Authentication and Authorization

Basic Concepts

Authenticate & Authorize

- **Authentication** - validate the identity of a "user", agent, or process
- **Authorization** - specifying rights to access a resource

Authentication is responsible for identifying who the user is.

Authorization is responsible for deciding what the user has permission to do.

Other Aspects of Security

- Access Control - controls access to resources
- Data Integrity - prevent data from being modified or corrupted, and *prove* that data hasn't been modified
- Confidentiality & Privacy - privacy is about people, confidentiality is about data
- Non-repudiation - prove that user has made a request
  - "repudiate" means to *deny* having done something
- Auditing - make a tamper-resistant record of security related events

Authentication Methods

Authentication methods for humans:

1. Username & password

2. Username & one-time password (TOTP, codes, SMS)

3. Biometrics - fingerprint, facial recognition, iris scan

4. Trusted 3rd Party - OAuth and OpenID
   "Login with Google" or "Login with Facebook"

5. Public-Private Keys

6. Passkeys

7. SQRL - similar to Passkeys (maybe better), by Steve Gibson

Mantra of Authentication

Use at least 2 of these...

Something you ____________

- *a username and password*

Something you ____________

- *key card, registered mobile phone*

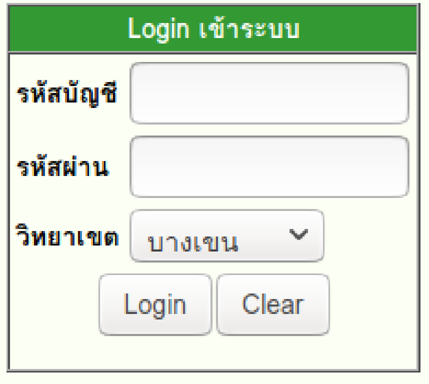
Something you ____________

- *finger print, face, iris pattern*

Username & Password

The oldest and one of the worst authentication methods.

KU



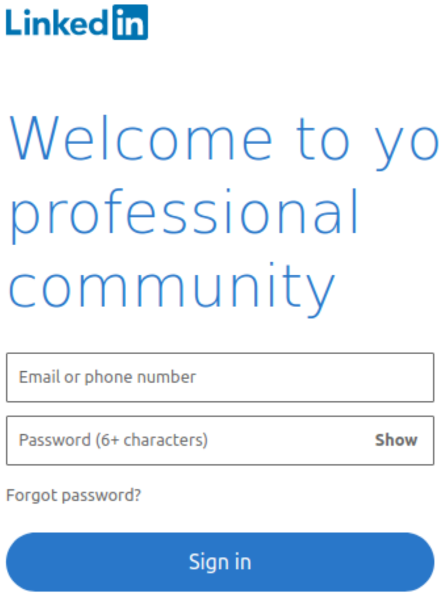
Login เข้าระบบ

รหัสบัญชี

รหัสผ่าน

วิทยาเขต บางเขน

Login Clear



LinkedIn

Welcome to yo professional community

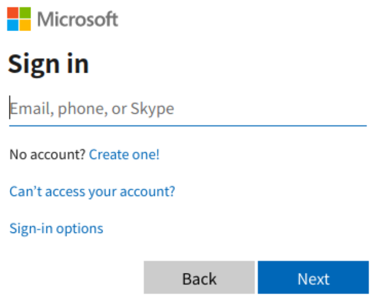
Email or phone number

Password (6+ characters) Show

Forgot password?

Sign in

Two page design



Microsoft

Sign in

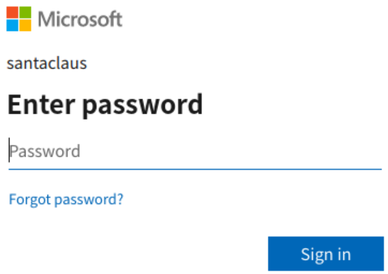
Email, phone, or Skype

No account? Create one!

Can't access your account?

Sign-in options

Back Next



Microsoft

santaclaus

Enter password

Password

Forgot password?

Sign in

Username & Password

Passwords are not secure (obviously)

- can be stolen
- can be guessed or "brute forced"
- vulnerable to man-in-the-middle & replay attack
- people reuse passwords or use weak passwords

Exercise: Have You Been Pwned?

Has your email address (and data) been stolen?

`https://haveibeenpwned.com/`

Has your **password** been seen in a data breach?

