Software Security

Software Security Requirements and Risk Assessment

Dr. Zeyad Safaa Younus Saffawi

Introduction

- Software security is not limited to implementing defensive mechanisms during coding or testing. It begins at the earliest **stages of the Software Development Life Cycle (SDLC), particularly during the requirements engineering phase**.
- Security must be treated as a **fundamental system property** rather than an **optional add-on**.
- Modern software systems operate in highly interconnected environments where vulnerabilities can lead to severe consequences, including **data breaches, financial losses, regulatory penalties, and reputational damage**.
- Therefore, defining clear security requirements and performing systematic risk assessment are essential steps in developing resilient and trustworthy software systems.

Software Security Requirements

What Are Security Requirements?

Software security requirements are formally specified conditions that a system must satisfy to ensure the protection of its **assets** (**data, systems, and users**) against **unauthorized access, misuse, modification, or disruption**.

They define:

- **What assets must be protected**
- **Who is allowed access**
- **What security controls must be implemented**

Functional vs Non-Functional Security Requirements

- **Security** is generally classified as a **non-functional requirement** because it **represents a quality attribute of the system**, describing how well the system protects data, users, and resources.
- **Functional Security Requirements**

Describe specific security features implemented by the system **(define what the system must do) such as:**

- The system must implement multi-factor authentication
- The system must validate password complexity rules
- The system must enforce role-based access control

- **Non-Functional Security Requirements**
  Describe security constraints, policies, or quality standards the system must meet **(define the system's security level or the required level of protection):**
  - The system must follow the appropriate **security rules and standards**, such as **ISO 27001** for **information security**, **GDPR** for **user data in Europe**, **PCI-DSS** for **payment card data**, or **HIPAA** for **health information**, depending on the type of system and local laws.
  - The system must **lock user accounts** after 5 failed login attempts
  - The system must **log all administrative activities**.
  - All **sensitive data must be encrypted** using trusted cryptographic methods, such as **AES-256, RSA, etc**.

Types of Security Requirements

Security requirements are commonly aligned with the CIA Triad:

1. Confidentiality Requirements

- Ensure that sensitive information is accessible only to authorized entities.
  - Data encryption (transition and in storage)
  - Access control mechanisms
  - Multi-Factor Authentication

2. Integrity Requirements

- Ensure that data remains accurate, consistent, and unaltered.
  - Data validation
  - Hashing and digital signatures
  - Audit logging

3. Availability Requirements

- Ensure that systems and services remain accessible when required.
  - Backup mechanisms
  - Protection against DoS attacks
  - System redundancy

How to Define Security Requirements

- **Security requirements** must be systematically identified using structured approaches:
  1. **Identify sensitive assets** such as: **databases, Customer information, and System credentials**
  2. **Identify possible source of threats** such as External attackers, Insider threats, Malware, and Misconfigurations.
  3. **Analyze regulatory requirements** (GDPR, HIPAA, etc.)
  4. **Define security controls**
  5. **Document requirements clearly**
- Security requirements must be:
  1. **Measurable**
  2. **Testable**
  3. **Clear and specific**

What Is Risk Assessment?

Risk assessment is a process used to **identify, analyze, and evaluate security risks** associated with software systems to reduce their impact.

- A risk exists when:
  - A threat exploits a vulnerability and affecting a valuable asset

Components of Risk

1. **Assets** Anything of value to the organization.
   - Databases
   - User data
   - Servers
2. **Threats** A potential source of damage.
   - Hackers
   - Malware
   - Insider threats
3. **Vulnerabilities** A weakness that can be exploited.
   - Weak passwords
   - Unpatched systems
   - Poor input validation
4. **Impact :The damage caused by a successful attack.**

Risk Assessment Process

Step 1: Identify Assets

- Determine what needs protection.

Step 2: Identify Threats

- Determine possible attack scenarios.

Step 3: Identify Vulnerabilities

- Identify weaknesses in the system design or implementation.

Step 4: Analyze Risk level

- Evaluate likelihood and impact.

Step 5: Prioritize Risks

- Classify risks (Low, Medium, High, Critical).

Types of Risks in Software Systems

- Data breach risk
- Unauthorized access risk
- Service downtime risk
- Compliance risk
- Financial loss risk

Risk Mitigation Strategies

- After identifying and assessing risks, organizations must decide how to handle them.
  Risk mitigation strategies define how an organization responds to identified security risks in order to minimize potential damage.
- There are four primary strategies:

1. **Risk Avoidance**: means eliminating the activity or condition that creates the risk.

   Examples:
   - Not storing sensitive credit card information.
   - Disabling a vulnerable service instead of trying to secure it.

2. **Risk Reduction** (Mitigation) means implementing controls to decrease the likelihood of risks occurring or their impact.

   Examples:
   - Encrypting sensitive data.
   - Applying multi-factor authentication.
   - Using firewalls and intrusion detection systems (IDS).

3. **Risk Transfer** means transferring the financial, legal, or operational impact of a potential risk to a third party.

   Examples:
   - Outsourcing cloud infrastructure to a certified service provider.

4. **Risk Acceptance** means acknowledging the risk and deciding not to take additional action.

   Examples:
   - Delaying patching for a low-severity vulnerability.

Why Risk Assessment Is Important

- **Helps prioritize security efforts:**
  - Enables organizations to focus on high-risk vulnerabilities and protect critical assets first.
- **Reduces financial losses:**
  - Prevents costly incidents such as data breaches, downtime, and regulatory penalties.
- **Supports decision-making:**
  - Provides measurable insights into threats and their impact, helping management to make informed investment decisions in the field of security.
- **Improves overall system resilience:**
  - Strengthens the system's ability to resist, respond to, and recover from cyber threats.

Relationship Between Security Requirements and Risk Assessment

- Risk assessment directly influences the definition of security requirements.
- **High-risk systems require**:
  - **Stronger authentication**
  - **Advanced encryption**
  - **Continuous monitoring**
  - **Strict access control policies**

Without risk assessment:

- Security requirements may be incomplete or ineffective.

References

- Kohnfelder, L. (2021). *Designing secure software: A guide for developers*. O'Reilly Media.

- McGraw, G. (2006). *Software security: Building security in*. Addison-Wesley Professional.