CSE 484 / CSE M 584:
Web Security: Wrap-up;
Web Privacy: Start

Fall 2024

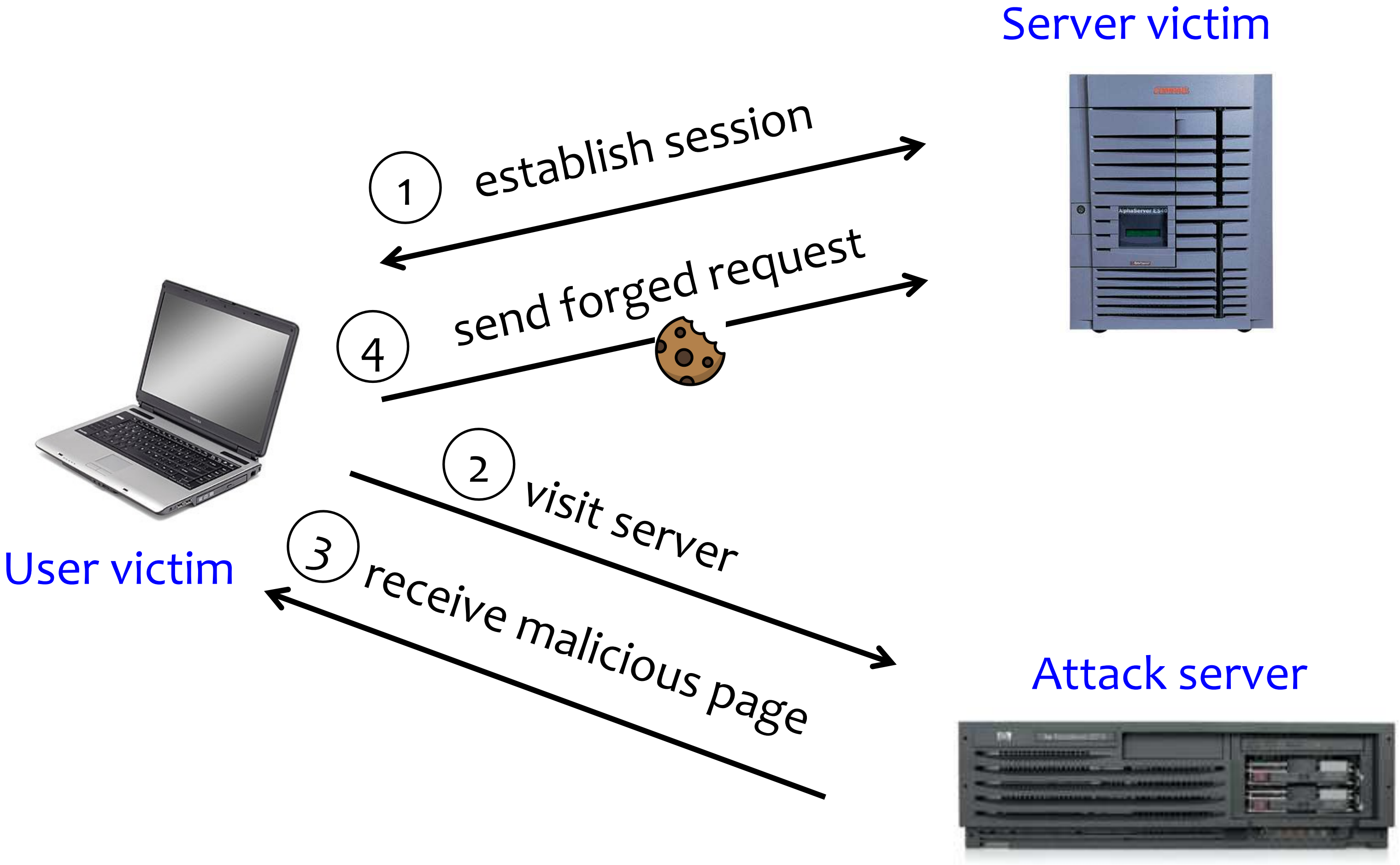
Franziska (Franzi) Roesner
franzi@cs

UW Instruction Team: David Kohlbrenner, Yoshi Kohno, Franziska Roesner. Thanks to Dan Boneh, Dieter Gollmann, Dan Halperin, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...

Announcements

- Where are we?
  - **Lab 2** due next Friday (11/15)
  - **Homework 3** will be out on ~Wednesday, due 11/22
  - **Final project** will be out on 11/18, due 12/10
  - Topics:
    - Finishing web security, followed by a "grab bag" of topics (*authentication, mobile platforms, usable security, anonymity, side channels, …*)

