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: Secure Network Architecture and Design
- Topic-2: Cryptographic Techniques for Ensuring Secure Data Transmission
- Topic-3: Security mechanisms, services, and attacks in OSI reference model

Agenda

01. Overview

02. Cyber Threats in the Maritime Network

03. Identify Vulnerabilities in the Maritime Network

04. Assessing the Likelihood, Impact, and Risk in the Maritime Network

05. Develop Protection Measures in the Maritime Network

06. Cybersecurity Regulations and Standards in Maritime

07. Ship's e-Nav Service Display Device

Overview

Cyber Security Characteristics of the Maritime

- The maritime industry's increasing reliance on technology **elevates** the importance of **cyber security**.

- It is crucial for **protecting ships**, **cargo**, **personnel**, and the **environment** from cyber threats.

THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS, Version 4, URL: 2021-Cyber-Security-Guidelines.pdf (ics-shipping.org),accessed on February 2024.

Cyber Incidents in Maritime Domain

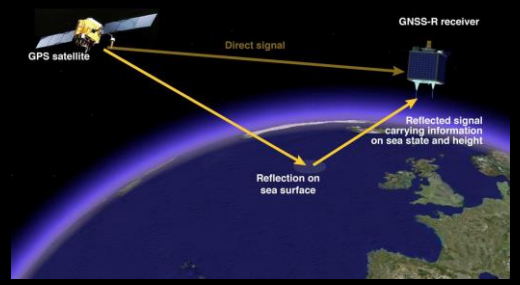
Cyber incidents can occur due to various reasons, such as:

A cyber security incident affecting the availability and integrity of **Operational Technology** (**OT**), like corruption of chart data in an **Electronic Chart Display and Information System** (**ECDIS**).

Source: Electronic Chart Display and Information System (ECDIS) Introduction - China Deyuan Marine

Unintended system **failures** during software **maintenance** and patching, for instance, from using an **infected USB drive**

Source: 3 Simple Rules to Stop Malware (calyptix.com)



Loss or **manipulation** of external sensor data critical for **ship operation**, including **Global Navigation Satellite Systems** (**GNSS**) of which the **Global Positioning System** (**GPS**) is the most frequently used.

Source: GNSS- Global Navigation Satellite System (blogfa.com)

THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS, Version 4, URL: 2021-Cyber-Security-Guidelines.pdf (ics-shipping.org),accessed on February 2024.

Cyber Incidents in Maritime Domain

Cyber **incidents** can occur due to various reasons, such as:

System failures are caused by software **crashes** or **bugs**.

Source: 12 Types of Software Bugs Every Developer Must Beware Of (enou.co)

Crew interaction with **phishing attempts**, a **common attack** vector by **threat actors**, **leads** to **data loss** and **malware** introduction to shipboard systems.

Source: Cybersecurity researchers discover Windows malware that gets installed via ads (consumeraffairs.com)

THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS, Version 4, URL: 2021-Cyber-Security-Guidelines.pdf (ics-shipping.org),accessed on February 2024.

Factors Influencing Maritime Vulnerability to Cyber Incidents

Characteristics affecting **maritime vulnerability** to cyber incidents:

The involvement of multiple **stakeholders** leads to a **potential lack** of **accountability** for **IT** and **OT system infrastructure** and ship networks.

Use **of legacy IT** and **OT** systems that are **unsupported** or **rely** on **outdated operating** systems.

Use of **OT systems** unable to be **patched** or **run antivirus** due to type approval issues.

Ships **interfacing** online with **shoreside parties** and global **supply chain** components.

Remote monitoring and access to **ship equipment** by **manufacturers** or support providers.

Sharing of **sensitive information** with shore-based service **providers** and **public authorities**.

The use of **computer-controlled** critical systems may not have the latest **patches** or **proper security measures** installed in a proper manner.

Cyber risk management culture may require improvement through formalized **training** and **exercises** and **clarified roles** and responsibilities.

Automation systems often comprise multiple sub-systems **integrated** by shipyards with minimal consideration for cyber issues.

THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS, Version 4, URL: 2021-Cyber-Security-Guidelines.pdf (ics-shipping.org),accessed on February 2024.

Differences between IT and OT systems

- The maritime industry faces significant cybersecurity risks due to the integration of **operational technology** (**OT**) and **information technology** (**IT**) systems.
- Previously standalone **OT** systems, which physically control **shipboard operations**, are now interconnected with **IT systems** onboard and on shore.
- Adoption of **cloud computing**, **Internet of Things** (**IoT**), and **autonomous technologies** further increases interconnectivity between **OT** and **IT**, heightening cybersecurity risks.
- **Cyberattacks** on the maritime industry's **OT** systems have surged by **900 percent** over the past few years.
- This trend underscores the **urgent** need for **robust cybersecurity** measures to safeguard **maritime** operations against potential cyber threats.

Navigating Cybersecurity Challenges in Maritime Operational Technology (maritime-executive.com), accessed in February 2024

Enhancing Cyber Risk Management in the Maritime Industry

1

Define **roles** and **responsibilities** of users, key personnel, and **management** both **onshore** and **onboard**.

2

Identify **critical systems**, **assets**, **data**, and capabilities **vulnerable** to disruption, **posing risks** to ship **operations** and **safety**.

3

Implement **technical** and **procedural measures** for protection against cyber **incidents**, **ensuring timely detection** and **continuity** of operations.

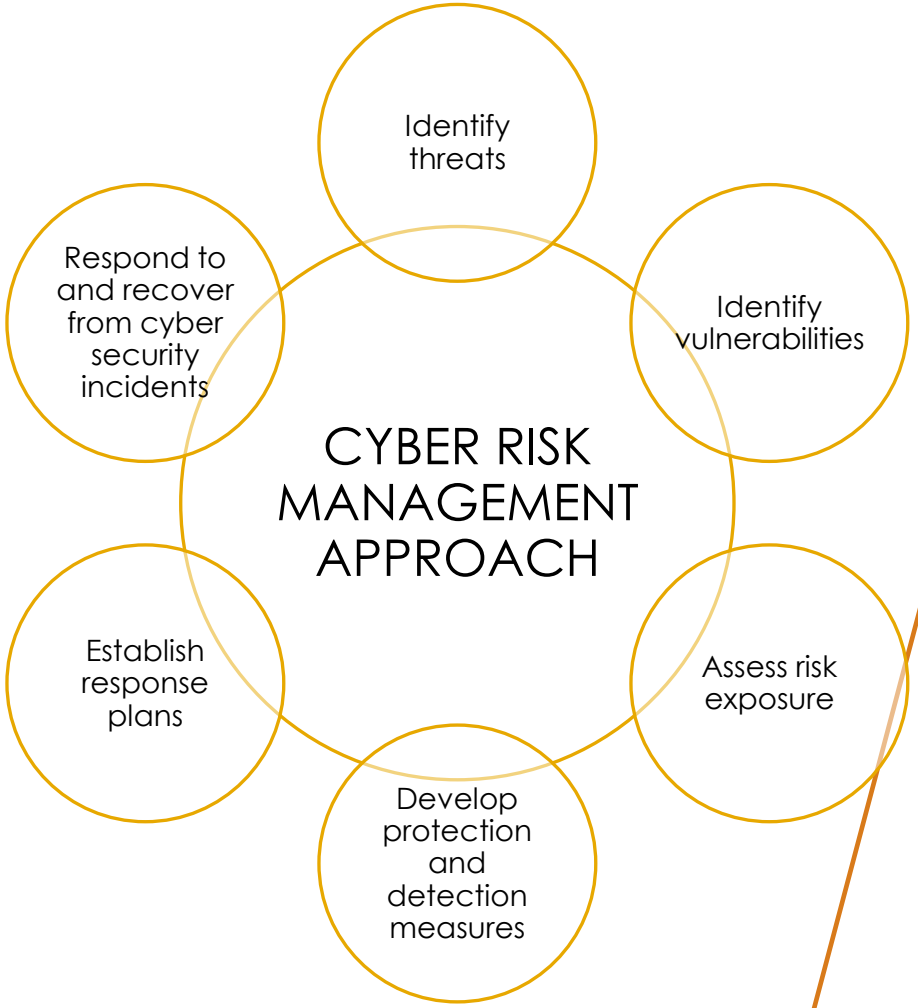
4

Develop and **regularly** exercise a **contingency** plan for cyber incidents.

The increasing adoption of **data analysis**, **smart ships**, and the **Industrial Internet of Things** (**IIoT**) expands the **data accessible** to **threat actors** and widens the potential for **cyber attacks**. Therefore, **strong cyber risk management** strategies are crucial.

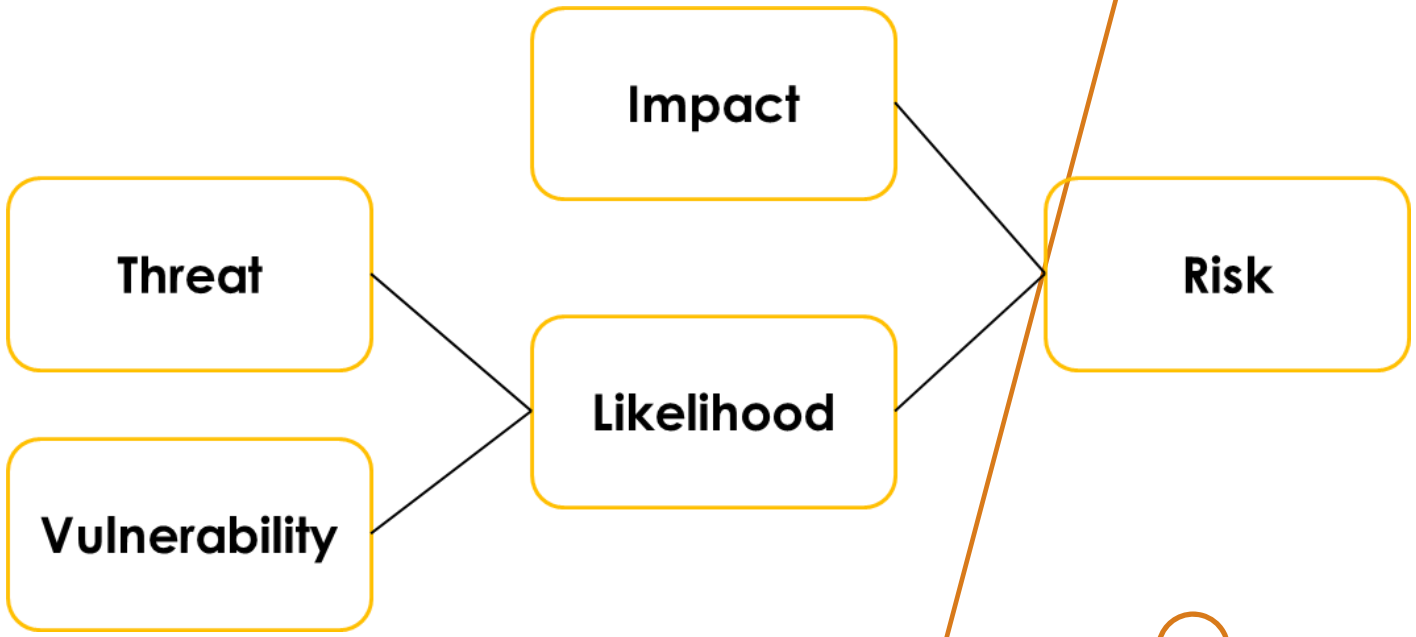
THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS, Version 4, URL: 2021-Cyber-Security-Guidelines.pdf (ics-shipping.org),accessed in February 2024.

Cyber Risk Management Approach



THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS, Version 4, URL: 2021-Cyber-Security-Guidelines.pdf (ics-shipping.org),accessed in February 2024.

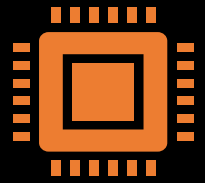
Cyber Risk Management Approach



THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS, Version 4, URL: 2021-Cyber-Security-Guidelines.pdf (ics-shipping.org),accessed in February 2024.

Cyber Risk Management Approach

Identify Threats



- Comprehend the cybersecurity risks originating from **external** sources to the ship.
- Understand the **internal** cybersecurity risks resulting from **improper usage** and **inadequate** cybersecurity protocols.

Identify Vulnerabilities

- Develop inventories of onboard systems with **direct** and **indirect** communications links.
- **Evaluate** the impact of **cyber threats** on these systems. Analyze the **effectiveness** and **limitations** of current **protective** measures.

Assess Risk Exposure

- **Determine** the likelihood of vulnerabilities being exploited by **external threats**.
- **Determine** the security and **safety impact** of any **individual** or **combination** of vulnerabilities being exploited.

THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS, Version 4, URL: 2021-Cyber-Security-Guidelines.pdf (ics-shipping.org),accessed in February 2024.

Cyber Risk Management Approach

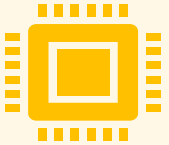
Develop protection and detection measures

- Reduce the likelihood of vulnerabilities being exploited through protection measures.
- Reduce the potential impact of a vulnerability being exploited.

Establish response plans

- Develop contingency plans to effectively respond to identified cyber risks.

Respond to and recover from cyber security incidents



Respond to and recover from cyber security incidents using the contingency plan.

Assess the impact of the effectiveness of the response plan and re-assess threats and vulnerabilities.

THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS, Version 4, URL: 2021-Cyber-Security-Guidelines.pdf (ics-shipping.org),accessed in February 2024.

Cyber Threats in the Maritime Network

Identify Threats

- Companies should analyze potential threat actors' **capability**, **opportunity**, and **intent** to attack.
- Threats can come from **external individuals** or **insiders acting** as unintentional middlemen (e.g., carrying threats on infected USB sticks).
- Once identified, threats should be evaluated alongside known vulnerabilities.
- Assess the **likelihood** of an **attack** or incident occurring.
- Combine the **likelihood** of an incident with its impact to **determine** the overall risk factor.
- Organisations and individuals can constitute an **intentional** or even **unintentional** threat to the **safety** and **security** of a crew, the environment, and the ship.

THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS, Version 4, URL: 2021-Cyber-Security-Guidelines.pdf (ics-shipping.org), accessed on February 2024.

Threat Actors

Group	Motivation
Accidental actors	• No malicious motivation, but causing unintended damage due to bad circumstances and lack of expertise, such as inserting an infected USB into onboard IT or OT systems.
Activists (including disgruntled employees)	• Revenge • disruption of operations • media attention • reputational damage
Criminals	• financial gain • commercial espionage • industrial espionage
Opportunists	• the challenge • reputational gain • financial gain
States State sponsored organisations Terrorists	• political/idealogical gain eg (un)controlled disruption to economies and critical • national infrastructure • Espionage • financial gain • commercial espionage • industrial espionage • commercial gain

THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS, Version 4, URL: 2021-Cyber-Security-Guidelines.pdf (ics-shipping.org),accessed in February 2024.

Types of Cyber Threats

- In general, there are **two categories** of cyber threats that may affect companies and ships:
  - **Untargeted attacks**: involve scenarios where a company or a ship's systems and data are just one of numerous possible targets.
  - **Targeted attacks**: occur when a company or a ship's systems and data are specifically aimed at or identified as one of several targets.

THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS, Version 4, URL: 2021-Cyber-Security-Guidelines.pdf (ics-shipping.org),accessed in February 2024.

Types of Cyber Threats

Untargeted attacks often leverage readily available **internet tools** and **techniques** to exploit widespread **vulnerabilities** present within both a **company's infrastructure** and **onboard ship systems**. Examples of such **tools** and **techniques** include:

Malware

also known as **malicious software**, is crafted to **penetrate** or **harm** a computer system without the **owner's awareness**

Water Holing

Establishing a **fake website** or **compromising** a genuine website to exploit **unsuspecting** visitors

Scanning

Searching large portions of the internet at random for **vulnerabilities** that could be exploited

Typosquatting

Also known as **URL hijacking** or **fake URLs**, this tactic exploits user typos in entering website addresses, redirecting them to potentially **malicious sites**

THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS, Version 4, URL: 2021-Cyber-Security-Guidelines.pdf (ics-shipping.org),accessed in February 2024.

Types of Cyber Threats

Targeted attacks: employ more **advanced methods** and utilize **specialized tools** designed specifically to **target** a particular company or ship. Examples of such tools and techniques utilized in these situations include:

- **Social engineering** is a **non-technical strategy** used by cyber attackers to manipulate insiders into breaching **security procedures**, but not exclusively through **social media interaction**.
- **Brute force** is an **attack method** where **multiple passwords** are attempted in order to **guess** the **correct one**. The attacker **systematically** tests each **possible password** until **finding** the **correct** combination.
- **Credential stuffing** utilizes **credentials** that have been **compromised** before or employs **commonly used passwords** to try to gain **unauthorized** entry into a **system** or **application**.
- **Denial of service (DoS)** disrupts legitimate **users' access** to information by **flooding** a network with **data**. **Distributed denial of service** (**DDoS**) involves **controlling** multiple **computers** and/or **servers** to carry out **such an attack**.
- **Phishing sending** emails to a **large number** of potential **targets** asking for particular pieces of **sensitive** or **confidential** information. The email may also contain a **malicious attachment** or request that a person **visit** a **fake website** using a **hyperlink** included in the email.
- **Spear-phishing** targets **individuals** with personalized **emails**, often containing **malicious software** or **links** for **automatic downloads**. In some cases, SAT-C messages (i.e., maritime communications) are used to establish familiarity with a malicious sender's email address.
- **Subverting the supply chain** by attacking a company or ship by **compromising equipment**, **software**, or supporting services being delivered to the company or ship.

THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS, Version 4, URL: 2021-Cyber-Security-Guidelines.pdf (ics-shipping.org),accessed in February 2024.

Identify Vulnerabilities in the Maritime Network

Identify vulnerabilities

Common vulnerabilities

- **Obsolete** and **unsupported** operating systems
- **Unpatched** system software
- **Outdated** or **missing antivirus software** and **malware protection**
- **Inadequate** security **configurations** and best **practices**, including default **administrator accounts and passwords**
- Shipboard computer networks **lacking** boundary **protection measures** and **network segmentation**
- **Safety-critical equipment** or **systems** consistently **connected** with the **shoreside**
- **Insufficient access controls** for **third parties**, including contractors and service providers
- **Staff lacking** adequate **training** and **skills** to manage cyber risks
- **Missing, inadequate, or untested** contingency **plans** and **procedures**

THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS, Version 4, URL: 2021-Cyber-Security-Guidelines.pdf (ics-shipping.org),accessed in February 2024.

Typical Vulnerable Systems

Identifying vulnerabilities involves **examining applications, systems**, and **procedures** to discover **weaknesses exploitable** by **potential threats.** This process may involve **internal experts** and, when necessary, **external experts f**amiliar with the **maritime industry** and its **critical processes**.

INCIDENT: Crash of integrated navigation bridge system at sea

A ship with an integrated navigation bridge system suffered a failure of nearly all navigation systems at sea, in a high traffic area and reduced visibility. The ship had to navigate by one radar and backup paper charts for two days before arriving in port for repairs. The cause of the failure of all ECDIS computers was determined to be attributed to the outdated operating systems. During the previous port call, a manufacturer technical representative performed a navigation software update on the ship's navigation computers. However, the outdated operating systems were incapable of running the software and crashed. The ship was required to remain in port until new ECDIS computers could be installed, classification surveyors could attend, and a near-miss notification had been issued as required by the company. The costs of the delays were extensive and incurred by the shipowner.

This incident emphasizes that not all computer failures are a result of a deliberate attack and that outdated software is prone to failure. More robust testing and proactive software maintenance on the ship may have prevented this incident from occurring.

Electronic Chart Display Information System (ECDIS)

THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS, Version 4, URL: 2021-Cyber-Security-Guidelines.pdf (ics-shipping.org),accessed in February 2024.

