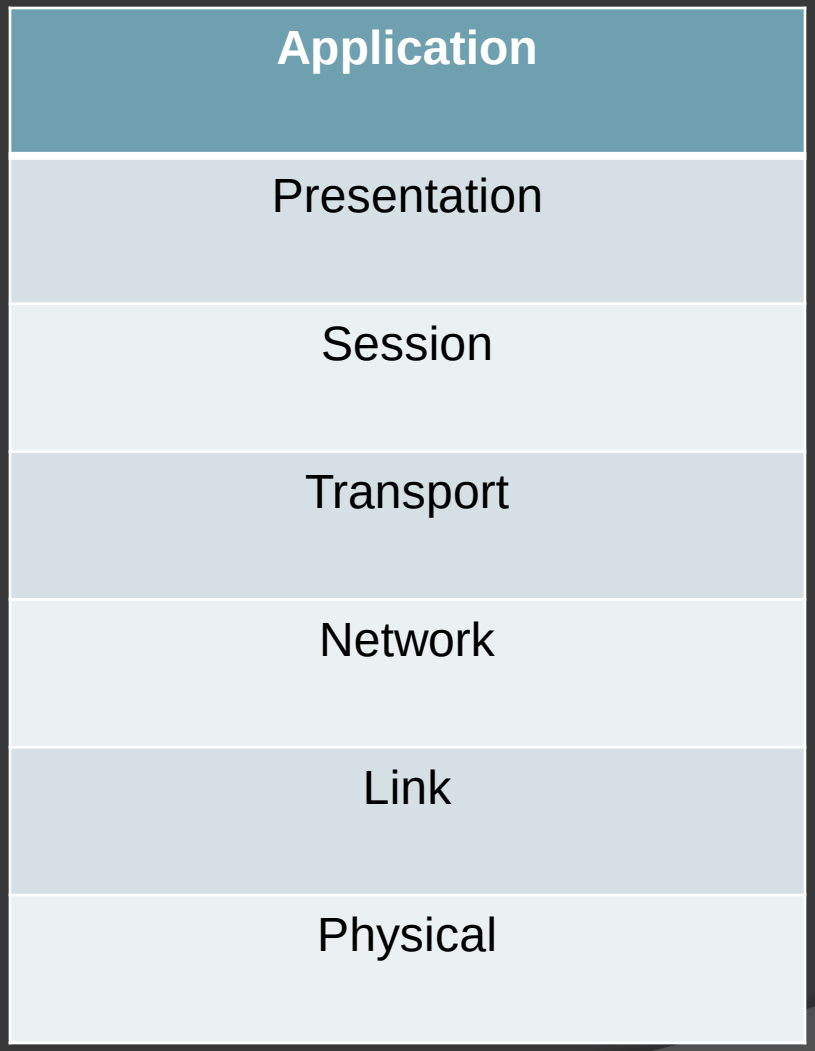
Challenges

- Not simple (example ciphers)
- must consider All possible attacks.
- must decide where to deploy mechanisms.
- not perceived on benefit until fails
- Security protocol conflict with transmission protocol.
- Performance (☹)

