

# software studio

**the web as a platform  
for distributed computing**

**Daniel Jackson**

# client/server, documents only



client browser

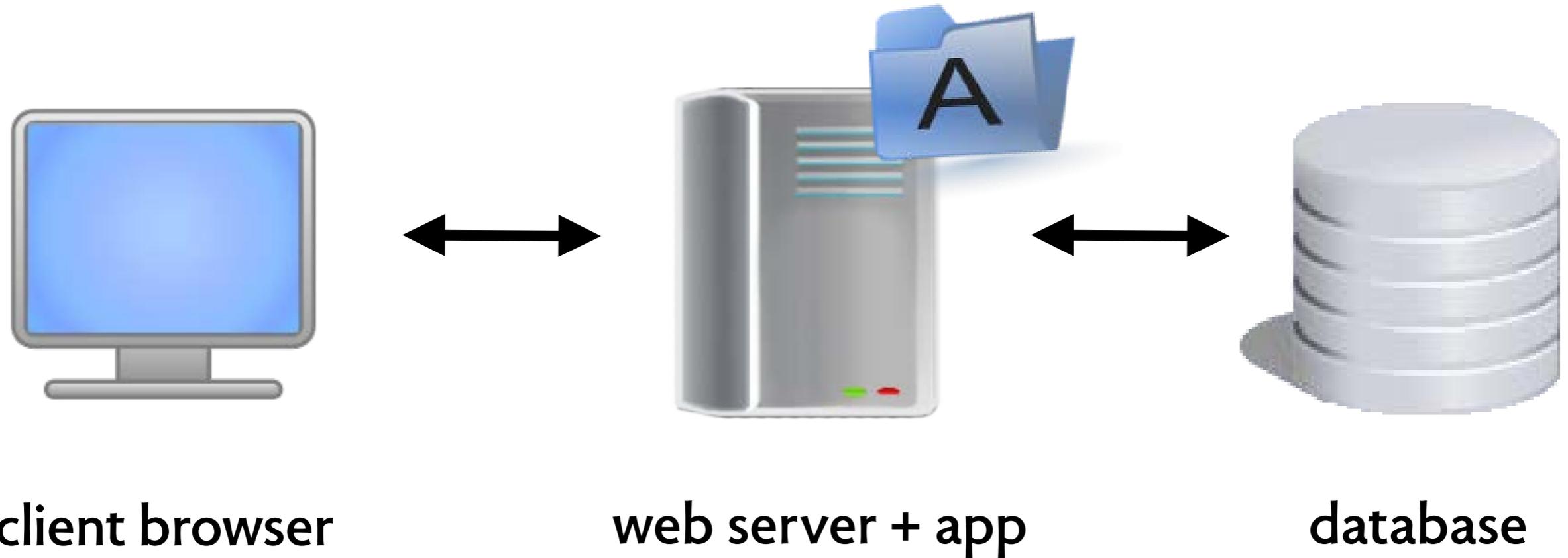


web server

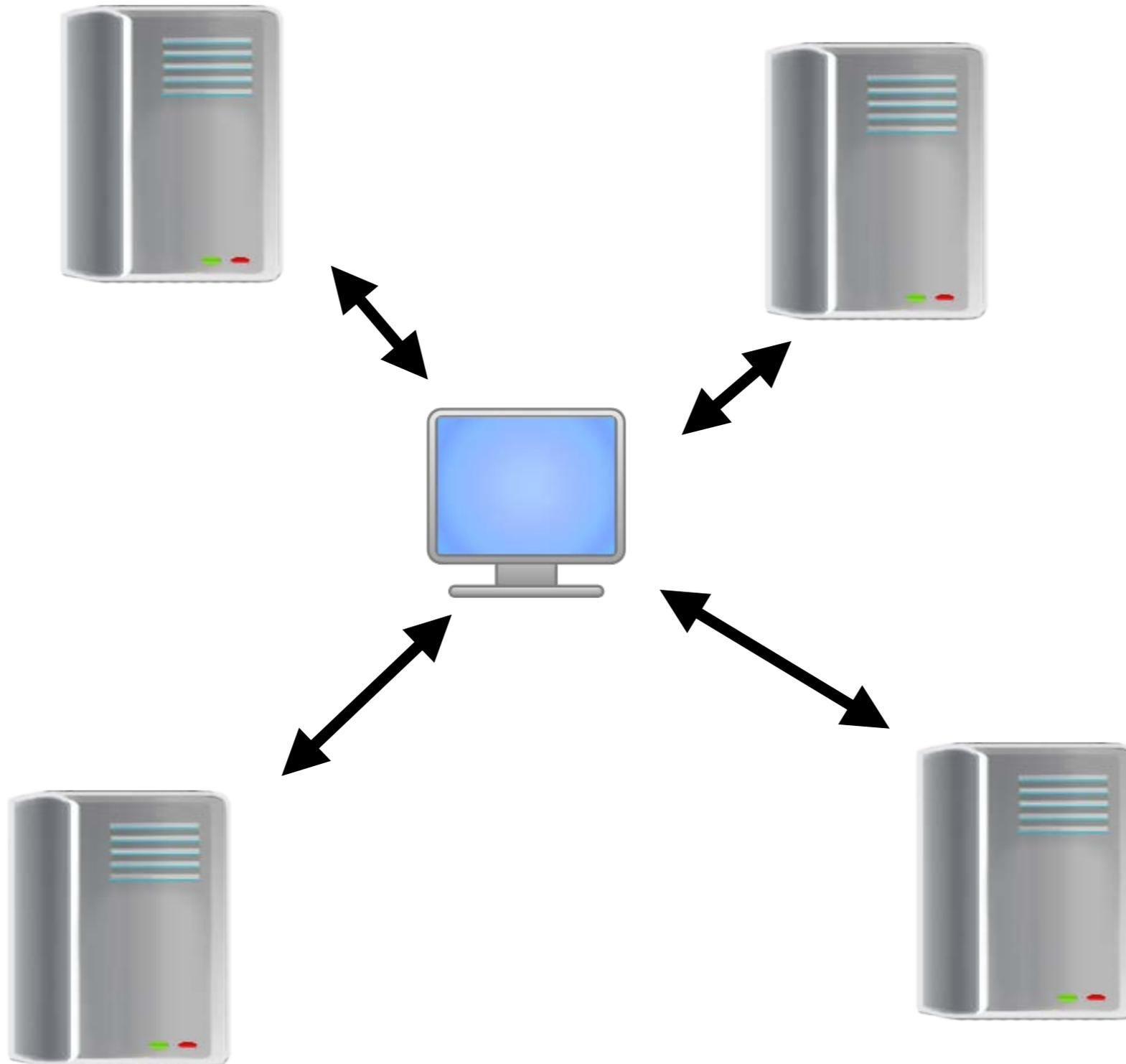


file system

# client/server, server apps



# client/server, multiple servers



The screenshot shows the 29travels website interface. At the top, there's a navigation bar with 'Home', 'Africa', 'Asia', 'Australia/Oceania', 'Europe', 'North America', 'South America/Caribbean', and 'USA'. Below this is a 'Nearby' section with a list of countries: Australia, New Zealand, Papua New Guinea, Tonga, and New Caledonia. A 'Map' section shows a map of Fiji with labels for Lautoka, Nadi, and Suva. The main content area is titled 'Fiji' and includes an 'Overview' section with text about the country's location and climate. Below the overview is a 'Best Sellers in Books' section featuring several book covers like 'Italy 2013', 'Crossing the Heart of Africa', and 'Wild'. At the bottom, there's a 'Fiji Flickr Photos' section displaying a grid of images. On the right side of the page, there are social media links for Twitter, Facebook, and Google Translate. The bottom of the page has a copyright notice for 29travels.

