Cryptography and Network Security

1. Overview

Lectured by
Nguyễn Đức Thái

cuu duong than cong . com

Outline

- Security concepts
- X.800 security architecture
- Security attacks, services, mechanisms
- Models for network (access) security
- Network security terminologies

Computer Security Objectives

Confidentiality

- Data confidentiality
  - Assures that private or 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

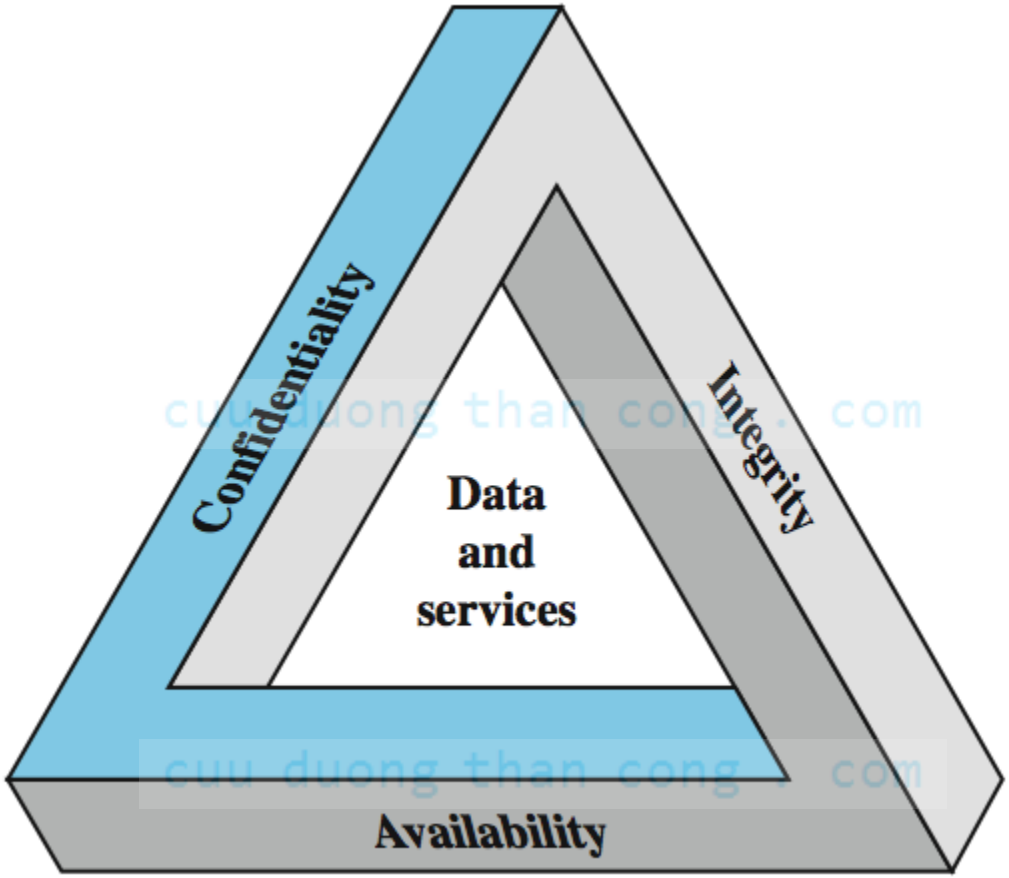
Integrity

- 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

Availability

- Assures that systems work promptly and service is not denied to authorized users

CIA Triad



The Security Requirements Triad

Possible Additional Concepts

Authenticity

- Verifying that users are who they say they are and that each input arriving at the system came from a trusted source

Accountability

- The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity

Terms

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 Attacks

- A means of classifying security attacks, used both in X.800 and RFC 4949, is in terms of *passive attacks* and *active attacks*

- A ***passive attack*** attempts to learn or make use of information from the system but does not affect system resources

- An ***active attack*** attempts to alter system resources or affect their operation

