PRINCIPLES OF CRYPTOGRAPHY

CSE 3121

What’s Computer Security

- Also known as Cyber Security
- Practice of Protection of stored and transmitted data
- Used to preserve different security goals (Confidentiality, Integrity, Availability, etc.) of the data from an adversary or a group of adversaries.

Syllabus

Security Goals, Attacks, Services, Mechanisms, Symmetric Cipher Model, Block Ciphers and DES, Strength of DES, Block Cipher Design Principles. AES, Equivalent Inverse Cipher. Block Cipher Operation- Multiple Encryption and Triple DES, Electronic Codebook, Cipher Block Chaining Mode, Cipher Feedback Mode, Output Feedback Mode, Counter Mode, XTS-AES Mode for Block-Oriented Storage Devices, Format-Preserving Encryption. Euclidean Algorithm, Modular Arithmetic, Prime Numbers, Fermat and Euler theorems, Testing for Primality, Chinese Remainder theorem, Discrete Logarithms. Pseudorandom Number Generation, Stream Ciphers, RC4. Public Key Cryptography and RSA. D-H Key Exchange, ElGamal System. Cryptographic Hash Functions. Message Authentication Codes, Security of MACs, HMAC.

Textbooks

1. William Stallings, Cryptography and Network Security: Principles and Practice, (7e), Prentice Hall, 2017.

2. Behrouz A. Forouzan and Debdeep Mukhopadhyay, Cryptography and Network Security, (2e), McGraw Hill, 2008

3. Atul Kahate, Cryptography and Network Security, Tata McGraw-Hill Publishing, 2008

