Security Aspects for Maritime Networks

CSP004_S_M

PRESENTATION BY:
DR. STEFAN SCHAUER
DR. ABDELKADER SHAABAN
AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

Acknowledgement

- *Co-Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.*
- *Project Agreement no. 101083594*

Security Aspects for Maritime Networks

Overview

- Topic-1: Security Aspects for Maritime Networks
- Topic-2: Cryptographic Techniques for Ensuring Secure Data Transmission
- Topic-3: Security mechanisms, services, and attacks in OSI reference model

Agenda

01. Overview

02. Security Attacks

03. Security Mechanisms

04. Relationship Between Security Mechanisms and Services

Overview

OSI Security Architecture

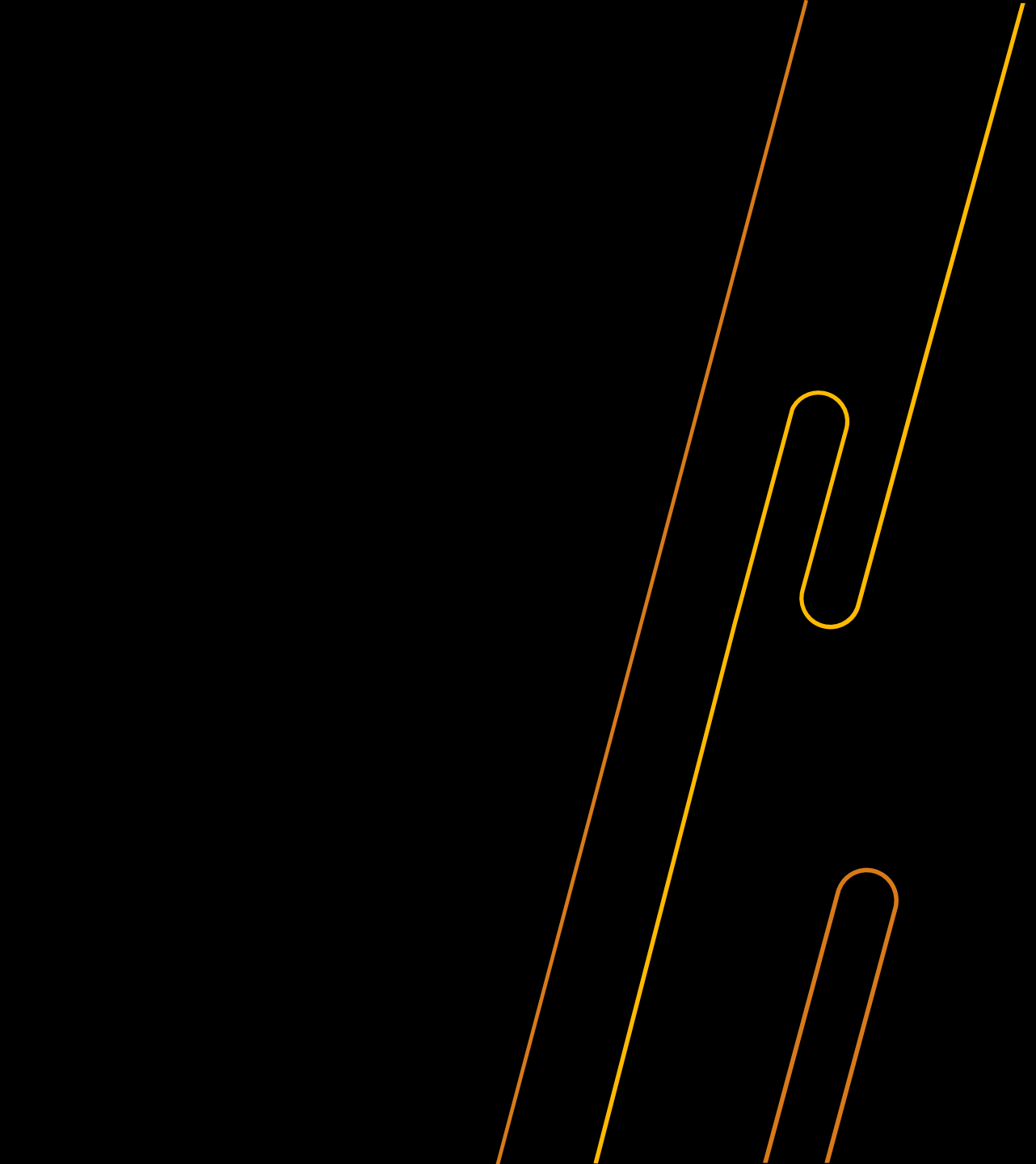
The OSI (open systems interconnection) security architecture provides a structured framework for addressing security concerns.

- **Security attacks** are categorized into **passive attacks**, involving **unauthorized access** or **monitoring** of data, and **active attacks**, including **data alteration** or **denial of service**.
- **Security mechanisms** are **tools** or **processes** designed to **detect**, **prevent**, or **mitigate security threats.**
  - Examples of **security mechanisms** include **encryption algorithms**, **digital signatures**, and **authentication protocols.**
- **Security services** include **authentication**, **access control, data confidentiality, data integrity**, **non-repudiation**, and **availability**.

The OSI Security Architecture

- Effective assessment of security **needs** and **selection** of security **products** and **policies** requires a systematic approach.
- ITU-T Recommendation **X.800**, Security Architecture for OSI, provides such a systematic approach.
- The OSI security architecture supports managers as a way of organizing the task of providing security.
- **Computer** and **communications** vendors have aligned their security features with the OSI security architecture.
- The OSI security architecture offers an abstract overview of security concepts.
- It focuses on security **attacks**, **mechanisms**, and **services**.
- **Security attacks compromise** information security.
- **Security mechanisms detect**, **prevent**, or **recover** from security attacks.
- **Security services enhance** the security of **data processing systems** and **information transfers**. These services counter security attacks using security mechanisms.