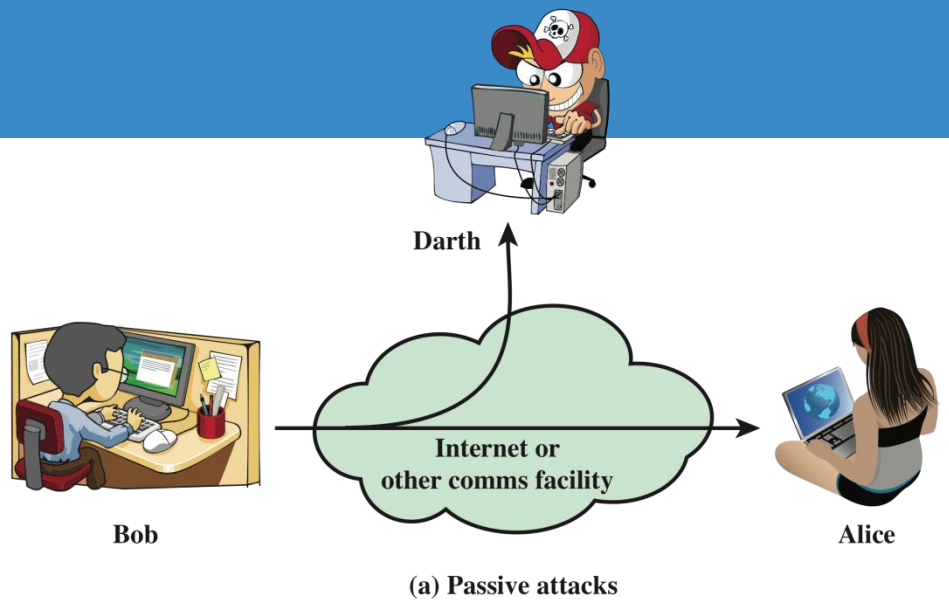


Figure 1.1 Security Attacks

Passive Attacks

- Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions.
- The goal of the opponent is to *obtain information* that is being transmitted.
- Two types of passive attacks are
  i. the release of message contents and
  ii. traffic analysis.

Active Attacks

- Involve some modification of the data stream or the creation of a false stream
- Difficult to prevent because of the wide variety of potential physical, software, and network vulnerabilities
- Goal is to detect attacks and to recover from any disruption or delays caused by them

Masquerade

- Takes place when one entity pretends to be a different entity
- Usually includes one of the other forms of active attack

