CSE 484: Computer Security and Privacy

Authentication + Tracking

Spring 2023

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 ...

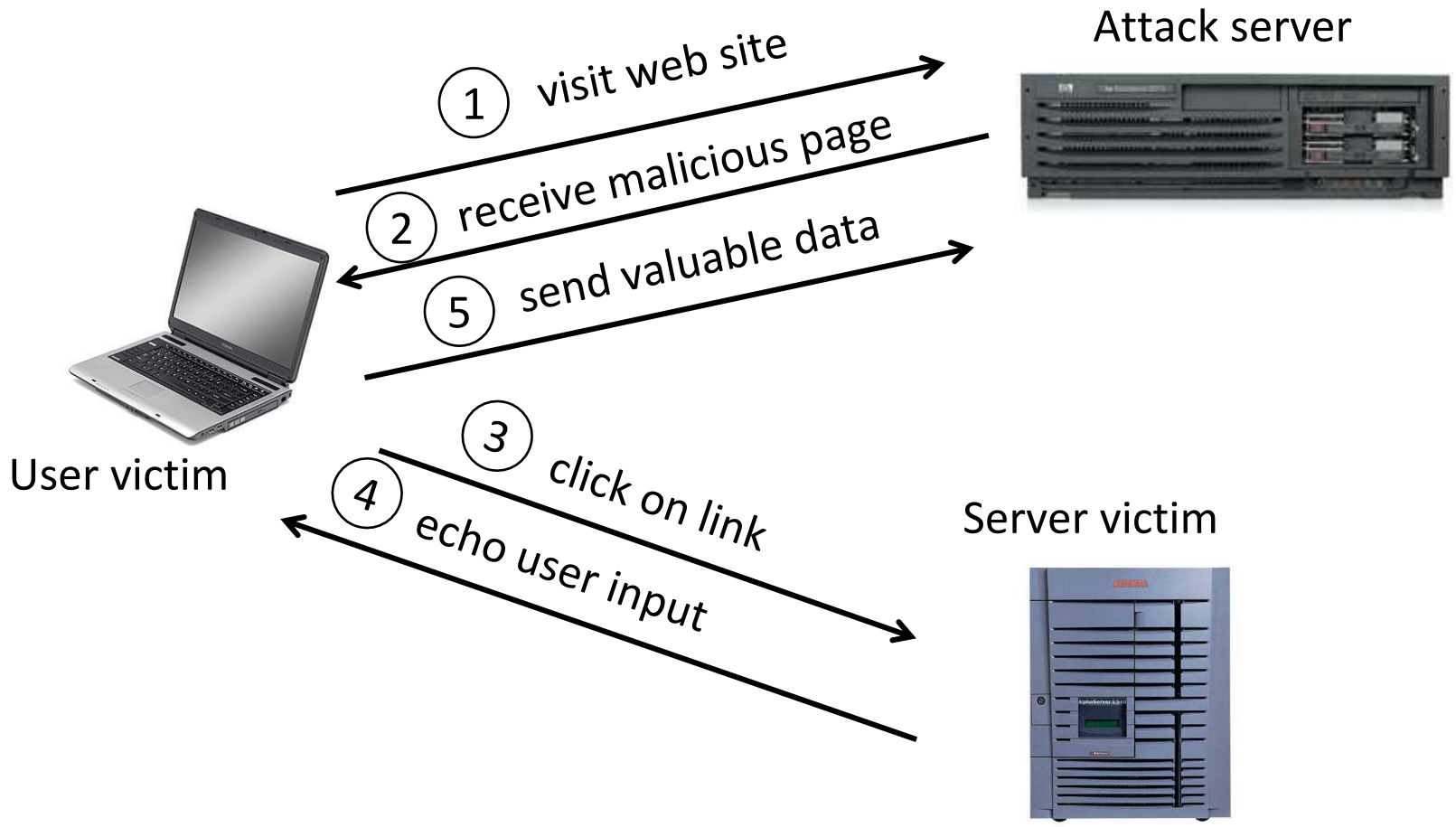
Logistics

- Lab 2 is due next week
  - Remember we have a lot of resources/recordings on lab2 stuff!
- Lab 3 will go out shortly(?) after Lab 2 is due

