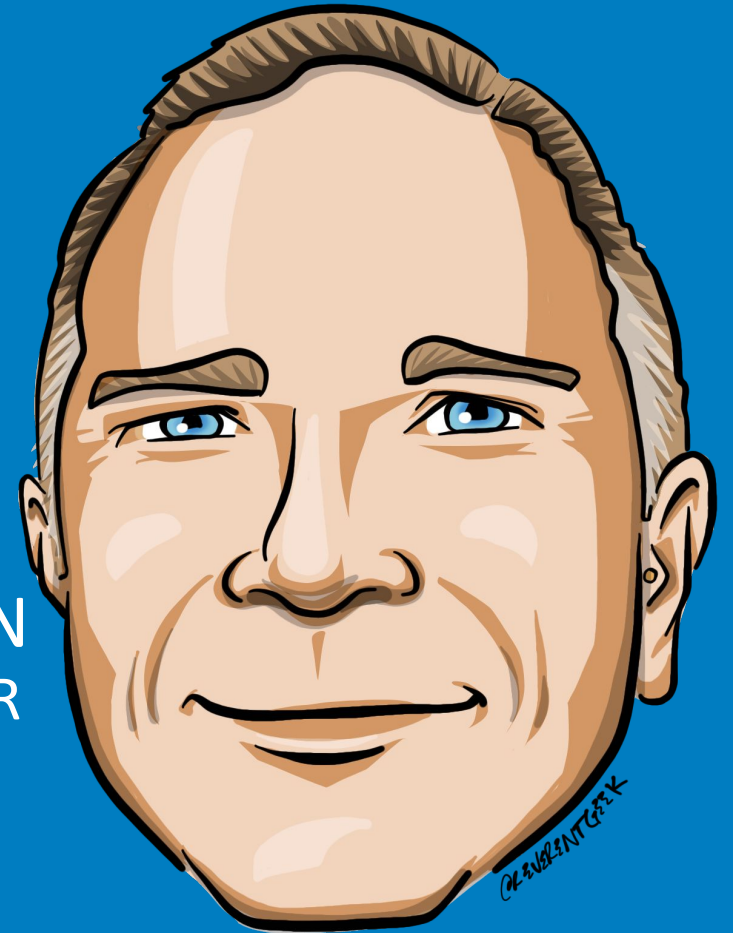


# Hacking OAuth: Pitfalls and Remedies

MICAH SILVERMAN  
Senior Security H@XOR  
@AFITNERD  
@OKTADEV



# Identity use cases (circa 2007)

- ★ Simple login – forms and cookies
- ★ Single sign-on across sites – SAML
- ★ Mobile app login – ???
- ★ Delegated authorization – ???

# Don't do it this way!

## Are your friends already on Yelp?

Many of your friends may already be here, now you can find out. Just log in and we'll display all your contacts, and you can select which ones to invite! And don't worry, we don't keep your email password or your friends' addresses. We loathe spam, too.

Your Email Service



Your Email Address

(e.g. bob@gmail.com)

Your Gmail Password

(The password you use to log into your Gmail email)

[Skip this step](#)

**Check Contacts**

# Don't do it this way!


Step 1  
Find Friends

Step 2  
Profile Information

Step 3  
Profile Picture

## Are your friends already on Facebook?


Many of your friends may already be here. Searching your email account is the fastest way to find your friends on Facebook.


 **Gmail**

Your Email:


Email Password:

[Find Friends](#)


 Facebook will not store your password.

 **Yahoo!**

[Find Friends](#)

 **Windows Live Hotmail**

[Find Friends](#)