Twitter

Facebook

Google translate

Wikitravel

Google Maps

Amazon

Flickr

# client/server, client apps



client browser + app

web server + app

database

*client app uses web service API*

# Nano Quiz #1: Separation of Concerns, MVC

File Edit View Insert Responses (58) Help

Theme... View responses View live form

Page 1 of 1

## 6.170 Nano Quiz No. 1

Topics: Separation of Concerns, Model-View-Controller Design  
Date: Feb 11, 2013

First Name \*

Last Name \*

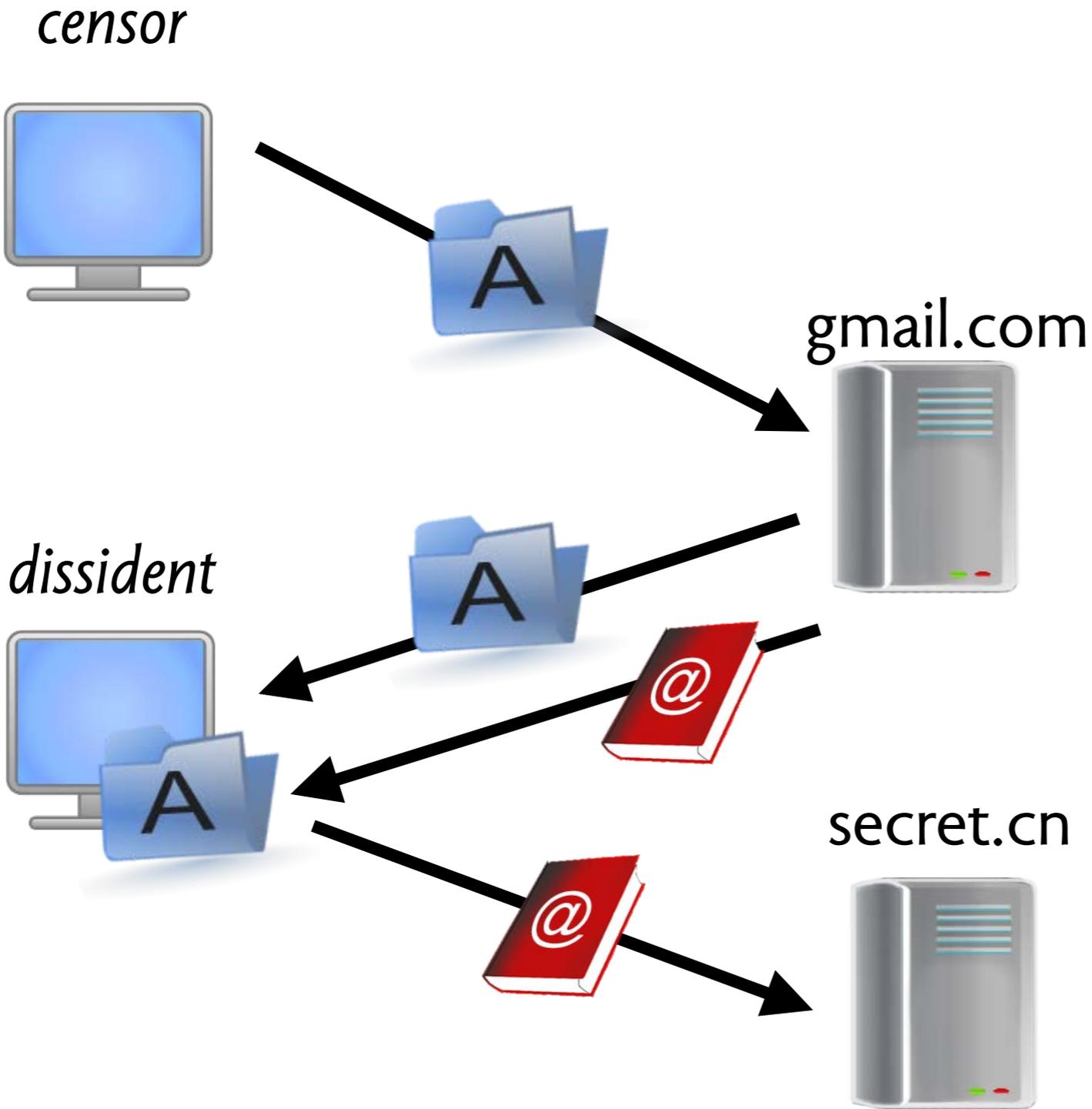
Athena Username \*

Which of the following best illustrates an example of "scientific thought" as advocated by Dijkstra?