Security Attacks

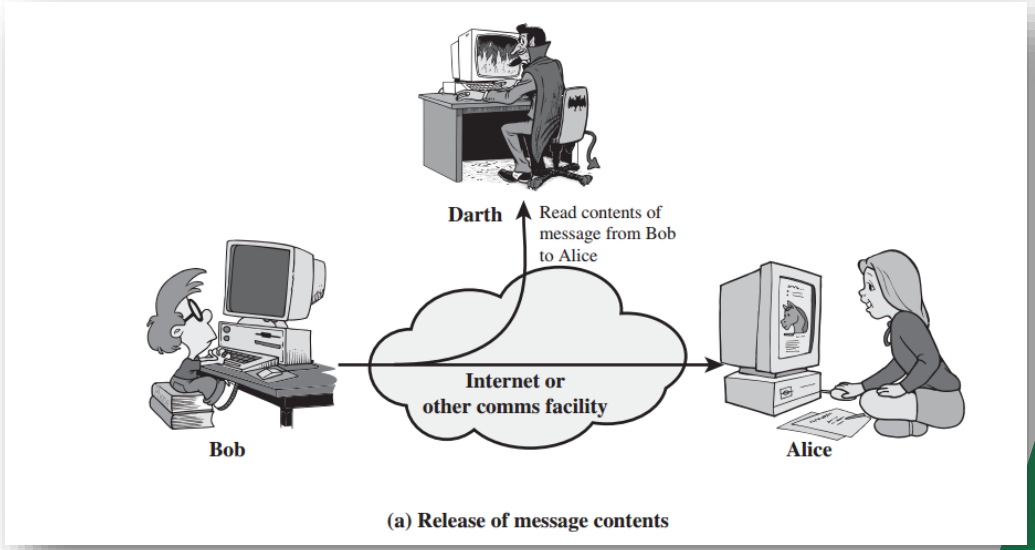


Security Attacks

- 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.
- **Threats**: A threat refers to the **potential danger** that could **exploit** a **vulnerability** and cause **harm**, posing a **risk** to security.
- **Attack**: A **security breach** caused by a **deliberate** and **intelligent attempt** to evade **security measures** and violate system **policies**.
- Types of attacks
  - Passive attack
  - Active attack

Passive Attacks

- **"Passive Attacks" which** attempt to **learn** or **make** use of information from the system but do not **affect system resources**.
- By **eavesdropping** on or **monitoring**, **transmissions** to:
  - obtain message contents, or
  - monitor traffic flows
- Are difficult to **detect** because they do not involve **any alteration** of the data.

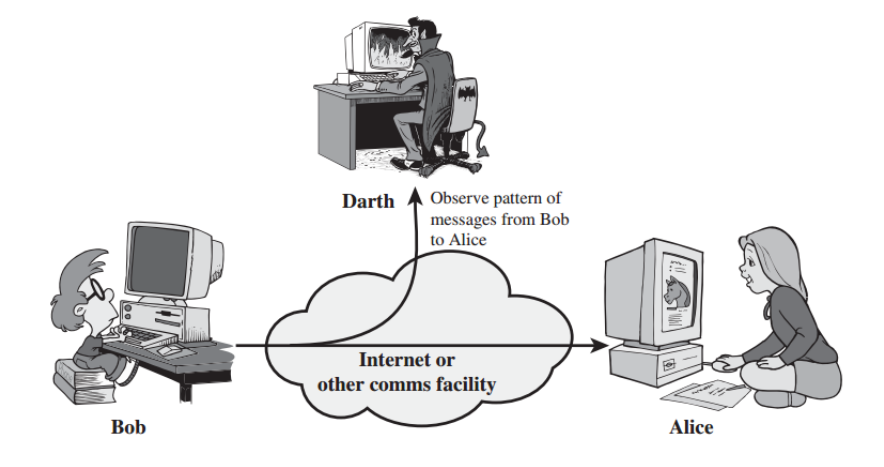


(a) Release of message contents

William Stallings, Cryptography and Network Security: Principles and Practice, Fifth Edition

Active Attacks

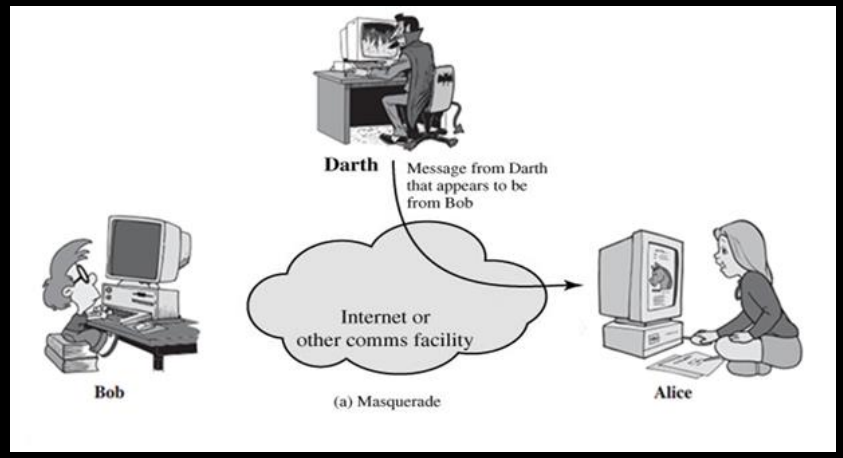
- "**Active attacks**" which attempt to **alter system resources** or **affect their operation**.
  - By modification of data stream to:
    - **masquerade** of one entity as some other
    - replay previous messages
    - modify messages in transit
    - denial of service
  - Active attacks present the opposite characteristics of passive attacks.
  - Whereas passive attacks are difficult to detect, measures are available to prevent their success.



