SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING-IOT Including CS&BCT

COURSE NAME : 19SB402 NETWORKING AND CYBERSECURITY

II YEAR / IV SEMESTER

Unit IV- **SECURITY ELEMENTS**

Topic : Security Requirements Specifications

- Security requirements specifications (SRS) are documents that outline the specific security requirements for a system, application, or project.

- When it comes to security elements, such as network infrastructure, software applications, or physical assets, the SRS helps define the necessary security controls and measures to protect them.

- Here are some common security elements and the considerations for their inclusion in the SRS:

1. Network Security:
    1. Define the required network architecture, including firewalls, routers, and intrusion detection/prevention systems.

    2. Specify encryption requirements for data transmission over the network, such as Transport Layer Security (TLS) or Virtual Private Networks (VPNs).

    3. Identify network segmentation and access control requirements to restrict unauthorized access.

2. Application Security:
    1. Specify authentication and authorization mechanisms, such as username/password combinations or multi-factor authentication (MFA).

    2. Define secure coding practices, including input validation, output encoding, and protection against common vulnerabilities (e.g., SQL injection, cross-site scripting).

    3. Specify session management controls, such as session timeouts and secure cookie handling.

3. Data Security:
    1. Define data classification requirements and access controls based on sensitivity levels (e.g., public, internal, confidential).

    2. Specify encryption requirements for data at rest, such as using disk-level encryption or database encryption.

    3. Identify backup and disaster recovery procedures to ensure data integrity and availability.

4. Physical Security:
    1. Define access control measures for physical facilities, including the use of badges, biometric systems, or security guards.

    2. Specify surveillance requirements, such as CCTV cameras and alarm systems, to monitor and protect physical assets.

    3. Identify procedures for secure equipment disposal or destruction to prevent data leakage.

5. Security Operations:

1. Define incident response and management procedures to handle security breaches, including reporting, investigation, and remediation.

2. Specify security monitoring and logging requirements to detect and respond to security events.

3. Identify security awareness and training programs to educate employees about security best practices.

6. Compliance and Legal Requirements:

1. Specify applicable regulations, standards, or industry-specific requirements (e.g., GDPR, PCI DSS, HIPAA) and ensure the system aligns with them.

2. Define privacy requirements, such as data anonymization or user consent for data processing.

Any Query????

Thank you……