

OAuth and OpenID Connect in plain English

... in less than 20 minutes
with Nate Barbettini

There's a lot of confusion about OAuth.

- Difficult terminology and jargon
- Incorrect advice

To understand the how,
we need to understand the why.

The delegated authorization problem

How can I let a website access my data without giving up my password?

Are your friends already on Yelp?

Many of your friends may already be here, now we 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

ima.t.k.guy@gmail.com (e.g. bob@gmail.com)

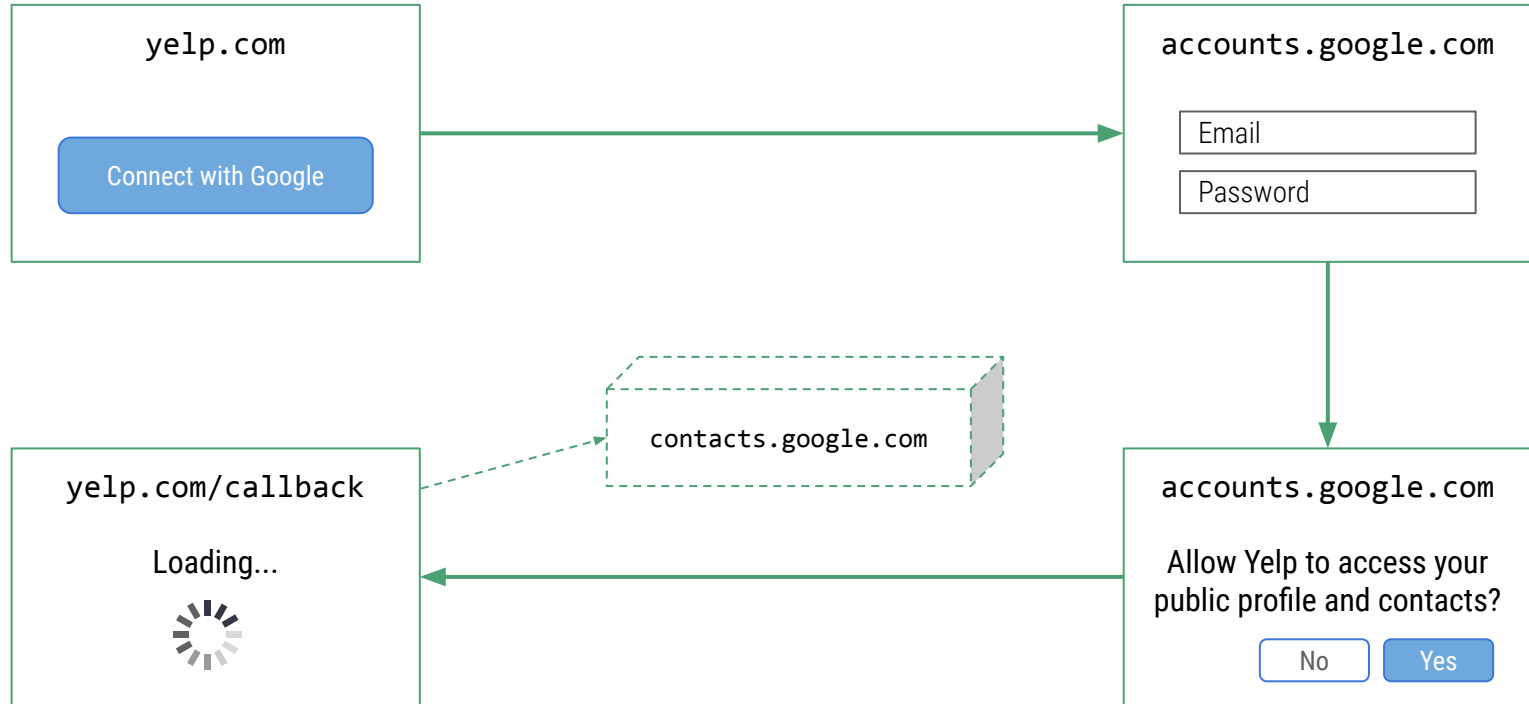
Your Gmail Password

..... (the password you use to log into your Gmail email)

