

10. Privacy on the Web



Blase Ur and David Cash
February 3rd, 2020
CMSC 23200 / 33250



THE UNIVERSITY OF
CHICAGO

Online Tracking

- Advertisers want to show you advertisements targeted to your interests and demographics

Ads Preferences

† Ads on Search and Gmail

† Ads on the web

Opt out

How your ads are personalized

Ads are based on personal info you've added to your Google Account, data from advertisers that partner with Google, and Google's estimation of your interests. Choose any factor to learn more or update your preferences. [Learn more](#)

Accounting & Finance Jobs

Action & Platform Games

Android OS

Banking

Beaches & Islands

Bollywood & South Asian Film

Business & Productivity Software

Action & Adventure Films

Adventure Games

Autos & Vehicles

Bars, Clubs & Nightlife

Blues

Books & Literature

Business News

Ads on the web

Make the ads you see on the web more interesting

Many websites, such as news sites and blogs, partner with us to show ads to their visitors. To see ads that are more related to you and your interests, edit the categories below, which are based on sites you have recently visited. [Learn More](#)

Your interests are associated with an advertising cookie that's stored in your browser. If you don't want us to store your interests, you can opt out below. Your ads preferences only apply in this browser on this computer. They are reset if you delete your browser's cookies.

† Watch a video: [Ads Preferences on GDN explained](#)

Your categories

Below you can review the interests and inferred demographics that Google has associated with your cookie. You can [remove](#) or [edit](#) these at any time.

Arts & Entertainment

Computers & Electronics

Computers & Electronics - Consumer Electronics - Gadgets & Portable Electronics - PDAs & Handhelds

Internet & Telecom

Internet & Telecom - Mobile & Wireless - Mobile Phones - Smart Phones

Law & Government

Science

Your demographics

We infer your age and gender based on the websites you've visited. You can [remove](#) or [edit](#) these at any time.