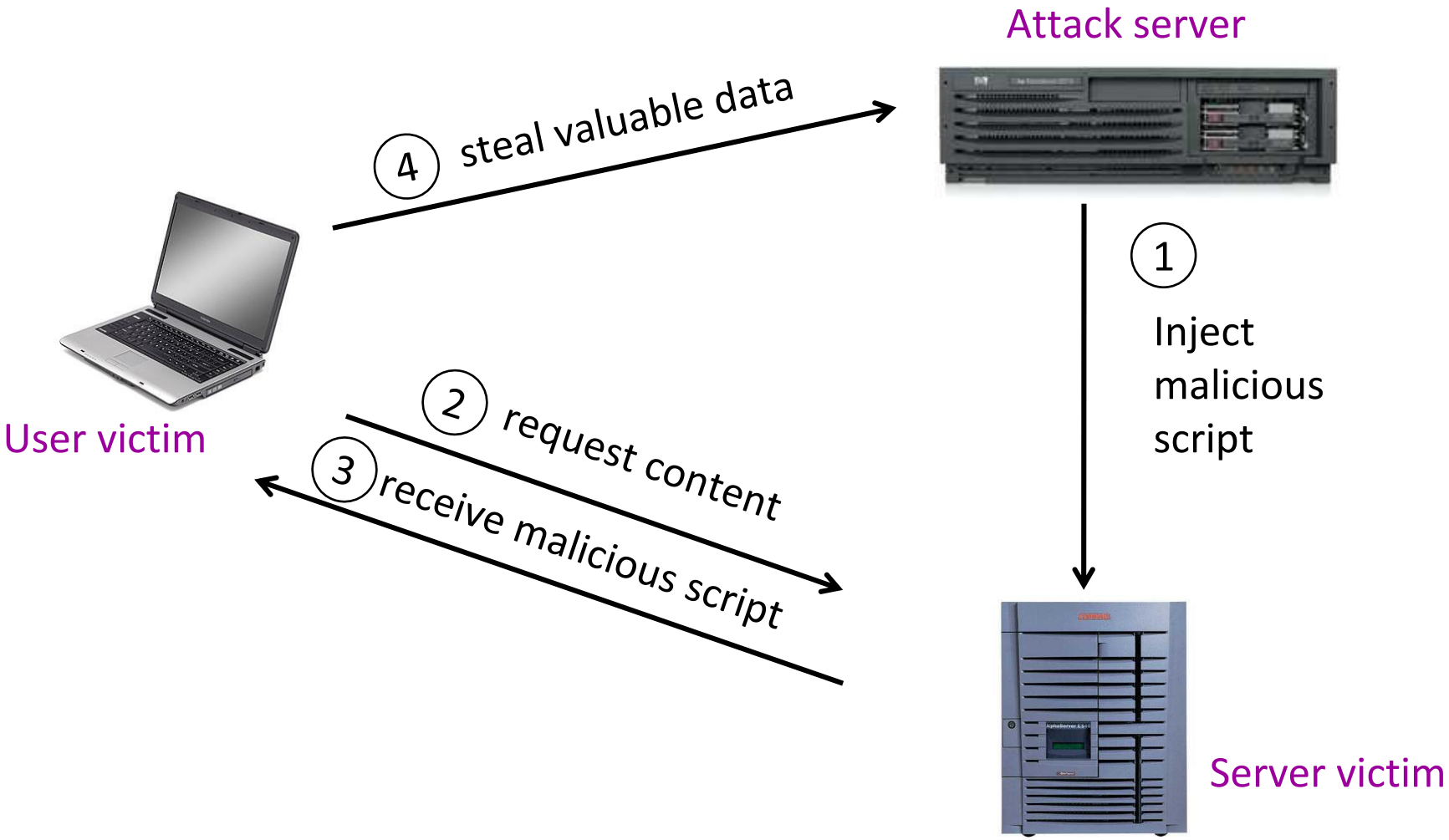
Surprise not-quiz time

XSS again

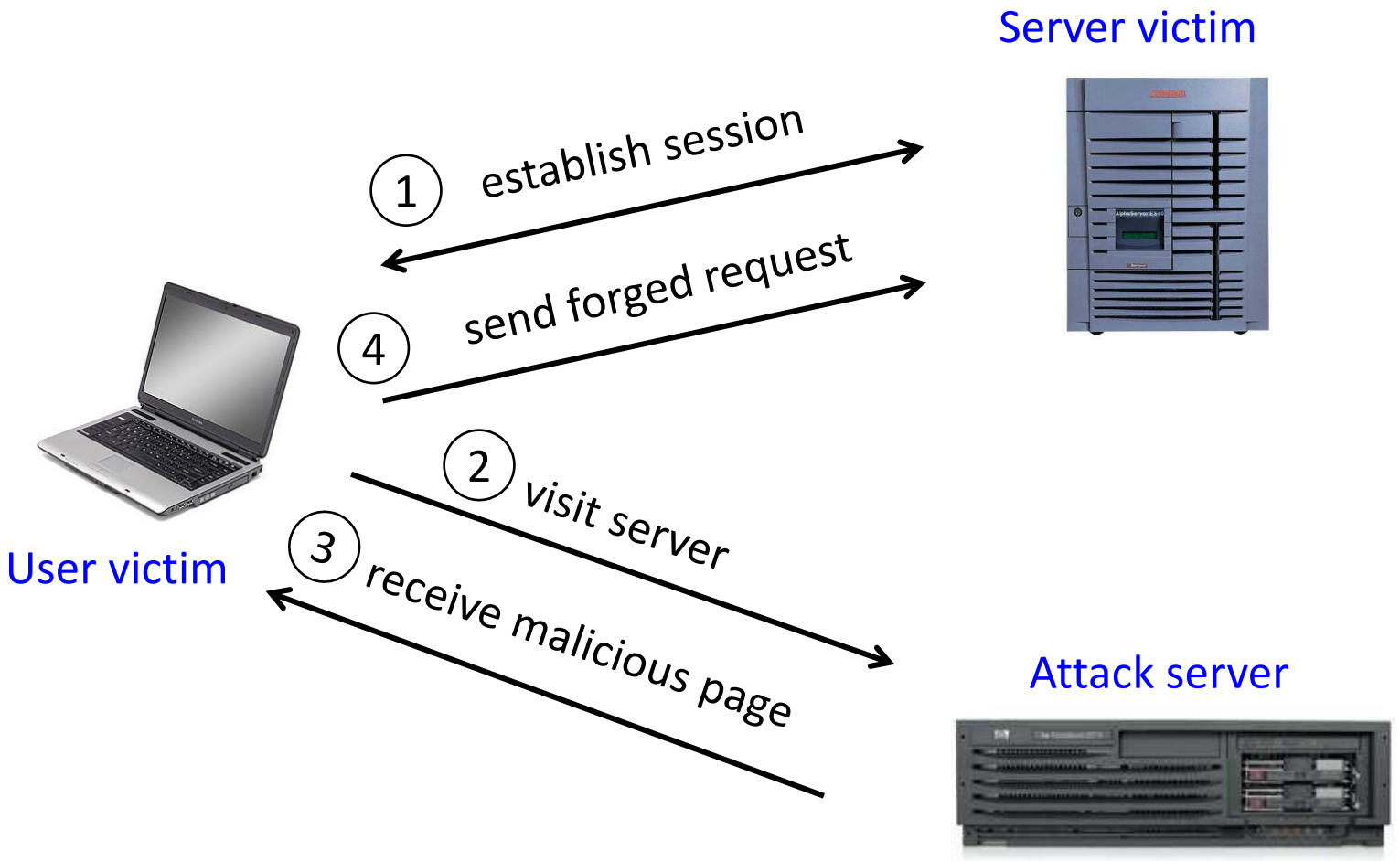
Reflected XSS



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

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

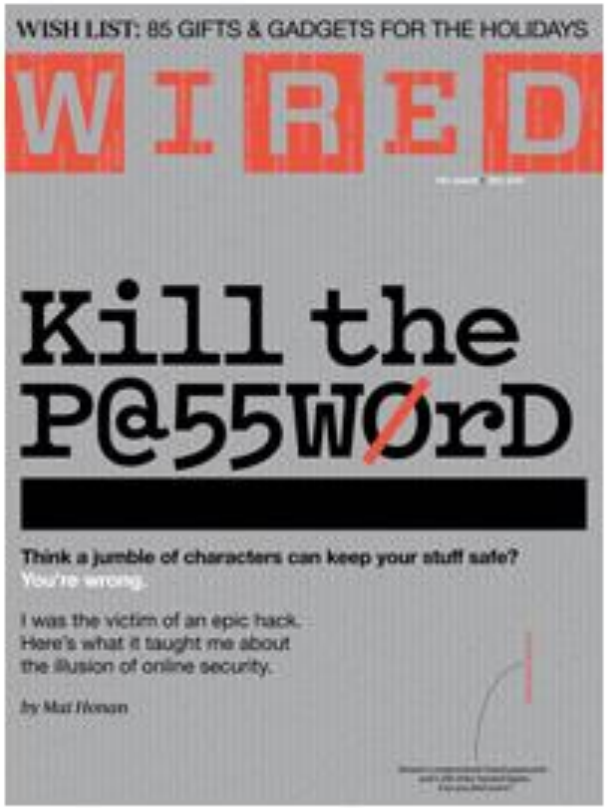
- Old recommendation:
  - 7 or 8 characters, at least 3 out of {digits, upper-case, lower-case, non-alphanumeric}, no dictionary words, change every 4 months, password may not be similar to previous 12 passwords…
- **But** … results in frustrated users and less security
  - Burdens of devising, learning, 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."

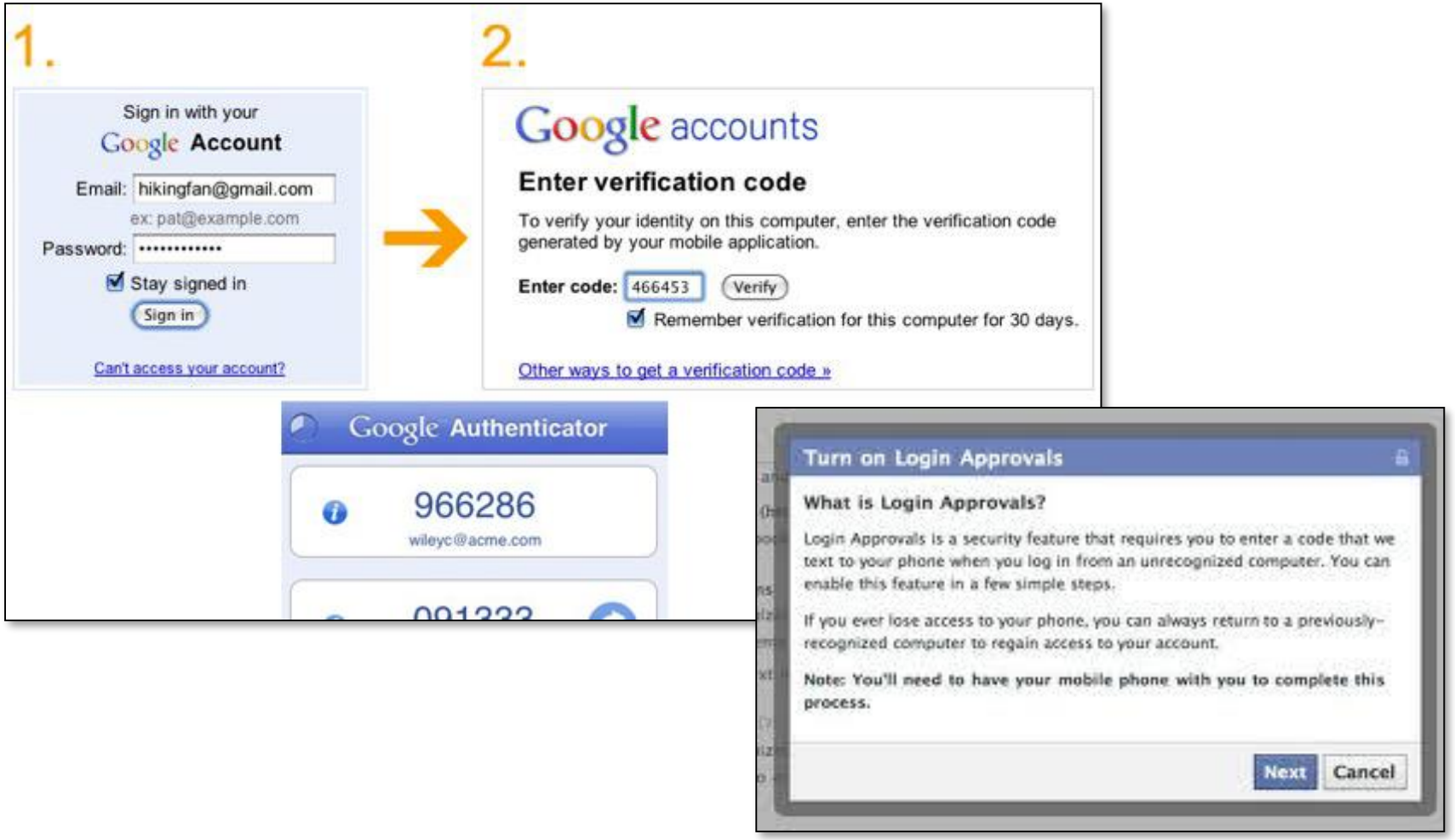
Improving(?) Passwords

- 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?

