

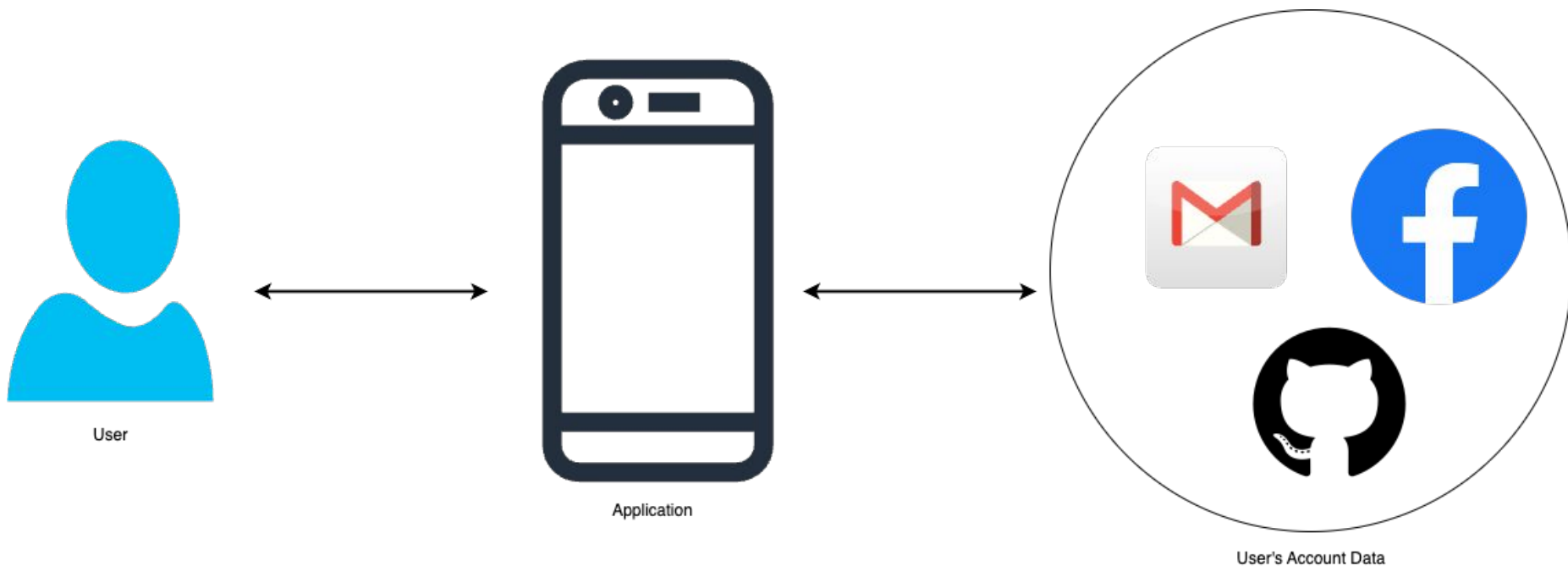
Introduction to OAuth 2.0

youtube.com/@java-rush



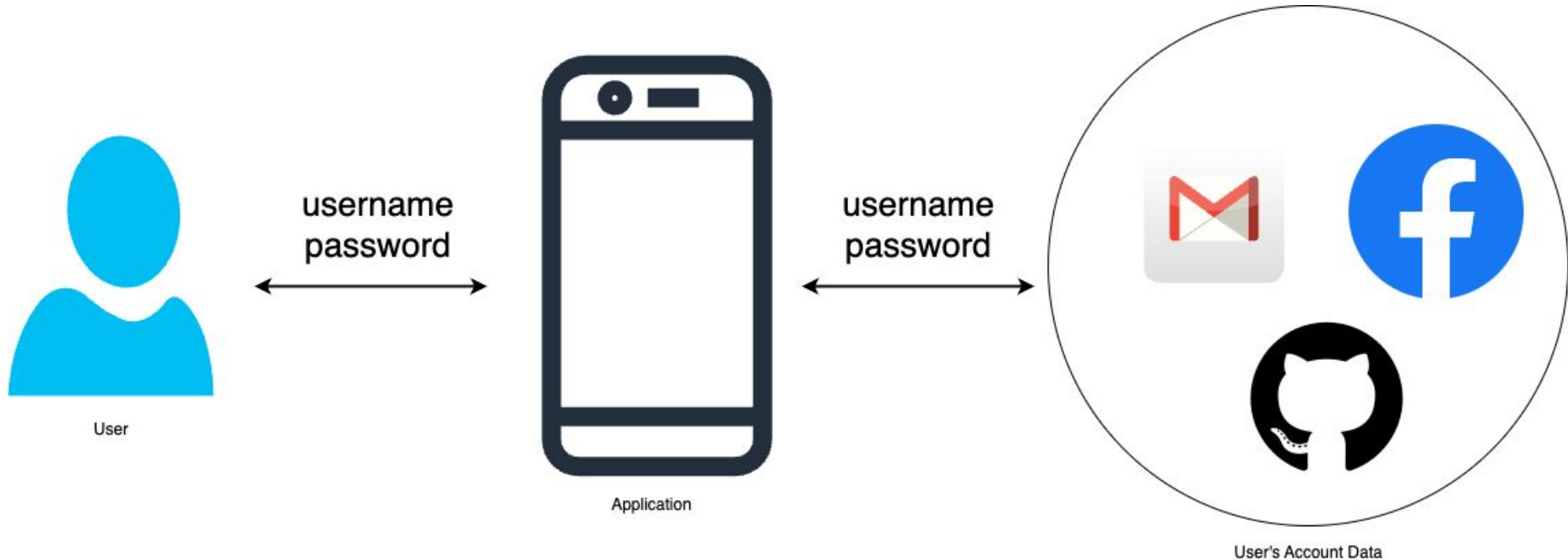
Goal

Enable the **application** to access user's **account** data.



Before OAuth

Give application username / password to the account





Problems

- Complete access to user's account
 - Can do anything (delete account, change password)
- Stores passwords in plain text
 - Other person can gain access to passwords
- You want to revoke access?
 - Change the password



Solution

- OAuth 1 
- OAuth 2 

Authentication vs Authorization

Authentication → Who are you?

Authorization → What access do you have?

Not Authenticated ⇒ 401 Unauthorized

Not Authorized ⇒ 403 Access Denied



Roles in OAuth 2

- Resource Owner
- Resource Server
- Authorization Server
- Client Application



Resource Owner

- The User
- Uses the application
- Who's resources application wants to access



Resource Server

- API Server
- Contains Resource Owner's (User's) data
- Validates **access tokens** 🔑



Authorization Server

- User's interaction point
- Grant Access Tokens
- Generally contains 2 urls
 - For authorization request
 - To grant access tokens
- May be same as the Resource Server
- OAuth Provider
- Identity Provider (if Authentication supported)



The Client

- Third party application
- Access User's resources
- Obtain permission from User
 - Using Authorization Server
- Types
 - Confidential Clients
 - Public Clients



Confidential Clients

- Stores `client_secret` confidentially
- Typically, runs on server
- Web apps
- Server side rendered websites

Public Clients

- Can not store client_secret secretly
- Secret not used
- Mobile Applications
- Javascript Applications
 - Standalone Angular, React, Vue...
- Anyone can view the source code of application

Access Token

- Issued by Authorization Server
- Used by The Client Application
 - To make authorized requests to Resource Server
- Contains
 - Expiry time
 - Scope
 - Other information...
- Meaningful to Resource & Authorization Server
- Types
 - Self contained
 - Key in database



Refresh Token

- To get a new access token
- Optional



Authorization Code

- Intermediate Token
- To get access token



OAuth 2.0 Clients - Server Side Apps