CSE 484: Computer Security and Privacy

Web Security + Authentication

Spring 2024

David Kohlbrenner

dkohlbre@cs

Thanks to Franzi Roesner, Dan Boneh, Dieter Gollmann, Dan Halperin, David Kohlbrenner, Yoshi Kohno, Ada Lerner, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...

Logistics

- Lab 2 due _Thursday_ night

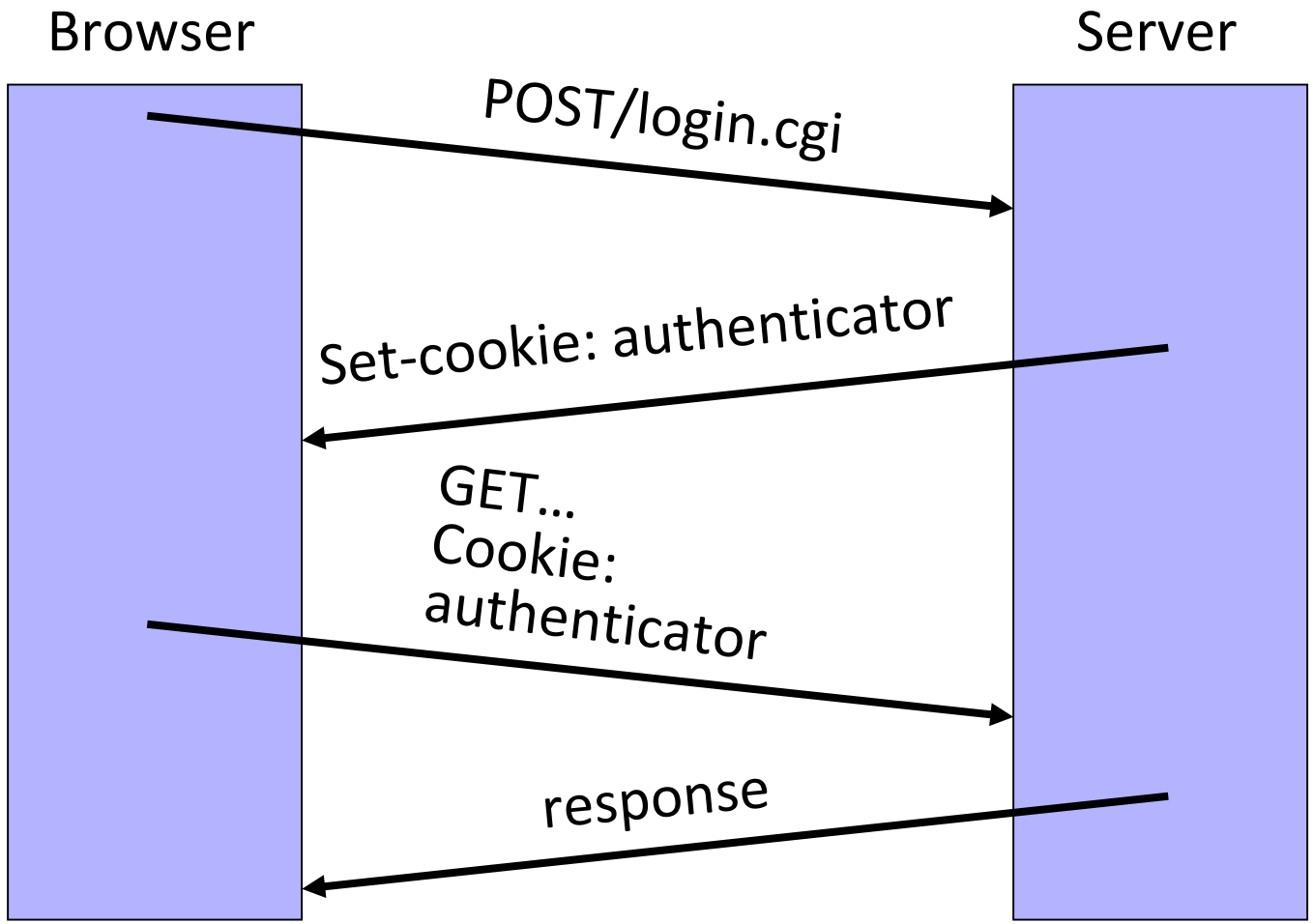
- HW3 will be relatively short, going out today
  - It will ask you to break some hashed passwords
  - Examine cryptography in an android app
  - Etc.
  - Note that you will need to do a bit of documentation reading and exploring the code on this, we aren't giving you an obvious skeleton to work off.
  - The problems themselves are not intended to be tricky, this is about reading documentation and navigating running tools.

Data-as-code

- XSS
- SQL Injection
- (Like buffer overflows)

Cross-Site Request Forgery (CSRF/XSRF)

Cookie-Based Authentication Review



Browser Sandbox Review

- Based on the same origin policy (SOP)
- Active content (scripts) can send anywhere!
  - For example, can submit a POST request
  - Some ports inaccessible -- e.g., SMTP (email)
- Can only *read* response from the *same origin*
  - … but you can do a lot with just sending!