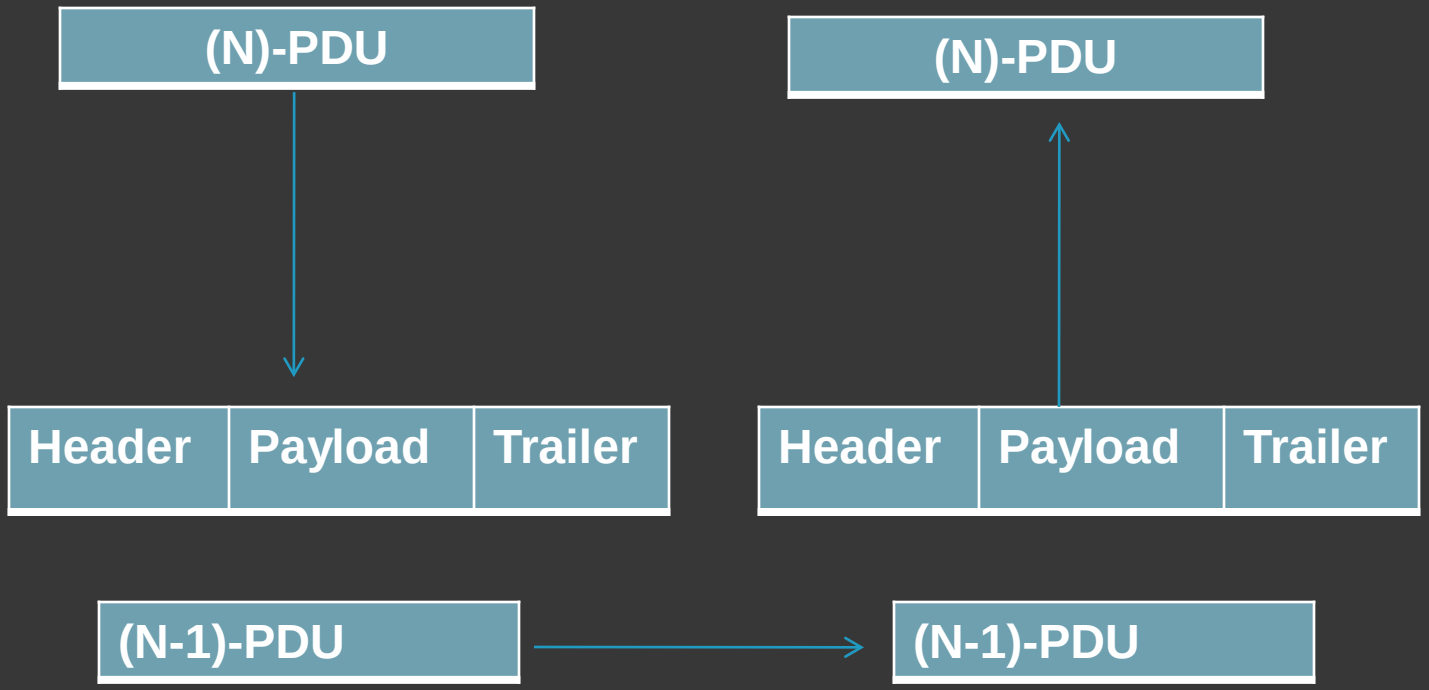
OSI Security Architecture

- defines a systematic way of defining and providing security requirements
- for us it provides a useful, if abstract, overview of concepts that we will study.