Typical Vulnerable Systems

- The objective of **assessing** a **ship's network**, **systems**, and **devices** is to **detect vulnerabilities** that may **jeopardize** the **confidentiality**, **integrity**, or **availability** of essential **data** and **systems** necessary for **operating equipment**, **networks**, or the **vessel** itself. These **vulnerabilities** can be classified into **several categories:**
  - **Temporary exposures** like **software flaws** or **outdated systems**
  - **Design flaws** such as **poor access management** or **uncontrolled network connections**
  - **Implementation errors** like **misconfigured firewalls**
  - **Procedural** or **user-related mistakes**

THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS, Version 4, URL: 2021-Cyber-Security-Guidelines.pdf (ics-shipping.org),accessed in February 2024.

Examples of Remote Access Equipment for Onboard Ships

- **Certain IT** and **OT systems remain remotely accessible**, maintaining a **continuous internet connection** for **tasks** like **remote monitoring**, **data collection**, **maintenance**, **safety**, and **security purposes**. These systems, known as "**third-party systems**," are **monitored** and **maintained remotely** by contractors. They may involve **two-way data flow** or **upload-only** capabilities. Examples of such systems include those with remote control, access, or **configuration functions**.
  - **Computers** and **workstations** in the **bridge** and **engine** room on the ship's **administrative network**
  - **Remote tracking** of cargo, including **containers** with **reefer temperature control systems** or **specialized cargo**
  - **Stability decision support systems**
  - **Hull stress monitoring systems**
  - Navigational systems such as **Electronic Navigation Chart** (ENC), **Voyage Data Recorder** (VDR), and **dynamic positioning** (DP)
  - **Load planning** and **cargo management systems**
  - **Engine monitoring** and **control systems safety and security networks** like **CCTV** (**closed-circuit television**)
  - **Specialized systems** for **drilling operations**, **blowout preventers**, **subsea installation systems**, **Emergency shutdown** (ESD) for **gas tankers**, and **submarine cable installation** and **repair**.

THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS, Version 4, URL: 2021-Cyber-Security-Guidelines.pdf (ics-shipping.org),accessed in February 2024.

System and Software Maintenance

IT and **OT systems**, **software**, and **maintenance** can be **delegated** to **third-party service providers**, making it challenging for the **company** to **ensure** the provided **security level**. Some companies utilize various **providers** for **software** and cybersecurity **assessments**.

INCIDENT: Navigation computer crash during pilotage

A ship was under pilotage when the ECDIS and voyage performance computers crashed. A pilot was on the bridge. The computer failures briefly created a distraction to the watch officers; however, the pilot and the Master worked together to focus the bridge team on safe navigation by visual means and radar. When the computers were rebooted, it was apparent that the operating systems were outdated and unsupported. The Master reported that these computer problems were frequent (referred to the issues as "gremlins") and that repeated requests for servicing from the shipowner had been ignored.

It is a clear case of how simple servicing and attention to the ship by management can prevent mishaps.

THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS, Version 4, URL: 2021-Cyber-Security-Guidelines.pdf (ics-shipping.org),accessed in February 2024.

Assessing the Likelihood

Assessing the Likelihood

The **probability** of a **cybersecurity incident** occurring is **determined** by the **combination** of the **threat** and the **vulnerability**. If either of these **factors** is nearly **absent**, the **likelihood** of an event will also be **minimal**. It's **important** to take this into **account** when **assessing** the **likelihood** of an **incident**.

Level	Likelihood description
1	**Never heard** of it in the industry. Close to being something **unimaginable**.
2	**Heard** of in the industry, but **only extremely rarely** and as the result of a **chain** of many **unfortunate** events.
3	**Incidents have** probably occurred in my **own company**, but in the context of **faulty equipment** or by **surprising mistakes** made by **people involved**.
4	It happens **occasionally** in one's **own company**, typically in the context of **faulty equipment** or **mistakes** by people involved (the kind of **mistakes** that tend to happen on board from time to time).
5	Happens frequently when **undertaking** the work in question.

THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS, Version 4, URL: 2021-Cyber-Security-Guidelines.pdf (ics-shipping.org), accessed in February 2024.

Assessing the Impact

Impact Assessment

The **confidentiality**, **integrity**, and **availability** (**CIA**) model provides a framework for assessing the impact of:

- Loss of **confidentiality**: **Unauthorized** access to and **disclosure** of **ship**, **crew**, **cargo**, and **passenger** information.
- Loss of **integrity**: Modification of information **critical** for safe and **efficient** ship **operation** and **management**.
- Loss of **availability**: **Destruction** of **information**/**data** or **disruption** to ship **system services**/**operation**.

THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS, Version 4, URL: 2021-Cyber-Security-Guidelines.pdf (ics-shipping.org),accessed in February 2024.

Quantifying the Impact

Level	Impact description
1	**No health effects/injuries**. **No damage** to the environment, **assets**, **finances**, or the company's **reputation**.
2	**Very slight health effects/injuries**. Very **slight damage** to the **environment**, **assets**, finances, or the company's **reputation**.
3	**Some health effects/minor injuries**. **Minor damage** to the environment, **assets**, **finances**, or the company's **reputation**.
4	**Major health effects**/relatively **serious injuries**. Local but **major damage** to the **environment**, **assets**, **finances**, or the company's **reputation**.
5	**Fatality** or **permanent disabilities**. Widespread, significant **damage to environment**, **assets**, **finances**, or company's **reputation**.

THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS, Version 4, URL: 2021-Cyber-Security-Guidelines.pdf (ics-shipping.org),accessed in February 2024.

Quantifying the Impact

There are several **assessment methodologies** that can help define the magnitude of the impact from a cyber incident

Potential impact	In practice
Low	A **limited** adverse **effect means** that a security breach might: (i) result in **minor harm** to individuals; (ii) result in **minor financial loss**; (iii) result in **minor damage** to organisational assets;
Moderate	A **substantial** adverse effect means that a security breach might: (i) result in **significant harm** to individuals that does not involve loss of life or **serious life-threatening injuries**; (ii) result in **significant financial loss**; (iii) result in **significant damage** to organisational assets
High	A **severe or catastrophic** adverse effect means that a security breach might: (i) result in **severe** or **catastrophic harm** to **individuals** involving loss of life or serious life-threatening injuries; (ii) result in **major financial loss**; (iii) result in **major damage** to the **environment** and/or organisational assets;

THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS, Version 4, URL: 2021-Cyber-Security-Guidelines.pdf (ics-shipping.org), accessed in February 2024.

"Critical" Equipment and Technical Systems

- The **impact assessment** should be carried out for **every system on board**.

Example

A ship is equipped with a complex power management system. It consists of switchboards and generators controlling systems for auto load sharing, power control and auto synchronizing. On top of the power management system, a supervisory control and data acquisition (SCADA) system provides output and makes it possible for the crew to control the distribution of onboard electric power.

Power management is important to the safety of the crew, ship, and cargo. It also has a clear environmental and financial impact as power is generated by use of fuel either by the ship's main engine (shaft generator) and/or auxiliary engines. Therefore, a cyber incident that disables or causes the power management system to malfunction can place the operation and safety of the ship at risk. To lower the risk, the company should add protection measures that minimize the possibility of such a cyber incident taking place.

The SCADA system contains real-time sensor data, which is used on board for power management. It also generates data about the power consumption, which is used by the shipping company for administrative purposes. To determine if the potential impact of data and information is being breached, the CIA model should be used. When doing so, the shipping company should determine the potential impact of the most sensitive information stored, processed or transmitted by the SCADA system.

Using the CIA model, the shipping company can conclude that:

- losing confidentiality of the sensor data acquired by the SCADA system will have a low impact as the sensors are publicly displayed on board. However, from a safety point of view, it is important that the information transmitted by the sensors can be relied upon. Therefore, there is a potential high impact from a loss of integrity. It will also be a safety issue if the information cannot be read. So, there is a potential high impact from a loss of availability.
- a loss of confidentiality regarding the power consumption information being sent to the shipping company for statistical purposes is assessed as a potential low impact. There will also be a potential low impact from a loss of integrity and availability as the data is only used for in-house considerations.

The following figure shows the result of the assessment:

SCADA system	Confidentiality	Integrity	Availability	Overall impact
Sensor data	Low	High	High	High
Statistical data	Low	Low	Low	Low

THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS, Version 4, URL: 2021-Cyber-Security-Guidelines.pdf (ics-shipping.org), accessed in February 2024.

Risk Assessment in the Maritime Network

The Four Phases of a Risk Assessment

A **risk assessment** can only be conducted after **thoroughly understanding** threats, **vulnerabilities**, **impacts**, and **likelihood**. It's crucial to **regularly update** the **risk assessment** to **maintain** its **accuracy** and **relevance**.

Phase 1: Pre-assessment activities

- **Risk assessments** are necessary for both **existing** and **new ships** joining the **fleet**. Assessing **cyber risks** is **complex** and **often requires external expertise** to **ensure accuracy**.

THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS, Version 4, URL: 2021-Cyber-Security-Guidelines.pdf (ics-shipping.org),accessed on February 2024.

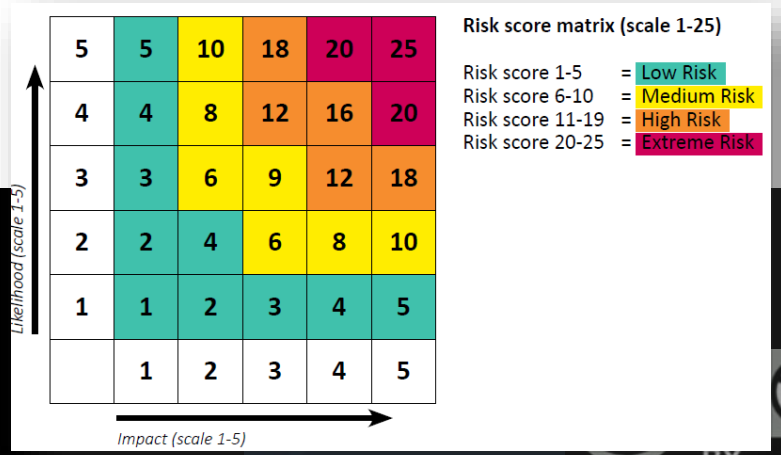
The Four Phases of a Risk Assessment

Phase 2: Ship assessment

- Once **all risk-related factors** (such as **threats**, **vulnerabilities**, **likelihood**, and **impact**) are **evaluated**, the risk **assessment** and **associated risk mitigation measures** can be **conducted**. This process involves **systematically** considering **relevant risk factors**.

- If the **initial risk** of a system **exceeds** the **acceptable level** outlined in the **company's risk** acceptance criteria, **mitigation measures** are necessary to **reduce** the residual risk to an acceptable level.

System	Impact	Likelihood	Initial risk	Mitigation	Residual risk
ECDIS	**Score 5** due to risk of catastrophic events like grounding and collision	**Score 4** due to active USB ports, computer used for other purposes, connection to admin network for access to shared printer, connection to automatic chart updates via satellite via trusted vendor	Risk = 5 x 4 = 20	Password protect and restrict PC use to ECDIS only	Risk = 5 x 3 = 15
				Disconnect from admin network	Risk = 5 x 2 = 10
				Blind off USB ports	Risk = 5 x 1 = 5



THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS, Version 4, URL: 2021-Cyber-Security-Guidelines.pdf (ics-shipping.org),accessed in February 2024.

The Four Phases of a Risk Assessment

Phase 2: Ship assessment

- The **Threat Index** (**TI**) evaluates the value of threats to assets, considering the likelihood of an attack occurring.

TI	Category
5	Definite
4	Probable
3	Occasional
2	Remote
1	Improbable

- **Vulnerability measures** the **likelihood** of a **successful** attack given that a cyber-attack happens, taking into account existing cybersecurity **controls**.
- The **Vulnerability Index** (**VI**) quantifies vulnerability based on implemented cybersecurity measures.

VI	Category
5	Very high
4	High
3	Medium
2	Low
1	Very low

- The Probability Index represents the likelihood of identified cyber-attack scenarios occurring, derived from the combination of the Threat Index and Vulnerability Index.

THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS, Version 4, URL: 2021-Cyber-Security-Guidelines.pdf (ics-shipping.org), accessed in February 2024.
Juntae Kim, Sanghoon Choi, Jinho Yoo, and Kaemyoung Park, The analysis of general cybersecurity requirements applicable to ship's e-Nav service display device based on international standards, url: ENAV28-5.1.1.4-The-analysis-of-general-cybersecurity-requirements-applicable-to-ships-e-Nav.pdf (iala-aism.org)

The Four Phases of a Risk Assessment

Phase 2: Ship assessment

Likelihood Index (**LI**)
Likelihood Index = Threat Index X Vulnerability Index

Likelihood Index	Calculation
5	21 ≤ TI X VI ≤ 25
4	16 ≤ TI X VI ≤ 20
3	11 ≤ TI X VI ≤ 15
2	6 ≤ TI X VI ≤ 10
1	1 ≤ TI X VI ≤ 5

Juntae Kim, Sanghoon Choi, Jinho Yoo, and Kaemyoung Park, The analysis of general cybersecurity requirements applicable to ship's e-Nav service display device based on international standards, url: ENAV28-5.1.1.4-The-analysis-of-general-cybersecurity-requirements-applicable-to-ships-e-Nav.pdf (iala-aism.org)

The Four Phases of a Risk Assessment

Phase 2: Ship assessment

Quantifying the Impact

- The **confidentiality**, **integrity**, and **availability** (CIA) mode provides a framework for **assessing the impact** of:
  - **loss of confidentiality of information**, e.g., unauthorized access to and disclosure of information or data about the ship, crew, cargo, and passengers.
  - **loss of integrity**, which would **modify information** and data relating to the safe and efficient operation and management of the ship.
  - **loss of availability** due to the **destruction** of the information and data and/or the disruption to **services**/ **operation** of ship systems.

Impact Index (Iml)	Category
5	Critical
4	Significant
3	Moderate
2	Minor
1	Negligible

Juntae Kim, Sanghoon Choi, Jinho Yoo, and Kaemyoung Park, The analysis of general cybersecurity requirements applicable to ship's e-Nav service display device based on international standards, url: ENAV28-5.1.1.4-The-analysis-of-general-cybersecurity-requirements-applicable-to-ships-e-Nav.pdf (iala-aism.org)

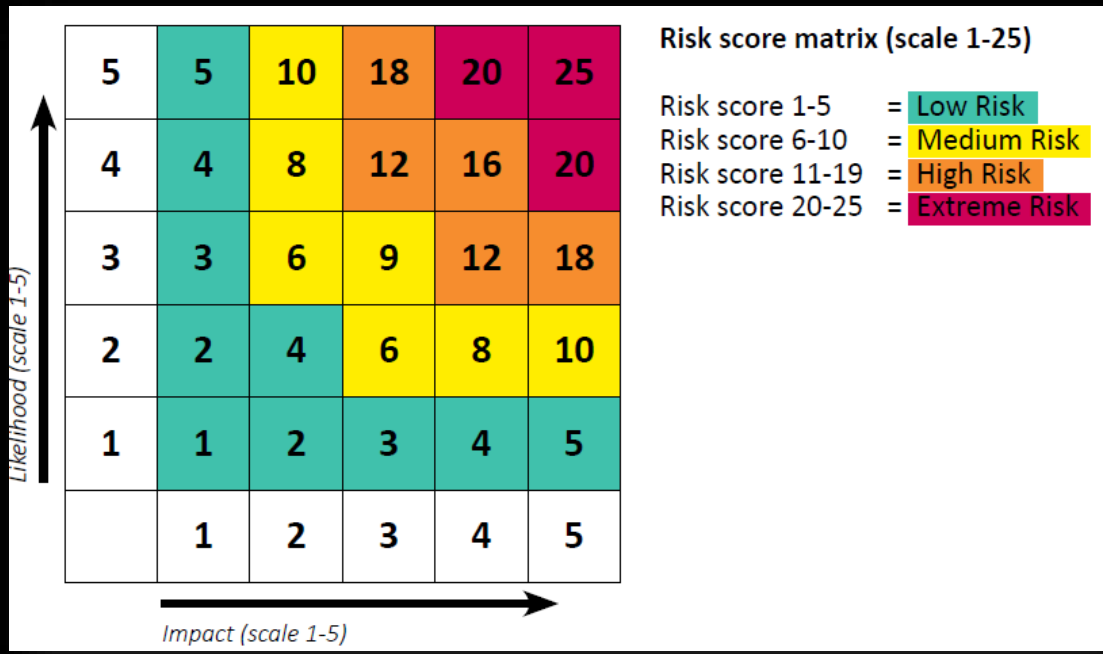
The Four Phases of a Risk Assessment

Phase 2: Ship assessment

Risk Analysis and Control Identification

Cyber security Risk Index (RI) = TI x VI x ImI

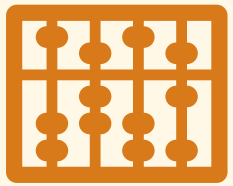
= Likelihood Index (TI x VI) x Impact Index (ImI)



Juntae Kim, Sanghoon Choi, Jinho Yoo, and Kaemyoung Park, The analysis of general cybersecurity requirements applicable to ship's e-Nav service display device based on international standards, url: ENAV28-5.1.1.4-The-analysis-of-general-cybersecurity-requirements-applicable-to-ships-e-Nav.pdf (iala-aism.org)

The Four Phases of a Risk Assessment

Phase 3: Debrief and reporting



- The **risk assessment** should be a **comprehensive** and regularly updated document that reflects **how risks** are **evaluated** and **managed**.

- It often **involves** considering various **mitigation options** until the optimal **combination** is determined based on legal **requirements**, **risk tolerance**, **feasibility**, **effectiveness**, and **cost**.

- If conducted by an **external party** due to **insufficient in-house expertise**, the **initial** report typically **serves** as an interim **assessment** with **recommendations**.
- Final **decisions** should be **incorporated** into the **updated** risk **assessment document**.

THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS, Version 4, URL: 2021-Cyber-Security-Guidelines.pdf (ics-shipping.org),accessed in February 2024.

The Four Phases of a Risk Assessment

Phase 3: Debrief and reporting

- An **initial third-party cyber risk assessment** could, for example, include the following:
  - The **executive summary** provides a **condensed overview** of the **assessment results**, **recommendations**, and the **overall security status of the ship**.
  - **Technical findings** detail **discovered vulnerabilities**, including their **likelihood** of **exploitation**, **potential financial impact**, and suggested **technical fixes** and **mitigation strategies**.
  - A **prioritized list** of **actions** is included, considering **factors** such as **effectiveness**, **cost**, and **applicability**, **ensuring** it encompasses all available options rather than **promoting specific services** or products.
  - **Supplementary** data **offers in-depth** technical information on key **findings** and **critical flaws**, along with any sample data obtained during **penetration testing** of **high-risk vulnerabilities**.

THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS, Version 4, URL: 2021-Cyber-Security-Guidelines.pdf (ics-shipping.org),accessed in February 2024.

The Four Phases of a Risk Assessment

Phase 4: Manufacturer's debrief

- After **reviewing assessment findings**, **shipowners** may need to **share select findings** with **system manufacturers** to **mitigate risks**.
- Identified **cyber vulnerabilities** in **critical systems** may **require analysis** with **external experts**.
- **External experts** collaborate **with manufacturers' cybersecurity** contacts to ensure a **comprehensive understanding** of the issue.
- This **collaboration** aims to **develop** a thorough **remediation** plan addressing **vulnerabilities effectively**.

THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS, Version 4, URL: 2021-Cyber-Security-Guidelines.pdf (ics-shipping.org),accessed in February 2024.

Third-Party Risk Assessments

Phase 4: Manufacturer's debrief

Consideration of third-party assistance for accurate risk assessments depends on the company's **capabilities**.

Third-party risk assessments may involve **penetration tests** of **critical IT** and **OT** infrastructure to match **defense levels** with the desired **cyber security** strategy.

Active **penetration tests** **simulate incidents** using **IT systems**, **social engineering**, and **physical security breaches**, while **passive methods** rely on **scanning data transmissions**.

Third-party assessments integrate specialized **skills** and **expertise** into **cyber risk** management **efforts**, **benefiting companies** with **limited resources**.

Various services beyond **penetration testing**, such as **asset discovery**, network **architecture reviews**, and vulnerability assessments, contribute to **understanding** organizational **environments**.