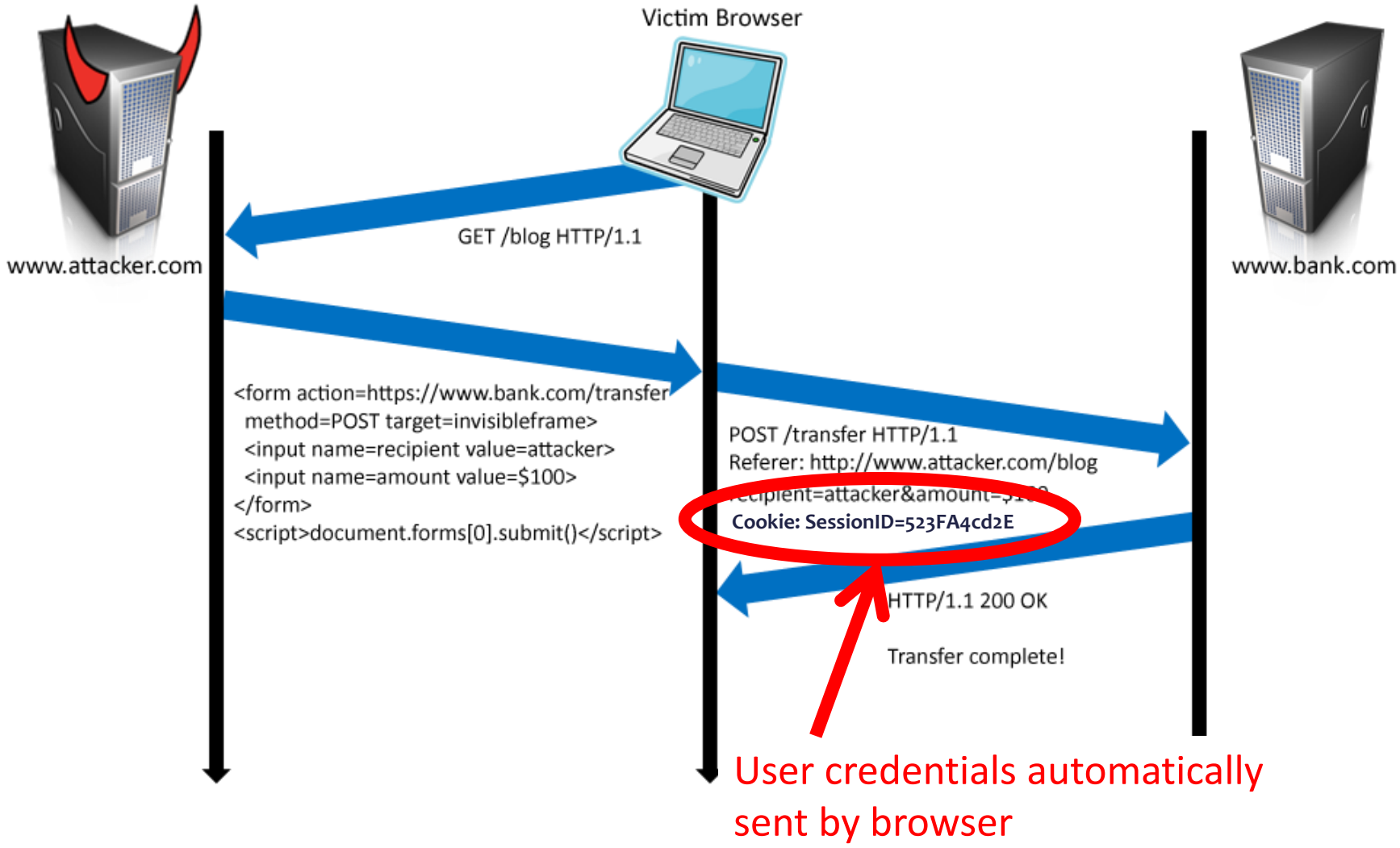
Cross-Site Request Forgery

- Users logs into bank.com, forgets to sign off
  - Session cookie remains in browser state
- User then visits a malicious website containing

```
<form  name=BillPayForm
action=http://bank.com/BillPay.php>
<input  name=recipient  value=attacker> …
<script> document.BillPayForm.submit(); </script>
```

- Browser sends cookie, payment request fulfilled!
- Lesson: cookie authentication is not sufficient when side effects can happen

Cookies in Forged Requests

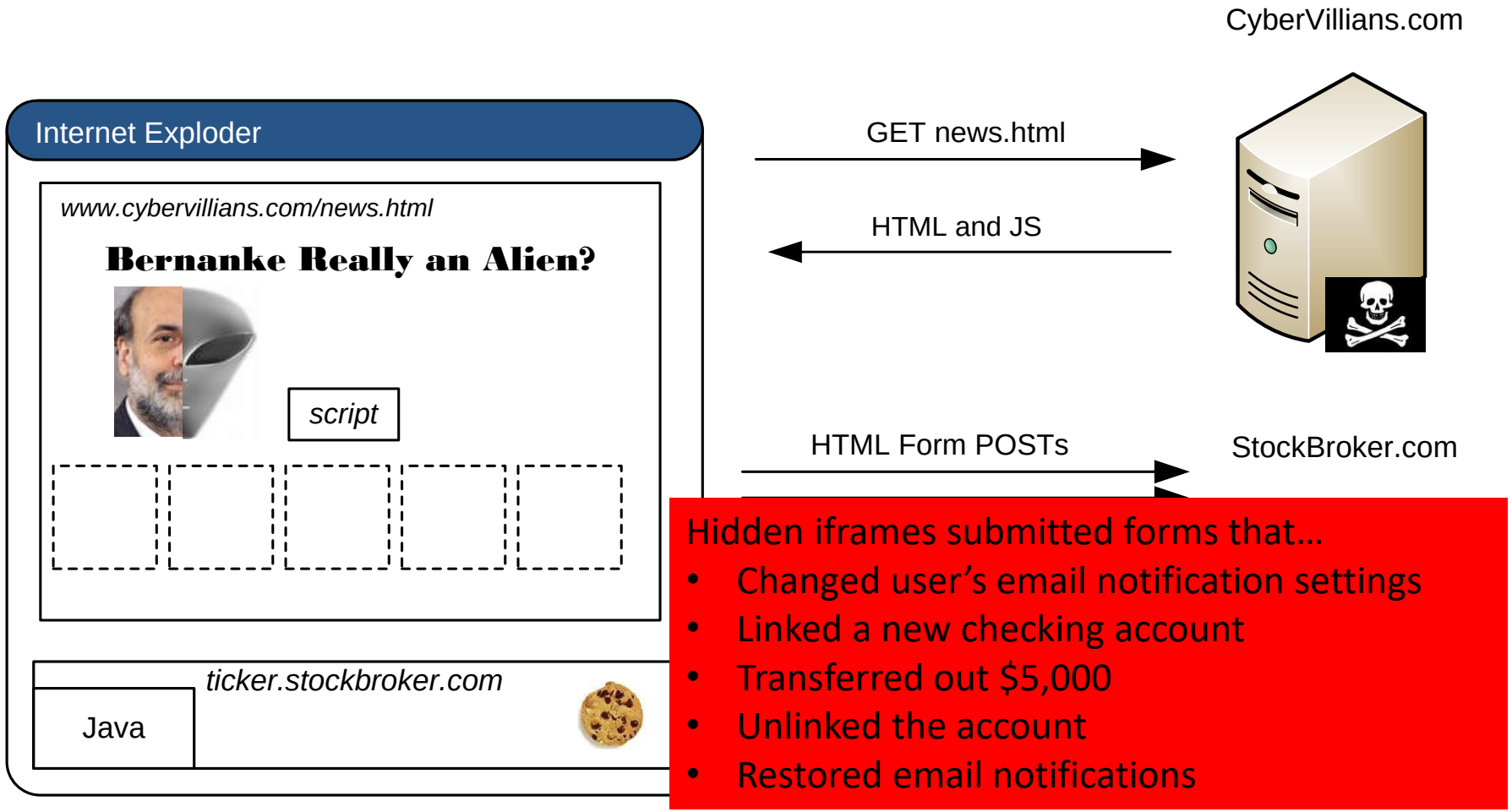


Impact

- Hijack any ongoing session (if no protection)
  - Netflix: change account settings, Gmail: steal contacts, Amazon: one-click purchase
- Reprogram the user's home router
- Login to the *attacker's* account
  - Why?