Age: 35-44

Gender: Male

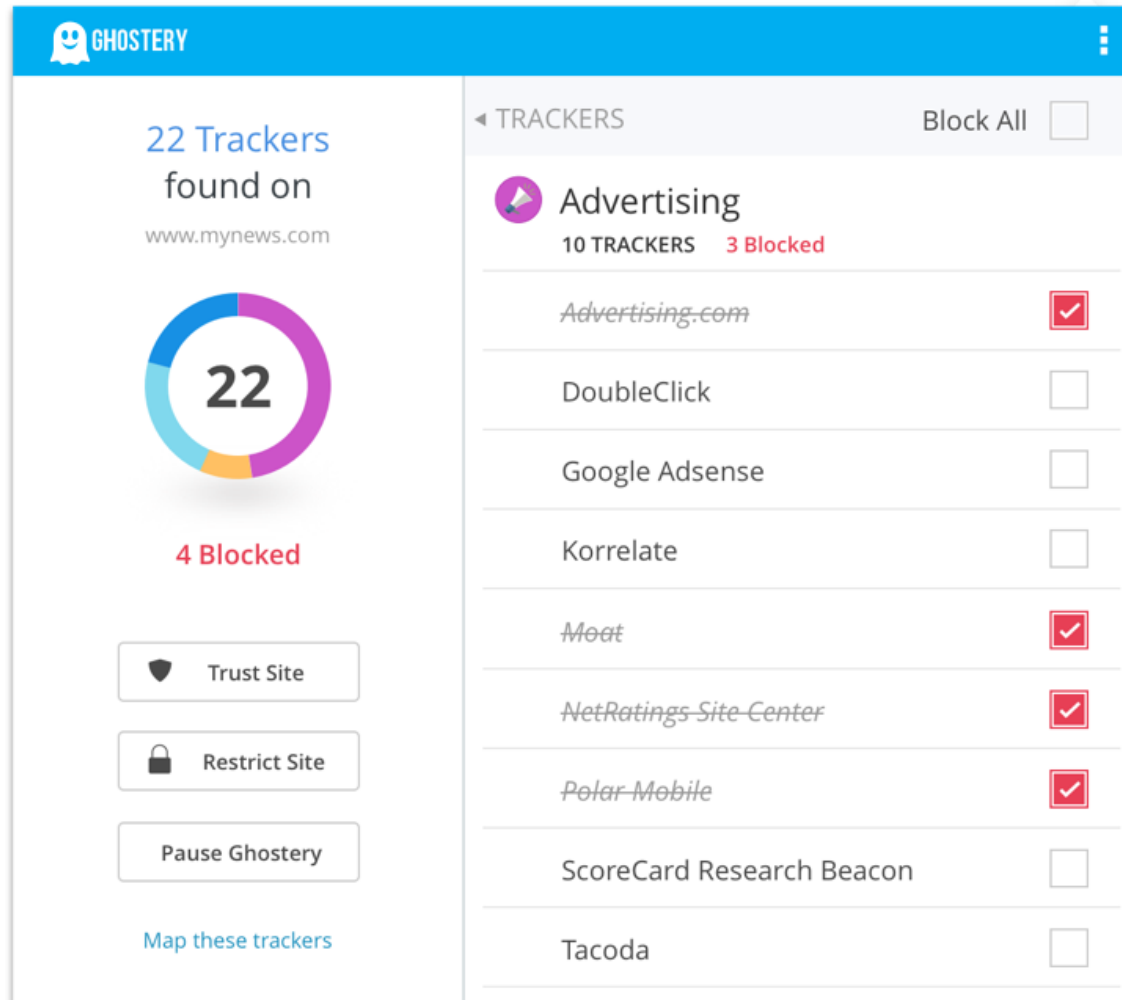
Online Tracking

- First party = the site you are visiting (whose address is in the URL bar)
- Third party = other sites contacted as a result of your visit to that site
- First-party tracking (e.g., for search)
 - Consider DuckDuckGo and alternatives

Online Tracking

- JavaScript / images from advertising networks loaded as part of your page
 - In iframes
 - Or sometimes not
 - Why does this matter?
 - Does this also apply to email? (Yes)

Ubiquity of Online Tracking



The screenshot displays the Ghostery browser extension interface. The top blue header features the Ghostery logo and a menu icon. The main content is split into two panels. The left panel, titled '22 Trackers found on www.mynews.com', includes a donut chart with the number '22' in the center, indicating 4 blocked trackers. Below the chart are three buttons: 'Trust Site' (with a shield icon), 'Restrict Site' (with a lock icon), and 'Pause Ghostery'. A link 'Map these trackers' is at the bottom. The right panel, titled 'TRACKERS', has a 'Block All' checkbox and lists individual trackers under the 'Advertising' category. The list includes 'Advertising.com' (checked), 'DoubleClick', 'Google Adsense', 'Korrelate', 'Moat' (checked), 'NetRatings Site Center' (checked), 'Polar Mobile' (checked), 'ScoreCard Research Beacon', and 'Tacoda'.

Tracker	Status
Advertising	10 TRACKERS 3 Blocked
Advertising.com	Blocked (checked)
DoubleClick	Not Blocked
Google Adsense	Not Blocked
Korrelate	Not Blocked
Moat	Blocked (checked)
NetRatings Site Center	Blocked (checked)
Polar Mobile	Blocked (checked)
ScoreCard Research Beacon	Not Blocked
Tacoda	Not Blocked