Replay

- Involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect

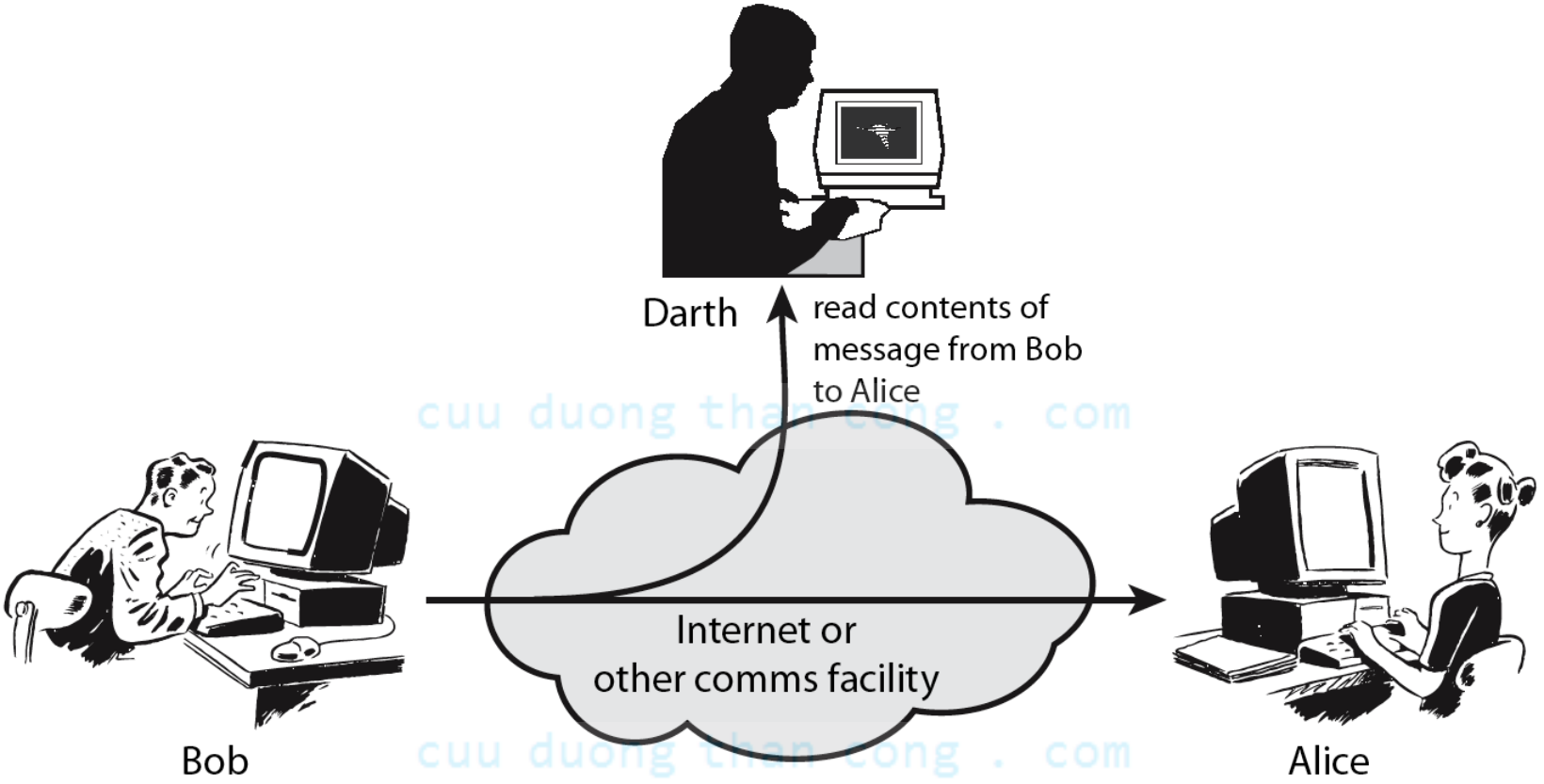
Modification of messages

- Some portion of a legitimate message is altered, or messages are delayed or reordered to produce an unauthorized effect

