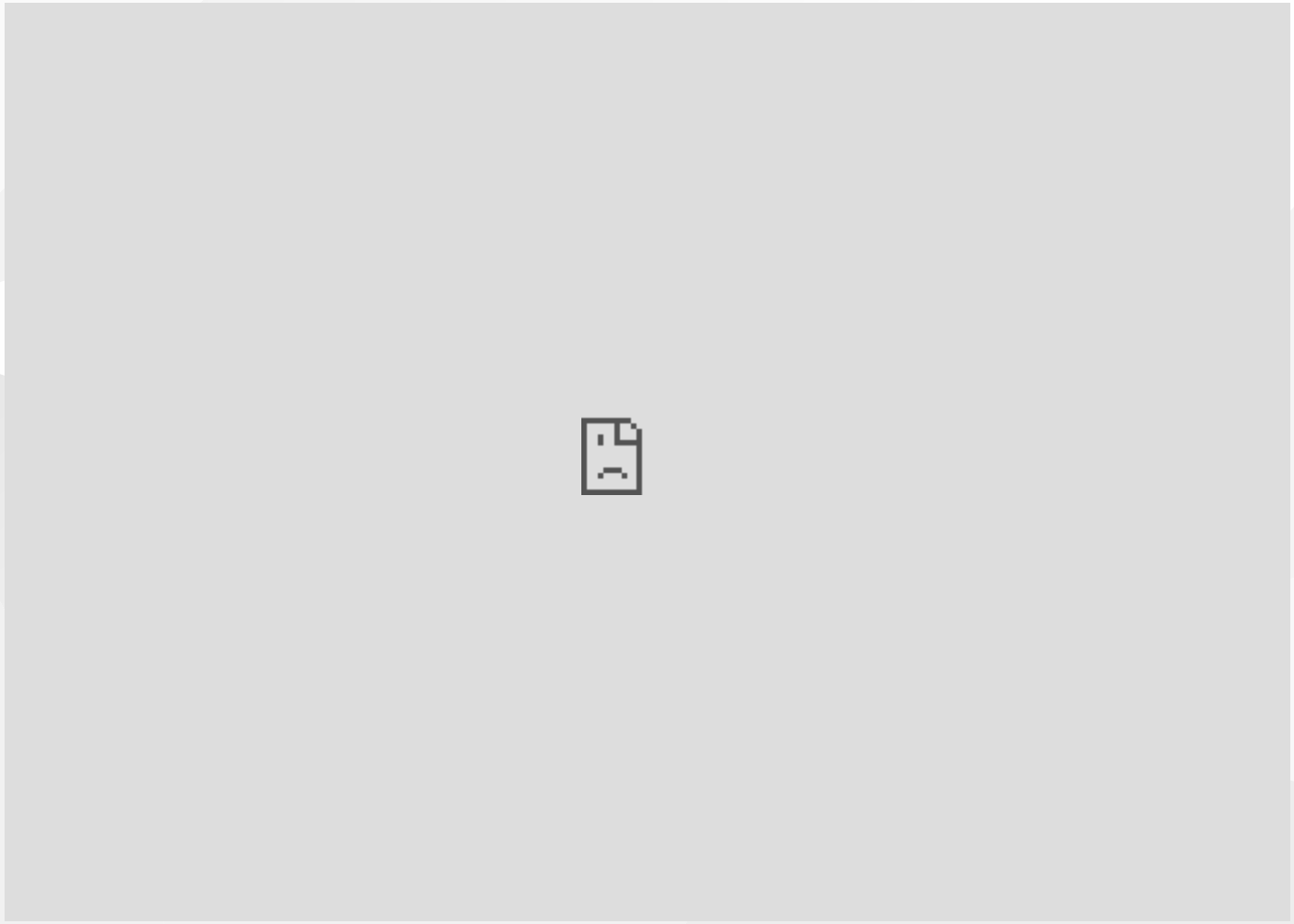
CEN429 Secure Programming

Week-12

Security Requirements and Standards

Download

- PDF
- DOC
- SLIDE
- PPTX



Outline

- Importance of Security Requirements
- International Security Standards
- Common Security Certifications

Week-12: Security Requirements and Standards

This week, we will learn how to define security requirements, how international security standards are developed, and why it is important to comply with widely used security certifications. Security requirements are designed to determine how resilient a system is to attacks. These standards are used in various sectors to ensure security.

