software studio

the web as a platform for distributed computing

Daniel Jackson

client/server, documents only

client browser

web server

file system

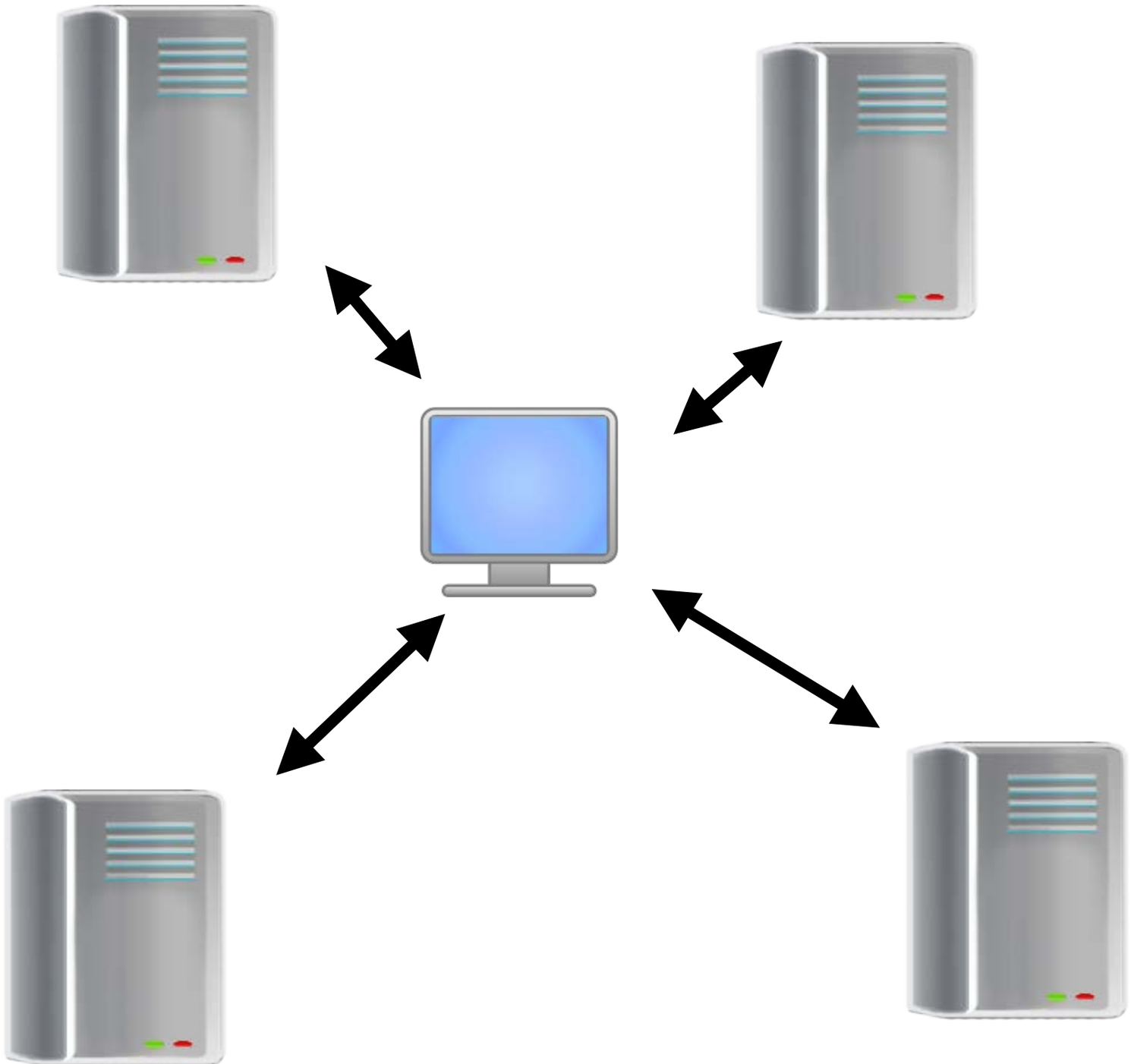
client/server, server apps

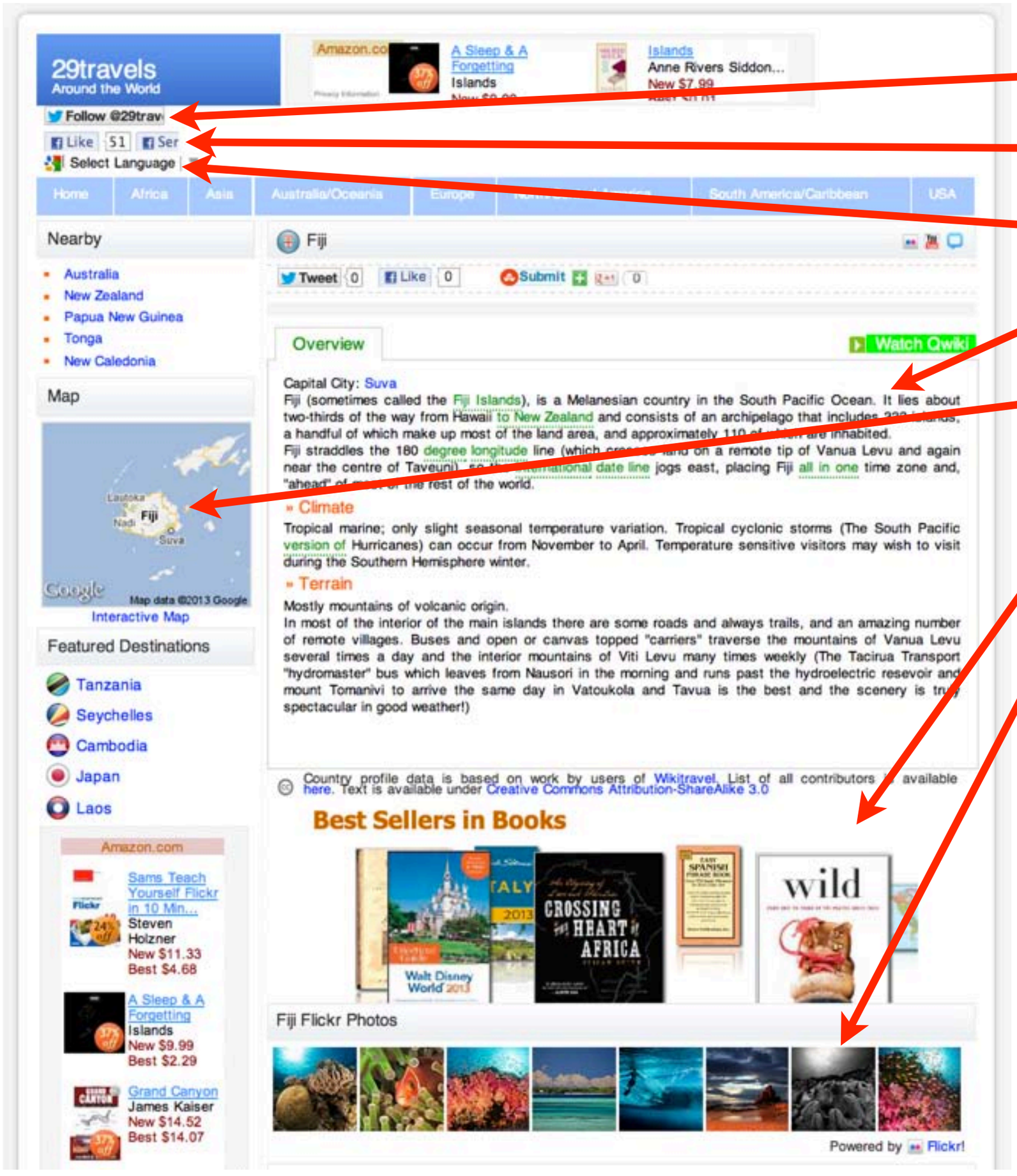
client browser

web server + app

database

client/server, multiple servers





client/server, client apps

client browser + app

web server + app

database

client app uses web service API

https://docs.google.com/forms/d/1ZB8fr4ye8bsbXnAgQY4w_wk_s7Dln0F16_a9clBFNkA/edit