Layers



Processing an (N)-PDU



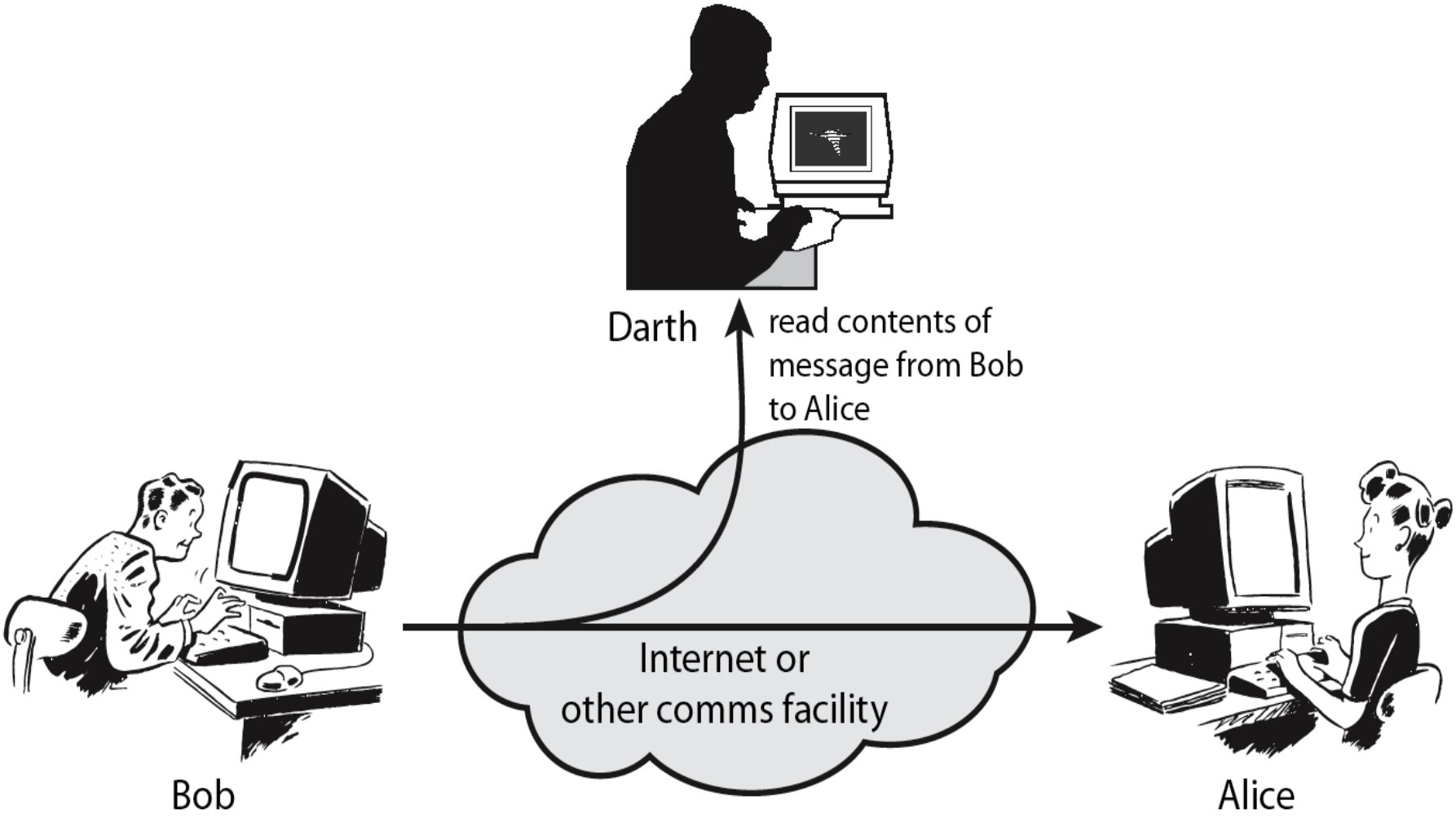
OSI defines 3 Aspects

- **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.

Passive Attacks

- Release of message content.
- Traffic Analysis.

