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?

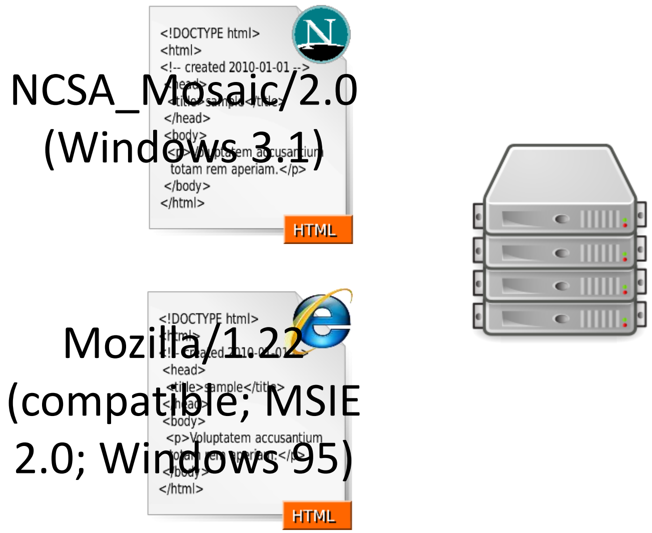
II. Defending against fingerprinting: Blink and FPRandom

III. Conclusion

I. Internet and web browsers

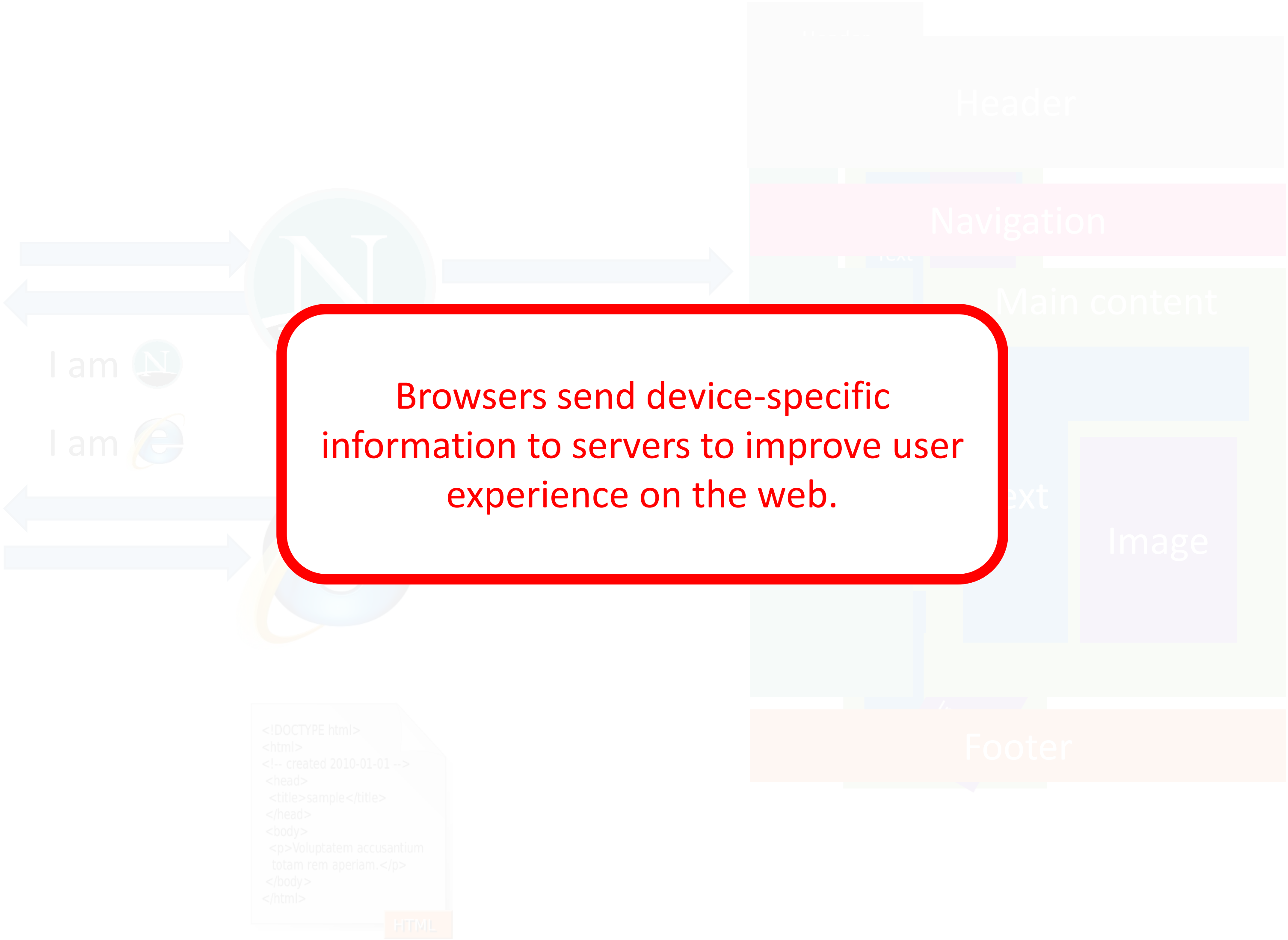
I. Internet in 1995

HTTP User agent



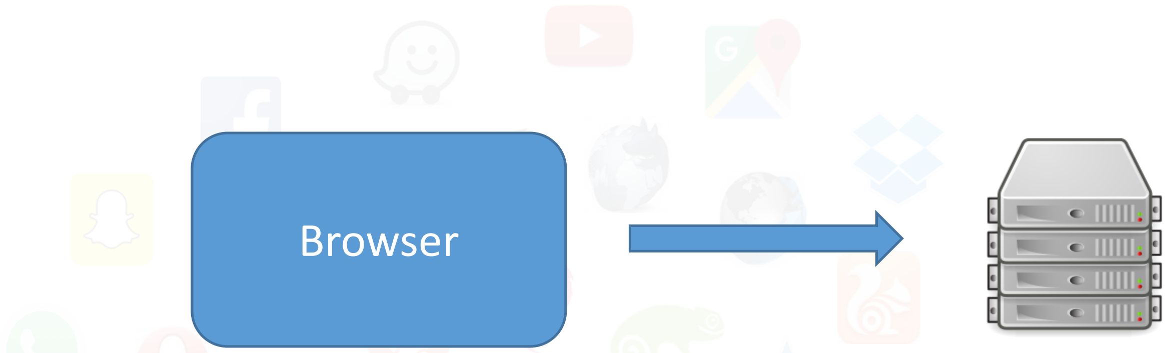
NCSA_Mosaic/2.0 (Windows 3.1)

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



Browsers send device-specific information to servers to improve user experience on the web.