XSRF (aka CSRF): Summary

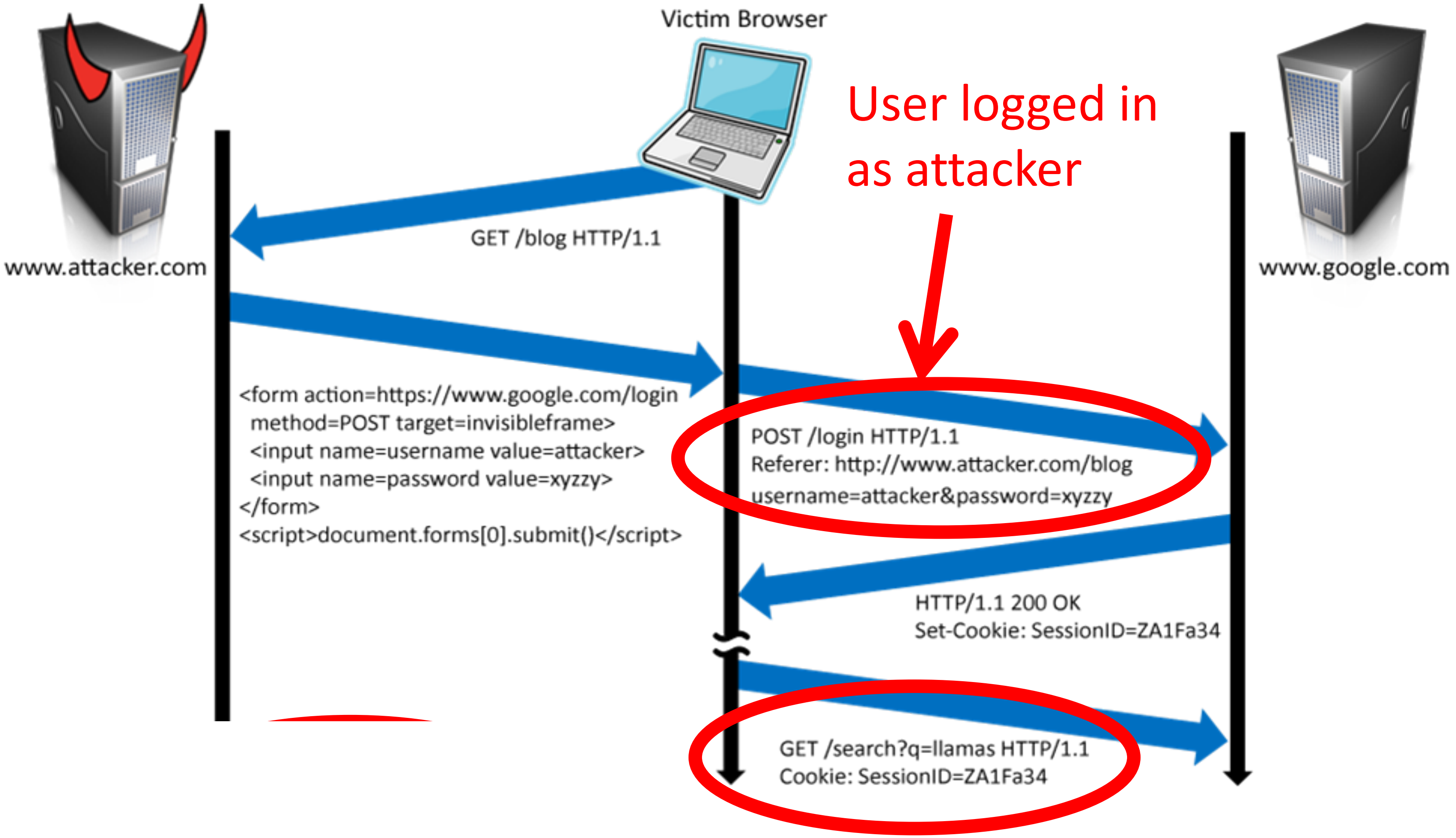


Q: how long do you stay logged on to Gmail? Financial sites?

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)

Login XSRF: Attacker logs you in as them!



```
GET /blog HTTP/1.1
```

```
<form action=https://www.google.com/login
  method=POST target=invisibleframe>
  <input name=username value=attacker>
  <input name=password value=xyzzy>
</form>
<script>document.forms[0].submit()</script>
```

```
POST /login HTTP/1.1
Referer: http://www.attacker.com/blog
username=attacker&password=xyzzy
```

```
HTTP/1.1 200 OK
Set-Cookie: SessionID=ZA1Fa34
```

```
GET /search?q=llamas HTTP/1.1
Cookie: SessionID=ZA1Fa34
```

User logged in as attacker

acker’s account reflects user’s behavior

XSRF Defenses

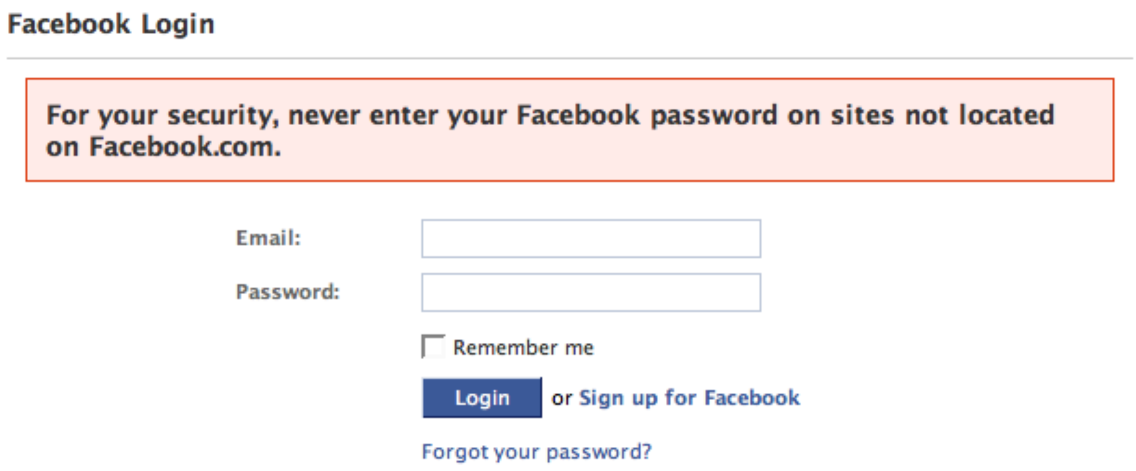
- Secret validation token

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

- Referer validation

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

Referer Validation



Facebook Login

For your security, never enter your Facebook password on sites not located on Facebook.com.