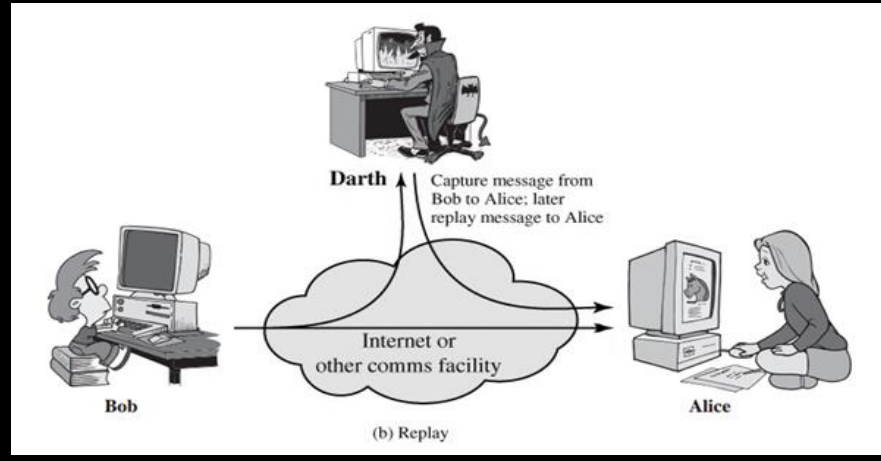
- It is quite difficult to prevent active attacks absolutely, because of the wide variety of **potential physical**, **software**, and **network vulnerabilities**.
- The goal is to **detect active attacks** and to **recover** from any disruption or delays caused by them.

Examples on Active Attacks

Masquerade

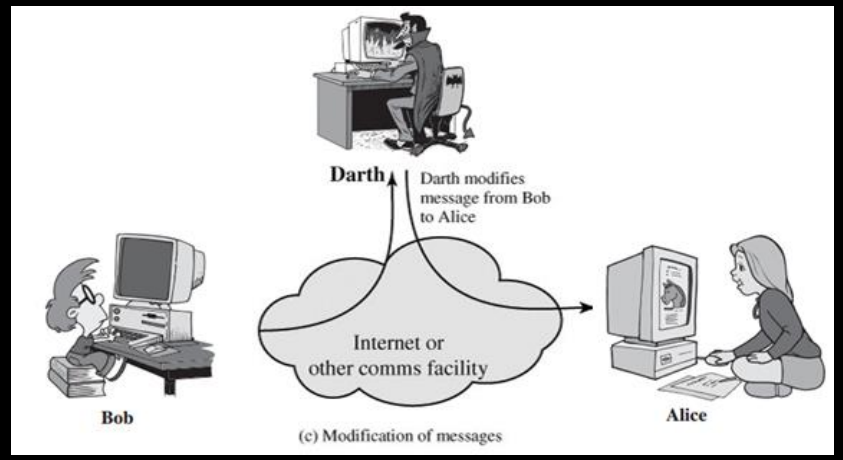


Replay

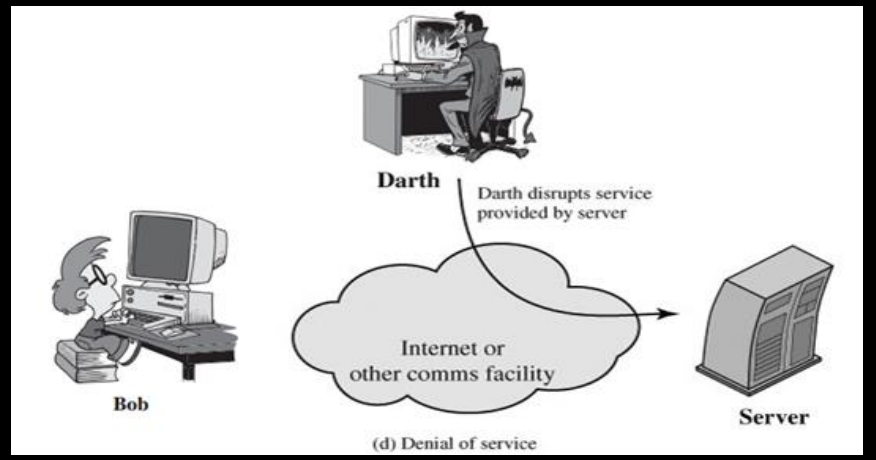


Examples on Active Attacks

Modification of Messages



Denial of Service



Security Services

Security Services

- **Services** are a **set of services** supplied by a **protocol layer** of communication systems. These services ensure that a **sufficient level** of **security** is maintained for the system or the data being exchanged.
- It categorizes these **services** into **five categories** and then divides them into fourteen specific services.
- These services are defined as follows:
  - **Authentication**: The authentication service is the one in charge of **making sure** that the communication is **authentic**:
    - **Peer Entity Authentication**: It is utilized **during** the **setup of a connection** or the **data transmission phase**.
    - **Data Origin Authentication**: This authentication service, which **confirms the origin of a data unit**, could be implemented in **applications** such as **electronic mail**, which do not require any prior communication setup to be established between the communicated terminals.

