OSI SECURITY ARCHITECTURE

UNIT 1 : TCS 491

INTRO TO CRYPTOGRAPHY

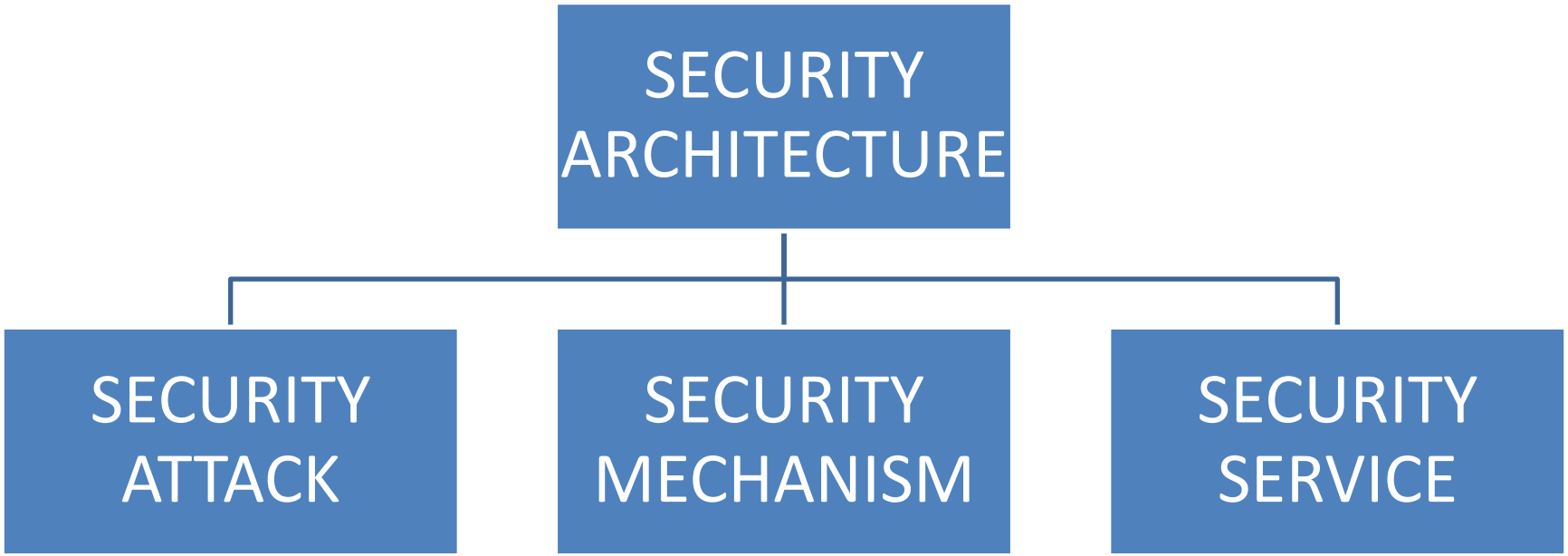
Security Architecture for OSI

- ITU-T Recommendation X.800, Security Architecture for OSI defines systematic way to
  - Define the requirements for security
  - Characterizing the approaches to satisfying those requirements

ITU-T- international Telecommunication Union

OSI- Open Systems Interconnections

OSI Security Architecture



OSI Security Architecture

The following concepts are used:

- **Security attack** : Any actions that compromises the security of information owned by an organization (or a person)
- **Security mechanism**: a mechanism that is designed to detect, prevent, or recover from a security attack
- **Security service**: a service that enhances the security of the data processing systems and the information transfers of an organization. The services make use of one or more security mechanisms to provide the service

ATTACK

GAINING THE ACCESS OF DATA BY UNAUTHORISED USER

GAINING MEANS :

1. **ACCESSING DATA**
2. **MODIFYING DATA**
3. **DESTROYING DATA**

TWO TYPES OF ATTACK :