Penetration testing, though effective, **carries more risk** and **expense** and should be used selectively based on **specific circumstances** and **technical requirements**.

Coordination with **supervising officers** and **shoreside** staff is **essential** for **safety** during **third-party assessments**, and **selecting experienced** providers with **fleet awareness** is **crucial**.

THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS, Version 4, URL: 2021-Cyber-Security-Guidelines.pdf (ics-shipping.org),accessed in February 2024.

Develop Protection Measures in the Maritime Network

Defence in Depth and in Breadth

The **defence in-depth** approach encourages a combination of:

- **physical security** of the ship in accordance with the **ship security plan** (SSP)
- **protection** of networks, including effective segmentation
- **intrusion detection**
- use of **firewall**
- periodic **vulnerability scanning** and **testing**
- software **whitelisting**
- **access** and **user controls**
- configuration and change management controls
- **appropriate procedures** regarding the use of **removable** media and password policies
- **personnel's cyber security awareness** and **understanding** of the risk to themselves and the industry
- **understanding** and **familiarity** with appropriate **procedures**, including **incident response**.

THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS, Version 4, URL: 2021-Cyber-Security-Guidelines.pdf (ics-shipping.org),accessed in February 2024.

Defence in Depth and in Breadth

Defence in breadth:

- The **trust boundary** model categorizes systems based on **implicit** or **explicit** trust **relationships**.
- **Threat modeling** helps identify areas for **implementing technical controls** between systems in **large** or **complex** networks.
- On ships with high **IT** and **OT** integration, **defense in depth** requires layered protection **measures** across all **vulnerable systems**.
- Defense in breadth **prevents vulnerabilities** in one system from **compromising** the **protection measures** of another system.

THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS, Version 4, URL: 2021-Cyber-Security-Guidelines.pdf (ics-shipping.org),accessed in February 2024.

Technical Protection Measures

- **Limitation** to and **control** of network **ports**, **protocols**, and **services**
- **Configuration** of network **devices** such as **firewalls**, **routers**, and **switches**
- **Physical security**
- **Satellite** and **radio communication**
- **Wireless access control**
- **Secure configuration** of **hardware** and **software**
- **Email** and **web browser** protection
- Application software security (**patch management**)

THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS, Version 4, URL: 2021-Cyber-Security-Guidelines.pdf (ics-shipping.org),accessed in February 2024.

Procedural Protection Measures

- Training and awareness
- Computer access for visitors
- Crew’s personal devices
- Upgrades and software maintenance
- Anti-virus and anti-malware tool management
- Use of administrator privileges
- Multi/factor authentication (MFA) and passwords
- Physical and removable media controls
- Equipment disposal, including data destruction

THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS, Version 4, URL: 2021-Cyber-Security-Guidelines.pdf (ics-shipping.org),accessed in February 2024.

Develop Detection Measures

Detection, blocking and alerts

- **Intrusion Detection System** (**IDS**) or an **Intrusion Prevention System** (**IPS**) into the **network** or as part of the **firewall**.
- **Identify threats**/**malicious** activity and **code**, and then **log**, **report**, and **attempt** to block the activity.

Malware detection

- **Scanning software** that can **automatically detect** and address the presence of **malware in systems**
- onboard should be kept up to **date** and **managed**.

THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS, Version 4, URL: 2021-Cyber-Security-Guidelines.pdf (ics-shipping.org),accessed in February 2024.

Establish Contingency Plans

- Develop a **response plan** covering various contingencies and maintain hard copies in case of **electronic access loss**.
- Understand the **importance** of cyber **incidents** as **safety concerns** when creating ship **contingency plans**.
- Collaboration with **shoreside management teams** is essential for **effective contingency planning**.
- **Assess** the impact of any **cyber incident** on **operations** and **assets**.
- In most **cases**, **except** for load **planning systems**, **IT system loss** or **data breaches** are primarily **business continuity** issues rather than immediate **safety concerns**.
- For **incidents affecting** only **IT systems**, notify **designated personnel** within the **shipowner** or **operating** company for **immediate response**.
- Designated personnel should be **available** to the ship's Master in case of a **cyber incident**.

THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS, Version 4, URL: 2021-Cyber-Security-Guidelines.pdf (ics-shipping.org),accessed in February 2024.

Respond to and Recover from Cyber Security Incidents

Response

- As determined by **NIST**, there are four key phases to incident response:
  - Preparation
  - Detection and analysis
  - Containment and eradication
  - Post-incident recovery.

Recovery

- Maintain **recovery plans** in hard copy both **onboard** and **ashore** accessible to **personnel responsible** for **cyber security** and **assisting** in cyber incidents.
- The plan aims to aid in the recovery of systems and data essential for restoring both **IT** (**Information Technology**) and **OT** (**Operational Technology**) to operational status.
- **Prioritize** the safety of **onboard personnel** by focusing on the **operation** and **navigation** of the ship within the plan.
- Tailor the **recovery plan's detail** and **complexity** based on the specific type of **ship** and the **IT**, **OT**, and other **systems installed onboard**.

THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS, Version 4, URL: 2021-Cyber-Security-Guidelines.pdf (ics-shipping.org),accessed in February 2024.

The Critical Importance of Maritime OT Cybersecurity

- With the integration of **connected technology**, **operational technology** (**OT**) functions like **bridge operations**, **navigation**, **communications**, and **cargo management** become **vulnerable** to **remote cyber threats**.
- **Threat actors** can **exploit vulnerabilities** through **navigation spoofing** and **satellite** communication **hacking** to manipulate a ship's **GPS**, potentially leading to **collisions** or physical **attacks**.
- **Cybercriminals** may also employ other **tactics**, such as **stealing sensitive information** and **holding data** or **cargo for ransom**, to **compromise maritime cybersecurity**.

Navigating Cybersecurity Challenges in Maritime Operational Technology (maritime-executive.com), accessed in February 2024

Escalating Cybersecurity Threats in the Maritime Industry: Major Shipping Firm Cyberattacks

- There has been a consistent rise in cyberattacks targeting **terminals** and **shipping companies** over recent years.
- In September 2020, CMA CGM SA **Compagnie Maritime d'Affrètement** (**CMA**) and **Compagnie Générale Maritime** (**CGM**), a French container shipping line, disclosed a **malware attack** affecting **two** of its Asia-Pacific **subsidiaries**.
- The attack involved encryption malware, resulting in **potential data theft**, disruption of the electronic booking platform, cargo delivery delays, and communication interruptions with customs authorities.

Navigating Cybersecurity Challenges in Maritime Operational Technology (maritime-executive.com), accessed in February 2024

Escalating Cybersecurity Threats in the Maritime Industry: Major Shipping Firm Cyberattacks

Date	Victim	Location	Incident Type	Malware
May 2017	Clarksons PLS	UK	Unidentified Hacker(s)	Unknown
June 2017	Maersk	130 countries	Ransomware	NotPetya
July 2018	China Ocean Shipping Company (COSCO) Terminal	Long Beach Port, CA, USA	Ransomware	Unknown
Sept 2018	Port of Barcelona	Spain	Unidentified Cyber Attack	Unknown
Sept 2018	Port of San Diego	USA	Ransomware	SamSam
July 2019	Deep Draft Vessel Bound for the Port of New York	New York, USA	Malware	Emotet
April 2020	Mediterranean Shipping Company (MSC)	Geneva, Switzerland	Malware	Unknown
May 2020	Shahid Rajaee Port Terminal	Iran	Unidentified Hacker(s)	Unknown
Sept 2020	CMA CGM SA	Asia-Pacific	Ransomware	Ragnar Locker
Sept 2020	US Tugboat	Louisiana	Phishing Email	Unknown
Oct 2020	The International Maritime Organization (IMO)	International	Malware	Unknown

Navigating Cybersecurity Challenges in Maritime Operational Technology (maritime-executive.com), accessed in February 2024

Cybersecurity Regulation in Maritime

Cybersecurity Regulations

- Starting from **January 2024**, adherence to **UR E26** and **UR E27** requirements regarding the **cyber resilience** of **ships** and **onboard** equipment **becomes obligatory**.

1. **UR E26** and **UR E27** are new **cybersecurity regulations** set forth by the **International Association of Classification Societies** (**IACS**).
2. Their **primary objective** is to **strengthen cyber resilience** within the **maritime industry**.
3. **UR E26** specifically focuses on integ**rating Operational Technology** (**OT**) and **Information Technology** (**IT**) **onboard ships**.
4. **UR E27** addresses the **security aspects** of **onboard equipment** and **systems supplied** by **third-party** entities.

2024: Cybersecurity Sea-Change – Four Crucial Points for Consideration (moxa.com)
(9) UR E26 & UR E27: Q&A for Busy Professionals | LinkedIn, accessed in February 2024.

Cybersecurity Regulations

To effectively adapt to **these regulations**, understanding **four** key points is essential.

Who Does UR E26 and UR E27 Apply To?

What Are the Benefits of Early Adoption of UR E27?

Which Classification Societies Will Release Verification Guidelines?

The Heart of UR E26 and UR E27

2024: Cybersecurity Sea-Change – Four Crucial Points for Consideration (moxa.com), accessed in March 2024

Cybersecurity Regulations

- **Who Does UR E26 and UR E27 Apply To?**
  - The **main objective** is pinpointing the maritime **stakeholders affected** by the **new cybersecurity regulations**.
  - Specifically, **UR E26**, "**Cyber Resilience of Ships**," places ship design firms, shipyards, and system designers at the forefront of **cybersecurity responsibility**.

Item	Application
IACS UR E26/27	• Propulsion • Steering • Anchoring and mooring • Electrical power generation and distribution • Fire detection and extinguishing systems • Cargo handling system (limited to safety-related elements) • Bilge and ballast systems, loading/unloading control systems, loading computer • Boiler control system • Scrubber control system and other systems needed for compliance with class or international regulations to prevent pollution to the environment • Watertight integrity and flooding detection • Lighting (e.g., emergency lighting, low locations, navigation lights, etc.) • Any other OT system whose disruption or functional impairing may pose risks to ship operations (e.g., LNG monitoring and control system, relevant gas detection system etc.) • Navigational systems required by statutory regulations • Internal and external communication systems required by class rules and statutory regulations

2024: Cybersecurity Sea-Change – Four Crucial Points for Consideration (moxa.com), accessed in March 2024

Cybersecurity Regulations

- **Who Does UR E26 and UR E27 Apply To?**
  - **UR E27**, "**Cyber Resilience of On-Board Systems and Equipment**," **expands regulations** to cover **all onboard** operational technology systems, involving all relevant personnel.
  - **Shipowners** must specify their **classification societies** and **security levels**.
  - Suppliers are required to develop resilient products meeting **security standards** like **IEC 62443-4-1** - **Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements**
  - and **IEC 62443-4-2** - **Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components**.

2024: Cybersecurity Sea-Change – Four Crucial Points for Consideration (moxa.com), accessed in March 2024

Cybersecurity Regulations

What Are the Benefits of Early Adoption of UR E27?

Early adopters conducting **a UR E27** compliant **gap analysis** and validation could gain a competitive edge in 2024.

Which Classification Societies Will Release Verification Guidelines?

Each classification society is expected to release its respective guidance documents and related supporting materials this year, all based on UR E26 and UR E27 requirements.

2024: Cybersecurity Sea-Change – Four Crucial Points for Consideration (moxa.com), accessed in March 2024

Cybersecurity Regulations

The Heart of UR E26 and UR E27

- **UR E26** establishes principles for building **cyber-resilient ships** and provides guidelines for maritime professionals constructing **Computer Based Systems** (**CBS**).
- It focuses on **five essential dimensions** of information security: **identification**, **protection**, **detection**, **response**, and **recovery**.
- **UR E27** operationalizes these principles, especially referencing the **IEC 62443-3-3 standard**.
- Understanding **IEC 62443** is crucial for meeting **UR E27's** security **criteria**.
- **IACS UR E27 4.1**, "**Required security capabilities**," outlines 31 **requirements corresponding** to various objectives and aligns them with **IEC-62443-3-3 SR system requirements**.

2024: Cybersecurity Sea-Change – Four Crucial Points for Consideration (moxa.com), accessed in March 2024

Cybersecurity Regulations

The Heart of UR E26 and UR E27

Sl No	Objective	Requirements
1	**Human user identification and authentication**	The **CBS** shall **identify** and **authenticate** all human users who can access the system directly or through interfaces (IEC 62443-3-3/SR 1.1)
2	**Account management**	The **CBS** shall provide the capability to support the **management** of all accounts by **authorized** users, including **adding**, **activating**, **modifying**, **disabling**, and **removing accounts** (IEC 62443-3-3/SR 1.3)
3	**Identifier management**	The **CBS** shall provide the capability to support the management of identifiers by **user**, **group**, and **role** (IEC 62443-3-3/SR 1.4)
4	**Authenticator management**	The **CBS** shall provide the capability to: - **Initiate authentication** - Change all default **authenticators** upon control system **installation** - **Change/refresh** all **authenticators** - **Protect** all **authenticators** from unauthorized **disclosure** and **modification** when **stored** and **transmitted** (IEC 62443-3-3/SR 1.5)
5	**Wireless access management**	The **CBS** shall provide the **capability** to **identify** and **authenticate** all users (humans, software processes or devices) engaged in **wireless communication** (IEC 62443-3-3/SR 1.6)
6	**Strength of password-based authentication**	The **CBS** shall provide the capability to enforce **configurable** password strength based on **minimum length** and variety of **character types** (IEC 62443-3-3/SR 1.7)
7	**Authenticator feedback**	The **CBS** shall obscure feedback during the **authentication process** (IEC 62443-3-3/SR 1.10)
8	**Authorization enforcement**	On all **interfaces**, **human users** shall be assigned **authorizations** in accordance with the principles of segregation of **duties** and **least privilege**. (IEC 62443-3-3/SR 2.1)
9	**Wireless use control**	The **CBS** shall provide the capability to **authorize**, **monitor**, and **enforce usage restrictions** for **wireless** connectivity to the **system according** to commonly accepted **security industry practices** (IEC 62443-3-3/SR 2.2)
10	**Use control for portable and mobile devices**	When the **CBS** supports the **use** of **portable** and **mobile** devices, the system shall include the capability.

Source: 2024: Cybersecurity Sea-Change – Four Crucial Points for Consideration (moxa.com) based on IACS UR E27 4.1

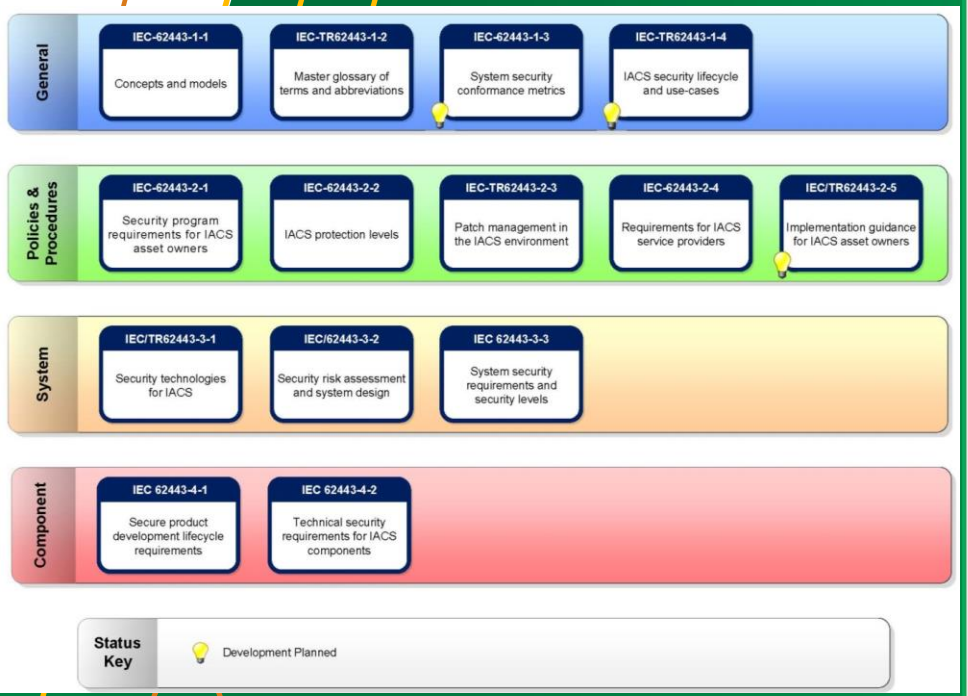
2024: Cybersecurity Sea-Change – Four Crucial Points for Consideration (moxa.com), accessed in March 2024

Cybersecurity Standards in Maritime

IEC 62443 Cybersecurity Standard

IEC 62443

- The **IEC 62443 series's** primary goal is to present a **framework** that addresses **current** and **future** security **vulnerabilities** in industrial systems.
- It enables **security** risk management for the **complete life cycle** and all **layers** of **industrial** networks.
- This is done by **dividing** the **system** into **zones**, defining **security levels** for each **zone**, and specifying security **capabilities** that enable a component to be integrated into a system environment at a given **security level** (**SL**).
- The **IEC 62443 standard consists** of multiple documents classified into four main groups: **General**, **Policies and Procedures**, **System**, and **Component**.



Source: https://syc-se.iec.ch/deliveries/cybersecurity-guidelines/security-standards-and-best-practices/iec-62443/

- The **first two groups** represent **concepts**, **uses cases**, **policies**, and **procedures associated** with ICS security.
- The other **two groups**, **System and Component**, define the **technical requirements** for **networks** and **system components**.

IEC. IEC 62443 - Security for industrial automation and control systems – part 4-2: Technical security requirements for IACS components. Technical report, International Standard, Feb. 2019.
ISA. The 62443 series of standards: Industrial automation and control systems security. (1-4), 2018.
Shaaban, A. An Ontology-Based Cybersecurity Framework for the Automotive Domain-Design, Implementation, and Evaluation. Ph.D. Thesis, Faculty of Computer Science, University of Vienna, Vienna, Austria, 2021. Available online: https://utheses.univie. ac.at/detail/59948 (accessed on 26 February 2024).

IEC 62443 Cybersecurity Standard

IEC 62443

General:

- The **first category** of this series is **General**, which involves **discussion** and **subjects** that are common throughout the entire series.
- The **IEC TS 62443-1-1** represents the **terminologies**, **principles**, and models for IACS security. There are **seven foundational requirements** (**FRs**), as follows:
  - **FR1: Identification and Authentication Control (IAC)**: The main objective of the **identification** and **authentication** control is to validate a user's identity before getting **permission** to access a system.
  - **FR2: Use Control (UC)**: This foundational requirement **restricts** system access to **authorized users only**.
  - **FR3: System Integrity (SI)**: Security **integrity** aims to prevent an **unauthorized entity** (i.e., individuals, processes, software, or hardware) from **compromising** any parts of the system.
  - **FR4: Data Confidentiality (DC)**: **Data confidentiality** intends to prevent **unauthorized disclosure** activities of data on communication **channels** or **data stores** in repositories.
  - **FR5: Restricted Data Flow (RDF)**: **Restricting** the **unnecessary** data flow by **creating security** boundaries called **security zones** and **conduits** for communication channels.
  - **FR6: Timely Response to Events (TRE)**: Create notifications to respond to any **malicious activities** on a **system**.
  - **FR7: Resource Availability (RA)**: **Ensure** the **availability** of a system **against** different **types** of **denial of service** attacks.

- Shaaban, A. An Ontology-Based Cybersecurity Framework for the Automotive Domain-Design, Implementation, and Evaluation. Ph.D. Thesis, Faculty of Computer Science, University of Vienna, Vienna, Austria, 2021. Available online: https://utheses.univie. ac.at/detail/59948 (accessed on 26 February 2024).
- SyC Smart energy. IEC 62443. https://syc-se.iec.ch/deliveries/cybersecurity-guidelines/security-standards-and-best-practices/iec-62443/, 2020. (Accessed on: February 26, 2024).
- IEC 62443-3-3: Industrial communication networks – network and system security – part 3-3: System security requirements and security levels, 2013.