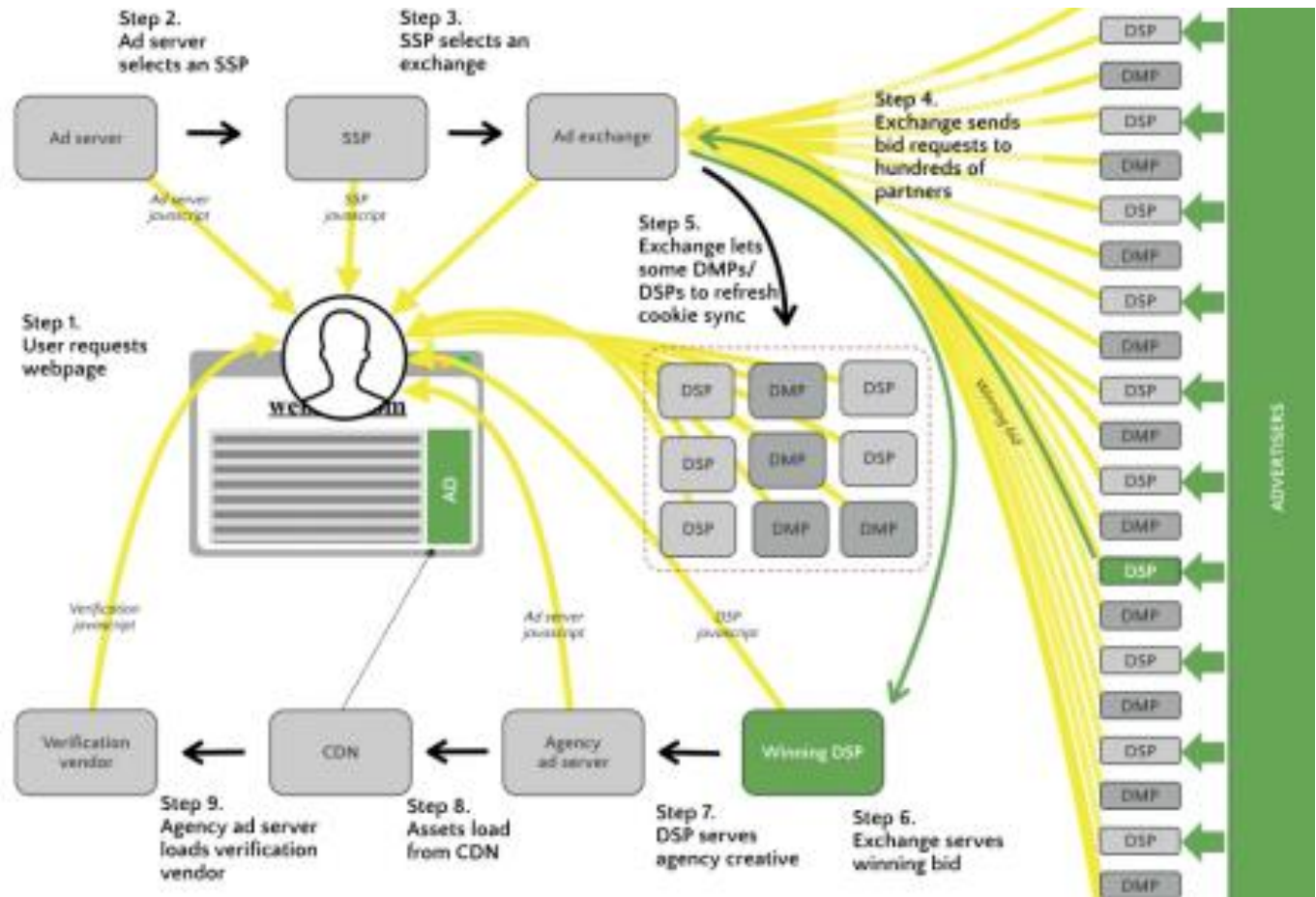
Ad Bidding Marketplaces

DATA LEAKAGE IN ONLINE ADVERTISING

This is the current process of real-time bidding that is used in online behavioural advertising.