XSRF True Story

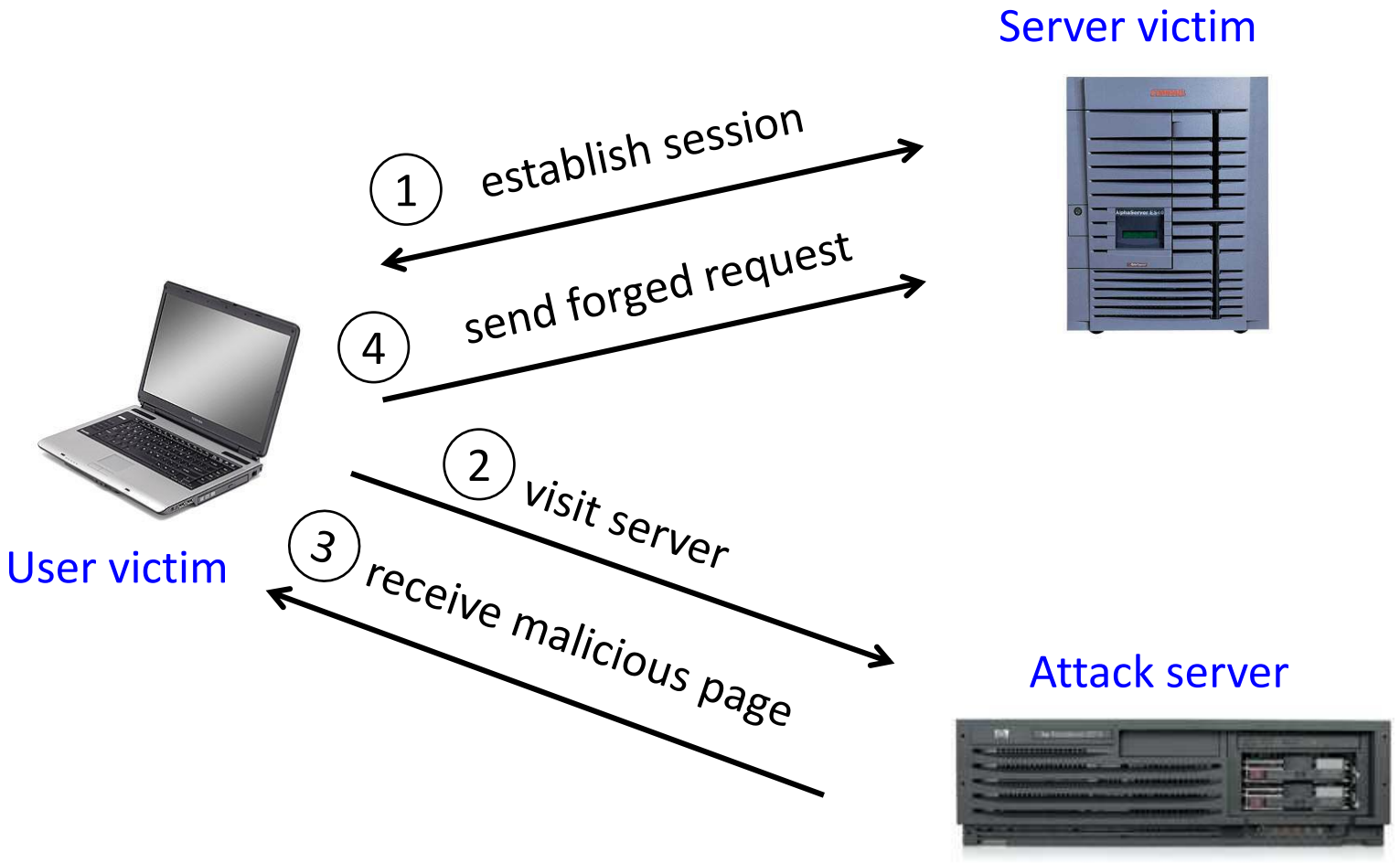
[Alex Stamos]



Hidden iframes submitted forms that…

- Changed user's email notification settings
- Linked a new checking account
- Transferred out $5,000
- Unlinked the account
- Restored email notifications

XSRF (aka CSRF): Summary

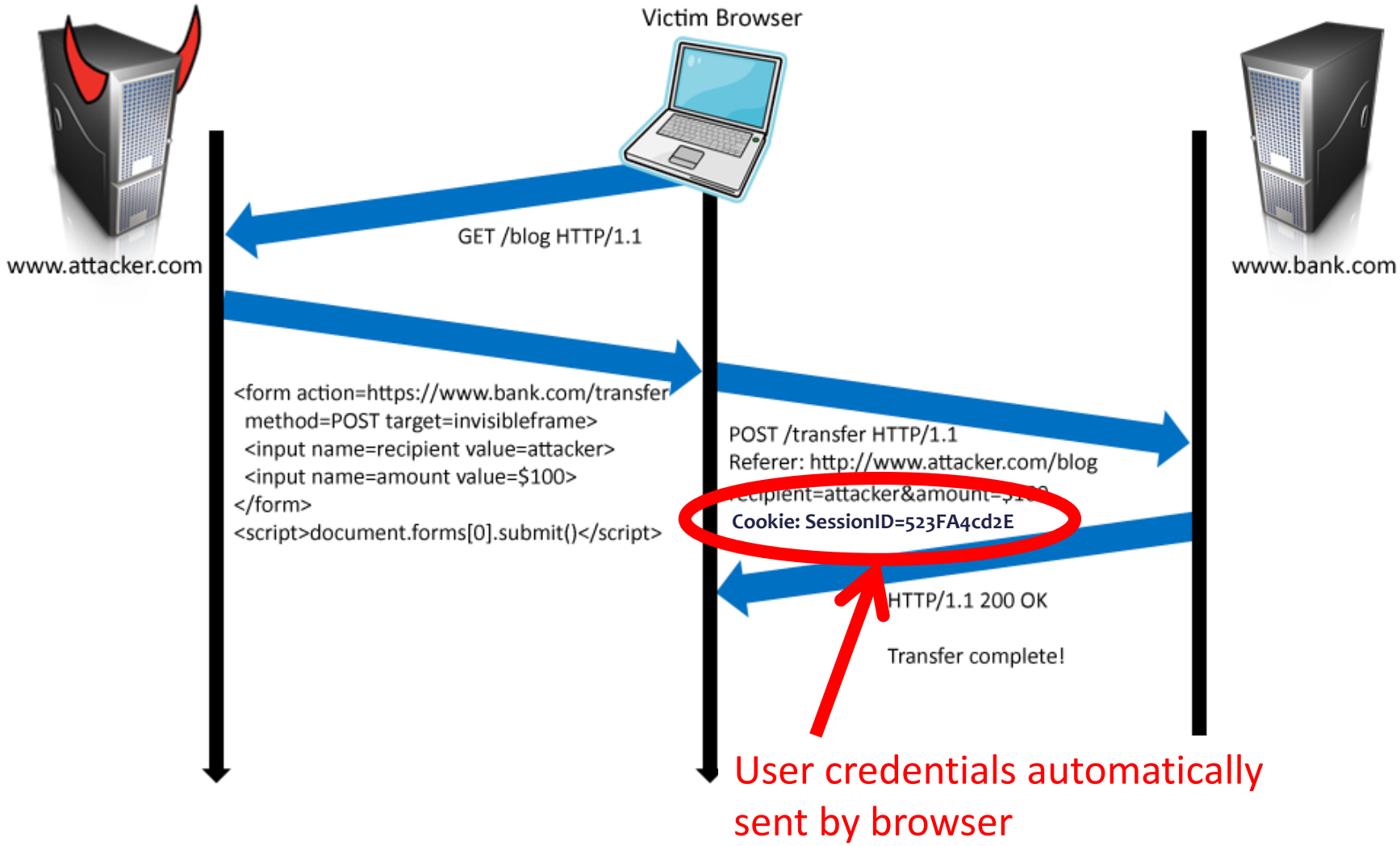


Q: how long do you stay logged on to Gmail? Financial sites?