`https://haveibeenpwned.com/Passwords`

Key Observation about Passwords

- password is not using the *computational ability* of the user's device. It's just a fixed string.

- with just *a little computation ability* we can create a much more secure protocols
  (like challenge - response)

Public-Private Key Algorithms

Public-private key pairs: Uses RSA (large prime numbers) or Elliptic Curves (Ecliptic Curve Cryptography)

Private key:	Public key:
p(m)	P(m)

m = a *message* to send

p(m) and P(m) are inverse:

P(p(m)) --> m

p(P(m)) --> m

PKI = public key infrastructure

Public-Private Auth Example

1. You connect to a server and give your username.

2. Server looks up your public key (P) and chooses a
   random message: **m1**

3. Server encrypts m1 with your public key:
   challenge = P(m1)

4. Server sends *challenge* to you and says:
   "*if this is really who you claim to be, then
   decrypt this challenge and send it back.*"

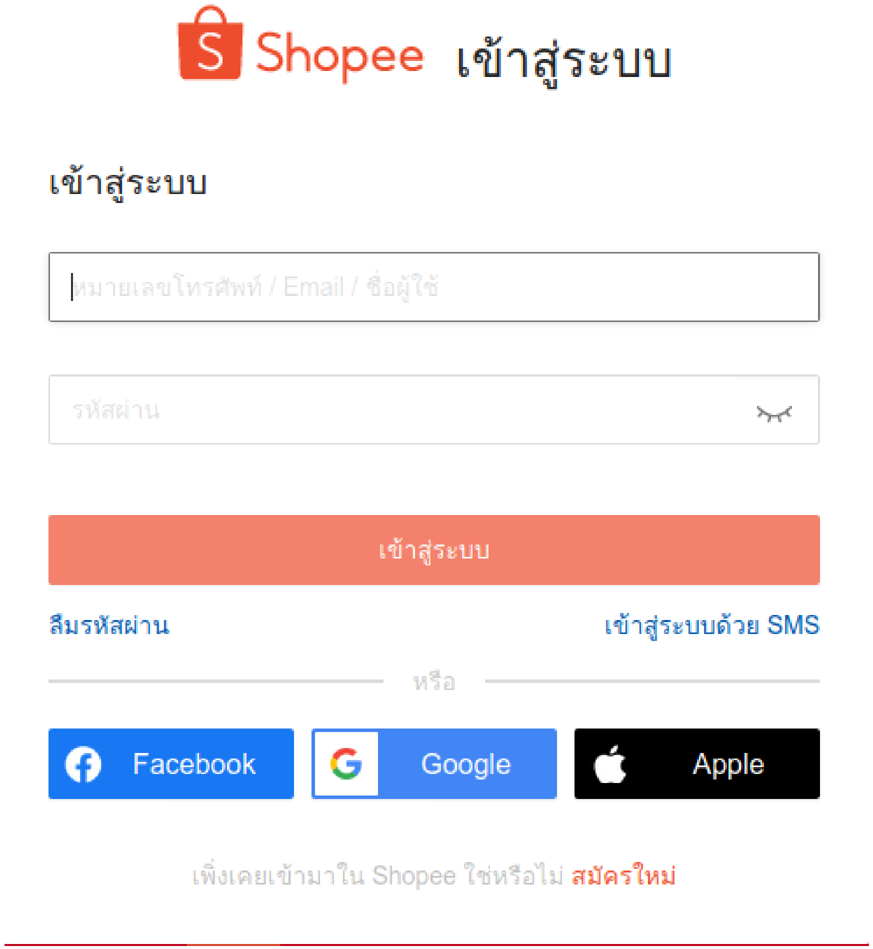
5. You decrypt the challenge: m2 = p(*challenge*)

