Secure your application using Facebook as Identity Provider

Asna Javed
Lead Developer Advocate, IBM PAK

IBM **Developer**

IBM

Overview

- Call for Code 2021

- AAA framework

- Identity Provider

- Social Login's

- AppID

- Hands On

The AAA Framework

Authentication → Authorization → Accounting

Authentication

Something **that you know**

- Passwords, Security questions
- Something **you are**
  - Biometrics, fingerprint
- Something **that you have**
  - 2FA keys, FIDO

Authorization

- **DAC** – Disectionary Access Control
- **RBAC** – Role Based Access Control
- **ABAC** – Attribute Based Access Control
- **MAC** – Mandatory Access Control

Accounting

- Once the user has logged in, their usage should be monitored
- This can be done with various tools such as IBM qRadar SIEM

Authentication != Authorization

Authentication

- Confirming a users identity
- Determines who is the person logging in based on different elements

- Types of authentication
  - Single Factor Authentication
  - Two Factor Authentication
  - Multi Factor Authentication

Authorization

- Once identified, we move to authorization
- Checks for the level of access a particular user is allowed to access within the system/organization

Identity Provider:

An identity provider (IdP) is a service that stores and manages digital identities.

An IdP workflow typically involves:

Request: The user can enter credentials from another login

Verification: The IdP checks with a company's IT to determine if the user has access and what work that person is allowed to do.

Unlocking: The user gains access to the specified resources, and the visit is logged.

Social Login's

Social login, also known as social sign-in
or social sign-on, uses information from
social networking sites to facilitate logins
on third-party applications and platforms.

f Login with Facebook

G+ Login with Google

— or —

Username:

Password: [Forgot Password](#)

Login

Why should you add Social Login?

One-click return experience:

After users register in your application using Social Login, their return experience will be very simple, as they will probably be logged into the social network, and just one click will be enough to login to your application.

Access richer user profiles:

Social network providers can give you additional information about users, such as location, interests, birthday, and more. Using this data, you can target personalized content to the user.
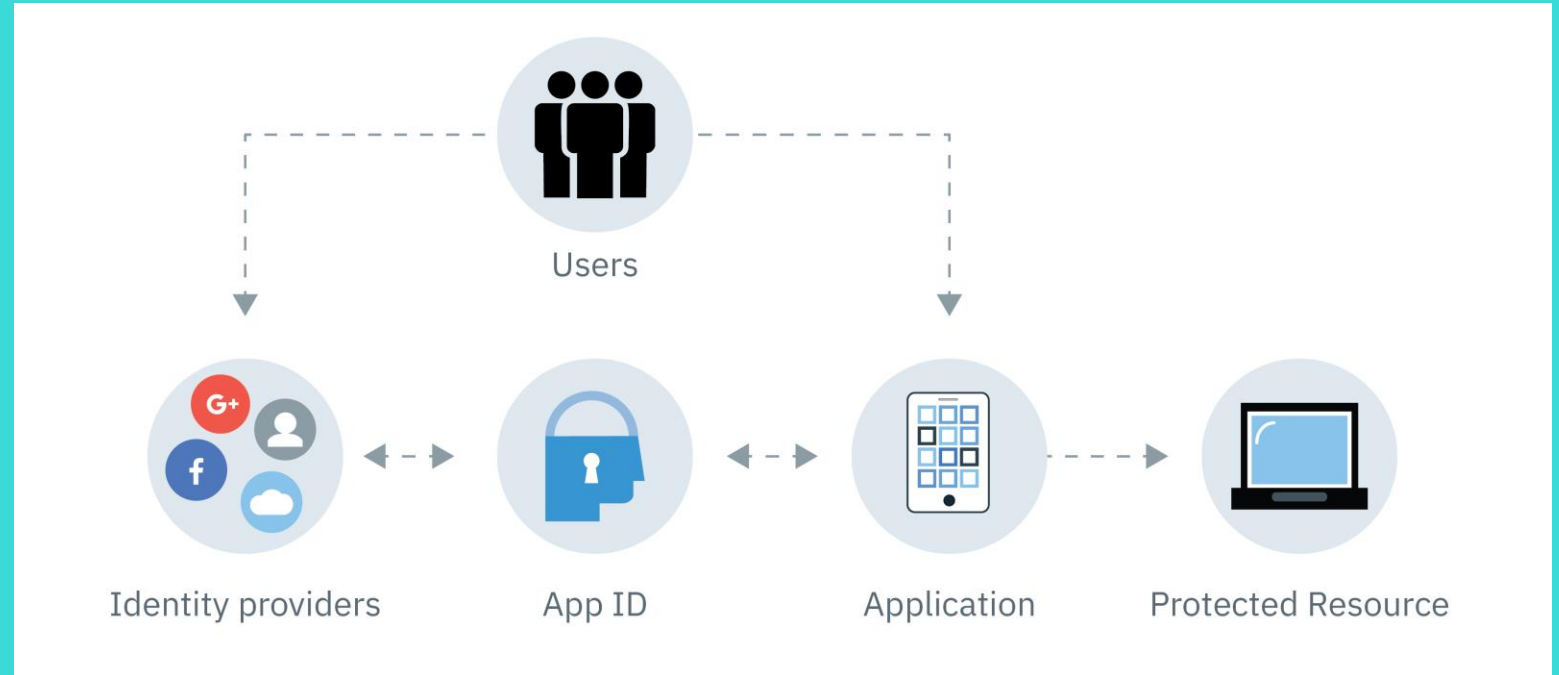
Email is verified:

The social network provider is in charge of verifying the user's email. Additionally, the providers will handle the password recovery process.

Increase registrations:

according to a Web Hosting Buzz survey: 86 percent of users report being bothered by having to create new accounts on websites. Some of these users would rather leave your site than register,

AppID

- Easily add authentication to web and mobile apps

- Several identity providers that the service can be configured to use such as Cloud Directory, SAML, Google & Facebook

- Create your Custom identity flow to work with App ID

- Use services such as Single Sign-on, Active Directory and Multifactor Authentication to manage your users

Users

Identity providers   App ID   Application   Protected Resource

Hands-on Session

- Sign up/Log in to your IBM Cloud Account: https://ibm.biz/BdfPad

- Follow Hands-on:

- https://github.com/asnajaved/Secure-your-application-using-Facebook-as-Identity-Provider

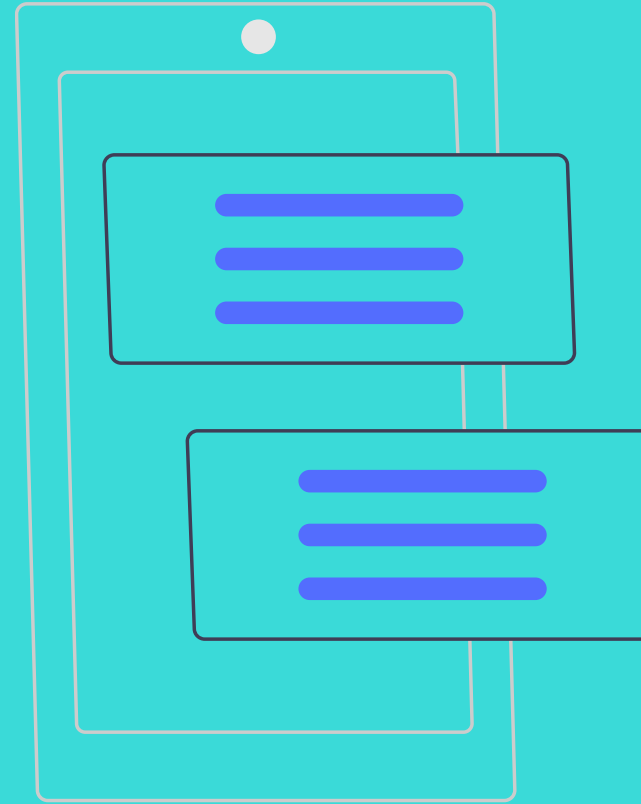# Resources

You can learn more using the following resources:

- IBM Developer (developer.ibm.com)
- Meetup Page: https://www.meetup.com/IBM-Developer-KSA/

Survey

https://ibm.biz/BdfPax

Thank you for joining us today!

Asna Javed
Lead Developer Advocate, PAK

Asna.Javed1@ibm.com