Abdelkader Magdy Shaaban, Oliver Jung, Christoph Schmittner, A PROPOSED X.800-BASED SECURITY ARCHITECTURE FRAMEWORK FOR UNMANNED AIRCRAFT SYSTEM, IDIMT 2022
ITU. (1991, March). Security architecture for open systems interconnection for CCITT applications (ITU-T Recommendation X.800)

Security Services

- **Access Control**: It is the capacity to **restrict** and **govern** access to host systems and applications via communication channels between devices. This capability is referred to as "**access control**." **Access control models come in a variety of types, including Role-Based Access Control (RBAC), Discretionary Access Control** (**DAC**), **Mandatory Access Control** (**MAC**), and **Attribute-Based Access Control** (**ABAC**)
- **Confidentiality**: The term "**confidentiality**" refers to the **protection** of transferred data from being **disclosed** inappropriately by **unauthorized** parties.
- According to X.800, there are different types of confidentiality:
  - **Connection Confidentiality**: This **protects** all **user data** on a connection.
  - **Connectionless Confidentiality**: This is defined to **protect** the **confidentiality** of all **users accessing** a single data block.
  - **Selective-Field Confidentiality**: This **confidentiality** service secures **specific fields** within a **user's data** on a connection or within a single **data block.**
  - **Traffic-Flow Confidentiality**: This service **protects** any data based on the observation of the **data flow**.

Abdelkader Magdy Shaaban, Oliver Jung, Christoph Schmittner, A PROPOSED X.800-BASED SECURITY ARCHITECTURE FRAMEWORK FOR UNMANNED AIRCRAFT SYSTEM, IDIMT 2022
ITU. (1991, March). Security architecture for open systems interconnection for CCITT applications (ITU-T Recommendation X.800)

Security Services

- **Non-Repudiation**: This aims at preventing either the **sender** or the **recipient** from **denying transmitting data.** Therefore, when a message is conveyed, it is feasible for the recipient to prove that the claimed **sender** of the message sent it.
- Two types of non-repudiation are defined:
  - **Non-repudiation Origin**: Proofs that a particular **sender** sent the data.
  - **Non-repudiation Destination**: Proofs that a **receiver** obtained the data.
- **Data Integrity**: The guarantee that the data received is **identical** to the data that an authorized party **sent**. X.800 defines different types of this service:
  - **Connection Integrity with Recovery**: It **protects user data** and **attempts** to recover any incorrect data.
  - **Connection Integrity without Recovery:** It only **detects any breach** of **data integrity** but **does not attempt t**o recover action.
  - **Selective-Field Connection Integrity**: Provides the integrity of **specified fields** within the user data of a data block transmitted across a connection
  - **Connectionless Integrity**: Protection of the integrity of a **single connectionless** data block, which can be achieved by **detecting** changes in the data.
  - **Selective-Field Connectionless Integrity**: This aims at **protecting** a single connectionless data block by detecting changes.
- **Availability**: A system or resource is **available** when an **authorized** system entity demands it.

Abdelkader Magdy Shaaban, Oliver Jung, Christoph Schmittner, A PROPOSED X.800-BASED SECURITY ARCHITECTURE FRAMEWORK FOR UNMANNED AIRCRAFT SYSTEM, IDIMT 2022
ITU. (1991, March). Security architecture for open systems interconnection for CCITT applications (ITU-T Recommendation X.800)

Security Mechanisms

Security Mechanisms

- X.800 defines multiple security **mechanisms** as a collection to **deliver security services** for the OSI model. The following is how these mechanisms are defined in:
  - **Encipherment**: It is a method of protecting the **confidentiality** of data by first **encrypting** it in a **not readable** format and then **decrypting** it so that an authorized party may handle it.
  - **Digital Signature**: The alteration of data via **cryptography** or **adding** extra data to a sensitive one helps **prevent** data from being **forged** by providing recipients with **evidence** of the data's integrity.
  - **Access Control**: It provides access **rights** to resources.
  - **Data Integrity**: It guarantees the **integrity** of **data units** or **data streams**.
  - **Authentication Exchange**: Its purpose is to **ensure** an **entity's identity** through information exchange.
  - **Traffic Padding**: The insertion of **random** bits into a **data stream** makes it impossible for an **unauthorized** third party to **analyze** the data.
  - **Routing Control**: In the event that a **breach** of security is **suspected**, particular physically secure pathways must be chosen for specific data.
  - **Notarization**: To ensure that specific **data flow characteristics** are maintained, it is essential to depend on a **trustworthy third party** to achieve a task.

Abdelkader Magdy Shaaban, Oliver Jung, Christoph Schmittner, A PROPOSED X.800-BASED SECURITY ARCHITECTURE FRAMEWORK FOR UNMANNED AIRCRAFT SYSTEM, IDIMT 2022
ITU. (1991, March). Security architecture for open systems interconnection for CCITT applications (ITU-T Recommendation X.800)