1. **PASSIVE**
2. **ACTIVE ATTACK**

PASSIVE ATTACK : NO MODIFICATION IS DONE BY THE UNAUTHORISED PERSON

ACTIVE : MODIFICATION IS DONE BY THE UNAUTHORISED PERSON

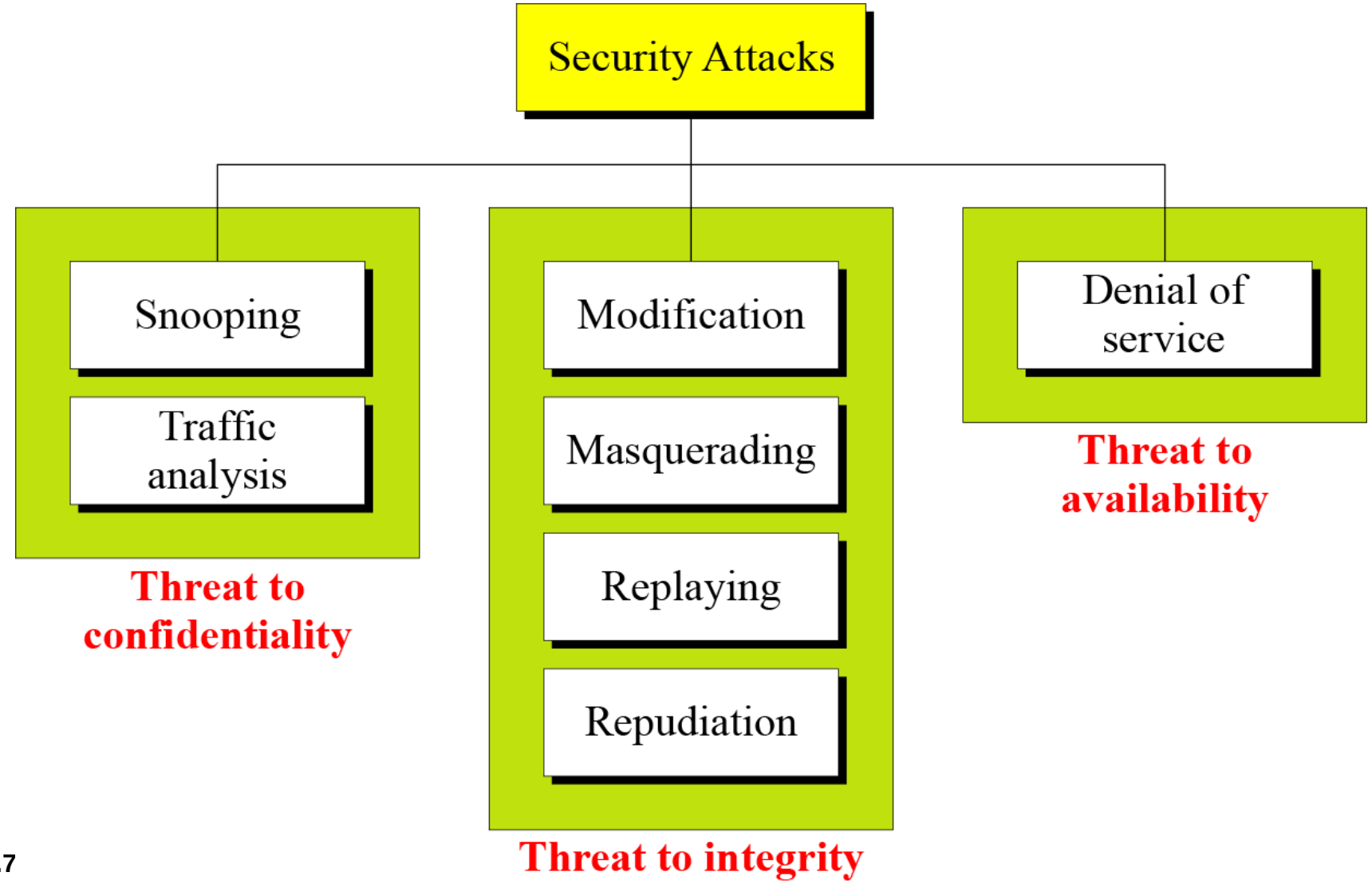
ATTACKS

The three goals of security—confidentiality, integrity, and availability—can be threatened by security attacks.

1 Attacks Threatening Confidentiality
2 Attacks Threatening Integrity
3 Attacks Threatening Availability

1.2 Continued

Taxonomy of attacks with relation to security goals



Attacks Threatening Confidentiality

Snooping refers to unauthorized access to or interception of data.

Traffic analysis refers to obtaining some other type of information by monitoring online traffic.

Attacks Threatening Integrity

Modification means that the attacker intercepts the message and changes it.

Masquerading or spoofing happens when the attacker impersonates somebody else.

Replaying means the attacker obtains a copy of a message sent by a user and later tries to replay it.

Repudiation means that sender of the message might later deny that she has sent the message; the receiver of the message might later deny that he has received the message.

REPLAY ATTACK

- A REPLAY ATTACK OCCURS WHEN AN UNAUTHORIZED USER CAPTURES NETWORK TRAFFIC AND THEN SEND THE COMMUNICATION TO ITS ORIGINAL DESTINATION
- TO PREVENT : USE TIMESTAMPS & SEQUENCE NUMBERS
- IF THE TIMESTAMP IS BEYOND A CERTAIN TIME THEN THE PACKET IS DISCARDED.

