Browser Fingerprinting: Exploring Device Diversity to Augment Authentication and Build Client-Side Countermeasures

Pierre Laperdrix
Congrès SIF
Insa Rennes et IRISA
7 février 2019
Outline

I. What is browser fingerprinting?

II. Defending against fingerprinting: Blink and FPRandom

III. Conclusion
1. Internet and web browsers
I. Internet in 1995

HTTP User agent

NCSA_Mosaic/2.0 (Windows 3.1)

Mozilla/1.22 (compatible; MSIE 2.0; Windows 95)

Browsers send device-specific information to servers to improve user experience on the web.
What happens when we start collecting all the information available in a web browser?
I. Definition of browser fingerprinting

Definitions

• A **browser fingerprint** is a set of information related to a user’s device from the hardware to the operating system to the browser and its configuration.

• Browser **fingerprinting** refers to the process of collecting information through a web browser to build a fingerprint of a device.
https://amiunique.org (Am I Unique)

- Website launched in November 2014
- Collected 980,000+ fingerprints so far
- Browser extension available to see the evolution of your own browser fingerprint
I. Example of a browser fingerprint

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User agent</td>
<td>Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:55.0) Gecko/20100101 Firefox/55.0</td>
</tr>
<tr>
<td>HTTP headers</td>
<td>text/html, application/xhtml+xml, application/xml;q=0.9, <em>/</em>;q=0.8 gzip, deflate, br en-US, en;q=0.5</td>
</tr>
<tr>
<td>Plugins</td>
<td>Plugin 0: QuickTime Plug-in 7.6.6; libtotem-narrowspace-plugin.so; Plugin 1: Shockwave Flash; Shockwave Flash 26.0 r0; 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>Platform</td>
<td>Linux x86_64</td>
</tr>
<tr>
<td>Screen resolution</td>
<td>1920x1080x24</td>
</tr>
<tr>
<td>Timezone</td>
<td>-480 (UTC+8)</td>
</tr>
<tr>
<td>OS</td>
<td>Linux 3.14.3-200.fc20.x86 32-bit</td>
</tr>
<tr>
<td>WebGL vendor</td>
<td>NVIDIA Corporation</td>
</tr>
<tr>
<td>WebGL renderer</td>
<td>GeForce GTX 650 Ti/PCIe/SSE2</td>
</tr>
<tr>
<td>Canvas</td>
<td>Cwm fjordbank glyphs vext quiz, 😐</td>
</tr>
<tr>
<td></td>
<td>Cwm fjordbank glyphs vext quiz, 😊</td>
</tr>
</tbody>
</table>
I. Example of values collected on AmIUnique

Some user-agents

- Mozilla/5.0 (Windows NT 6.1; WOW64; rv:34.0) Gecko/20100101 Firefox/34.0
- Mozilla/5.0 (iPhone; CPU iPhone OS 8_1_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12B440 Safari/600.1.4
- Mozilla/5.0 (Android; Mobile; rv:27.0) Gecko/27.0 Firefox/27.0
- Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/39.0.2171.95 Safari/537.36
- Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:34.0) Gecko/20100101 Firefox/34.0
I. Example of values collected on AmIUnique

Other custom user-agents

- godzilla/5.0 (X122; BSD; rv:500.0) Gecko/20100101
- pouet
- “54. When a warlike prince attacks a powerful state, his generalship shows itself in preventing the concentration of the enemy's forces. He overawes his opponents, and their allies are prevented from joining against him.”
- Deepnet Explorer 1.5.3; Smart 2x2; Avant Browser; .NET CLR 2.0.50727; InfoPath.1)
- NSA
- Game Boy Advance
- eat it
1. Canvas fingerprinting – Test on AmIUnique

Cwm fjordbank glyphs vext quiz, 😊

Cwm fjordbank glyphs vext quiz, 😊
I. Impact on privacy

What makes fingerprinting a threat to online privacy?