5. You *encrypt* and return a response = p(m2 + 1)

6. Server checks response: P(response) == m1 + 1 ??

OAuth & OpenID

Use a 3rd party to validate the user's identity



Shopee เข้าสู่ระบบ

เข้าสู่ระบบ

หมายเลขโทรศัพท์ / Email / ชื่อผู้ใช้

รหัสผ่าน

เข้าสู่ระบบ

ลืมรหัสผ่าน

เข้าสู่ระบบด้วย SMS

หรือ

Facebook

Google

Apple

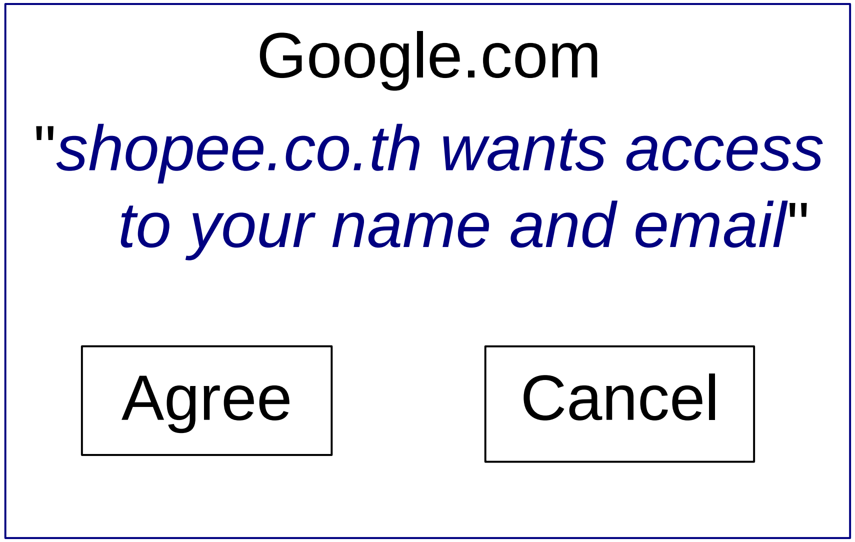
เพิ่งเคยเข้ามาใน Shopee ใช่หรือไม่ สมัครใหม่

OAuth providers →

OAuth 2.0

You choose "Google".

Shopee ***redirects*** you to Google (may open a pop-up):



Google.com

"*shopee.co.th wants access to your name and email*"

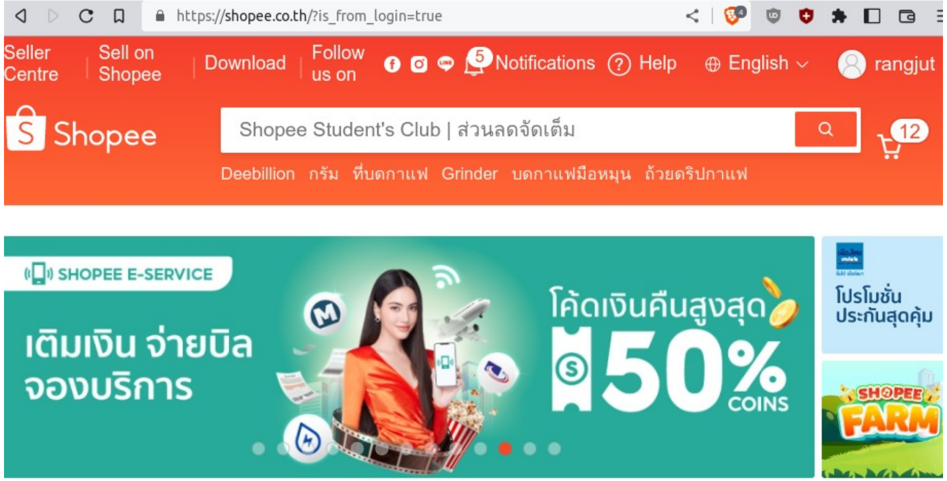
- tells Shopee who you are (grant access to your name & email),
  and **proves** that you have authenticated yourself to Google.

After You Approve...

You are *redirected* back to Shopee (the client).

What happened?

- Google gave your browser an "authorization code", & redirected the browser to Shopee "callback address"
- Shopee used the "authorization code" to get an "access token" to access your resources
- Shopee uses Google API and the "access token" to get your name and email address.