Broader View of XSRF

- Abuse of cross-site data export
  - SOP does not control data export
  - Malicious webpage can initiates requests from the user's browser to an honest server
  - Server thinks requests are part of the established session between the browser and the server (automatically sends cookies)

How might you protect against XSRF?

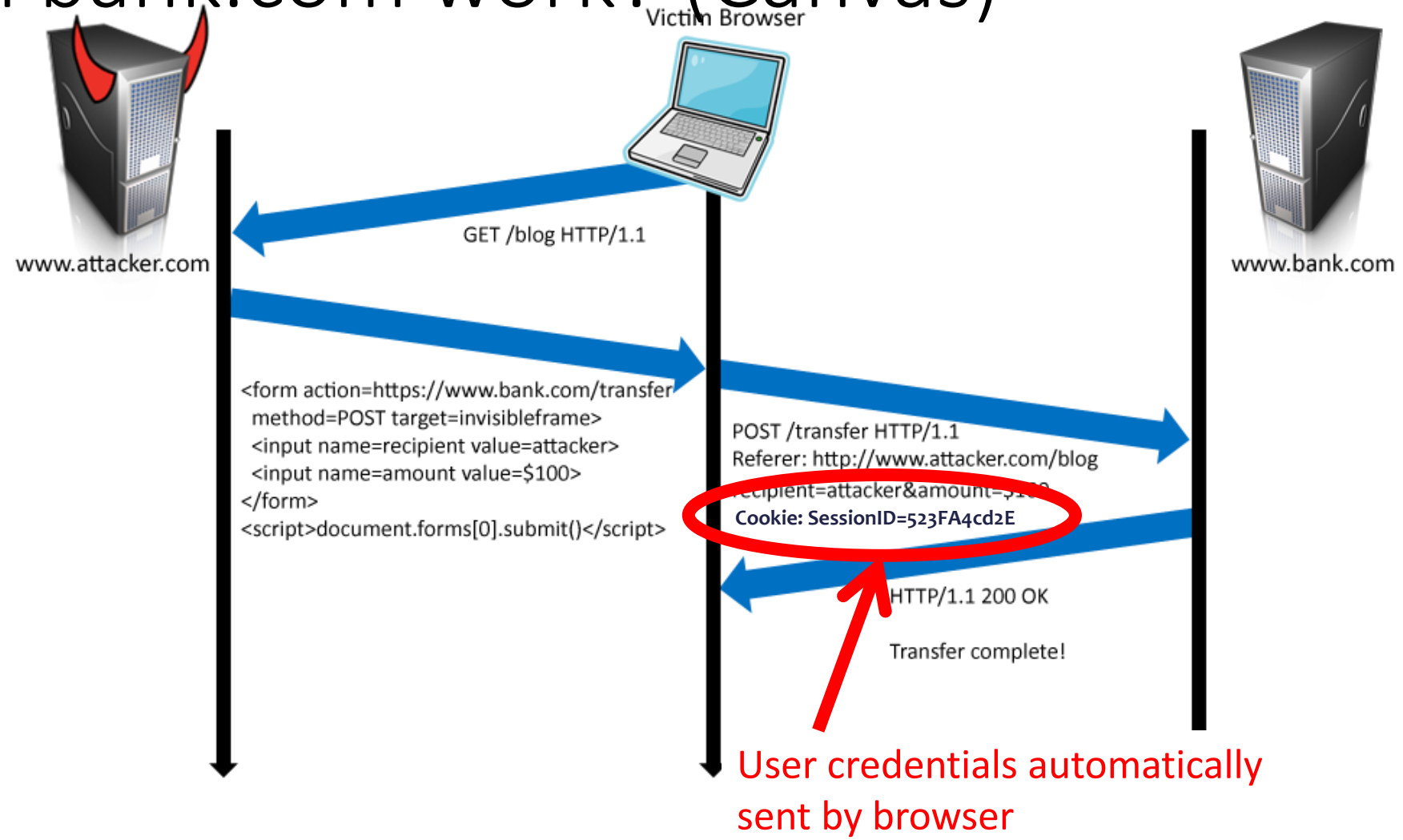


XSRF Defenses

- Secret validation token

<input type=hidden value=23a3af01b>

Why does adding a magic value to the form from bank.com work? (Canvas)



XSRF Defenses

- Secret validation token

<input type=hidden value=23a3af01b>

- Referrer validation

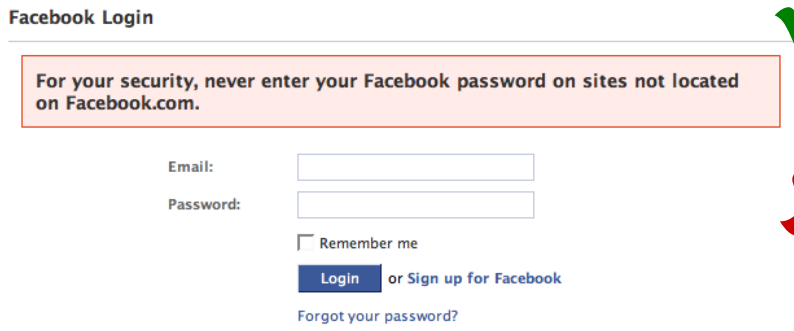
Referer:
http://www.facebook.com/home.php

Add Secret Token to Forms

```
<input type=hidden value=23a3af01b>
```

- "Synchronizer Token Pattern"
- Include a secret challenge token as a hidden input in forms
  - Token often based on user's session ID
  - Server must verify correctness of token before executing sensitive operations
- Why does this work?
  - **Same-origin policy:** attacker can't read token out of legitimate forms loaded in user's browser, so can't create fake forms with correct token

Referer Validation



Referer:
http://www.facebook.com/home.php

Referer:
http://www.evil.com/attack.html

Referer:

- Lenient referer checking – header is optional
- Strict referer checking – header is required