 **Other Email Service**

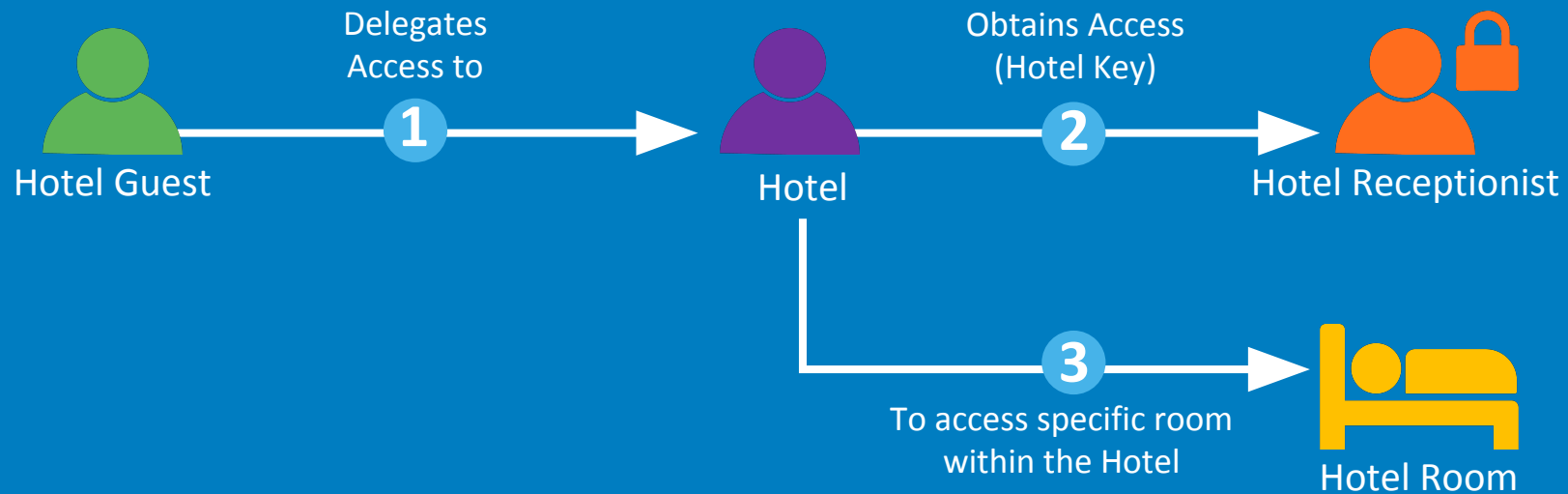
[Find Friends](#)

The delegated authorization problem  
HOW CAN I LET A WEBSITE ACCESS  
MY DATA, WITHOUT GIVING IT MY  
PASSWORD?

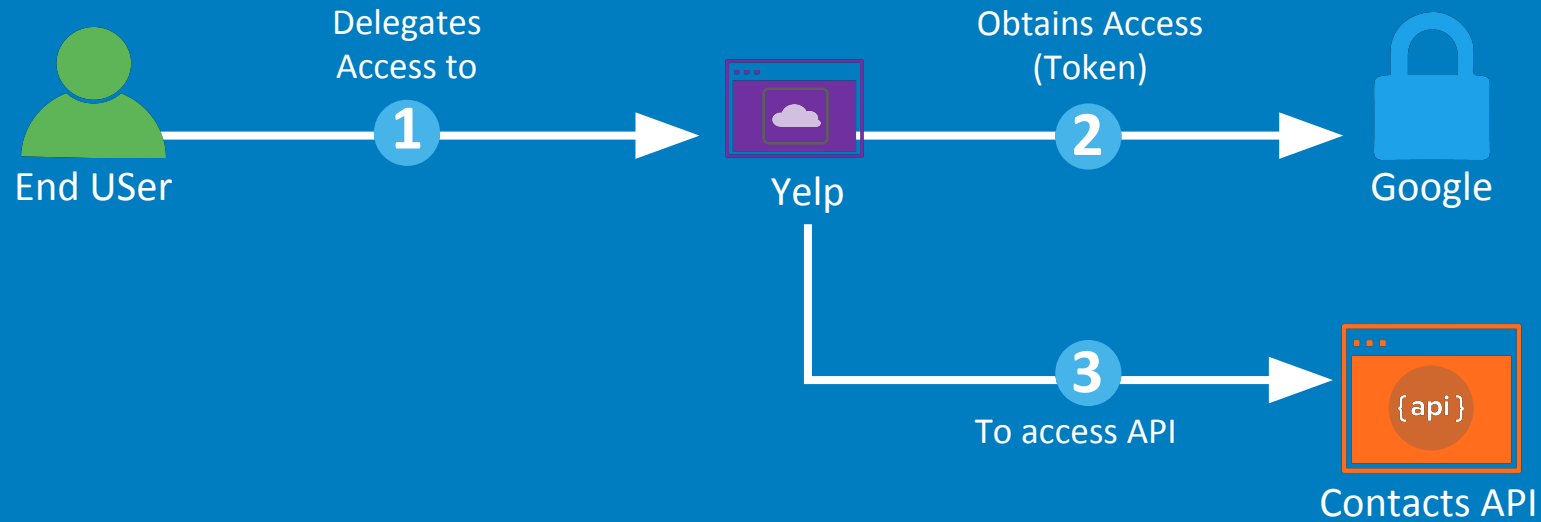
# A lot of confusion around OAuth:

- ✗ Terminology and jargon
- ✗ Incorrect advice
- ✗ Hard to find a life-like example

# Hotel Analogy



# OAuth: App Scenario





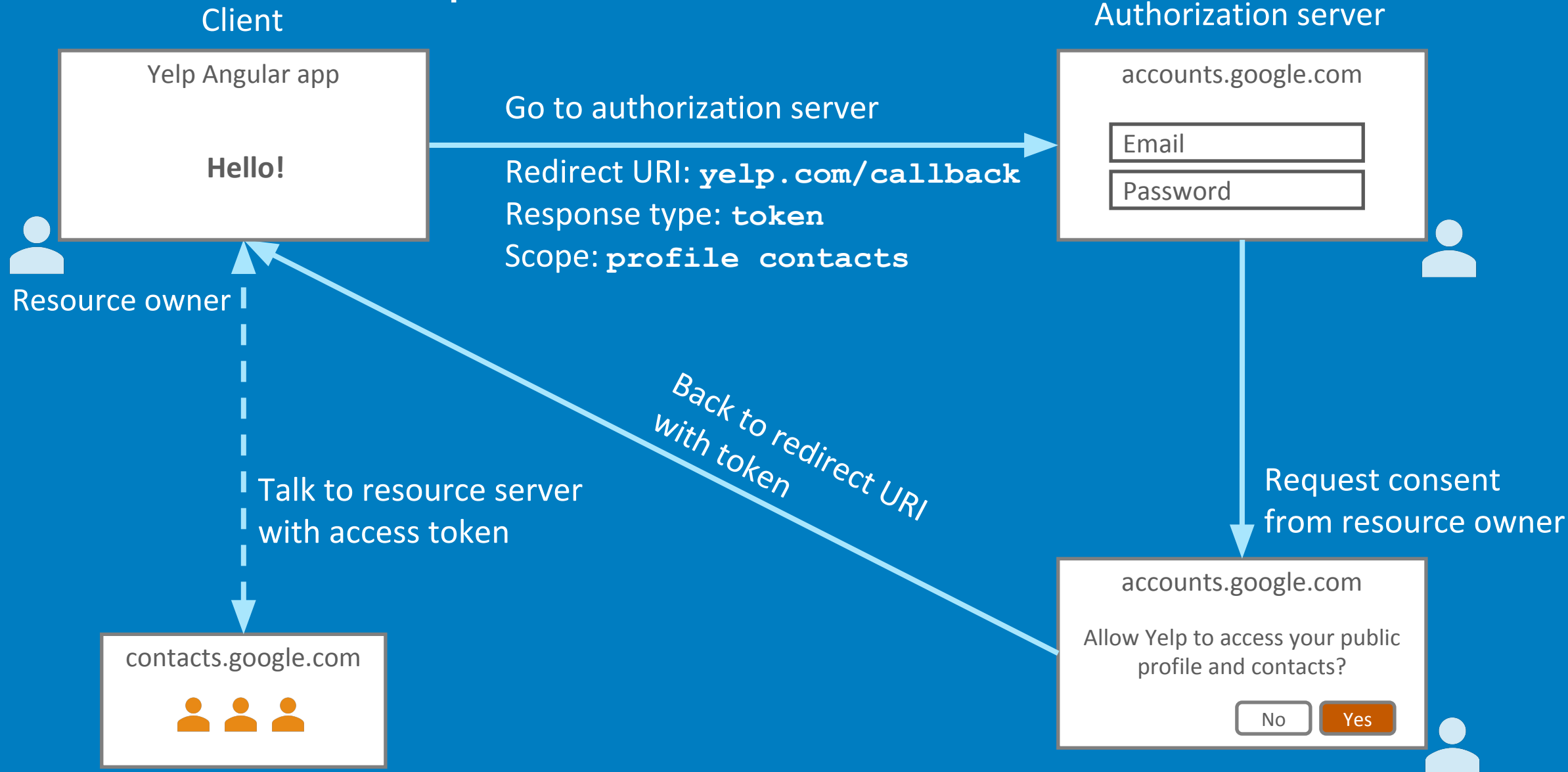
# OAuth 2.0 Terminology

Hotel	App	OAuth	Description
Hotel Guest	End User	Resource Owner	Wants a Client App to do something on their behalf
Hotel	Yelp	Client Application	Needs authorization to interact with an API on behalf of a user
Hotel Receptionist	Google	Authorization Server	Grants access (in the form of tokens) to an app
Hotel Room	Contacts API	Resource Server	Has an API that an app can use if presented with a token