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 *

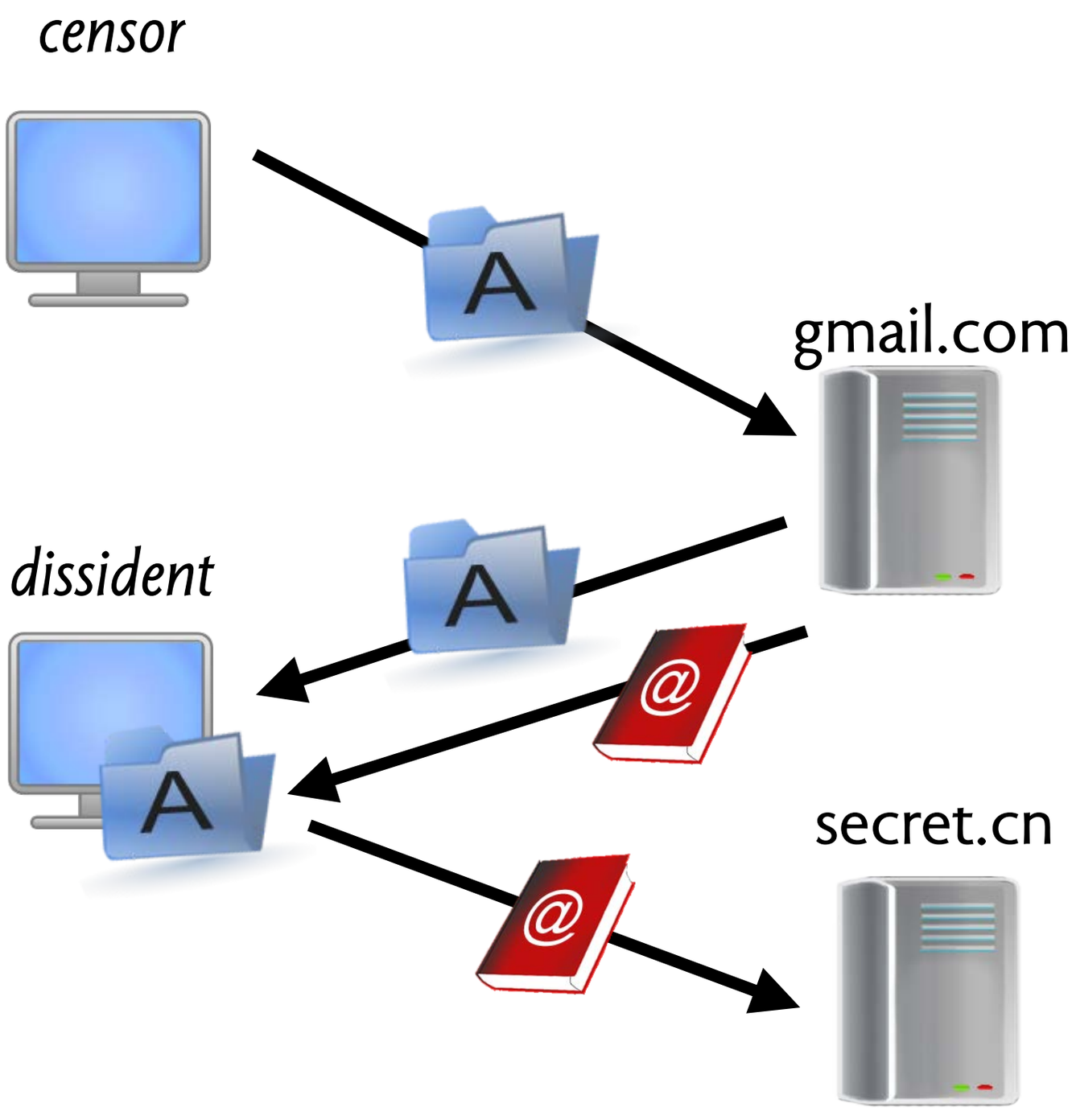
Which of the following best illustrates an example of "scientific thought" as advocated by Dijkstra?

