Authentication

Web Dev, Spring 2021

Last time....

HTTP is a stateless protocol

So any session state must be maintained manually

Cookies: storage on the browser, can be read + updated by server

Can maintain session state on the browser directly in a cookie

Can maintain session state on the server keyed by a sessionId stored in a cookie

Authentication

Intuitively:

- provide credentials to a server to prove that you are who you claim you are

How do you prove your identity?

- know a secret (password)
- possess a unique device (authentication token)
- biometrics

Authentication

Implementing authentication in a system is a two-steps process:

1. Prove your identity once at the beginning
2. Keep a token that shows you've proved your identity

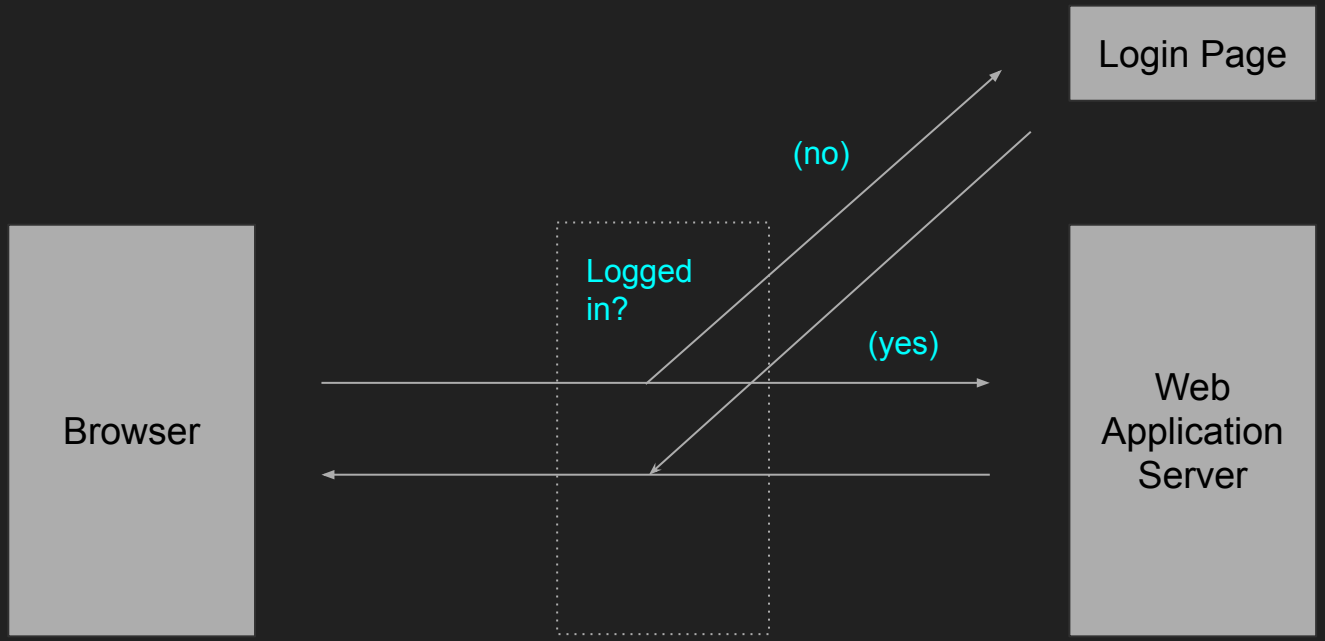
Proving your identity:

- page that lets you enter credentials

Token:

- cookie that you can only have if you've proved your identity

Common setup



Session authentication versus token authentication

Same question as last time:

- do we keep authentication information on the browser (token auth)
  - generally done with JWT (JSON Web Token)
  - useful for SSO [login to one site, provide access to other sites]

- or do we keep authentication information on the server (session auth)
  - session state kept on the server
  - sessionId kept in the browser

Demo

Content of session cookie:
- *sessionId*

Session state on the browser:
- for each sessionId:
  - *name of (authenticated) user*
  - *set of visited pictures*

A user is authenticated if they have a session cookie with a valid sessionId