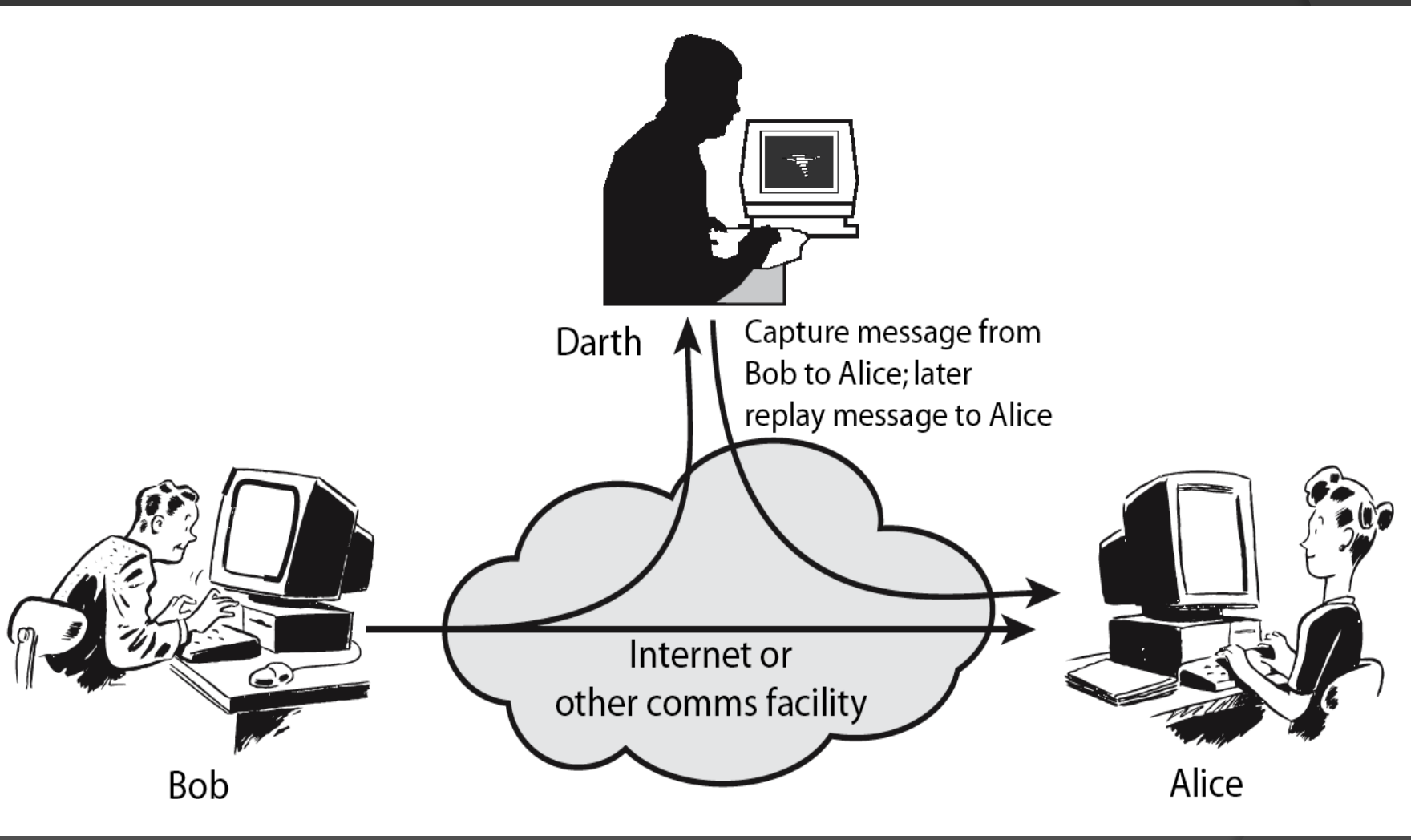
Release of Message



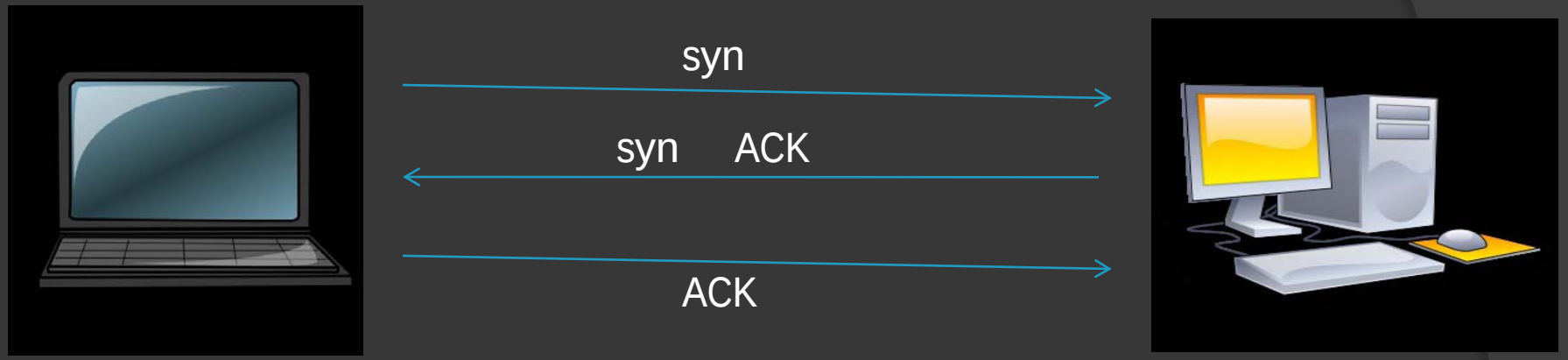
Active

- Masquerade
- Reply
- Denial of service
- Modfication of a message.

Replay attack



Handshake protocol



Could create a Denial-of-Service (DoS) attack
☐ SYN floods create many half-open connections

Security Service

- enhance security of data processing systems and information transfers of an organization
- intended to counter security attacks
- using one or more security mechanisms
- often replicates functions normally associated with physical documents
  - which, for example, have signatures, dates; need protection from disclosure, tampering, or destruction; be notarized or witnessed; be recorded or licensed

Security services

- **Authentication** - assurance that communicating entity is the one claimed
  - have both peer-entity & data origin authentication
- **Access Control** - prevention of the unauthorized use of a resource
- **Data Confidentiality** –protection of data from unauthorized disclosure
- **Data Integrity** - assurance that data received is as sent by an authorized entity
- **Non-Repudiation** - protection against denial by one of the parties in a communication
- **Availability** – resource accessible/usable

