Le traçage par empreintes de navigateur

Pierre Laperdrix [1]

Pierre Laperdrix a soutenu sa thèse [2] en octobre 2017 à l'IRISA, à Rennes, sous la direction de Benoit Baudry et Gildas Avoine. Après avoir effectué un séjour de recherche à l'université de Stony Brook aux États-Unis, il est actuellement chercheur postdoctoral au laboratoire CISPA en Allemagne.

L'arrivée de l'Internet a révolutionné notre société à l'aube du 21e siècle. Nos habitudes se sont métamorphosées pour prendre en compte cette nouvelle manière de communiquer et de partager avec le monde. Grâce aux technologies qui en constituent ses fondations, le web est une plateforme universelle. Que vous utilisiez un PC de bureau sous Windows, un PC portable sous MacOS, un serveur sous Linux ou une tablette sous Android, chacun a les moyens de se connecter à ce réseau de réseaux pour partager avec le monde. La technique dite de *Browser fingerprinting* est née de cette diversité logicielle et matérielle qui compose nos appareils du quotidien (voir Figure 1).

En exécutant un script dans le navigateur web d'un utilisateur, un serveur peut récupérer une très grande quantité d'informations. Il a été démontré qu'il est possible d'identifier de façon unique un appareil en récoltant suffisamment d'informations. L'impact d'une telle approche sur la vie privée des internautes est alors conséquente,

1. plaperdrix@cs.stonybrook.edu
2. https://tel.archives-ouvertes.fr/tel-01729126

FIGURE 1. Diversité de l'Internet moderne

car le *browser fingerprinting* est totalement indépendant des systèmes de traçage connus comme les *cookies*.

Pendant ma thèse, mon objectif était de comprendre ce phénomène d'empreintes de navigateurs et de développer des systèmes de défense appropriés. Que peut-on récolter ? Quels sont les mécanismes qui influencent les valeurs récoltées ? Comment peut-on s'en protéger ? Pour répondre à ces questions, j'ai lancé le site `AmIUnique.org` [3] (« *Am I unique ?* » ou « Suis-je unique ? » en français).

Plus de quatre ans après son lancement, le site recense plus de mille connexions par jour, et plus d'un million d'utilisateurs sont déjà venus consulter leur empreinte de navigateur et vérifier ainsi si elle était unique ou non (voir Figure 2). Si vous n'avez pas encore fait le test, rendez-vous vite sur le site ! Vous y trouverez des explications ainsi que des liens vers des outils pour vous protéger du traçage sur Internet. Dans le cadre de mes travaux, les données récoltées par ce site ont été une source d'informations essentielles qui m'a permis de comprendre en détail ce qui était possible avec cette technique [10].

Comment se protéger du traçage par empreintes ?

Aujourd'hui, le *browser fingerprinting* est toujours au cœur de l'actualité, et des grands noms de l'Internet comme Apple [3], Mozilla [4] ou Brave [1] travaillent activement dans ce domaine pour protéger leurs internautes. Ils développent des patchs

3. `https://amiunique.org`.

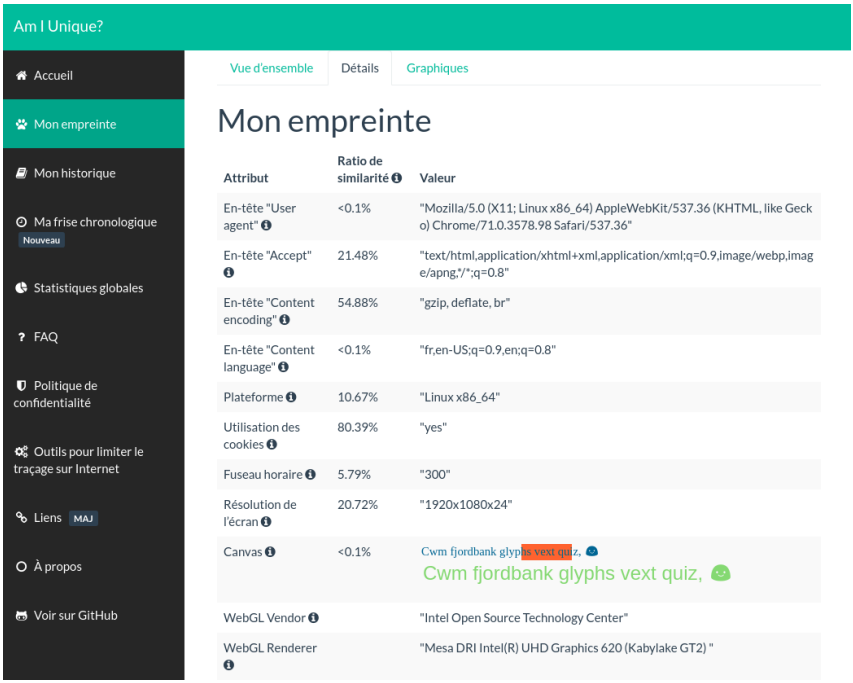
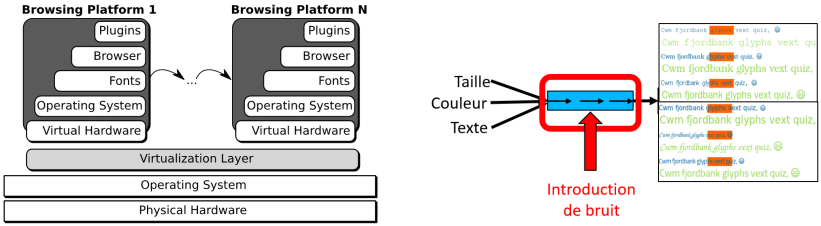