4. Bruce Schneier, Applied Cryptography-Protocols, Algorithms, and source code in C, (2e), John Wiley & Sons, Inc., 2013

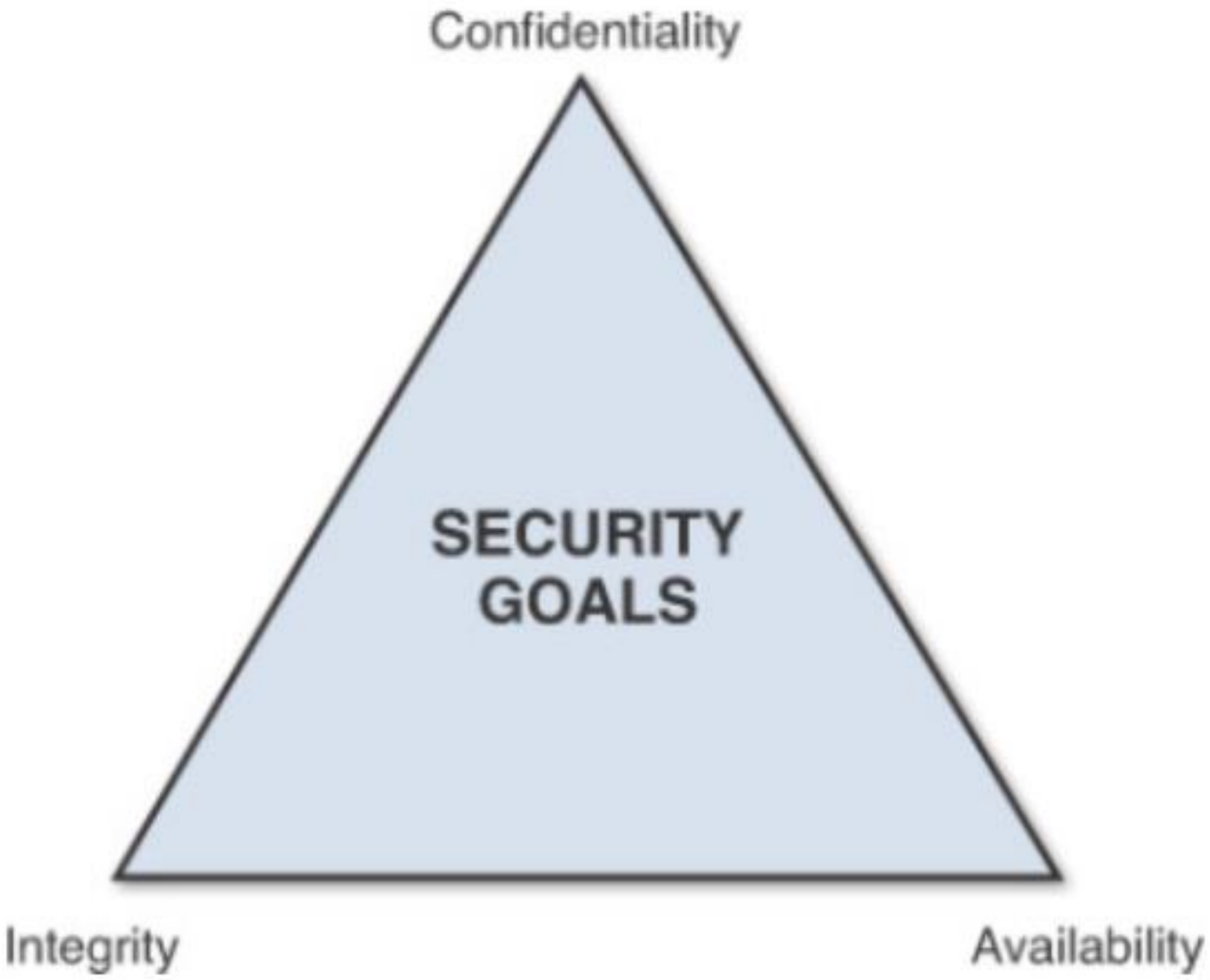
CO

- CO1: Illustrate the cryptographic attacks, services, and classical symmetric ciphers
- CO2: Analyze the various block ciphers and modes of operation.
- CO3: Utilize the concepts of number theory and pseudo random number generation.
- CO4: Explain public key crypto system.
- CO5: Apply various data integrity algorithms

SECURITY GOALS

Security goals defined by FIPS 199

- FIPS (Standards for Security Categorization of Federal Information and Information Systems)
- CIA Triad defined by FIPS



Confidentiality (🔒)

- Ensures that sensitive information is accessed only by authorized individuals, entities, or processes.
- It protects data from unauthorized disclosure.

Integrity (✓)

- Ensures that data is not tampered with and remains in its original state, providing assurance that the information is trustworthy and accurate.
- Data can be changed only by authorized entities.

Availability (🕒)

- Ensures that information, systems, and services are accessible and usable upon demand by authorized users.
- Timely access to Google Drive, One Drive backups, etc.

2 Additional Security Goals

Authenticity (🔑):-

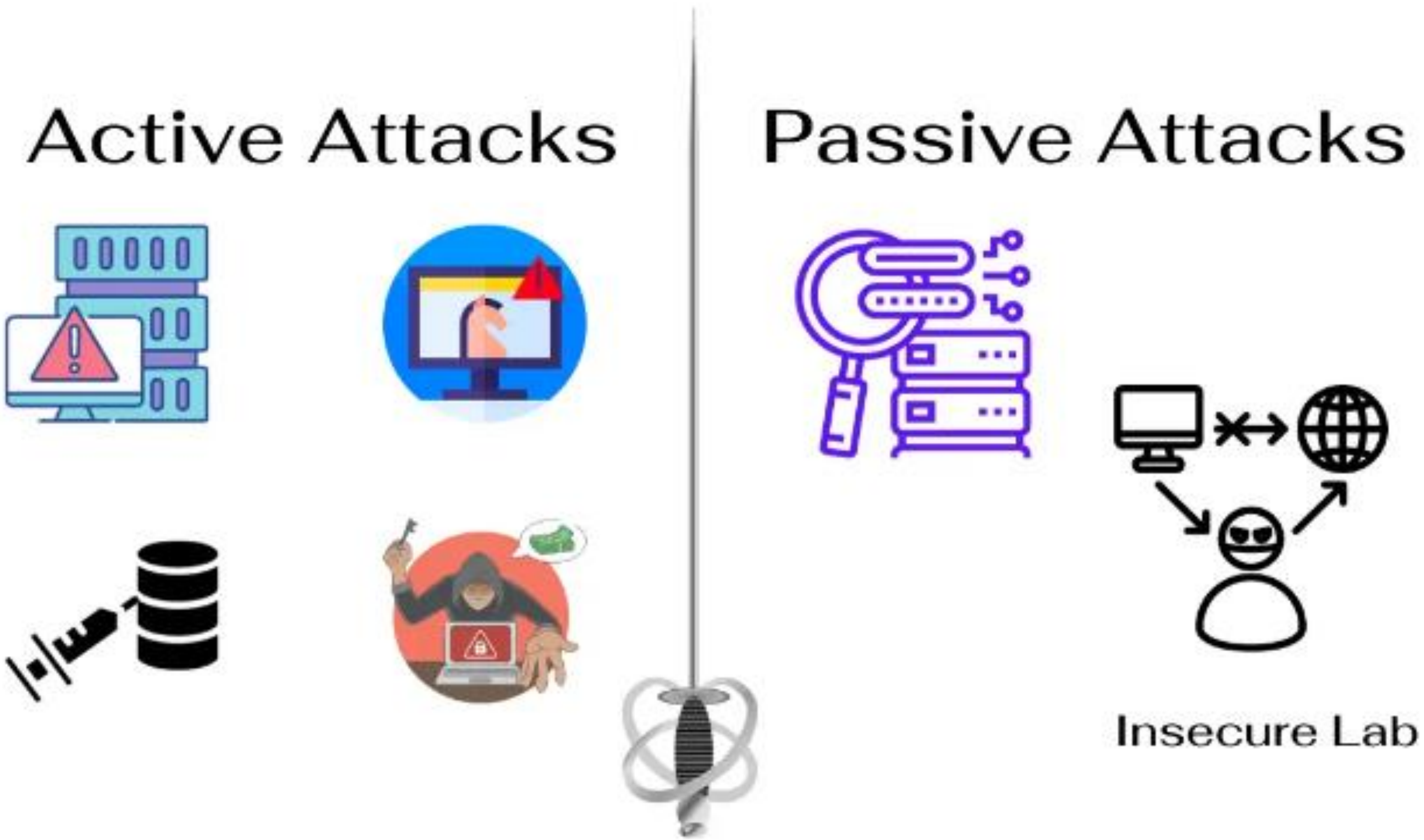
- Ensures that an entity (user, device, or system) is who or what it claims to be.
- Some examples could be Password based, Biometric based, etc.

