Cryptography (CS-501)

Introduction

Dr Samayveer Singh
Assistant Professor
Department of Computer Science & Engineering
National Institute Technology Jalandhar, Punjab, India
samays@nitj.ac.in

Secure Communication

Needs and Requirements

Well established needs for secure communication

- ✓ War time communication,
- ✓ Business transactions,
- ✓ Email sharing,
- ✓ Payments using cards,
- ✓ Electronic commerce,
- ✓ Computer passwords,
- ✓ Digital currencies,
- ✓ Sim card authentication,
- ✓ Social media communication platforms,
- ✓ etc.

Secure Communication

- ✓ Information Security requirements have changed in recent times
- ✓ traditionally provided by physical and administrative mechanisms
  - ➢ Rugged filing cabinets with locks
  - ➢ Personnel screening procedures during hiring process
- ✓ Computer use requires automated tools to protect files and other stored information
  - ➢ It is the case for a shared system that can be accessed over a public telephone network, data network, or the Internet.
- ✓ Use of networks and communications links requires measures to protect data during transmission

Secure Communication

- ✓ **Computer Security -** generic name for the collection of tools designed to protect data and to thwart hackers
- ✓ **Network Security -** measures to protect data during their transmission
- ✓ **Internet Security -** measures to protect data during their transmission over a collection of interconnected networks

Aim of Course

In this course, our focus is on Internet Security which consists of measures to deter, prevent, detect, and correct security violations that involve the transmission & storage of information.

1. SECURITY GOALS

There are three security goals and their taxonomy are given as follows.

- ✓ **Confidentiality**
- ✓ **Integrity**
- ✓ **Availability**

Figure 1: Taxonomy of Security Goals

1.1 Confidentiality

- ✓ **Confidentiality is probably the most common aspect of information security.**
- ✓ **We need to protect our confidential information.**
- ✓ **An organization needs to guard against those malicious actions that endanger the confidentiality of its information.**

1.2 Integrity

- ✓ **Information needs to be changed constantly.**
- ✓ **Integrity means that changes need to be done only by authorized entities and through authorized mechanisms.**

1.3 Availability

- ✓ **The third component of information security is availability.**
- ✓ **The information created and stored by an organization needs to be available to authorized entities.**
- ✓ **Information needs to be constantly changed, which means it must be accessible to authorized entities.**

2. CRYPTOGRAPHIC ATTACKS

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

Security attacks- any action that compromises the security of information owned by an organization.

Information security is about how to prevent attacks, or failing that, to detect attacks on information-based systems

- ✓ **Attacks Threatening Confidentiality**
- ✓ **Attacks Threatening Integrity**
- ✓ **Attacks Threatening Availability**
- ✓ **Passive versus Active Attacks**

Continued….

