Online Tracking

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

<table>
<thead>
<tr>
<th>Trackers Found on</th>
<th>22 Trackers found on <a href="http://www.mynews.com">www.mynews.com</a></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>22 Trackers</strong></td>
<td></td>
</tr>
<tr>
<td><strong>4 Blocked</strong></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Trackers</th>
<th>Block All</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Advertising</strong></td>
<td>10 TRACKERS 3 Blocked</td>
</tr>
<tr>
<td>Advertising.com</td>
<td>✓</td>
</tr>
<tr>
<td>DoubleClick</td>
<td></td>
</tr>
<tr>
<td>Google Adsense</td>
<td></td>
</tr>
<tr>
<td>Korrelate</td>
<td></td>
</tr>
<tr>
<td>Met</td>
<td>✓</td>
</tr>
<tr>
<td>NetRatings-Site-Center</td>
<td>✓</td>
</tr>
<tr>
<td>Polar-Mobile</td>
<td>✓</td>
</tr>
<tr>
<td>ScoreCard Research Beacon</td>
<td></td>
</tr>
<tr>
<td>Tacoda</td>
<td></td>
</tr>
</tbody>
</table>

Map these trackers

Trust Site
Restrict Site
Pause Ghostery
Ad Bidding Marketplaces
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
Existing Privacy Tools

- Disconnect
- ESPN Blocking tracker

- Tracker blocking:
  - Google Adsense: blocked
  - Demdex: blocked
  - Twitter Badge: blocked
  - Omniture: blocked

- Statistics:
  - 8 trackers blocked
  - 21 trackers blocked since Feb '17

- Additional features:
  - See tracker blocking stats and learn more about these companies

- Correct how Blur works in the form below

- BLUR
  - Settings
  - Help
  - Go Premium
Existing Privacy Tools

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
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://panopticlick.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 it is critical to look before attacking.

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 domain are hosted on the same machine, the attacker can conduct a timing attack.
Web Side Channels Include:

• Color

• link one
• second link
• link three (visited)
• fourth link