Accountability (📜):-

- Mechanisms which ensure that individuals or communicating entities can be held responsible for their actions.

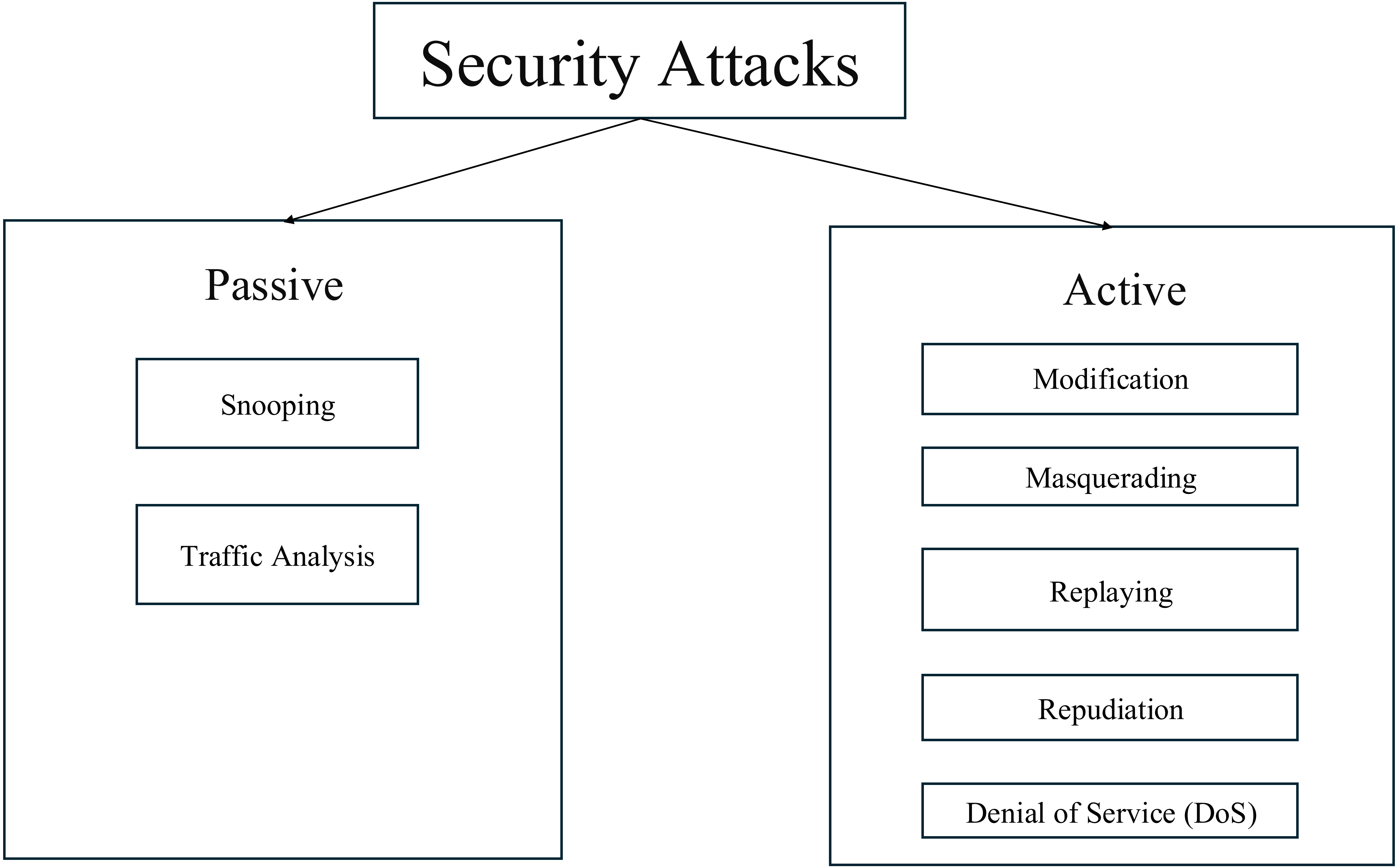
SECURITY ATTACKS

Security Attacks



Security Attacks

- A useful means of classifying security attacks
  - **Passive attacks:** A passive attack attempts to learn or make use of information from the system but does not affect system resources.
  - **Active attacks:** An active attack attempts to alter system resources or affect their operation