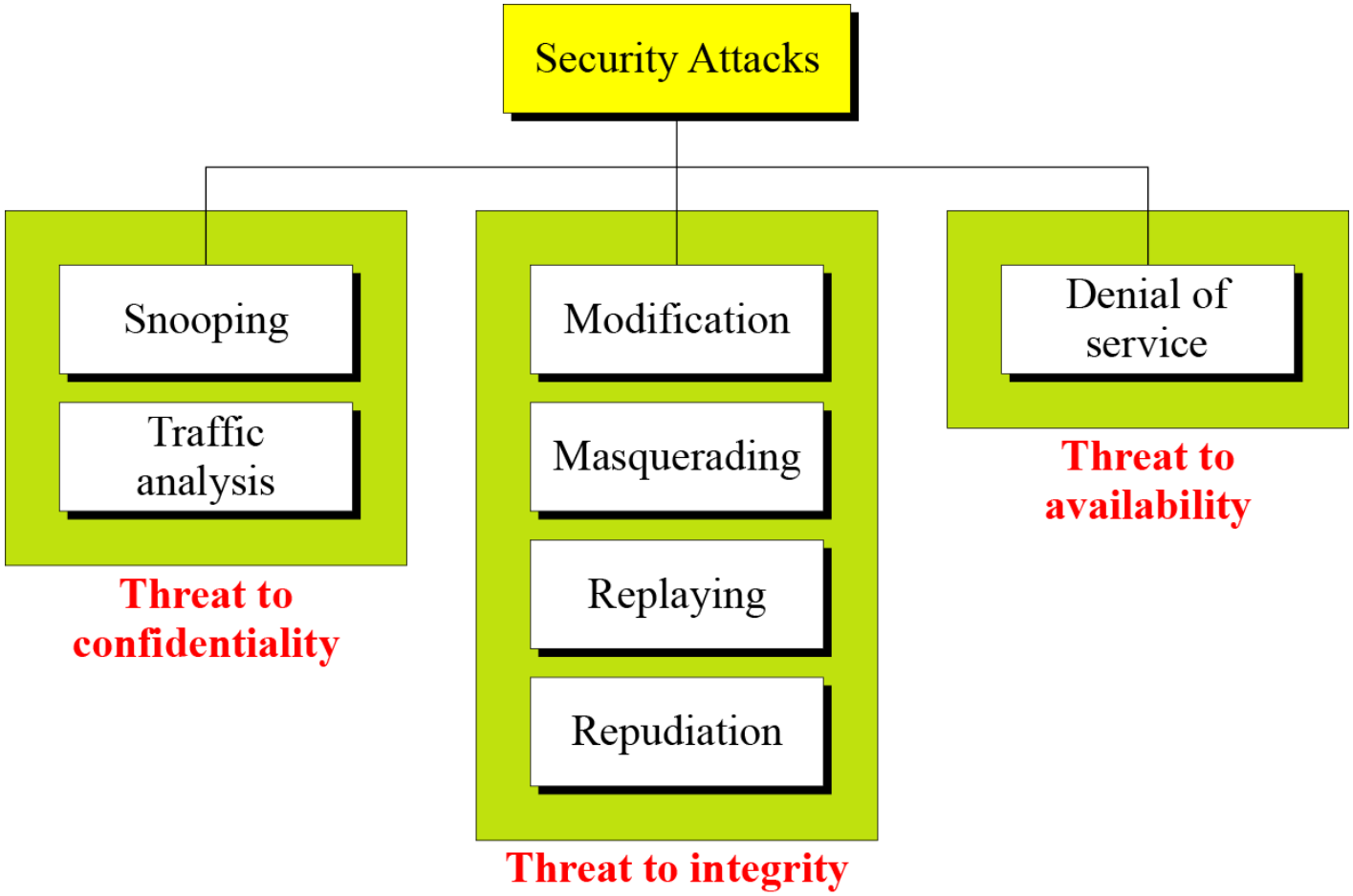


Figure 2 **Taxonomy of attacks with relation to security goals**

2.1. 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.**

2.2. Attacks Threatening Integrity

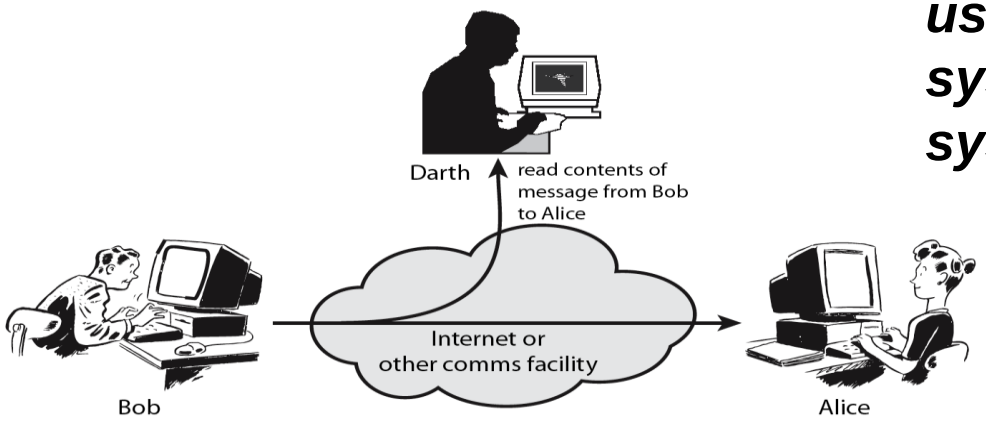
- ✓ **Modification means that the attacker intercepts the message and changes it.**
- ✓ **Masquerading or spoofing happens when the attacker impersonates somebody else.**
- ✓ **Replaying means the attacker obtains a copy of a message sent by a user and later tries to replay it.**
- ✓ **Repudiation means 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.**

