Software Security

Authentication and Access Control

Dr. Zeyad Safaa Younus Saffawi

Dr.Zeyad Safaa Younus

Authentication

- **Authentication** is a fundamental aspect of software security, **ensuring** that only **authorized users or systems can access the software and its resources**.
- It involves **verifying the identity of a user, device, or other entity before granting access to the system**.
- The **important components** and **methods of authentication** in software security include the following:
  1. **Password-Based Authentication**
     - **Strength and Complexity**: Users are required to **create strong passwords that combine uppercase and lowercase letters, numbers, and special characters** to **resist brute-force attacks**.
  2. **Multi-Factor Authentication (MFA)**
     - **Something You Know**: This is usually a **password or PIN**.
     - **Something You Have**: A **physical token, smartphone, or a one-time password (OTP)** generated by an authenticator app.
     - **Something You Are**: **Biometric authentication**, such as **fingerprint, facial recognition, or iris scanning**.
- MFA adds an additional layer of security by requiring two or more forms of authentication.

Dr. Zeyad Safaa Younus

Access Control

- **Access control** policies are a fundamental component of **software development** that governs the **permissions and restrictions** placed on **users accessing a system or its resources**.
- These **policies** define the **rules and guidelines** for **granting or denying access to different functionalities, data, or areas within the software**.
- There are **several types of access control policies** that can be implemented in **software development** to **manage and enforce access to resources**.
- These **policies** determine **how permissions are granted or denied** based on **various factors**, such as **user roles, attributes, or predefined security levels**.

Dr. Zeyad Safaa Younus

Access Control

1. **Role-Based Access Control** (**RBAC**). Here, **access rights** are **assigned** to **users** based on their **roles within the system**. For example, an **administrator** may have **full access** to **all functionalities**, while a **regular user** may only have **access to specific features**.

2. **Attribute-Based Access Control** (**ABAC**) is another type of **access control policy** that considers **additional attributes or characteristics** of **user**s when **granting or denying access**. These attributes can include **user location, time of access, device used, or any other relevant information**.

Dr. Zeyad Safaa Younus

CIA **Triad Principles**

- **Confidentiality, Integrity, and Availability** (**CIA**) are the three core principles of information security, often referred to as the **CIA Triad (The Core of Security)**. These **principles form the foundation for designing and evaluating the security of systems, data, and processes**.
- Every security control must address at least one of these three principles **Confidentiality, Integrity, and Availability** :

1. **Confidentiality: ensures that sensitive information is accessed** only by a**uthorized individuals or systems** and is **protected from unauthorized disclosure**.

- Purpose: To **protect information** from being *disclosed to unauthorized parties*, thereby **preventing breaches of privacy and security**.
- Important Practices:
  - **Encryption, Access Control Lists (ACLs).**
- **Examples** of **Confidentiality Breaches**:
  - **Data Leaks**: Sensitive information, like personal data or trade secrets, being **exposed due to inadequate access controls**.
  - **Unauthorized Access**: Hackers **gaining access to confidential informati**on through **phishing, malware**, or other attack vectors.

Dr. Zeyad Safaa Younis

CIA Triad Principles

2. **Integrity** ensures that **data is not altered or tampered** with by **unauthorized parties**. It ensures the **accuracy and completeness of data**.

- Purpose: To **maintain the trustworthiness and accuracy of information**, ensuring that it **remains unchanged** from **its original state unless properly authorized**.
- Important Practices:
  - **Checksums and Hashing**: Using **checksums or cryptographic hashing** (e.g., SHA-256) to **detect alterations in data**. **Any changes** to the **data** will result in a **different hash value**.
  - **Digital Signatures**: Applying **digital signatures** to **data** to **verify** its **origin** and ensure it has **not been modified during transmission**.
- Examples of Integrity Breaches:
  - **Data Tampering**: **Unauthorized modification of data**, such as **altering financial records**, which can lead to fraud or misinformation.
  - **Man-in-the-Middle Attacks**: **Attackers intercepting and altering data** during **transmission, potentially compromising the integrity of communication**.

Dr. Zeyad Safaa Younus

CIA Triad Principles

3. Availability: ensures **that information, data and systems are accessible** and **usable** when **needed by authorized users**.

- Purpose: To ensure that **systems and data are available to users** in a **timely manner, supporting** the **continuity** of **business operations**.
- Important Practices:
  - **Redundancy**: **Implementing redundant systems**, such as **backup servers**, **failover clusters,** and **data backups**, to ensure **continuous availability even if a component fails**.
  - **Load Balancing**: **Distributing workloads across multiple systems or servers to prevent overload** and ensure that **resources are available even under heavy usage**.
- Examples of **Availability** Breaches:
  - **DDoS Attacks**: **Overloading a system with traffic** to make it **unavailable to legitimate users**.
  - **Hardware Failures**: **System crashes** or **server outages leading to unavailability** of **critical services**.

Dr. Zeyad Safaa Younus

References

- Payer, M. (2021). *Software security: Principles, policies, and protection* (Version 0.37).

Dr. Zeyad Safaa Younus