I. Internet in 2019



1995	2019
Browser: Netscape Language: Fr	Browser: Chrome v71 OS: Linux Screen: 1920x1080 Language: Fr Timezone: GMT+1 Graphic card: GTX 1080Ti …

A bigger and richer web

- Audio
- Video
- 3D rendering
- Real-time communications
- Web payments
- Virtual reality

…

What happens when we start collecting all the information available in a web browser?

I. Definition of browser fingerprinting

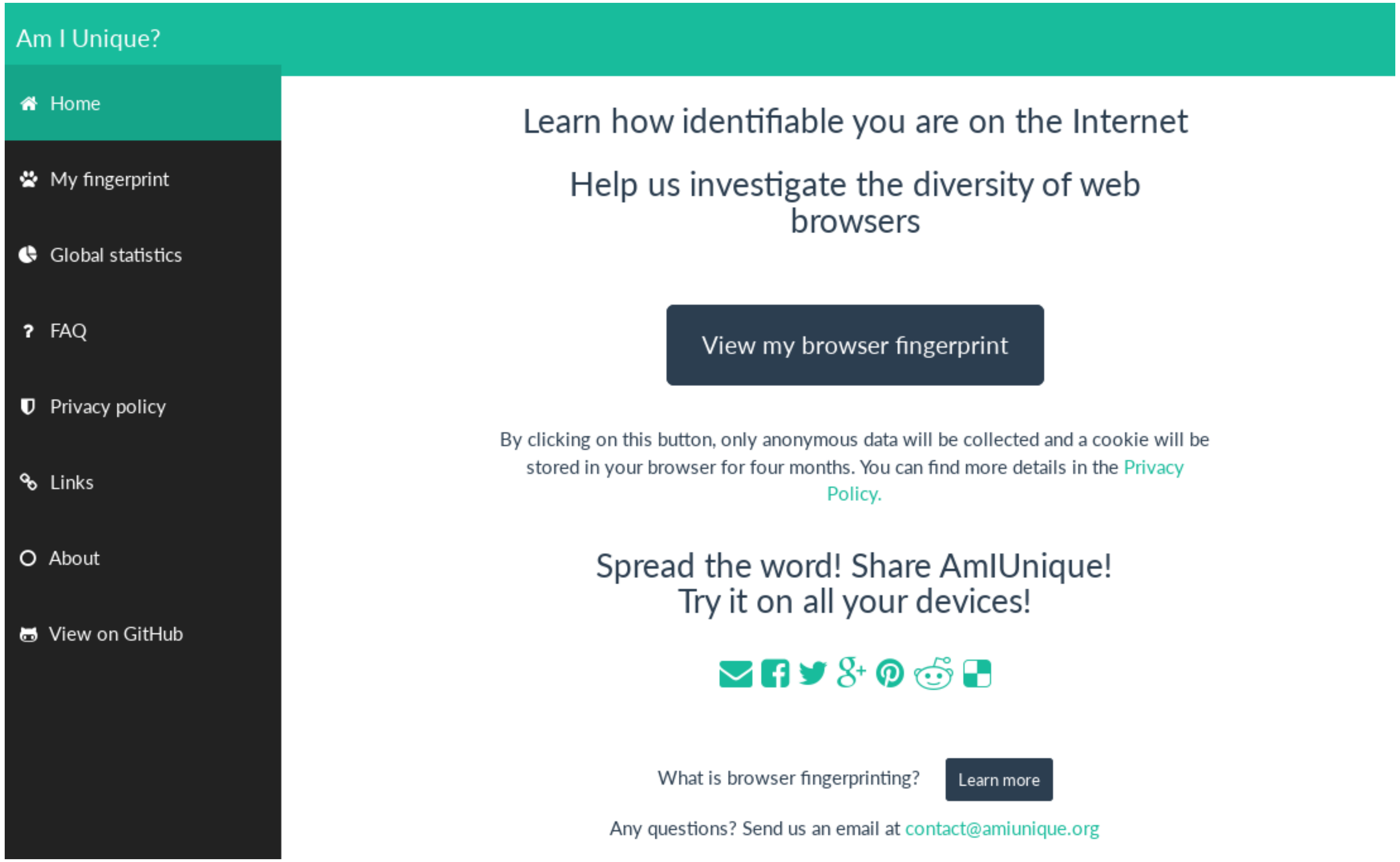
Definitions

- 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.

I. See your own fingerprint

https://amiunique.org (Am I Unique)



Learn how identifiable you are on the Internet

Help us investigate the diversity of web browsers

By clicking on this button, only anonymous data will be collected and a cookie will be stored in your browser for four months. You can find more details in the Privacy Policy.

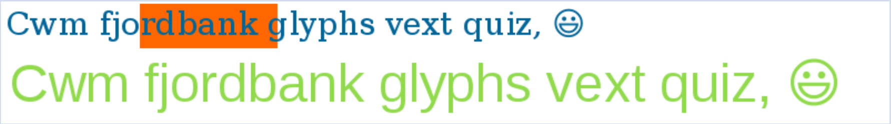
Spread the word! Share AmIUnique!
Try it on all your devices!

What is browser fingerprinting?

Any questions? Send us an email at contact@amiunique.org

- 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

Attribute	Value
User agent	Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:55.0) Gecko/20100101 Firefox/55.0
HTTP headers	text/html, application/xhtml+xml, application/xml;q=0.9,*/*;q=0.8 gzip, deflate, br en-US,en;q=0.5
Plugins	Plugin 0: QuickTime Plug-in 7.6.6; libtotem-narrowspace-plugin.so; Plugin 1: Shockwave Flash; Shockwave Flash 26.0 r0; libflashplayer.so.
Fonts	Century Schoolbook, Source Sans Pro Light, DejaVu Sans Mono, Bitstream Vera Serif, URW Palladio L, Bitstream Vera Sans Mono, Bitstream Vera Sans, ...
Platform	Linux x86_64
Screen resolution	1920x1080x24
Timezone	-480 (UTC+8)
OS	Linux 3.14.3-200.fc20.x86 32-bit
WebGL vendor	NVIDIA Corporation
WebGL renderer	GeForce GTX 650 Ti/PCIe/SSE2
Canvas	 Cwm fjordbank glyphs vext quiz, 😃 Cwm fjordbank glyphs vext quiz, 😃

I. Example of values collected on AmIUnique

Some user-agents

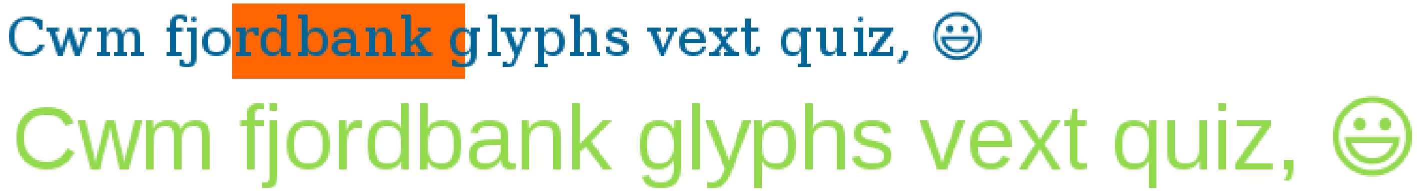
- Mozilla/5.0 (Windows NT 6.1; WOW64; rv:34.0) Gecko/20100101 Firefox/34.0
- Mozilla/5.0 (iPhone; CPU iPhone OS 8_1_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12B440 Safari/600.1.4
- Mozilla/5.0 (Android; Mobile; rv:27.0) Gecko/27.0 Firefox/27.0
- Mozilla/5.0 (Macintosh; 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