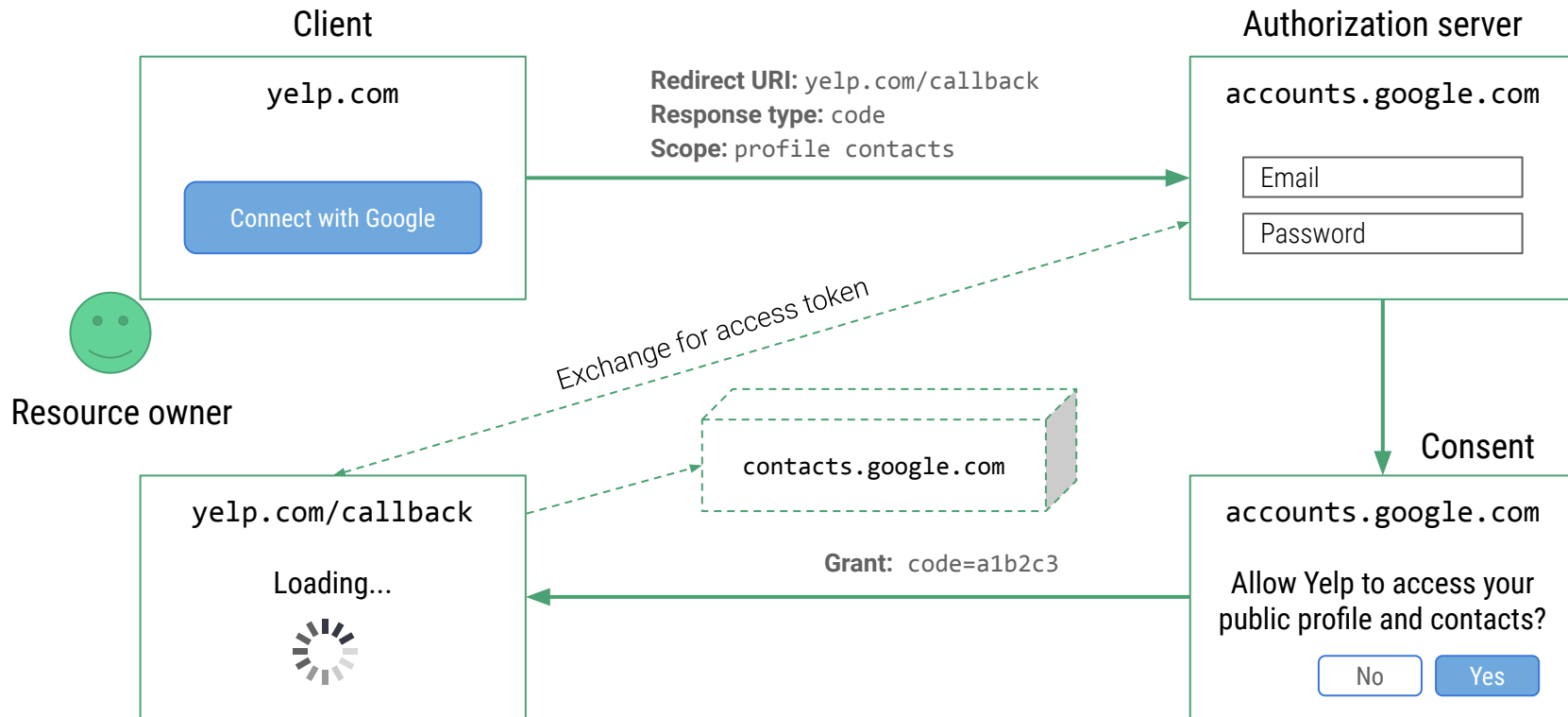
[Skip this step](#)

[Check Contacts](#)

Delegated authorization with OAuth 2.0



Delegated authorization with OAuth 2.0



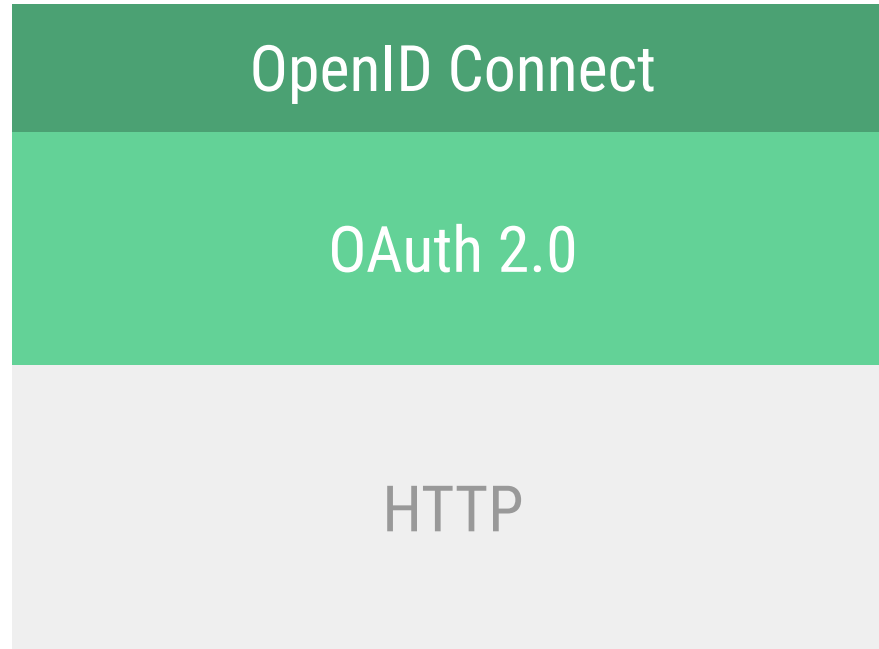
What happened next?

- OAuth 2.0 became widely adopted for authorization.
- Facebook and others introduced social login (using OAuth 2.0 under the hood)

New problem: Not good for authentication.

No standard way to get the user's profile info.

OAuth 2.0 and OpenID Connect



Current practice

- Asking for permissions -- OAuth 2.0
- Authentication and single-sign on -- OpenID Connect

Questions?

Long version: <https://oauthacademy.com/talk>

Twitter: @nbarbettini