✓
```
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
- **Many web application frameworks include CSRF defenses today**

Better Idea: 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!*

Web App Vulnerabilities: Summary

- XSS (CSS) – cross-site scripting
  - Malicious code injected into a trusted context (e.g., malicious data presented by an honest website interpreted as code by the user's browser)
- SQL injection
  - Malicious data sent to a website is interpreted as code in a query to the website's back-end database
- XSRF (CSRF) – cross-site request forgery
  - Bad website forces the user's browser to send a request to a good website

Stepping Back: Two Sides of Web Security

(1) Web browser

- Responsible for securely confining content presented by visited websites

(2) Web applications

- Online merchants, banks, blogs, Google Apps …
- Mix of server-side and client-side code
  - Server-side code written in PHP, JavaScript, C++ etc.
  - Client-side code written in JavaScript (… sort of)
- Many potential bugs: XSS, XSRF, SQL injection

Review: Browser Security Model

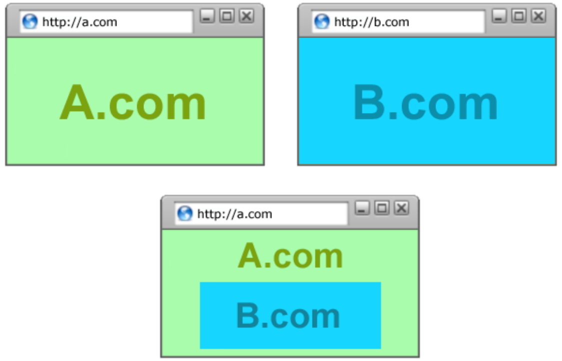
Goal 1: Protect local system from web attacker

→ Browser Sandbox

http://a.com
A.com

Goal 2: Protect/isolate web content from other web content

→ Same Origin Policy



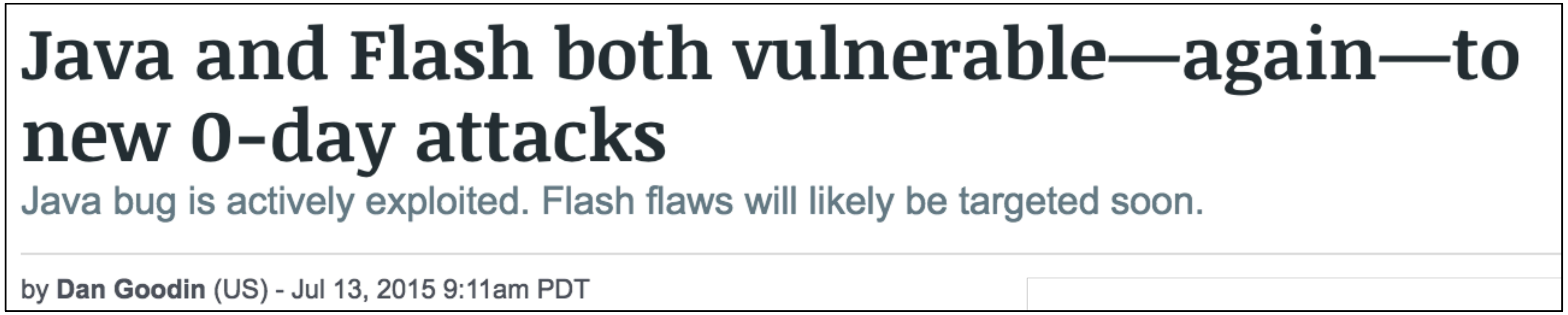
Cross-Origin Communication

- Sometimes you want to do it…
- Cross-origin Resource Sharing (CORS)
  - Access-Control-Allow-Origin: <list of domains>
    - Unfortunately, often:

      Access-Control-Allow-Origin: *
- Cross-origin client side communication
  - HTML5 postMessage between frames