# Delegated authorization with OAuth 2.0



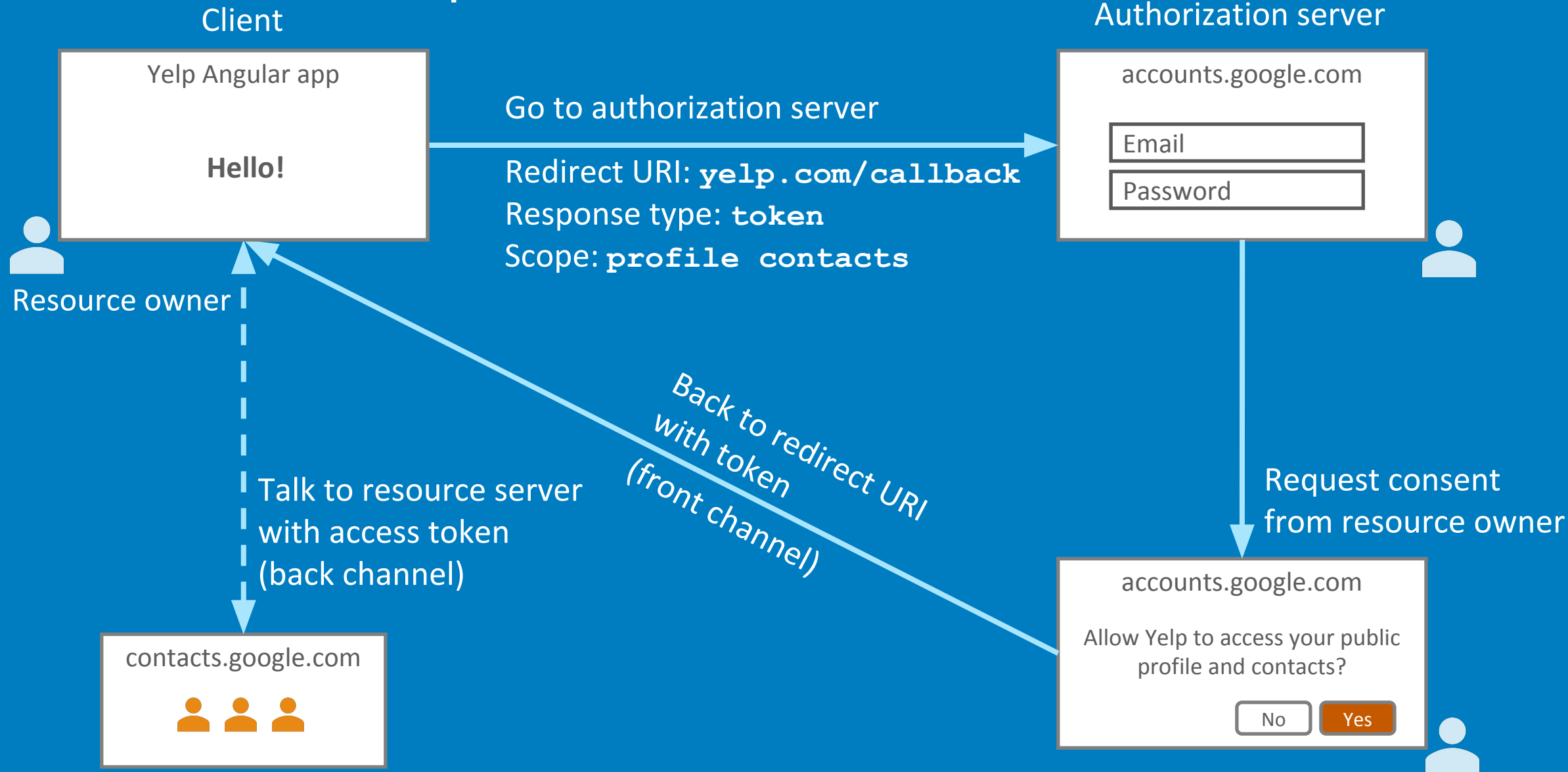
# OAuth 2.0 implicit flow



# More OAuth 2.0 terminology

- ★ Back channel (highly secure channel)
- ★ Front channel (less secure channel)

# OAuth 2.0 implicit flow



# DEMO

## Implicit Flow Detector

# Confidential Clients



## Application running on a server

Has the ability to keep strings secret  
since code is running in a trusted environment