Security Attacks

Passive

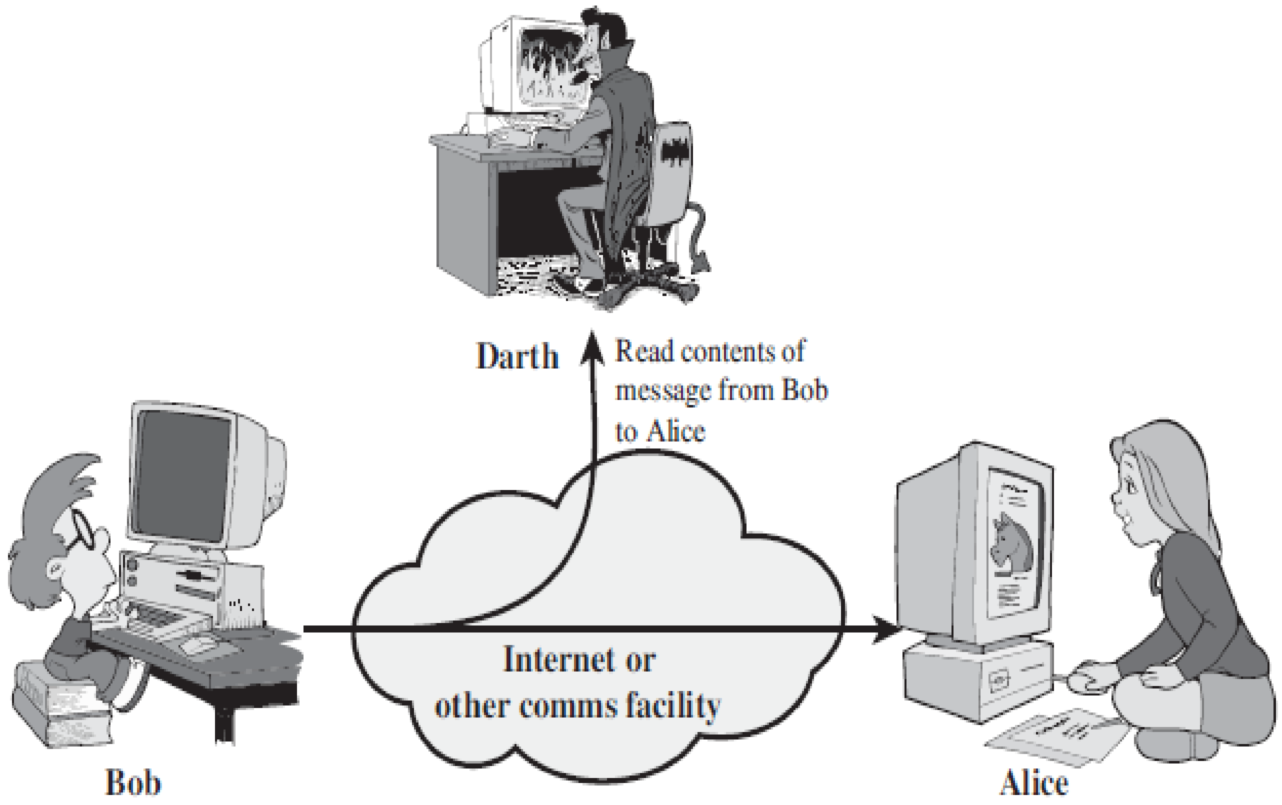
- Snooping
- Traffic Analysis

Active

- Modification
- Masquerading
- Replaying
- Repudiation
- Denial of Service (DoS)