Attacks Threatening Availability

Denial of service (DoS) is a very common attack. It may slow down or totally interrupt the service of a system.

Passive Versus Active Attacks

Table *Categorization of passive and active attacks*

ATTACKS	TYPE	THREAT
SNOOPING TRAFFIC ANALYSIS	PASSIVE	CONFIDENTIALITY
MODIFICATION MASQUERADING REPLAYING REPUDIATION	ACTIVE	INTEGRITY
DENIAL OF SERVICE	ACTIVE	AVAILABILITY

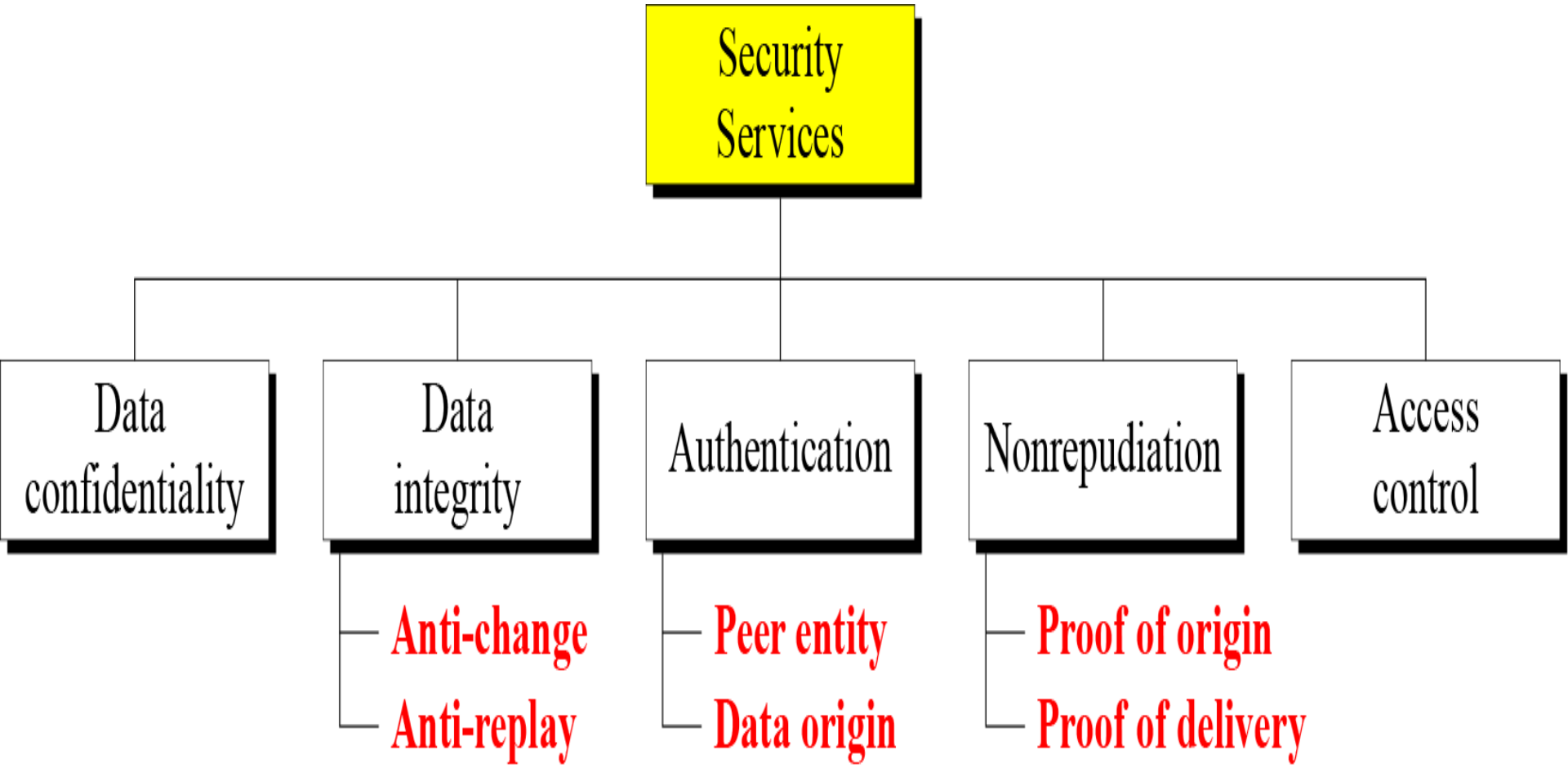
SERVICES AND MECHANISMS

ITU-T provides some security services and some mechanisms to implement those services. Security services and mechanisms are closely related because a mechanism or combination of mechanisms are used to provide a service..