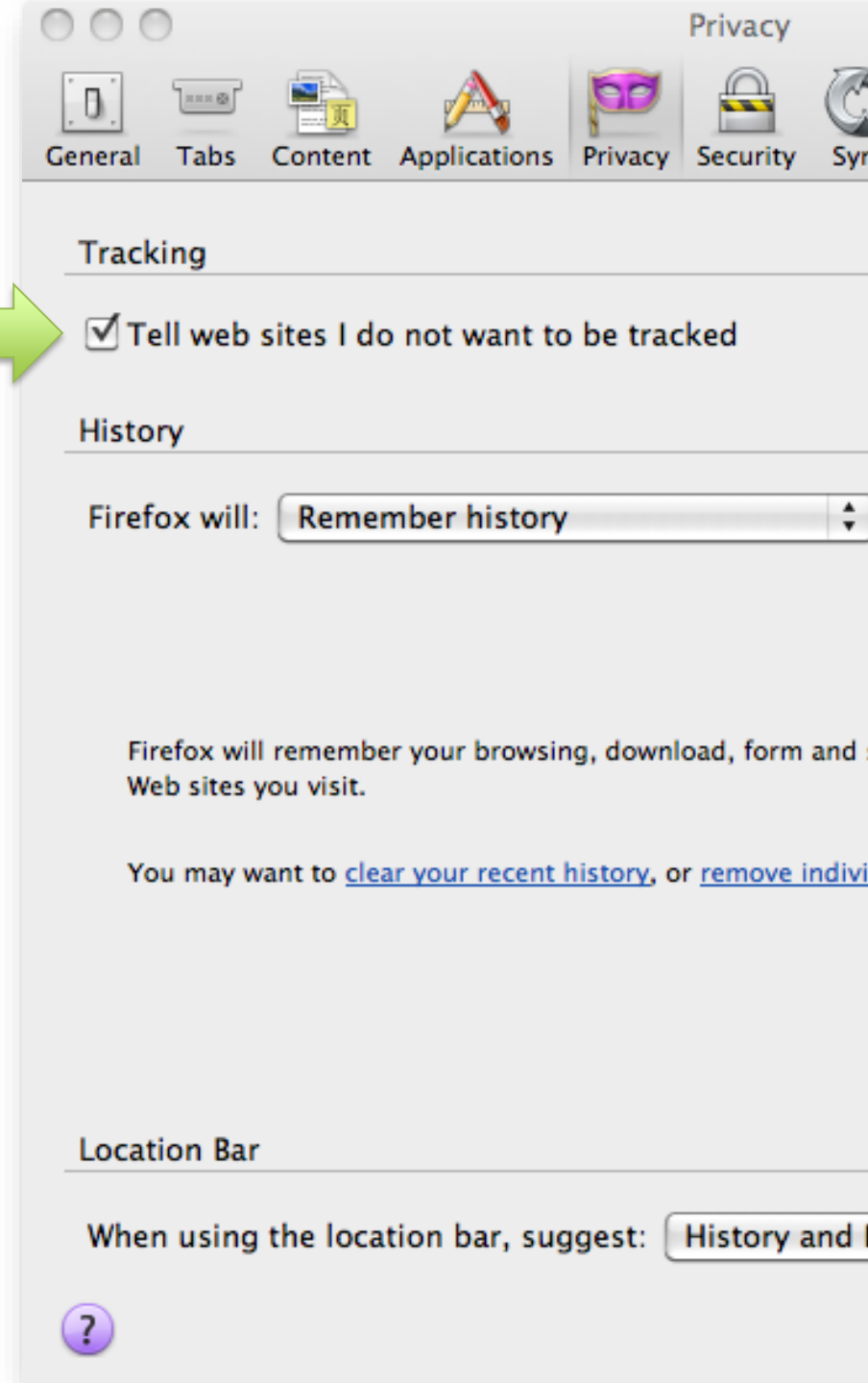
Legend

- Channel of data leakage
- Money
- Personally identifiable information



Do not track

- Proposed W3C standard
- User checks a box
- Browser sends “do not track” header to website
- Website stops “tracking”
- W3C working group trying to define what that means



Tools to stop tracking, effective?

- Browser privacy settings
 - Cookie blocking
 - P3P
 - Tracking Protection Lists
 - Do Not Track
- Browser add-ons
- Opt-out cookies
- Digital Advertising Alliance (DAA) AdChoices icon and associated opt-out pages



DoNotTrackMe



Existing Privacy Tools

The Disconnect browser extension interface is shown. It features a top bar with the 'DISCONNECT' logo, 'Help', and 'Share' links. Below this is a social media section with icons for Facebook (0), Google+ (1), and Twitter (1). The main content area is divided into categories: Advertising (2 requests), Analytics (7 requests), Social (0 requests), and Content (0 requests). Each category has a list of blocked trackers with checkboxes. At the bottom, there are options to 'Whitelist site', 'Visualize page', 'Show counter', and 'Cap counter'. A bar chart shows 'Time saved' and 'Bandwidth saved'. A green button at the bottom says 'Get Mobile Protection'.