    - Unfortunately, many bugs in how frames check sender's origin

What about Browser Plugins?

- **Examples:** Flash, Silverlight, Java, PDF reader
- **Goal:** enable functionality that requires transcending the browser sandbox
- Increases browser's attack surface



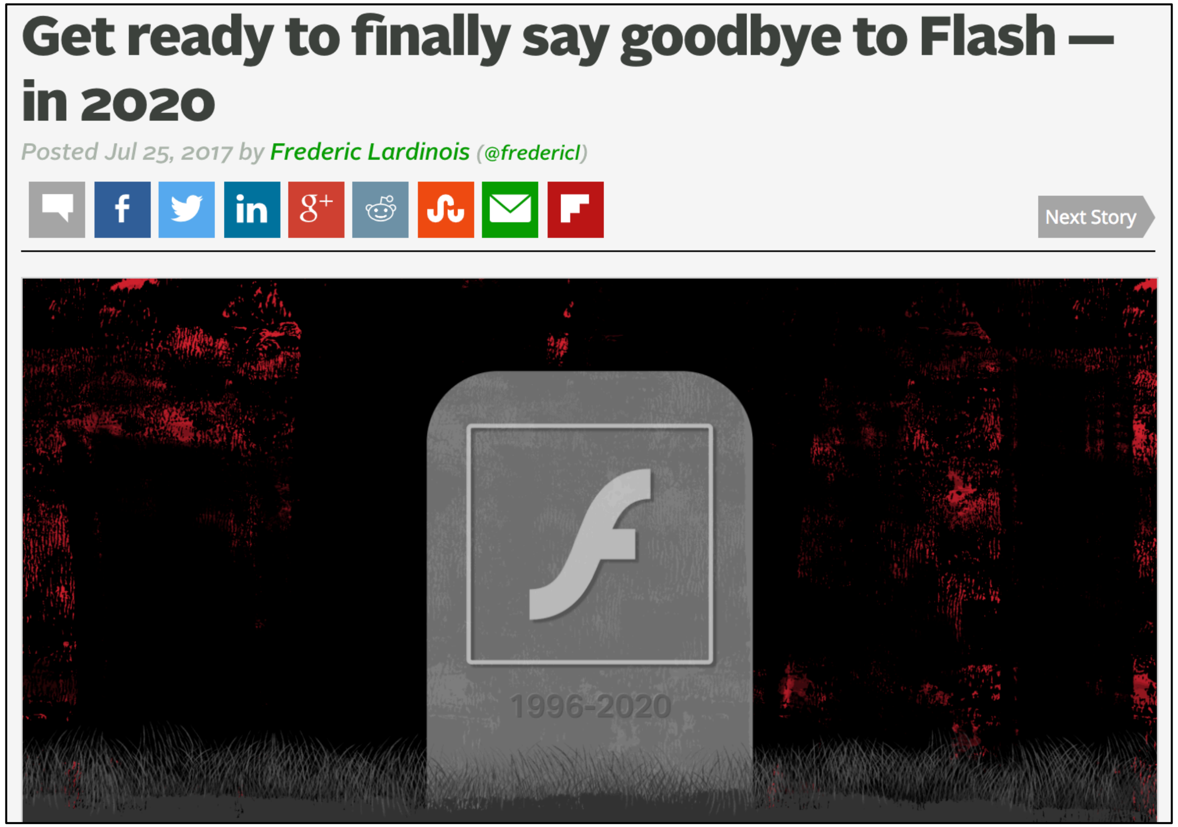
Java and Flash both vulnerable—again—to new 0-day attacks

Java bug is actively exploited. Flash flaws will likely be targeted soon.

by **Dan Goodin** (US) - Jul 13, 2015 9:11am PDT

- Good news: plugin sandboxing improving, and need for plugins decreasing (due to HTML5 and extensions)

Goodbye Flash



Get ready to finally say goodbye to Flash — in 2020

Posted Jul 25, 2017 by Frederic Lardinois (@fredericl)

"As of mid-October 2020, users started being prompted by Adobe to uninstall Flash Player on their machines since Flash-based content will be blocked from running in Adobe Flash Player after the EOL Date."
https://www.adobe.com/products/flashplayer/end-of-life.html

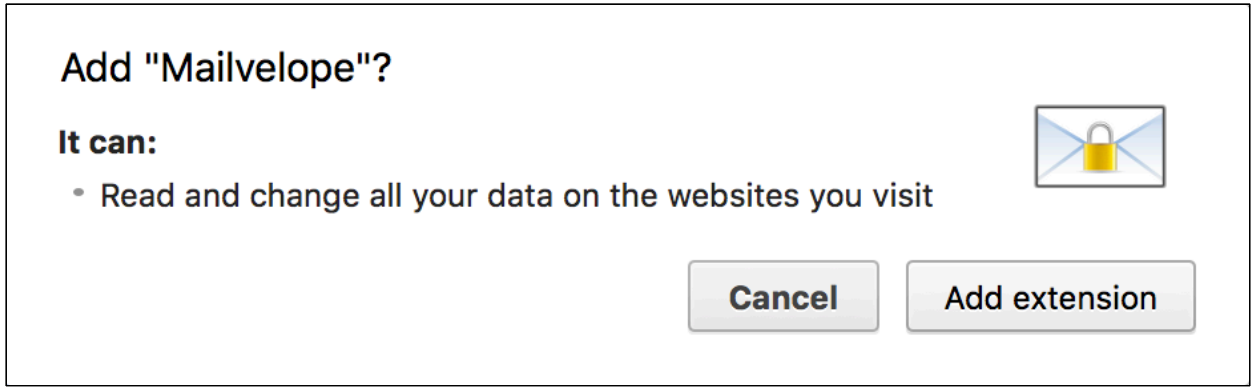
What about Browser Extensions?

- Most things you use today are probably extensions
- **Examples:** AdBlock, Ghostery, Mailvelope
- **Goal:** Extend the functionality of the browser

- (Chrome:) Carefully designed security model to **protect from malicious websites**
  - Privilege separation: extensions consist of multiple components with well-defined communication
  - Least privilege: extensions request permissions

What about Browser Extensions?

- But be wary of malicious extensions: **not subject to the same-origin policy** – can inject code into any webpage!



Add "Mailvelope"?

It can:

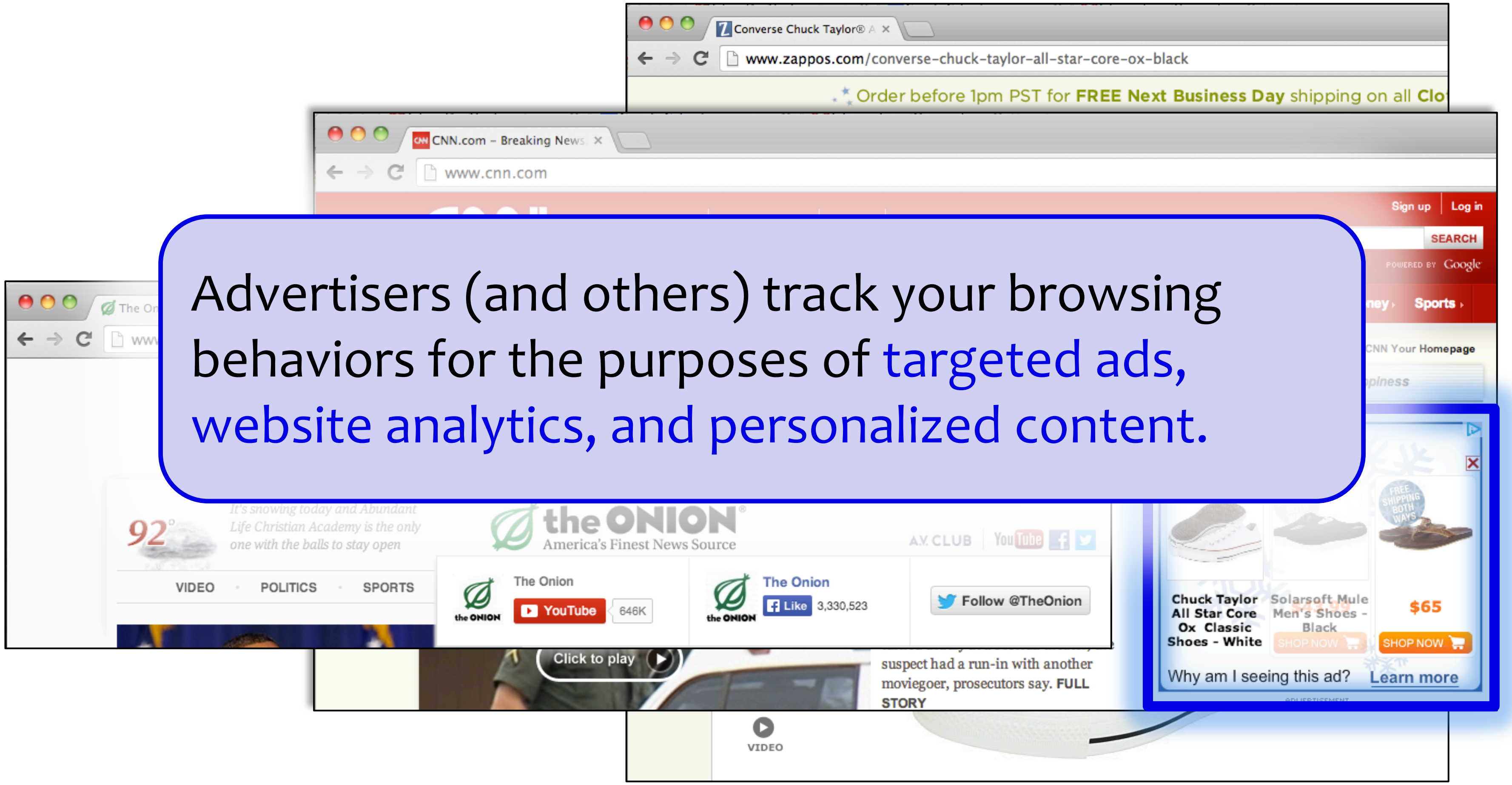
