

Internship “Detecting the tool and the filter lists used by ad blocking solutions”

Advisors:

Walter Rudametkin (Univ. Rennes, Inria, CNRS, IRISA, IUF)

Pierre Bourhis (CNRS, Univ. Lille, Inria)

Pierre Laperdrix (CNRS, Univ. Lille, Inria)

October 9, 2024

1 Subject

Online tracking is an integral part of the Internet. As reported by the 2022 Web Almanac¹, 82% of websites contain at least one third-party tracker. While tracking can be good if the collected data is used to improve the user experience like providing relevant recommendations or an easier way to login, it can also be bad if the collected data is used negatively to target an individual or a group of individuals to influence their choices or even cause them harm. For this reason, a lot of users opt to use ad blocking solutions to protect their privacy online.

To block ads, users can opt for different solutions from ad blocking extensions like uBlock Origin² or AdBlock³ to browsers with a built-in blocker like Brave⁴ to DNS servers that block dangerous connections like NextDNS⁵. Each of these solutions has its own way of working but the consequence is that they could all be potentially detected with the right set of tests, which would contribute to the fingerprint of the device [2]. A fingerprint is a list of attributes that has been collected by a website that provides information on the browser, the OS and even the hardware used by the user. Because the diversity of all those components is so great in the general population, it has been shown that it can be used to identify a user online. The use of an ad blocking solution can act as an additional attribute in a device’s fingerprint.

The goal of this internship is to design tests that can be used to detect as much as possible about the usage of an ad blocker, notably what is the exact tool being used and which filter lists are currently enabled [1]. Several research paths can be explored from the detection of specific selectors to the measurement of the blocking performance to distinguish different solutions [3].

2 Prerequisites

Experience in JavaScript and Web technologies is optional but strongly recommended.

3 Bibliography

- [1] Working with filters – eyeo. <https://developers.eyeo.com/working-with-filters>.
- [2] LAPERDRIX, P., BIELOVA, N., BAUDRY, B., AND AVOINE, G. Browser fingerprinting: A survey. *ACM Trans. Web 14*, 2 (apr 2020).

¹<https://almanac.httparchive.org/en/2022/privacy>

²<https://ublockorigin.com/>

³<https://getadblock.com/>

⁴<https://brave.com/learn/best-ad-blocker/>

⁵<https://nextdns.io/>

[3] MOSTSEVENKO, S. How ad blockers can be used for browser fingerprinting – Fingerprint. <https://fingerprint.com/blog/ad-blocker-fingerprinting/>.

4 Comments

The internship will take place in the Spirals team at Inria Lille. To apply, send your CV to Walter Rudametkin <walter.rudametkin@inria.fr>, Pierre Bourhis <pierre.bourhis@inria.fr> and Pierre Laperdrix at <pierre.laperdrix@inria.fr>