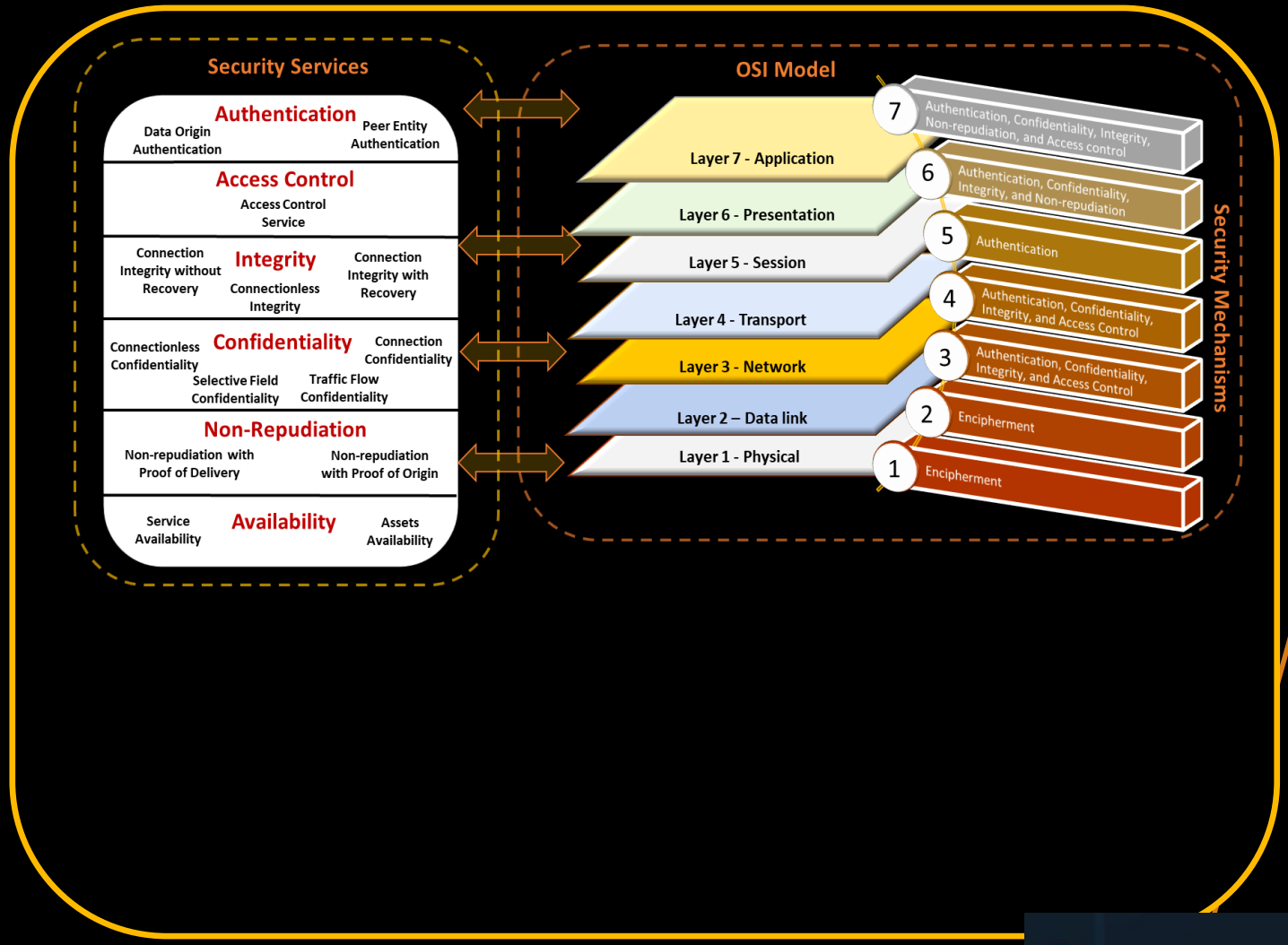
Relationship Between Security Mechanisms and Services