DISCONNECT Help Share

f 0 g 1 t 1

Advertising
2 requests

- ☒ Adobe 1 request
- ☒ Nielsen 1 request

Analytics
7 requests

Social
0 requests

Content
0 requests

Whitelist site Visualize page

☒ Show counter ☒ Cap counter

Time saved Bandwidth saved

Get Mobile Protection

The Blur browser extension interface is shown on the ESPN website. It features a blue header with the 'espn.com' logo and '8 trackers blocked'. Below this, a toggle switch indicates 'Tracker blocking is on for this website'. A list of blocked trackers is shown: Google AdSense, Demdex, Twitter Badge, and Omniture, each with a 'blocked' status and a green checkmark. A red eye icon is next to a link that says 'see your tracker blocking stats and learn more about these companies'. A blue bar at the bottom shows '21 trackers blocked since Feb '17'. Below this, a link says 'Correct how Blur works in the form below'. The bottom of the interface has the 'oBLUR' logo and links for 'Settings', 'Help', and 'Go Premium'.

Final Final

espn.com X
8 trackers blocked

Tracker blocking is **on** for this website

Google AdSense blocked

Demdex blocked

Twitter Badge blocked

Omniture blocked




[see your tracker blocking stats and learn more about these companies](#)

21 trackers blocked since Feb '17




[Correct how Blur works in the form below](#)

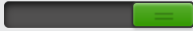


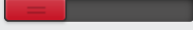
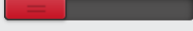

oBLUR [Settings](#) [Help](#) [Go Premium](#)

Existing Privacy Tools

 **Privacy Badger**  

Privacy Badger detected 45 potential **trackers** on this page. These sliders let you control how Privacy Badger handles each one. You shouldn't need to adjust them unless something is broken.



  

weather.api.cnn.io	
rtax.criteo.com	
ad.doubleclick.net	
googleads.g.doubleclick.net	
securepubads.g.doubleclick.net	
connect.facebook.net	


Disable Privacy Badger for This Site

Did Privacy Badger break this site? Let us know!


Donate to EFF


 **GHOSTERY** 

15 Trackers found on www.cnn.com




14 Blocked


 Trust Site











 Restrict Site


Pause Ghostery

[Map These Trackers](#)

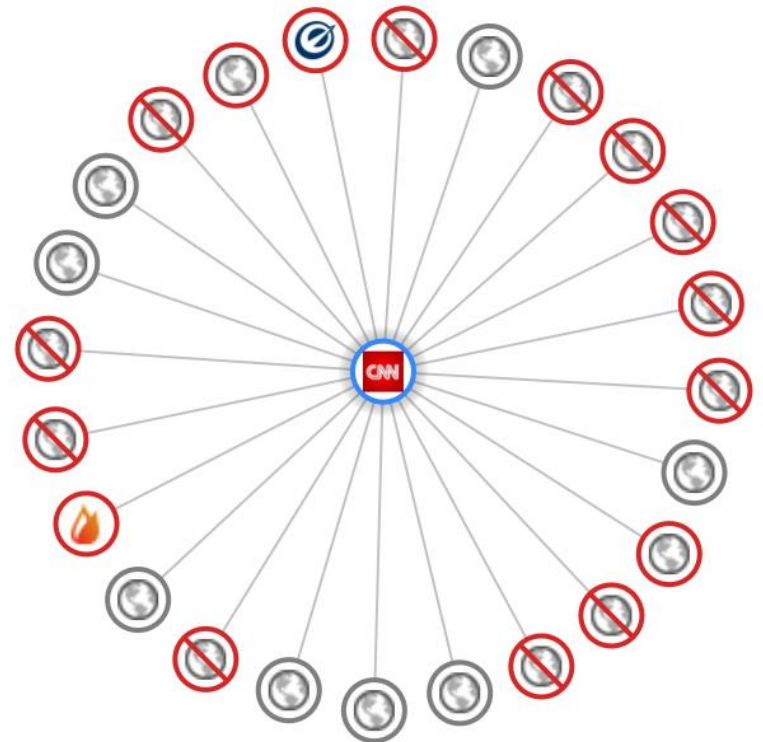
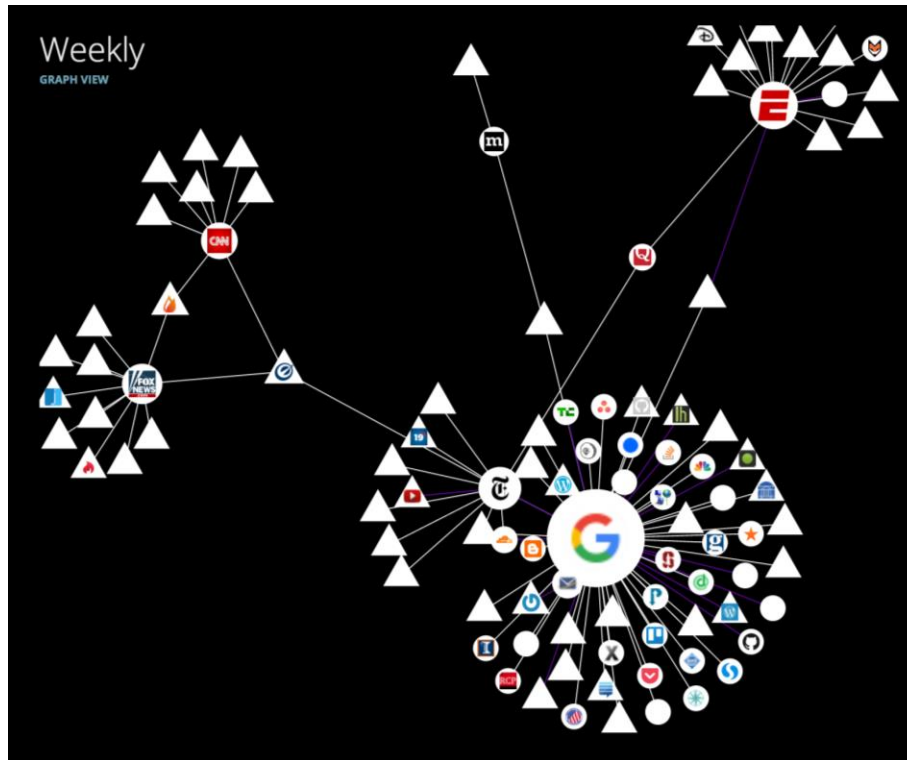
Trackers Block All 