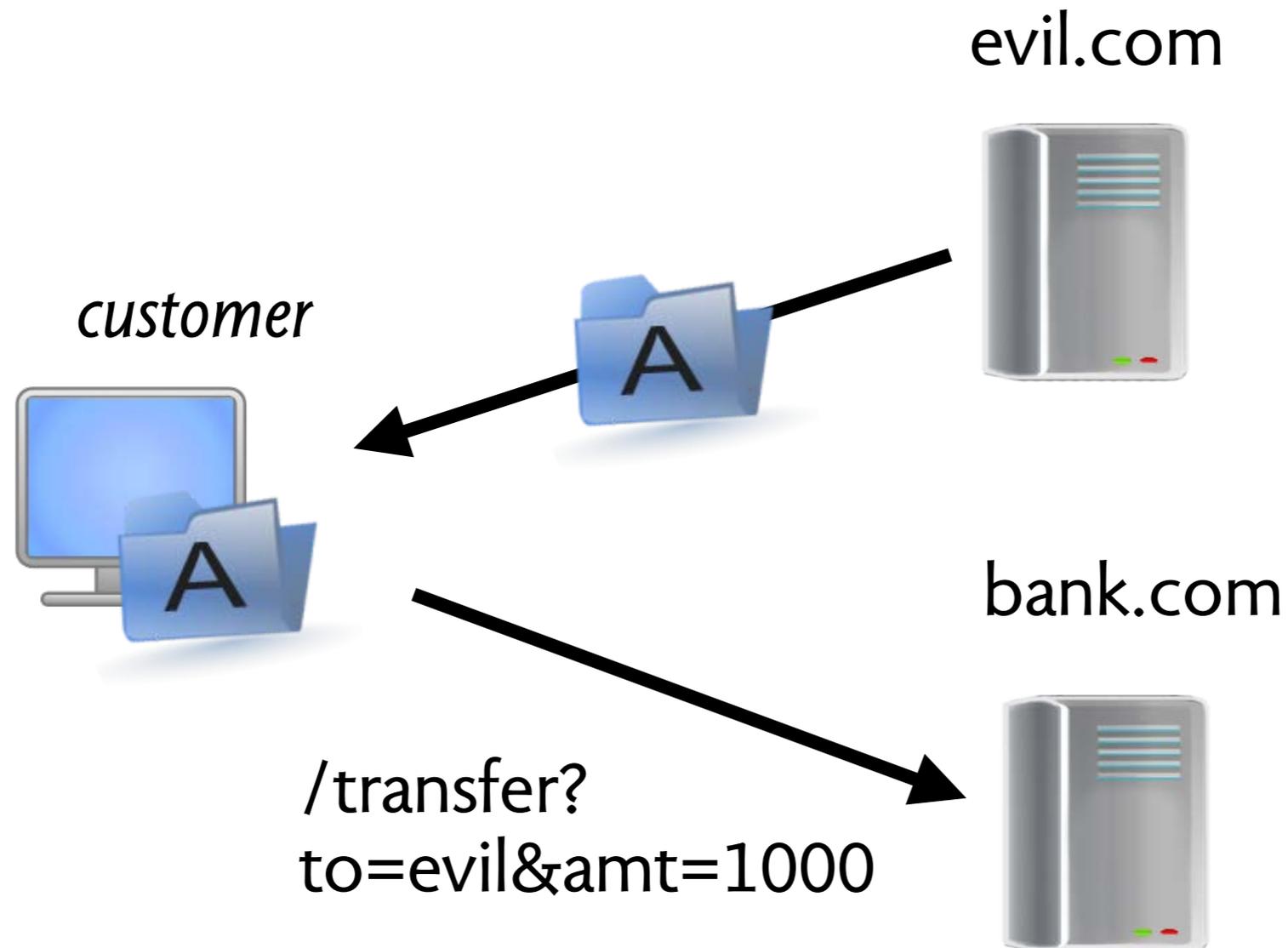
- Collecting a large set of data to show that coffee has negative effects on health
- Weighing the trade-offs between Java and C++ for your next project
- Constructing a cogent argument against your opponents in a political debate
- Delaying the performance optimization of your new web site until it functions correctly