I. Canvas fingerprinting – Test on AmIUnique



Cwm fjordbank glyphs vext quiz, 😃

Cwm fjordbank glyphs vext quiz, 😃

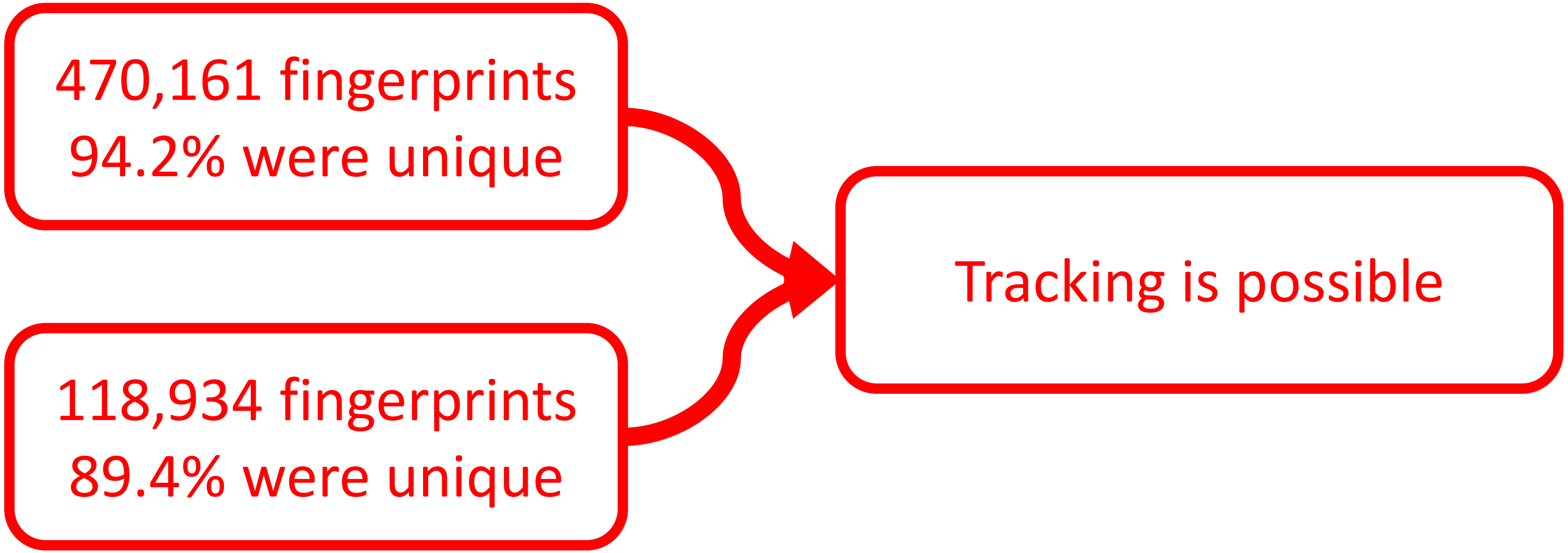
I. Impact on privacy

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.

Panopticlick
How Unique — and Trackable — Is Your Browser?

Am I Unique?



470,161 fingerprints
94.2% were unique

118,934 fingerprints
89.4% were unique

Tracking is possible

Outline

I. What is browser fingerprinting?

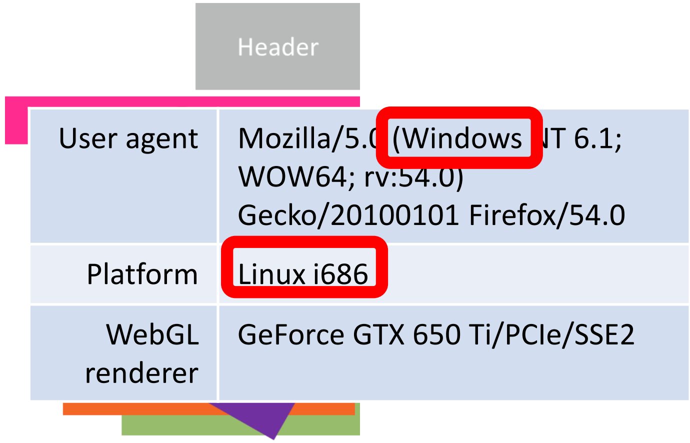
II. Defending against fingerprinting: Blink and FPRandom

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

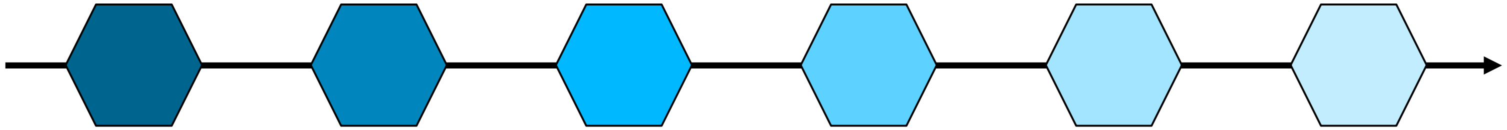
- The proposed defense solution should:
  - not break browsing.
  - not be detectable (no inconsistencies or no side-effects).
  - work automatically without requiring user interaction.



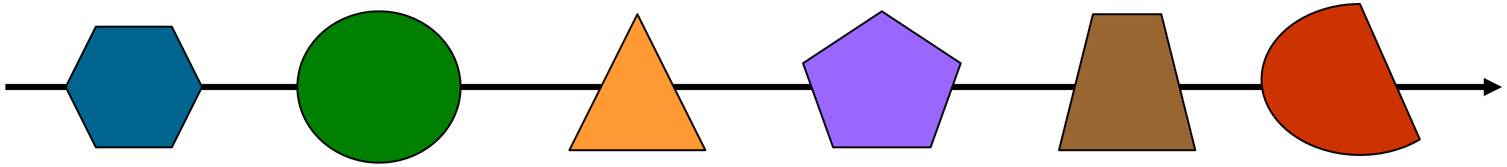
User agent	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0
Platform	Linux i686
WebGL renderer	GeForce GTX 650 Ti/PCIe/SSE2