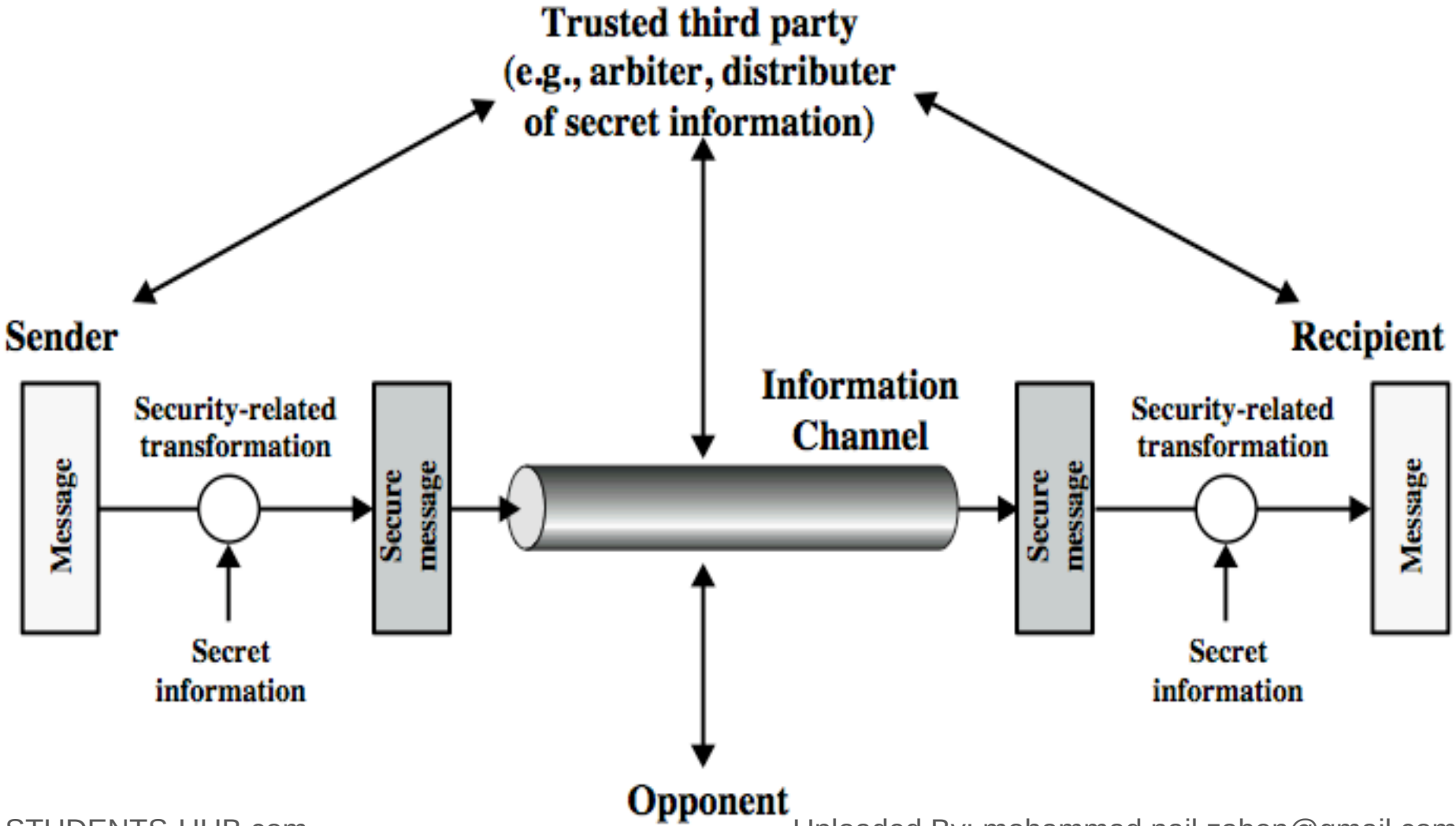
security mechanisms

- feature designed to detect, prevent, or recover from a security attack
- no single mechanism that will support all services required
- however one particular element underlies many of the security mechanisms in use:
  - **cryptographic techniques**

Examples

- specific security mechanisms:
  - encipherment, digital signatures, access controls, data integrity, authentication exchange, traffic padding, routing control, notarization
- pervasive security mechanisms:
  - trusted functionality, security labels, event detection, security audit trails, security recovery