<span>Elements</span> <span>Resources</span> <span>Network</span> <span>Sources</span> <span>Timeline</span> <span>Profiles</span> <span>Audits</span> <span>Console</span>							
Name Path	Method	Status Text	Type	Initiator	Size Content	Time Latency	Timeline
<b>edit</b> /forms/d/1ZB8fr4ye8bsbXnAgQY4w_wk_s7D	GET	200 OK	text/html	Other	0B 75.29KB	106ms 90ms	
<b>3169340563-formeditor_ltr.css</b> /static/forms/client/css	GET	200 OK	text/css	<u>edit:35</u> Parser	0B 120.33KB	31ms 22ms	
<b>2986332158-formeditor_prd.js</b> /static/forms/client/js	GET	200 OK	text/javascr...	<u>edit:35</u> Parser	0B 704.09KB	115ms 30ms	
<b>checkmark_2x.png</b> ssl.gstatic.com/ui/v1/menu	GET	200 OK	image/png	<u>edit:36</u> Parser	0B 358B	213ms 98ms	
<b>helpBubble1.png</b> ssl.gstatic.com/ac/common	GET	200 OK	image/png	<u>edit:36</u> Parser	0B 306B	213ms 98ms	
<b>photo.jpg</b> lh6.googleusercontent.com/-hCcelX3_RqE/A	GET	200 OK	image/png	<u>edit:36</u> Parser	0B 640B	207ms 83ms	
<b>k2_aca6bcc6.png</b> ssl.gstatic.com/gb/images	GET	200 OK	image/png	<u>edit:36</u> Parser	0B 33.00KB	202ms 74ms	
<b>jfk_sprite_hdpi18.png</b> ssl.gstatic.com/docs/common	GET	200 OK	image/png	<u>edit:36</u> Parser	0B 54.31KB	203ms 80ms	
<b>peruserchrome?id=1ZB8fr4ye8bsbXnAgQY</b> /forms/d/1ZB8fr4ye8bsbXnAgQY4w_wk_s7D	GET	200 OK	application/...	<u>2986332158-formeditor</u> Script	0B 182B	1.52s 1.52s	
<b>getresponsecount?sid=49222550666bf9bc</b> /forms/d/1ZB8fr4ye8bsbXnAgQY4w_wk_s7D	GET	200 OK	application/...	<u>2986332158-formeditor</u> Script	0B 28B	122ms 55ms	
<b>read?id=1ZB8fr4ye8bsbXnAgQY4w_wk_s7I</b> /forms/d/1ZB8fr4ye8bsbXnAgQY4w_wk_s7D	GET	200 OK	application/...	<u>2986332158-formeditor</u> Script	0B 22B	118ms 49ms	
<b>about:blank</b>	GET	Success	text/html	<u>2986332158-formeditor</u> Script	13B 0B	2ms 0ms	
<b>share?id=1ZB8fr4ye8bsbXnAgQY4w_wk_s;</b> /e	GET	(canceled)	text/html	Other	355B 0B	389ms 381ms	
<b>csi?v=3&amp;s=freebird&amp;action=edit&amp;it=dns_.</b> csi.gstatic.com	GET	204 No Content	image/gif	<u>edit:40</u> Script	258B 0B	402ms 402ms	
<b>spinner.gif</b> ssl.gstatic.com/docs/spreadsheets	GET	200 OK	image/gif	<u>2986332158-formeditor</u> Script	0B 1.42KB	72ms 18ms	
<b>checkmark.png</b>	GET	200 OK	image/png	<u>2986332158-formeditor</u> Script	0B	72ms	

# cross site scripting (XSS)



# cross site request forgery (CSRF)



# mitigating attacks

## to prevent XSS

- › sanitization (in server)
- › rejects injected scripts

## to prevent CSRF

- › server embeds secret key in forms
- › only requests containing key accepted

## to prevent both: SOP

- › same origin policy (in browser)
- › browser tracks origin of pages
- › will only “phone home”

