INFORMATION SECURITY

LECTURE 1

Security - An Introduction

Khalid Abdullah

MSc computer and Network Security

Computer Science Dept.

University Of Zakho

OUTLINE

Security: some basic definitions

- Security services
  - •Confidentiality
  - •Authentication
  - •Integrity
  - •Non-repudiation
  - •Access control
  - •Availability

Attacks

Security mechanisms

LESSON OBJECTIVE

- Understand the need of Security
- Identify and discuss basic security services
- Describe security mechanisms
- Understand and discuss various attacks

Understand the need of Security

- Information needs to be kept about every aspect of our live.
- Information is an asset, it need to be secured from attacks.
- Information need to be hidden from unauthorized.
- Information need to be protected from unauthorized change.
- Information need to be available to an authorized entity when needed.

SECURITY?

- *"A judgment of how likely it is that the system can resist accidental or deliberate intrusion"*

  - Ian Somerville

- *"Security is keeping anyone from doing things you do not want them to do to, with, or from your computers or any peripherals"*

  -William R. Cheswick

- *"Security is risk management"*

  -Bruce Schneider

SECURITY SERVICES

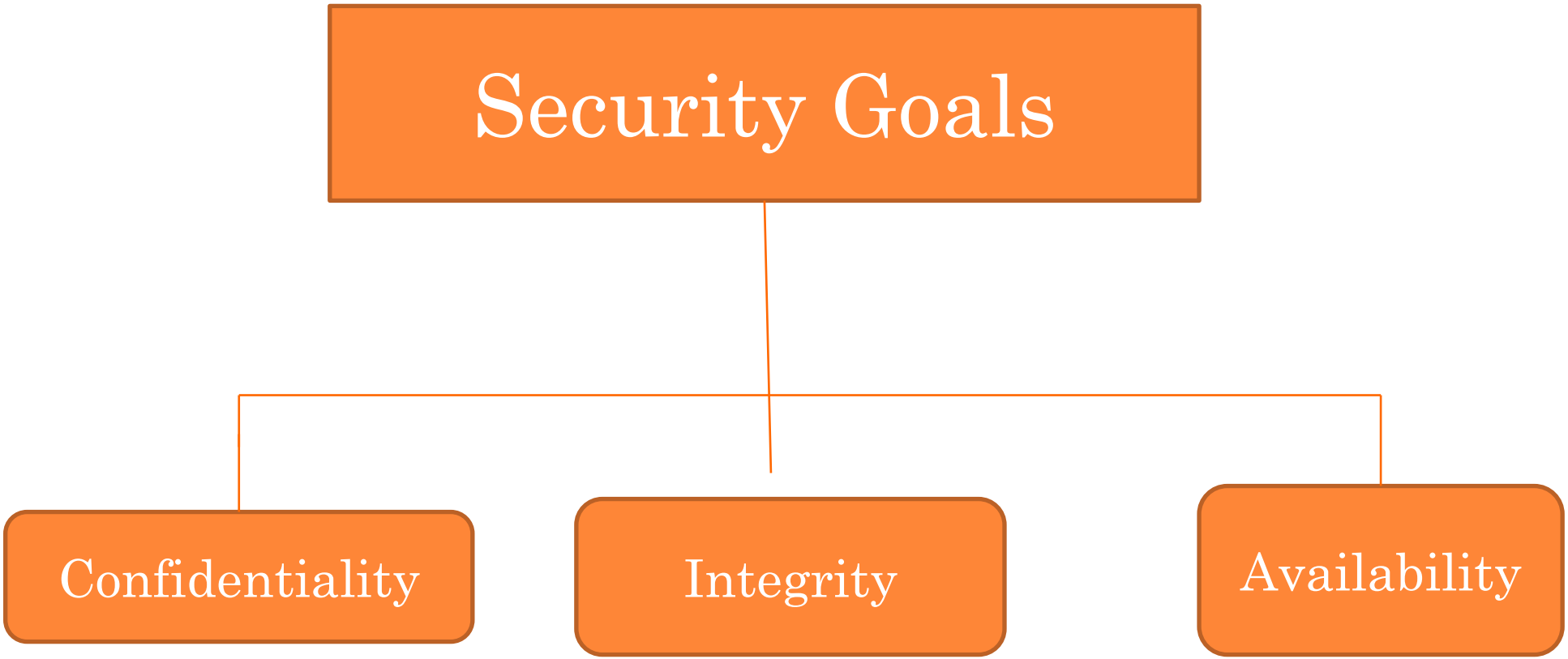
A security service as one provided by a protocol layer ISO X(800)

Security services are implemented through security mechanisms RFC2828

Services

- Confidentiality
- Authentication
- Nonrepudiation
- Integrity
- Availability
- Access control

- Mechanisms
- Encryption
- Hash
- Digital signature


Security Goals
Confidentiality
Integrity
Availability

What is Network Security?

- **Confidentiality:** "The property that information is not made available or disclosed to unauthorized individuals, entities, or processes [i.e., to any unauthorized system entity]."