IEC 62443 Cybersecurity Standard

IEC 62443

Policies and Procedures:

- This category is concerned with the security of the **IACS**, which **provides security requirements** to **evaluate** the **protection level** of operational IACS.
  - The **IEC 62443-2-1** describes the **asset owner** for **IACS** and outlines the requirements for **creating** and **evolving** the security program. This series specifies the necessary **capabilities** of the **protection** needed to ensure the **operation** of an **IACS**.
  - The second set is **IEC/IS 62443-2-2**, which specifies a **methodology** and **framework** of an **IACS** for **assessing** defence according to the **security level** and **implementation** of the related processes.
  - The **next** and **third series** in this category is **IEC / TR 62443-2-3**, which offers details about the **exchanging format** from **asset owners** to **product suppliers**. Additionally, it **describes activities** associated with the **suppliers** and **deployment** of the patches by **asset owners**.
  - The **last series** of this category is the **IEC 62443-2-4**, which defines security requirements for **IACS** service **providers**. Such **capabilities** are specified in **IEC 62443-3-3**, which the **service** provider **guarantees** are to be maintained within the scope of the **automation Solution.**

- Shaaban, A. An Ontology-Based Cybersecurity Framework for the Automotive Domain-Design, Implementation, and Evaluation. Ph.D. Thesis, Faculty of Computer Science, University of Vienna, Vienna, Austria, 2021. Available online: https://utheses.univie. ac.at/detail/59948 (accessed on 26 February 2024).
- SyC Smart energy. IEC 62443. https://syc-se.iec.ch/deliveries/cybersecurity-guidelines/security-standards-and-best-practices/iec-62443/, 2020. (Accessed on: February 26, 2024).

IEC 62443 Cybersecurity Standard

IEC 62443

System:

- The **IEC 62443-3-1** standard provides an **overview** of the **advantages** and **limitations** of existing network security technologies.
- **IEC 62443-3-2** standard addresses security **risk assessment** and **network design**.
- Finally, the **IEC 62443-3-3** standard outlines general system **security requirements**, **emphasizing** that performance should not be **jeopardized** during the addressing process of these requirements.

Component:

- The Component group **consists** of **two documents**.
  - **The IEC 62443-4-1** standard defines the **development process** of **ICS** products to reduce the number of **security vulnerabilities** in control system solutions.
  - The **IEC 62443-4-2** standard **specifies** the **technical requirements** for **securing** the individual **components** of an **ICS network**. The standard documents are aligned with **IACS life-cycle phases**.

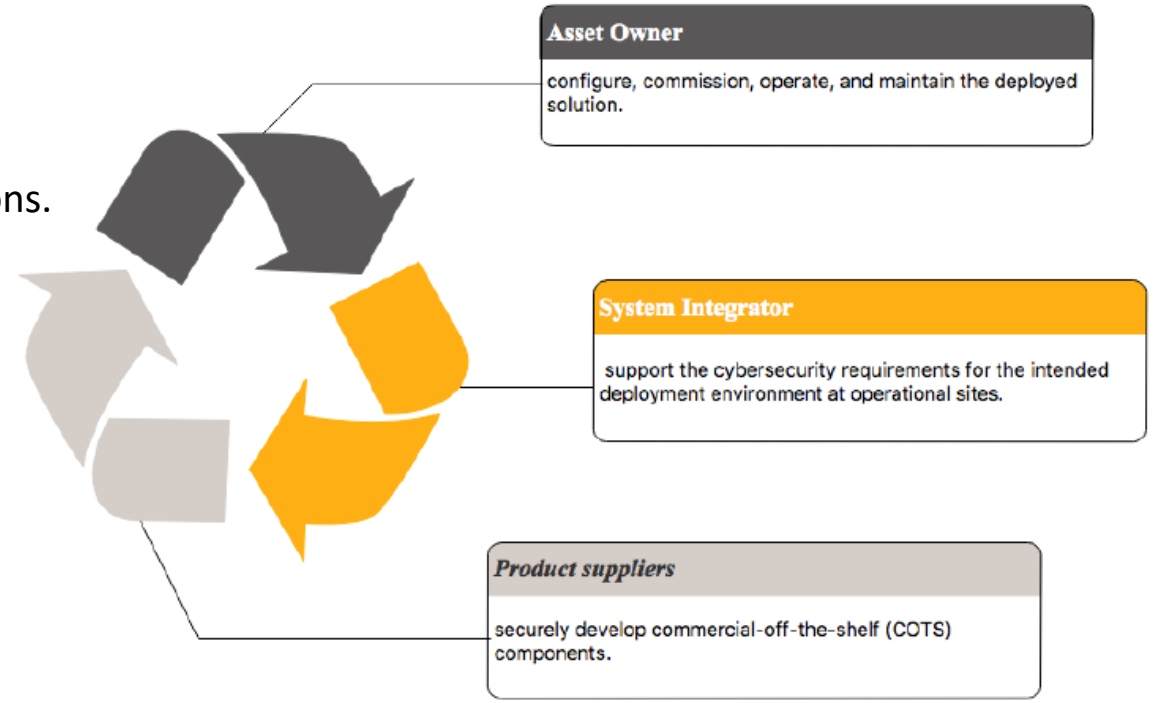
- Shaaban, A. An Ontology-Based Cybersecurity Framework for the Automotive Domain-Design, Implementation, and Evaluation. Ph.D. Thesis, Faculty of Computer Science, University of Vienna, Vienna, Austria, 2021. Available online: https://utheses.univie. ac.at/detail/59948 (accessed on 26 February 2024).
- SyC Smart energy. IEC 62443. https://syc-se.iec.ch/deliveries/cybersecurity-guidelines/security-standards-and-best-practices/iec-62443/, 2020. (Accessed on: 26 February 2024).
- Security Levels in ISA-99 / IEC 62443. ISA 99 security levels proposal. https://www.scribd.com/document/129590220/ISA-99-SecurityLevels-Proposal/, 2020. (Accessed on: 26 February 2024).

IEC 62443 Cybersecurity Standard

IEC 62443

- In order to be successful in **IACS cybersecurity**, all target **audiences** (**Owner**, **Integrator**, **Supplier**) have "**shared responsibility**" for all phases of the IACS cybersecurity life cycle.

- The **IEC 62443** standard defines **rules** and **methods** to operate **IACS networks** by **requirements**, **controls** and best practices recommendations.



- Andre Ristaino. Industrial automation cybersecurity conformity assessments. http://www.isasecure.org/en-US/Articles/Industrial-automation-cybersecurity-conformity-ass.
- Shaaban, A. An Ontology-Based Cybersecurity Framework for the Automotive Domain-Design, Implementation, and Evaluation. Ph.D. Thesis, Faculty of Computer Science, University of Vienna, Vienna, Austria, 2021. Available online: https://utheses.univie.ac.at/detail/59948 (accessed on 26 February 2024).

Zones and Conduits Concept in IEC 62443

IEC 62443

- The **IEC 62443** security standard **highlights** the importance of conducting a **security analysis** for **manufacturing facilities**.
- It **divides** the facility into sections known as "**security zones**".
- The **standard** also **recommends delineating data flows** between **interconnected security zones** using **conduits**, referred to as communication channels.
- It specifies the **zones** and **conduit requirements**, known as **ZCRs**, for assessing the system.
- The **System Under Consideration**(**SuC**) involves **defining** a group of **IACS** and **associated** assets to perform a **risk analysis**.
- **IEC 62443** provides **guidelines** for establishing **zones**, **conduits**, and **their connections** to **ZCRs**.

Shaaban, A.M.; Chlup, S.; El-Araby, N.; Schmittner, C. Towards Optimized Security Attributes for IoT Devices in Smart Agriculture Based on the IEC 62443 Security Standard. *Appl. Sci.* **2022**, *12*, 5653. https://doi.org/10.3390/app12115653

Zones and Conduits Concept in IEC 62443

ZCR1—identification of the SuC The identification of the System under Consideration (SuC) must include detailing the **security limits** and **identifying** all **access points** to the SuC.

ZCR2—high-level risk assessment: A **high-level risk assessment** of the SuC is conducted to identify **unaddressed risks**, defining the **worst-case scenario** associated with the SuC. This evaluation helps **categorize assets** into **separate zones** and **conduits**. High-level risk can be quantified using a **risk matrix** to define the **relationship** between the **likelihood** and the **impact** values. There are **five different** levels of parameter values for the **likelihood** and **impact** values.

Likelihood levels:

- Level 1: Trivial
- Level 2: Minor
- Level 3: Moderate
- Level 4: Major
- Level 5: Critical

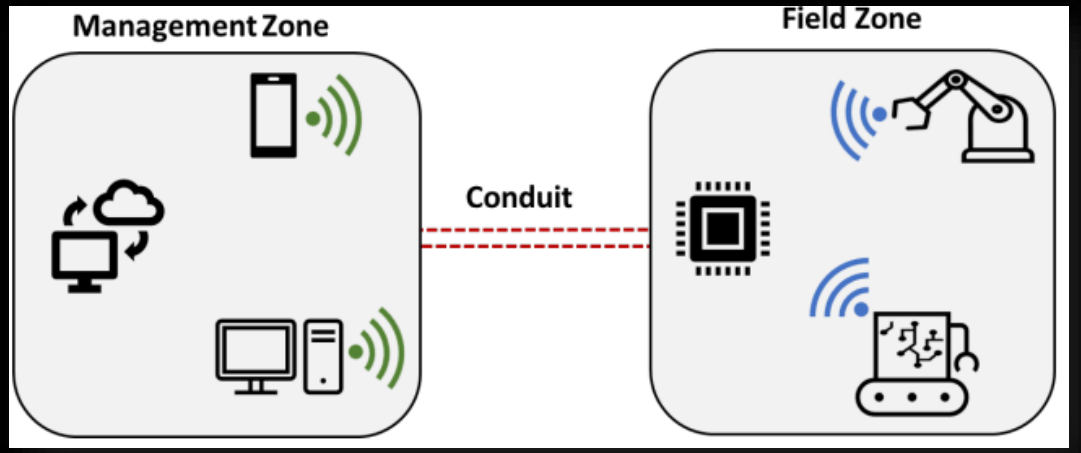
Impact levels:

- Level 1: Remote
- Level 2: Unlikely
- Level 3: Possible
- Level 4: Likely
- Level 5: Certain

Shaaban, A.M.; Chlup, S.; El-Araby, N.; Schmittner, C. Towards Optimized Security Attributes for IoT Devices in Smart Agriculture Based on the IEC 62443 Security Standard. *Appl. Sci.* **2022**, *12*, 5653. https://doi.org/10.3390/app12115653

Zones and Conduits Concept in IEC 62443

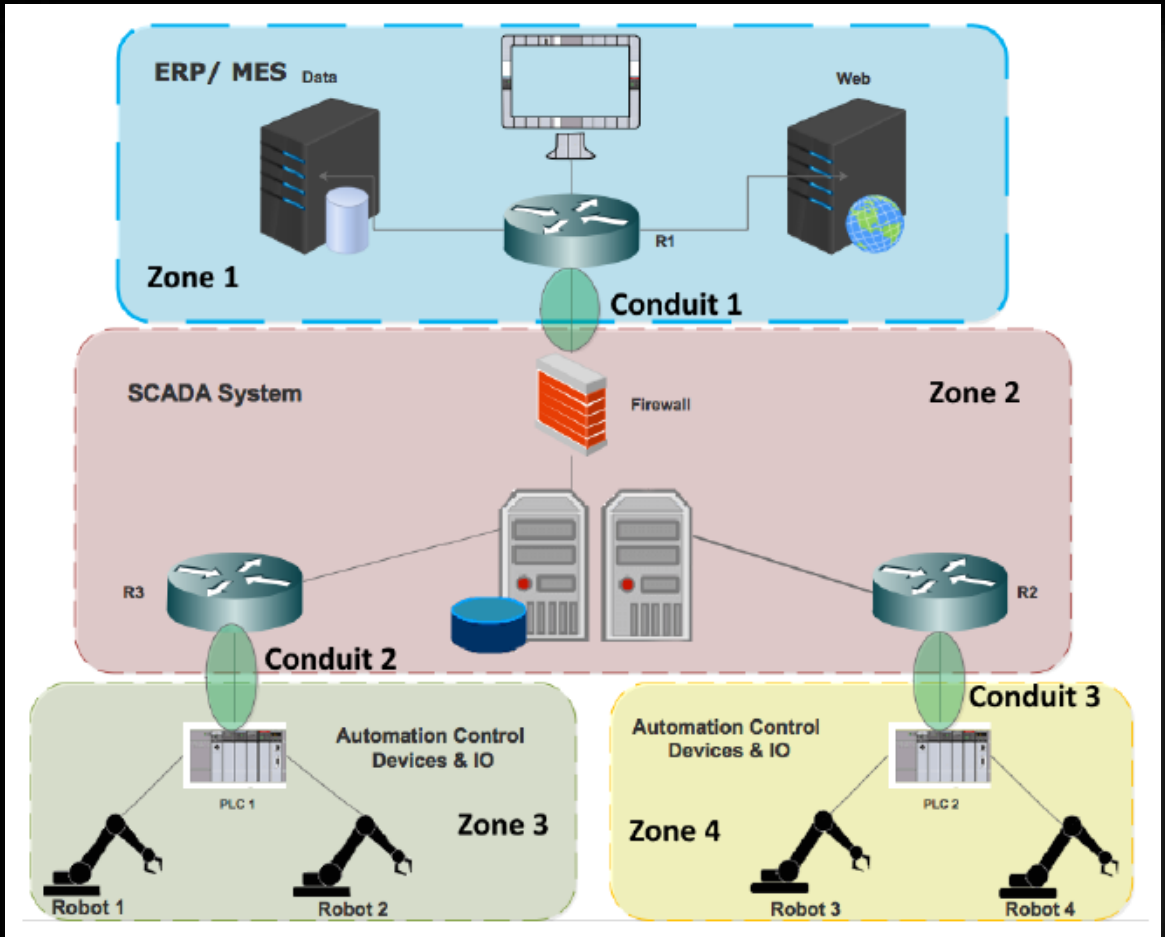
ZCR 3—Partition the SuC into zones and conduits: This phase **splits** up the complex overall system into separate **zones** and **conduits**.



ZCR 4—document cyber security requirements, assumptions and constraints: This is the last phase to assess the cyber risk for each **zone** and **conduit** to individually evaluate **target security levels**

Shaaban, A.M.; Chlup, S.; El-Araby, N.; Schmittner, C. Towards Optimized Security Attributes for IoT Devices in Smart Agriculture Based on the IEC 62443 Security Standard. *Appl. Sci.* **2022**, *12*, 5653. https://doi.org/10.3390/app12115653

Case-Study: Operating Plant



- The operating plant is divided into **four security zones** (Zone 1, Zone 2, Zone 3, and Zone 4).
- **Three conduits** (Conduit 1, Conduit 2, and Conduit 3) define the communication paths between these zones.
- The **interconnection** and **communication** paths between the **zones** are then defined as "**Conduits**", the pipes where **secure data** and **information** exchange is performed.

- Shaaban, A. An Ontology-Based Cybersecurity Framework for the Automotive Domain-Design, Implementation, and Evaluation. Ph.D. Thesis, Faculty of Computer Science, University of Vienna, Vienna, Austria, 2021. Available online: https://utheses.univie. ac.at/detail/59948 (accessed on 26 February 2024).

Security Levels

- The **IEC 62443** standard presents the concept of **security levels** (**SL**) applicable to various **elements** such as **zones**, **conduits**, **channels**, and **products**.
- To define a **security level**, **an in-depth analysis** of a specific **device** is conducted to ascertain the appropriate security level based on its **role** and **place** in the system.
- These **security levels** are categorized into **four unique** levels, ranging from **1** to **4**.

- After **establishing** the **targeted security** level for a **zone**, evaluate whether the **devices** within that zone comply with the set **security level**.
- Should the **devices fail** to **meet** the required **security level**, it's essential to **strategize** and **implement countermeasures** to achieve the **security level goal**.
- These **countermeasures** can **vary**, including technical **solutions** like **firewalls**, **administrative measures** such as **policies and procedures**, or **physical safeguards** like securing areas with **locked doors**.

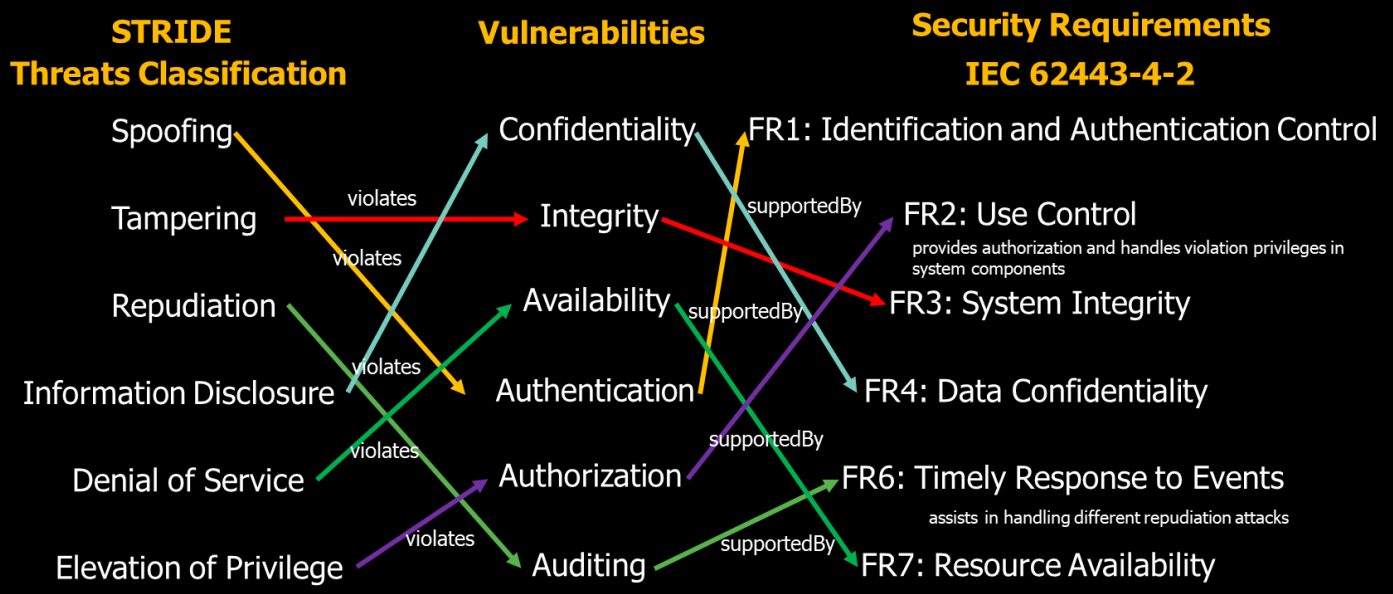
A Practical Approach to Adopting the IEC 62443 Standards (isa.org), accessed in February 2024.
Shaaban, Abdelkader Magdy, et al. "Ontology-based model for automotive security verification and validation." *Proceedings of the 21st International Conference on Information Integration and Web-based Applications & Services*. 2019.

Device Security

- The **IEC 62443-4-2** standard **defines** security requirements for four **component types**: **software applications** (**SAR**), **embedded devices** (**EDR**), **host devices** (**HDR**), and **network devices** (**NDR**).
- For each component type, seven **foundational requirements** (**FR**) are specified, covering aspects such as **identification and authentication control** (**IAC**), **use control** (**UC**), **system integrity** (**SI**), **data confidentiality** (**DC**), **restricted data flow** (**RDF**), **timely response to events** (**TRE**), and **resource availability** (**RA**).
- These definitions **assist asset owners** in **simplifying** technical **specifications** and **selecting products** aligned with their desired **security level**.
- Each **security level** (**SL**) is defined by distinct **foundational requirements** and **measurable criteria**, simplifying **comparison** and **implementation** processes.
- Security requirements are categorized based on their level of **capability**, known as **Security-Level Capability** (SL-C).
- This level indicates the security level that system units must meet without further measures.
- Additionally, each **security zone** and **conduit** has specific **Security Targets** (**ST**) that must be achieved.