Multi-Factor Authentication



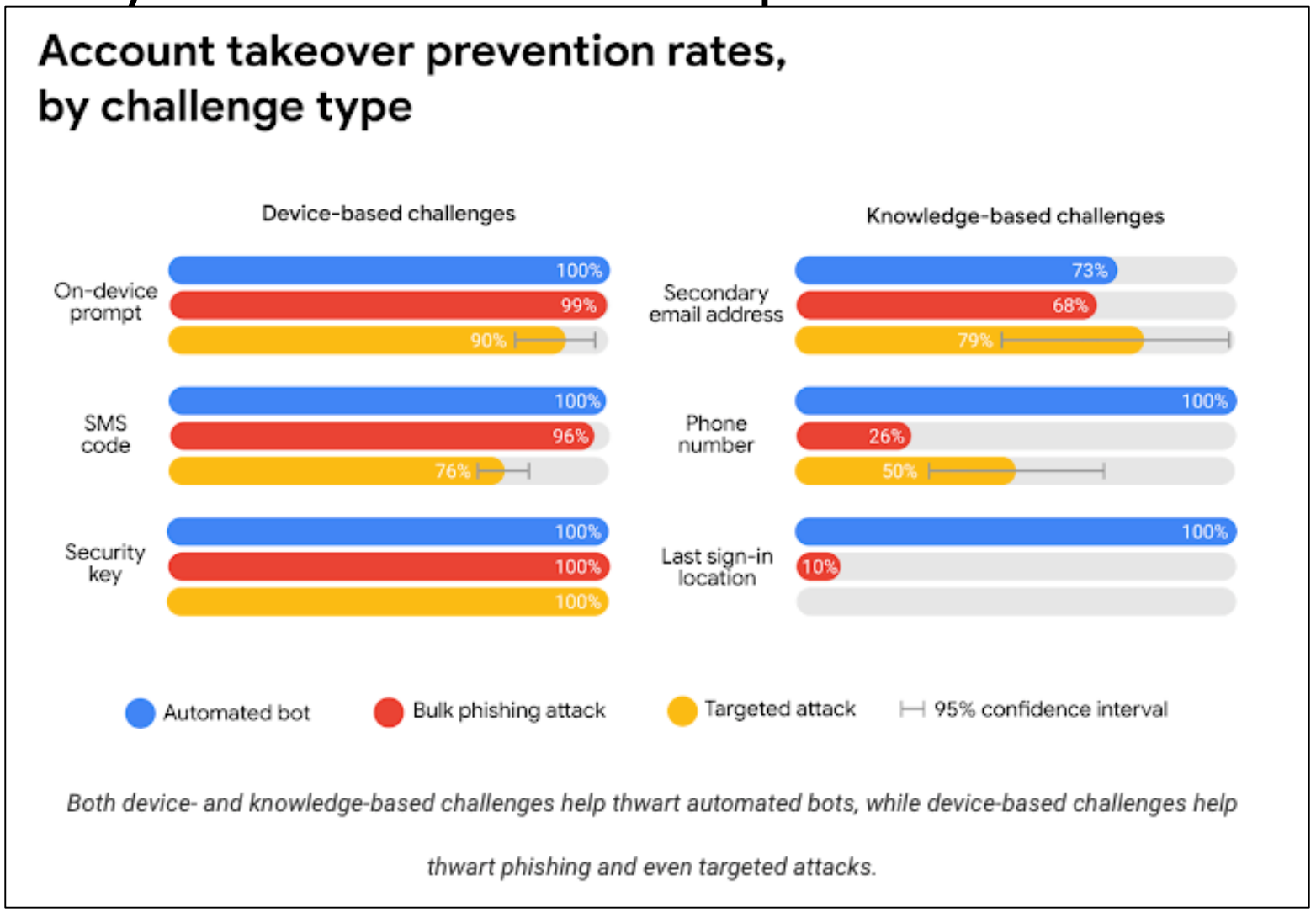
Questions:

Do you use 2-factor auth?
Do you use a password manager?
Why or why not?

How to compromise account protected with hardware second factor?

https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html

Secondary Factors Do Help!



Why does 2FA (sometimes) work?

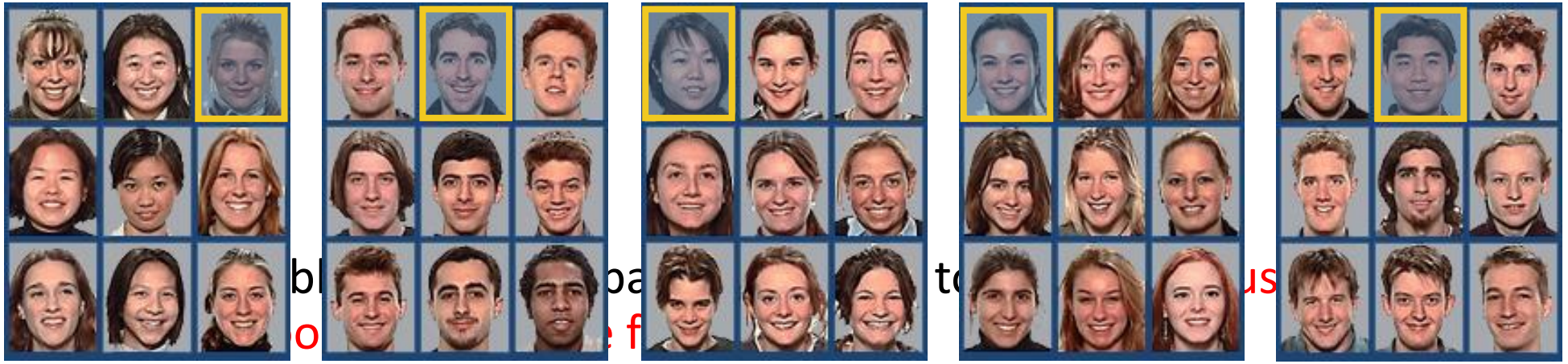
- Stops phishing, when it is hardware token

- Doesn’t when it is SMS ☹
  - (Curious for an example? Attend Ariana’s lecture in 1.5 weeks!)

Hardware 2FA tokens (U2F/FIDO)

Graphical Passwords

- Many variants… one example: Passfaces
  - Assumption: easy to recall faces

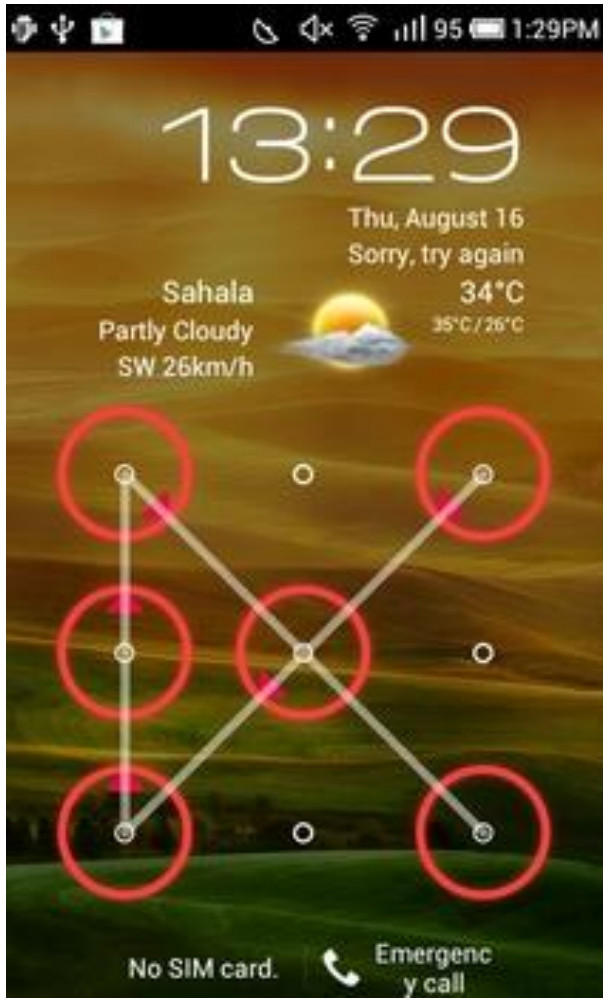


Graphical Passwords

- Another variant: draw on the image (Windows 8)

- Problem: users choose predictable points/lines

Unlock Patterns



- Problems:
  - Predictable patterns (familiar pattern by now)
  - Smear patterns
  - Side channels: apps can use accelerometer and gyroscope to extract pattern!

What About Biometrics?

- Authentication: **What you are**
- Unique identifying characteristics to authenticate user or create credentials
  - Biological and physiological: Fingerprints, iris scan
  - Behaviors characteristics - how perform actions: Handwriting, typing, gait
- Advantages:
  - Nothing to remember
  - Passive
  - Can't share (generally)
  - With perfect accuracy, could be fairly unique

What are reasons to use/*not* use biometrics?

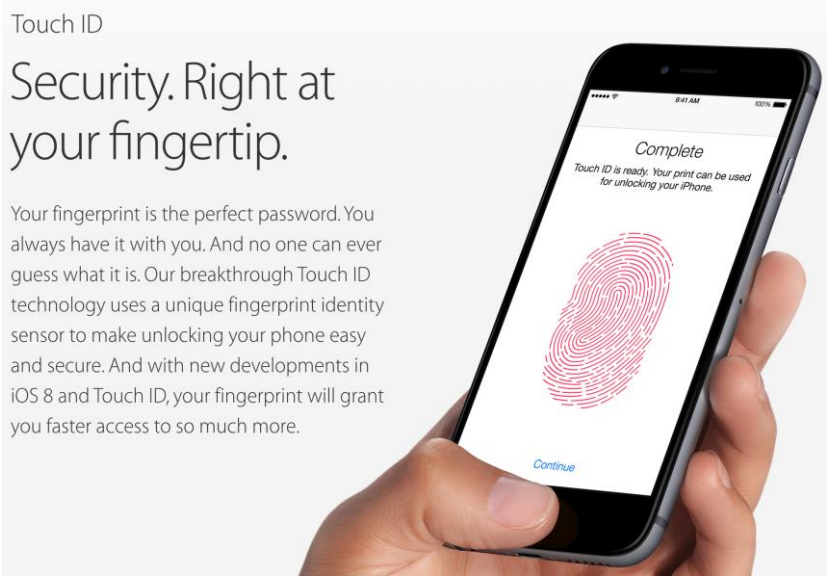
- Canvas

Issues with Biometrics

- Private, but not secret
  - Maybe encoded on the back of an ID card?
  - Maybe encoded on your glass, door handle, ...
  - Sharing between multiple systems?
- Revocation is difficult (impossible?)
  - Sorry, your iris has been compromised, please create a new one...
- Physically identifying
  - Soda machine to cross-reference fingerprint with DMV?
- Birthday paradox
  - With false accept rate of 1 in a million, probability of false match is above 50% with only 1609 samples