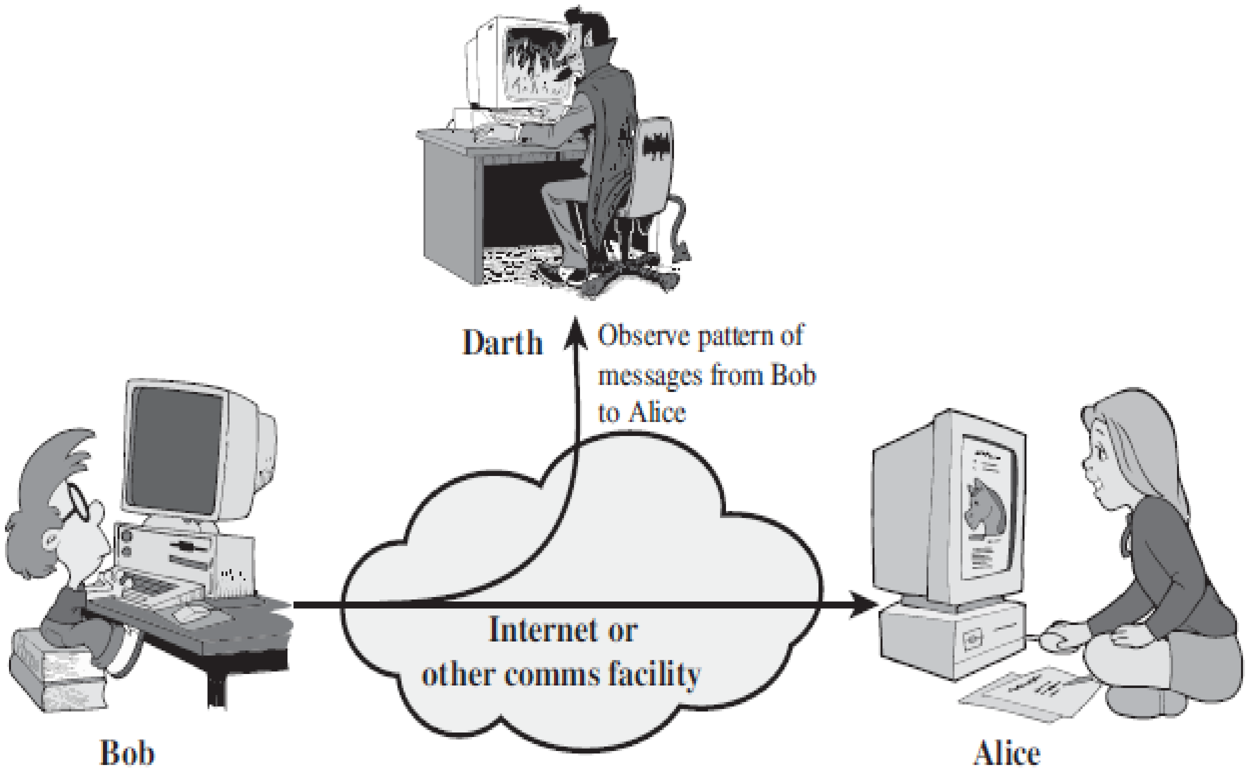
Snooping

- Captures and reads sensitive data transmitted across a network.
- The attacker concentrates on contents of the data.


