Mashups (continued)

- We don't want to share our password with the Mashup server
  - So we want our browser to talk directly to server A and server B
- Same Origin Policy is an issue
  - JS loaded from Mashup can only open connections back to the mashup server
  - We can have the mashup server give us a script which is src'd from service A\B
    - Like a dynamically linked library
  - We can use iframes
    - An iframe is like a separate web page within a webpage
    - Cannot have cross iframe communication

HTML5 Post Message

- Allows iframes to send each other messages
- Browser tells receiving iframe where message came from (which website the iframe was embedded in)
  - Browser provides ID of message sender

Overview of Defenses To Discuss

- Design
  - eg. Separation of privilege
- Coding
  - eg. ban sql.query
  - automatic code auditing
- Testing
  - eg. Fuzzing
- Prevent bug from being exploited
  - Like ASLR
- Damage Mitigation
  - eg. IDS, chroot jails, VMs, etc