ST10092354
Lerato Kekana

APDS7311 ICE Task 2

Question 1

New registration requirements are essential for creating a secure, efficient, and user-friendly system when users sign up for services or applications. Here's a concise overview of the key reasons why these requirements matter:

1. Enhanced Security

Registration is often the first point of contact, making it a target for attacks like account takeovers.

- **Strong Password Policies:** Require complex passwords to reduce cracking risks.
- **Two-Factor Authentication (2FA):** Adds a second verification step for security.
- **CAPTCHA:** Prevents automated bot registrations.

2. Identity Verification

Ensures user authenticity, especially in sensitive industries.

- **Email and Phone Verification:** Confirms valid communication channels.
- **KYC (Know Your Customer):** In regulated sectors, requires ID checks to prevent fraud.

3. Compliance with Regulations

New requirements help meet global data privacy laws like GDPR and CCPA.

- **User Consent:** Explicitly obtain consent for data collection.
- **Data Minimisation:** Collect only essential information.
- **Age Verification:** Ensures compliance for age-restricted content.

4. Improved User Experience

Simplifying registration while maintaining security enhances onboarding.

- **Single Sign-On (SSO):** Allows users to register via existing accounts.
- **Progressive Profiling:** Gathers information gradually to ease initial signup.
- **User-Friendly Interfaces:** Features like auto-fill and real-time feedback enhance usability.

5. Fraud Prevention

Focus on preventing fraudulent account creation, particularly in high-stakes environments.

- **Address Validation:** Helps prevent fake purchases.
- **Device Fingerprinting:** Detects suspicious patterns in account creation.

6. Tailored Services and Personalisation

Collecting detailed user information enables personalised experiences.

- **Preference Gathering:** Asks for user preferences during registration.
- **Segmentation:** Allows targeted offers based on user data.

7. Account Recovery and Management

Capturing recovery information improves user access in case of issues.

- **Backup Recovery Options:** Collects alternate contact details for recovery.
- **Security Questions:** Though becoming less common, they still assist in recovery.

8. Data Integrity and Validation

Mechanisms ensure the accuracy of submitted data, maintaining a reliable user database.

- **Input Validation:** Confirms correct formatting of entries.
- **Duplicate Account Prevention:** Stops multiple registrations using the same email or phone.

9. Scalability and Integration

Modern systems need to scale and integrate seamlessly as the user base grows.

- **APIs for Registration:** Enable third-party service integration.
- **CRM Integration:** Automatically updates customer data in existing business systems.

These new registration requirements are crucial for enhancing security, user experience, compliance, and operational efficiency.

Question 2

Storing sensitive data in cookies introduces several security risks that compromise both user privacy and application security. Here's a summary of the key dangers and mitigations:

1. Exposure to Cross-Site Scripting (XSS) Attacks

Attackers can use XSS to inject malicious scripts and access cookies containing sensitive data.
Mitigation: Use the HttpOnly flag to prevent JavaScript access.

2. Insecure Transmission (Man-in-the-Middle Attacks)

Sensitive cookies sent over HTTP can be intercepted by attackers.
Mitigation: Use HTTPS and mark cookies as Secure to enforce transmission over encrypted connections.

3. Session Hijacking

Attackers who steal session cookies can impersonate users.
Mitigation: Use short session expiration times, HttpOnly, Secure, and SameSite cookie flags, and rotate session tokens regularly.

4. Persistent Storage of Sensitive Data

Cookies can persist after sessions, exposing sensitive information to unauthorised users.
Mitigation: Avoid storing sensitive data in cookies; store only session tokens or non-sensitive identifiers.

5. Cookie Theft via Cross-Site Request Forgery (CSRF)

CSRF attacks use the victim's cookies to execute malicious requests.
Mitigation: Implement CSRF protection (e.g., anti-CSRF tokens) and avoid storing sensitive data in cookies.

6. Cookie Manipulation

Attackers can tamper with cookies to modify sensitive data, like user roles.
Mitigation: Don't store sensitive data in cookies. For data stored in cookies, use cryptographic signing to ensure integrity.

7. Exceeding Cookie Size Limits

Storing large amounts of data in cookies can lead to performance issues and data exposure.
Mitigation: Store only session identifiers in cookies; keep complex or sensitive data on the server.

8. Lack of Data Encryption at Rest

Cookies stored on devices may be unencrypted, exposing them to attackers.
Mitigation: Avoid storing sensitive data in cookies. For non-sensitive data, consider encryption, but this should only be in low-risk cases.

General Rule: Keep cookies for essential, non-sensitive data, and avoid storing personal or critical information directly within them. Always implement best practices like secure flags, validation, and encryption where necessary.

Question 3

Credential security is vital as it serves as the foundation for protecting systems, data, and users from various security threats. Here's why it's essential, along with examples and consequences of weak practices:

1. Prevents Unauthorised Access

Securing credentials prevents unauthorised users from accessing critical systems and data.