Darth
Read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

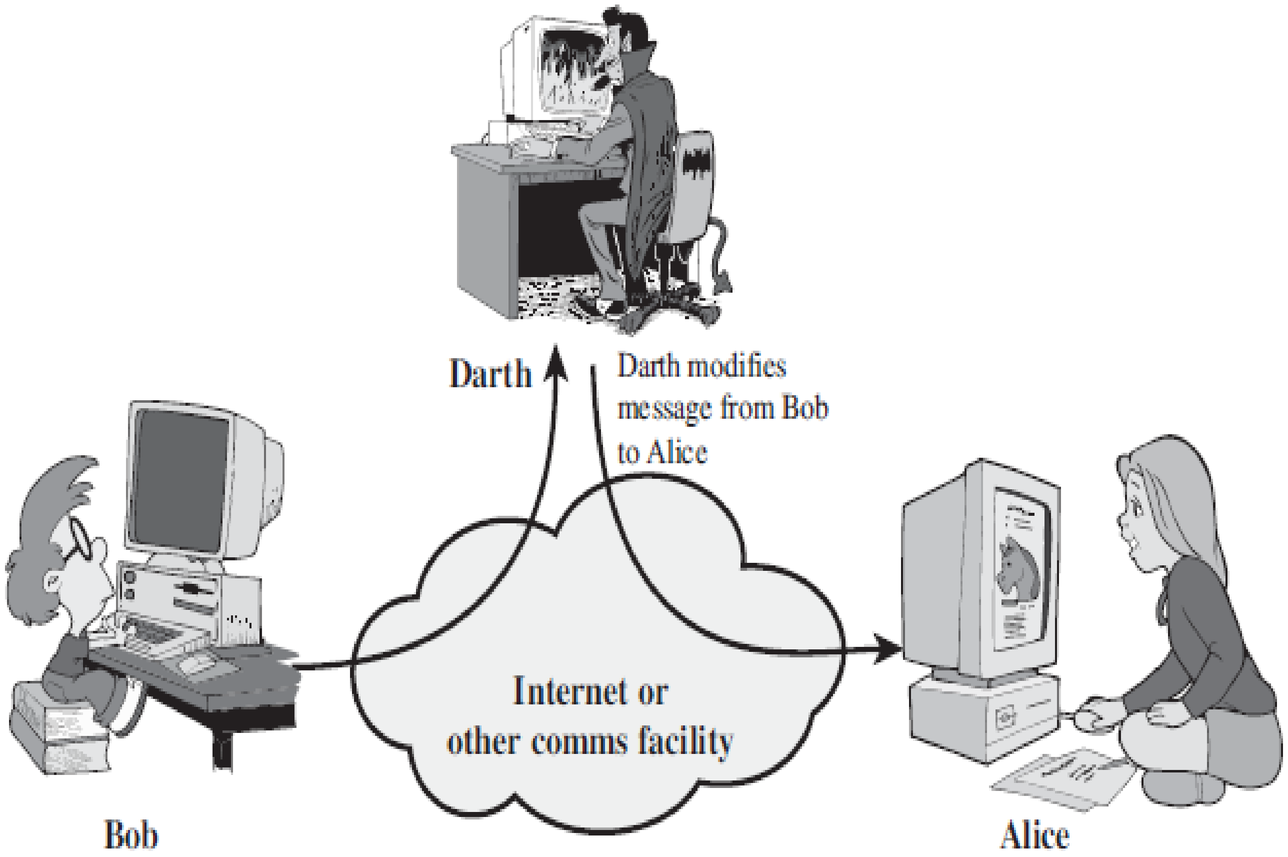
Traffic Analysis

- The attacker collects information and analyzes the network communication patterns.
- Concentrates on Metadata and traffic flow in a network.


Darth
Observe pattern of messages from Bob to Alice
Internet or other comms facility
Bob
Alice

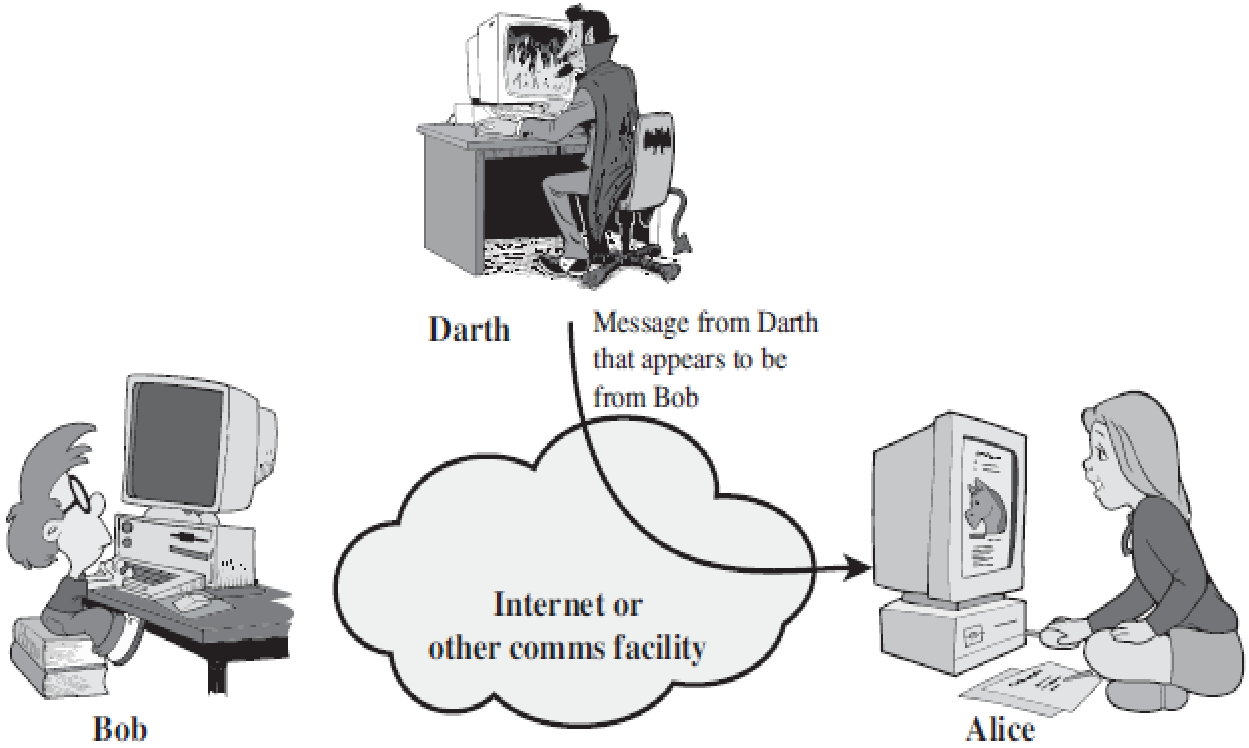
Modification

- Unauthorized manipulation, tampering, etc., of the legitimate data communicated over a network.


