A black background with red text

Description automatically generated

Implementing Basic Two-Factor Authentication (2FA)

IS451: Information and Systems Security

Dr. Govindha Ramaiah Yeluripati

8th October, 2024

Team 24

Joseph Narteh Lartey

Kwabena Kootin-Sanwu Nuamh

**Workflow of the Two-Factor Authentication (2FA) System**

The 2FA system combines the use of **secure passwords** and **One-Time Passwords (OTPs)** to enhance user security. This ensures safety in systems and minimizes the risk involves in identity or data theft.

**User Registration**

* Users create an account by providing a username, email, and a secure password.
* After registration, the system generates a unique OTP and sends it to the user's email.

**OTP Verification**

* Once the user receives the OTP, they enter it on the verification page.
* The system compares the entered OTP with the stored OTP (valid for 2 minutes).
* If the OTP matches, the user's account is successfully activated, and access is granted.

**User Login**

* The user logs in by entering their email and secure password.
* Upon successful password verification, the system generates a new OTP and sends it to the user's registered email for a second layer of authentication.
* The user must enter the received OTP to complete the login process.
* If both the password and OTP are correct, access is granted to the user.

**Forgot Password**:

* If the user forgets their password, they can request a password reset.
* After verifying the user's identity through OTP, they can create a new secure password.

**Resending OTP**:

* Users can request the system to resend the OTP if they don't receive it or it expires.

**Possible Attacks and Countermeasures**

**1. Phishing Attacks**:

Some attackers can trick users into providing their passwords or OTPs on fake websites, call and emails.

**Countermeasure**:

* Educate users on recognising legitimate OTP messages and system alerts.
* Introduce email alerts for suspicious login attempts from unrecognised devices or locations.

**2. Brute Force Attacks**:

An attacker could try to guess the user's password or OTP. This may take a while, but with the use of some fast computers like supercomputers, they have a higher chance of succeeding.

**Countermeasure**:

* Enforce strong password policies requiring a mix of characters.
* Limit the number of OTP attempts; account can be locked after a certain number of wrong inputs until unblocked by an admin.
* Using CAPTCHAs during login and OTP entry to prevent automated bots.

**3. Man-in-the-Middle (MITM) Attacks**:

Cybercriminals can intercept user and server communication to steal OTPs or passwords.

**Countermeasure**

* Use HTTPS to secure communication.
* Implement HSTS (HTTP Strict Transport Security) to ensure users only connect via secure channels.
* Use end-to-end encryption for sensitive data transmission, especially OTPs.

**5. SQL Injection Attacks**:

Attackers might try to manipulate database queries by injecting malicious SQL code.

**Countermeasure**:

* Use prepared statements and parameterised queries to interact with the database.
* Sanitize and validate all user inputs, particularly in login, registration, and password reset forms.

**Conclusion**

To conclude, a two-factor authentication system significantly strengthens login security by combining password protection with OTP verification. However, continuous monitoring and updates to security policies will be crucial to ensuring long-term system integrity.

**Important Links**  
Youtube Link : <https://youtu.be/yclrF2AIbrY>

Github Link : <https://github.com/Kootin-Sanwu/Two-Factor-Authentication-System>

Webiste Link : <http://13.60.47.185/Two-Factor-Authentication-System/>