Denial of service

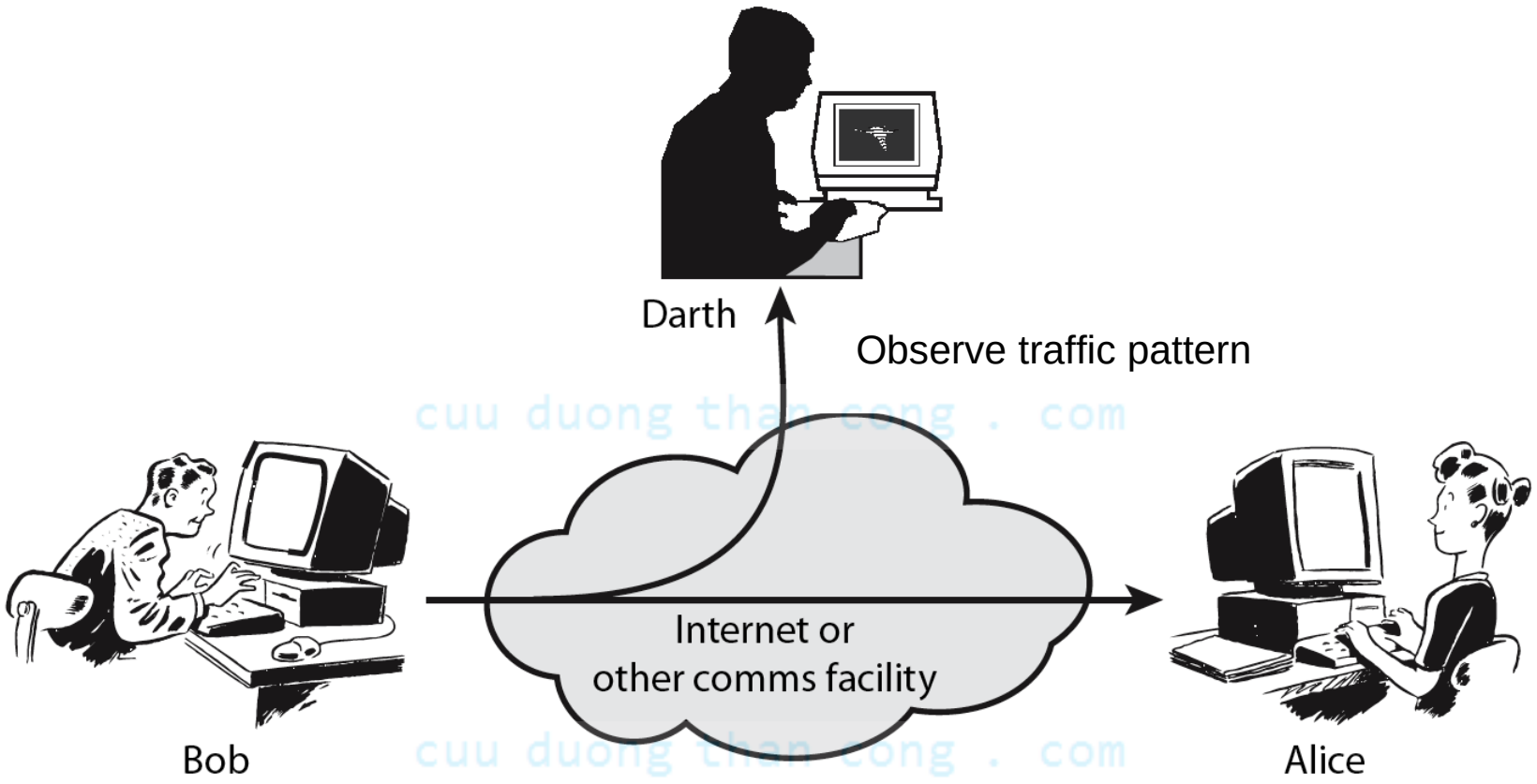
- Prevents or inhibits the normal use or management of communications facilities

Passive Attacks - Interception



Release of message contents

Passive Attacks – Traffic Analysis



Traffic analysis

Handling Attacks

- **Passive attacks – focus on Prevention**
  - Easy to stop
  - Hard to detect

- **Active attacks – focus on Detection and Recovery**
  - Hard to stop
  - Easy to detect

Security Services (X.800)

- **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

Authentication

- Concerned with assuring that a communication is authentic
  - In the case of a single message, assures the recipient that the message is from the source that it claims to be from
  - In the case of ongoing interaction, assures the two entities are authentic and that the connection is not interfered with in such a way that a third party can masquerade as one of the two legitimate parties

cuu duong than cong . com

Two specific authentication services are defined in X.800:

- Peer entity authentication
- Data origin authentication

Access Control

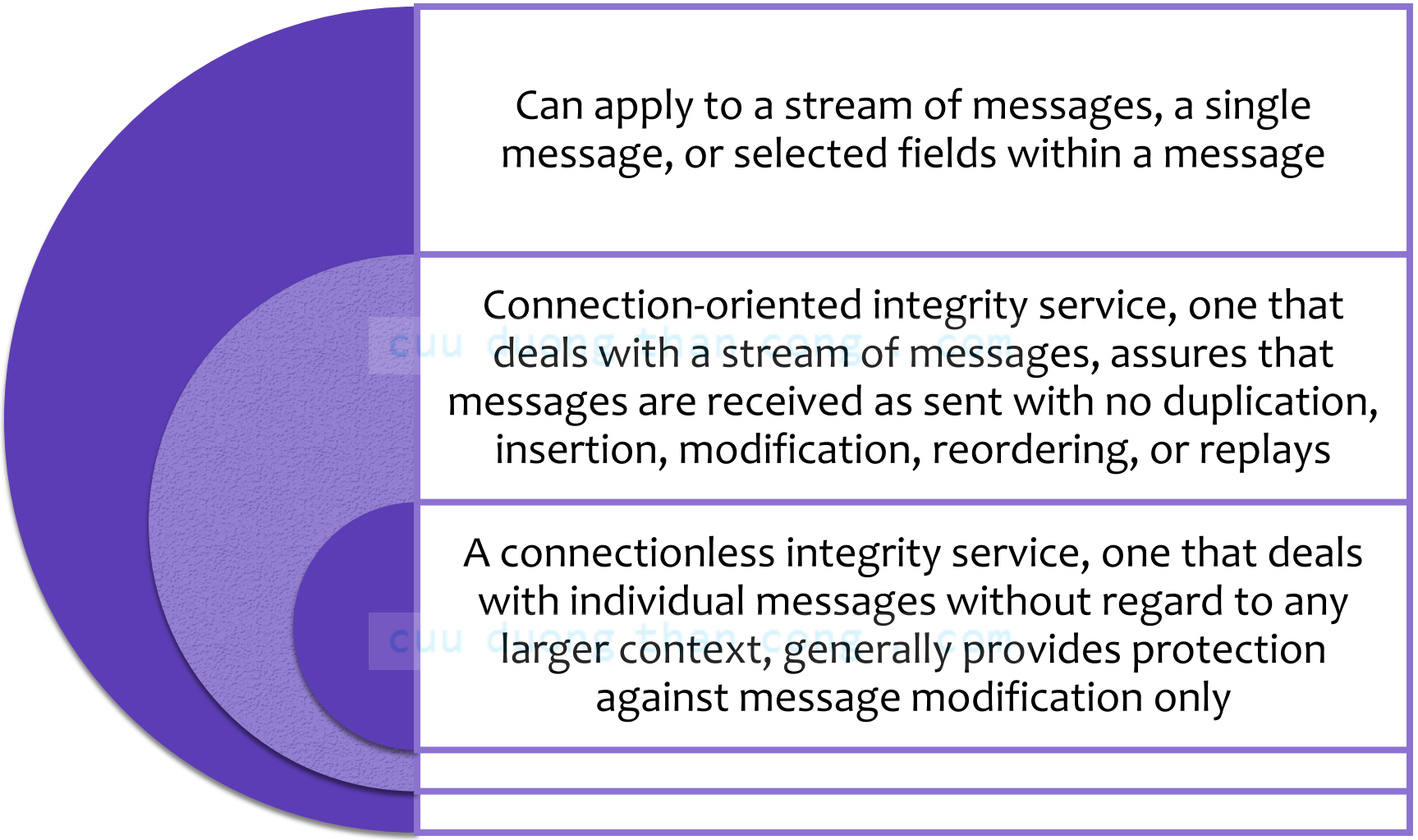
- The ability to limit and control the access to host systems and applications via communications links

- To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual

Data Confidentiality

- The protection of transmitted data from passive attacks
  - Broadest service protects all user data transmitted between two users over a period of time
  - Narrower forms of service includes the protection of a single message or even specific fields within a message
- The protection of traffic flow from analysis
  - This requires that an attacker not be able to observe the source and destination, frequency, length, or other characteristics of the traffic on a communications facility