Security Mechanisms and Services

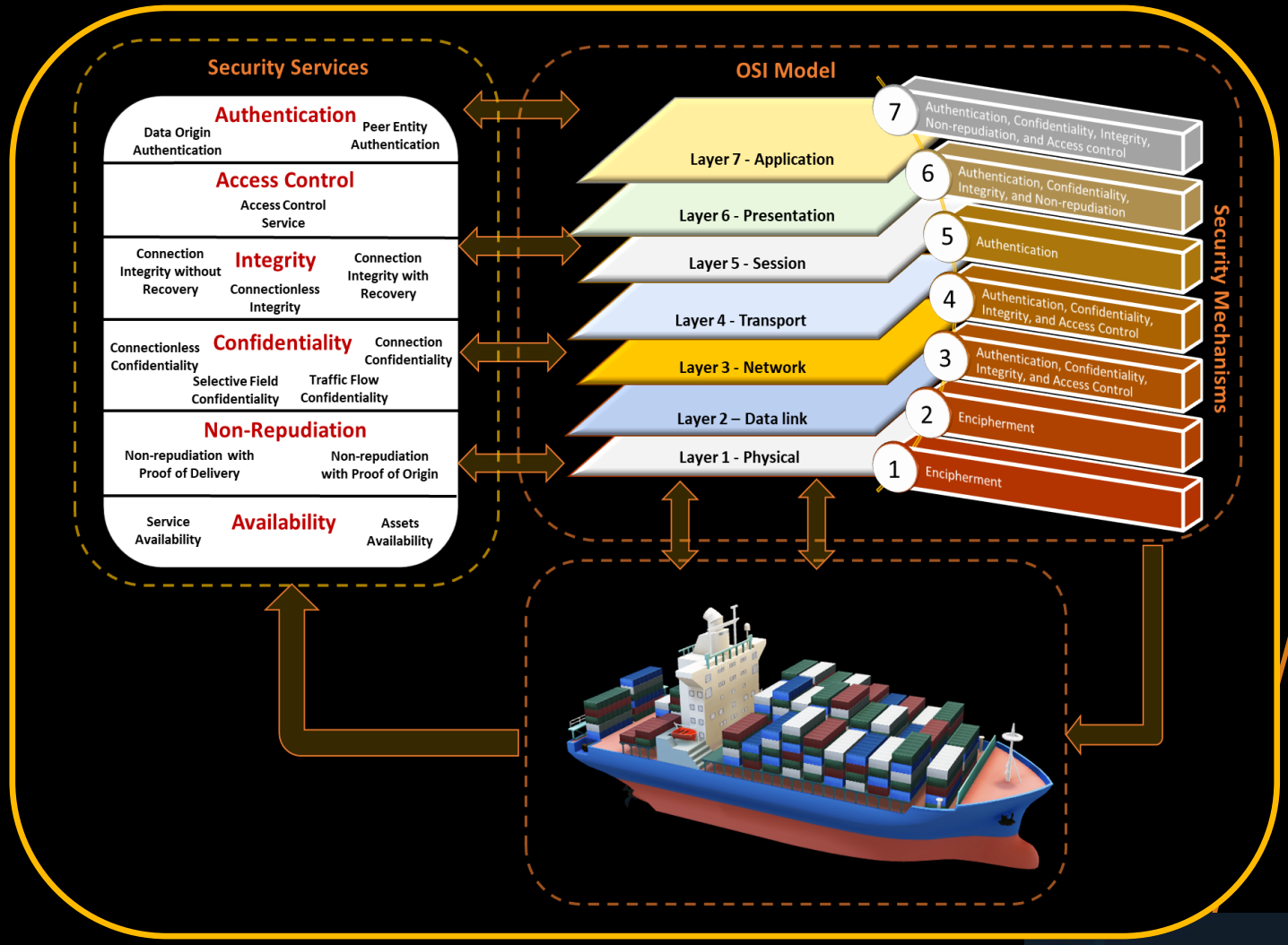
Mechanisms

Service	Encipherment	Digital Signature	Access Control	Data Integrity	Authentication Exchange	Traffic Padding	Routing Control	Notarization
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y			Y				
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y		
Data integrity	Y	Y			Y			
Nonrepudiation		Y						Y
Availability			Y			Y	Y	

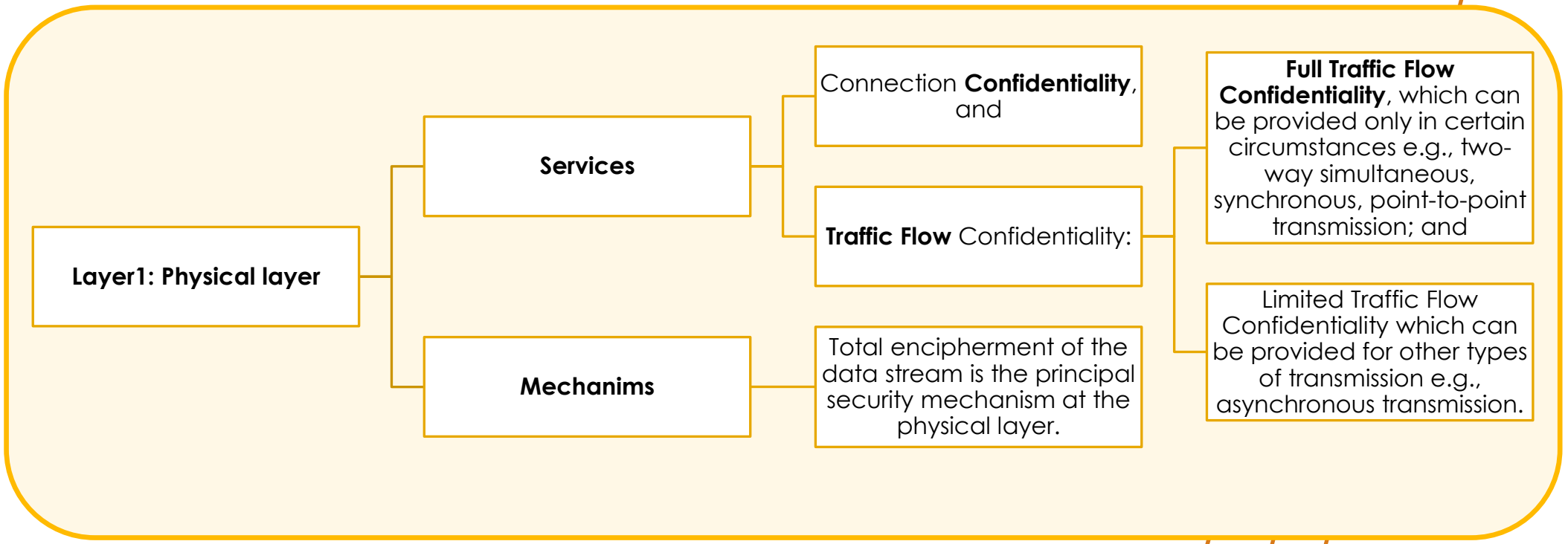
Exploring Relationship Distribution within the OSI Model Framework