II. Blink – Approach

- Increase temporal diversity of fingerprints
- Browsing without Blink

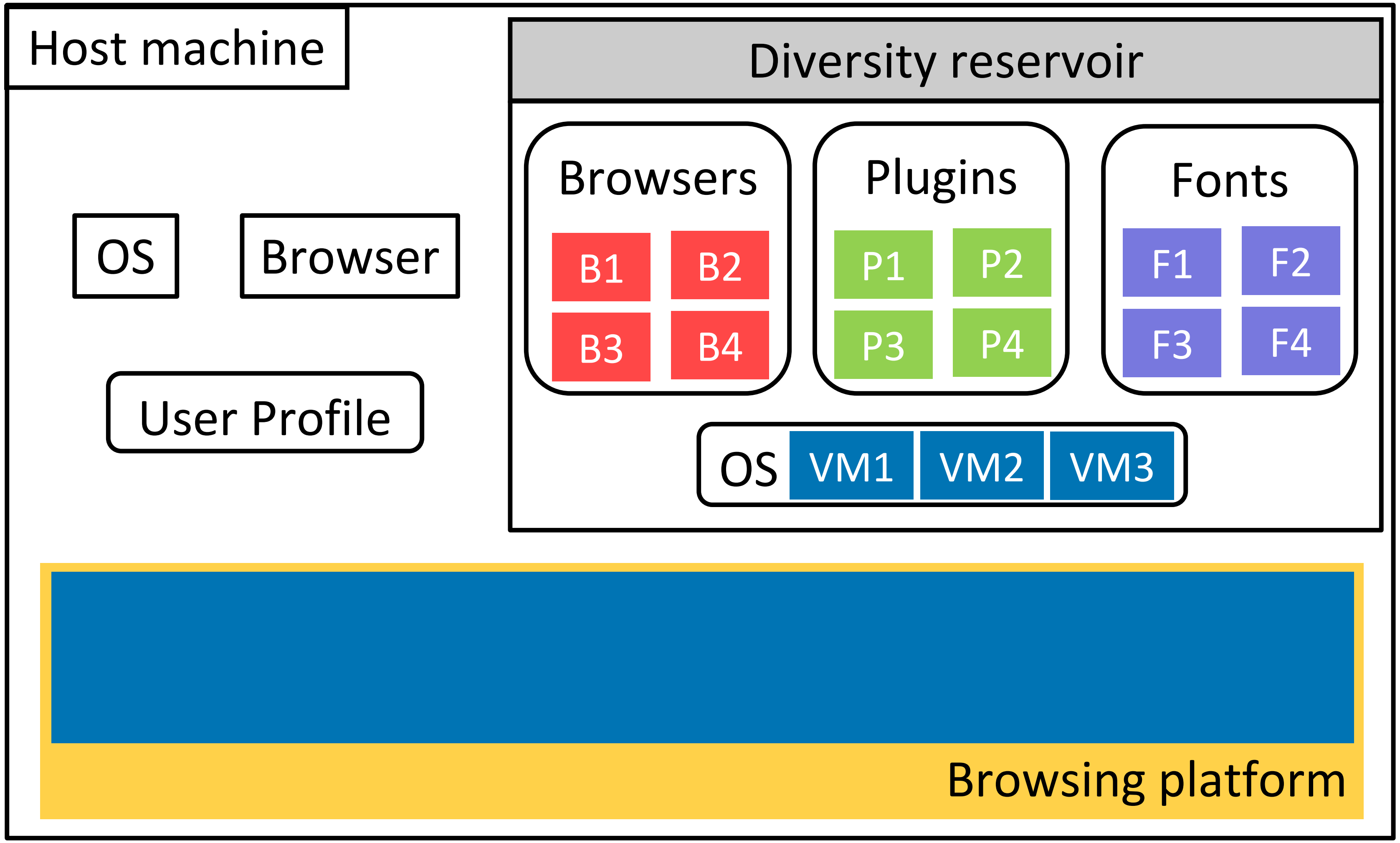


- Browsing with Blink



- Reconfigure platform at runtime

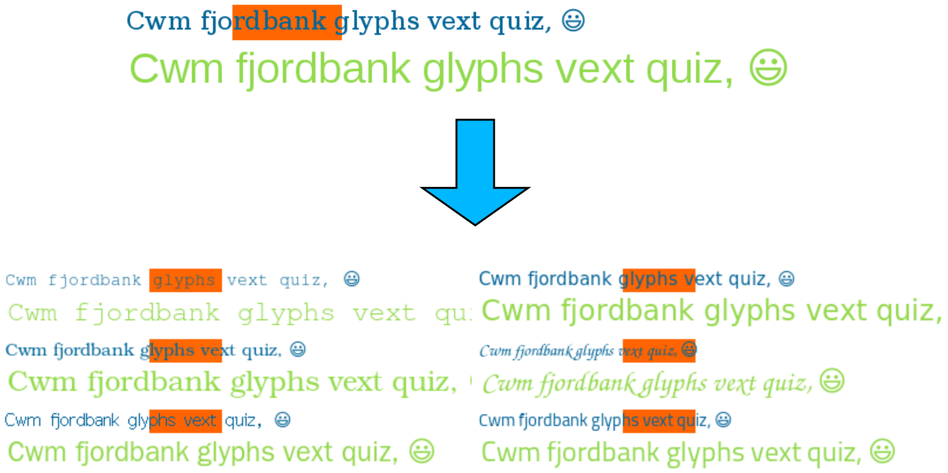
II. Blink – Prototype



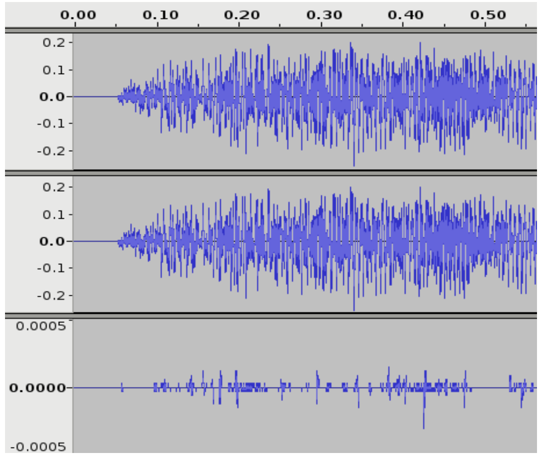
II. FPRandom

- 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

Canvas fingerprinting


Cwm fjordbank glyphs vext quiz, 😃
Cwm fjordbank glyphs vext quiz, 😃
Cwm fjordbank glyphs vext quiz, 😃
Cwm fjordbank glyphs vext qu
Cwm fjordbank glyphs vext quiz, 😃
Cwm fjordbank glyphs vext quiz,
Cwm fjordbank glyphs vext quiz, 😃
Cwm fjordbank glyphs vext quiz,
Cwm fjordbank glyphs vext quiz, 😃
Cwm fjordbank glyphs vext quiz, 😃
Cwm fjordbank glyphs vext quiz, 😃
Cwm fjordbank glyphs vext quiz, 😃
Cwm fjordbank glyphs vext quiz, 😃
Cwm fjordbank glyphs vext quiz, 😃
Cwm fjordbank glyphs vext quiz, 😃
Cwm fjordbank glyphs vext quiz, 😃