A Practical Approach to Adopting the IEC 62443 Standards (isa.org), accessed on February 2024.
Shaaban, A.M., Jung, O., Fas Millan, M.A. (2022). Toward Applying the IEC 62443 in the UAS for Secure Civil Applications. In: Haber, P., Lampoltshammer, T.J., Leopold, H., Mayr, M. (eds) Data Science – Analytics and Applications. Springer Vieweg, Wiesbaden. https://doi.org/10.1007/978-3-658-36295-9_7

Mapping Threats, Vulnerabilities, and Security Requirements: A Comprehensive Analysis



Ship's e-Nav Service Display Device

Risk Assessment for Ship's e-Nav Service Display Device

[General specifications]

- Power Supply : 230 VAC, 50/60Hz
- Display UnQit : 26 in LCD display
- Main Control Unit
- OS : Windows 10
- Interfaces
- Multiple Ethernet LAN ports (1GB)
- Multiple serial ports (IEC 61162-1 & IEC 61162-2) (Out of our scope – we mainly focus on the IEC 62443-4-2)
- Multiple USB port
- CD/DVD-ROM : optional
- Keyboard, trackball mouse

[General functions]

- Display of e-Navigation service information.
- Elctronic chart display
- Display of AIS vessels

Juntae Kim, Sanghoon Choi, Jinho Yoo, and Kaemyoung Park, The analysis of general cybersecurity requirements applicable to ship's e-Nav service display device based on international standards, url: ENAV28-5.1.1.4-The-analysis-of-general-cybersecurity-requirements-applicable-to-ships-e-Nav.pdf (iala-aism.org)

Risk Assessment for Ship's e-Nav Service Display Device

Threat Index (TI)

TI	Category
5	Definite
4	Probable
3	Occasional
2	Remote
1	Improbable

Vulnerability Index (VI)

VI	Category
5	Very high
4	High
3	Medium
2	Low
1	Very low

Likelihood Index = Threat Index X Vulnerability Index

LI	Calculation
5	21 ≤ TI X VI ≤ 25
4	16 ≤ TI X VI ≤ 20
3	11 ≤ TI X VI ≤ 15
2	6 ≤ TI X VI ≤ 10
1	1 ≤ TI X VI ≤ 5

Impact Index (Iml)

Iml	Category
5	Critical
4	Significant
3	Moderate
2	Minor
1	Negligible

Cyber security Risk Index (RI) = TI x VI x Iml
= Likelihood Index (TI x VI) x Impact Index (Iml)

Juntae Kim, Sanghoon Choi, Jinho Yoo, and Kaemyoung Park, The analysis of general cybersecurity requirements applicable to ship's e-Nav service display device based on international standards, url: ENAV28-5.1.1.4-The-analysis-of-general-cybersecurity-requirements-applicable-to-ships-e-Nav.pdf (iala-aism.org)

Risk Assessment for Ship's e-Nav Service Display Device

Identified threats list

No.	Threat	No.	Threat
1	Malware	9	Man-in-the-middle attack
2	Brute force	10	Erroneous use or erroneous administration of devices
3	Denial of Service (DOS)	11	Careless use of removable media or device (USB, Laptop, etc)
4	Social engineering	12	OS vulnerabilities
5	Data breach	13	Application software vulnerabilities
6	Phishing	14	Hardware failure
7	Scanning	15	Credential stuffing
8	Network manipulation and information gathering	16	Subverting the supply chain

Juntae Kim, Sanghoon Choi, Jinho Yoo, and Kaemyoung Park, The analysis of general cybersecurity requirements applicable to ship's e-Nav service display device based on international standards, url: ENAV28-5.1.1.4-The-analysis-of-general-cybersecurity-requirements-applicable-to-ships-e-Nav.pdf (iala-aism.org)

Risk Assessment for Ship's e-Nav Service Display Device

No	Threats	Potential cause	Potential consequence	VI	TI	ImI	RI	Proposed controls	62443-4-2 requirements
1	Malware	1) Installation of unauthorized software 2) 2) Use of email or internet 3) 3) Use of USB	1) Malware infection 2) 2) System malfunction 3) 3) Service interruption 4) 4) Data loss	5	4	4	20	1) Protection from malicious code	IEC 62443-4-2 SAR 3.2 The application product supplier shall qualify and document which protection from malicious code mechanisms are compatible with the application and note any special configuration requirements. (SL1)
2	Brute force	1) Hacking attampt by attacker	1) Unauthorized access 2) Illegal system manipulation or parameter setting change 3) Confidential data leakage 4) Important data deletion	3	2	4	8	1) Strength of password-based authentication	IEC 62443-4-2 CR 1.7 For components that utilize password-based authentication, those components shall provide or integrate into a system that provides the capability to enforce configurable password strength according to internationally recognized and proven password guidelines. (SL1)
3	Denial of Service (DOS)	1) DDOS attack by attacker via network	1) Network disruption 2) Service interruption	3	2	4	8	1) Denial of service(DoS) protection 2) Resource management	IEC 62443-4-2 CR 7.1: Components shall provide the capability to maintain essential functions when operating in a degraded mode as the result of a DoS event. (SL1) IEC 62443-4-2 CR 7.2: Components shall provide the capability to limit the use of resources by security functions to protect against resource exhaustion. (SL1)

Juntae Kim, Sanghoon Choi, Jinho Yoo, and Kaemyoung Park, The analysis of general cybersecurity requirements applicable to ship's e-Nav service display device based on international standards, url: ENAV28-5.1.1.4-The-analysis-of-general-cybersecurity-requirements-applicable-to-ships-e-Nav.pdf (iala-aism.org)

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

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: Secure Network Architecture and Design
- Topic-2: Cryptographic Techniques for Ensuring Secure Data Transmission
- Topic-3: Security mechanisms, services, and attacks in OSI reference model

Agenda

01. Introduction

02. Overview

03. Symmetric Encryption

04. Asymmetric Encryption

05. Digital Signature

Introduction

Significance of Cryptography: The Korean Register (KR) underscores the critical role of cryptography in the safekeeping of data.

Objectives

The Korean Register outlines the **goals of type approval** for **maritime** cybersecurity.

Security Requirements

Details the specific **security requirements** needed and their respective **levels**.

Cryptography

Highlights the importance of **cryptography** in **securely** storing crucial **data**.

https://safety4sea.com/kr-explains-the-importance-of-cryptography-in-safekeeping-data/

Introduction

- **Maritime Cyber Security Type Approval**
  - This type of approval certifies manufacturers for **equipment intended** for use
  - The approval is granted based on the results of **examinations**, **tests**, and **inspections** as specified in the guidance.
  - Equipment must **meet** these before **installation** on **board** is **approved** by the society.

- KR notes that the use of cryptography is a **common requirement across security levels 1 to 4.**

- **Manufacturers** seeking **cybersecurity type approval** from the Korean Register must **demonstrate** that the encryption algorithms used in their systems/equipment are **secure** and **not vulnerable**.

•Use of cryptography: "If **cryptography** is required, the component should use **cryptographic security** mechanisms according to **internationally recognized** and **proven** security **practices** and **recommendations**" … Korean Register reports

Section 1 General	Section 5 Data Confidentiality	Section 9 Software Application Requirements
Sections 2 Identification and Authentication	Section 6 Restricted Data Flow	Section 10 Embedded Device Requirements
Section 3 Use Control	Section 7 Timely Response to Events	Section 11 Host Device Requirements
Section 4 System Integrity	Section 8 Resource Availability	Section 12 Network Device Requirements

https://safety4sea.com/kr-explains-the-importance-of-cryptography-in-safekeeping-data/
http://krs.westus.cloudapp.azure.com/Files/KRRules/KRRules2020/data/data_other/ENGLISH/gc31e000.pdf

Cryptography

- **Cryptography** is the field of applying **mathematical principles** to **encrypt** and **decrypt** data.
- It allows for the secure **storage** and **transmission** of sensitive **information**, **protecting** it from **unauthorized** access, **particularly** when traversing insecure **networks** such as the **Internet**.
- While cryptography **focuses** on **data security**, **cryptanalysis concentrates** on **analyzing** and **breaking** secure communication.
- Classical **cryptanalysis** involves a **combination** of **analytical reasoning**, **mathematical tools**, pattern **recognition**, patience, **determination**, and **sometimes** luck.
- Those **engaged** in cryptanalysis are often referred to as **attackers**.

Cryptography Academy, https://cryptographyacademy.com/introduction/, accessed in February 2024

Cryptography

- Cryptographic strength is assessed based on the **time** and **resources** needed to **decrypt** the plaintext.
- **Strong cryptography** produces **ciphertext** that is exceptionally **challenging** to **decipher** without employing the appropriate **decryption tool** or **method**.
- Even with the huge **computational power of modern computers**, including a billion computers performing a billion checks per **second**, **deciphering strong cryptography** would take longer than the **lifespan** of the universe.

Cryptography Academy, https://cryptographyacademy.com/introduction/, accessed in February 2024

History of Cryptography

- The origin of **cryptography** is linked to the **age** when **humans** started **writing**.
- As **civilizations** evolved, **societies** were organized into **tribes**, **groups**, and **kingdoms**.
- This resulted in the rise of concepts like **power**, **battles**, **supremacy**, and **politics**.
- These increased the need for **secret communication** among **individuals**.
- Cryptography evolved **continuously** to **meet** this demand for **covert communication**.
- The **roots** of **cryptography** are found in **Roman** and **Egyptian civilizations**.

History of Cryptography

- Scholars later transitioned to employing simple **mono-alphabetic substitution** ciphers around **500** to **600** BC.
- This method entailed **replacing letters** in a **message** with other **letters** according to a **secret rule**.
- The rule served as a key to **deciphering** the **message** from the **scrambled** text.
- The **ancient Roman cryptographic** technique, commonly referred to as the **Caesar Shift Cipher**, involves **shifting** the **letters** of a message by a **predetermined number** (often three).
- The **recipient** of the message would then **reverse** the **shift** by the **same number** to **retrieve** the original message.

History of Cryptography

Hieroglyph – The Oldest Cryptographic Technique

- The first known evidence of **cryptography** can be traced to the use of '**hieroglyph**'.
- Around **4000** years ago, the **Egyptians** communicated through **messages** written in **hieroglyphs**, a code kept **confidential** by **scribes** entrusted with **transmitting** messages for the **kings**.
- An example of such a **hieroglyph**.

https://www.tutorialspoint.com/cryptography/origin_of_cryptography.htm, accessed in February 2024

Features of Cryptography

Confidentiality

Data is **exclusively accessible** to its **intended recipient**, **preventing** access by any **unauthorized** individuals

Integrity

Data remains **unaltered** during **storage** or **transmission** between the **sender** and intended **recipient**, with any **modifications** being readily **detectable**

Non-repudiation

The **creator** or **sender** of data **cannot** disclaim their **intent** to **transmit** the **information** at a later stage

Authentication

The identities of **both** the **sender** and **receiver** are **verified**, along with the **confirmation** of the information's **source** and **destination**

https://www.tutorialspoint.com/cryptography/origin_of_cryptography.htm, accessed in February 2024

Types Of Cryptography

Symmetric Key Cryptography: In this encryption system, both the **sender** and **receiver** share a **single key** for **encrypting** and **decrypting** messages. While **Symmetric** Key Systems **offer speed** and **simplicity**, **securely** exchanging the **key** between the **sender** and **receiver** poses a challenge. Common **examples** of symmetric key cryptography systems include the **Data Encryption Standard** (**DES**) and the **Advanced Encryption Standard** (**AES**).

Hash Functions: This algorithm operates **without** any **key**. It computes a **fixed-length hash** value based on the **input plain text**, rendering it **impossible** to **retrieve** the original content from the hash. Hash **functions** are commonly employed in various **operating systems** for **password encryption** purposes.

Asymmetric Key Cryptography: In this system, a **pair of keys** is employed to **encrypt** and **decrypt** data. The **receiver's public** key is utilized for **encryption**, while their **private** key is employed for **decryption**. The **public** and **private** keys are **distinct**. Even if the **public** key is **widely known**, only the intended **recipient**, who **possesses** the **private key**, can **decode** the **message**. The **RSA** algorithm is **one** of the most **well-known asymmetric** key **cryptography algorithms**.

Cryptography and its Types – GeeksforGeeks, accessed in February 2024

Symmetric Encryption

Symmetric Encryption

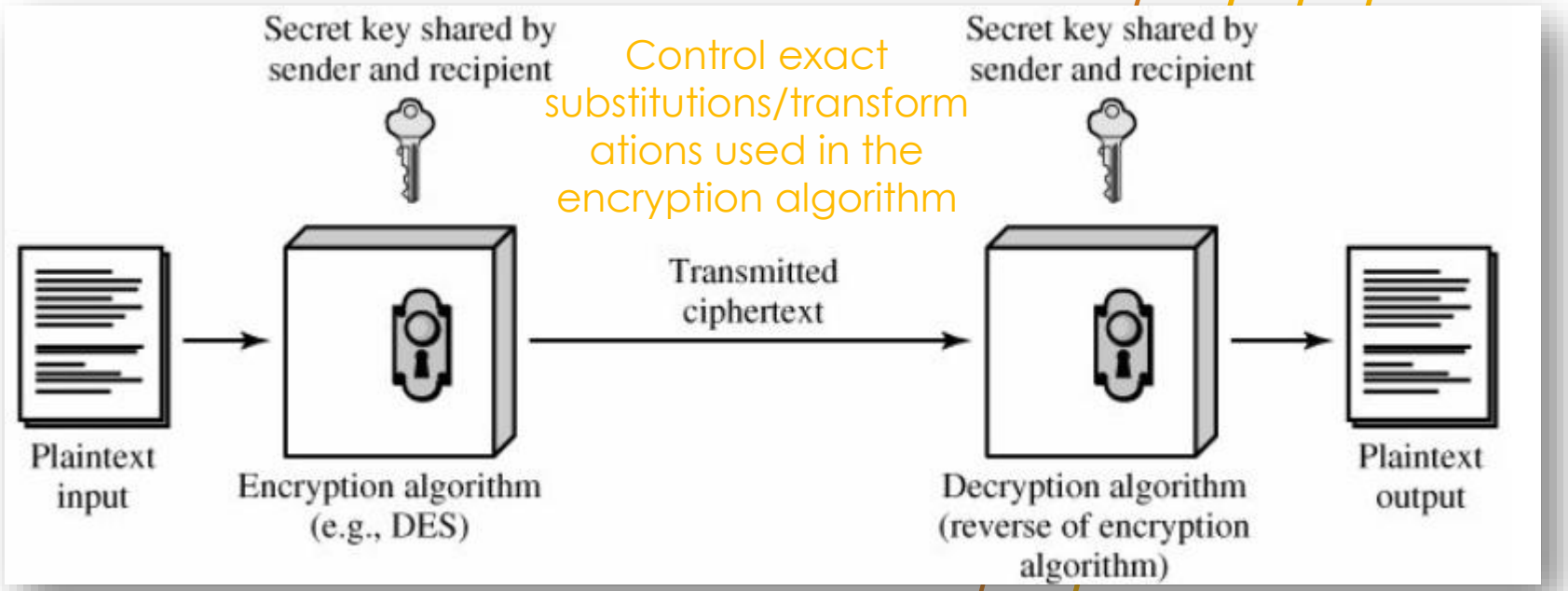
- Symmetric **encryption**, also called **conventional** or **single-key** encryption, was the only type of **encryption** in use prior to the **development** of **public-key** encryption in the **1970s**.
- It **remains** the **more widely** used **encryption** method.
- **Symmetric encryption** employs a **single key** for both **encryption** and **decryption**.
- This key is **shared** between the **sender** and **receiver**.
- Both **parties** can **encrypt** or **decrypt** messages using the **same key**.

Some Basic Terminology

- **Plaintext** - original message
- **Ciphertext** - coded message
- **Cipher** - algorithm for **transforming plaintext** to **ciphertext**
- **Key** - **info used** in cipher known only to **sender/receiver**
- **Encipher (Encrypt)** - converting **plaintext** to **ciphertext**
- **Decipher (Decrypt)** - recovering **ciphertext** from plaintext
- **Cryptography** - study of encryption **principles/methods**
- **Cryptanalysis (Codebreaking)** - study of **principles/ methods** of **deciphering** ciphertext ***without*** knowing key
- **Cryptology** - field of **both cryptography** and **cryptanalysis**

Symmetric Cipher Model

original message



original message

Performs substitutions/transfor mations on plaintext

Performs an inverse action of the encryption algorithm

Main Requirements

- We assume that it is **impractical** to **decrypt** a message on the basis of the **cipher text** plus knowledge of the **encryption/decryption algorithm** and do not need to keep the **algorithm secret**; rather, we only need to keep the **key secret**.
- This feature of **symmetric encryption** is what makes it **feasible** for **widespread use**. It allows easy **distribution** of s/w and h/w implementations.
- two requirements for secure use of symmetric encryption:
- a **strong** encryption algorithm
- a **secret** key known only to **sender/receiver**
- **mathematically** have:

  $Y = E_K(X)$

  $X = D_K(Y)$
- It can be considered a pair of functions with **plaintext X**, **ciphertext Y**, **key K**, **encryption algorithm EK**, and **decryption algorithm DK**.

Cryptography Dimensions

1. **The type of operations used for transforming plaintext to ciphertext**:

- **Encryption algorithms** rely on two main principles: substitution and transposition.
  - **Substitution** involves **mapping** each element in the **plaintext** (i.e., **bit**, **letter**, **group of bits**, or **letters**) to another element.
  - **Transposition** **rearranges** elements within the **plaintext**.
- The **primary requirement** is to ensure **reversibility**, meaning no information **loss**.
- Most **systems**, known as product **systems**, incorporate multiple **stages** of **substitutions** and **transpositions**.

Cryptography Dimensions

2. The number of keys used

- When both **sender** and **receiver** utilize the **same** key, it's called **symmetric**, **single-key**, or **conventional** encryption.
- If the **sender** and **receiver** use **different keys**, it's termed **asymmetric** or **public-key encryption**.

3. The way in which the plaintext is processed

- A **block cipher** operates on **input blocks**, generating an **output block** for each **input block**.
- In contrast, a **stream cipher** processes **input elements continuously**, producing **output one element** at a time.

Cryptanalysis and Brute-force Attack

Typically, the objective is to **recover** the key in use rather than simply to **recover** the plaintext of a single ciphertext.

There are two general approaches:

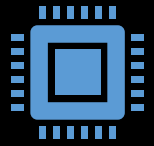
Cryptanalytic attacks rely on the **nature** of the **algorithm** plus perhaps some **knowledge** of the **general characteristics** of the **plaintext** or even some sample **plaintext-ciphertext** pairs.

Brute-force attacks try **every possible key** on a piece of ciphertext until an **intelligible translation** into plaintext is obtained. On average, half of **all possible keys** must be **tried** to achieve success.

Cryptanalysis and Brute-force Attack

Types of **Attacks** on **Encrypted** Messages

Ciphertext only



- Encryption algorithm
- Ciphertext

Known plaintext

- Encryption algorithm
- Ciphertext
- One or more plaintext-ciphertext pairs formed with the secret key

Chosen plaintext

- Encryption algorithm
- Ciphertext
- Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key

Chosen ciphertext

- Encryption algorithm
- Ciphertext
- Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

Chosen text

- Encryption algorithm
- Ciphertext
- Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
- Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

Cryptanalysis and Brute-force Attack

Two additional definitions of **encryption** schemes are **either** they take **too long** or are **too expensive** to break the cipher.

Unconditionally secure

No matter how **much computer power** or **time** is available, the cipher cannot be **broken since** the **ciphertext provides insufficient** information to uniquely **determine** the **corresponding** plaintext

Computationally secure

Given **limited computing resources** (e.g., the **time needed** for calculations is greater than the age of the universe), the cipher cannot be broken.