Attacking Biometrics

- An adversary might try to steal biometric info
  - Malicious fingerprint reader
    - Consider when biometric is used to derive a cryptographic key
  - Residual fingerprint on a glass



Passkeys (2023)

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

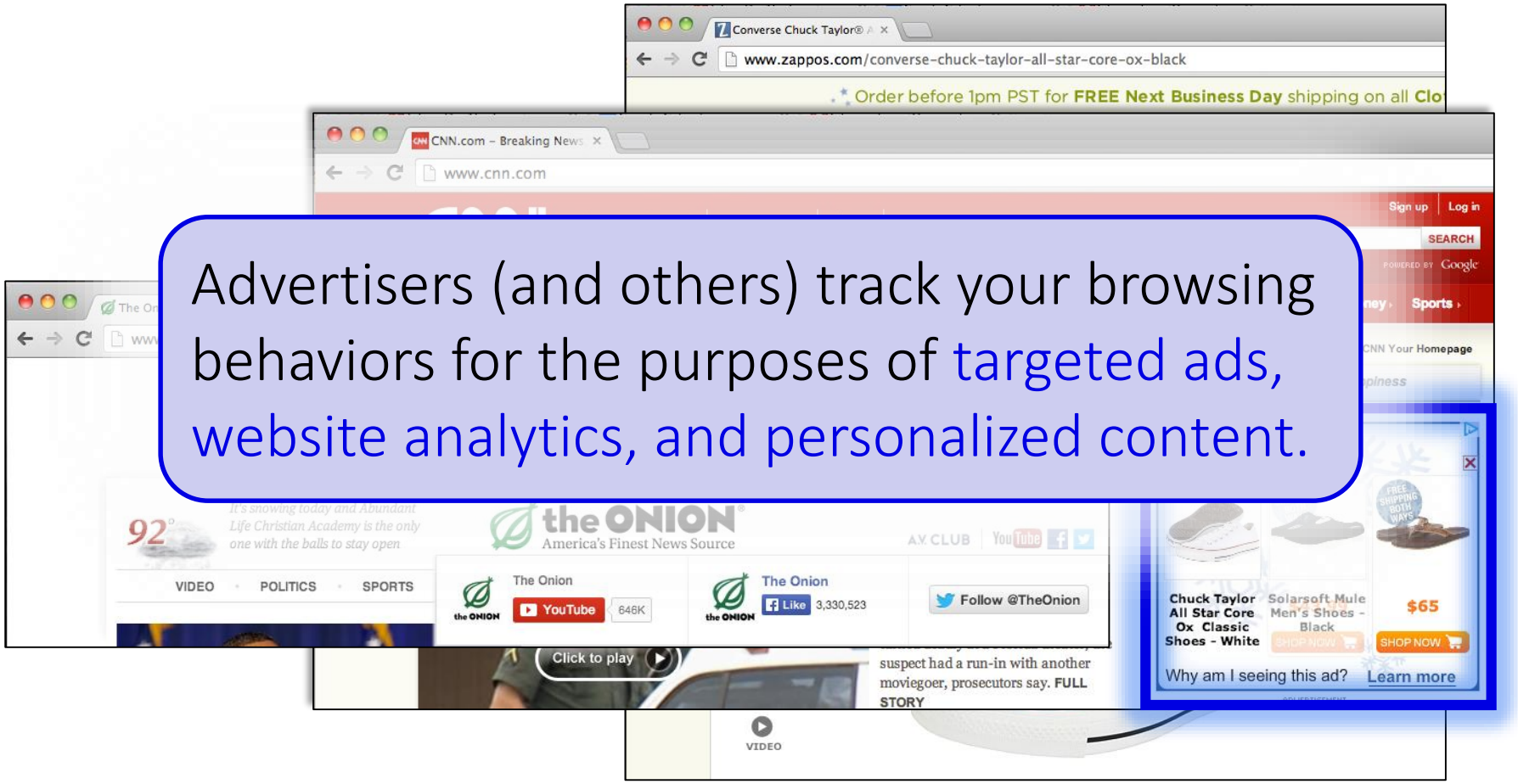
- Basic goals:
  - Store some sort of key on user end-devices
  - Use that key to login to Stuff
  - Don’t allow losing the key
  - Somehow make the key moving between devices Easy

Privacy and web tracking

A topic in flux

- Tracking via cookies
- Tracking via other methods
- Fingerprinting

Ads That Follow You



Third-Party Web Tracking

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

chiefmartec.com April 2020

Marketing Technology Landscape

The Martech 5000

Total Solutions	8,000
Advertising & Promotion	922
Content & Experience	1,936
Social & Relationships	1,969
Commerce & Sales	1,314
Data	1,258
Management	601

Access all the data of this landscape & more at martech5000.com

2019
7,040 solutions

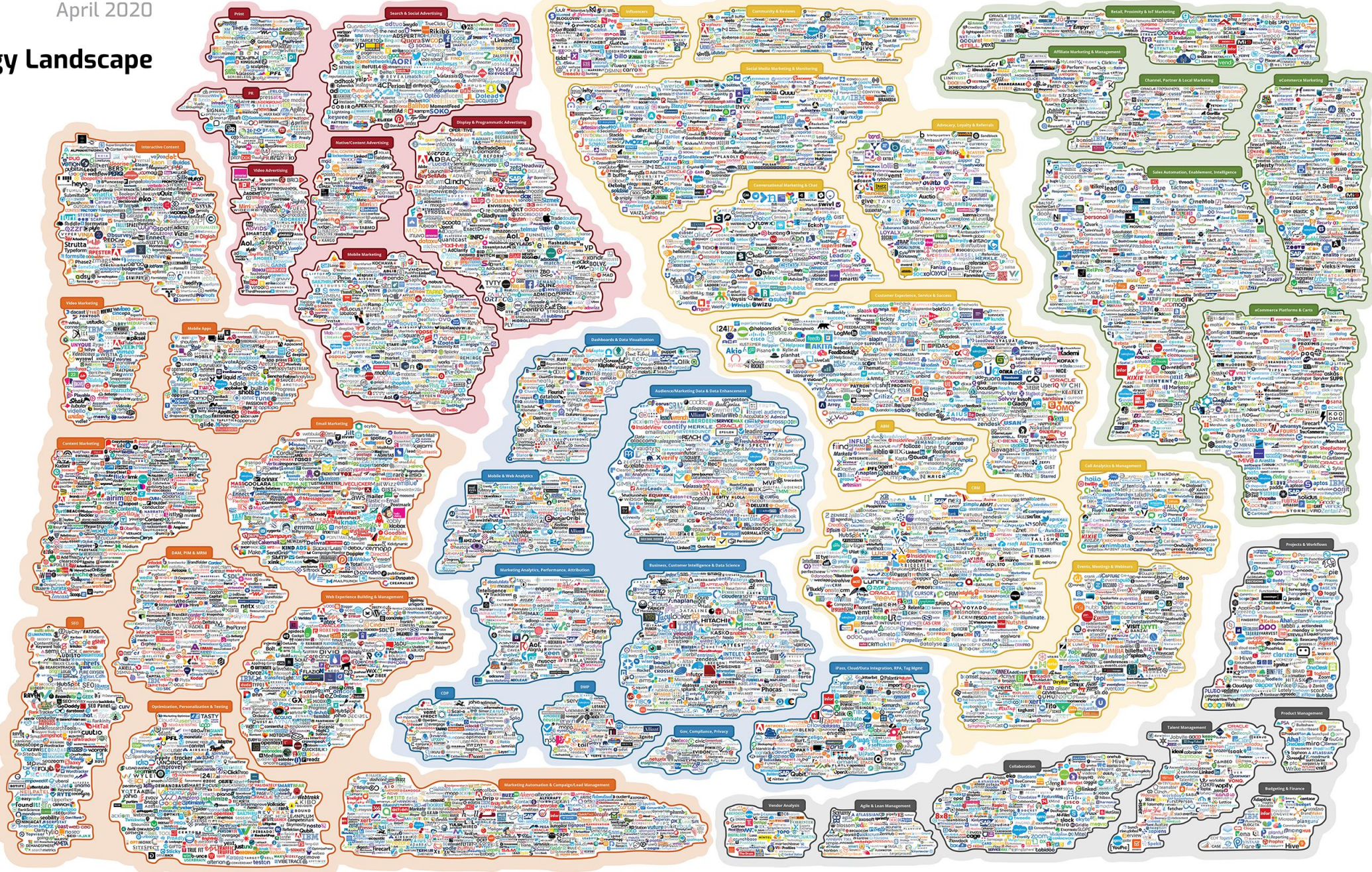
2018
6,829 solutions

2017
5,381 solutions

2016
3,874 solutions

2015
1,876 solutions

2014
947 solutions



Produced by Scott Brinker (@chiefmartec) and Blue Green Brands (@bluegreenbrands).