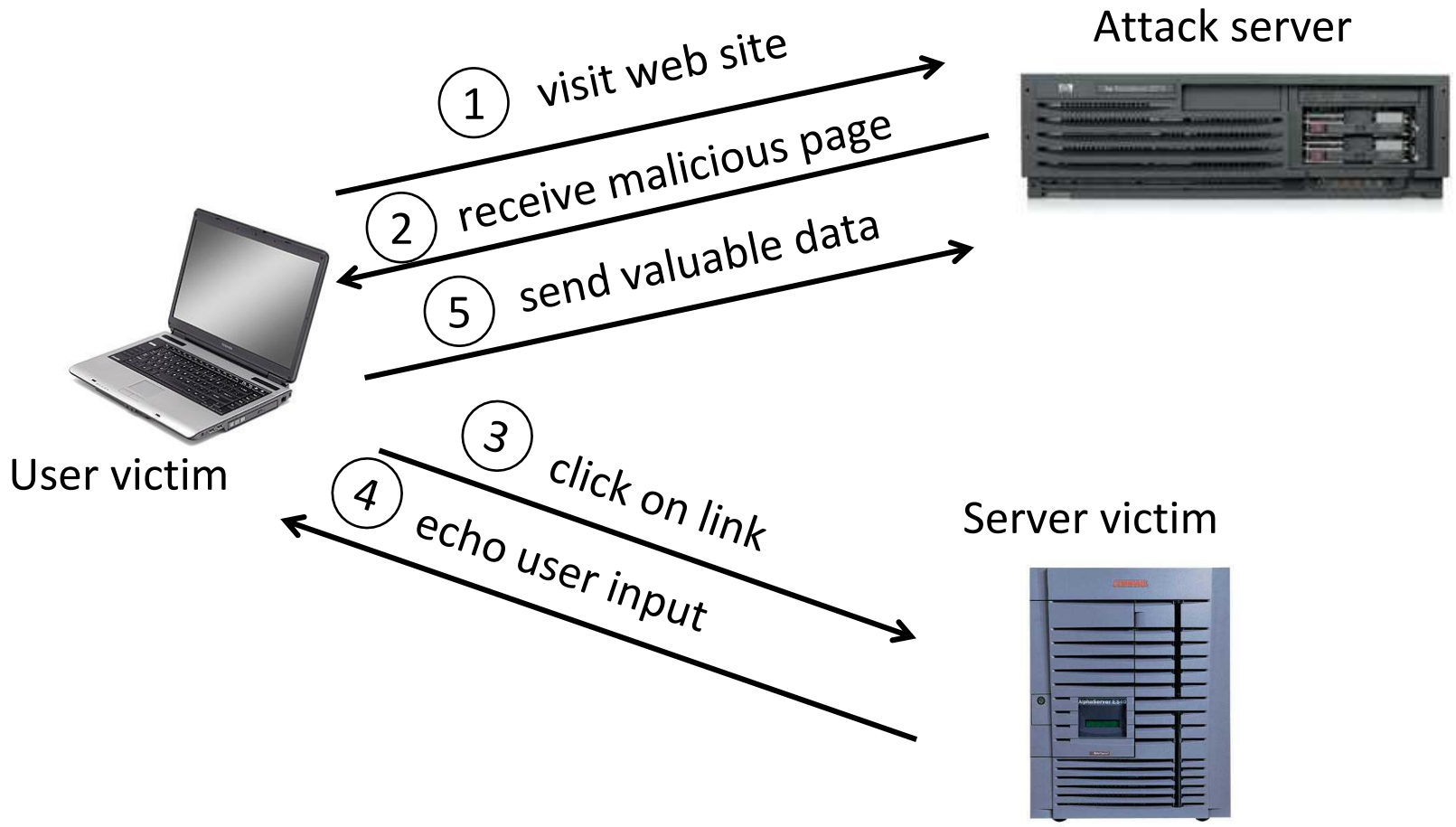
Why Not Always Strict Checking?

- Why might the referer header be suppressed?
  - Stripped by the organization's network filter
  - Stripped by the local machine
  - Stripped by the browser for HTTPS → HTTP transitions
  - User preference in browser
  - Buggy browser
- Web applications can't afford to block these users
- **Most web application frameworks include CSRF defenses today**