2.3. Attacks Threatening Availability

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

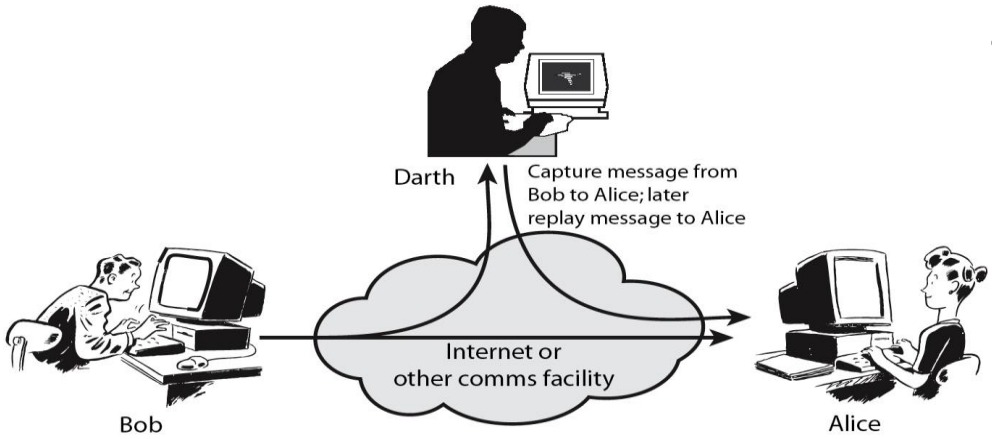
2.4. Passive Versus Active Attacks

Passive Attacks



attempt to learn or make use of information from the system but does not affect system resources.

Active Attacks



attempt to alter system resources or affect their operation.

2.4. Passive Versus Active Attacks

Table 1 *Categorization of passive and active attacks*

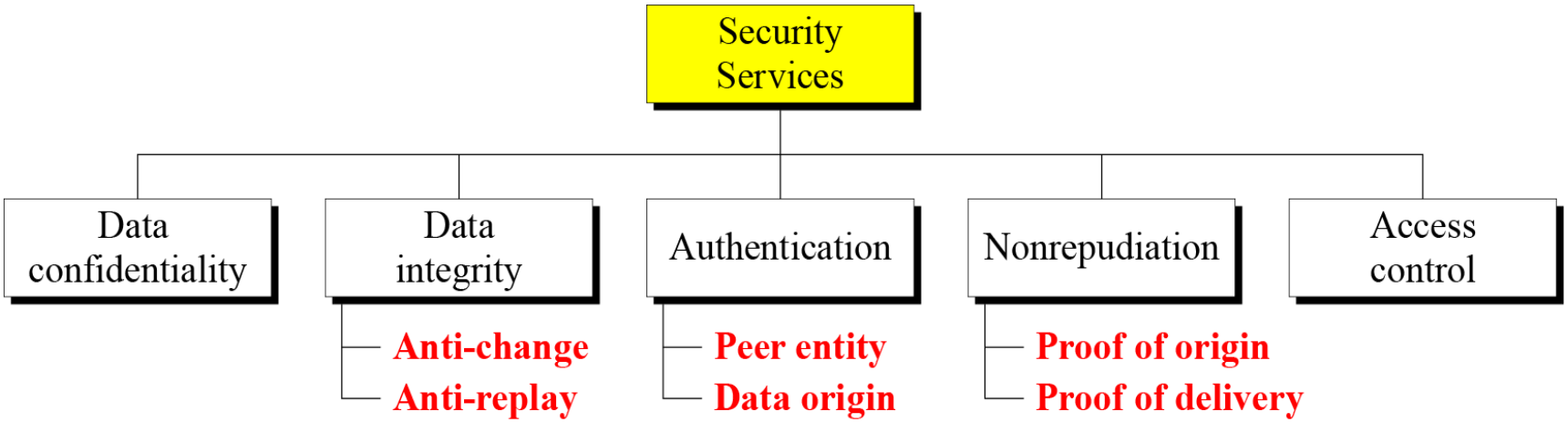
Attacks	*Passive/Active*	*Threatening*
Snooping Traffic analysis	Passive	Confidentiality
Modification Masquerading Replaying Repudiation	Active	Integrity
Denial of service	Active	Availability

3. 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..