 **Advertising**
10 Trackers 10 Blocked

<i>Amazon Associates</i>	
<i>ChartBeat</i>	
<i>Criteo</i>	
<i>DoubleClick</i>	
<i>Google Publisher Tags</i>	
<i>Krux Digital</i>	
<i>NetRatings SiteCensus</i>	
<i>Outbrain</i>	
<i>Rubicon</i>	
<i>ShareThrough</i>	

 **Site Analytics**
2 Trackers 2 Blocked

Connection Graphs

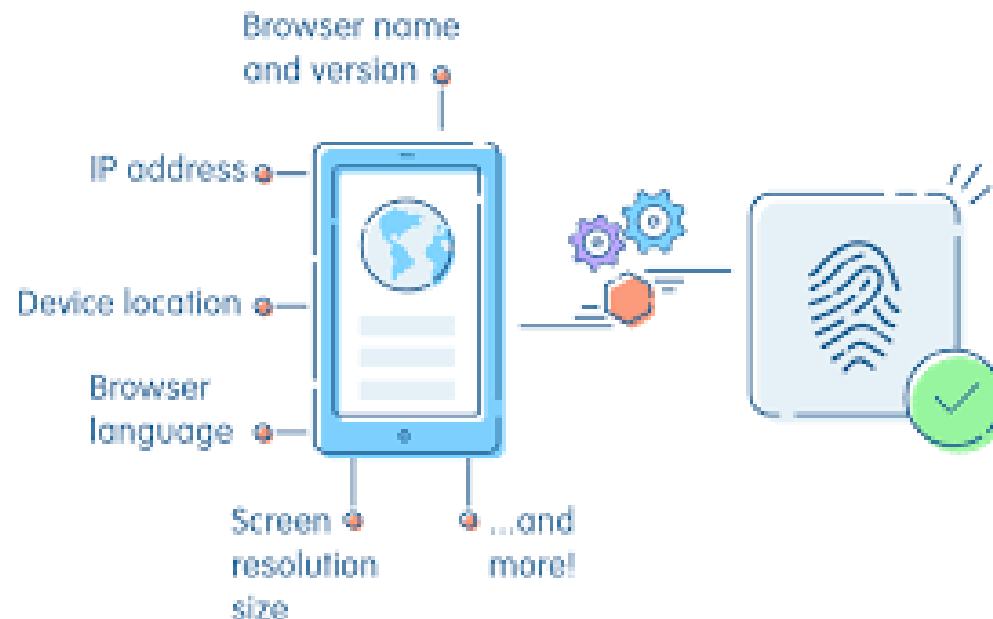


Browser fingerprinting

- Use features of the browser that are relatively unique to your machine
 - Fonts
 - GPU model anti-aliasing (Canvas fingerprinting)
 - User-agent string
 - *(Often not) IP address (Why not?)*

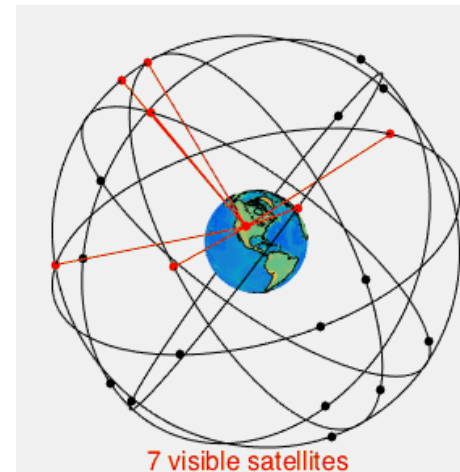
Device Fingerprinting

- Use unique(-ish) combination of device features as an identifier
- <https://panopticklick.eff.org/>



Location Tracking

- IP Geolocation
 - Hierarchy of IP addresses
- GPS (Global Positioning System)
 - ~31 satellites in semi-synchronous orbit in OUTER SPACE with atomic clocks
 - Always ~6 satellites in line of sight
 - Multilateration

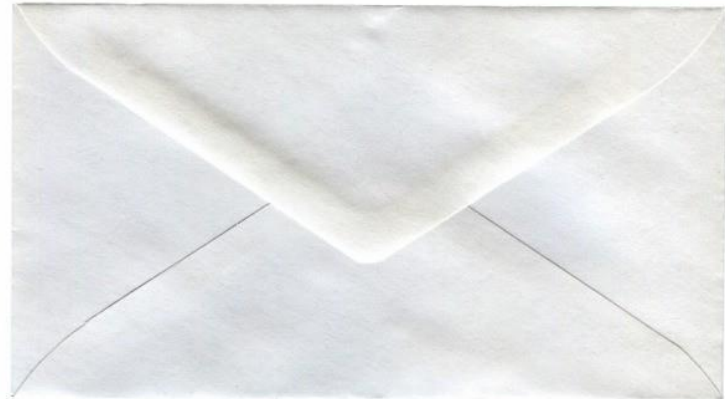


What Does HTTPS Hide? (GCSSP)

- Body of the HTTP request / response is hidden
- ...So what's left to be seen / inferred?

Side Channels

- Using metadata or outside observations to make inferences about the data



Web Side Channels Include:

- Size of packets
 - How can this reveal what pages you are visiting?
- Timing

Remote Timing Attacks are Practical

David Brumley
Stanford University
dbrumley@cs.stanford.edu

Dan Boneh
Stanford University
dabo@cs.stanford.edu

Abstract

Timing attacks are usually used to attack weak computing devices such as smartcards. We show that timing attacks apply to general software systems. Specifically, we devise a timing attack against OpenSSL. Our experiments show that we can extract private keys from an OpenSSL-based web server running on a machine in the local network. Our results demonstrate that timing attacks against network servers are practical and therefore security engineers should defend against them.

The attacking machine and the server were in different buildings with three routers and multiple switches between them. With this setup we were able to extract the SSL private key from common SSL applications such as a web server (Apache+mod_SSL) and a SSL-tunnel.

Interprocess. We successfully mounted the attack between two processes running on the same machine. A hosting center that hosts two domains on the same machine might give management access to the admins of each domain. Since both domains are hosted on the same machine, one admin could use

Web Side Channels Include:

- Color

- [link one](#)
- [second link](#)
- [link three \(visited\)](#)
- [fourth link](#)