Introduction to Browser Fingerprinting

Fabio Fontana
Supervisor: Prof. Marina Ribaudo

University of Genoa

2023

What is Browser Fingerprinting

Browser Fingerprinting, also known as Device Fingerprinting, is a sophisticated method that allows websites and online services to collect and analyze specific data about a user's device without relying on traditional tracking techniques like cookies or IP addresses. When a user visits a website, their browser voluntarily shares certain configuration and setting details. A server can collate this information, resulting in a unique fingerprint for the user's device.

Which data is collected

- **Browser Info:**
  - User Agent, Plugins, HTTP Accept Headers
  - Cookie, Do Not Track, and Storage Settings
  - WebGL Renderer, Canvas Fingerprinting
  - WebRTC Leak, Navigator API Data
  - Ad Blockers, Performance, Errors Handling
- **Device Info:**
  - Screen Resolution, Color Depth, Available Fonts
  - Touch Support, Accelerometer, Gyroscope
  - Audio Stack, CPU, Memory, Platform
- **Network & Session:**
  - Time Zone, Language, Battery Status API
  - Network Information, TLS/SSL Session IDs
  - Active Media Queries, Mouse & Event Capabilities

Browser Fingerprinting properties: uniqueness

It is highly improbable for two users to have identical fingerprints. In fact, studies have suggested the uniqueness can be so specific that only one in several hundred thousand users might share the same fingerprint.

Browser Fingerprinting properties: stateless

Even if users disable cookies or use privacy-focused browsing modes, fingerprinting can still function, making it both challenging to detect and thwart. Unlike cookies, this method is stateless, not relying on stored data in the browser, and hence, it leaves no obvious trace.

Why it is used: the constructive way

- combat fraud or credential hijacking by checking that a user who logs into a specific site is likely the legitimate user
- suggesting updates whether a device is out of date and verify that it is genuine and known to the system
- bot detection: generic or missing fingerprints, consistency across sessions and behavioral analysis

Why it is used: the questionable way

- track users across websites and collect information about their habits and their tastes without the users knowing about it:
  - **Fingerprints as Global Identifiers:** if a device has a unique fingerprint, it is akin to a cookie that cannot be deleted
  - **Fingerprint + IP address**
    - **as Cookie Regenerators:** since users often retain the same IP for extended period their deleted cookies can be restored by matching the IP and the fingerprint
    - **in the absence of Cookies:** unmask different machines behind the same IP

Why it is used: advertising and customizing the online experience

- data collected through browser fingerprinting methods allows advertising businesses to create a custom profile for targeted advertising which indirectly means higher revenue for the company
- adapt content and prices due to your habits, status and location

Why it is used: the destructive way

Deliver exploits that are tailored for a specific user configuration

How data is collected

- with HTTP requests from the user to the website
- JavaScript scripts and browser/flash APIs
- Advanced methods like Canvas fingerprinting, WebGL and TLS fingerprinting

How data is collected: Canvas fingerprinting

How data is collected: WebGL fingerprinting

How data is collected: TLS fingerprinting

What about privacy: GDPR and ePrivacy Directive

Since browser fingerprinting relies on the collection of personal data, companies using this technique must comply with the strict requirements of the GDPR and the ePrivacy Directive. That means that companies must be transparent about the data collection process and must ask for consent when personal data processing is involved. Otherwise, companies often have proprietary methods to perform browser fingerprinting and those are often hard to be detected.

What about privacy: prevention and mitigation

- use privacy-focused browsers like Tor and anti-fingerprinting extensions like Privacy-Badger and uBlock Origin
- disable unnecessary plugins, disable useless extensions and consider using default settings to blend in with a larger crowd
- keep the software updated
- if you are a developer, build your own anti-fingerprinting countermeasure

Any questions?

References

- **Bibliography**
  - Browser Fingerprinting: A survey
  - How Unique Is Your Web Browser?
  - A Survey of Browser Fingerprint Research and Application
- **External sources**
  - https://amiunique.org
  - https://coveryourtracks.eff.org
  - https://pixelprivacy.com/resources/browser-fingerprinting