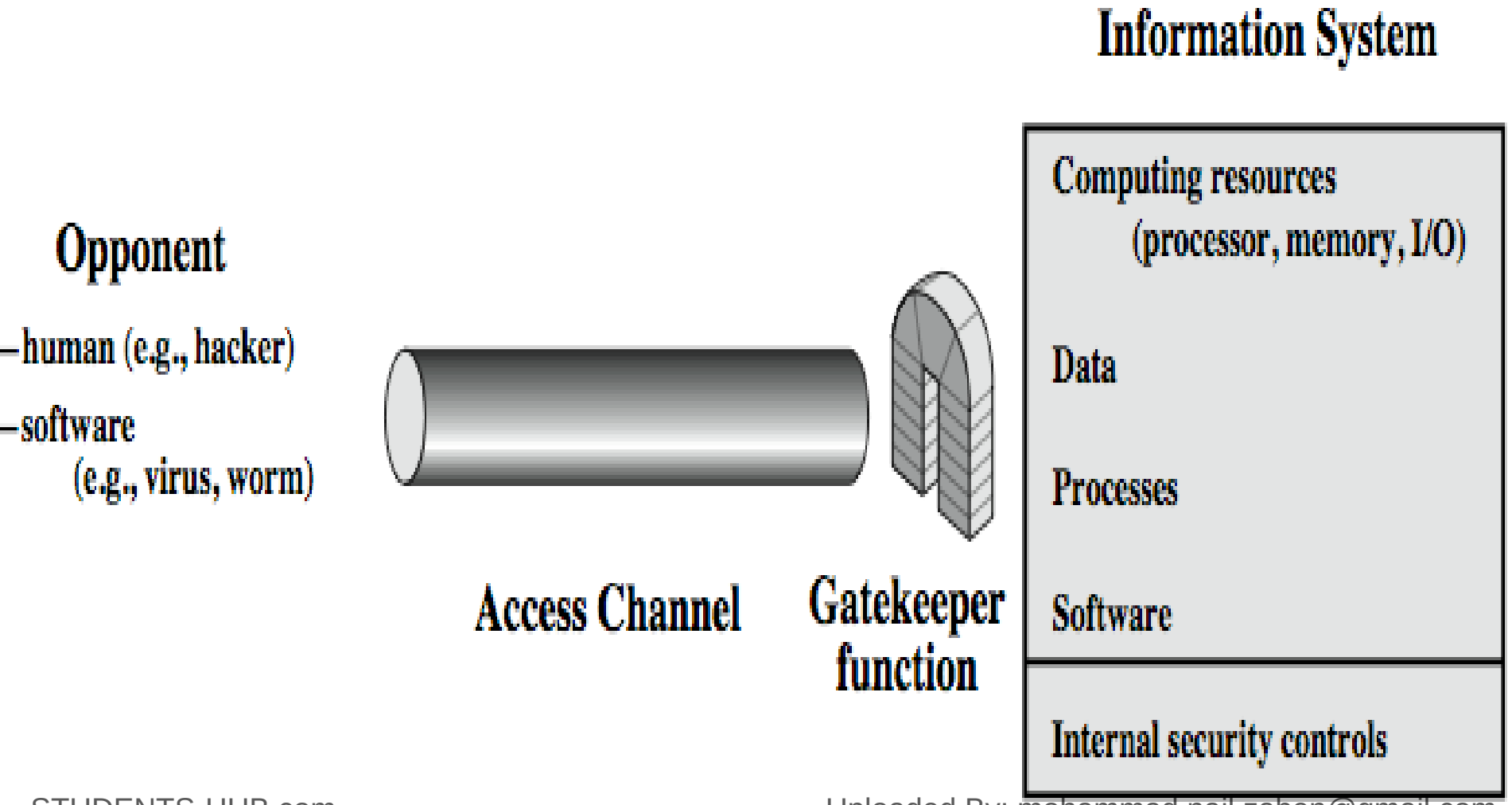
Model for Network Security



Model-cont.

- using this model requires us to:
  1. design a suitable algorithm for the security transformation
  2. generate the secret information (keys) used by the algorithm
  3. develop methods to distribute and share the secret information
  4. specify a protocol enabling the principals to use the transformation and secret information for a security service

Model for Network Access Security



Model2-cont.

- using this model requires us to:
  1. select appropriate gatekeeper functions to identify users
  2. implement security controls to ensure only authorised users access designated information or resources