- only sender, intended receiver should "understand" message contents, sender encrypts message receiver decrypts message.

Integrity

- **Data integrity:** "The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner."

- **System integrity:** "The quality that a system has when it can perform its intended function in a unimpaired manner, free from deliberate or in advertent unauthorized manipulation."

Availability

- "The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system; i.e., a system is available if it provides services according to the system design whenever users request them."

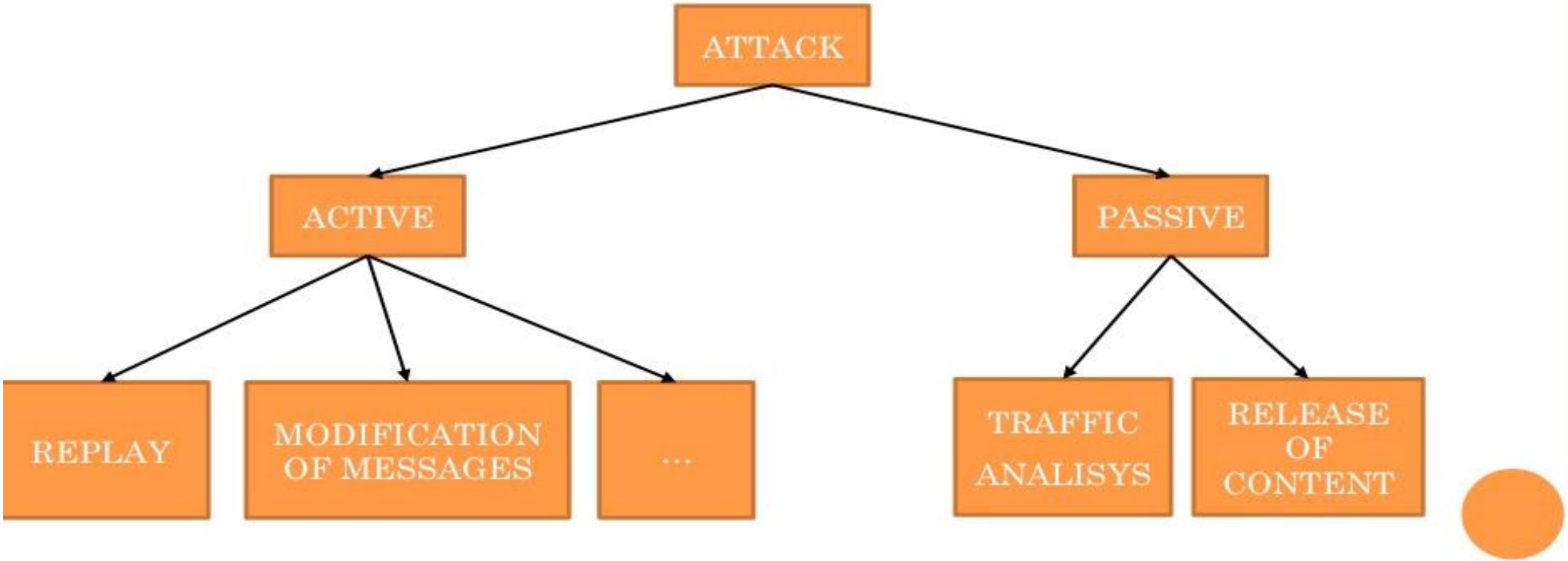
- Turning off a computer provides confidentiality and integrity, but hurts availability…