AudioContext fingerprinting



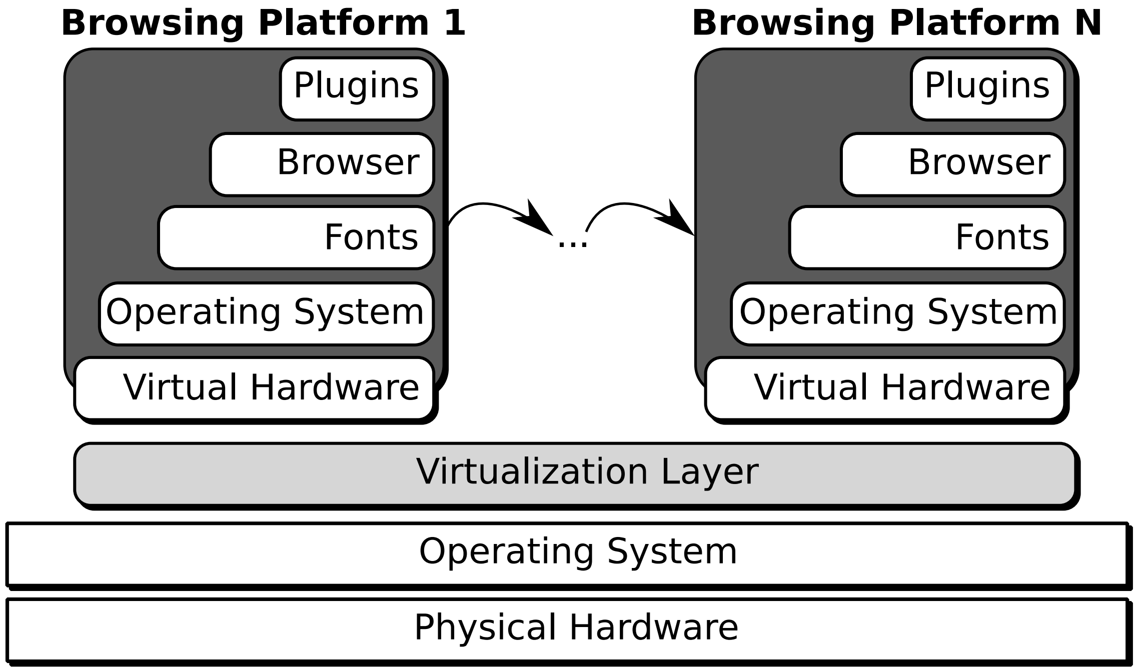
Enumeration order

sendBeacon;vibrate;javaEnabled;getGamepads;mozGetUserMedia;requestMediaKeySystemAccess;registerProtocolHandler;registerContentHandler;taintEnabled;permissions…..

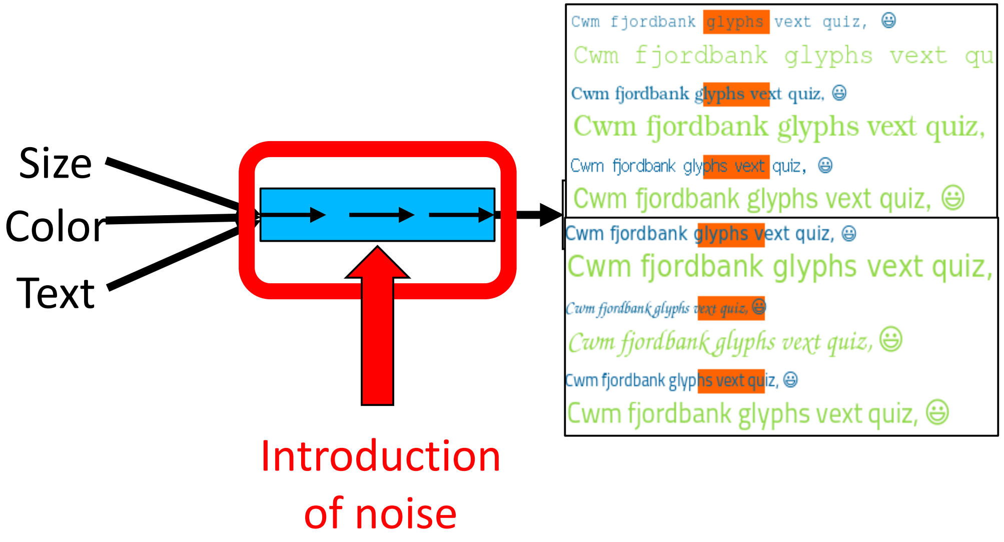
plugins;oscpu;doNotTrack;getVRDisplays;mimeTypes;vibrate;vendorSub;vendor;productSub;cookieEnabled;mozGetUserMedia;getBattery;buildID;javaEnabled;getGamepads;permissions…

II. Blink and FPRandom

Blink
OS level



FPRandom
Browser level



Outline

I. What is browser fingerprinting?

II. Defending against fingerprinting: Blink and FPRandom

III. Conclusion

III. Conclusion – Overview on fingerprinting

Past

Understand fingerprinting

Panopticlick
How Unique – and Trackable – Is Your Browser?

Am I Unique?

Add new attributes

Cwm fjordbank glyphs vext quiz, 😃

Cwm fjordbank glyphs vext quiz, 😃

Design defense mechanisms

Present

Use fingerprints

ThreatMetrix, SHIELDSQUARE, distil networks, sift science, perimeterx, iovation, MAXMIND, DATADOME, INFISECURE

Protect against it

Tracking at large scale

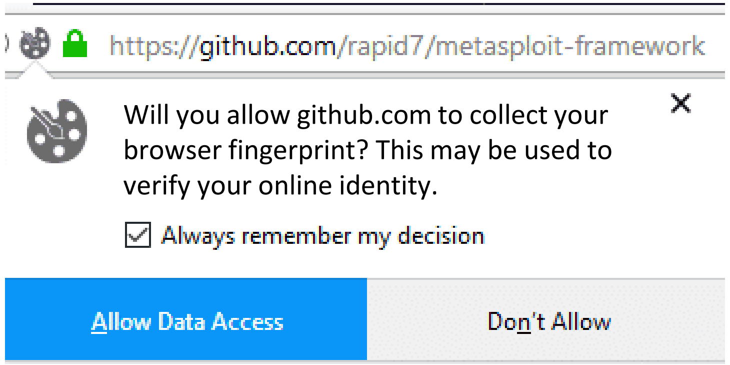
🤔

Future

Increase online security?

Regulate fingerprinting

Control fingerprinting?


https://github.com/rapid7/metasploit-framework

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

☑ Always remember my decision

Thank you!
Any questions?