Data Integrity



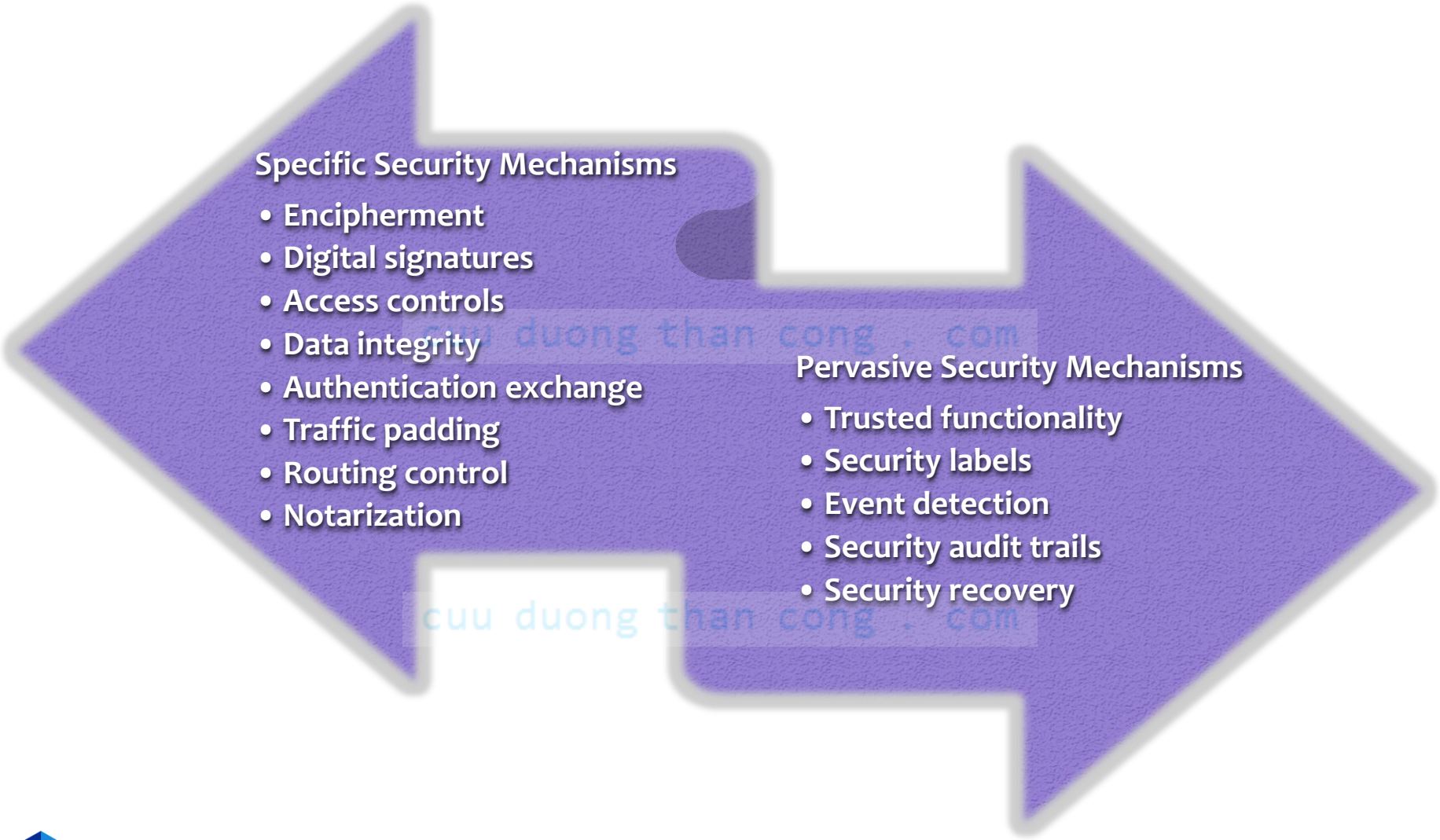
Non-repudiation

- Prevents either sender or receiver from denying a transmitted message
- When a message is sent, the receiver can prove that the alleged sender in fact sent the message
- When a message is received, the sender can prove that the alleged receiver in fact received the message