- Denial of service attacks are direct assaults on availability

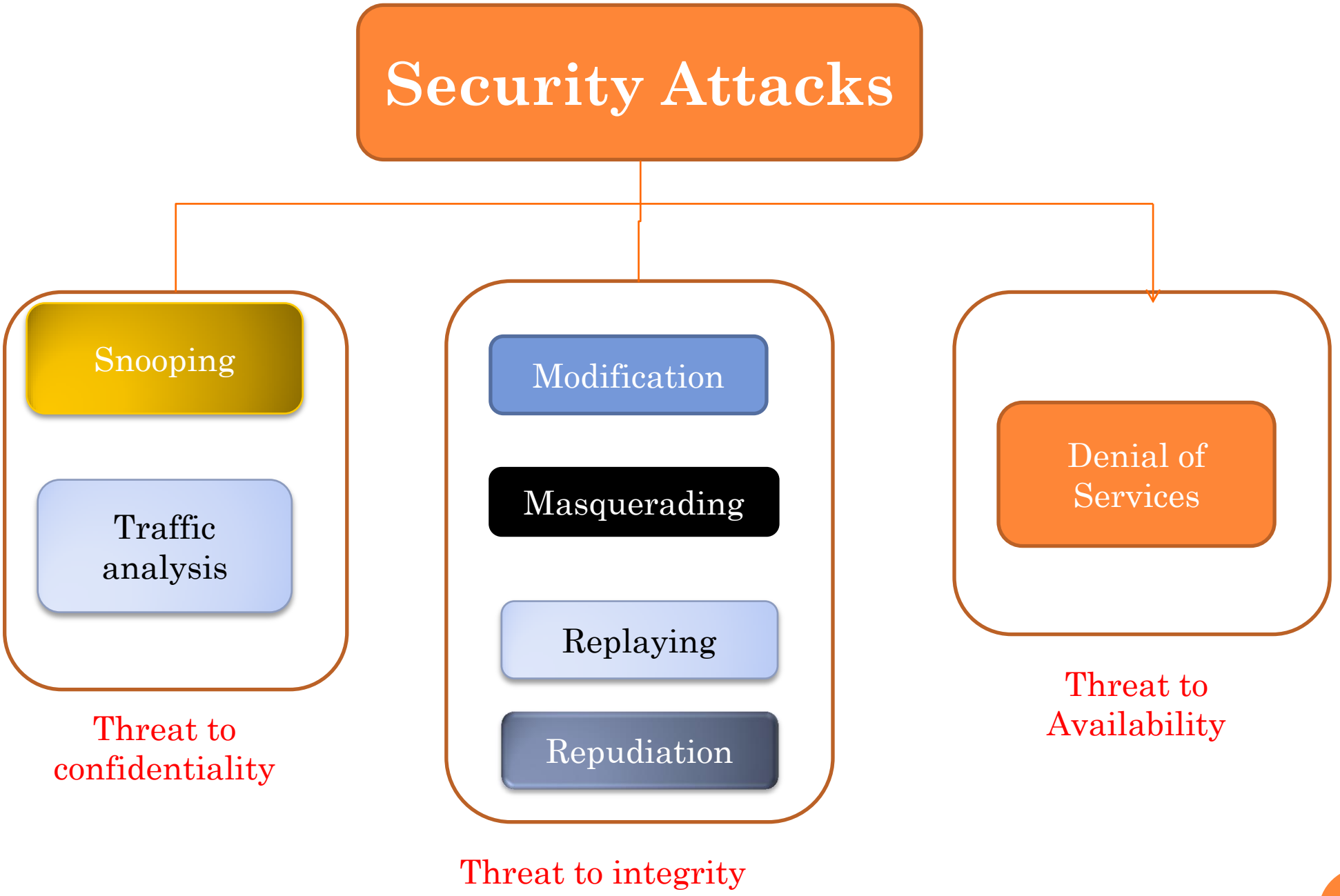
ATTACKS

Attacks are prevented using security services

ISO X800 and RFC2828 classify attacks as passive and active



Security Attacks



Attacks threatening confidentiality

- **Snooping:** Refers to unauthorized access to or interception of data. For example, a file transferred through the internet may contain confidential information.
- Unauthorized entity may intercept the transmission and use the contain for own benefit.
- By using encipherment technique the data can be unintelligible to the interceptor (prevent snooping).

- **Traffic analysis:** Getting some information by monitoring online traffic such as email address of the sender or receiver even the data is unintelligible for the intercepter.
- It is possible to collect a pair of requests and responses to help his/her guess for nature transaction.

Attacks threatening integrity

- **Modification:** it is the intercepter ability to accessing the data and modify the information for his own benefit (tamper with information or network resources).

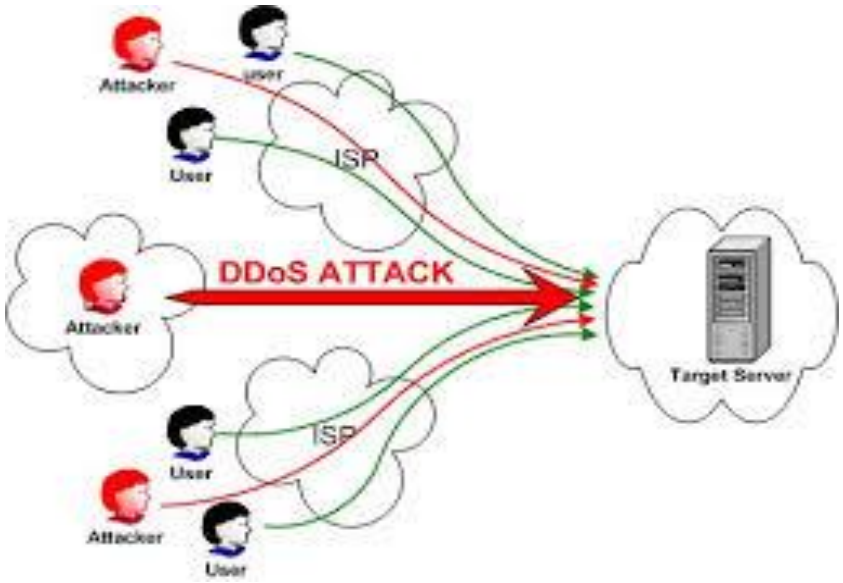
- **Masquerading (Spoofing**): It happens when the attacker impersonates somebody to obtain some sensitive information from the user such as PIN code for bank card.
- In an interception attack (snooping), an unauthorised individual gains access to confidential or private information.