- Read and change all your data on the websites you visit

- Today: Extensions in flux – new "Manifest v3" specification from Google, trying to make things safer.

Web Security Summary

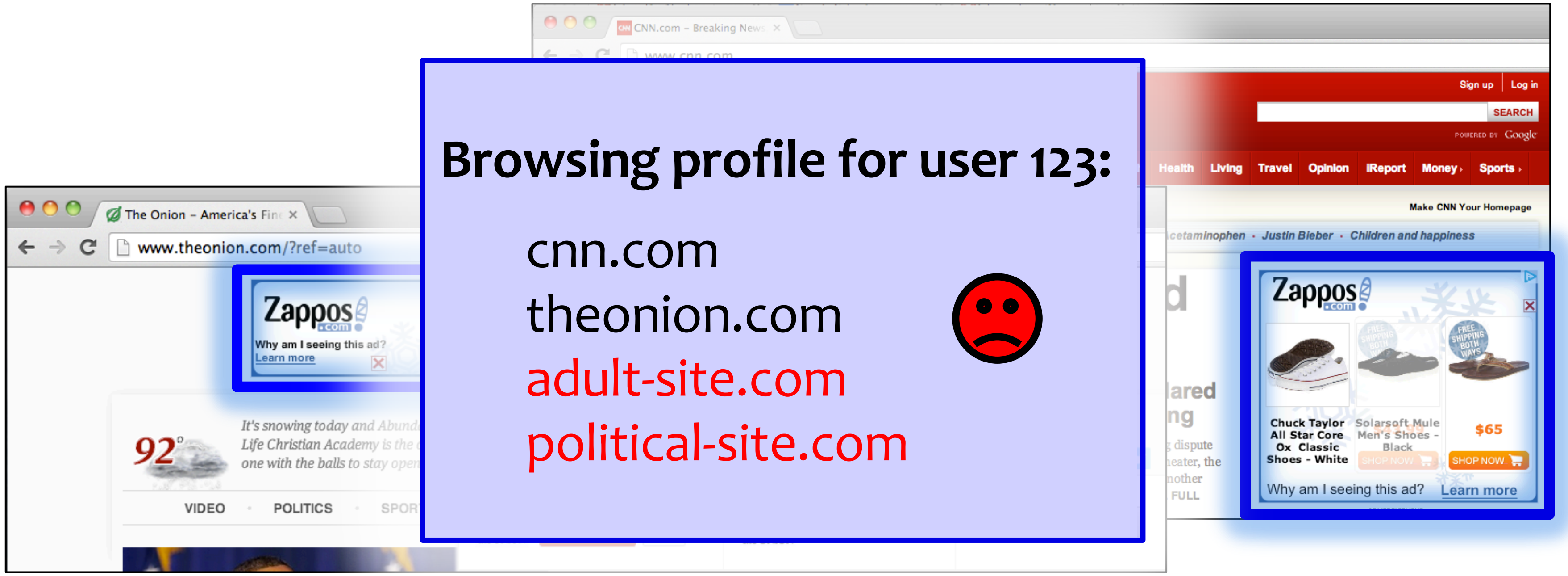
- Browser security model
  - Browser sandbox: isolate web from local machine
  - Same origin policy: isolate web content from different domains
  - Also: Isolation for plugins and extensions
- Web application security
  - How (not) to build a secure website
- Next: web ***privacy***

Ads That Follow You


Converse Chuck Taylor®
www.zappos.com/converse-chuck-taylor-all-star-core-ox-black
Order before 1pm PST for FREE Next Business Day shipping on all Clo
CNN.com – Breaking News
www.cnn.com
Sign up
Log in
SEARCH
POWERED BY Google
Sports
CNN Your Homepage
The Or
92°
It's snowing today and Abundant Life Christian Academy is the only one with the balls to stay open
the ONION
America's Finest News Source
A.V. CLUB
VIDEO
POLITICS
SPORTS
The Onion
YouTube
646K
Like 3,330,523
Follow @TheOnion
Click to play
suspect had a run-in with another moviegoer, prosecutors say. FULL STORY
VIDEO
Chuck Taylor All Star Core Ox Classic Shoes - White
Solarsoft Mule Men's Shoes - Black
$65
SHOP NOW
Why am I seeing this ad?
Learn more

Advertisers (and others) track your browsing behaviors for the purposes of targeted ads, website analytics, and personalized content.

Third-Party Web Tracking

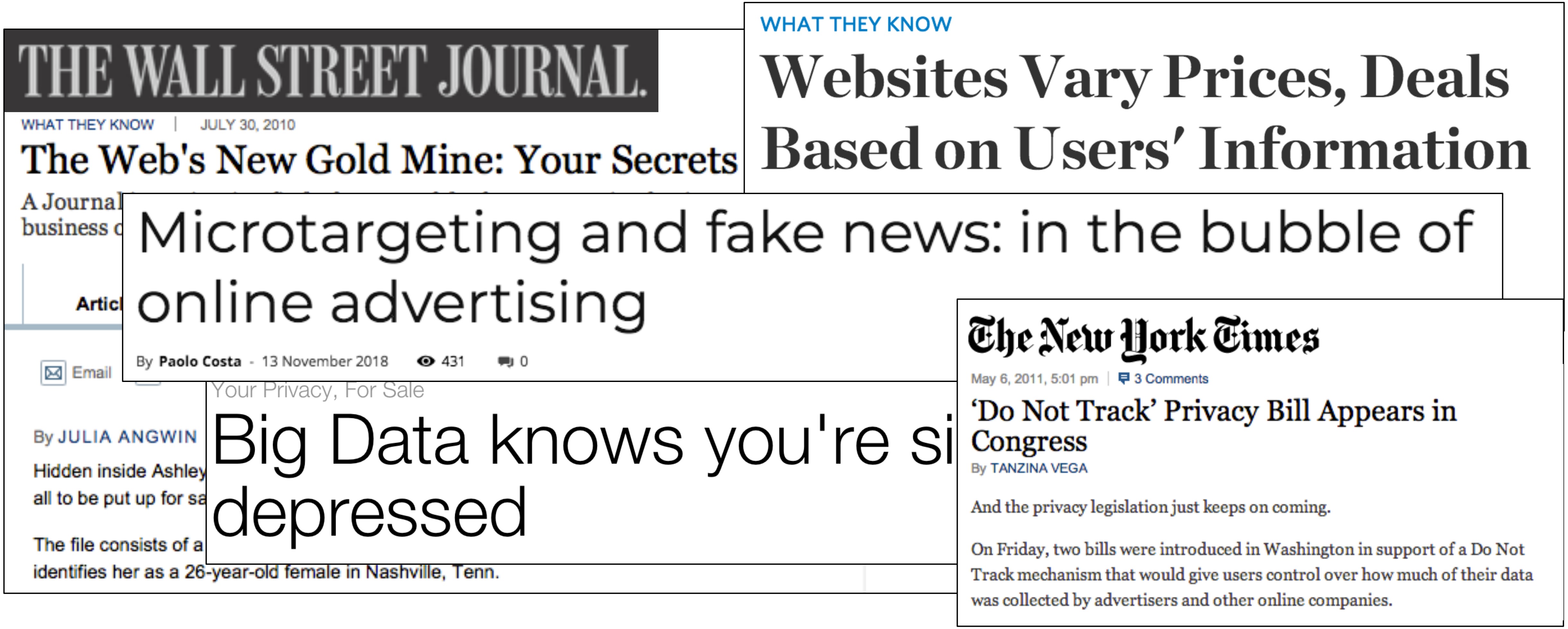


Browsing profile for user 123:

cnn.com
theonion.com
adult-site.com
political-site.com

These ads allow **criteo.com** to link your visits between sites, even if you never click on the ads.