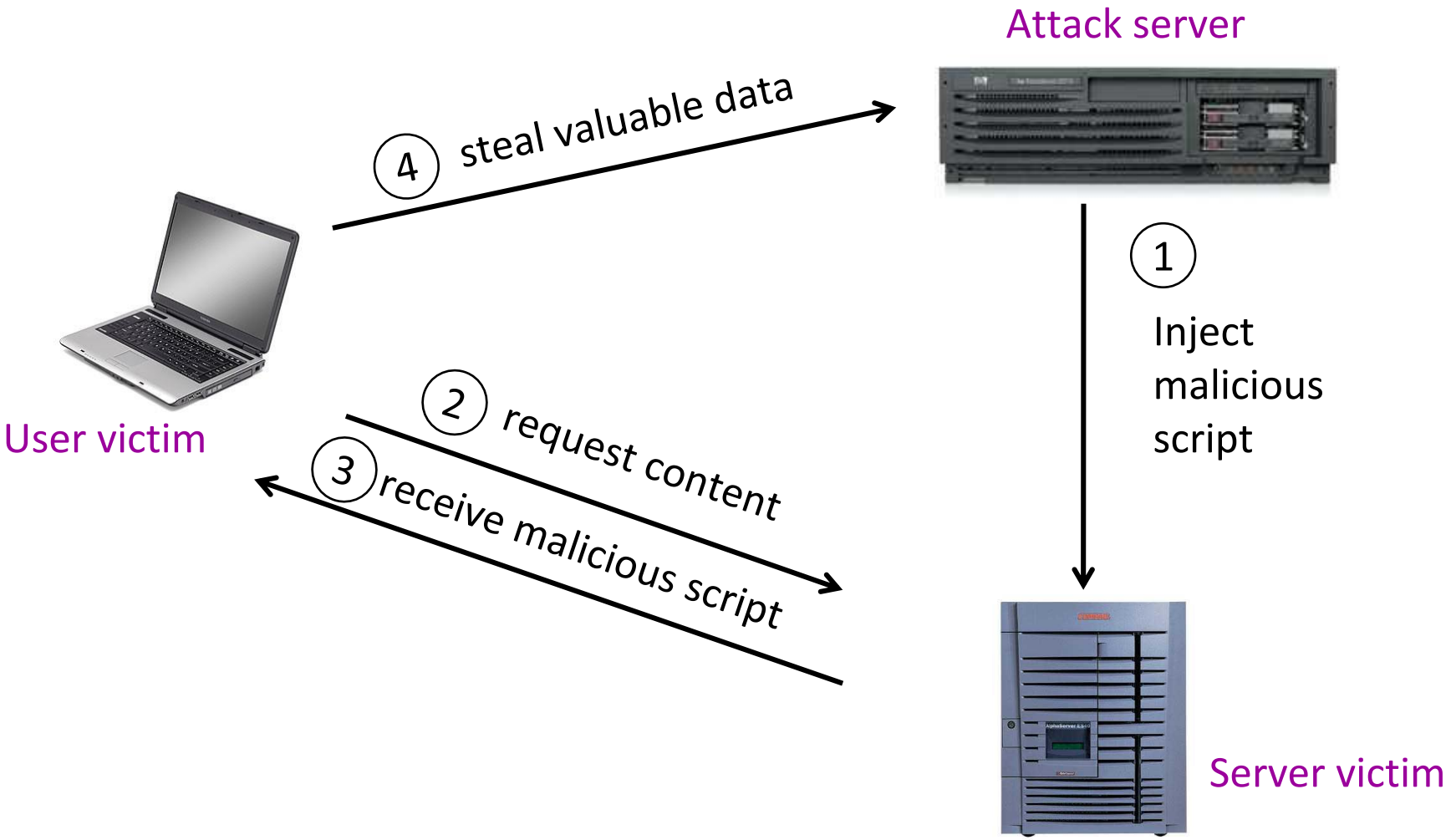
Surprise not-quiz time

XSS again

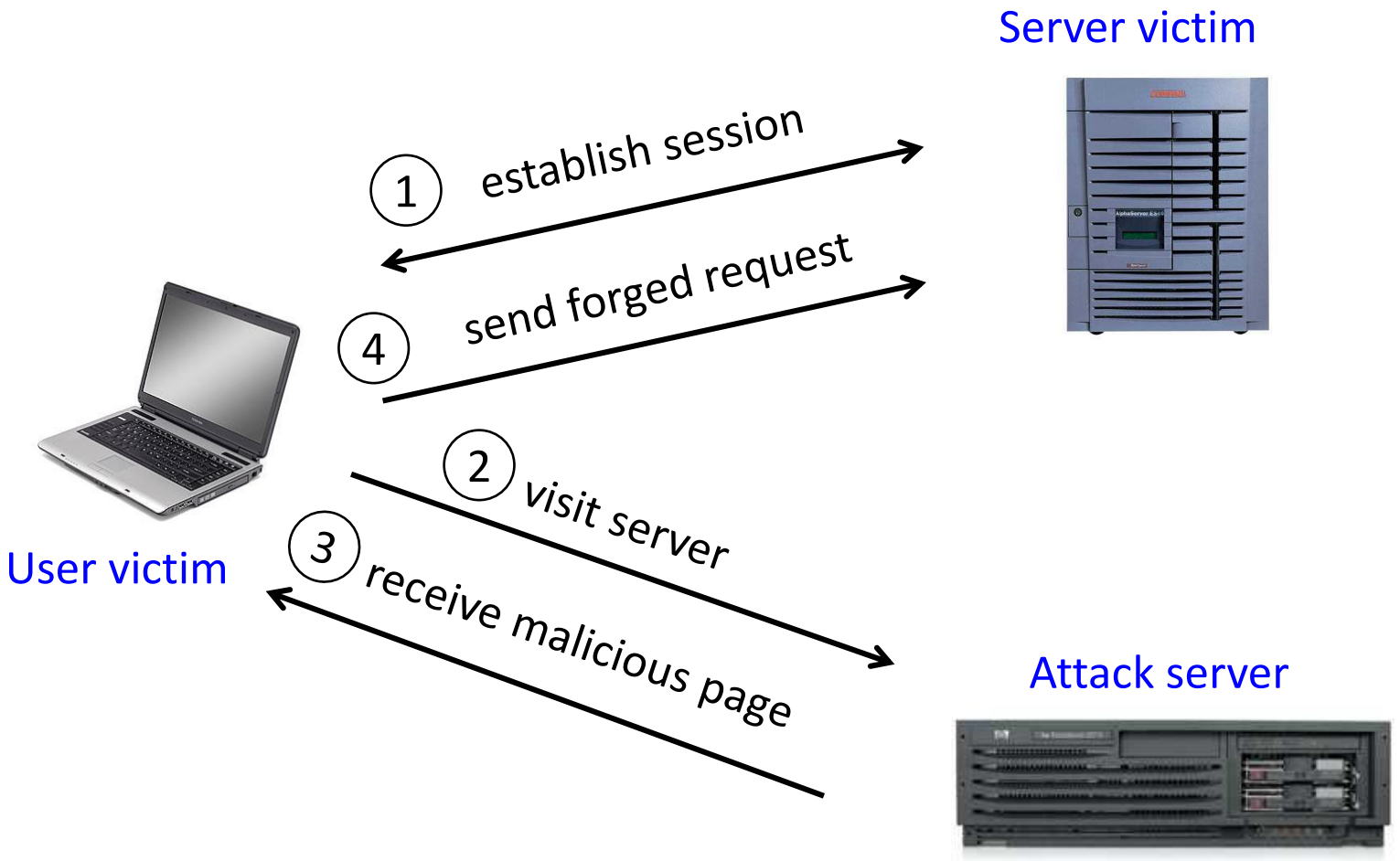
Reflected XSS



Stored XSS

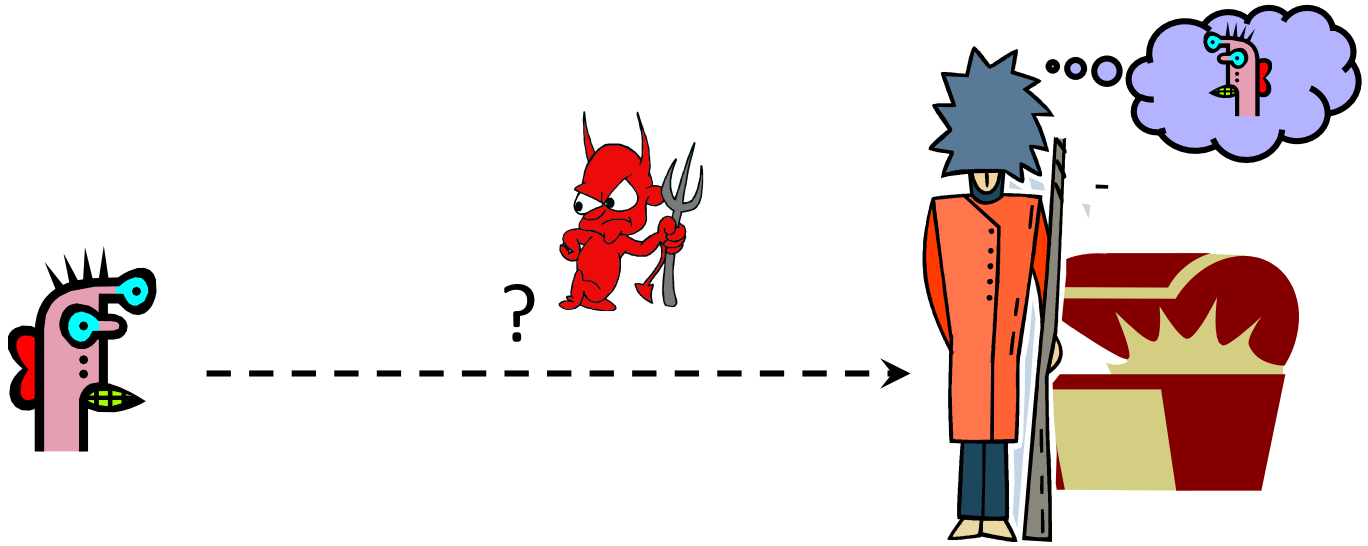

Attack server
4 steal valuable data
1
Inject malicious script
2 request content
3 receive malicious script
User victim
Server victim

XSRF (aka CSRF)



Authentication

Basic Problem



How do you prove to someone that you are who you claim to be?

Any system with access control must solve this problem.