- **Replaying:** The attacker obtains a copy of message sent by a user and later tries to replay it.

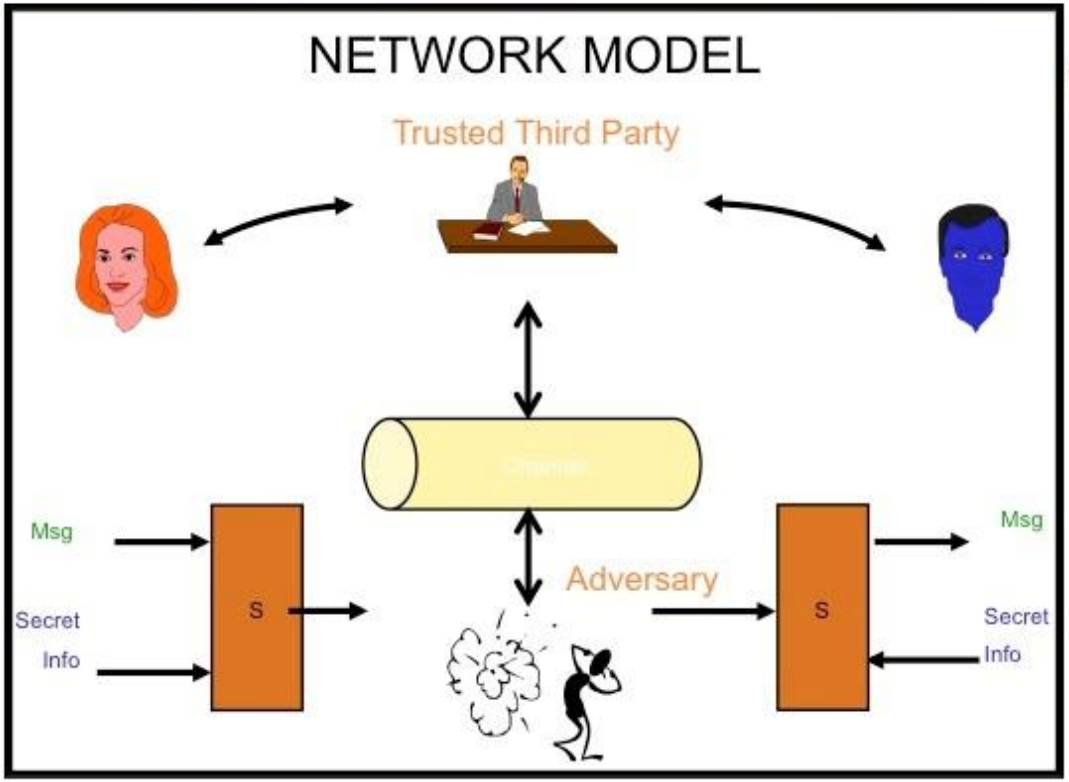
- **Repudiation:** It is the process of denying by the sender or receiver that he/she transmitted any message to other party.

Attacks Threatening the availability

- **Denial Of Service (DoS):** is an attempt to make a machine or network resource unavailable to its intended users.
- Slow down the system and then interrupt the service to the users.
- The attacker may send so many bogus requests to the server that the server crashes because of heavy load.



NETWORK SECURITY MODEL

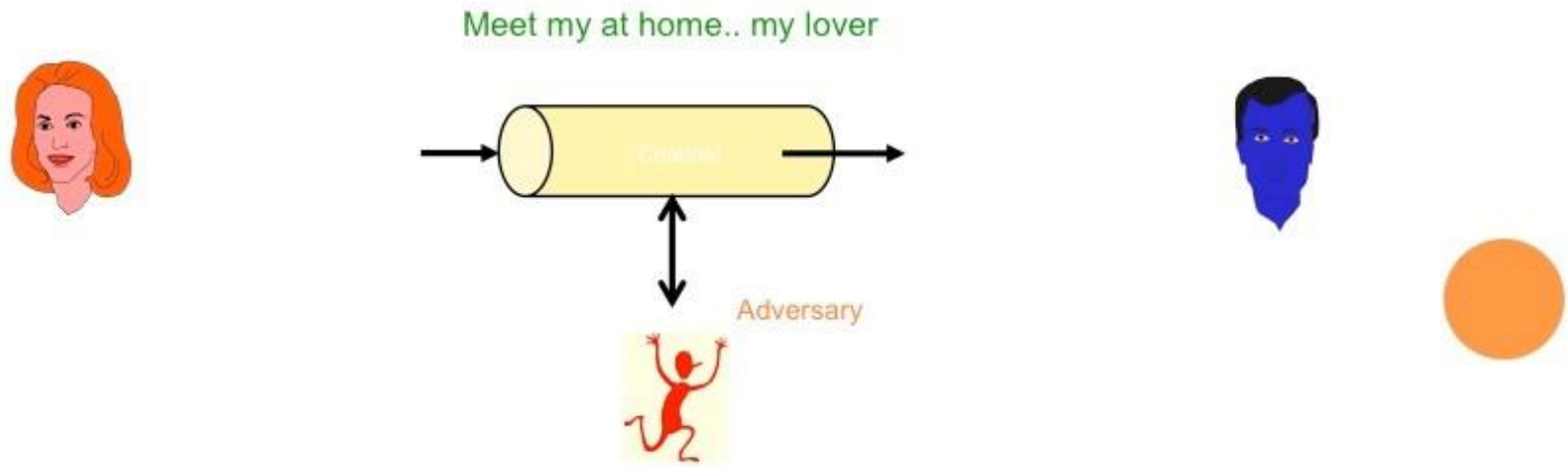


- A **model** is a simplified version of the reality to study
  - Security **services**
  - Security **attacks**
  - Security **mechanisms**