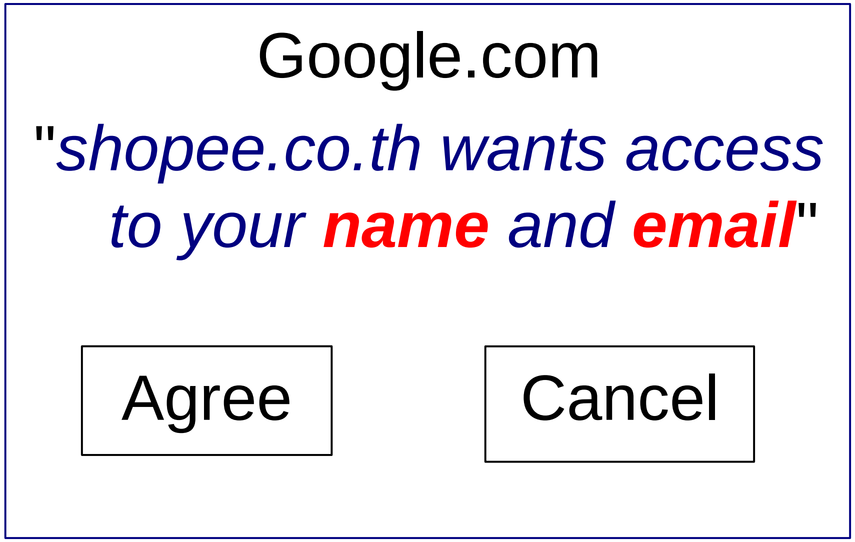


https://shopee.co.th/?is_from_login=true

OAuth is for Authorization

OAuth is *really* about granting access to resources.

But, as a side effect, you confirm your identity.



Google.com

"*shopee.co.th wants access to your **name** and **email***"

What Happened?

When you click "Login with Google",
what happens *behind the scene*?

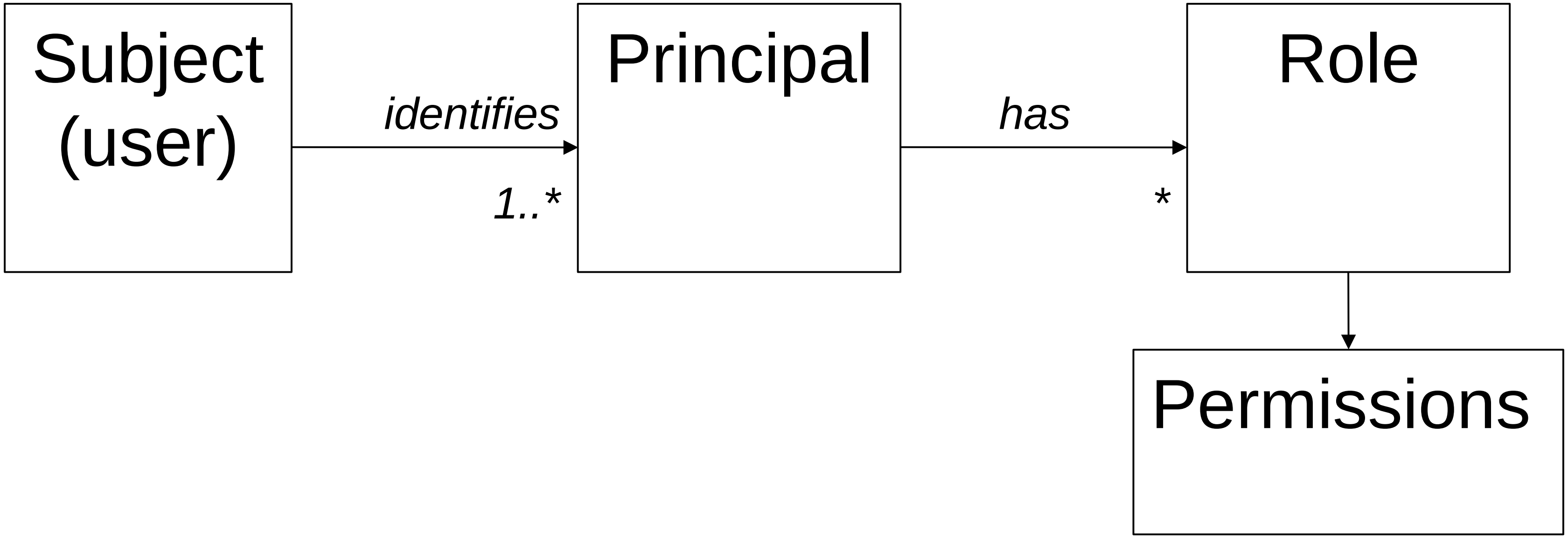
details in OAuth presentation

Role Based Authorization

Permissions are based on the ***roles*** a user possesses.

A user may have many roles.

Example: “joe” has roles “voter” and “administrator”


Subject (user)
identifies
1..*
Principal
has
*
Role
Permissions