Many Ways to Prove Who You Are

- "Something you know"
  - Passwords
  - Answers to questions that only you know
- "Something you have"
  - Secure tokens, mobile devices
- "Something you are"
  - Biometrics

A slightly more fundamental question

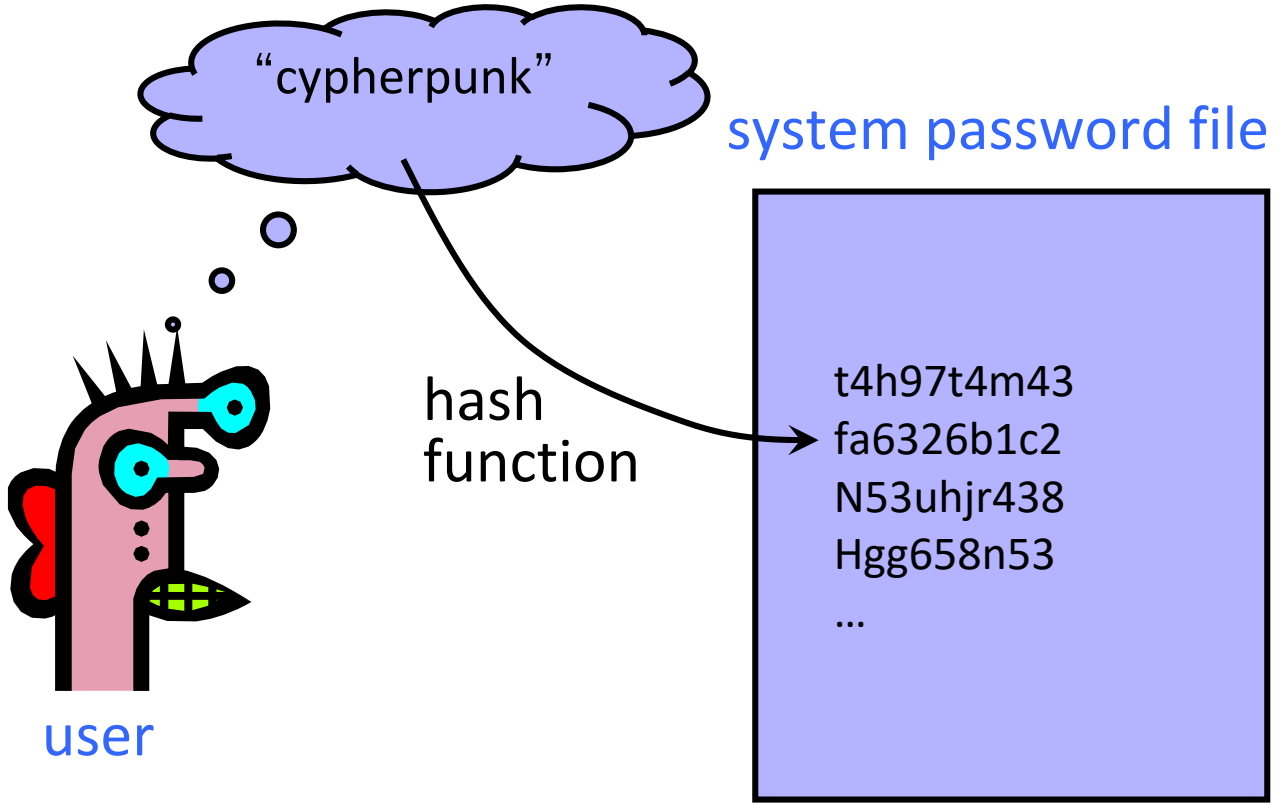
- What are we trying to prove?

Passwords and Computer Security

- In 2012, 76% of network intrusions exploited weak or stolen credentials (username/password)
  - Source: Verizon Data Breach Investigations Report
- In Mitnick's "Art of Intrusion" 8 out of 9 exploits involve password stealing and/or cracking
- First step after any successful intrusion: install sniffer or keylogger to steal more passwords
- Second step: run cracking tools on password files
  - Cracking needed because modern systems usually do not store passwords in the clear

UNIX-Style Passwords

- How should we store passwords on a server?
  - In cleartext?
  - Encrypted?
  - Hashed?



Password Hashing

- Instead of user password, store H(password)
- When user enters password, compute its hash and compare with entry in password file
  - System does not store actual passwords!
  - System itself can't easily go from hash to password
    - Which would be possible if the passwords were encrypted
- Hash function H must have some properties
  - One-way: given H(password), hard to find password
    - No known algorithm better than trial and error
  - "Slow" to compute

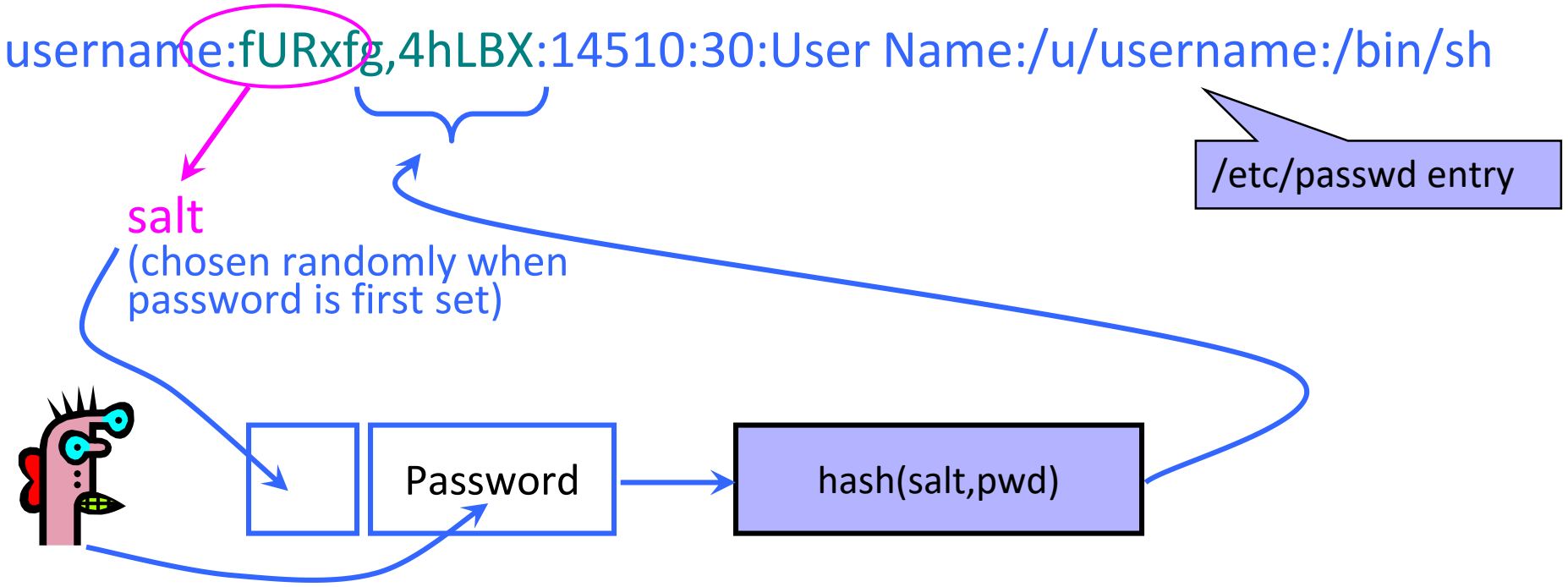
UNIX Password System

- Approach: Hash passwords
- Problem: passwords are not truly random
  - With 52 upper- and lower-case letters, 10 digits and 32 punctuation symbols, there are 94^8 == 6 quadrillion possible 8-character passwords ($\sim 2^{52}$)
  - **BUT:** Humans like to use dictionary words, human and pet names == 1 million common passwords

Dictionary Attack

- Dictionary attack is possible because many passwords come from a small dictionary
  - Attacker can pre-compute H(word) for every word in the dictionary – this only needs to be done once!
    - This is an offline attack
    - Once password file is obtained, cracking is instantaneous
  - Sophisticated password guessing tools are available
    - Take into account freq. of letters, password patterns, etc.