Brute Force Search

Always possible to simply **try every key**

Most basic attack, **proportional to key size**

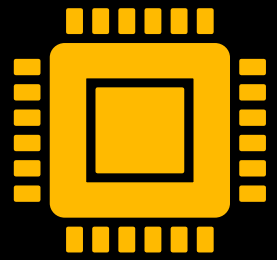
Assume either know/**recognise** plaintext

Key Size (bits)	Number of Alternative Keys	Time required at 1 decryption/μs	Time required at 10^6 decryptions/μs
32	$2^{32} = 4.3 \times 10^9$	2^{31} μs = 35.8 minutes	**2.15 milliseconds**
56	$2^{56} = 7.2 \times 10^{16}$	2^{55} μs = 1142 years	**10.01 hours**
128	$2^{128} = 3.4 \times 10^{38}$	2^{127} μs = 5.4×10^{24} years	**5.4×10^{18} years**
168	$2^{168} = 3.7 \times 10^{50}$	2^{167} μs = 5.9×10^{36} years	**5.9×10^{30} years**
26 characters (permutation)	$26! = 4 \times 10^{26}$	2×10^{26} μs = 6.4×10^{12} years	**6.4×10^6 years**

Substitution Techniques

Classical Substitution Ciphers

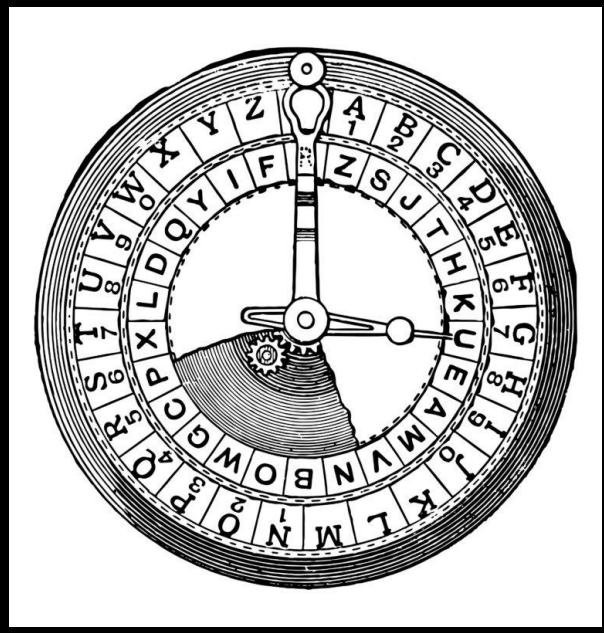
where letters of **plaintext** are **replaced** by other **letters** or by **numbers** or symbols



or if **plaintext** is viewed as a **sequence** of **bits**, then **substitution** involves **replacing plaintext** bit patterns with **ciphertext** bit **patterns**

Caesar Cipher

- The **Caesar Cipher** is one of the **earliest** encryption techniques, **attributed** to **Gaius Julius Caesar**, involving **replacing** each letter in a text with **another** letter a **fixed number** of **positions** down the alphabet.
- For instance, shifting each letter by "**1**" would change **A** to **B** and **B** to **C**.
- Traditionally, the shift value is **3**, but any number of **shifts** can be applied.
- **Decryption** involves **reversing** the shift by the **same number of positions**.
- While the **Caesar Cipher** is not considered **strong encryption** due to its ease of **decoding**, it remains a part **of more complex encryption methods**.
- Despite its simplicity, this encryption was **valuable** during **Caesar's military campaigns**, preventing intercepted messages from **being** easily understood by **adversaries**.



What is a Caesar Cipher? | IT Wiki | GateKeeper Proximity Passwordless 2FA Solution (gkaccess.com)

Caesar Cipher

- Can define transformation as:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

- Mathematically give each letter a number

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

- Then have Caesar cipher as:

  $c = E(p) = (p + k) \bmod (26)$

  $p = D(c) = (c - k) \bmod (26)$

plaintext letter p, substitute the ciphertext letter C, k takes on a value in the range 1 to 25

Monoalphabetic Techniques

Monoalphabetic Cipher Security

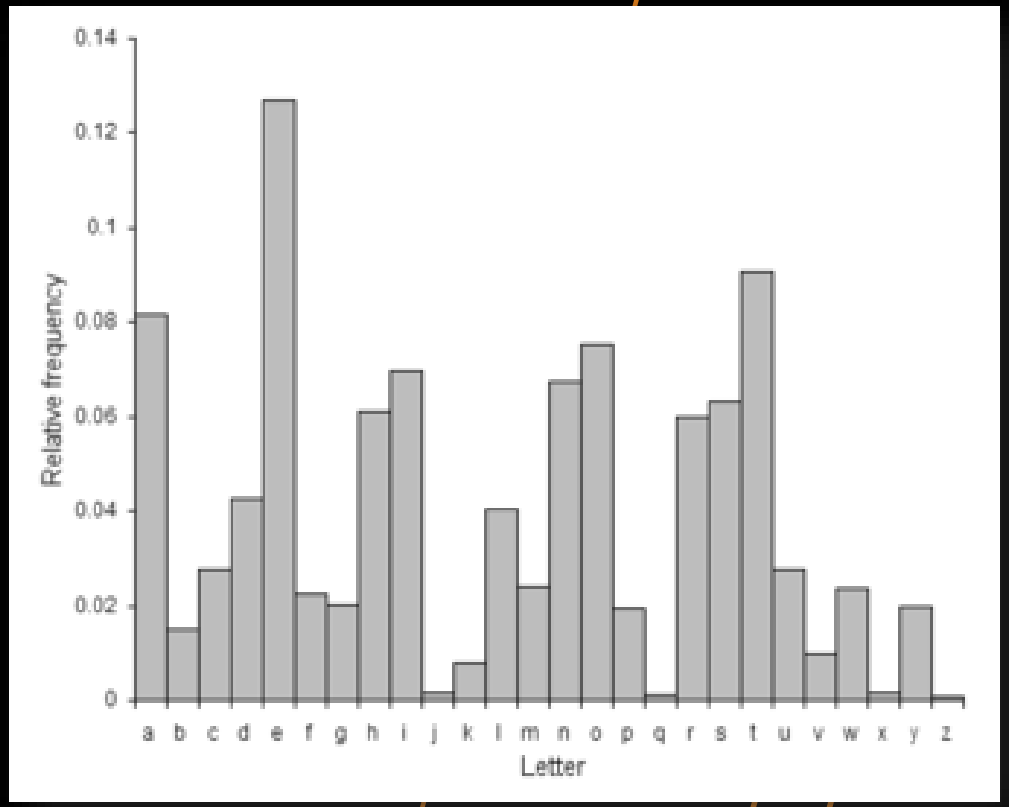
- Rather than just **shifting** the alphabet
- Could **shuffle** (jumble) the **letters arbitrarily**
- Each **plaintext letter** maps to a **different** random ciphertext letter
- Hence key is 26 letters long

Plain	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Cipher	D	K	V	Q	F	I	B	J	W	P	E	S	C	X	H	T	M	Y	A	U	O	L	R	G	Z	N

Plaintext: if we wish to replace letters
Ciphertext: WI RF RWAJ UH YFTSDVF SFUUFYA

Monoalphabetic Cipher Security

- The "cipher" line can be any **permutation** of the **26** alphabetic characters, then there are **26!** or **greater than 4 x 10^{26}** possible keys.
- With so **many keys**, might think is secure
- but it would be **!!!WRONG!!!**



- The problem is language **characteristics**
- We don't actually need all the **letters** in order to understand written ***English text***.
- Human languages are **redundant**
- In English **E** is by far the most **common letter**
  - followed by **T**, **R**, **N**, **I**, **O**, **A**, **S**
- Other letters like **Z**, **J**, **K**, **Q**, **X** are fairly rare

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

Example Cryptanalysis

Given ciphertext:

```
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMET
SXAIZVUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZ
UHSXEPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
```

- Count relative letter frequencies

P 13.33	H 5.83	F 3.33	B 1.67	C 0.00
Z 11.67	D 5.00	W 3.33	G 1.67	K 0.00
S 8.33	E 5.00	Q 2.50	Y 1.67	L 0.00
U 8.33	V 4.17	T 2.50	I 0.83	N 0.00
O 7.50	X 4.17	A 1.67	J 0.83	R 0.00
M 6.67				

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
2	2	0	6	6	4	2	7	1	1	0	0	8	0	9	16	3	0	10	3	0	5	4	5	2	14

- Guess **P** & **Z** are **e** and **t**
- Guess **ZW** is **th** and hence **ZWP** is **the**
- Proceeding with trial and error finally get:

```
it was disclosed yesterday that several informal
but direct contacts have been made with political
representatives of the viet cong in moscow
```

Other Techniques

01. Playfair Cipher

02. Hill Cipher

03. Polyalphabetic Ciphers

04. One-Time Pad

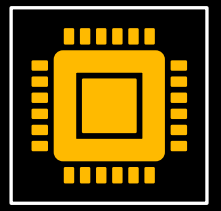
Transposition Ciphers

Transposition Ciphers

Previously discussed techniques examined so far involve the **substitution** of a **ciphertext** symbol for a plaintext symbol.

A very **different kind** of mapping is achieved by performing some sort of **permutation** on the **plaintext** letters.

This technique is referred to as a **transposition** cipher and forms the **second** basic **building** block of ciphers.



The core idea is to **rearrange** the order of basic units (**letters**/**bytes**/**bits**) without **altering** their actual values.

Rail Fence Cipher

- The **rail fence** technique is one of the **simplest** transposition ciphers used for **encryption**.
- In this **method**, the plaintext **message** is arranged in a **zigzag pattern** across multiple "**rails**" or **rows**.
- For instance, to encrypt the message "**meet me after the toga party**" using a rail **fence depth** of **2**, the plaintext is written **diagonally** across two rows.

```
m e m a t r h t g p r y
e t e f e t e o a a t
```

- The encrypted ciphertext is then formed by reading the characters **row** by **row**.
- This technique provides a **basic level** of encryption but may **not** be secure against **advanced cryptanalysis methods**.

MEMATRHTGPRYETEFETEOAAT

Row Transposition Ciphers

- A more complex method **involves arranging** the message in a **rectangular grid**, filling it **row** by **row**.
- The ciphertext is then **generated** by **reading** the **grid column** by **column**, with the order of **columns** altered according to a **predetermined** key.
- Example
  - Plain text: Attack postponed until two am

```
Key 3 4 2 1 5 6 7
```

```
Column number: 1 2 3 4 5 6 7
Plaintext:     a t t a c k p
               o s t p o n e
               d u n t i l t
               w o a m x y z
```

```
Key:           3 4 2 1 5 6 7
Plaintext:     t a t a c k p
               t p s o o n e
               n t u d i l t
               a m o w x y z
```

- then reorder the columns **according** to some key **before reading off** the rows
  - Ciphertext: **TTNAAPTMTSUOAODWCOIXKNLYPETZ**

Rotor Machines

Rotor Machines

- Before modern **ciphers**, **rotor machines** were most common **complex ciphers** in use
- Widely used in **WW2**

German Enigma

Source: Enigma machine - Wikipedia

Allied Hagelin

Source: Hagelin BC-543 (cryptomuseum.com)

Japanese Purple

Secrets Abroad: A History of the Japanese Purple Machine - Wonders & Marvels (wondersandmarvels.com)

- Implemented a very complex, varying **substitution** cipher
- Used a series of **cylinders**, each giving one **substitution**, which **rotated** and **changed** after each letter was encrypted
- With 3 cylinders have **26^3=17576** alphabets

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

Claude Shannon and Substitution-Permutation Ciphers

- Claude **Shannon** introduced idea of **substitution-permutation** (S-P) networks in **1949** paper
- form basis of modern **block ciphers**
- **S-P** nets are based on the two primitive **cryptographic operations** seen before:
  - ***substitution*** (S-box)
  - ***permutation*** (P-box)
- provide ***confusion*** & ***diffusion*** of message & key

Confusion and Diffusion

- The terms **diffusion** and **confusion** were introduced by Claude Shannon to capture the **two basic building blocks** for any cryptographic system.
- Every **block** cipher involves a transformation of a **block of plaintext** into a **block of ciphertext**, where the transformation depends on the key.
- The **mechanism of diffusion** seeks to make the **statistical relationship** between the **plaintext** and **ciphertext** as **complex** as possible in order to **thwart attempts** to deduce the key.
- Confusion seeks to make the relationship between the **statistics** of the **ciphertext** and the value of the **encryption key** as **complex as possible**, again to **thwart attempts to discover the key**.
- So successful are **diffusion** and **confusion** in capturing the essence of the desired attributes of a block cipher that they have become the **cornerstone** of modern block cipher design.

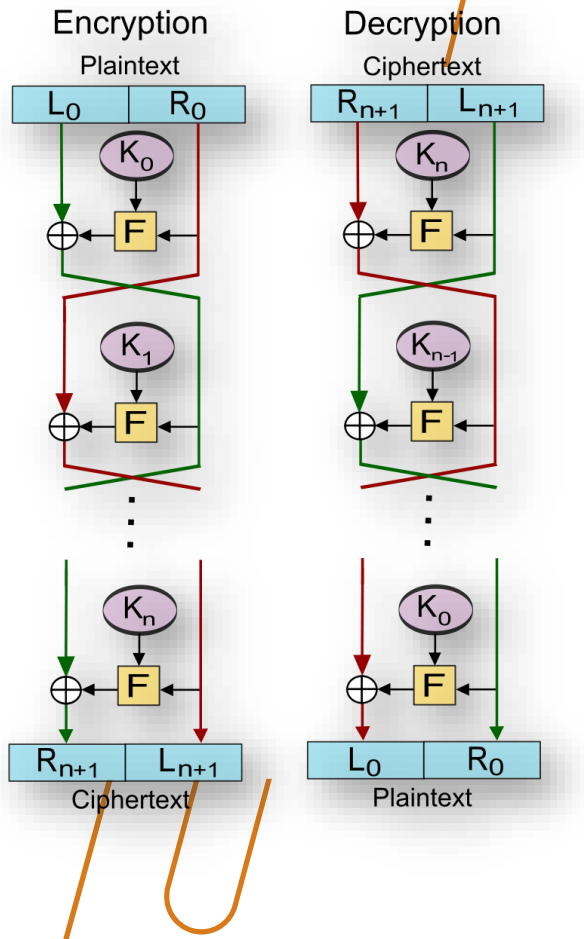
Feistel Cipher Structure

- Horst Feistel, working at **IBM Thomas J Watson Research Labs**, devised a suitable **invertible cipher structure** in the early 70's.
- One of Feistel's main contributions was the **invention** of a **suitable structure** that adapted **Shannon's S-P** network in an easily inverted structure.
- It **partitions** the **input block** into **two halves**, which are processed **through multiple rounds** that perform a **substitution** on the **left data half**, based on the **round function** of the **right half** & **subkey**, and then have **permutation swapping halves**.
- Essentially the same **h/w** or **s/w** is used for **both encryption** and **decryption**, with just a **slight change** in how the **keys are used**.
- One layer of **S-boxes** and the following **P-box** are used to form the round function.

Feistel Cipher Encryption/Decryption

The exact realization of a Feistel network depends on the choice of the following parameters and design features:

- **block size** - increasing size improves security but slows cipher
- **key size** - increasing size improves security, makes exhaustive key searching harder, but may slow cipher
- **number of rounds** - increasing the number improves security, but slows cipher
- **subkey generation** algorithm - greater complexity can make analysis harder, but slows cipher
- **round function** - greater complexity can make analysis harder, but slows cipher
- **fast software en/decryption -** more recent concern for practical use
- **ease of analysis - for easier validation &** testing of strength



DES Algorithm – Symmetric Cipher

DES Decryption

The **Data Encryption Standard** (**DES**) is a block cipher widely used for **data security**, characterized by a **56-bit** key length.

Despite its historical significance, **DES** has faced increasing vulnerabilities to **powerful attacks over time**.

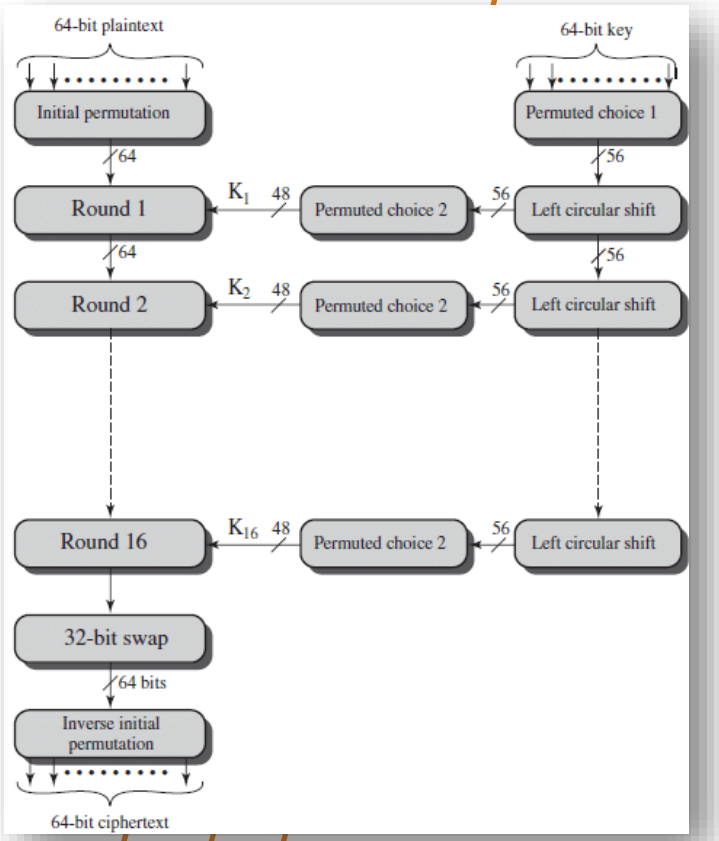
Consequently, the popularity of **DES** has declined due to these security concerns.

DES operates by encrypting data in blocks of **64 bits** each, meaning that **64 bits** of **plaintext** are inputted to produce **64** bits of ciphertext.

Both **encryption** and **decryption** processes in DES utilize the same **algorithm** and **key**, with **minor** differences.

The key length in DES is fixed at **56 bits**.

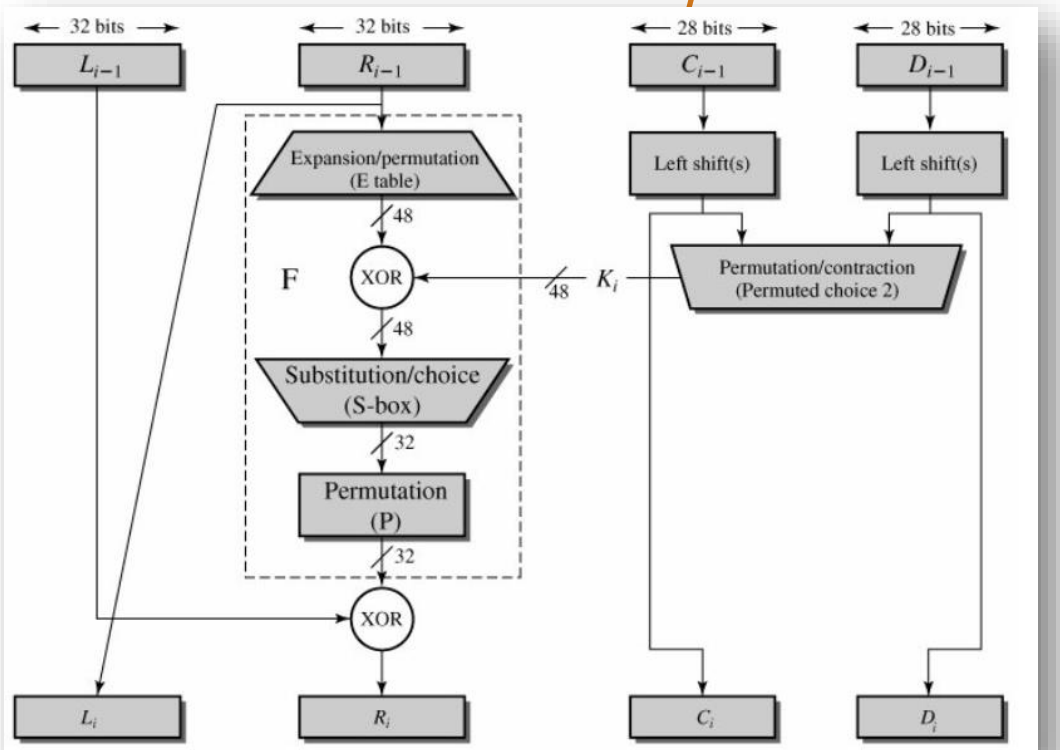
The function expects a **64-bit** key as input. However, only **56** of these bits are ever used; the other 8 bits can be used as parity bits or simply set arbitrarily



William Stallings, Cryptography and Network Security: Principles and Practice, Fifth Edition
Data encryption standard (DES) | Set 1 – GeeksforGeeks, accessed in February 2024.