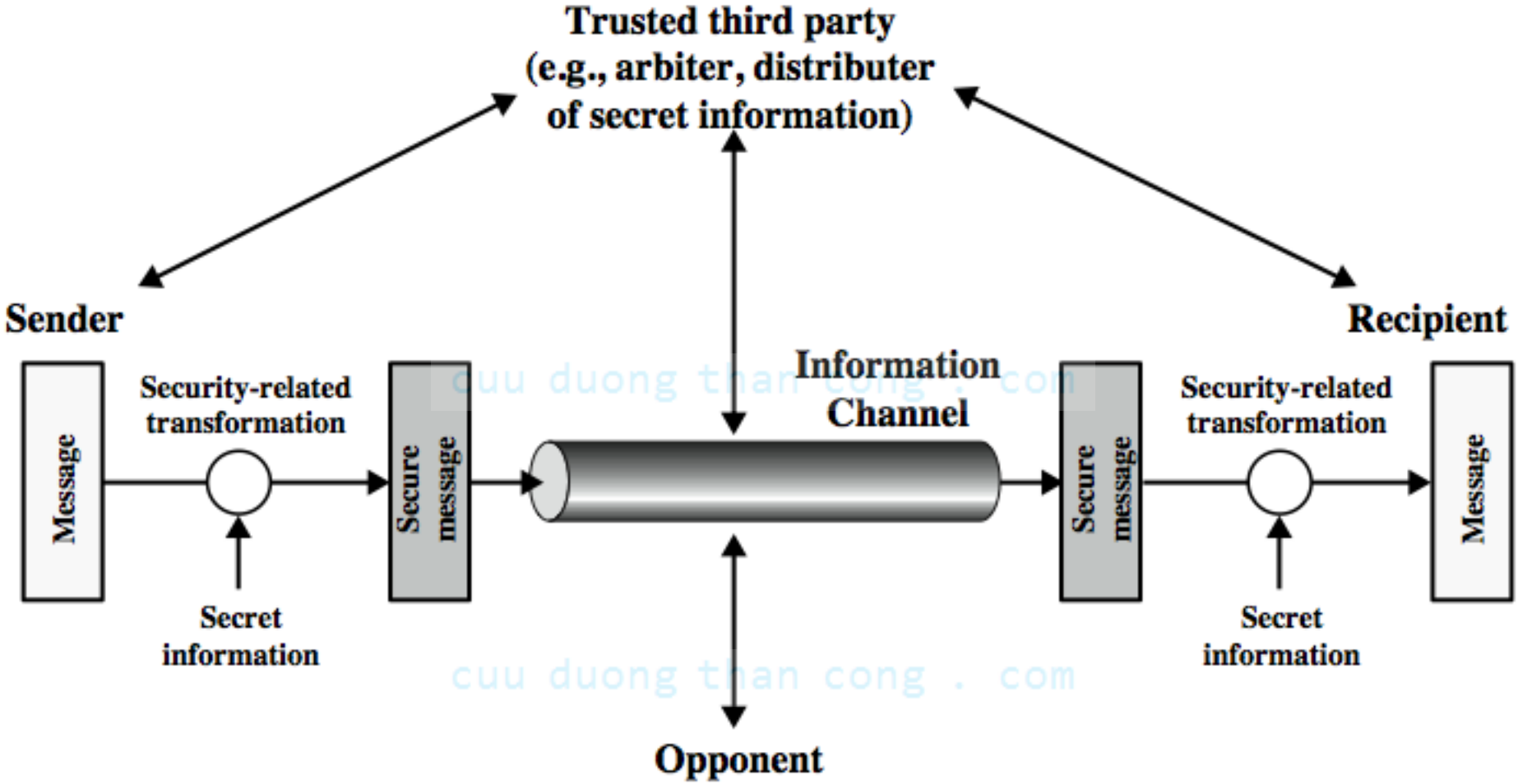
Security Mechanism

- As known as **control**
- 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

Security Mechanism (X.800)