1. It is really easy to collect all this data. No need for extra permissions.

2. Two studies have investigated the diversity of browser fingerprints.

470,161 fingerprints
94.2% were unique

118,934 fingerprints
89.4% were unique

Tracking is possible
Outline

I. What is browser fingerprinting?

II. Defending against fingerprinting: Blink and FPRandom

III. Conclusion
II. Blink – Defending against fingerprinting

- Goal: to protect users against browser fingerprinting, i.e. to prevent them from being tracked online

- Challenge: finding the right balance between protection and usability

- The proposed defense solution should:
  - not break browsing.
  - not be detectable (no inconsistencies or no side-effects).
  - work automatically without requiring user interaction.
II. Blink – Approach

• Increase temporal diversity of fingerprints

• Browsing without Blink

• Browsing with Blink

• Reconfigure platform at runtime
II. Blink – Prototype

Host machine

- OS
- Browser
- User Profile

Diversity reservoir

- Browsers: B1, B2, B3, B4
- Plugins: P1, P2, P3, P4
- Fonts: F1, F2, F3, F4

Browsing platform

OS: VM1, VM2, VM3
II. FPRandom

- Protection against specific techniques of fingerprinting at the browser level
- Targeting “dynamic” attributes, i.e. those that are the result of a computation, by introducing noise
II. Blink and FPRandom

Blink
OS level

FPRandom
Browser level

Browsing Platform 1
Plugins
Browser
Fonts
Operating System
Virtual Hardware

Browsing Platform N
Plugins
Browser
Fonts
Operating System
Virtual Hardware

Virtualization Layer
Operating System
Physical Hardware

Introduction of noise

Size
Color
Text
I. What is browser fingerprinting?

II. Defending against fingerprinting: Blink and FPRandom

III. Conclusion
III. Conclusion – Overview on fingerprinting

Past

Understand fingerprinting
Add new attributes
Design defense mechanisms

Present

Use fingerprints
Protect against it

Future

Increase online security?
Regulate fingerprinting
Control fingerprinting?

Will you allow github.com to collect your browser fingerprint? This may be used to verify your online identity.

https://github.com/rapid7/metasploit-framework
Thank you!
Any questions?

Contact
plaperdrix@cs.stonybrook.edu
@RockPartridge

Websites on fingerprinting
https://amiunique.org
https://fpcentral.tbb.torproject.org/
Additional slides
Am I Unique?

- Study performed on 118,934 in 2016
- 90% of unique fingerprints → Tracking is possible
- Validates Panopticlick’s findings
- Fingerprinting mobile devices is possible
  - List of plugins and fonts are strongest on desktops
  - User-agents and canvas are strongest on mobile devices
- Online privacy could be improved with simple browser modifications
**AmIUnique – Entropy for all collected attributes**

**Normalized Shannon Entropy [0,1]**

- User agent
- List of plugins
- List of fonts
- Screen resolution
- Timezone
- Cookies enabled
- Accept
- Content encoding
- Content language
- List of HTTP headers
- Platform
- Do Not Track
- Use of local storage
- Canvas

Legend:
- **All**
- **Desktop**
- **Mobile**
• Project developed as part of the Google Summer of Code 2016
• Help Tor users to see if their fingerprint only has acceptable values
• Help Tor developers react to new fingerprinting vectors rapidly
• Will integrate the Quality Assurance process of the Tor Browser to verify the non-regression of the Tor fingerprinting protection
• In theory, all fingerprints from the Tor Browser should be identical.

• In reality, differences can still be found (screen resolution, platform...).
Plugins – Current state in browsers

• Plugins are considered to be a source of hangs, crashes, security incidents, and code complexity.

• HTML5 now replaces the features offered by plugins.

• Support for the plugin architecture called NPAPI was removed from Chrome in April 2015 and Firefox in March 2017.
Plugins – Data from AmIUnique (2015)

- The global entropy of plugins is rapidly dropping.
- Their use in fingerprinting is becoming limited.
Timeline from “Battery Status Not Included: Assessing Privacy in Web Standards” by Olejnik et al.