A **security service** is implemented through one or more **security mechanisms** and is used as a countermeasure for **security attacks**.

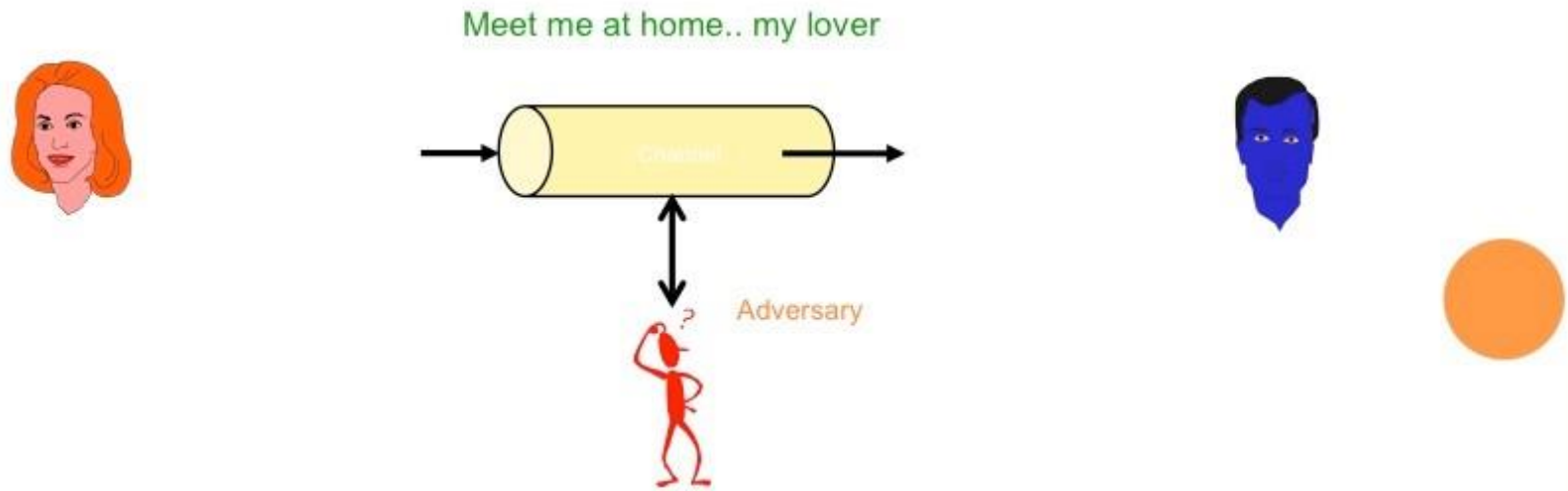
SECURITY SERVICES: CONFIDENTIALITY

- THREAT
  - **Interception:** an unauthorized entity gain access to data



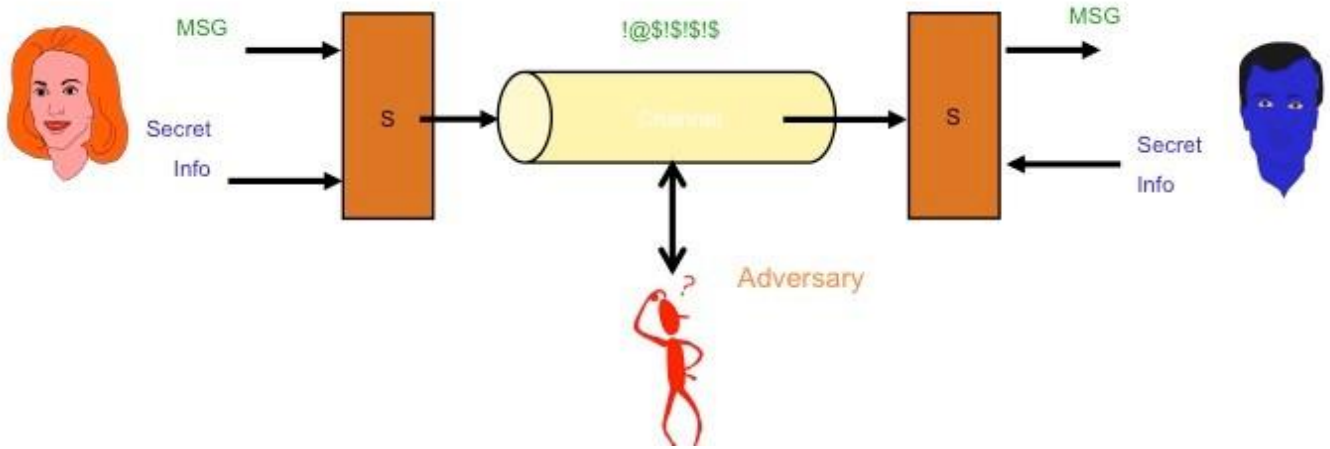
SECURITY SERVICES: CONFIDENTIALITY

- THREAT
  - **Interception:** an unauthorized entity gain access to data
- SECURITY SERVICE
  - **CONFIDENTIALITY**: ensuring that information is accessible only to those authorized to have access



SECURITY SERVICES: CONFIDENTIALITY

- THREAT
  - **Interception:** an unauthorized entity gain access to data
- SECURITY SERVICE