Darth
Darth modifies message from Bob to Alice
Internet or other comms facility
Bob
Alice

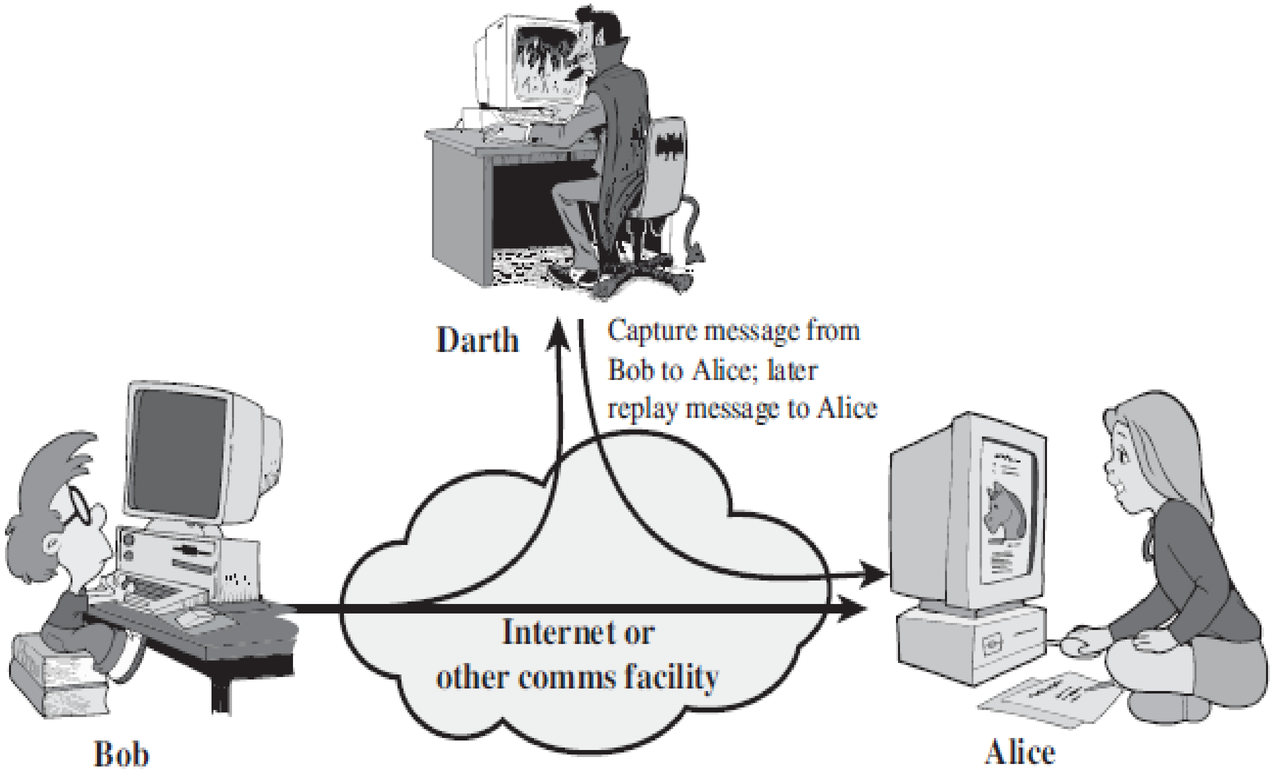
Masquerading

- Attacker pretends to be a legitimate entity to other legitimate entities in a network.


Darth
Message from Darth that appears to be from Bob
Bob
Internet or other comms facility
Alice

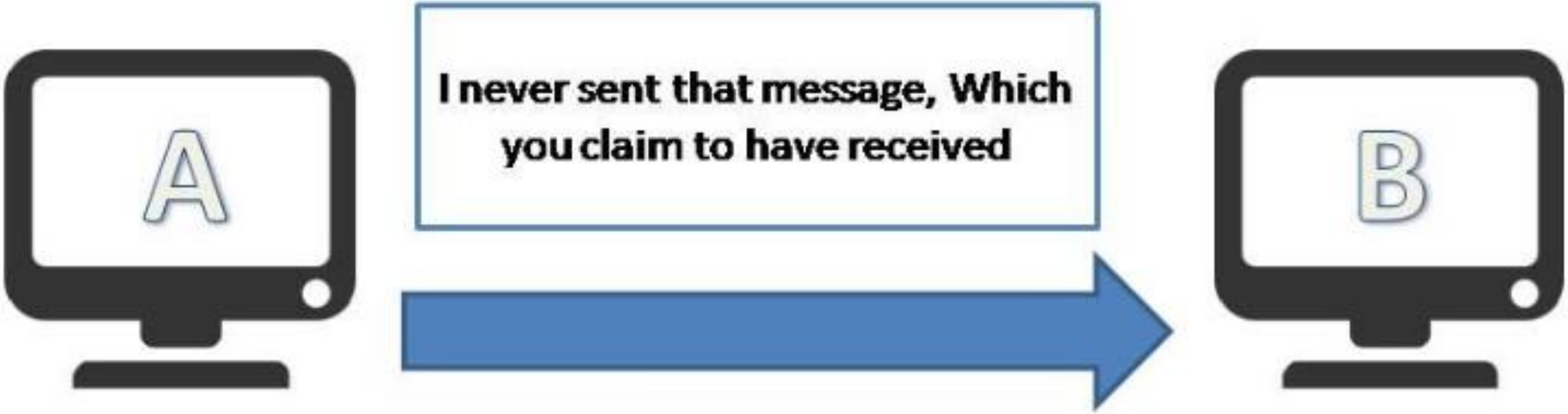
Replaying

- Subsequent retransmissions of a previously captured data packet.


Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

Repudiation

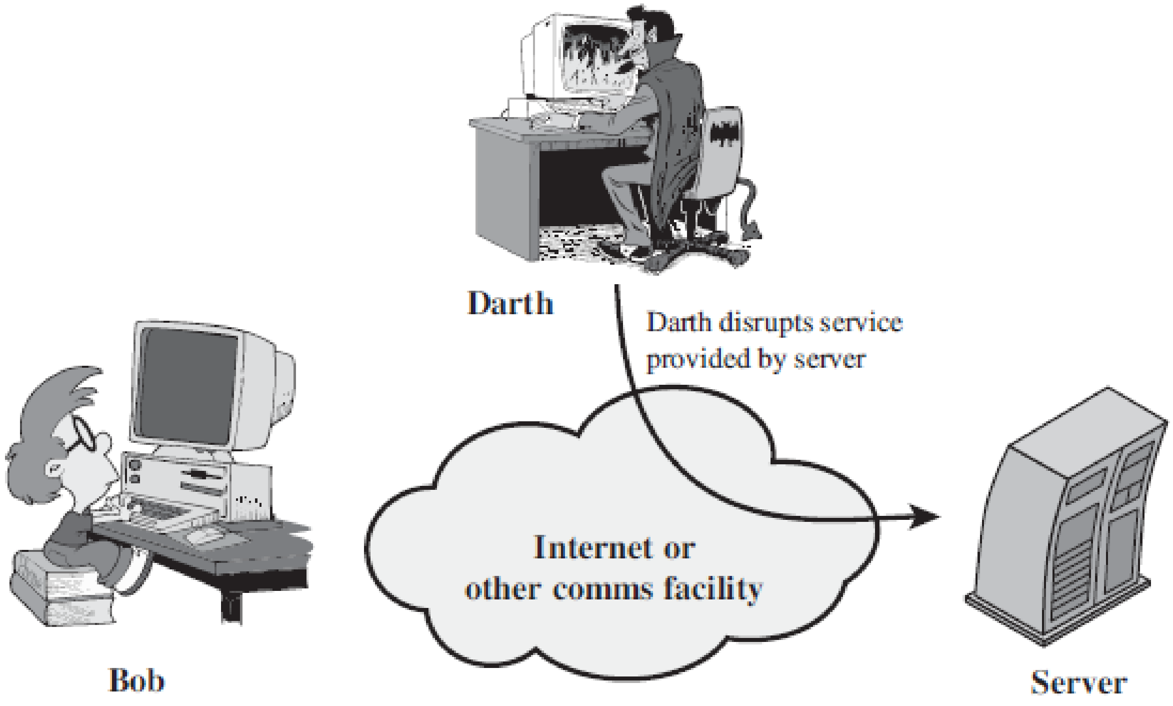
- Denying the fact that an entity was involved in a data communication.



I never sent that message, Which you claim to have received

DoS

- The attacker degrades a computer network by overloading it with unnecessary data traffic.


Darth
Darth disrupts service provided by server
Internet or other comms facility
Bob
Server

Passive Attacks	Active Attacks
• Eavesdropping and/or Collecting Data	• Altering/Manipulating Data
• Zero/Negligible impact on the system operations and/or the network performance.	• Major impact on the system operations and/or the network performance
• Comparatively harder to detect	• Comparatively easier to detect

SECURITY SERVICES

Security Services

Peer Entity Authentication

Data Origin Authentication

Access Control

Confidentiality

Data Integrity

Non-Repudiation

Availability

Security Services (Contd..)

Peer Entity Authentication:- Verification of the identities of the communicating entities.

Data Origin Authentication:- Verification of the source of the data, and that it is from a legitimate communicating entity.

Access Control:- Mechanisms and Policies which are defined to manage and restrict access to resources and data.

Confidentiality:- Includes 4 types of Confidentiality (Connection Confidentiality, Connectionless Confidentiality, Selective-Field Confidentiality, and Traffic Flow Confidentiality)

Security Services (Contd..)

Data Integrity:- Involves 5 types (Connection Integrity with Recovery, Connection Integrity without Recovery, Selective-Field Connection Integrity, Connectionless Integrity, and Selective-Field Connectionless Integrity)

Non-Repudiation:- 2 types (for Origin, and for Destination)

Availability

SECURITY MECHANISMS

Security Mechanisms

Encipherment

Digital Signature

Access Control

Data Integrity

Authentication Exchange

Traffic Padding

Routing Control

Notarization