Contact

✉ plaperdrix@cs.stonybrook.edu

@RockPartridge

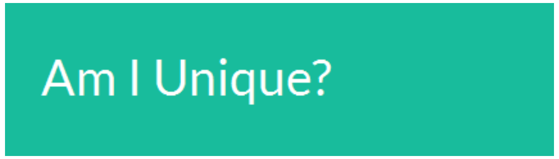
Websites on fingerprinting

https://amiunique.org

https://fpcentral.tbb.torproject.org/

Additional slides

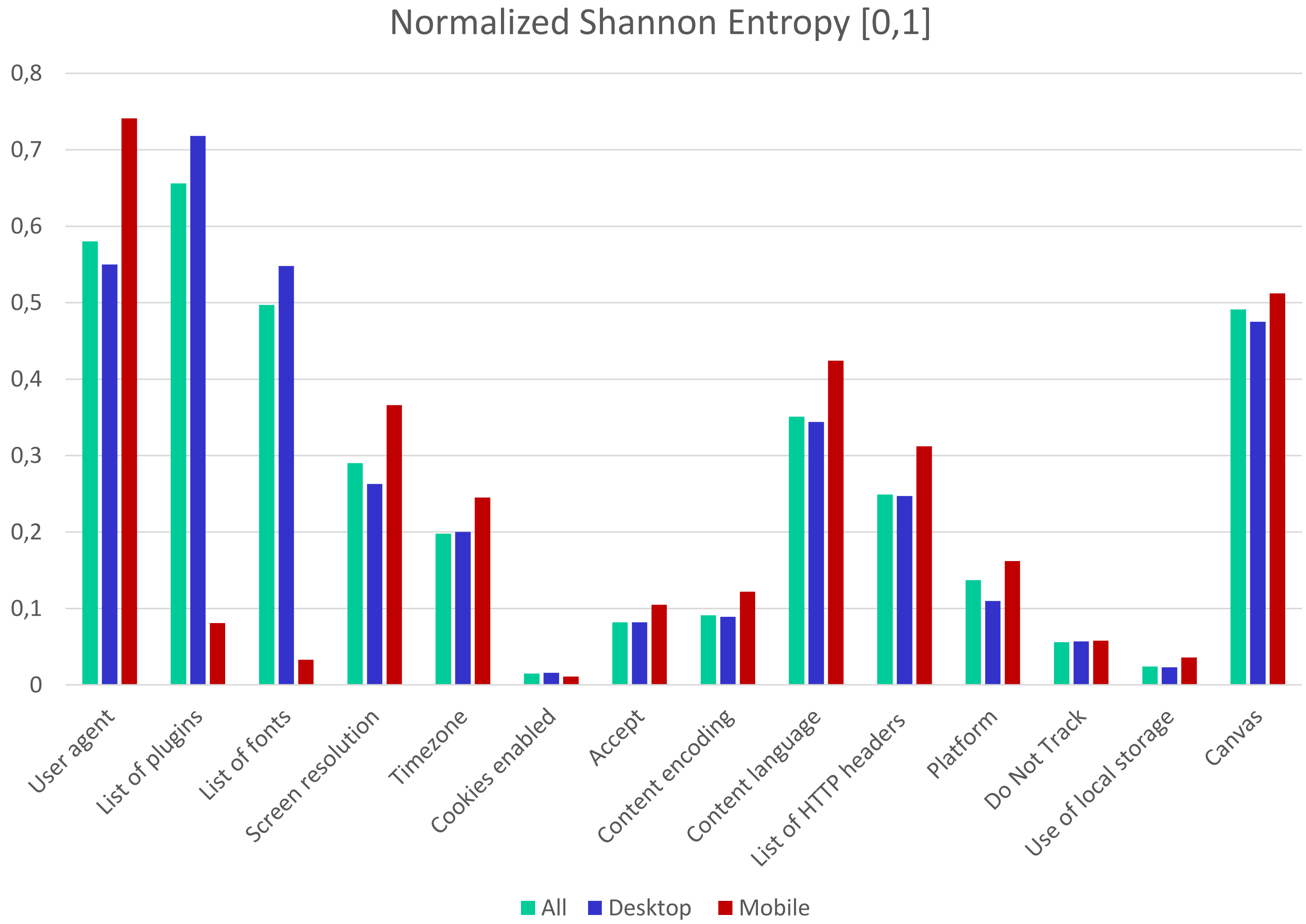
AmIUnique – Study



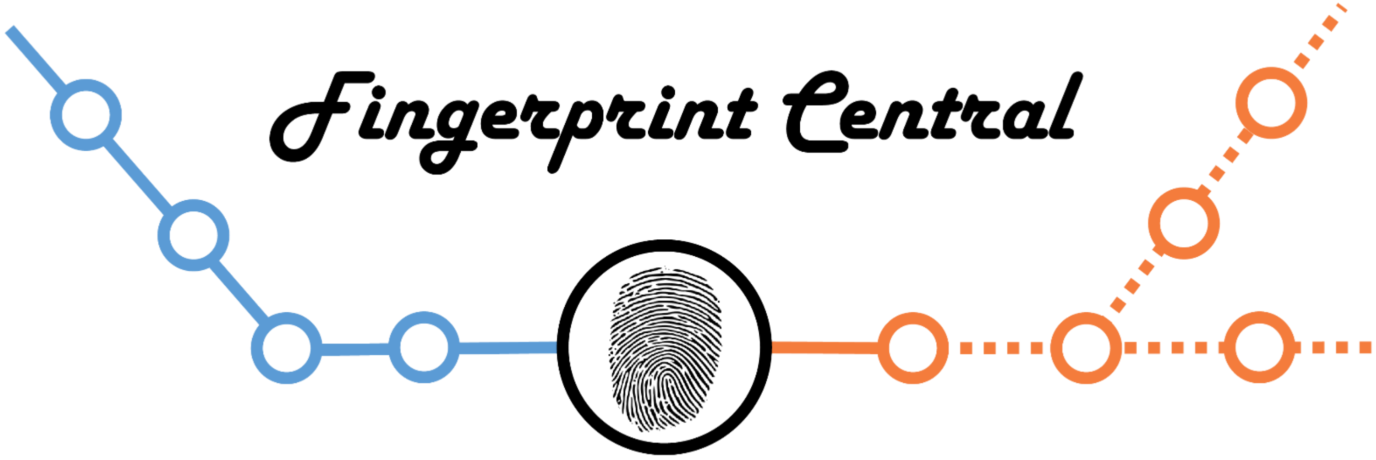
Am I Unique?