DES Round Structure

- uses two **32-bit L & R** halves
- as for any Feistel cipher can describe as:
- $L_i = R_{i-1}$
- $R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$
  - F takes **32-bit R** half and **48-bit subkey**:
- expands **R** to **48-bits** using perm E
- adds to subkey using **XOR**
- passes through **8 S-boxes** to get **32-bit** result
- finally permutes using **32-bit** perm P



Strength of DES – Key Size

- **56-bit** keys have **2^{56} = 7.2 x 10^{16} values**
- **Brute force** search looks hard
- However **DES** was finally and definitively proved **insecure** in **July 1998**, when the **Electronic Frontier Foundation** (**EFF**) announced that it had broken a DES encryption using a special-purpose "**DES cracker**" machine that was built for less than **$250,000**.
- The attack took **less than three days**.
- We must clearly consider **alternatives** to **DES**, the most important of which are **AES** and **triple DES**.

DES vs Triple DES (3DES)

- **Triple DES** (**TDES** or **3DES**) is an encryption algorithm that applies the **Data Encryption Standard** (**DES**) cipher **three times** successively to encrypt data.
- While DES performs encryption in **16** rounds for each **data block**, **3DES increases** the number of rounds to **48**, enhancing its cryptographic strength.
- Despite being somewhat **stronger** than **DES**, **3DES** has demonstrated **vulnerabilities** in **securing** data transmissions.
- Due to its **susceptibility** to **brute force attacks**, the **National Institute of Standards and Technology** (**NIST**) has **officially prohibited** the use of **3DES beyond 2023**.
- As a result, the **cryptography community** has shifted its **focus** towards the **Advanced Encryption Standard** (**AES**) as a more secure **alternative** to **3DES**.

What Is DES Encryption? A Look at the DES Algorithm - InfoSec Insights (sectigostore.com), accessed in February 2024

Asymmetric Encryption

What is Asymmetric Encryption?

- **Asymmetric encryption**, or **public-key cryptography**, utilizes **two keys** – a **public key**, **shared openly**, and a **private key**, **kept secret.** This method allows for **secure data transmission** without a **shared secret key**.
- The **sender employs** the recipient's **public key** to **encrypt the data**, while the recipient uses their **private key** for **decryption**, ensuring secure communication.
- **Unlike** symmetric encryption, which requires the **exchange of secret keys**, **asymmetric encryption eliminates this need**, simplifying the process, especially in **multi-party** communication.
- Additionally, **asymmetric encryption enables** the **creation** of **digital signatures**, crucial for **verifying data authenticity**.
- Common applications of asymmetric encryption include **secure online communication**, **digital signatures**, and **secure data transfer**.
- Examples of asymmetric encryption algorithms include **RSA**, **Diffie-Hellman**, and **Elliptic Curve Cryptography** (**ECC**).

What is Asymmetric Encryption? – GeeksforGeeks, accessed in February 2024

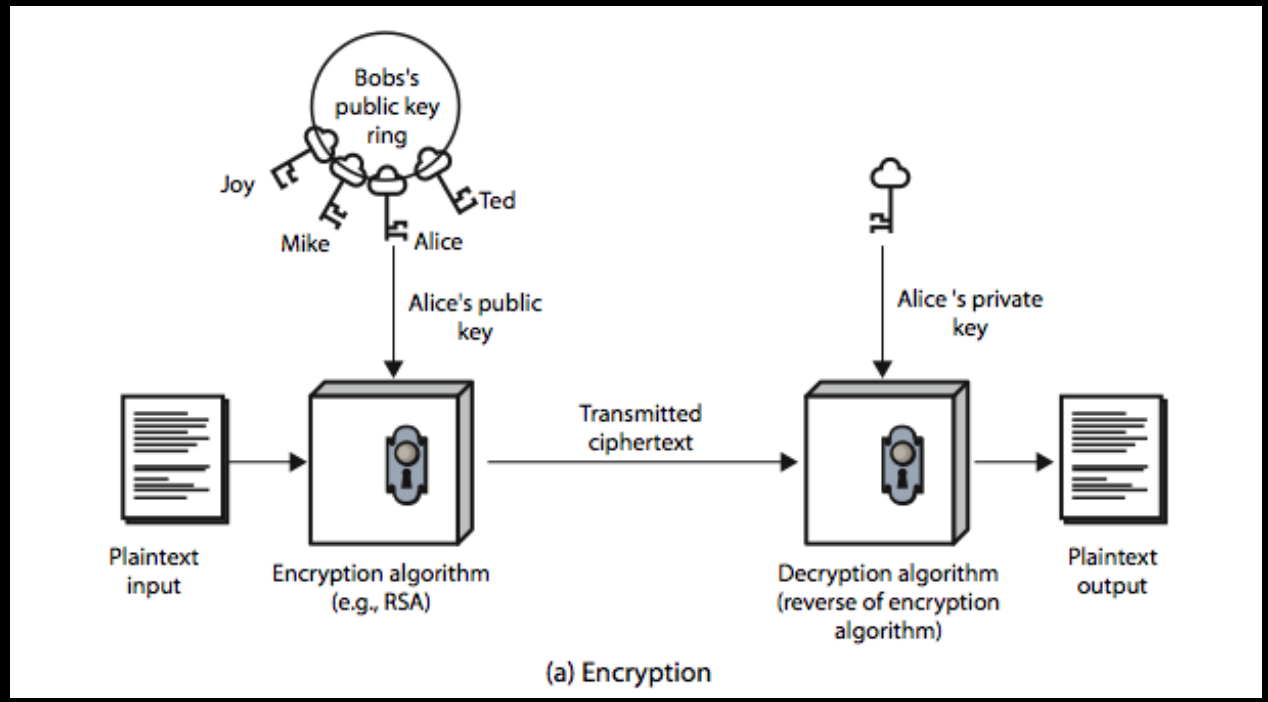
Advantages of Asymmetric Encryption

- **Enhanced Security**: **Unlike symmetric encryption**, where **one key** is used for both **encryption** and **decryption**, asymmetric encryption utilizes **different keys** for each process. The **private key,** used for **decryption**, **remains secret**, making it **challenging for attackers** to **intercept** and **decrypt data**.
- **Authentication**: **Asymmetric encryption** facilitates **authentication** by allowing the **receiver** to verify the **sender's identity**. The **sender encrypts** a **message with their private key,** which can only be decrypted using their **public key. Successful decryption confirms** the **sender's identity**.
- **Non-repudiation**: Asymmetric encryption **ensures non-repudiation**, preventing the **sender** from **denying sending a message** or **altering** its content. **Messages encrypted** with the **sender's private key** can only be **decrypted with their public key**, providing assurance of the sender's identity and message integrity.
- **Key Distribution**: Unlike **symmetric encryption**, which requires a secure **key distribution** system, **asymmetric encryption** eliminates this need. The public key can be **openly shared**, while the **private key remains** secret, simplifying key management.
- **Versatility**: Asymmetric encryption finds applications in various **fields**, including secure **email communication**, **online banking transactions**, **e-commerce**, and securing SSL/TSL connections for **internet traffic**.

What is Asymmetric Encryption? – GeeksforGeeks, accessed in February 2024

Public-Key Cryptography

A public-key encryption scheme has six ingredients: plaintext, encryption algorithm, public & private keys, ciphertext & decryption algorithm.



Public-Key Applications

Can classify uses into 3 categories:

- **Encryption/decryption:** The sender **encrypts** a message with the **recipient's public key**.
- **Digital Signatures:** The sender "**signs**" a message with its **private key**, either to the **whole message** or to a **small block** of **data** that is a function of the message.
- **Key Exchange:** Two sides cooperate to exchange a **session key**. Several different approaches are possible involving the **private** key(s) of **one** or **both** parties.

Some **algorithms** are suitable for all **three applications**, whereas others can be used only for one or two of these applications.

Security of Public Key Schemes

- Like **private key** schemes brute force **exhaustive search** attack is always theoretically possible
- But keys used are **too large** (>**512bits**)
- Security relies on a **large enough** difference in difficulty between **easy** (**en/decrypt**) and **hard** (**cryptanalysis**) problems
- More generally the **hard** problem is known, but is made hard enough to be **impractical** to break
- Requires the use of **very large numbers**
- Hence is **slow** compared to **private key schemes**

RSA Algorithm – Asymmetric Cipher

RSA

- RSA is the best known, and by far the most widely used **general public key encryption algorithm**, and was first published by **Rivest**, **Shamir** & **Adleman** of **MIT** in **1978**.
- Since that time, RSA has reigned supreme as the **most widely accepted** and implemented **general-purpose** approach to **public-key encryption**.
- Uses large integers (eg. **1024** bits).
- Its security is due to the cost of factoring large numbers.
- **Prime Numbers** play an essential role in **RSA**.
- If we have the number **30**, which numbers can be multiplied to give the same result?
  - 15 x 2
  - 3 x 10
  - 5 x 6
  - So we have multiple options to reach 30.
- However, if I repeat the same question with **35**.
- **5 x 7** is the only answer, according to "**A prime number is a natural number greater than 1 that has no positive integer divisors other than 1 and itself**."

Prime Numbers | Brilliant Math & Science Wiki, accessed in February 2024
William Stallings, Cryptography and Network Security: Principles and Practice, Fifth Edition

RSA Idea

- The **RSA encryption scheme** is founded on the challenge of **factoring large integers**, making it hard to **decipher**.
- Public keys in **RSA** comprise **two numbers**, one of which is the product of **two large prime numbers**, while the **private key** is derived from the **same primes**.
- Security in RSA hinges on the difficulty of factoring the large number, ensuring **private key protection**.
- Encryption strength is **directly proportional** to the **key size**, with **doubling** or **tripling** exponentially **increasing** encryption **robustness**.
- RSA keys are typically **1024** or **2048** bits in length, with concerns over the **vulnerability** of **1024-bit** keys in the future.
- Despite **experts' predictions**, breaking **1024-bit keys** remains an **unfeasible** task at present.

RSA Algorithm in Cryptography – GeeksforGeeks, accessed in February 2024

The Crucial Roles of RSA in Internet Security

- RSA plays two crucial roles in today's internet.
  - Firstly, it's used in over **90% of internet connections** during the **SSL handshake**, which initiates secure communication.
  - This handshake is a key moment where an **attack** could **jeopardize** the **entire session**, potentially **exposing** sensitive **information** such as **personal data**, **financial records**, and **intellectual property**.
  - Another critical function of RSA is generating cryptographic **digital signatures**. These signatures are used for various purposes, such as **authenticating emails**, **documents**, and **software updates**. When a **file** or **program** is **digitally signed**, it is trusted by **computers** and **mobile** devices. Failure at this point could lead to serious consequences.

RSA Is Dead — We Just Haven't Accepted It Yet (forbes.com), accessed in February 2024

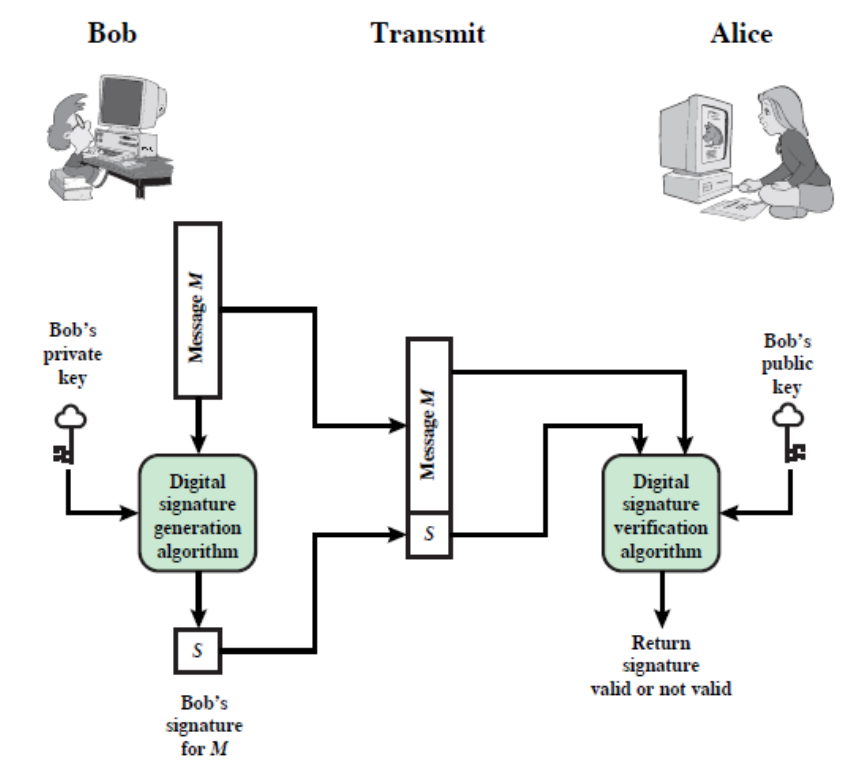
Digital Signature

Digital Signature

- The most important development from the work on public-key cryptography is the digital signature.
- A digital signature is **analogous to a handwritten** signature and provides a set of **security capabilities** that would be difficult to implement in any other way.
- A **digital signature** serves as an **authentication** method, allowing the message creator to **attach a code functioning as a signature**.
- It is generated by hashing the message and then encrypting it with the **creator's private key**.
- The signature **ensures** the message's **source** and **integrity**.

Digital Signature Model

- Bob can generate a **digital signature** for a message using an algorithm.
- This process involves **Bob's private key** and the message as **inputs**.
- Other users, like **Alice**, can verify the **signature**.
- Verification requires the **message**, **signature**, and **Bob's public key** as **inputs**.



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

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

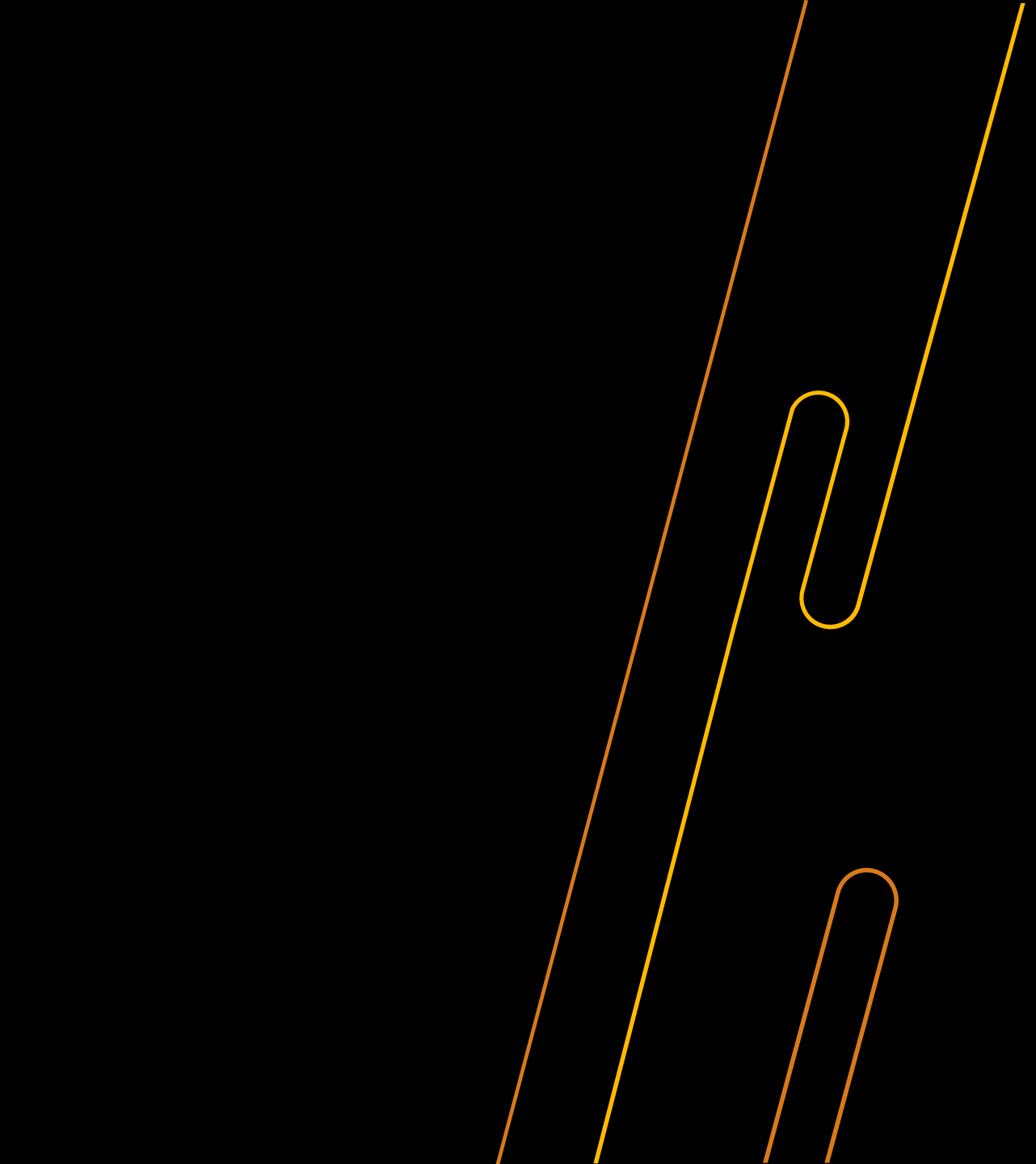
The OSI (open systems interconnection) security architecture provides a structured framework for addressing security concerns.

- **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

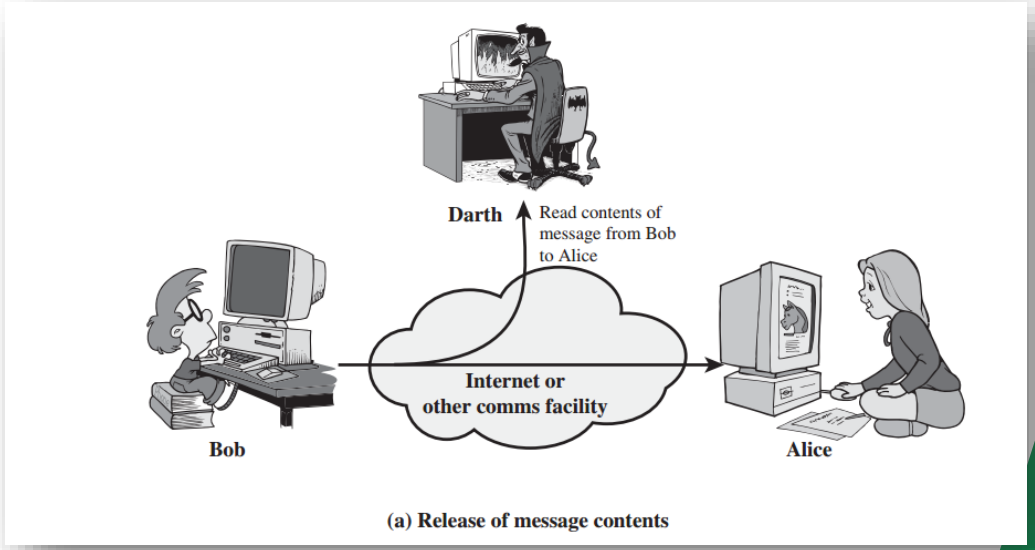


Security Attacks

- 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.