Concerns About Privacy



THE WALL STREET JOURNAL.

WHAT THEY KNOW | JULY 30, 2010

The Web's New Gold Mine: Your Secrets

A Journal

business c

Articl

Email

By JULIA ANGWIN

Hidden inside Ashley

all to be put up for sa

The file consists of a

identifies her as a 26-year-old female in Nashville, Tenn.

WHAT THEY KNOW

Websites Vary Prices, Deals Based on Users' Information

Microtargeting and fake news: in the bubble of online advertising

By **Paolo Costa** - 13 November 2018 👁 431 0

Your Privacy, For Sale

Big Data knows you're si depressed

The New York Times

May 6, 2011, 5:01 pm | 3 Comments

'Do Not Track' Privacy Bill Appears in Congress

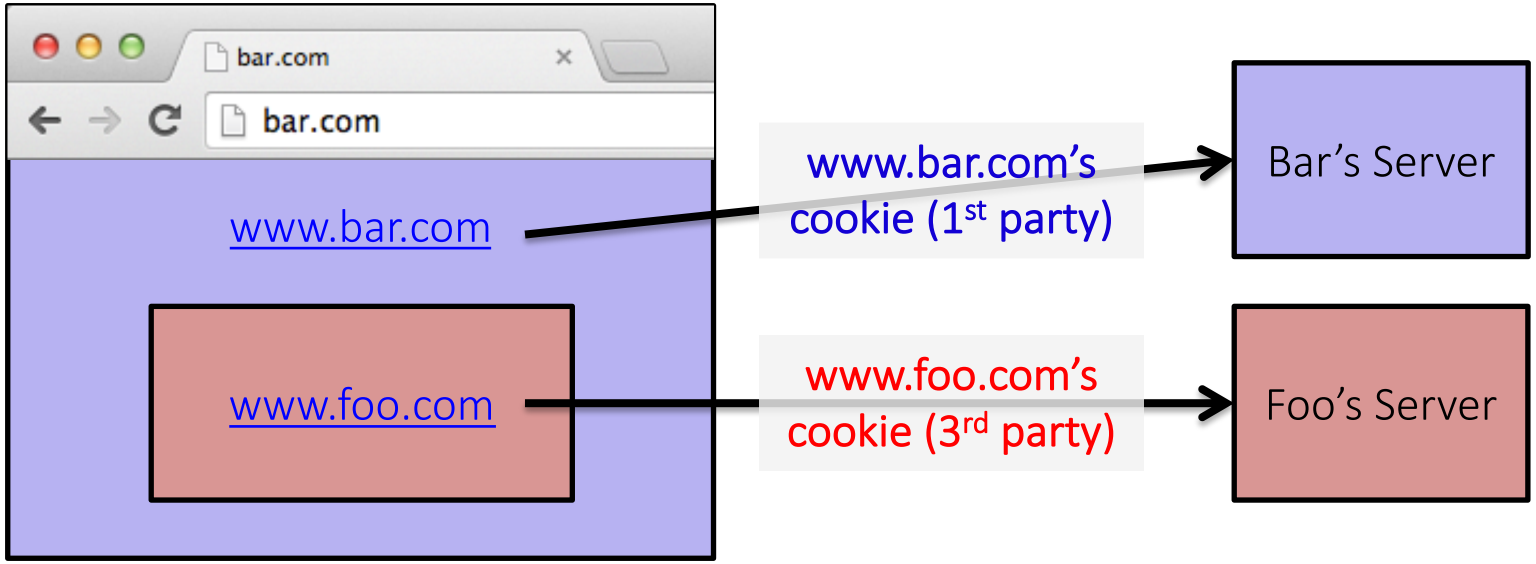
By TANZINA VEGA

And the privacy legislation just keeps on coming.

On Friday, two bills were introduced in Washington in support of a Do Not Track mechanism that would give users control over how much of their data was collected by advertisers and other online companies.

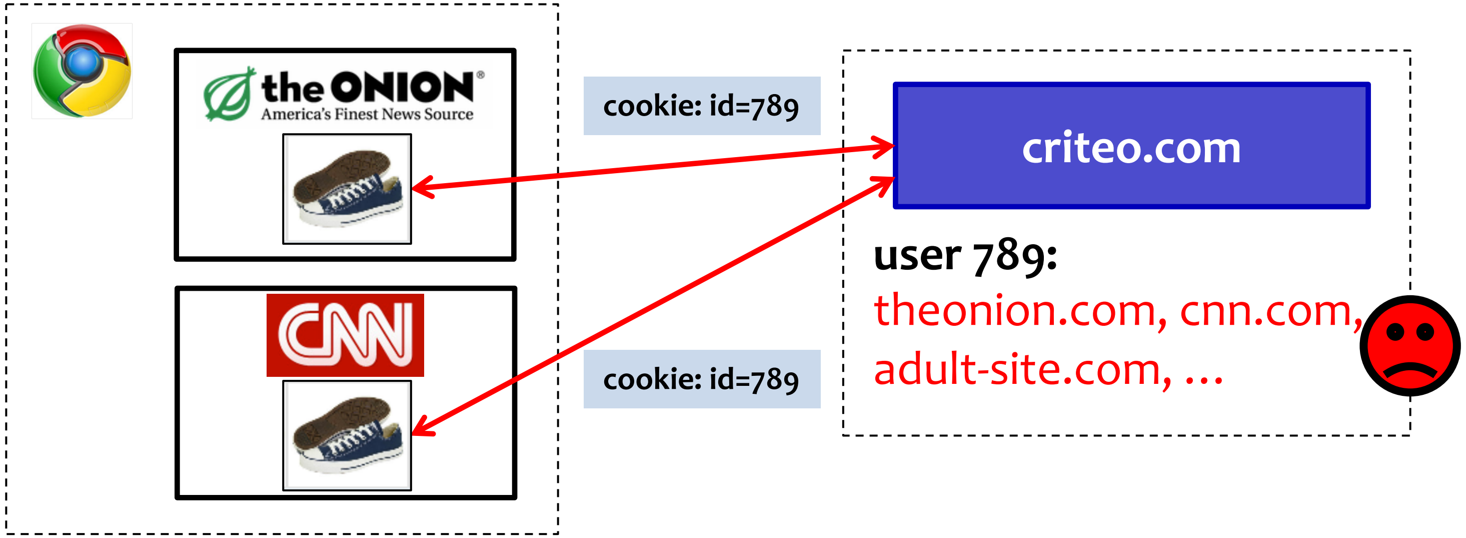
Reminder: First and Third Parties

- First-party cookie: belongs to top-level domain.
- Third-party cookie: belongs to domain of embedded content (such as image, iframe).


bar.com
bar.com
www.bar.com
www.foo.com
www.bar.com's cookie (1st party)
www.foo.com's cookie (3rd party)
Bar's Server
Foo's Server

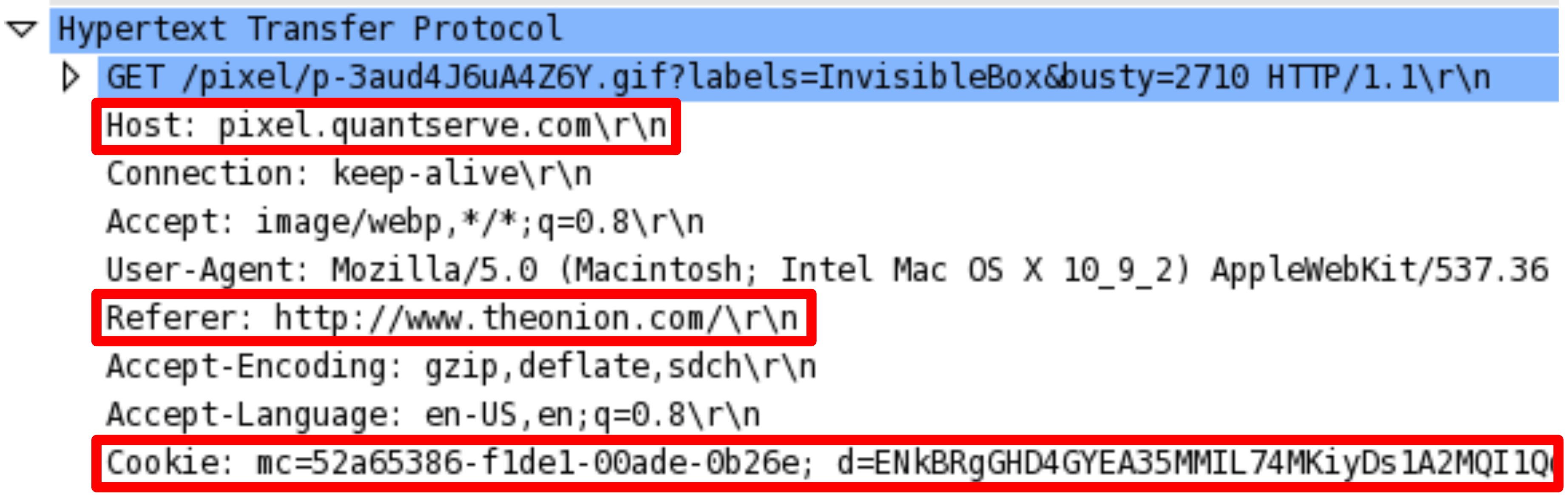
Cookies (etc.) Enable “Anonymous” Tracking

Trackers included in other sites use third-party cookies containing unique identifiers to create browsing profiles.



Basic Tracking Mechanisms

- Tracking requires:
  (1) re-identifying a user.
  (2) communicating id + visited site back to tracker.