  - **CONFIDENTIALITY**: ensuring that information is accessible only to those authorized to have access
- SECURITY MECHANISMS
  - **ENCRYPTION**: for instance symmetric (AES) and asymmetric (RSA) cryptography



SECURITY SERVICES: AUTHENTICATION

- THREAT
  - FABRICATION: Insertion of "counterfeit" messages

SECURITY SERVICES: AUTHENTICATION

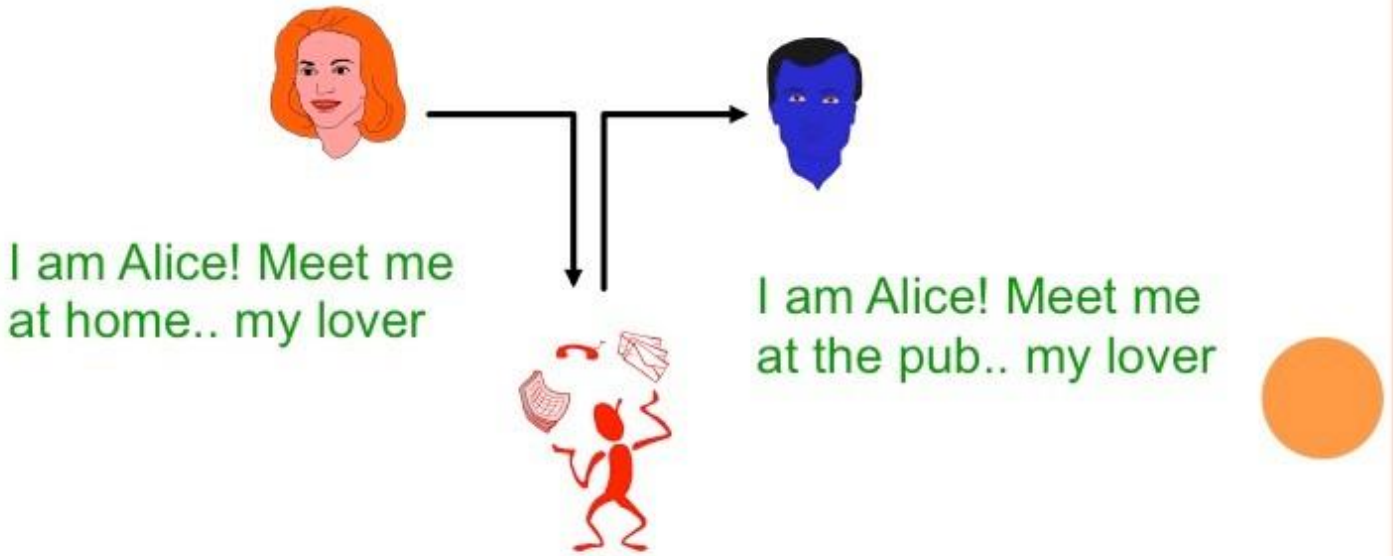
- THREAT
  - FABRICATION: Insertion of "counterfeit" messages
- SECURITY SERVICE
  - AUTHENTICATION: the entity is whom he claims to be

SECURITY SERVICES: AUTHENTICATION

- THREAT
  - FABRICATION: Insertion of "counterfeit" messages
- SECURITY SERVICE
  - AUTHENTICATION: the entity is whom he claims to be
- SECURITY MECHANISMS
  - AUTHENTICATION PROTOCOLS: Kerberos, X.509 authentication service