Salt



- Users with the same password have <u>different</u> entries in the password file
- Offline dictionary attack becomes much harder

Advantages of Salting

- Without salt, attacker can pre-compute hashes of all dictionary words once for all password entries
  - Same hash function on all UNIX machines
  - Identical passwords hash to identical values; one table of hash values can be used for all password files
- With salt, attacker must compute hashes of all dictionary words once for each password entry
  - With 12-bit random salt, same password can hash to 2^{12} different hash values
  - Attacker must try all dictionary words **for each salt value** in the password file
- Pepper: Secret salt (not stored in password file)

Other Password Security Risks

- Keystroke loggers
  - Hardware
  - Software (spyware)
- Shoulder surfing
- Same password at multiple sites
- Broken implementations
  - Recall TENEX timing attack
- Social engineering

Other Issues

- Usability
  - Hard-to-remember passwords?
  - Carry a physical object all the time?
- Denial of service
  - Attacker tries to authenticate as you, account locked after three failures

Default Passwords

- Examples from Mitnick's "Art of Intrusion"
  - U.S. District Courthouse server: "public" / "public"
  - NY Times employee database: pwd = last 4 SSN digits
- Mirai IoT botnet
  - Weak and default passwords on routers and other devices

Weak Passwords

- RockYou hack
  - "Social gaming" company
  - Database with 32 million user passwords from partner social networks
  - Passwords stored in the clear
  - December 2009: entire database hacked using an SQL injection attack and posted on the Internet
  - One of many such examples!

Weak Passwords

- RockYou hack
  - "
  - D
  - P
  - D
    p

rockyou™

Password Popularity – Top 20

Rank	Password	Number of Users with Password (absolute)
1	123456	290731
2	12345	79078
3	123456789	76790
4	Password	61958
5	iloveyou	51622
6	princess	35231
7	rockyou	22588
8	1234567	21726
9	12345678	20553
10	abc123	17542

Rank	Password	Number of Users with Password (absolute)
11	Nicole	17168
12	Daniel	16409
13	babygirl	16094
14	monkey	15294
15	Jessica	15162
16	Lovely	14950
17	michael	14898
18	Ashley	14329
19	654321	13984
20	Qwerty	13856

[Inglesant and Sasse, "The True Cost of Unusable Password Policies"]

Password Policies

- Old recommendation:
  - 7 or 8 characters, at least 3 out of {digits, upper-case, lower-case, non-alphanumeric}, no dictionary words, change every 4 months, password may not be similar to previous 12 passwords…

[Inglesant and Sasse, "The True Cost of Unusable Password Policies"]

Password Policies

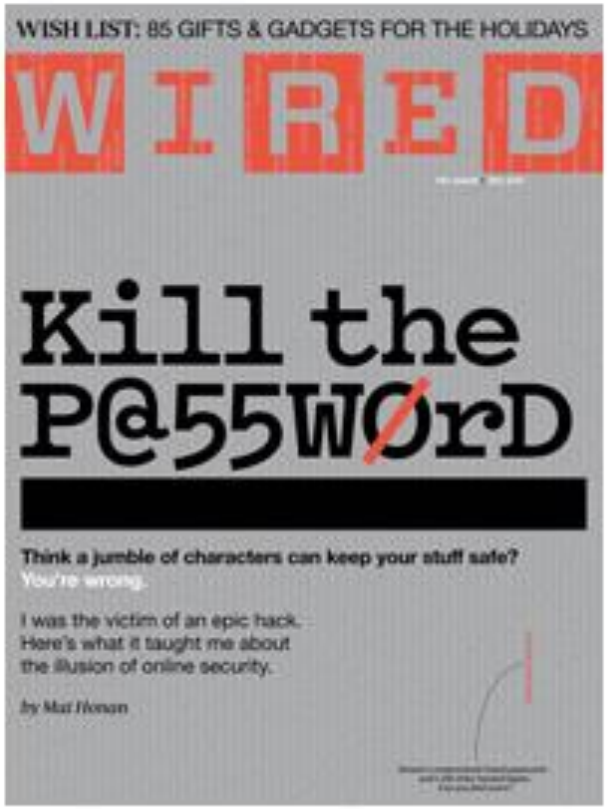
- Old recommendation:
  - 7 or 8 characters, at least 3 out of {digits, upper-case, lower-case, non-alphanumeric}, no dictionary words, change every 4 months, password may not be similar to previous 12 passwords…
- **But** … results in frustrated users and less security
  - Burdens of devising, learning, forgetting passwords
  - Users construct passwords insecurely, write them down
    - Can't use their favorite password construction techniques (small changes to old passwords, etc.)
  - Heavy password re-use across systems
  - (Password managers can help)

“New” (2017) NIST Guidelines ☺

- Remove requirement to periodically change passwords
- Screen for commonly used passwords
- Allow copy-paste into password fields
  - But concern: what apps have access to clipboard?
- Allow but don’t require arbitrary special characters
- Etc.

https://pages.nist.gov/800-63-3/sp800-63b.html

Wired Cover Story (Dec 2012)



"This summer, hackers destroyed my entire digital life in the span of an hour. My Apple, Twitter, and Gmail passwords were all robust—seven, 10, and 19 characters, respectively, all alphanumeric, some with symbols thrown in as well—but the three accounts were linked, so once the hackers had conned their way into one, they had them all. They really just wanted my Twitter handle: @mat."

Improving(?) Passwords

- Add biometrics
  - For example, keystroke dynamics or voiceprint
- Graphical passwords
  - Goal: easier to remember? no need to write down?
- Password managers
  - Examples: LastPass, KeePass, built into browsers
  - Can have security vulnerabilities…
- Two-factor authentication
  - Leverage phone (or other device) for authentication

Password managers

- Generation
  - Secure generation of random passwords
- Management
  - Allows for password-per-account
- Safety?
  - Single point of failure
  - Vulnerability?
  - Phishing?

Passkeys (2024)

- An actual, deployed, genuine *password replacement*
  - *Also a 2fa replacement!*
  - *And a username replacement!*

- Basic goals:
  - Store some sort of key on user end-devices
  - Use that key to login to Stuff
  - Don’t allow losing the key
  - Somehow make the key moving between devices Easy