- ✓ **Security Services**
- ✓ **Security Mechanism**
- ✓ **Relation between Services and Mechanisms**

3.1 Security Services



3.2 Security Mechanism

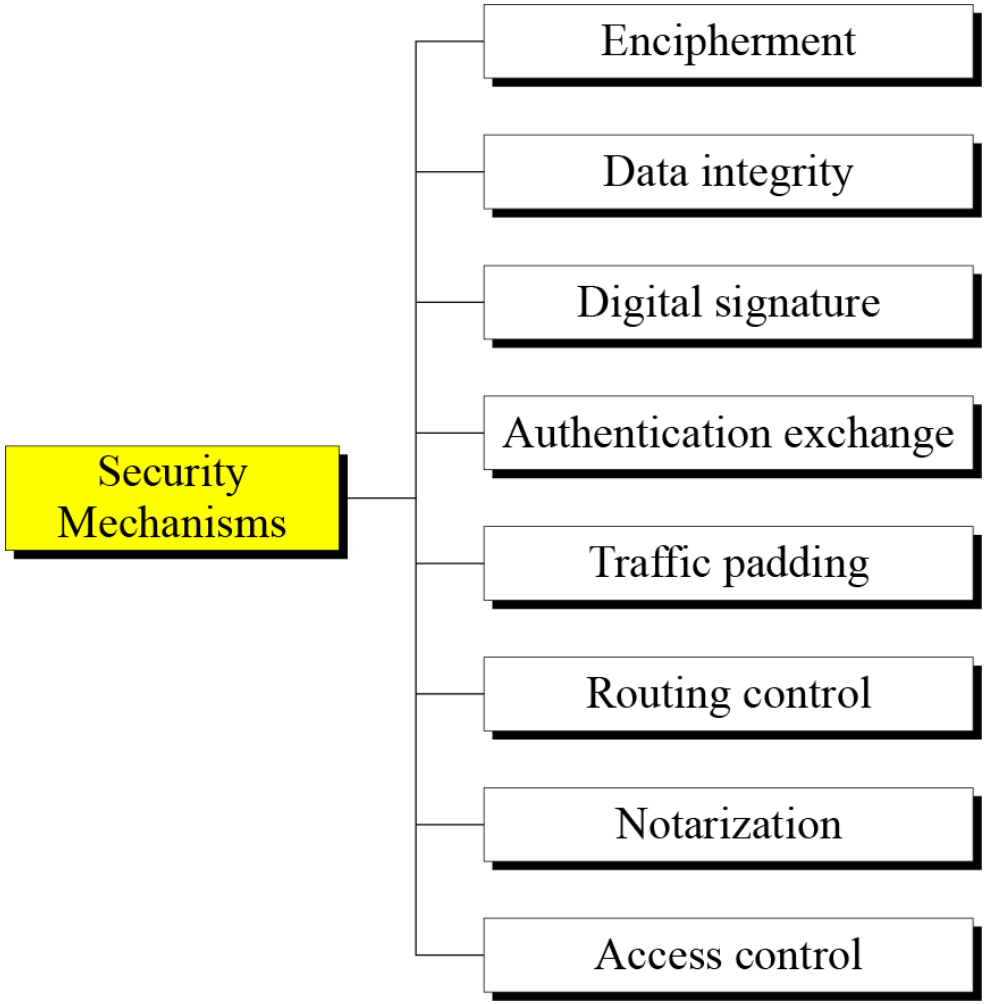


Figure 4 ***Security mechanisms***

3.3 Relation between Services and Mechanisms

Table 2 ***Relation between security 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

4 TECHNIQUES

Mechanisms discussed in the previous sections are only theoretical recipes to implement security. The actual implementation of security goals needs some techniques.

Two techniques are prevalent today:

- ✓ **Cryptography**
- ✓ **Steganography**

4.1 Cryptography

- ***Cryptography, a word with Greek origins, means "secret writing."***
- ***However, we use the term to refer to the science and art of transforming messages to make them secure and immune to attacks.***
- ***Cryptography is the science of secret, or hidden writing***

4.2 Steganography

- ✓ ***The word steganography, with origin in Greek, means "covered writing," in contrast with cryptography, which means "secret writing."***

Example: covering data with text

This book is mostly about cryptography, not steganography.

□ □□□ □ □ □ □□

0 1 0 0 0 0 1

4.2 Continued

Example: using dictionary

A	friend	called	a	doctor.
0	10010	0001	0	01001

Example: covering data under color image

01010011	10111110	01010101
01011110	10111110	01100101
01111110	01001010	00010101