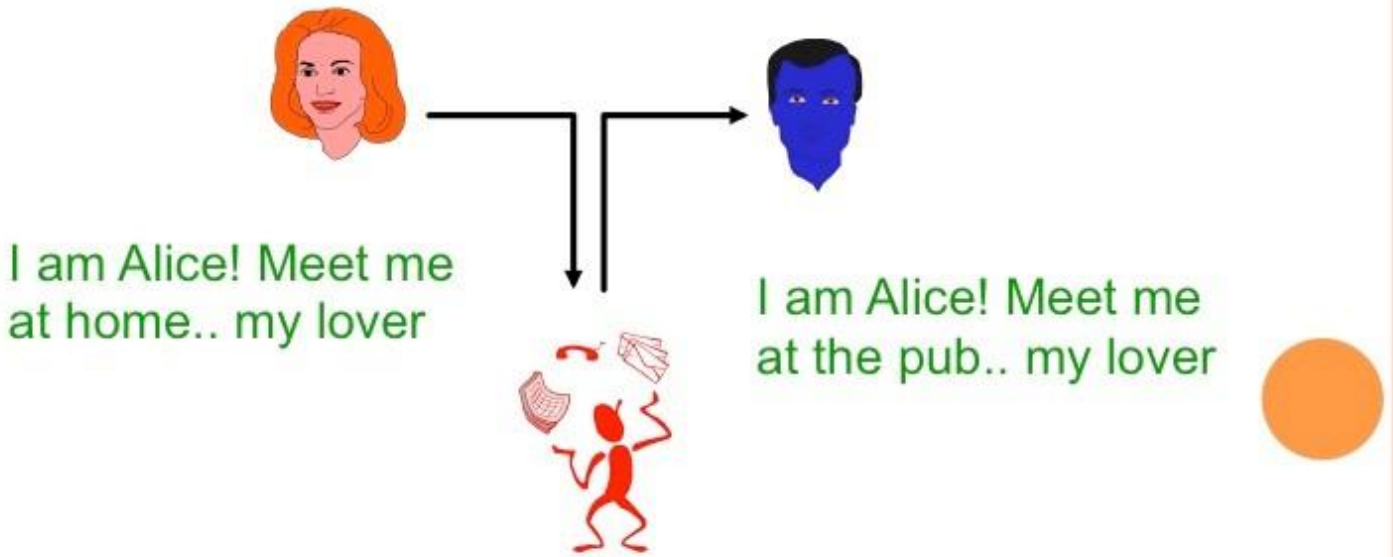
Security Services: Integrity

- THREAT
  - MODIFICATION: Gain access and “tampers” with messages



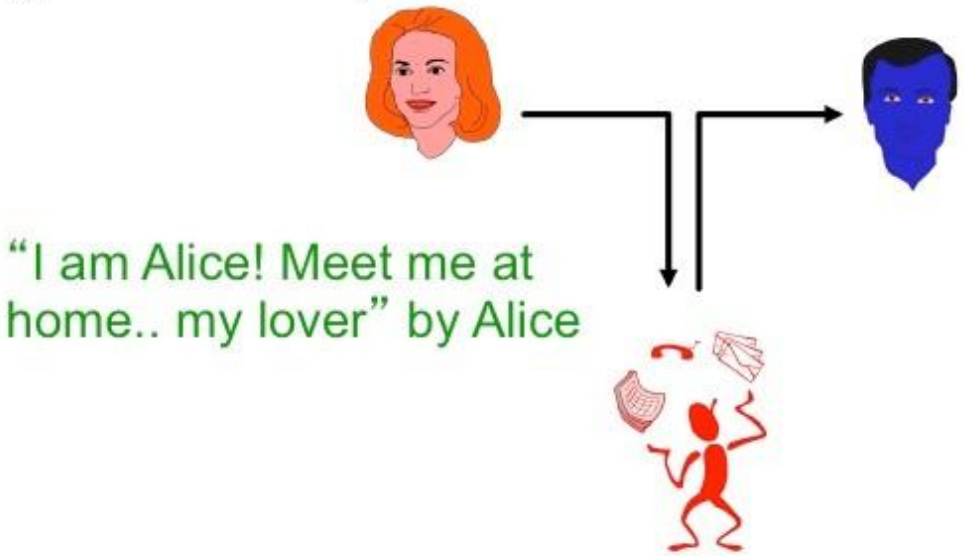
Security Services: Integrity

- THREAT
  - MODIFICATION: Gain access and “tampers” with messages
- SECURITY SERVICE
  - INTEGRITY: the message is received as it was sent