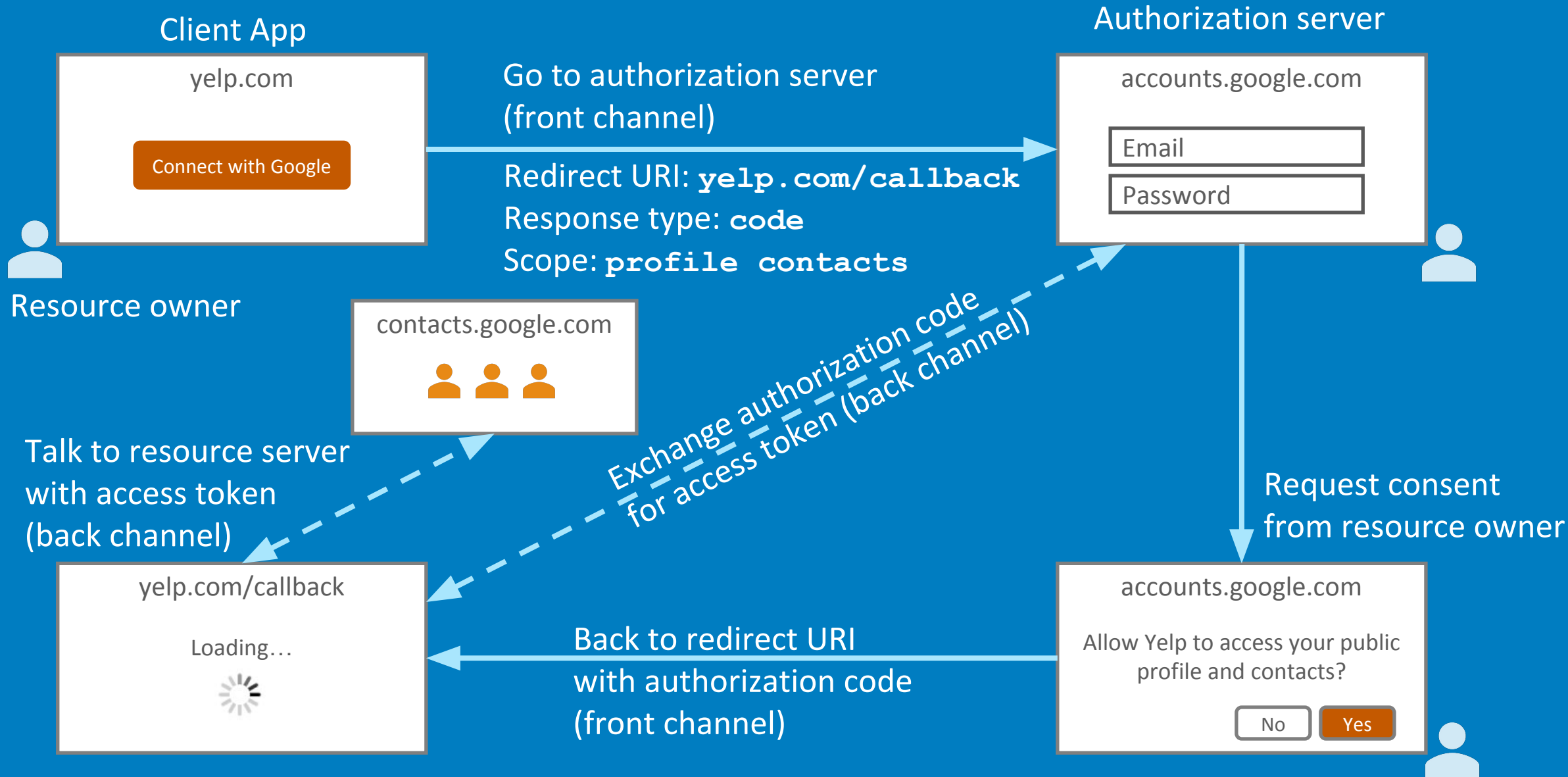
# Public Clients



## The application can't keep strings secret

