Mitigating Browser Fingerprint Tracking: Multi-level Reconfiguration and Diversification

Pierre Laperdrix, Walter Rudametkin, Benoit Baudry
Seams – May, 19th 2015
# Table of contents

1. What is fingerprint-based tracking?
2. Presentation of Blink
3. Experimental validation
4. Conclusion and perspectives
Tracking users

Cookies

- Installation of a file on the user’s computer
- Possibility for the user to delete first and third-party cookies
- Browser extensions can manage and block cookies
Tracking users

Device fingerprinting

- Side-effect of software diversity
- Collection of information on the device
  - Browser
  - Operating system
  - Hardware
## Example of a fingerprint

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User agent</td>
<td>Mozilla/5.0 (X11; Linux i686; rv:25.0) Gecko/20100101 Firefox/25.0</td>
</tr>
<tr>
<td>HTTP accept</td>
<td>text/html, application/xhtml+xml, application/xml;q=0.9,/*;q=0.8 gzip, deflate en-US,en;q=0.5</td>
</tr>
<tr>
<td>Plugins</td>
<td>Plugin 0: QuickTime Plug-in 7.6.6; libtotem-narrowospace-plugin.so; Plugin 1: Shockwave Flash; Shockwave Flash 11.2 r202; libflashplayer.so;</td>
</tr>
<tr>
<td>Fonts</td>
<td>Century Schoolbook, Source Sans Pro Light, DejaVu Sans Mono, Bitstream Vera Serif, URW Palladio L, Bitstream Vera Sans Mono, Bitstream Vera Sans, ...</td>
</tr>
<tr>
<td>HTTP DoNotTrack</td>
<td>1</td>
</tr>
<tr>
<td>Cookies enabled</td>
<td>Yes</td>
</tr>
<tr>
<td>Platform</td>
<td>Linux i686</td>
</tr>
<tr>
<td>OS</td>
<td>Linux 3.14.3-200.fc20.x86 32-bit</td>
</tr>
<tr>
<td>Screen resolution</td>
<td>1920x1080x24</td>
</tr>
<tr>
<td>Timezone</td>
<td>-480</td>
</tr>
<tr>
<td>DOM Session storage</td>
<td>Yes</td>
</tr>
<tr>
<td>DOM Local storage</td>
<td>Yes</td>
</tr>
<tr>
<td>I.E. User data</td>
<td>No</td>
</tr>
</tbody>
</table>
How unique and trackable are we?

- 83.6% of unique fingerprints
- 86.4% of unique fingerprints

Panopticlick
How Unique — and Trackable — Is Your Browser?

Am I Unique?
How widespread is fingerprinting?

Google

- **Device information**

  We may collect device-specific information (such as your hardware model, operating system version, unique device identifiers, and mobile network information including phone number). Google may associate your device identifiers or phone number with your Google Account.

Yahoo

Yahoo automatically receives and records information from your computer and browser, including your IP address, Yahoo cookie information, software and hardware attributes, and the page you request.

Amazon

- **Automatic Information**

  Examples of the information we collect and analyze include the Internet protocol (IP) address used to connect your computer to the Internet; login; e-mail address; password; computer and connection information such as browser type, version, and time zone setting, browser plug-in types and versions, operating system, and platform; purchase history, which we sometimes aggregate with similar information.

Twitter

- **Log Data**: Our servers automatically record information ("Log Data") created by your use of the Services. Log Data may include information such as your IP address, browser type, operating system, the referring web page, pages visited, location, your mobile carrier, device and application IDs, search terms, and cookie information. We receive Log Data when you interact with our Services, for example, when you visit our websites,
Device fingerprinting

- Silent
- Complement usage of cookies
- Hard to detect and block fingerprinting scripts
- Already adopted by major web actors
- Track users without their knowledge
- Real privacy problem
Table of contents

1) What is fingerprint-based tracking?
2) Presentation of Blink
3) Experimental validation
4) Conclusion and perspectives
Properties of a fingerprint

- Uniqueness: we can precisely identify a device thanks to its unique combination of features

- Stability: a fingerprint does not drastically change over time

- These two properties combined are the source of a real privacy problem.
Blink

• Increase temporal diversity of fingerprints.
• Reconfigure platform at runtime.
• No lies.
• Browsing without Blink

• Browsing with Blink
Browsing platform

Diversifiable elements
Blink’s generation process
# Table of contents

1) What is fingerprint-based tracking?

2) Presentation of Blink

3) Experimental validation

4) Conclusion and perspectives
Objectives

1. Does dynamic reconfiguration break fingerprint stability?

2. What is the impact of the user’s plugins and fonts on global diversity?

Requirements

• A fingerprinting script
• A metric to quantify the difference between two synthesized platforms
Experimental protocol

Initial situation n°1
User browsing platform
1 plugin
20 fonts

Initial situation n°25
User browsing platform
25 plugins
500 fonts

100 synthesized b.p.
1 5
2 6
3 7
4 8

100 synthesized b.p.
1 5
2 6
3 7
4 8

2500 synthesized browsing platforms
Research questions

1. How different from the original user’s fingerprint are the fingerprints exhibited by the synthesized platform?
Research questions

2. How diverse is the set of fingerprints exhibited by the synthesized platforms?
Table of contents

1) What is fingerprint-based tracking?
2) Presentation of Blink
3) Experimental validation
4) Conclusion and perspectives
Conclusion and perspectives

- Blink: break fingerprint stability thanks to automatic and complete synthesis of a new browsing platform for each browsing session.
- AmIUnique.org: Collection of fingerprints to refine Blink’s randomization algorithms. [https://amiunique.org](https://amiunique.org)
- Blink on Docker: Fast and lightweight prototype already available. [https://github.com/plaperdr/blink-docker](https://github.com/plaperdr/blink-docker)
Thank you for listening!

Any questions?
# Summary of current solutions

<table>
<thead>
<tr>
<th>Solution</th>
<th>Focus</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blocking extension</td>
<td>Blocking</td>
<td>Does not block everything</td>
</tr>
<tr>
<td>Spoofing extension</td>
<td>Lying</td>
<td>Creates detectable inconsistencies</td>
</tr>
<tr>
<td>Multiple browsers</td>
<td>Increasing diversity</td>
<td>Decreases usability and is inefficient</td>
</tr>
<tr>
<td>Tor browser</td>
<td>Removing diversity</td>
<td>Decreases usability</td>
</tr>
<tr>
<td>Blink</td>
<td>Increasing diversity and changing fingerprint for each browsing session</td>
<td>No inconsistencies, no decrease in usability, no brittleness</td>
</tr>
</tbody>
</table>
Blink’s Coffee break mode

Host machine
- OS
- Browser
- Plugins
  - UP1
  - UP2
- Fonts
  - UF1
  - UF2
- User Profile

Diversity reservoir
- Browsers
  - B1
  - B2
  - B3
  - B4
- Plugins
  - P1
  - P2
  - P3
  - P4
- Fonts
  - F1
  - F2
  - F3
  - F4
- VMs
  - VM1
  - VM2
  - VM3

Browsing platform

24/22
Comparison with cookies

**COOKIES**

- Server request
- Transfer of a cookie
- Cookie

**FINGERPRINTING**

- Use of a script
- Transfer of the fingerprintable data