Web Design & Programming

User Accounts Management

Xavier Belanger

Initial Situation

- Modern web sites usually requires for a user to create an account, to personalize the content, place orders, interacting with other users, …
- There is no universal way to manage user accounts, either from a technical or legal standpoint. There is best practices rules and local laws, especially around PII (Personable Identifiable Information).

User Account Lifecycle

- A user account will need to go through various steps over time:
  - Creation
  - Validation
  - Updates
  - Deletion or transfer
- Depending on the type of organization and web site, some of those steps could be managed internally or by a third-party.

User Experience

- Slow or cumbersome account processes can discourage users to register or to come back to your website.
- Depending on the service provided, you may want to allow a “guest-only” access, that doesn’t requires to create an account.

Network Security

- All user account-related actions must take place over an encrypted network connection.
- This also applies to third-party connections.
- User token, ID and similar information should not be used directly in an URL.

Authentication and Authorization

- Authentication is the process to confirm the user identity, allowing access, or not, to a resource.
- Authorization is related to the actions that a user can (or cannot) perform once authenticated into a system.

HTTP Authentication

- Allows to authenticate a user against a user database configured through the web server (local password file, external directory, …).
- Not customizable, not directly integrated into a web application.
- Doesn’t offer a ‘logout’ function.
- Accounts management can get complicated.

Internal Authentication

- Internal authentication is performed when the web application itself includes all the user account management process.
- This provides more flexibility to update all user settings.
- Design choices need to be made first and the code should cover all possible cases and functions.

Third-party Authentication

- You can delegate the user account management process to a third-party partially or entirely.
- Large and popular web services offer authentication services (Amazon, Facebook, Google, Microsoft, …) that can be integrated with your own web application.
- OAuth (Open Authorization) is the open standard used in most cases. It relies on secure access tokens. Two versions are currently deployed.

Single-Sign On

- Single-Sign On (SSO) refers to the fact that when authenticating against one identity provider, you can get access to other services linked to that same provider, hence removing the need to authenticate multiple times.
- This requires to establish a trusted relationship between multiple parties; with a reliable validation over time.

LDAP

- Lightweight Directory Access Protocol
- LDAP is mostly used for internal authentication, inside an organization. Microsoft Active Directory can be used as a LDAP server.

SAML

- Security Assertion Markup Language
- SAML allows to establish single-sign on mechanisms across security domains.
- It relies on XML configuration files between an Identity Provider (IdP) and a Service Provider (SP).
- SAML itself is not an authentication source, it requires another source as a backend (directory, database, …).

Multi-Factor Authentication

- Granting access is usually based on a user name and a password. That system is not necessarily secured enough and can be improved by adding a second step, different from the first one, confirming the user identity.
- MFA can be achieved by using text messages, an authenticator application or a physical token.
- This is still vulnerable to some form of social engineering attacks.

CAPTCHA

- “Completely Automated Public Turing test to tell Computers and Humans Apart”
- Reading or identification challenge supposed to be easy to solve by humans and difficult for computers, in order to prevent automatic connections.
- This presents accessibilities issues and slow down the logon process.

Security Questions

- Security questions are used to allow a user to regain access to her or his account when the password has been lost.
- Some systems provide pre-established questions, other may let the end-user define the questions herself or himself.
- Most questions are based on information that can be found on social media or similar public records.
- Answers should be stored at the same security level than passwords or other personal information.

Corroborative User Information

- Other piece of data could be used to verify user access:
  - Web browser name
  - Geo-location
  - Time zone
  - …
- An unusual pattern could be used to raise alerts or prevent a connection.
- Those techniques requires more tracking, could be considered as invasive and may lead to false positive errors.