```
▽ Hypertext Transfer Protocol
  ▷ GET /pixel/p-3aud4J6uA4Z6Y.gif?labels=InvisibleBox&busty=2710 HTTP/1.1\r\n
    Host: pixel.quantserve.com\r\n
    Connection: keep-alive\r\n
    Accept: image/webp,*/*;q=0.8\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_2) AppleWebKit/537.36
    Referer: http://www.theonion.com/\r\n
    Accept-Encoding: gzip,deflate,sdch\r\n
    Accept-Language: en-US,en;q=0.8\r\n
    Cookie: mc=52a65386-f1de1-00ade-0b26e; d=ENkBRgGHD4GYEA35MMIL74MKiyDs1A2MQI1Q
```

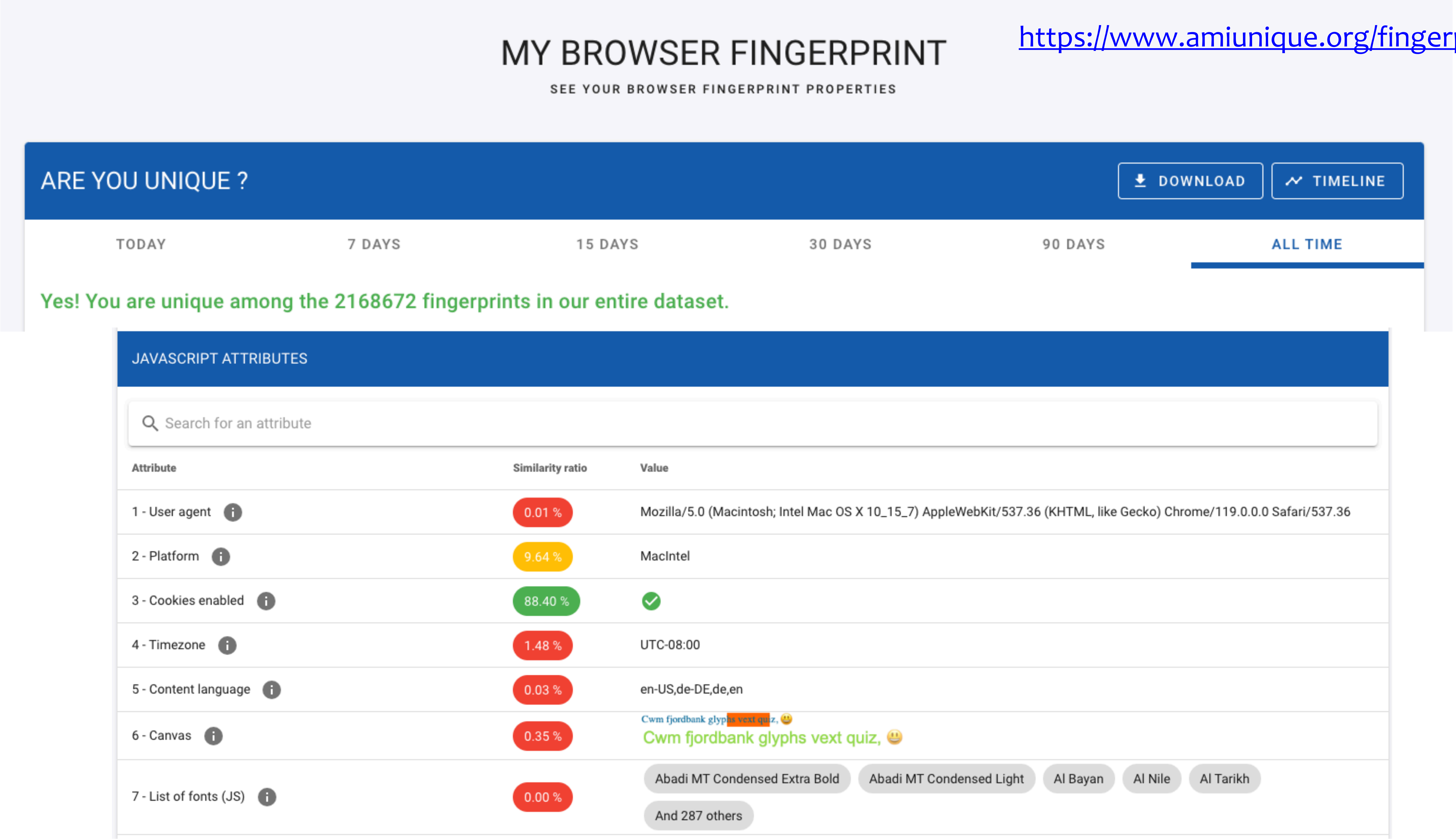
Lots of Places to Store Identifiers…

- HTTP Cookies
- HTTP Auth
- HTTP Etags
- Content cache
- IE userData
- HTML5 protocol and content handlers
- HTML5 storage
- Flash cookies
- Silverlight storage
- TLS session ID & resume
- Browsing history
- window.name
- HTTP STS
- DNS cache
- “Zombie” cookies that respawn (http://samy.pl/evercookie)

You Don’t Need Identifiers: Fingerprinting

- User agent
- HTTP ACCEPT headers
- Browser plug-ins
- MIME support
- Clock skew
- Installed fonts
- Cookies enabled?
- Browser add-ons
- Screen resolution
- HTML5 canvas (differences in graphics SW/HW!)
- Etc. etc.

https://www.amiunique.org/fingerprint



MY BROWSER FINGERPRINT

SEE YOUR BROWSER FINGERPRINT PROPERTIES