1. Importance of Security Requirements

Theoretical Explanation: For a system to be secure, it must meet specific security requirements. These requirements determine what threats the system should be protected against and what security measures should be implemented.

- **Main Categories of Security Requirements:**
  - **Confidentiality:** Preventing unauthorized access to information.
  - **Integrity:** Preventing unauthorized changes to data.
  - **Authentication:** Verifying the identity of users accessing the system.
  - **Authorization:** Ensuring only certain users can access specific resources.
  - **Auditing:** Recording and tracking system events.
  - **Availability:** Ensuring the system operates continuously without interruption.

Practical Examples:

1. Defining security requirements for an application.
2. Analyzing how to secure a database.

2. ETSI (European Telecommunications Standards Institute)

Theoretical Explanation: ETSI is responsible for defining standards, particularly in the areas of network security, mobile communications, and IoT devices.

- **ETSI's Roles:**
  - Developing international standards for telecommunications technologies.
  - Providing security solutions for mobile networks.
  - Creating security standards for 5G.

Practical Examples:

1. Evaluating the security of an IoT device according to ETSI standards.
2. Configuring a network according to ETSI-defined security requirements.

3. GSMA (GSM Association)

Theoretical Explanation: GSMA defines security standards for mobile devices and networks, particularly focusing on SIM card security, network security, and protocols for mobile operators.

- **GSMA's Role:**
  - Creating security standards for protocols used in mobile networks.
  - Managing security standards for SIM and eSIM cards.
  - Ensuring secure data exchange between mobile operators.

Practical Examples:

1. Defining security requirements for a mobile device according to GSMA standards.
2. Integrating security protocols suggested by GSMA into mobile application development processes.

4. EMV (Europay, MasterCard, Visa)

Theoretical Explanation: EMV is a standard created to ensure the security of payment cards. It is widely used to enhance the security of credit cards and POS devices.

- **EMV Standards:**
  - **MasterCard:** Ensuring card security and protection of payment systems.
  - **Visa:** Protocols for securing cardholders and POS devices.

Practical Examples:

1. Creating security requirements for a payment system compliant with EMV standards.
2. Integrating security protocols provided by MasterCard and Visa into a POS device.

5. EAL (Evaluation Assurance Level)

Theoretical Explanation: EAL, or Evaluation Assurance Level, indicates the level of security a product meets. EAL levels help define how extensively a system's security is tested.

- **EAL Levels:**
  - **EAL1:** Functionally tested.
  - **EAL2:** Structurally tested.
  - **EAL3:** Methodically tested and checked.
  - **EAL4:** Methodically tested, designed, and reviewed.
  - **EAL5 and above:** Systems with high-security requirements.

Practical Examples:

1. Determining the security rating of a system according to EAL levels.
2. Developing test scenarios for a system at EAL4 level.

6. Common Criteria

Theoretical Explanation: Common Criteria is an international security certification standard used to evaluate the security level of products, widely recognized worldwide.

- **Advantages of Common Criteria:**
  - Ensures product security is globally acknowledged.
  - Provides a common language for verifying security features.
  - Compatible with EAL certification processes.

Practical Examples:

1. Initiating a security certification process under Common Criteria.
2. Preparing a software development plan compliant with Common Criteria.

7. FIPS (Federal Information Processing Standards)

Theoretical Explanation: FIPS defines information processing standards used by the U.S. government. It is particularly known for setting security standards for cryptographic modules.

- **Importance of FIPS:**
  - Defines security protocols used in U.S. government systems.
  - Ensures the certification of cryptographic algorithms and modules.
  - Provides security standards developed to protect sensitive information.

Practical Examples:

1. Developing a cryptographic module compliant with FIPS standards.
2. Integrating FIPS-certified security algorithms into an application.

Conclusion

This week, we explored security requirements and standards like ETSI, GSMA, EMV, EAL, Common Criteria, and FIPS. These standards help ensure the security of systems and products by defining internationally recognized security protocols. Security certifications demonstrate that products and systems have been evaluated and approved for security.

$$End - of - Week - 12$$