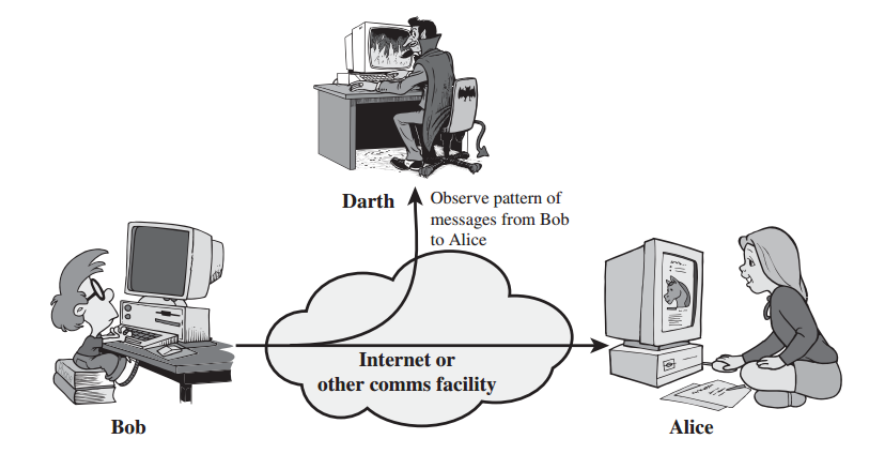


(a) Release of message contents

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

Active Attacks

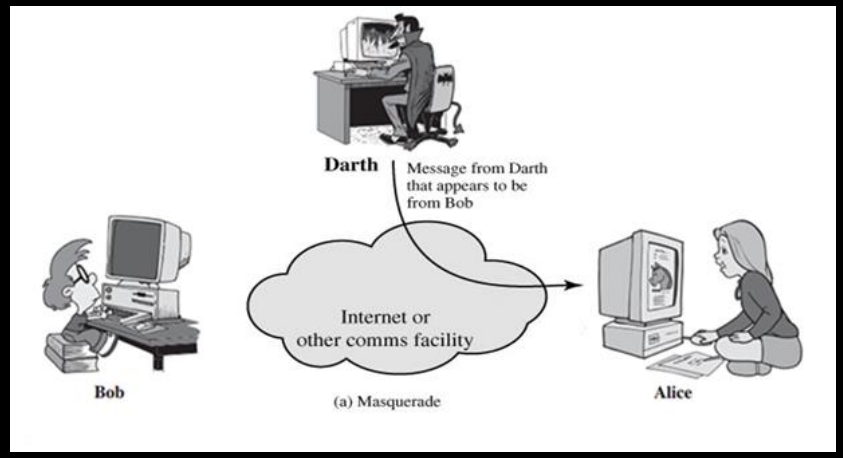
- "**Active attacks**" which attempt to **alter system resources** or **affect their operation**.
  - By modification of data stream to:
    - **masquerade** of one entity as some other
    - replay previous messages
    - modify messages in transit
    - denial of service
  - Active attacks present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



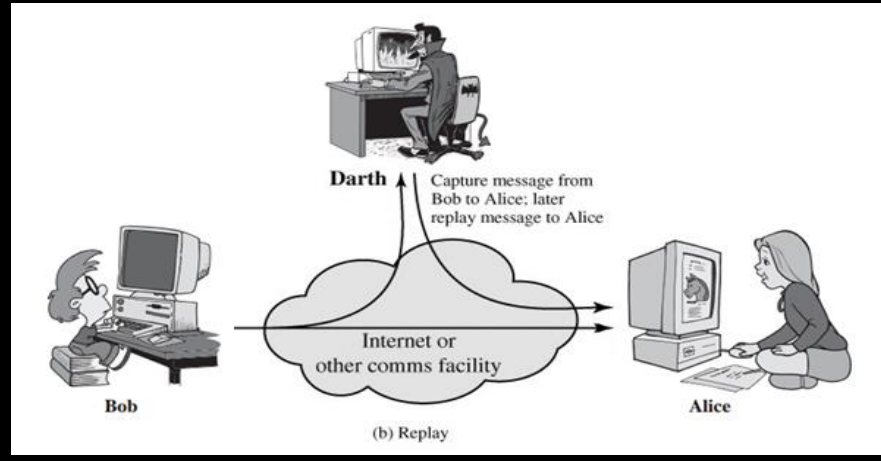
- It is quite difficult to prevent active attacks absolutely, because of the wide variety of **potential physical**, **software**, and **network vulnerabilities**.
- The goal is to **detect active attacks** and to **recover** from any disruption or delays caused by them.

Examples on Active Attacks

Masquerade

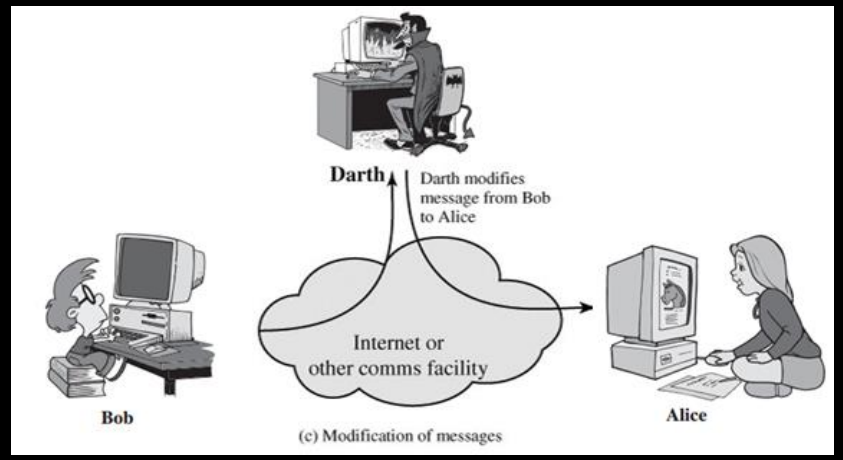


Replay

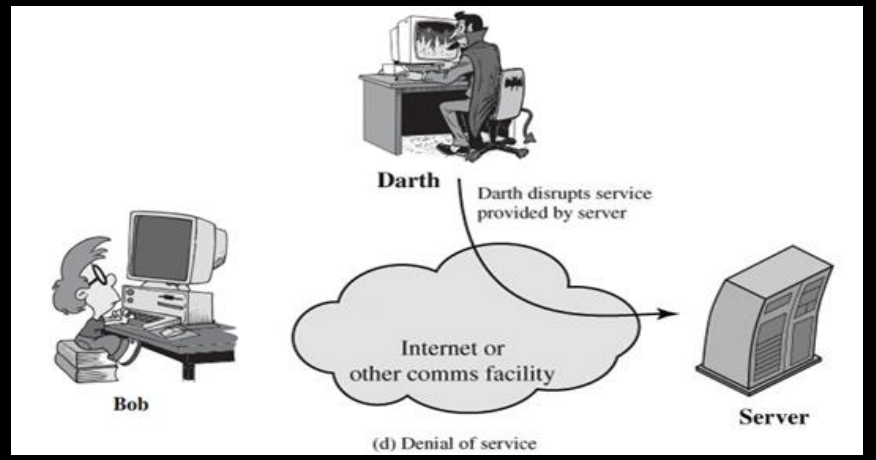


Examples on Active Attacks

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)

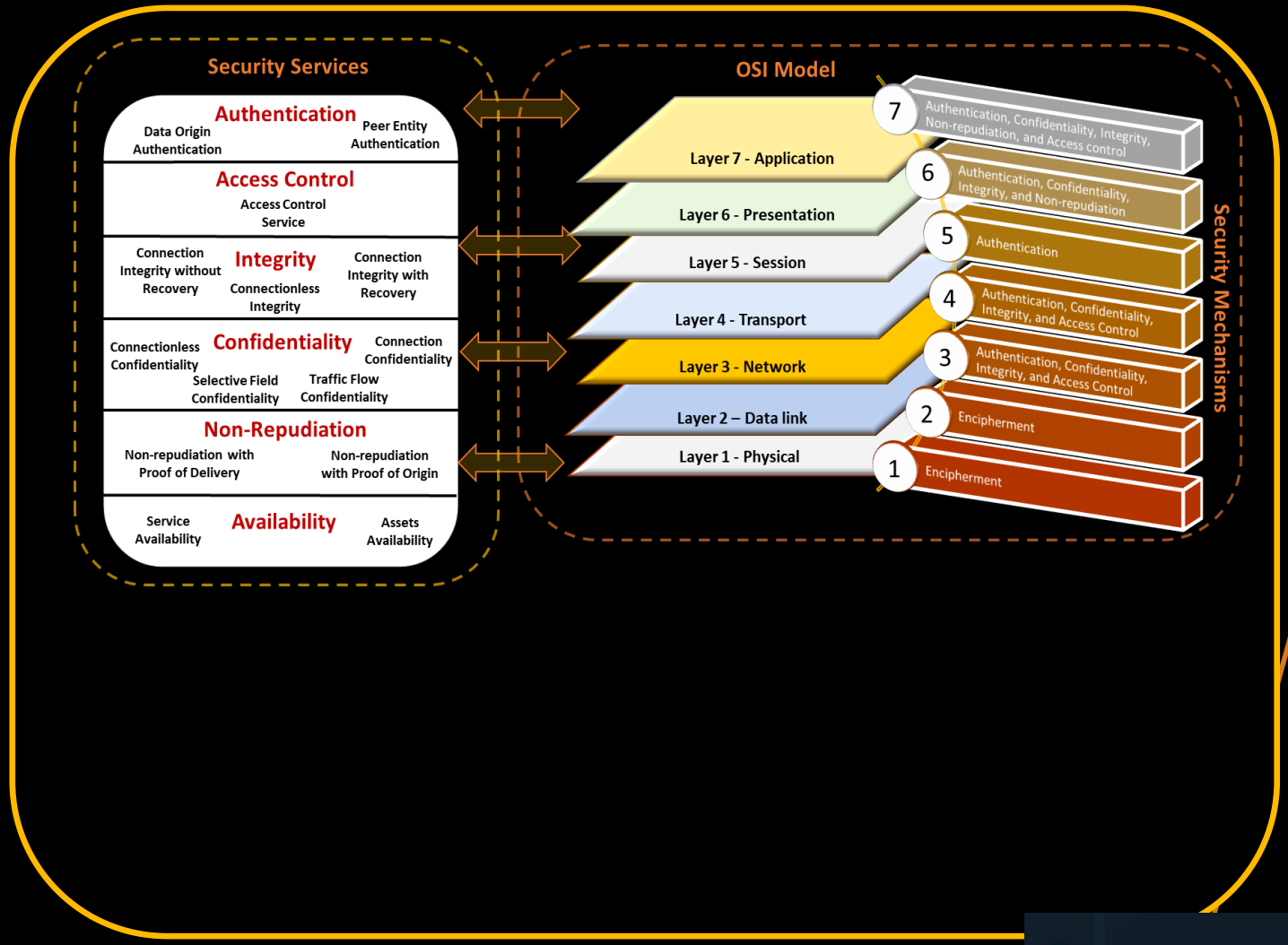
Relationship Between Security Mechanisms and Services

Security Mechanisms and Services

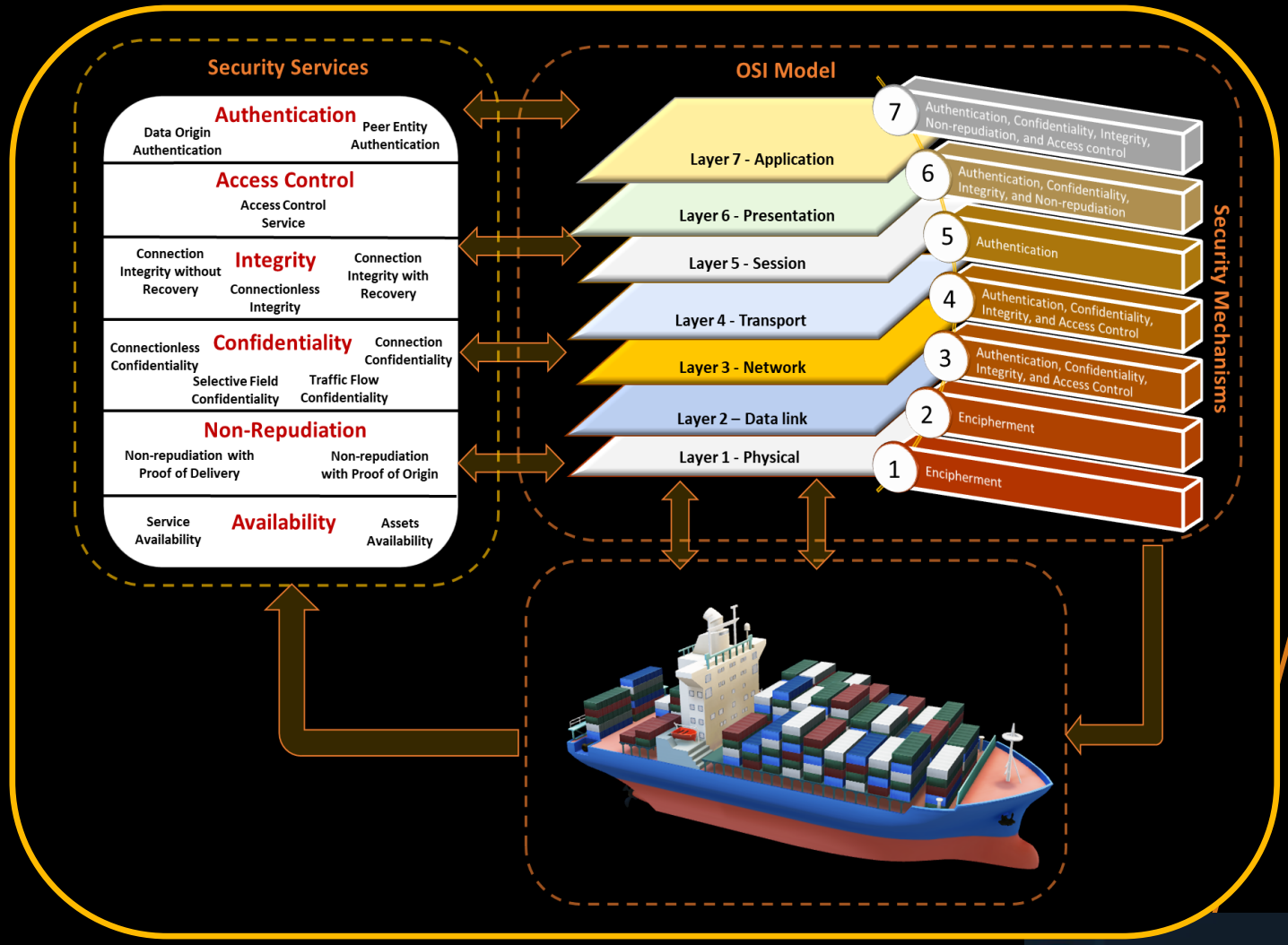
Mechanisms

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	

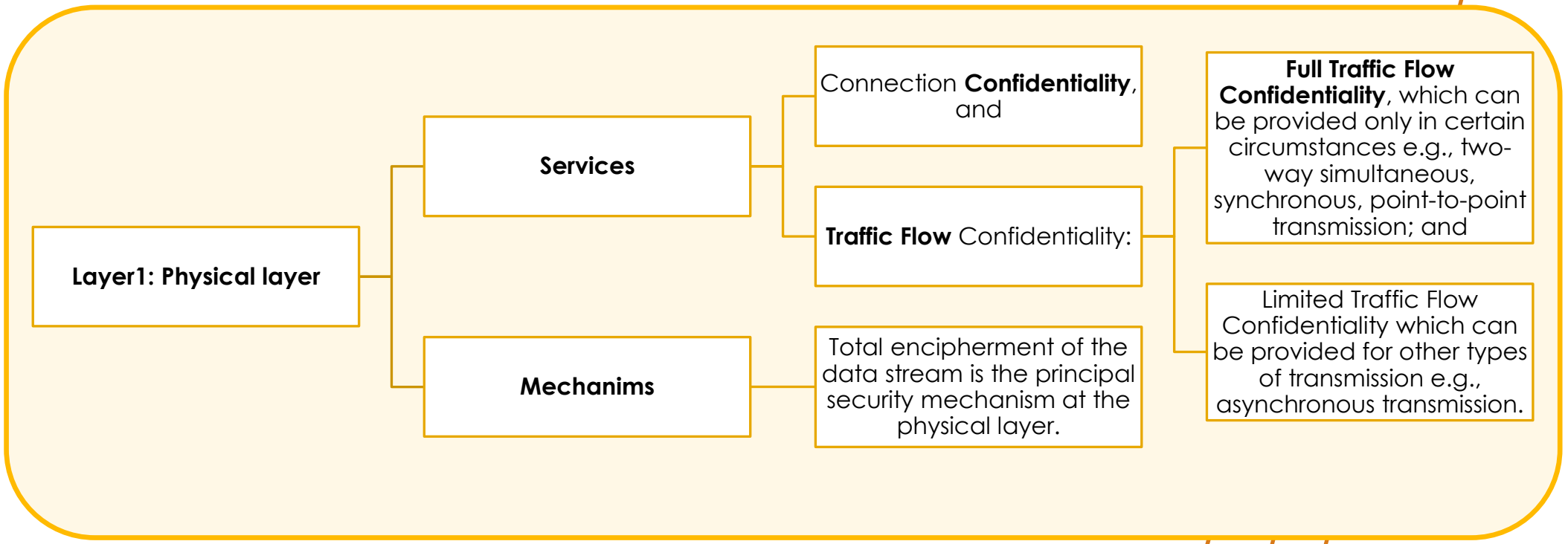
Exploring Relationship Distribution within the OSI Model Framework



Exploring Relationship Distribution within the OSI Model Framework

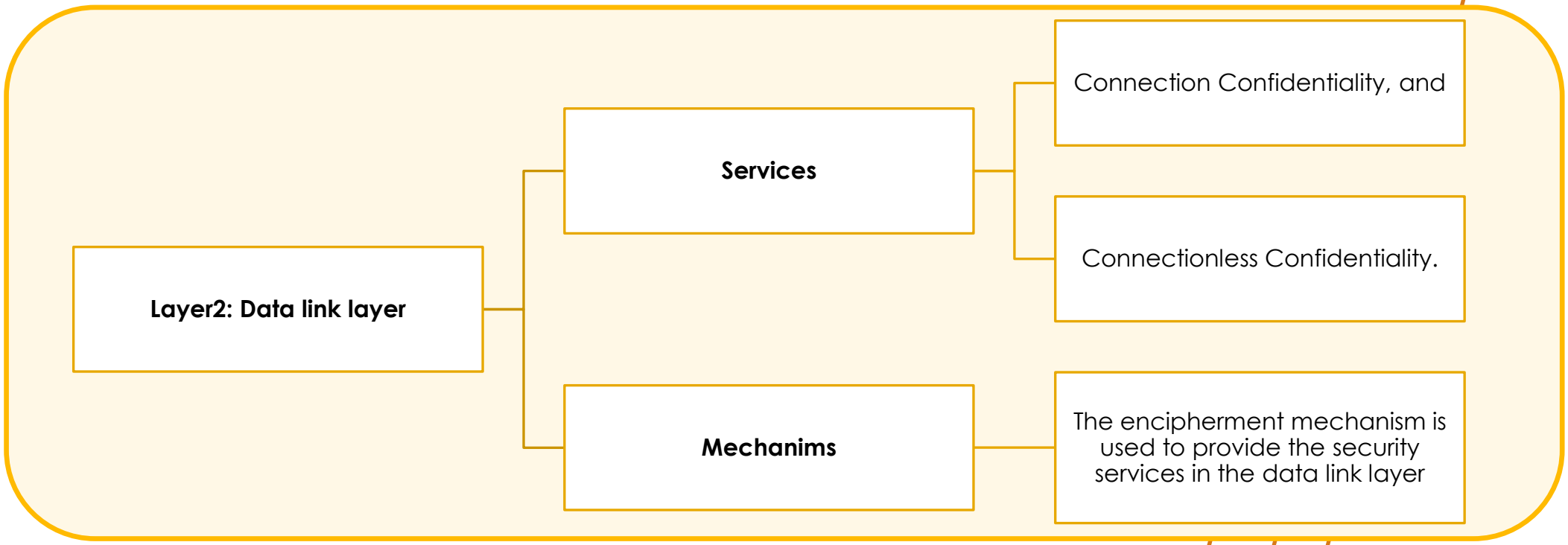


Placement of Security Services and Mechanisms



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