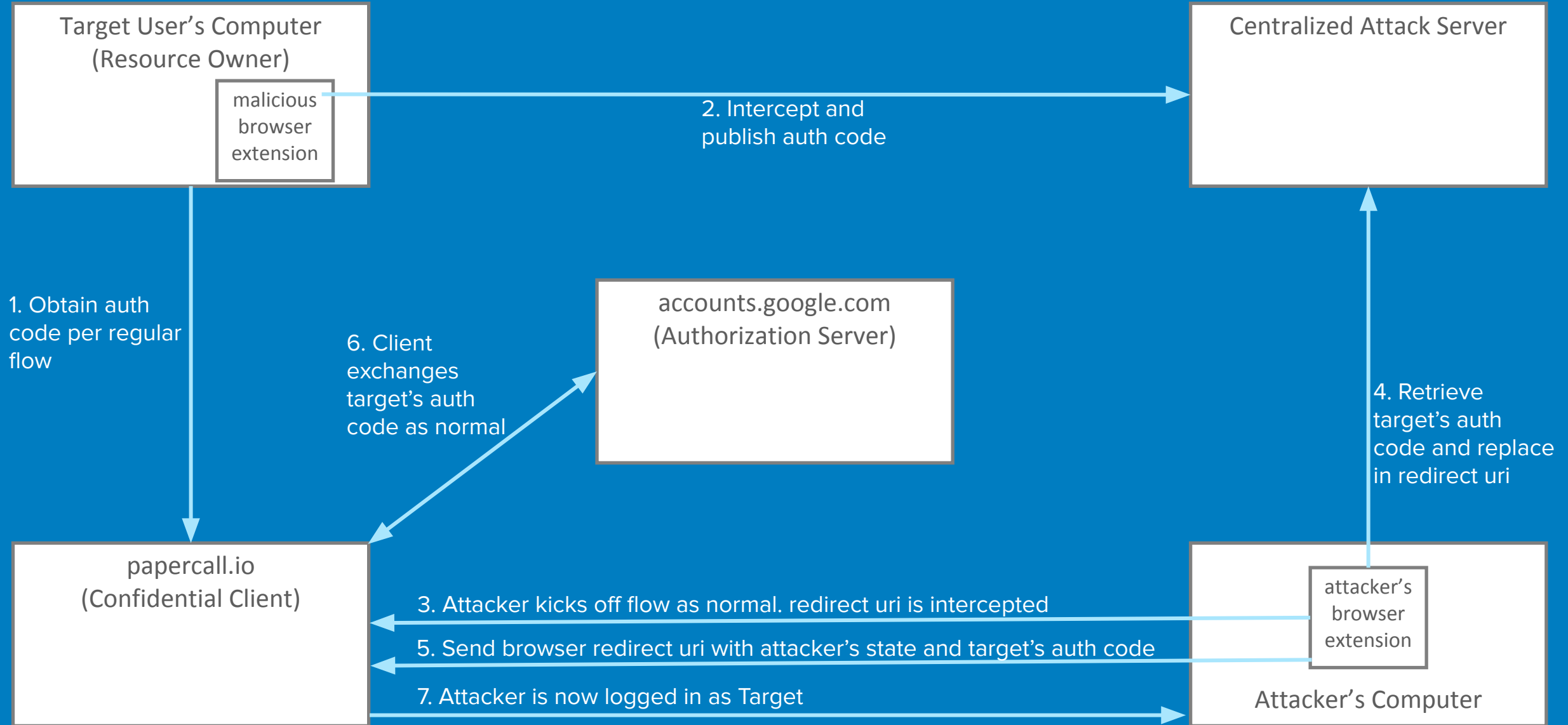
Javascript/Single-Page apps: “view source”  
Native apps: decompile and extract strings