- 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



Fingerprint Central



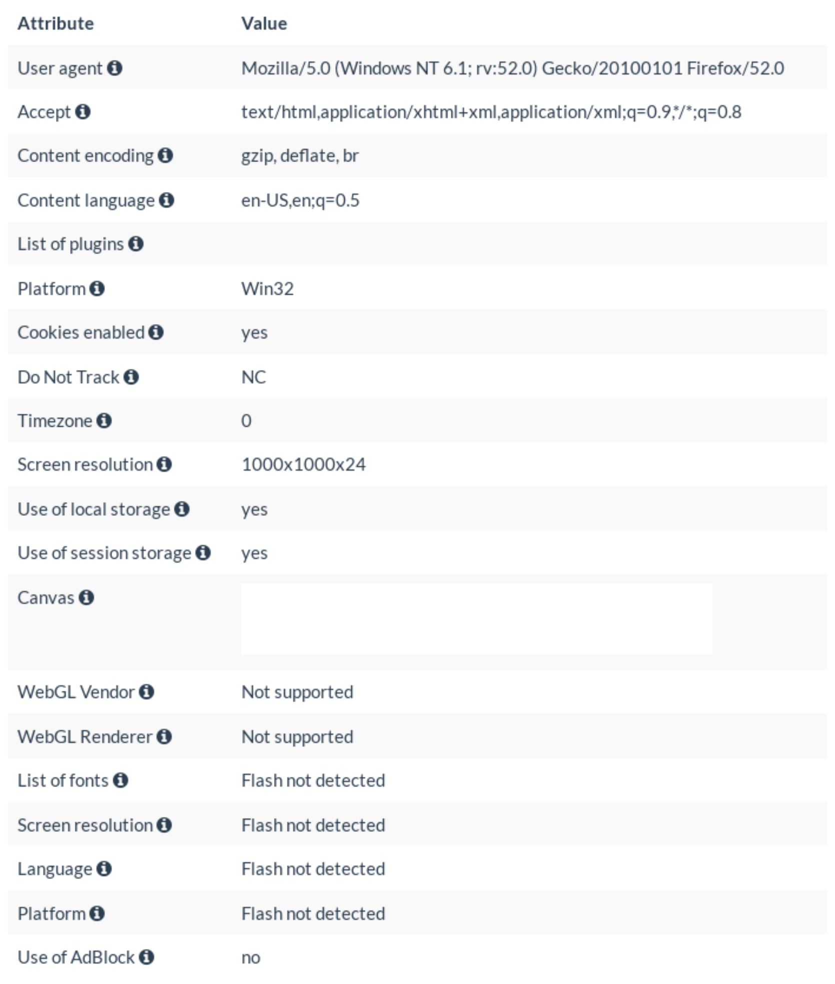
Your privacy starts here.

- 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

Tor browser

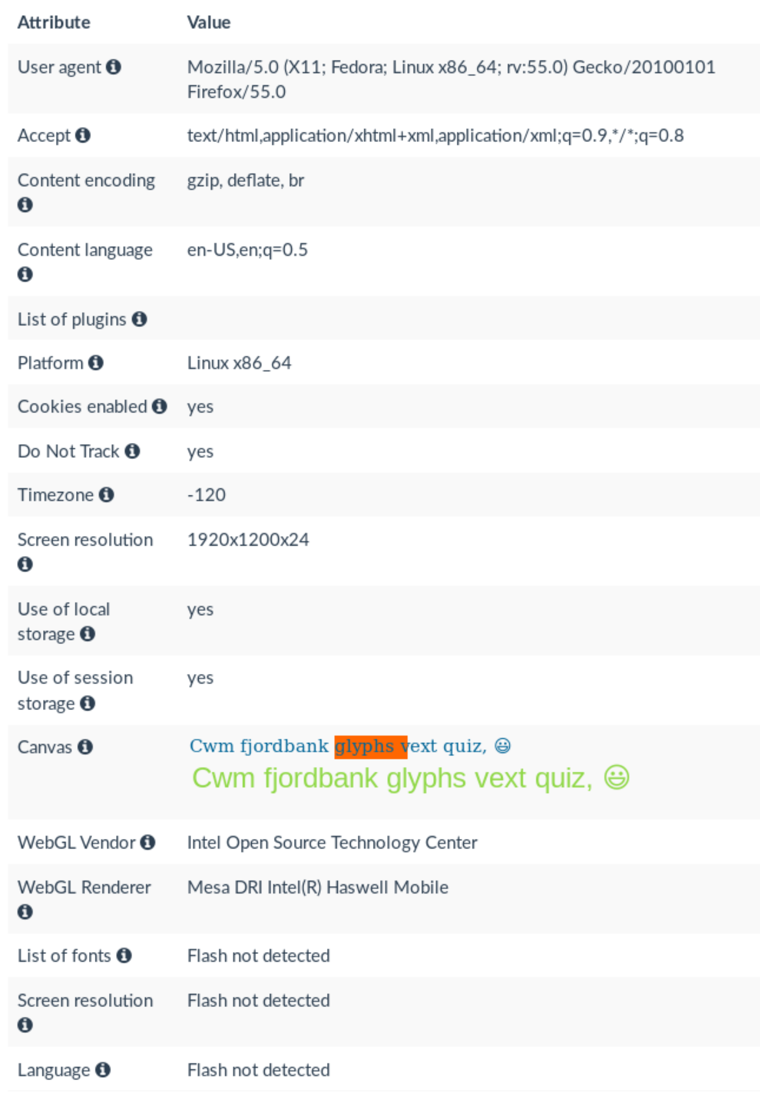
- In theory, all fingerprints from the Tor Browser should be identical.
- In reality, differences can still be found (screen resolution, platform…).

Tor browser on Fedora 25



Attribute	Value
User agent	Mozilla/5.0 (Windows NT 6.1; rv:52.0) Gecko/20100101 Firefox/52.0
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Content encoding	gzip, deflate, br
Content language	en-US,en;q=0.5
List of plugins	
Platform	Win32
Cookies enabled	yes
Do Not Track	NC
Timezone	0
Screen resolution	1000x1000x24
Use of local storage	yes
Use of session storage	yes
Canvas	
WebGL Vendor	Not supported
WebGL Renderer	Not supported
List of fonts	Flash not detected
Screen resolution	Flash not detected
Language	Flash not detected
Platform	Flash not detected
Use of AdBlock	no

Firefox browser on Fedora 25



Attribute	Value
User agent	Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:55.0) Gecko/20100101 Firefox/55.0
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Content encoding	gzip, deflate, br
Content language	en-US,en;q=0.5
List of plugins	
Platform	Linux x86_64
Cookies enabled	yes
Do Not Track	yes
Timezone	-120
Screen resolution	1920x1200x24
Use of local storage	yes
Use of session storage	yes
Canvas	Cwm fjordbank glyphs vext quiz, 😃 Cwm fjordbank glyphs vext quiz, 😃
WebGL Vendor	Intel Open Source Technology Center
WebGL Renderer	Mesa DRI Intel(R) Haswell Mobile
List of fonts	Flash not detected
Screen resolution	Flash not detected
Language	Flash not detected