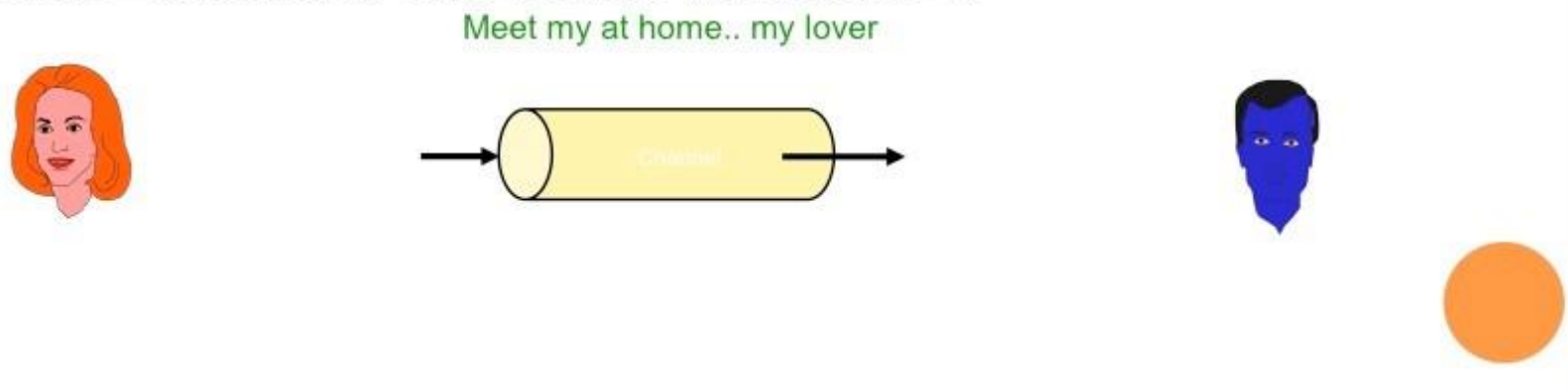
SECURITY SERVICES: INTEGRITY

- THREAT
  - MODIFICATION: Gain access and “tampers” with messages
- SECURITY SERVICE
  - INTEGRITY: the message is received as it was sent
- SECURITY MECHANISMS
  - Digital signature: DSA, RSA with SHA-1



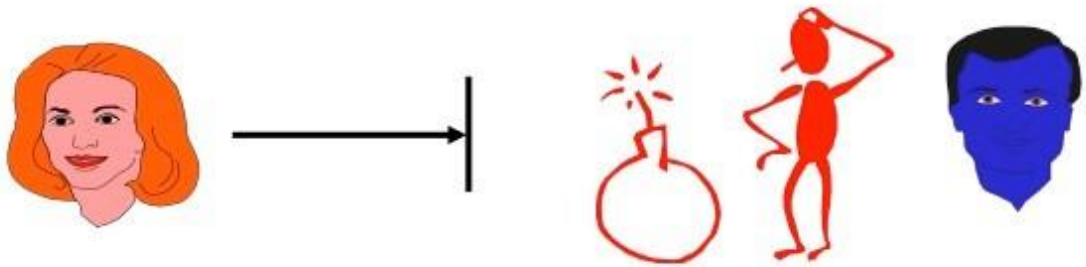
SECURITY SERVICES: NON-REPUDIATION

- THREAT
  - REPUDIATION ATTEMPT: Party anonymously publishes his or her message/key(s) and falsely claims that they were stolen
- SECURITY SERVICE
  - NON-REPUDIATION: the entity cannot deny sending/ receiving a message
- SECURITY MECHANISMS
  - DIGITAL SIGNATURE: RSA with SHA-1



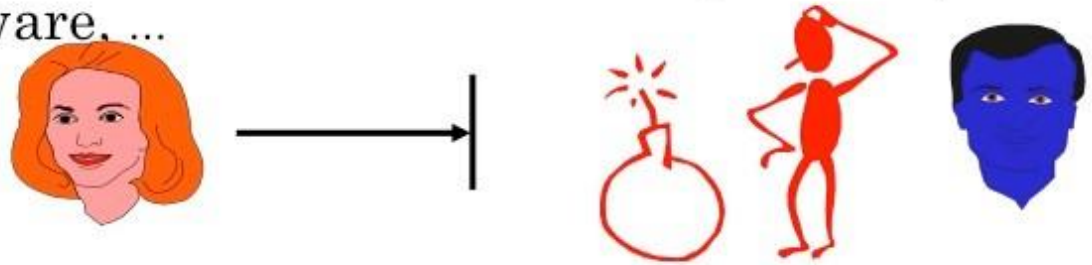
SECURITY SERVICES: ACCESS CONTROL

- THREATS
  - **UNAUTHORISED ACCESS**: unauthorised use of the resources
- SECURITY SERVICE
  - **ACCESS CONTROL**: The prevention of unauthorised use of resources (service controls who can have access to resources, under what conditions,…)
- SECURITY MECHANISMS
  - Access control list, role based access control



SECURITY SERVICES: AVAILABILITY

- THREATS
  - **INTERRUPTION** Loss of communication (cut the cable)
  - **DENIAL OF SERVICE** Noisy comms
- SECURITY SERVICE
  - **AVAILABILITY**: services are always available to authorised users
- SECURITY MECHANISMS
  - Improve" the infrastructure": Replication, increase bandwidth, hardware, ...



Passive Versus Active Attacks

Attacks	Passive/ Active	Threatening
➢Snooping ➢Traffic analysis		**confidentiality**
➢Modification ➢Masquerading ➢Replaying ➢Repudiation		**Integrity**
➢Denial Of service		**Availability**

QUESTION?

- How would you perform a successfully denial of service on GOOGLE?
  - Distributed denial of service

SUMMARY

- Security: some basic definitions
- Security services
  - Confidentiality
  - Authentication
  - Integrity
  - Non-repudiation
  - Availability
- Attacks
- Security mechanisms

WHAT IS NEXT

- Encryption -Basic definitions
  - Caesar's code