Comparison of Privacy Preserving Tools in Web Browsers and Extensions

Bc. Vojtěch Fiala

Supervisor: Ing. Libor Polčák, Ph.D.

Gen™

BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY

January 20, 2025

- Over 90 % (2) of all websites track their visitors.
- Users are often tracked for targeted advertising (1).
- Multiple anti-tracking methods and tools exist.
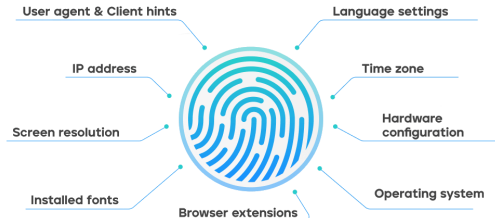- How do they compare?
- Which one to choose?

Image taken from (4)

- Design of repeatable and deterministic comparisons.
- Evaluation of API-based anti-tracking tools.
- Evaluation of content-blocking tools.
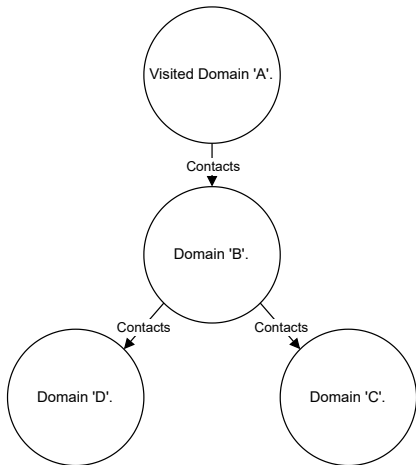- Evaluation of a tool's impact on real sites.

- What are the capabilities of each tool?
- Based on Master's Thesis by Jana Petráňová (3).
- Fingerprinting server to observe anti-tracking capabilities.
- Analysis of the results.
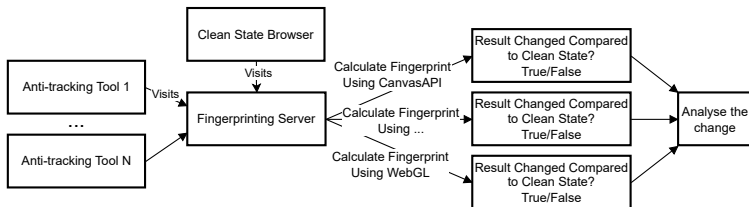
- How many fingerprinting attempts does a tool prevent?
- Use JShelter Fingerprinting Detector to observe fingerprinting attempts.
- Log the attempts to ensure repeatability and determinism.
- Compare the results with observed capabilities of each tool.
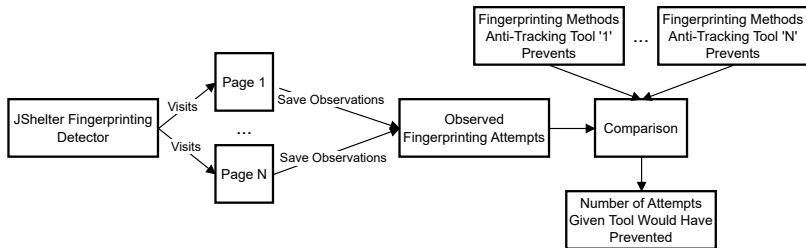
- What requests and how many of them does a tool prevent?
- Observe the traffic associated with several websites.
- Log the traffic and maintain the request structure.
- Simulate the traffic with content-blocking tool present.
- Observe the results.

Visited Domain 'A'.

Contacts

Domain 'B'.

Contacts   Contacts

Domain 'D'.   Domain 'C'.

Evaluation of Content-blocking Tools

- **How many** fingerprinting attempts does a tool **prevent**?
- Observe **fingerprinting attempts** associated with several websites.
- Log the traffic and maintain the **request structure**.
- **Simulate** the traffic with content-blocking tool **present**.
- Obtain the number of tracking attempts prevented.
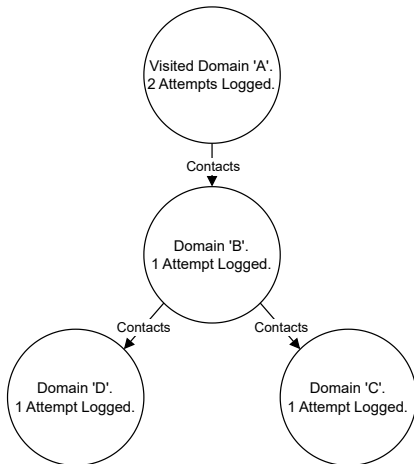
- **How many** websites does a tool **break**?
- Based on Master's Thesis by Jana Petráňová.
- Visit a website **several times** with no anti-tracking tools present.
- **Log** the **outputs** and **detect** the **content**.
- Visit the website **again** with anti-tracking tool present.
- Log the outputs and **compare** them.

- Implement the evaluators.
- Use the evaluations to compare selected anti-tracking tools.
- Draw conclusions based on the results.

(1) CYPHERS, B. and GEBHART, G. *Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance* online. Electronic Frontier Foundation, 2019. Available at: `https://www.eff.org/wp/behind-the-one-way-mirror`. (cit. 2025-01-13).

(2) DAMBRA, S.; SANCHEZ ROLA, I.; BILGE, L. and BALZAROTTI, D. *When Sally Met Trackers: Web Tracking From the Users' Perspective*. In: *31st USENIX Security Symposium (USENIX Security 22)*. Boston, MA: USENIX Association, August 2022, p. 2189–2206. ISBN 978-1-939133-31-1.

(3) PETRÁŇOVÁ, J. *Běhová prostředí pro testování činnosti rozšíření pro webový prohlížeč*. 2024. Master's thesis. Brno University of Technology, Faculty of Information Technology.

(4) VORSTER, A. *What is a Digital Fingerprinting and How Does It Work?* online. 2022. Available at: `https://blog.octobrowser.net/your-digital-fingerprint-what-it-is-and-how-it-is-used-to-deanonymize-you`. (cit. 2025-01-14).

Discussion