MartechMap an initiative by chiefmartec & MartechTribe

2022 Marketing Technology Landscape May 2022

Advertising & Promotion

Display & Programmatic Advertising

Mobile Marketing

Native/Content Advertising

PR

Print

Search & Social Advertising

Video Advertising

Content & Experience

Content Marketing

CMS & Web Experience Management

DAM & MRM & PIM

Email Marketing

Interactive Content

Marketing Automation & Campaign/Lead Management

Mobile Apps

Optimization Personalization & Testing

SEO

Video Marketing

Social & Relationships

ABM

Call Analytics & Management

Customer Experience Service & Success

Influencers

CRM

Advocacy Loyalty & Referrals

Community & Reviews

Events, Meetings & Webinars

Social Media Marketing & Monitoring

Live Chat & Chatbots

Commerce & Sales

Retail, Proximity & IOT

Affiliate Marketing & Management

Sales Automation Enablement & Intelligence

eCommerce Platforms & Carts

eCommerce Marketing

Channel Partner & Local Marketing

Data

Marketing Analytics Performance & Attribution

Audience/Marketing Data & Data Enhancement

Ipaas Cloud/Data Integration & Tag Management

Business/Customer Intelligence & Data Science

DMP

Dashboards & Data Visualization

Governance Compliance And Privacy

Mobile & Web Analytics

Customer Data Platform

Management

Agile & Lean Management

Collaboration

Talent Management

Budgeting & Finance

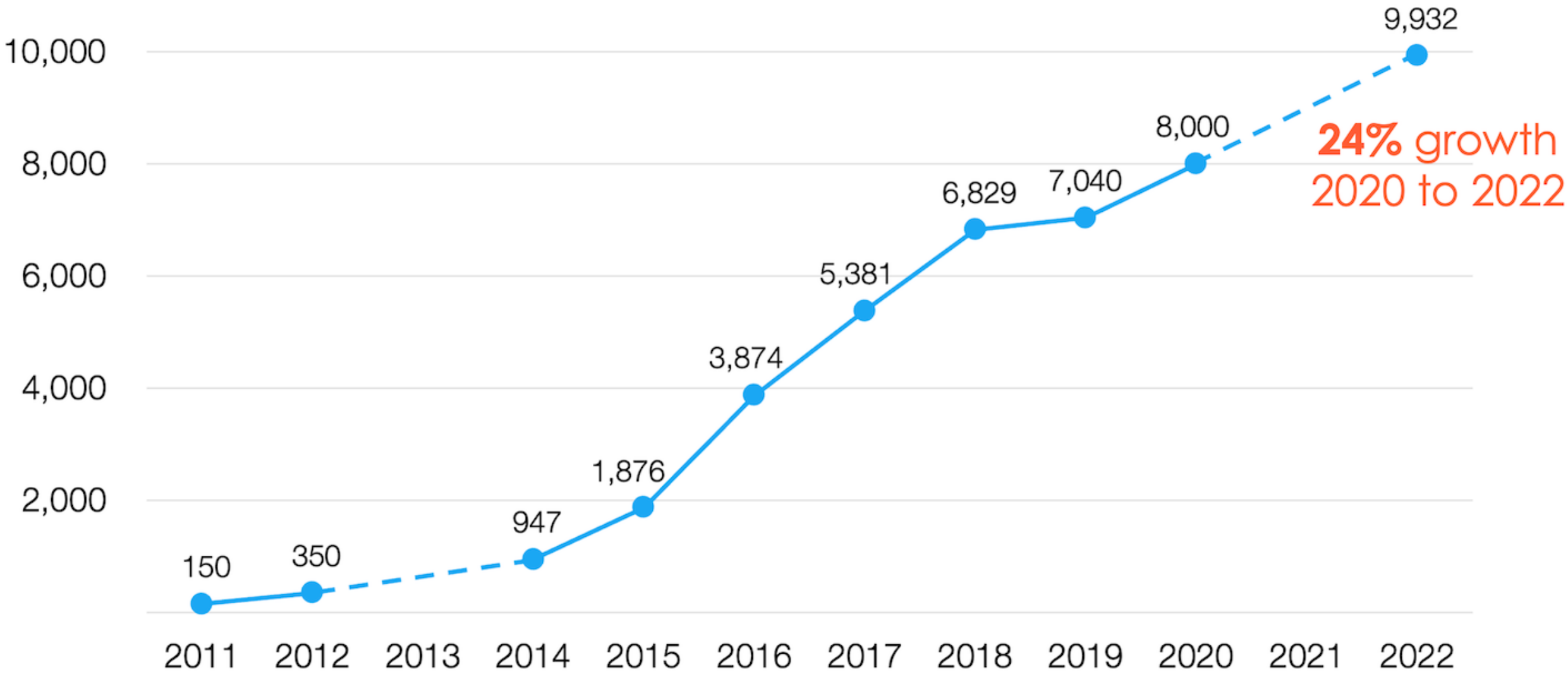
Projects & Workflow

Product Management

Vendor Analysis & Management

visit martechmap.com to search, sort & filter

6,521% growth 2011 to 2022

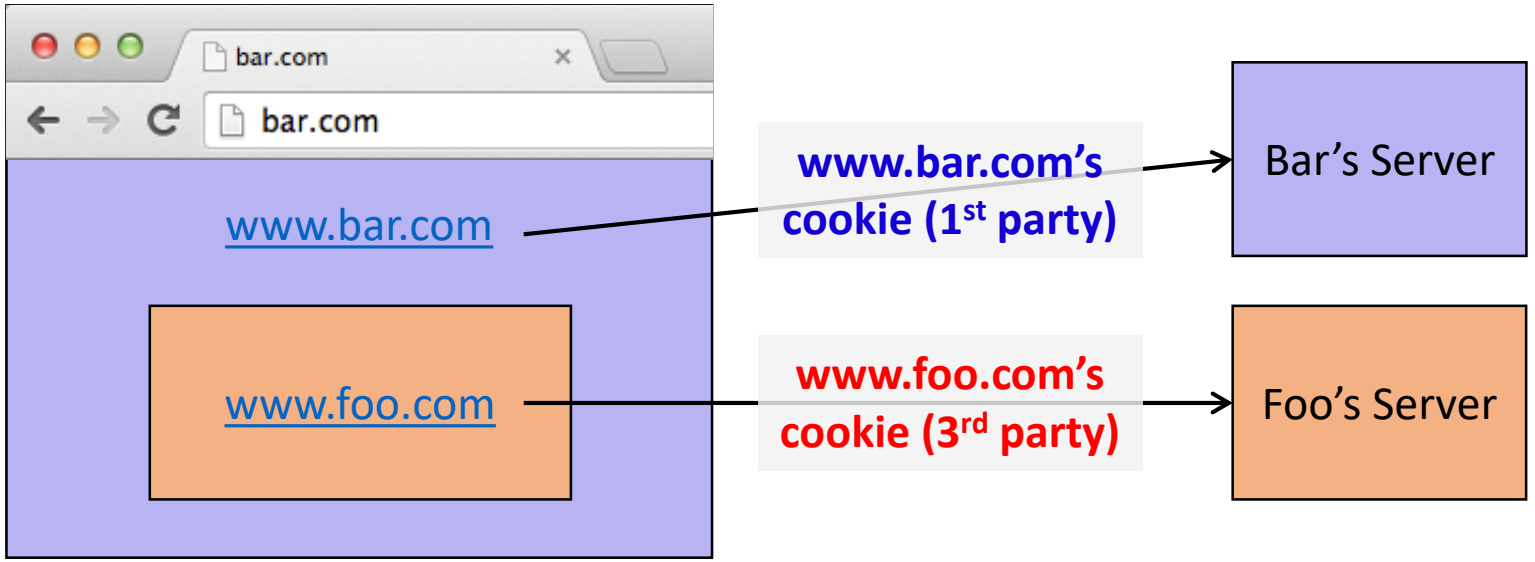


https://chiefmartec.com/2022/05/marketing-technology-landscape-2022-search-9932-solutions-on-martechmap-com/

Concerns About Privacy

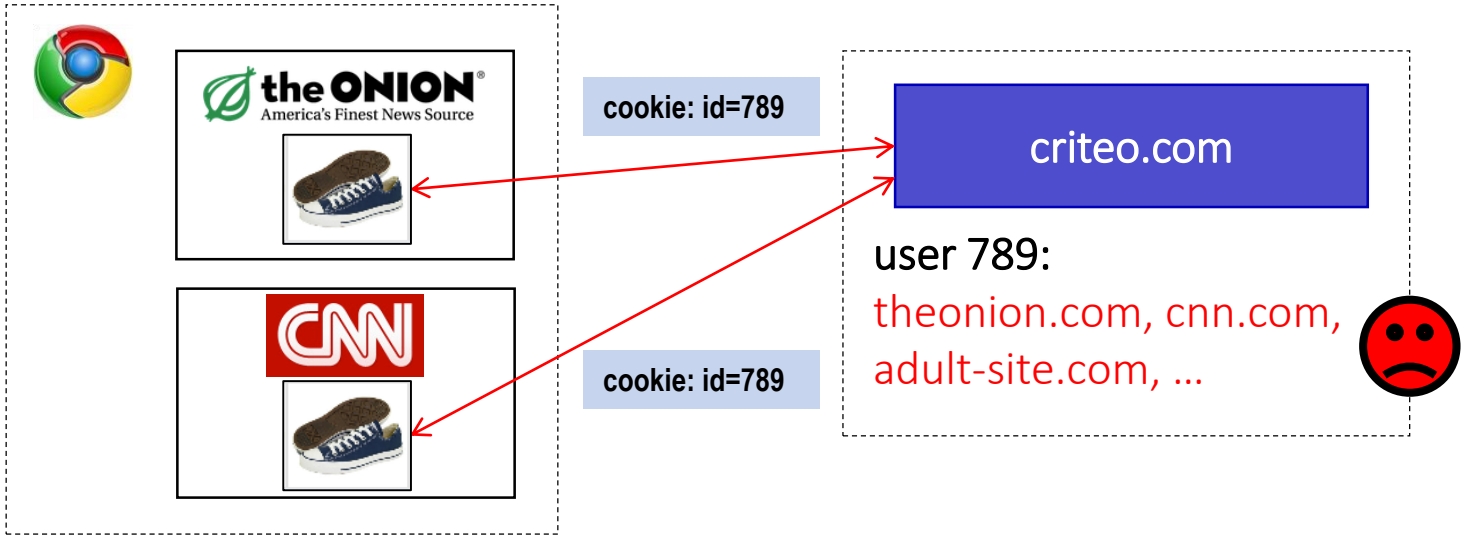
First and Third Parties

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



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.