- **Example:** Secure authentication systems limit access to sensitive databases using strong credentials.
- **Consequence:** Weak credentials allow attackers to bypass protections, leading to unauthorised access.

2. Mitigates Data Breaches

Compromised credentials are a leading cause of data breaches.

- **Example:** In breaches like the 2013 Target breach or 2020 SolarWinds attack, stolen credentials were the entry point.
- **Consequence:** Breaches lead to data theft, financial losses, and repetitional damage.

3. Reduces the Risk of Account Takeover (ATO)

ATOs occur when attackers hijack accounts using stolen credentials.

- **Example:** Multi-factor authentication (MFA) protects user accounts on an e-commerce site.
- **Consequence:** Account takeovers lead to fraud, financial loss, and loss of user trust.

4. Protects Against Credential Stuffing and Brute-Force Attacks

Attackers use stolen credentials to gain unauthorised access to multiple accounts.

- **Example:** Implementing rate limiting, account lockouts, and MFA can thwart such attacks.
- **Consequence:** Weak protections lead to mass account compromise and system exploitation.

5. Ensures Compliance with Data Privacy and Security Regulations

Data privacy laws mandate secure credential management.

- **Example:** Regulations like GDPR require strong passwords and MFA to protect credentials.
- **Consequence:** Non-compliance results in hefty fines and legal action.

6. Limits the Impact of Phishing Attacks

Phishing tricks users into revealing their credentials.

- **Example:** MFA prevents attackers from accessing accounts even if they steal a password.
- **Consequence:** Insecure credentials allow phishing attacks to directly compromise accounts.

7. Supports Zero Trust Security Models

Zero Trust requires strict authentication and authorisation for all users and devices.

- **Example:** Strong credential mechanisms like MFA and adaptive authentication enable Zero Trust.
- **Consequence:** Weak credential security undermines Zero Trust, allowing unauthorised access.

8. Prevents Insider Threats

Insiders can misuse their access to sensitive data.

- **Example:** Privileged Access Management (PAM) and regular access reviews reduce insider risk.
- **Consequence:** Poor credential management lets insiders exploit their access to harm systems.

9. Builds Customer Trust

Secure credential handling builds user confidence.

- **Example:** Companies that enforce secure password storage and regular updates gain customer trust.
- **Consequence:** A breach in credential security leads to loss of users, revenue, and reputation.

10. Minimises the Risk of Lateral Movement in Attacks

Attackers often move laterally within networks using compromised credentials.

- **Example:** Role-based access control (RBAC) and unique credentials for different systems limit lateral movement.
- **Consequence:** Credential reuse and excessive permissions allow attackers to compromise multiple systems.

Key Takeaway: Implementing strong credential security measures—such as MFA, secure password storage, and proper access control—helps prevent breaches, mitigate threats, and build trust with users, making it a crucial part of an organisation's security strategy.

Question 4

Multi-Factor Authentication (MFA) is a security method that requires multiple forms of verification for access, enhancing security beyond just passwords. Here's why it's essential:

1. Adds Extra Protection

MFA requires additional verification beyond a password, protecting against attacks like phishing and brute force.

- **Example:** Even with a stolen password, an attacker can't log in without a second factor like an app-generated code.

2. Mitigates Credential Theft

MFA reduces the impact of stolen or reused passwords by requiring an additional factor.

- **Example:** Even with breached credentials, an attacker still needs the second factor.

3. Defends Against Phishing

MFA stops attackers from logging in, even if they trick users into providing passwords.

- **Example:** An attacker can't log in without the second factor, like a code sent via SMS.

4. Secures High-Risk Environments

Essential in industries like banking and healthcare, MFA provides extra protection for critical systems.

- **Example:** Banks require additional verification for unrecognised devices or locations.

5. Limits Data Breach Impact

Even if passwords are leaked, MFA prevents attackers from gaining access without the second factor.

- **Example:** Breached accounts stay secure if MFA is enabled.

6. Supports Compliance

MFA helps meet regulatory requirements, such as GDPR and HIPAA, and avoids penalties.

- **Example:** Healthcare organisations use MFA to protect patient data.

7. Secures Remote Access

MFA ensures only authorised users can access corporate systems from remote locations.

- **Example:** Employees working remotely must verify their identity with an additional step.

8. Prevents Account Takeovers

MFA adds an extra hurdle, preventing attackers from gaining full control of compromised accounts.

- **Example:** A one-time passcode or biometric scan is required for access.

9. Builds User Trust

Users gain confidence knowing their accounts are protected by additional security measures.

- **Example:** Social media platforms offering MFA assure users of better security against unauthorised access.

In short, MFA strengthens authentication, reduces risks, and enhances overall security.