FIGURE 2. Exemple d'empreinte récoltée sur le site `AmIUnique.org`

pour leur navigateur pour éliminer le plus possible les différences observables entre appareils. Le navigateur `Tor`, très célèbre pour sa protection forte de l'anonymat sur Internet, va même encore plus loin en exhibant la même empreinte pour chacun de ses utilisateurs [7, 6].

De mon côté, j'ai exploré dans mes travaux comment tromper les traçeurs sur Internet en changeant constamment d'empreintes. En exploitant la diversité logicielle, j'ai développé une contre-mesure nommée Blink [9] qui assemble différents composants en temps-réel pour créer un environnement de navigation aléatoire (voir Figure 3(a)). En modifiant le comportent du navigateur, j'ai réalisé une deuxième contre-mesure nommée FPRandom [8] qui introduit du bruit dans différentes fonctions utilisées pour du *fingerprinting* (voir Figure 3(b)).

Au final, la méthode la plus simple pour se prémunir de cette pratique est tout simplement de bloquer les scripts de traçage et de les éviter. L'utilisation d'un bloqueur de publicités comme `uBlock Origin` ou de moteurs de recherche respectueux de la vie privée comme `Qwant` [5] ou `DuckDuckgo` [2] est très fortement conseillée.



(a) Bink : protection au niveau du système d'exploitation

(b) FPRandom : protection au niveau du navigateur

FIGURE 3. Deux contre-mesures contre le traçage par empreintes

Références

[1] Brave browser — Fingerprinting Protection Mode. https://github.com/brave/browser-laptop/wiki/Fingerprinting-Protection-Mode.

[2] DuckDuckGo — Privacy, simplified. https://duckduckgo.com/.

[3] Engadget — What you need to know about Apple's war on 'digital fingerprinting'. https://www.engadget.com/2018/06/05/apple-safari-canvas-fingerprinting/.

[4] Mozilla — Security/Fingerprinting. https://wiki.mozilla.org/Security/Fingerprinting.

[5] Qwant — The search engine that respects your privacy. https://www.qwant.com/.

[6] Tor Project — Fingerprint Central. https://fpcentral.tbb.torproject.org/.

[7] Tor Project — The Design and Implementation of the Tor Browser. https://www.torproject.org/projects/torbrowser/design/#fingerprinting-linkability.

[8] Pierre Laperdrix, Benoit Baudry, and Vikas Mishra. FPRandom : Randomizing core browser objects to break advanced device fingerprinting techniques. In *9th International Symposium on Engineering Secure Software and Systems (ESSoS 2017)*, Bonn, Germany, July 2017.

[9] Pierre Laperdrix, Walter Rudametkin, and Benoit Baudry. Mitigating browser fingerprint tracking : multi-level reconfiguration and diversification. In *10th International Symposium on Software Engineering for Adaptive and Self-Managing Systems (SEAMS 2015)*, Firenze, Italy, May 2015.

[10] Pierre Laperdrix, Walter Rudametkin, and Benoit Baudry. Beauty and the Beast : Diverting modern web browsers to build unique browser fingerprints. In *37th IEEE Symposium on Security and Privacy (S&P 2016)*, San Jose, United States, May 2016.