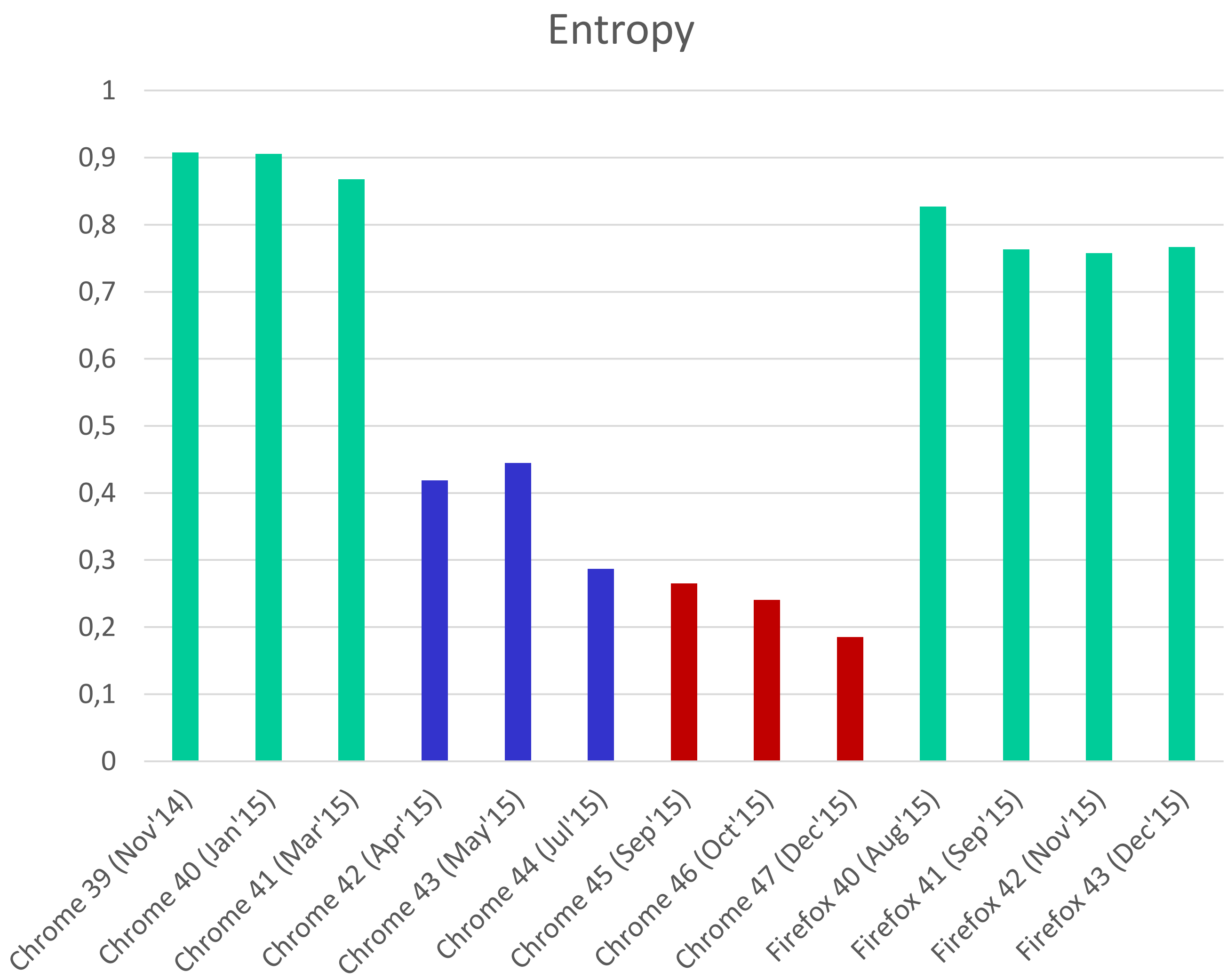
Plugins – Current state in browsers

- 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)

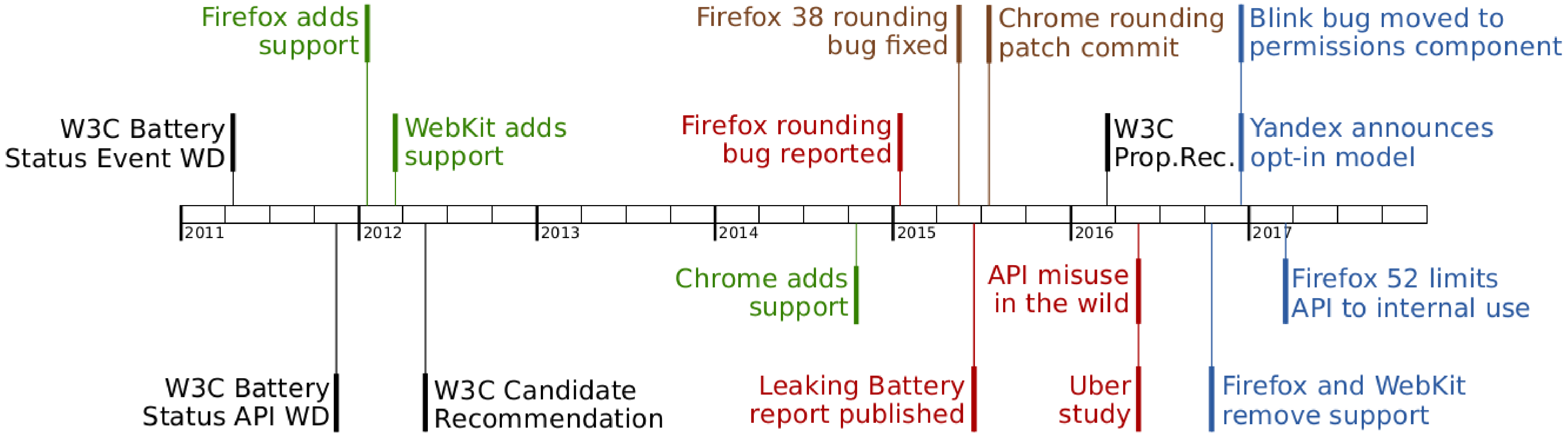


NPAPI support

- 🟩 Enabled
- 🟦 Disabled
- 🟥 Removed

- The global entropy of plugins is rapidly dropping.
- Their use in fingerprinting is becoming limited.

Battery API - History


Firefox adds support
W3C Battery Status Event WD
WebKit adds support
Firefox 38 rounding bug fixed
Firefox rounding bug reported
Chrome rounding patch commit
W3C Prop.Rec.
Blink bug moved to permissions component
Yandex announces opt-in model
2011
2012
2013
2014
2015
2016
2017
Chrome adds support
API misuse in the wild
Firefox 52 limits API to internal use
W3C Battery Status API WD
W3C Candidate Recommendation
Leaking Battery report published
Uber study
Firefox and WebKit remove support

Timeline from “Battery Status Not Included: Assessing Privacy in Web Standards” by Olejnik et al.