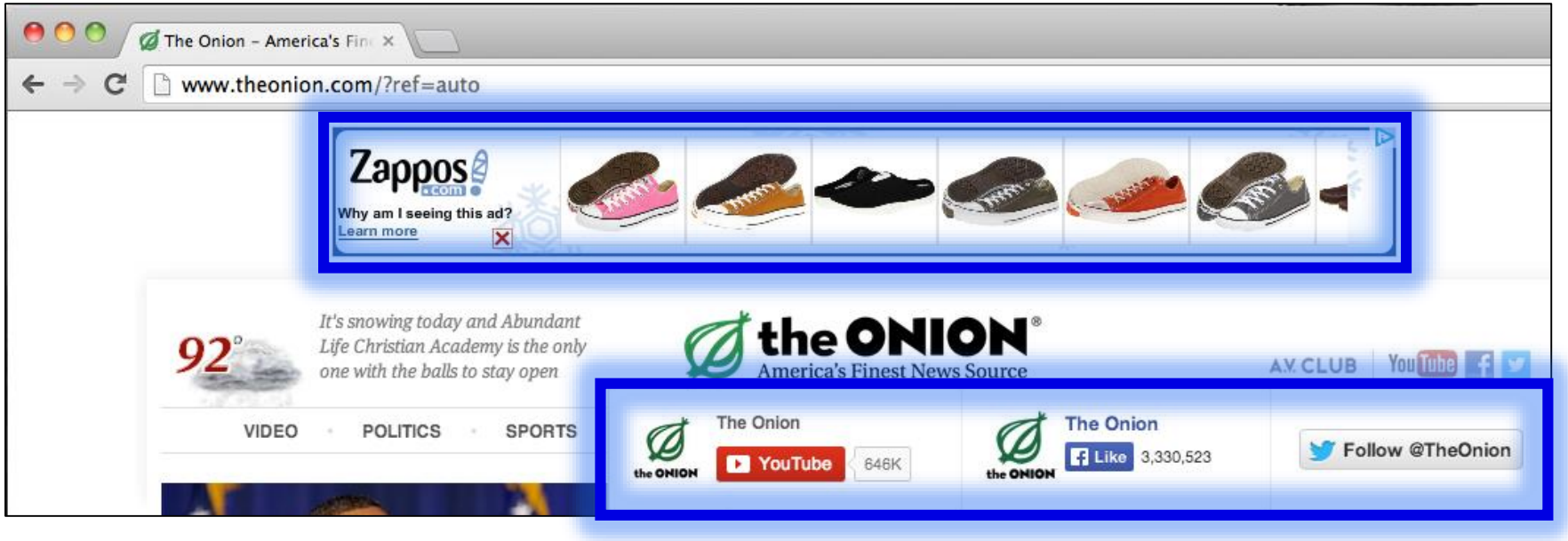
```
▽ Hypertext Transfer Protocol
  ▷ GET /pixel/p-3aud4J6uA4Z6Y.gif?labels=InvisibleBox&busty=2710 HTTP/1.1\r\n
    Host: pixel.quantserve.com\r\n
    Connection: keep-alive\r\n
    Accept: image/webp,*/*;q=0.8\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_2) AppleWebKit/537.36
    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
```

Tracking Technologies

- 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

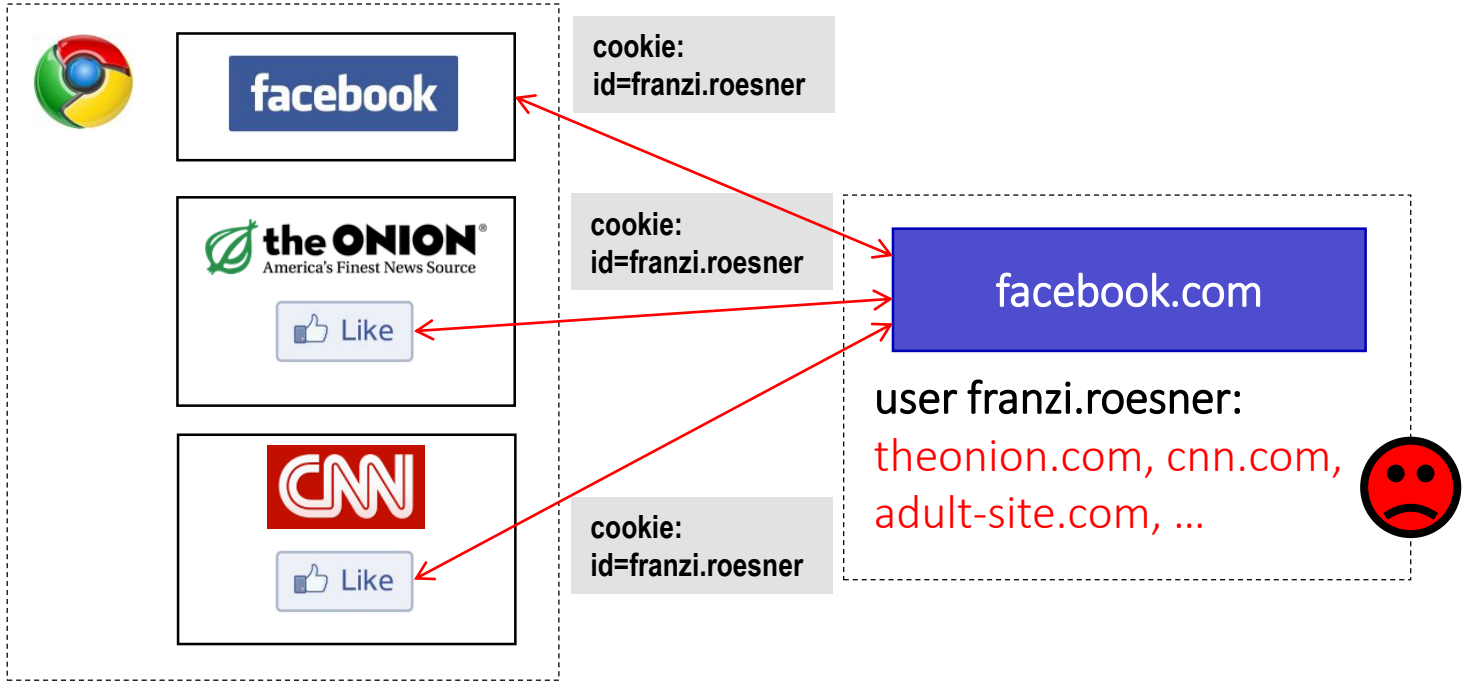
- "Zombie" cookies that respawn (http://samy.pl/evercookie)

Other Trackers?



"Personal" Trackers

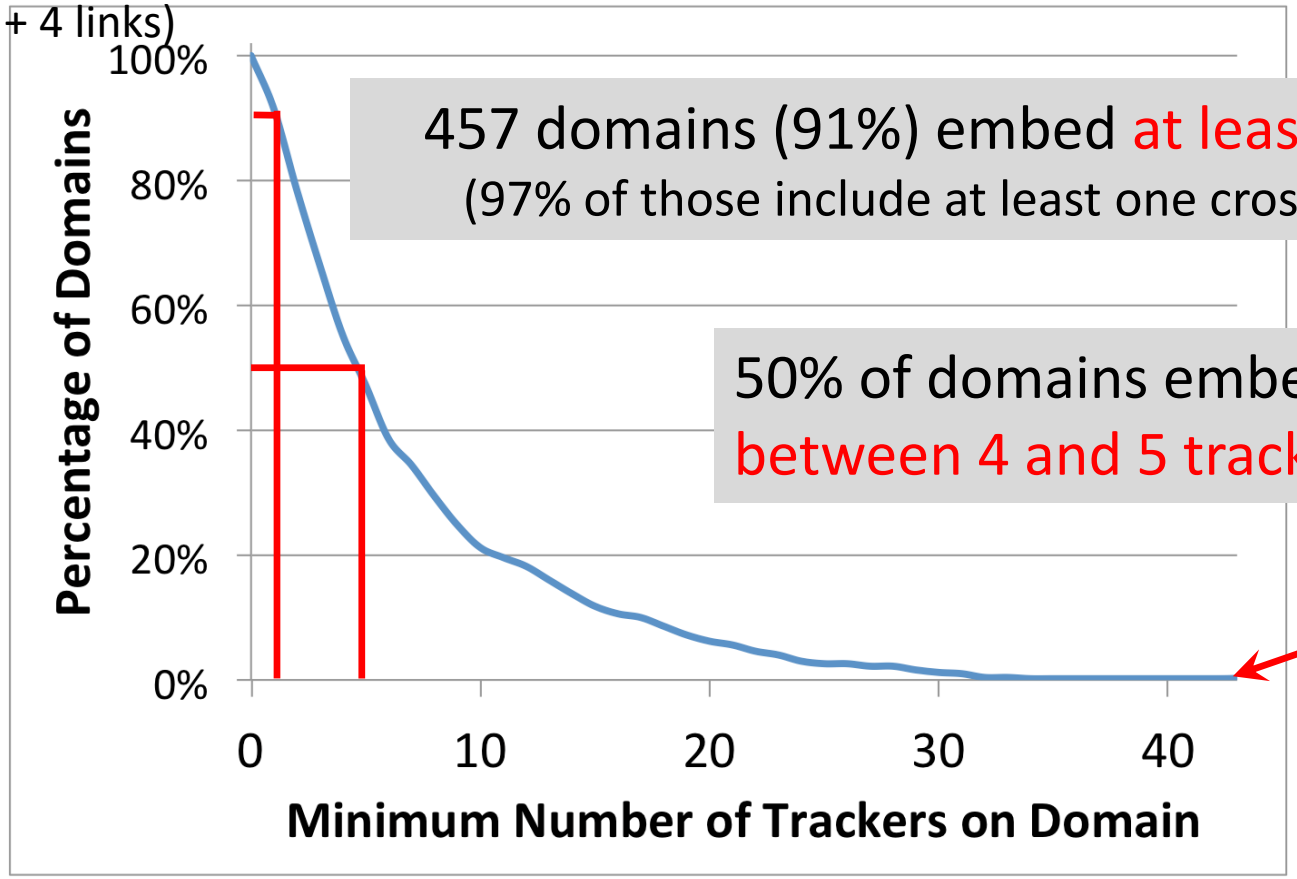
Personal Tracking



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

How prevalent is tracking? (2011)