- 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

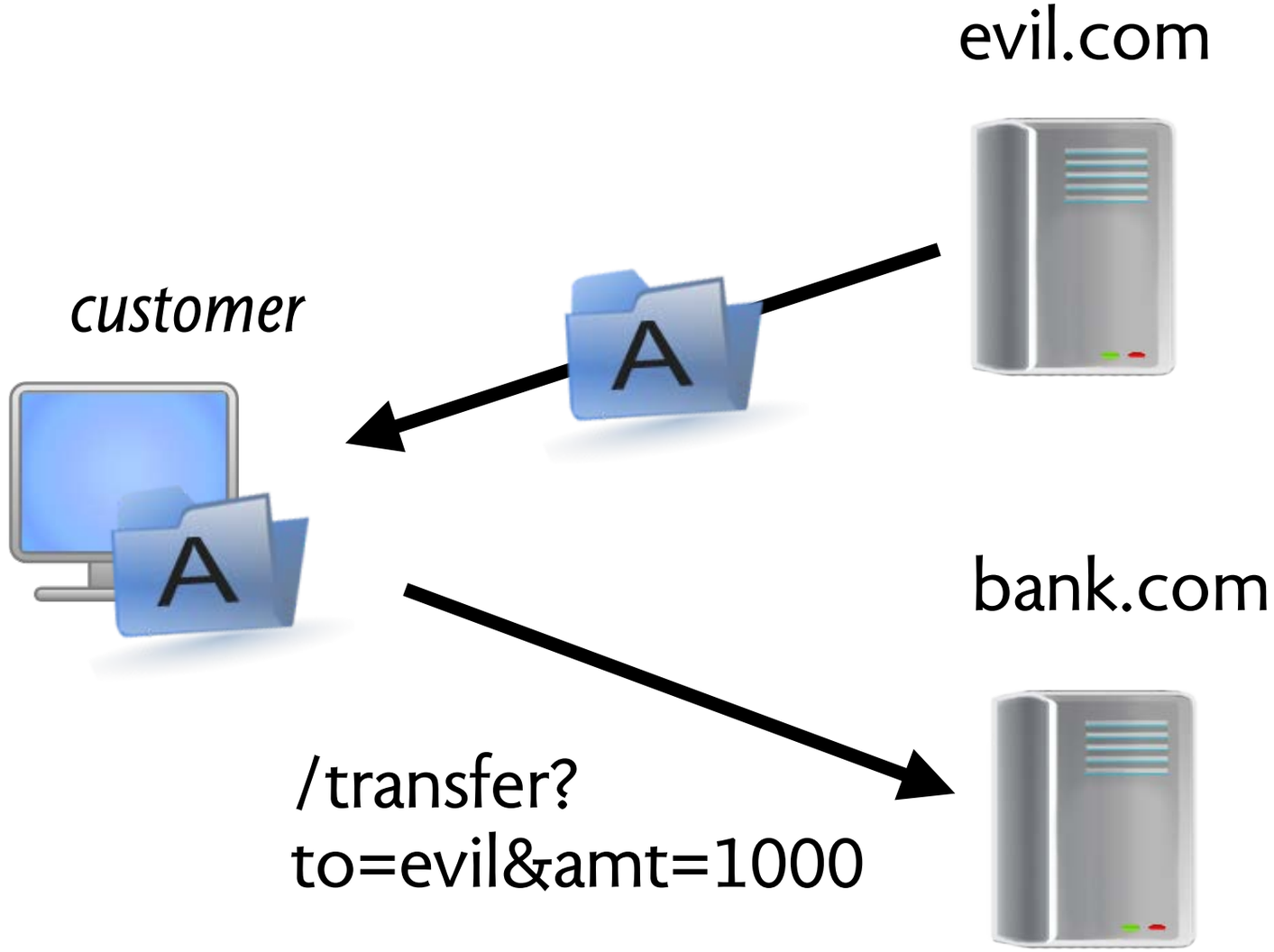
Elements | Resources | Network | Sources | Timeline | Profiles | Audits | Console

Name Path	Method	Status Text	Type	Initiator	Size Content	Time Latency	Timeline
edit /forms/d/1ZB8fr4ye8bsbXnAgQY4w_wk_s7D	GET	200 OK	text/html	Other	0B 75.29KB	106ms 90ms	
3169340563-formeditor_ltr.css /static/forms/client/css	GET	200 OK	text/css	edit:35 Parser	0B 120.33KB	31ms 22ms	
2986332158-formeditor_prd.js /static/forms/client/js	GET	200 OK	text/javascr...	edit:35 Parser	0B 704.09KB	115ms 30ms	
checkmark_2x.png ssl.gstatic.com/ui/v1/menu	GET	200 OK	image/png	edit:36 Parser	0B 358B	213ms 98ms	
helpBubble1.png ssl.gstatic.com/ac/common	GET	200 OK	image/png	edit:36 Parser	0B 306B	213ms 98ms	
photo.jpg lh6.googleusercontent.com/-hCceIX3_RqE/A/	GET	200 OK	image/png	edit:36 Parser	0B 640B	207ms 83ms	
k2_aca6bcc6.png ssl.gstatic.com/gb/images	GET	200 OK	image/png	edit:36 Parser	0B 33.00KB	202ms 74ms	
jfk_sprite_hdpi18.png ssl.gstatic.com/docs/common	GET	200 OK	image/png	edit:36 Parser	0B 54.31KB	203ms 80ms	
peruserchrome?id=1ZB8fr4ye8bsbXnAgQY /forms/d/1ZB8fr4ye8bsbXnAgQY4w_wk_s7D	GET	200 OK	application/...	2986332158-formeditor Script	0B 182B	1.52s 1.52s	
getresponsecount?sid=49222550666bf9bc /forms/d/1ZB8fr4ye8bsbXnAgQY4w_wk_s7D	GET	200 OK	application/...	2986332158-formeditor Script	0B 28B	122ms 55ms	
read?id=1ZB8fr4ye8bsbXnAgQY4w_wk_s7I /forms/d/1ZB8fr4ye8bsbXnAgQY4w_wk_s7D	GET	200 OK	application/...	2986332158-formeditor Script	0B 22B	118ms 49ms	
about:blank	GET	Success	text/html	2986332158-formeditor Script	13B 0B	2ms 0ms	
share?id=1ZB8fr4ye8bsbXnAgQY4w_wk_s7 /e	GET	(canceled)	text/html	Other	355B 0B	389ms 381ms	
csi?v=3&s=freebird&action=edit&it=dns_.(csi.gstatic.com	GET	204 No Content	image/gif	edit:40 Script	258B 0B	402ms 402ms	
spinner.gif ssl.gstatic.com/docs/spreadsheets	GET	200 OK	image/gif	2986332158-formeditor Script	0B 1.42KB	72ms 18ms	

