Introduction to Authentication and Authorization

Prerequisites

- Basic Knowledge of Web Technologies
- Programming Fundamentals
- Knowledge of APIs and RESTful services.
- Databases and Data Storage Concepts
- Familiarity with databases, tables, and data storage concepts.

Learning Objectives

- Define Authentication and Authorization
- Understand Authentication Methods
- Identify Authorization Frameworks
- Differentiate Between Access Control Models
- Implement Basic Authentication and Authorization
- Recognize Best Practices for Secure Authentication and Authorization

Authentication

- Authentication is the process of verifying the identity of a user or system.
- Methods
  - Knowledge-Based (Something You Know)
    - Passwords and PINs: Common but vulnerable to attacks like phishing and brute force.
    - Security Questions: Often insecure due to easily guessable answers.
  - Possession-Based (Something You Have)
    - Smart Cards and Security Tokens: Provide an additional layer of security but can be lost or stolen.
    - Mobile Devices: Used for receiving one-time passwords (OTPs) or push notifications.

Authentication....

    - Inherence-Based (Something You Are)
        - Biometrics: Includes fingerprints, facial recognition, and iris scans.\
    -

- Multi-Factor Authentication (MFA)
    - Combines two or more methods to enhance security.
        - Example: Using a password (something you know) and a fingerprint scan (something you are).

Authentication....

Best Practices:

- Enforce strong password policies, including minimum length and complexity requirements.
- Implement MFA, especially for sensitive systems.
- Regularly update and patch authentication systems to address vulnerabilities.
- Educate users about phishing and social engineering attacks.

Authorization

- Authorization determines what an authenticated user is allowed to do.
- Access Control Models:
  - Role-Based Access Control (RBAC):
    - Access is based on user roles within an organization.
    - Example: An employee's role determines their access to company resources.
  - Attribute-Based Access Control (ABAC):
    - Access decisions are based on attributes (user, resource, environment).
    - Example: Access granted based on time of day or device used

Feature	Authentication	Authorization
Purpose	Verifies identity	Determines permissions
Happens when?	First step before authorization	After authentication
Responsibility	User identification	Access control based on roles/permissions
Examples	Login with username/password	Accessing files based on role
Common Methods	Passwords, biometrics, tokens	Attribute-Based Access Control (ABAC), Role-Based Access Control (RBAC)

Password Hashing

- Transforms passwords into fixed-size strings (hashes) to protect them from unauthorized access.
  - MD5 and SHA-1:
    - Considered insecure due to vulnerabilities.
  - SHA-256:
    - Part of the SHA-2 family, widely used and considered secure.
  - bcrypt:
    - Incorporates a salt to protect against rainbow table attacks and is adaptive to increase computational cost over time.
  - PBKDF2:
    - Uses a salt and iterates the hashing process to slow down brute-force attacks.

Salting

- Adding a unique, random value to each password before hashing to ensure that identical passwords have different hashes.
  - Prevents attackers from using precomputed hash tables (rainbow tables) to crack passwords.
  - Ensures that even if two users have the same password, their hashes will differ.

Key Stretching

- Applying a hash function multiple times to increase the computational effort required to hash each password.

- Benefits:
  - Slows down brute-force attacks by making each password guess more time-consuming.
  - Algorithms like bcrypt, PBKDF2, and Argon2 implement key stretching.
  -

Password Hashing....

Best Practices:

- Use modern, secure hashing algorithms with salting and key stretching.
- Ensure salts are unique, random, and stored securely alongside the hash.
- Avoid using deprecated or weak hash functions like MD5 or SHA-1.
- Regularly update hashing algorithms and parameters to keep up with advancements in computational power.

Thank you....