# OAuth 2.0 authorization code flow



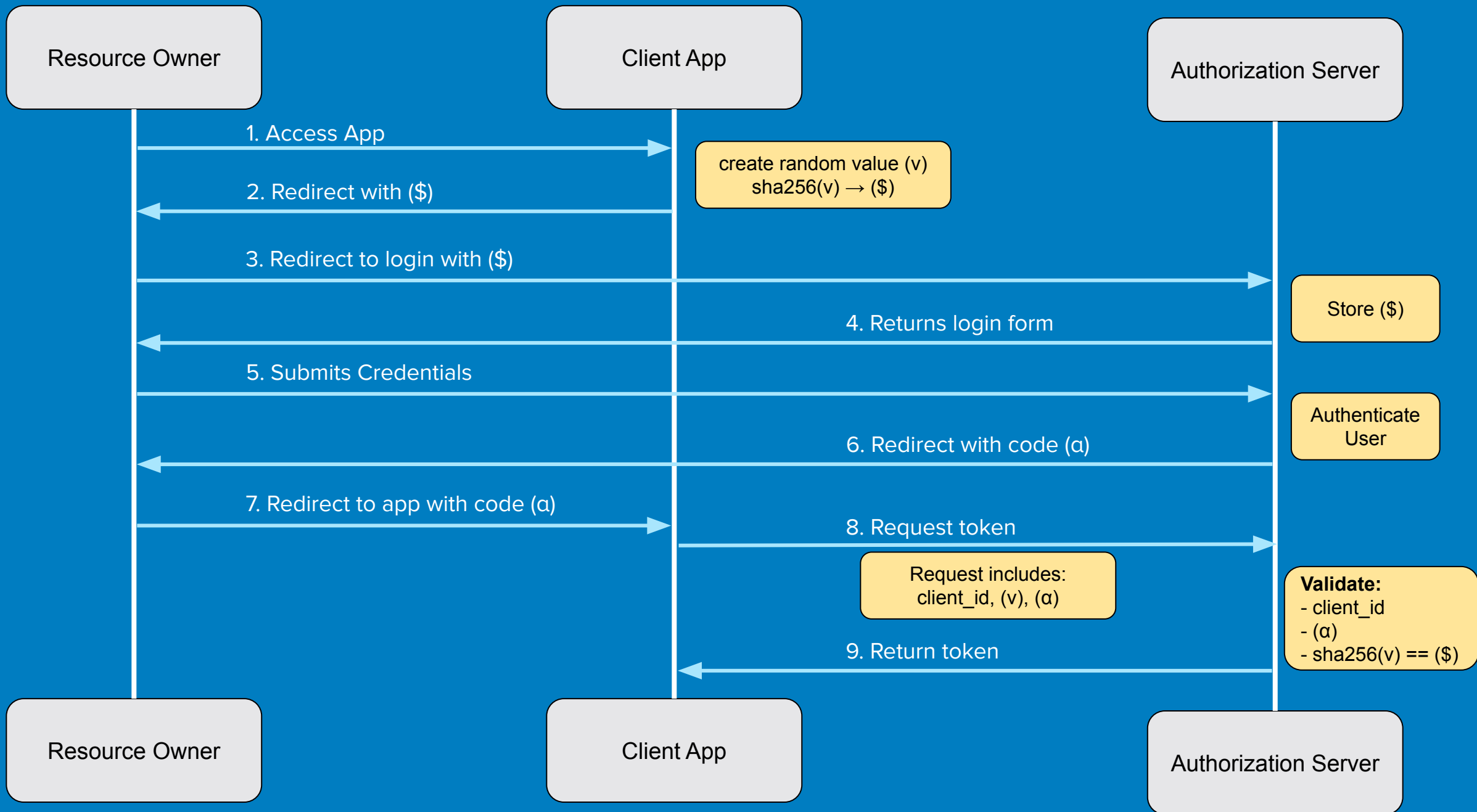


# Authorization Code Injection Attack



# DEMO

## Auth Code Injection





# DEMO

PKCE

Auth Code Injection: Foiled

Micah Silverman  
@afitnerd

oauth.com  
@oktadev

Free hosted authorization server:  
**developer.okta.com**