524 unique trackers on Alexa top 500 websites (homepages + 4 links)

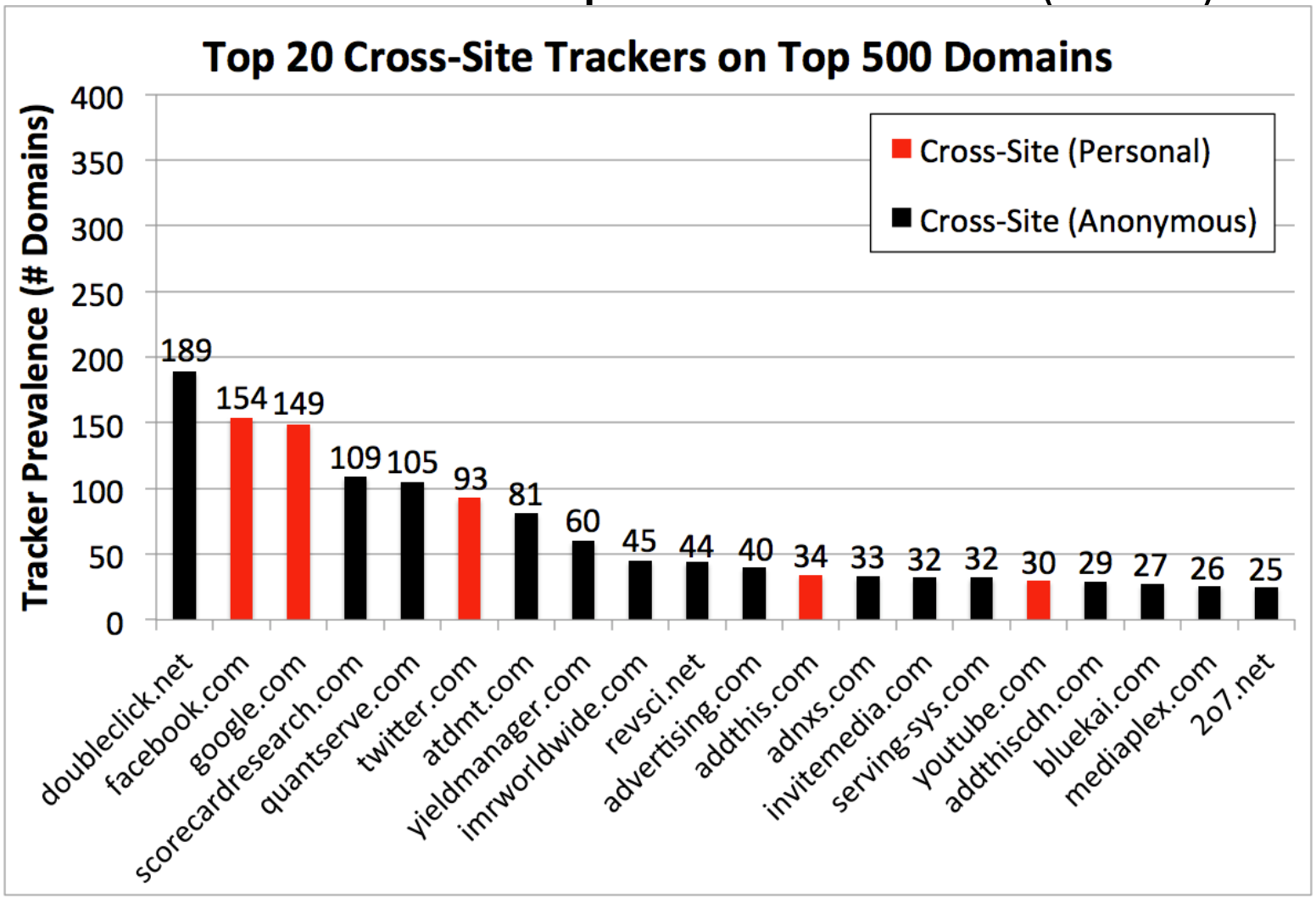


457 domains (91%) embed at least one tracker.
(97% of those include at least one cross-site tracker.)

50% of domains embed between 4 and 5 trackers.

One domain includes 43 trackers.

Who/what are the top trackers? (2011)

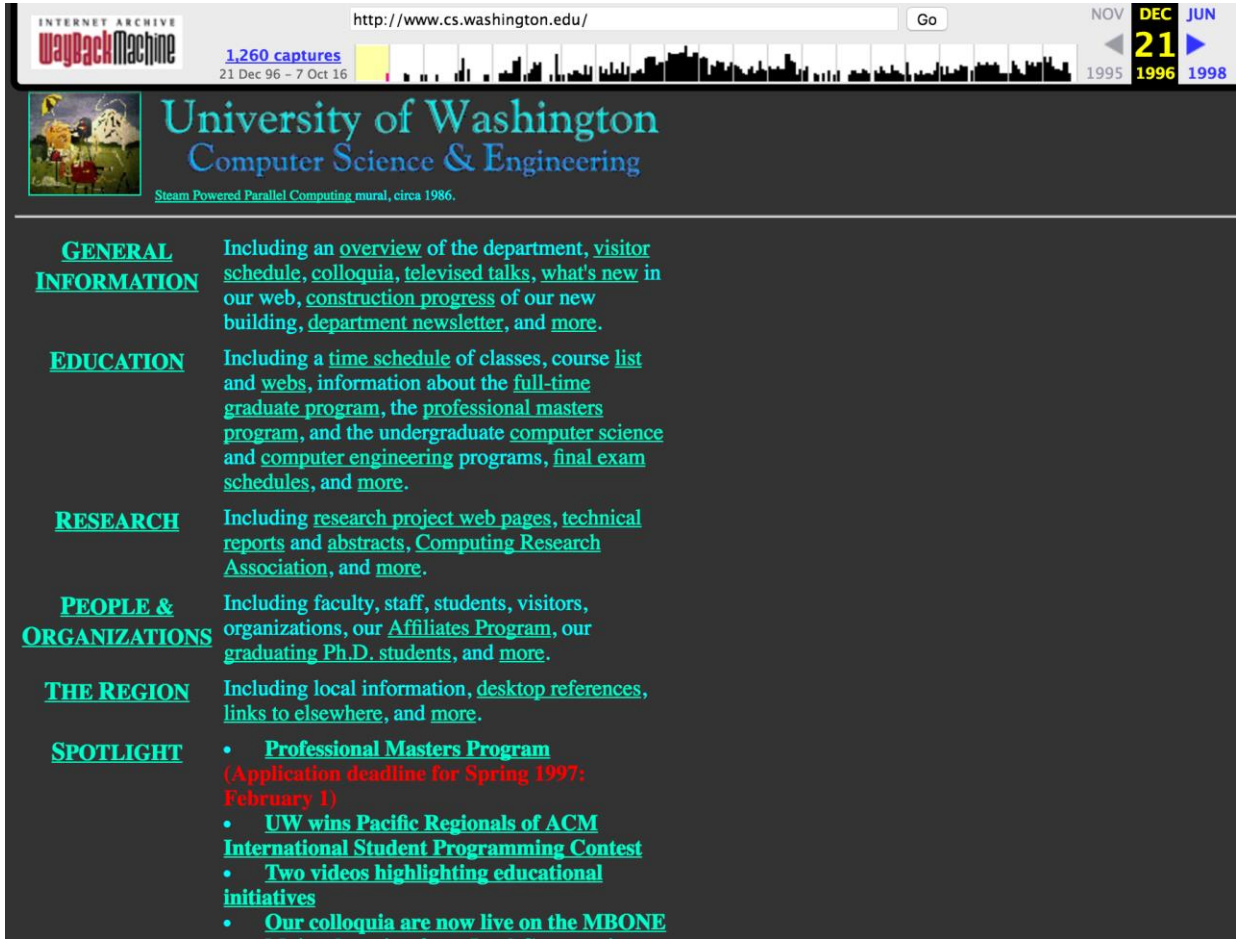


How has this changed over time?

- The web has existed for a while now…
  - What about tracking before 2011?
  - What about tracking before 2009?

- Solution: time travel!