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

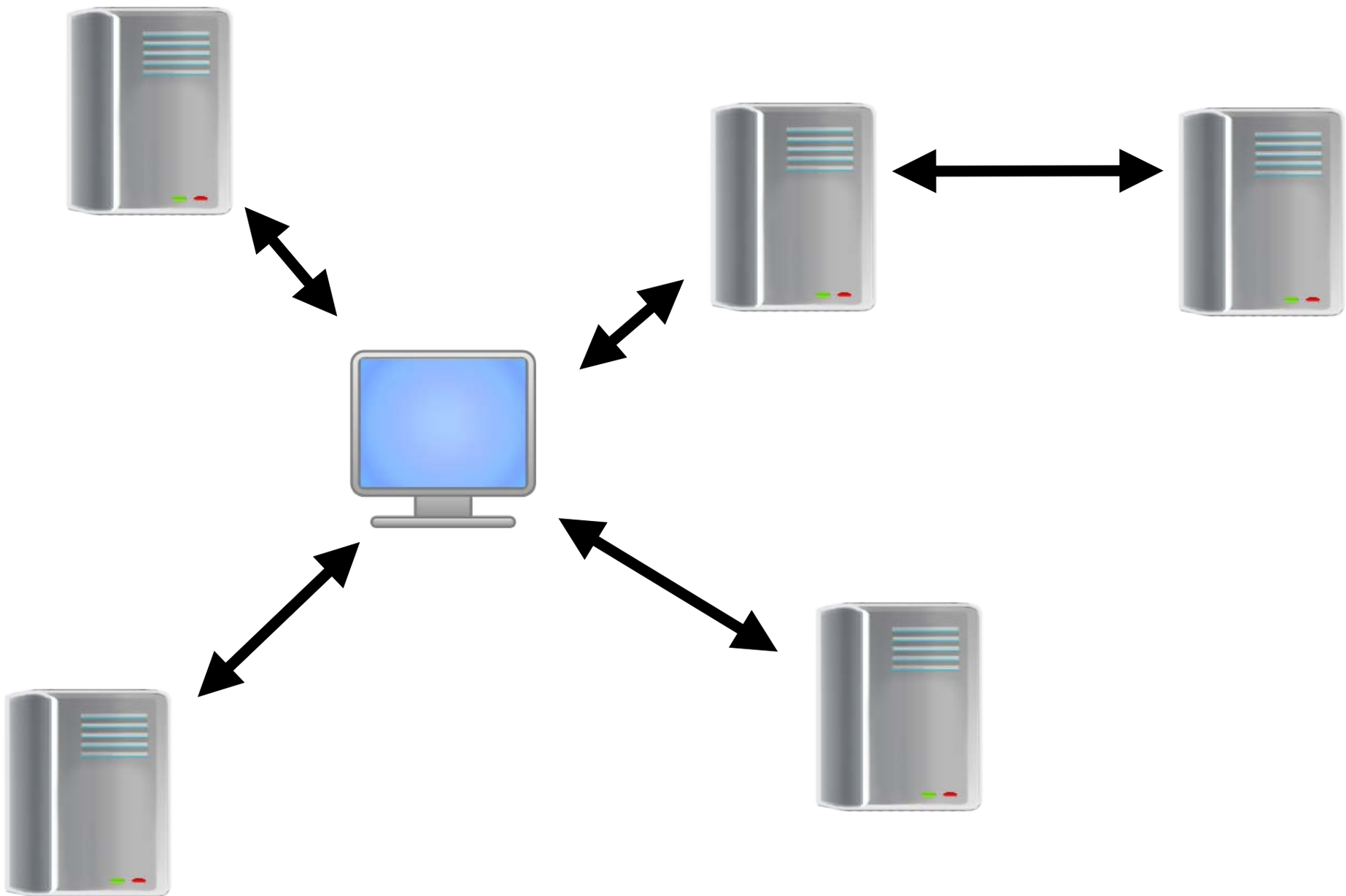
how to work around?

› 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



6.170 Software Studio
Spring 2013