A Model for Network Security



A Model for Network Security

- **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

A Model for Network Access Security

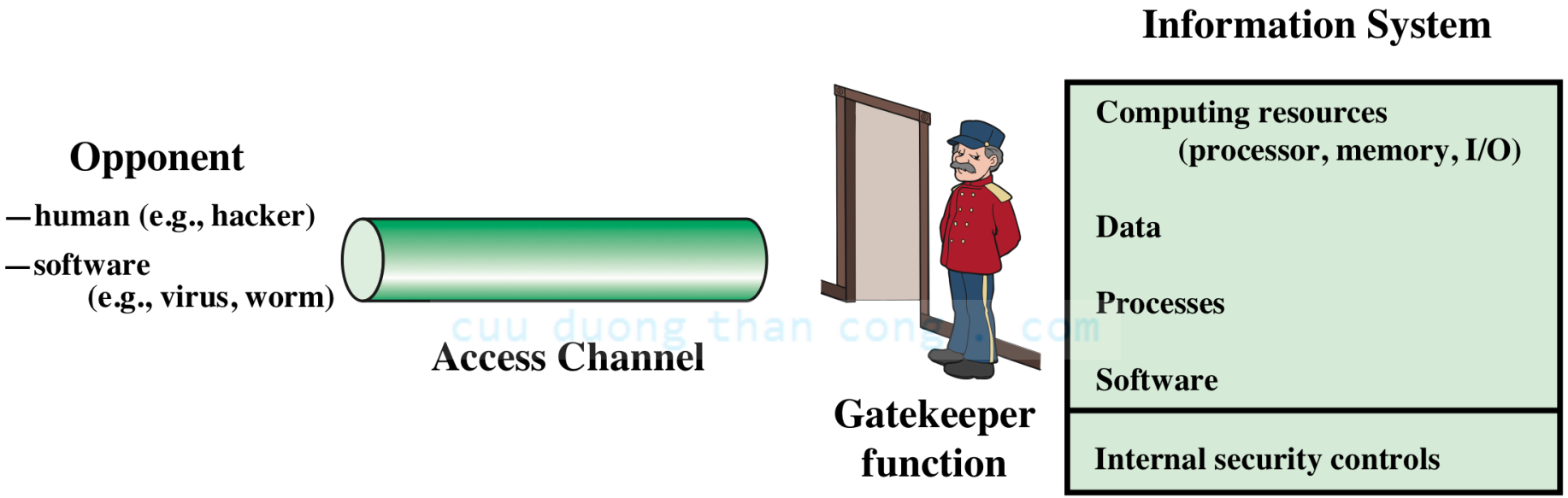


Figure 1.3 Network Access Security Model

A Model for Network Access Security

- **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

- **Note that model does not include:**
  1. monitoring of system for successful penetration
  2. monitoring of authorized users for misuse
  3. audit logging for forensic uses, etc.

Unwanted Access

- Placement in a computer system of logic that exploits vulnerabilities in the system and that can affect application programs as well as utility programs such as editors and compilers

- Programs can present two kinds of threats:
  - Information access threats
    - Intercept or modify data on behalf of users who should not have access to that data
  - Service threats
    - Exploit service flaws in computers to inhibit use by legitimate users

Some Basic Terminologies

- **plaintext** - original message
- **ciphertext** - coded message
- **cipher** - algorithm for transforming plaintext to ciphertext
- **key** - info used in cipher known only to sender/receiver
- **encipher (encrypt)** - converting plaintext to ciphertext
- **decipher (decrypt)** - recovering plaintext from ciphertext
- **cryptography** - study of encryption principles/methods
- **cryptanalysis (codebreaking)** - study of principles/ methods of deciphering ciphertext without knowing key
- **cryptology** - field of both cryptography and cryptanalysis

Summary

- Security concepts
  - Confidentiality,
  - Integrity,
  - Availability
- X.800 security architecture
- Security attacks, services, mechanisms
- Models for network (access) security

References

- *Cryptography and Network Security*, Principles and Practice, William Stallings, Prentice Hall, Sixth Edition, 2013

cuu duong than cong . com