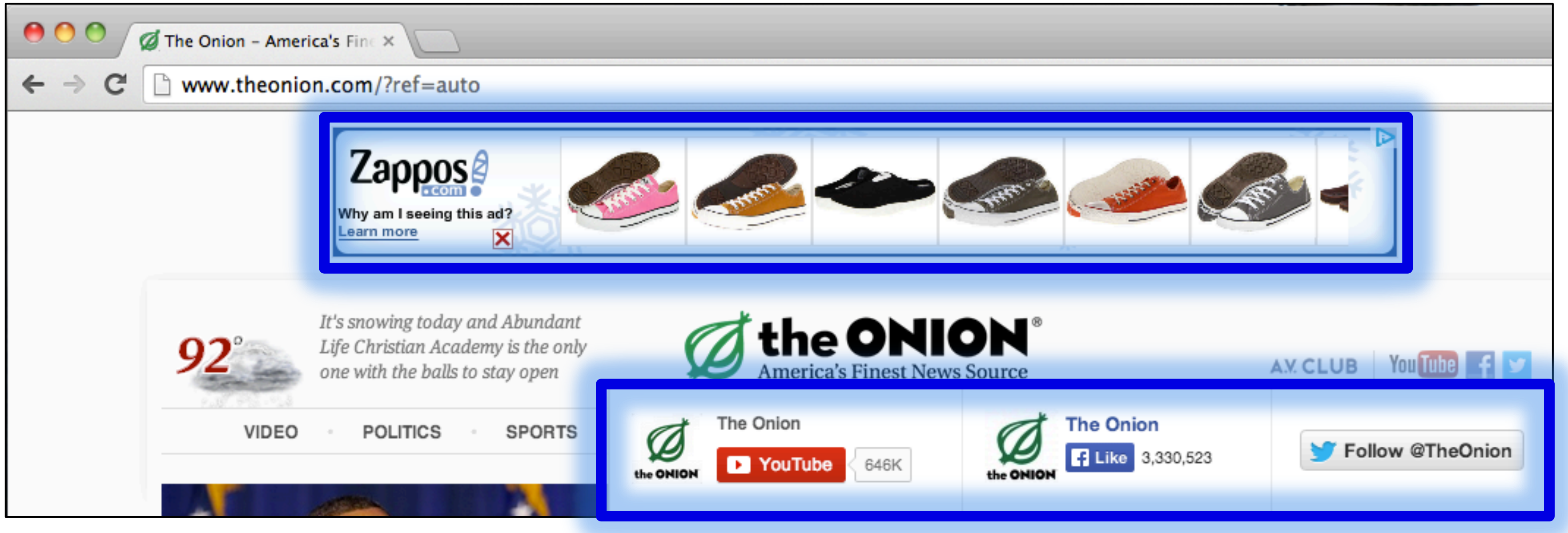
ARE YOU UNIQUE ?

Yes! You are unique among the 2168672 fingerprints in our entire dataset.

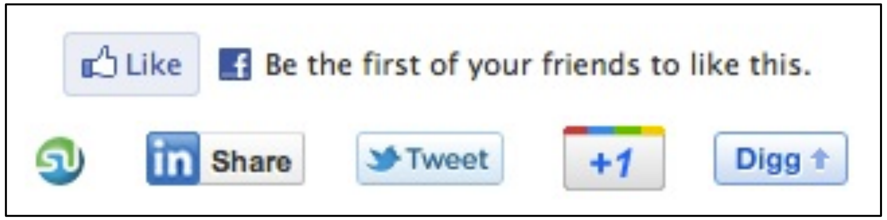
JAVASCRIPT ATTRIBUTES

Attribute	Similarity ratio	Value
1 - User agent	0.01 %	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
2 - Platform	9.64 %	MacIntel
3 - Cookies enabled	88.40 %	✓
4 - Timezone	1.48 %	UTC-08:00
5 - Content language	0.03 %	en-US,de-DE,de,en
6 - Canvas	0.35 %	Cwm fjordbank glyphs vext quiz, 😃 Cwm fjordbank glyphs vext quiz, 😃
7 - List of fonts (JS)	0.00 %	Abadi MT Condensed Extra Bold Abadi MT Condensed Light Al Bayan Al Nile Al Tarikh And 287 others

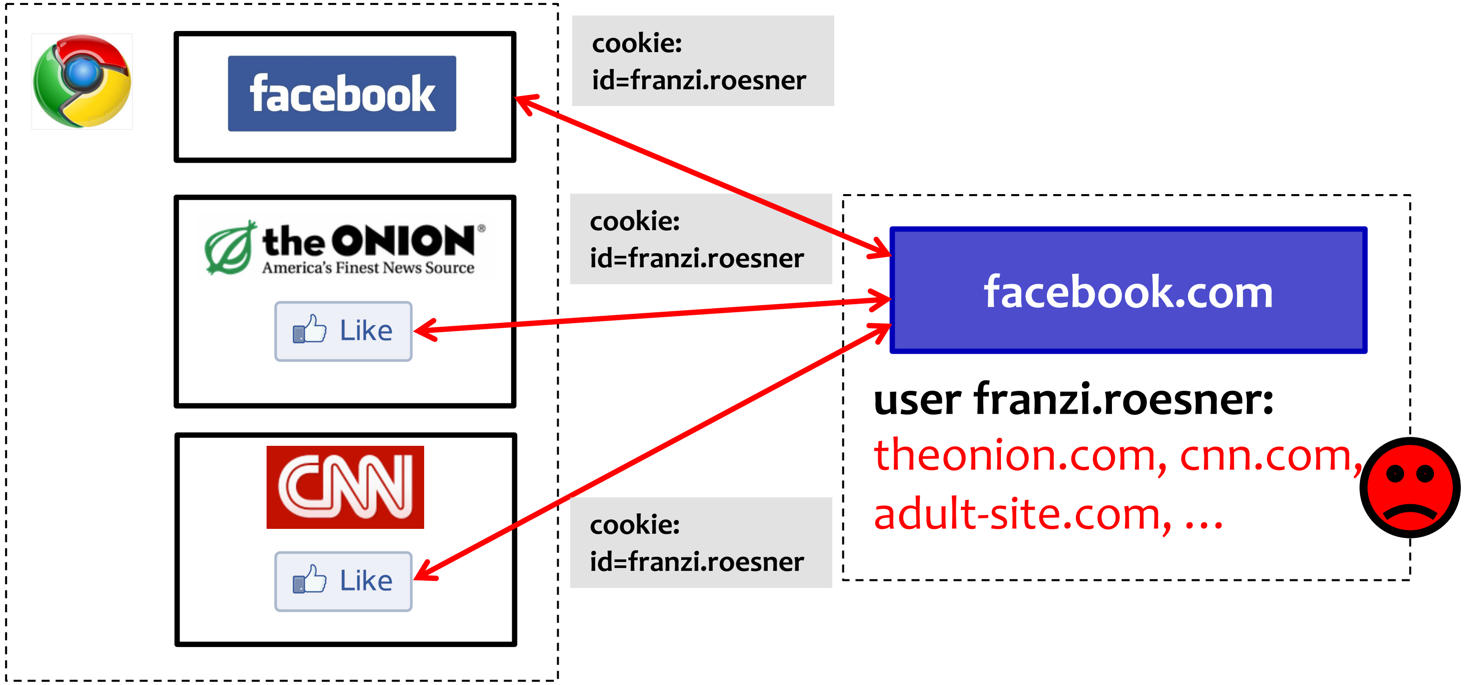
Other Trackers?


The Onion – America's Fin
www.theonion.com/?ref=auto
Zappos.com
Why am I seeing this ad?
Learn more
92°
It's snowing today and Abundant Life Christian Academy is the only one with the balls to stay open
the ONION
America's Finest News Source
A.V. CLUB
YouTube
VIDEO
POLITICS
SPORTS
The Onion
YouTube
646K
The Onion
Like
3,330,523
Follow @TheOnion

"Personal" Trackers



“Personal” Tracking



- Tracking is not anonymous (linked to accounts).
- Users directly visit tracker’s site → evades some defenses.