Experiment 09

Learning Objective: Design and implement a Secure Authentication Protocol/System for any critical infrastructure area

Tools: C/C++/Java/Python

Theory:

User authentication is a method that keeps unauthorized users from accessing sensitive information. For example, User A only has access to relevant information and cannot see the sensitive information of User B. Cybercriminals can gain access to a system and steal information when user authentication is not secure.

Common Authentication Types

Cybercriminals always improve their attacks. As a result, security teams are facing plenty of authentication-related challenges. This is why companies are starting to implement more sophisticated incident response strategies, including authentication as part of the process. The list below reviews some common authentication methods used to secure modern systems.

1. Password-based authentication

Passwords are the most common methods of authentication. Passwords can be in the form of a string of letters, numbers, or special characters. To protect yourself you need to create strong passwords that include a combination of all possible options.

However, passwords are prone to phishing attacks and bad hygiene that weakens effectiveness. An average person has about 25 different online accounts, but only 54% of users use different passwords across their accounts.

The truth is that there are a lot of passwords to remember. As a result, many people choose convenience over security. Most people use simple passwords instead of creating reliable passwords because they are easier to remember.

The bottom line is that passwords have a lot of weaknesses and are not sufficient in protecting online information. Hackers can easily guess user credentials by running through all possible combinations until they find a match.

2. Multi-factor authentication

Multi-Factor Authentication (MFA) is an authentication method that requires two or more independent ways to identify a user. Examples include codes generated from the user’s smartphone, Captcha tests, fingerprints, voice biometrics or facial recognition.

MFA authentication methods and technologies increase the confidence of users by adding multiple layers of security. MFA may be a good defense against most account hacks, but it has its own pitfalls. People may lose their phones or SIM cards and not be able to generate an authentication code.

3. Certificate-based authentication

Certificate-based authentication technologies identify users, machines or devices by using digital certificates. A digital certificate is an electronic document based on the idea of a driver’s license or a passport.

The certificate contains the digital identity of a user including a public key, and the digital signature of a certification authority. Digital certificates prove the ownership of a public key and issued only by a certification authority.

Users provide their digital certificates when they sign into a server. The server verifies the credibility of the digital signature and the certificate authority. The server then uses cryptography to confirm that the user has a correct private key associated with the certificate.

4. Biometric authentication

Biometrics authentication is a security process that relies on the unique physical characteristics of an individual. Here are key advantages of using biometric authentication technologies:

- Physical characteristics can be easily compared to authorized features saved in a database.
- Biometric authentication can control physical access when installed on gates and doors.
- You can add biometrics into your multi-factor authentication process.

Biometric authentication technologies are used by consumers, governments and private corporations including airports, military bases, and national borders. The technology is increasingly adopted due to the ability to achieve a high level of security without creating friction for the user. Common biometric authentication methods include:

- **Facial recognition**—matches the different face characteristics of an individual trying to gain access to an approved face stored in a database. Face recognition can be inconsistent when comparing faces at different angles.
- **Fingerprint scanners**—match the unique patterns on an individual’s fingerprints. Some new versions of fingerprint scanners can even assess the vascular patterns in people’s fingers. Fingerprint scanners are currently the most popular biometric technology for everyday consumers.
- **Eye scanners**—include technologies like iris recognition and retina scanners. Iris scanners project a bright light towards the eye and search for unique patterns in the colored ring around the pupil of the eye. The patterns are then compared to approved information stored in a database. Eye-based authentication may suffer inaccuracies if a person wears glasses or contact lenses.

5. Token-based authentication

Token-based authentication technologies enable users to enter their credentials once and receive a unique encrypted string of random characters in exchange. You can then use the token to access protected systems instead of entering your credentials all over again. The digital token proves that you already have access permission. Use cases of token-based authentication include RESTful APIs that are used by multiple frameworks and clients.

Implementation:

```
$servername = "localhost";
$username1 = "root";
$password1 = "";
$dbname = "dcs lead";
$conn = mysqli_connect($servername, $username1, $password1, $dbname);

$user = $_POST["admin-username"];
$pass = $_POST["admin-password"];
$sql1 = "SELECT * FROM admins";
$result = mysqli_query($conn, $sql1);
```

```
if ($result->num_rows > 0) {
    while ($row = $result->fetch_assoc()) {
        if ($row['username'] == $user && $row['password'] == $pass) {
            $_SESSION['admin_username'] = $row['username'];
            header("location: http://localhost/DCS%20Lead/admin/admin_dashboard.php");
            exit;
        } else {
            header("location: http://localhost/DCS%20Lead/admin/admin_login.html");
            exit;
        }
    }
}
```

Learning Outcomes: The student should have the ability to
LO1: Identify potential threats & vulnerabilities for any critical infrastructure area
LO2: Implement Secure Authentication Protocol/System
LO3: Understand usage of these Secure Authentication Protocol/System

Course Outcomes: Upon completion of the course students will be able to understand the concept of Authentication Systems and will be able to apply it for security purposes.

Conclusion: Through this experiment we learned the concept of Authentication Systems and we apply this for secure Authentication purposes.

Name:
Class: SE-CSE
Roll No.:

For Faculty Use:

Correction Parameters	**Formative Assessment [40%]**	**Timely completion of Practical [40%]**	**Attendance / Learning Attitude [20%]**	
Marks Obtained				

Theory Questions:

1. Discuss the fundamental principles and requirements of a secure authentication protocol/system.
2. Compare and contrast various authentication mechanisms.

Case-Studies/Open-Ended Questions:

1. How will the implementation of a secure authentication protocol/system impact the overall resilience and reliability of critical infrastructure operations in the face of emerging cyber threats and vulnerabilities?