Exploring Relationship Distribution within the OSI Model Framework

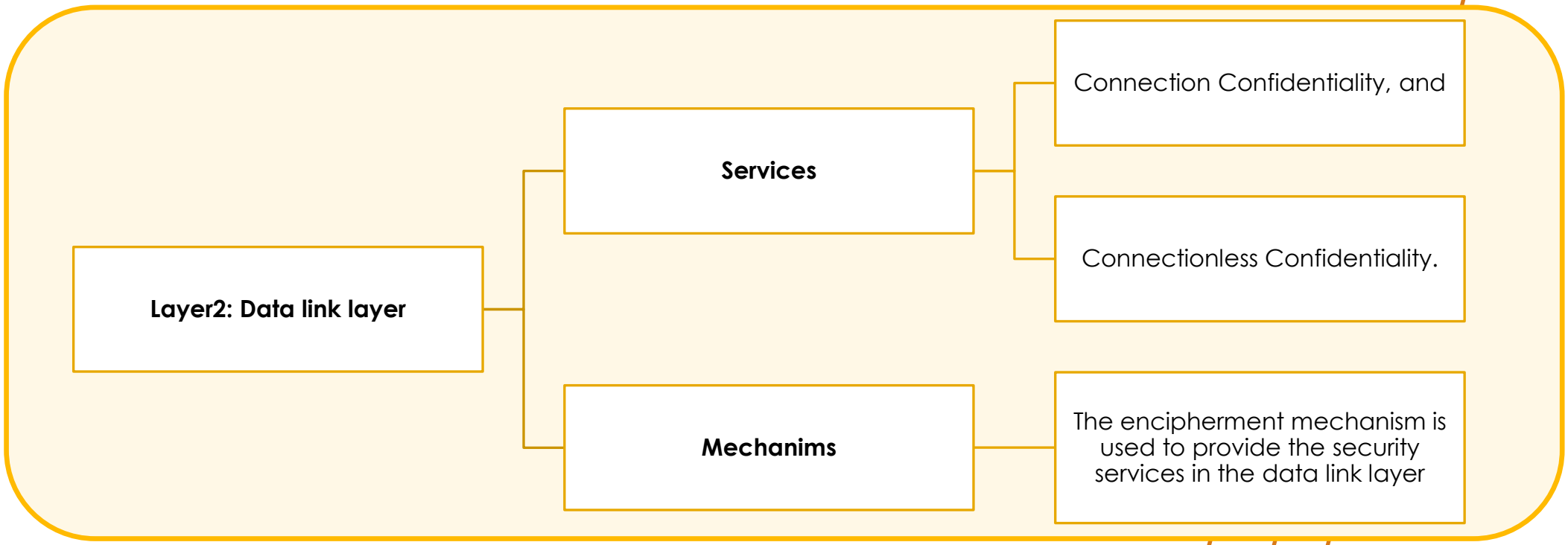


Placement of Security Services and Mechanisms



ITU. (1991, March). Security architecture for open systems interconnection for CCITT applications (ITU-T Recommendation X.800)

Placement of Security Services and Mechanisms



ITU. (1991, March). Security architecture for open systems interconnection for CCITT applications (ITU-T Recommendation X.800)

Placement of Security Services and Mechanisms

- ***Layer3: Network layer***: The **network layer** is internally organized to provide protocol(s) to perform the following operations:
  - sub-network access;
  - sub-network-dependent convergence;
  - sub-network-independent convergence; and
  - relaying and routing.
  - ***Services:*** The security services that may be provided by the **protocol** which performs the sub-network access functions associated with the provision of the OSI network service are as follows:
    - Peer Entity Authentication;
    - Data Origin Authentication;
    - Access Control service;
    - Connection Confidentiality;
    - Connectionless Confidentiality;
    - Traffic Flow Confidentiality;
    - Connection Integrity without recovery; and
    - Connectionless Integrity.

ITU. (1991, March). Security architecture for open systems interconnection for CCITT applications (ITU-T Recommendation X.800)

Placement of Security Services and Mechanisms

- **Layer3: Network layer**
  - **Mechanisms**: Security **mechanisms** are employed by the **protocols** responsible for sub-network access, relaying, and **routing** to facilitate the OSI network service between end systems.
  - The OSI model provides various security services:
    - **Peer Entity Authentication**: Achieved through **cryptographic authentication exchanges**, **protected password exchange**, and **signature mechanisms.**
    - **Data Origin Authentication**: Can be ensured by **encipherment** or **signature mechanisms**.
    - **Access Control**: Implemented through specific **access control** mechanisms.
    - **Connection Confidentiality**: Ensured via **encipherment** mechanism and/or **routing control.**
    - **Connectionless Confidentiality**: Implemented using **encipherment** mechanism and/or **routing control.**
    - **Traffic Flow Confidentiality**: Achieved through **traffic padding** mechanism, in combination with **confidentiality** services at or below the network layer and/or **routing control.**
    - **Connection Integrity without Recovery**: Maintained by **data integrity** mechanism, sometimes with **encipherment**.
    - **Connectionless Integrity**: Ensured by **data integrity** mechanism, sometimes with **encipherment**.

ITU. (1991, March). Security architecture for open systems interconnection for CCITT applications (ITU-T Recommendation X.800)

Placement of Security Services and Mechanisms

- **Layer4: Transport layer**
- **Services**: The security services that may be provided, **single** or in **combination**, in the transport layer are:
- Peer Entity Authentication;
- Data Origin Authentication;
- Access Control service;
- Connection Confidentiality;
- Connectionless Confidentiality;
- Connection Integrity with Recovery;
- Connection Integrity without Recovery; and
- Connectionless Integrity.

ITU. (1991, March). Security architecture for open systems interconnection for CCITT applications (ITU-T Recommendation X.800)

Placement of Security Services and Mechanisms

- **Layer4: Transport layer**
- **Mechanims**:
- **Peer Entity Authentication**: Utilized through a combination of **cryptographic** authentication exchanges, **protected password exchange**, and **signature** mechanisms.
- **Data Origin Authentication**: Achieved through **encipherment** or **signature** mechanisms.
- **Access Control**: Implemented by specific **access control** mechanisms.
- **Connection Confidentiality**: Ensured via an **encipherment** mechanism.
- **Connectionless Confidentiality**: Implemented using an **encipherment** mechanism.
- **Connection Integrity Recovery**: Maintained using a **data integrity** mechanism, sometimes with an encipherment mechanism.
- **Connection Integrity without Recovery**: Ensured using a **data integrity** mechanism, sometimes with an **encipherment** mechanism.
- **Connectionless Integrity**: Achieved through a **data integrity** mechanism, sometimes with an **encipherment** mechanism.