**SOP stops mashups from working?**

# working around SOP in mashups

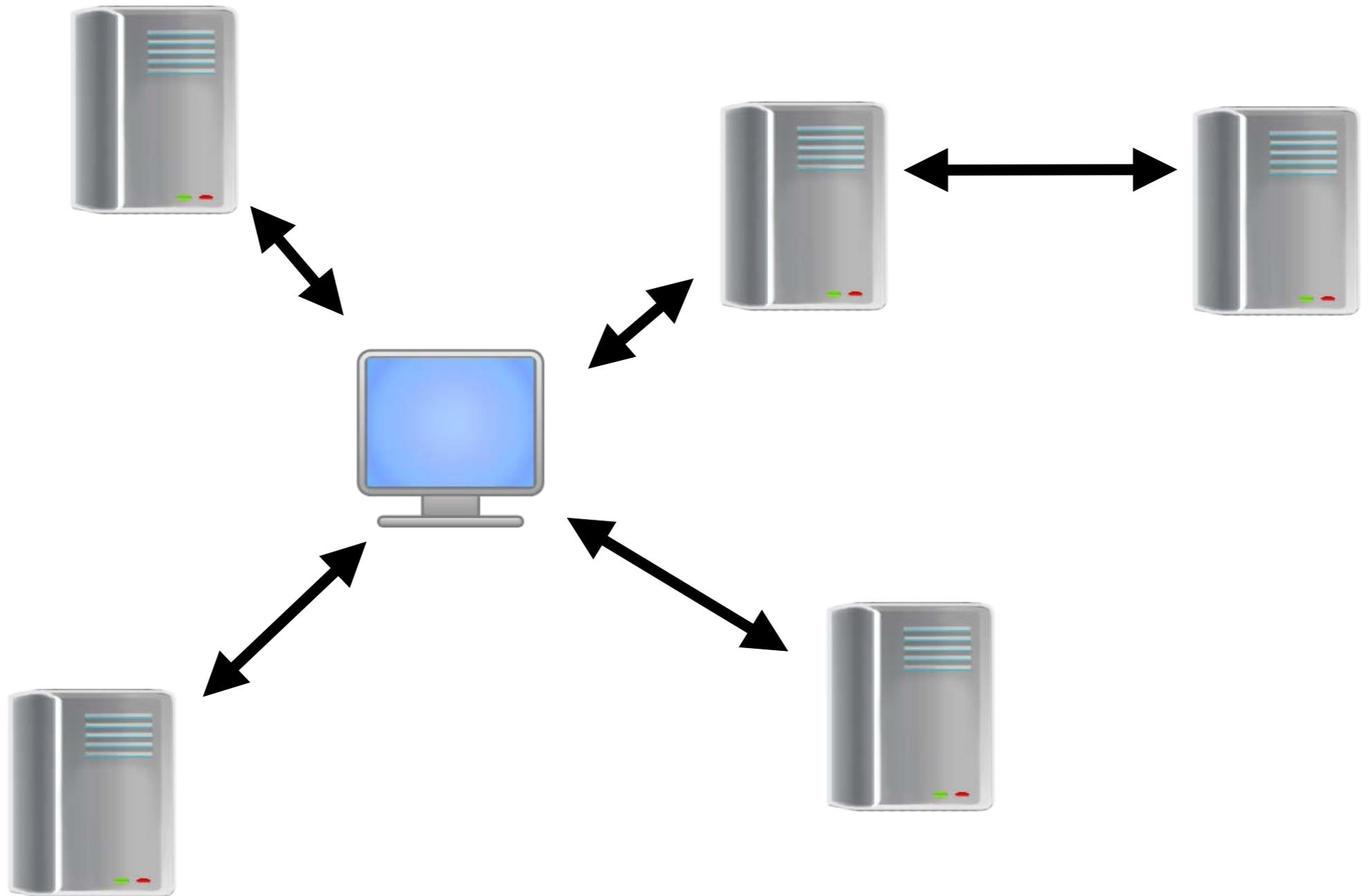
## how to work around?

- › JSONP: a hack, exploits script download not being checked
- › CORS: cross origin resource sharing

## how CORS works

- › server says it'll accept requests from other sources
- › server response has header saying which origins are ok; resource is dropped if doesn't match origin of request
- › non-GET requests: browser sends "preflight request" first

# web services



MIT OpenCourseWare  
<http://ocw.mit.edu>

6.170 Software Studio  
Spring 2013

For information about citing these materials or our Terms of Use, visit: <http://ocw.mit.edu/terms>.