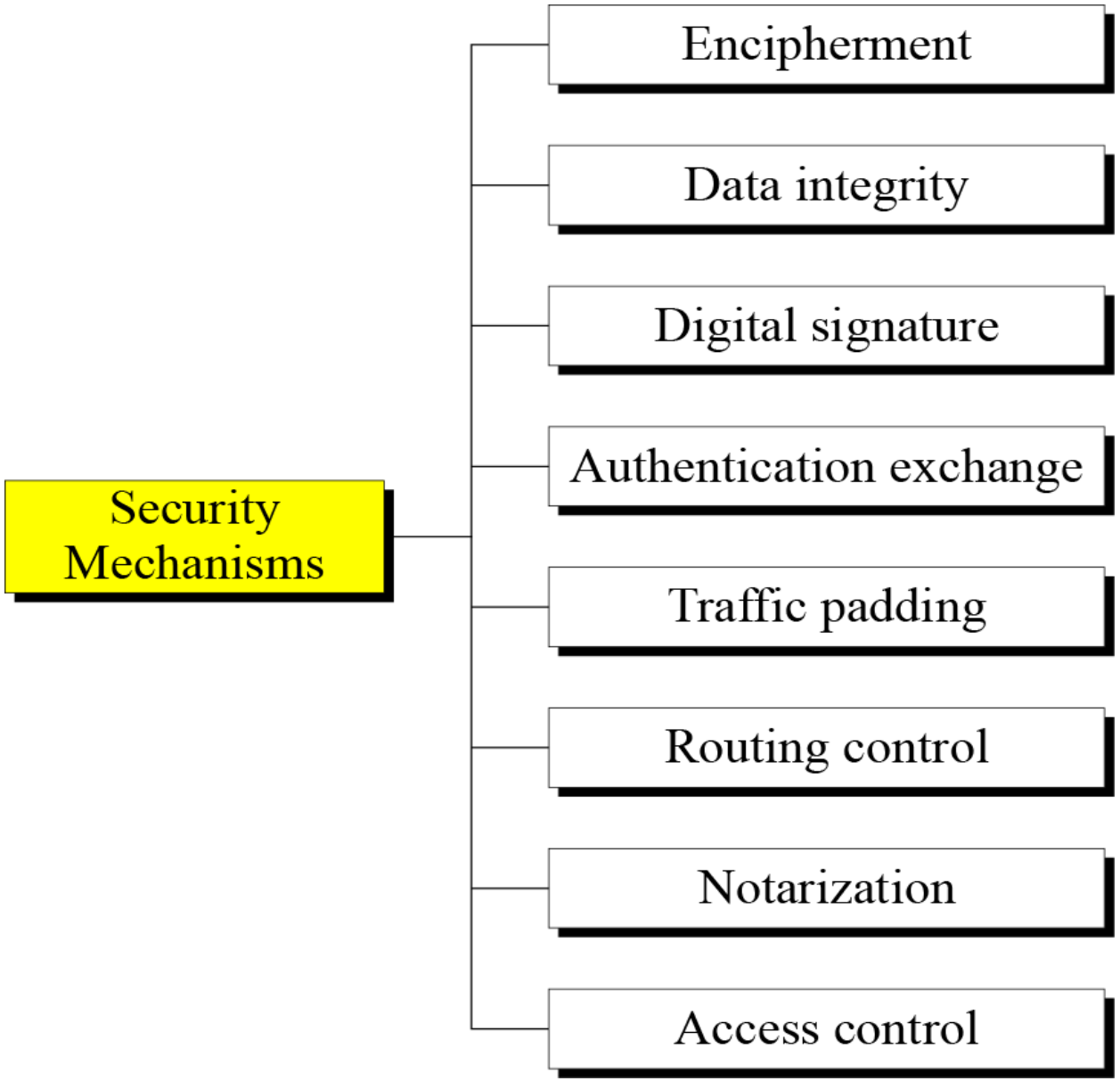
Main Topics :

1 Security Services (5 Types)
2 Security Mechanism (8 Types)
3 Relation between Services and Mechanisms

Security Services



Security Mechanism



Relation between Services and Mechanisms

Security Service	*Security Mechanism*
Data confidentiality	Encipherment and routing control
Data integrity	Encipherment, digital signature, data integrity
Authentication	Encipherment, digital signature, authentication exchanges
Nonrepudiation	Digital signature, data integrity, and notarization
Access control	Access control mechanism