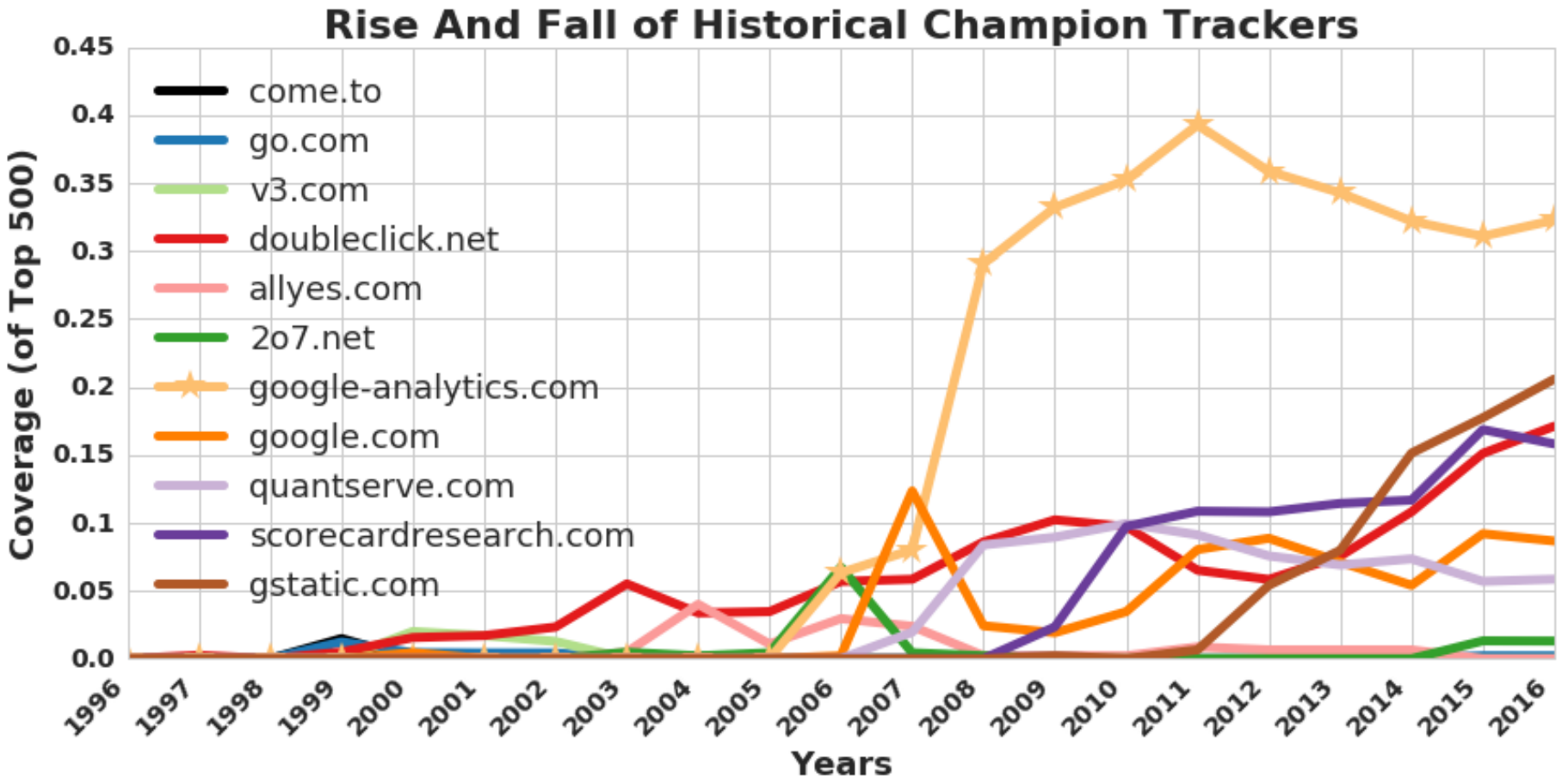
The Wayback Machine to the Rescue



Time travel for web tracking: http://trackingexcavator.cs.washington.edu

1996-2016: More & More Tracking

- More trackers of more types, more per site, more coverage



Defenses to Reduce Tracking

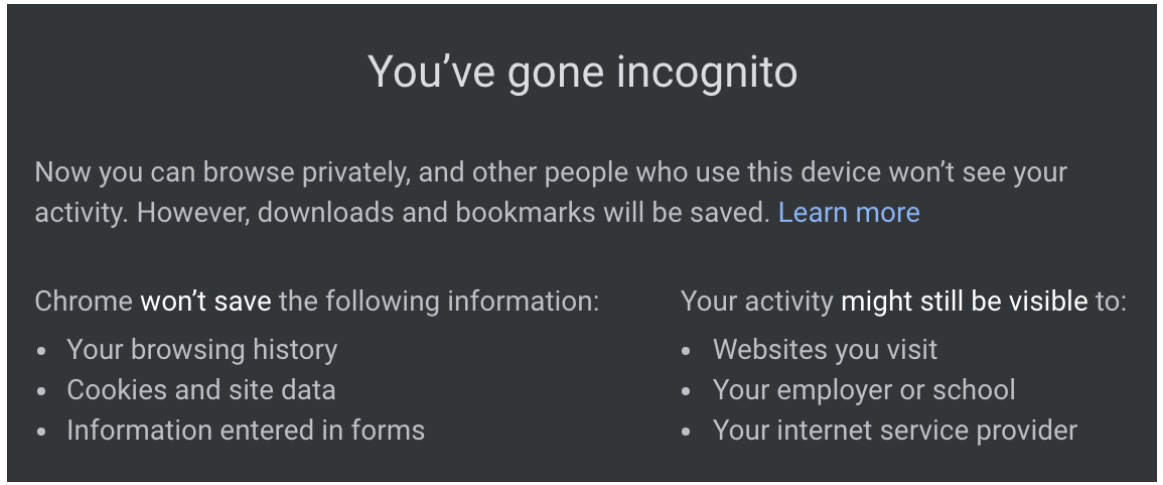
- Do Not Track?

Do Not Track is not a technical defense: trackers must honor the request.

Defenses to Reduce Tracking

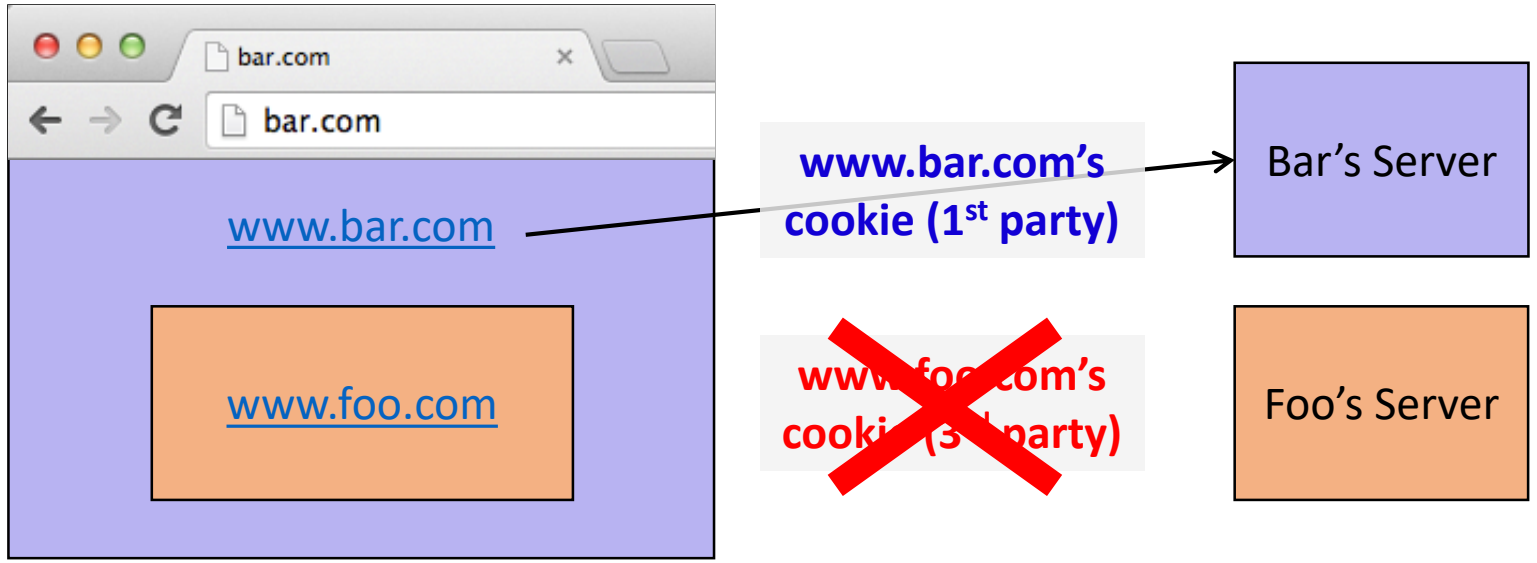
- Do Not Track proposal?
- Private browsing mode?

Private browsing mode doesn't protect against network attackers fully.



Defenses to Reduce Tracking

- Do Not Track proposal?
- Private browsing mode?
- Third-party cookie blocking?



3rd party cookies

- Safari and FF (mostly) now block 3rd party cookies
  - https://webkit.org/blog/10218/full-third-party-cookie-blocking-and-more/
  - https://blog.mozilla.org/blog/2019/09/03/todays-firefox-blocks-third-party-tracking-cookies-and-cryptomining-by-default/

- Chrome…

"By undermining the business model of many ad-supported websites, blunt approaches to cookies encourage the use of opaque techniques such as fingerprinting (an invasive workaround to replace cookies), which can actually reduce user privacy and control. We believe that we as a community can, and must, do better."

Aug 2022: Remove 3rd party cookies by 2024