ITU. (1991, March). Security architecture for open systems interconnection for CCITT applications (ITU-T Recommendation X.800)

Placement of Security Services and Mechanisms

- **Layer5: Session layer**
- Services: **No security services** are provided in the session layer.
- **Layer6: Presentation layer**
- **Services**
- Connection Confidentiality;
- Connectionless Confidentiality; and
- Selective Field Confidentiality.
- Traffic Flow Confidentiality;
- Peer Entity Authentication;
- Data Origin Authentication;
- Connection Integrity with Recovery;
- Connection Integrity without Recovery;
- Selective Field Connection Integrity;
- Connectionless Integrity;
- Selective Field Connectionless Integrity;
- Non-repudiation with Proof or Origin; and
- Non-repudiation with Proof of Delivery.

ITU. (1991, March). Security architecture for open systems interconnection for CCITT applications (ITU-T Recommendation X.800)

Placement of Security Services and Mechanisms

- **Layer6: Presentation layer**
- **Mechanims:** The OSI model offers various ways to support different security services:
- **Peer Entity Authentication**: Supported by syntactic transformation mechanisms like encipherment.
- **Data Origin Authentication**: Supported by encipherment or signature mechanisms.
- **Connection Confidentiality**: Supported by an encipherment mechanism.
- **Connectionless Confidentiality**: Supported by an encipherment mechanism.
- **Selective Field Confidentiality**: Supported by an encipherment mechanism.
- **Traffic Flow Confidentiality**: Supported by an encipherment mechanism.
- **Connection Integrity with Recovery**: Supported by a data integrity mechanism, sometimes with encipherment.
- **Connection Integrity without Recovery**: Supported by a data integrity mechanism, sometimes with encipherment.
- **Selective Field Connection Integrity**: Supported by a data integrity mechanism, sometimes with encipherment.
- **Connectionless Integrity**: Supported by a data integrity mechanism, sometimes with encipherment.
- **Selective Field Connectionless Integrity**: Supported by a data integrity mechanism, sometimes with encipherment.
- **Non-repudiation with Proof of Origin**: Supported by a combination of data integrity, signature, and notarization mechanisms.
- **Non-repudiation with Proof of Delivery**: Supported by a combination of data integrity, signature, and notarization mechanisms.

ITU. (1991, March). Security architecture for open systems interconnection for CCITT applications (ITU-T Recommendation X.800)

Placement of Security Services and Mechanisms

- **Layer7:Application layer**
- **Services**
- Peer Entity Authentication;
- Data Origin Authentication;
- Access Control Service;
- Connection Confidentiality;
- Connectionless Confidentiality;
- Selective Field Confidentiality;
- Traffic Flow Confidentiality;
- Connection Integrity with Recovery;
- Connection Integrity without Recovery;
- Selective Field Connection Integrity;
- Connectionless Integrity;
- Selective Field Connectionless Integrity;
- Non-repudiation with Proof of Origin; and
- Non-repudiation with Proof of Delivery.

ITU. (1991, March). Security architecture for open systems interconnection for CCITT applications (ITU-T Recommendation X.800)

Placement of Security Services and Mechanisms

- **Layer7:Application layer**
- **Mechanims**
- **Peer Entity Authentication**: Can use authentication information protected by presentation or lower layer encipherment mechanisms.
- **Data Origin Authentication**: Supported by signature mechanisms or lower layer encipherment mechanisms.
- **Access Control**: Can be provided by a combination of access control mechanisms in the application layer and lower layers.
- **Connection Confidentiality**: Supported by lower layer encipherment mechanism.
- **Connectionless Confidentiality**: Supported by lower layer encipherment mechanism.
- **Selective Field Confidentiality**: Supported by an encipherment mechanism at the presentation layer.
- **Limited Traffic Flow Confidentiality**: Supported by a traffic padding mechanism at the application layer along with lower layer confidentiality service.

ITU. (1991, March). Security architecture for open systems interconnection for CCITT applications (ITU-T Recommendation X.800)

Placement of Security Services and Mechanisms

- **Layer7:Application layer**
- **Mechanims**
- **Connection Integrity with Recovery**: Supported by lower layer data integrity mechanism, sometimes with encipherment.
- **Connection Integrity without Recovery**: Supported by lower layer data integrity mechanism, sometimes with encipherment.
- **Selective Field Connection Integrity**: Supported by a data integrity mechanism at the presentation layer, sometimes with encipherment.
- **Connectionless Integrity**: Supported by lower layer data integrity mechanism, sometimes with encipherment.
- **Selective Field Connectionless Integrity**: Supported by a data integrity mechanism at the presentation layer, sometimes with encipherment.
- **Non-repudiation with Proof of Origin**: Supported by a combination of signature and lower layer data integrity mechanisms, possibly with third-party notaries.
- **Non-repudiation with Proof of Delivery**: Supported by a combination of signature and lower layer data integrity mechanisms, possibly with third-party notaries.

ITU. (1991, March). Security architecture for open systems interconnection for CCITT applications (ITU-T Recommendation X.800)

Connect with CyberSecPro:
How to register and other practical information

1. Website:
   www.cybersecpro-project.eu
2. X (Twitter):
   https://twitter.com/CyberSecPro_eu
3. LinkedIn:
   https://www.linkedin.com/company/cybersecpro-euproject/

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.

Project Agreement no. 101083594

Thank you

Please send all questions to:
Abdelkader Shaaban,
abdelkader.Shaaban@ait.ac.at
Stefan Schauer
Stefan.Schauer@ait.ac.at