Introduction to Browser Fingerprinting

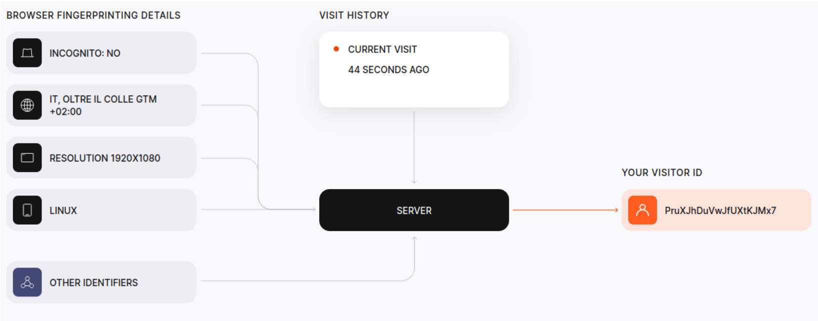
Candidate: Fabio Fontana
Supervisor: Prof. Marina Ribaudo

University of Genoa

Academic Year 2022/2023

What is Browser Fingerprinting

Browser Fingerprinting is a method that allows websites and online services to **collect** and **analyze** specific data about a user's device resulting in a **unique fingerprint** of it

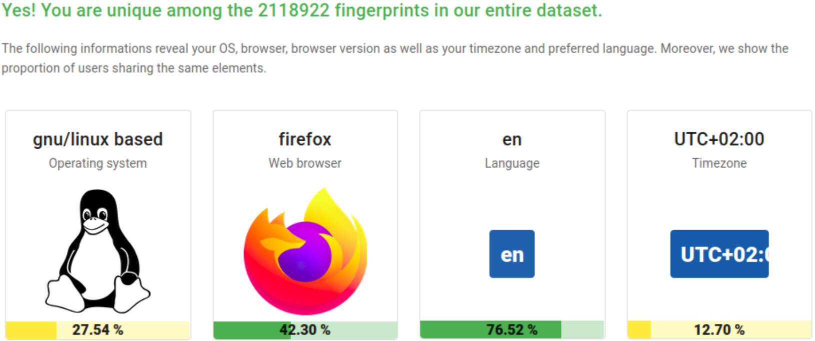


Collected data

- **Browser info:** type, version, language, plugins, settings, ...
- **Device info:** OS, GPU, screen size, fonts, battery info, ...
- **Network and Session info:** public IP, local IP, VPN, timezone, supported protocols, ...

Browser Fingerprinting properties: uniqueness

- highly improbable for two users to have identical fingerprints
- **uniqueness can be so specific** that only one in several hundred thousand users might share the same fingerprint



Yes! You are unique among the 2118922 fingerprints in our entire dataset.

The following informations reveal your OS, browser, browser version as well as your timezone and preferred language. Moreover, we show the proportion of users sharing the same elements.

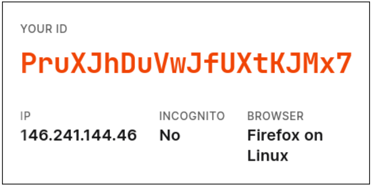
gnu/linux based Operating system	firefox Web browser	en Language	UTC+02:00 Timezone
27.54 %	42.30 %	76.52 %	12.70 %

Browser Fingerprinting properties: stateless

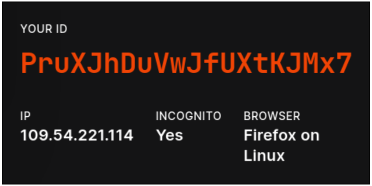
Still works even if users:

- disable cookies
- change IP
- use privacy-focused browsing modes

This method is stateless, not relying on stored data in the browser, and hence, it leaves no obvious trace.



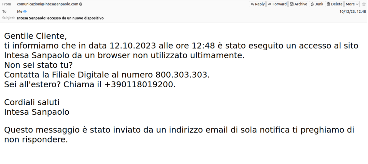
YOUR ID		
PruXJhDuVwJfUXtKJMx7		
IP	INCOGNITO	BROWSER
146.241.144.46	No	Firefox on Linux



YOUR ID		
PruXJhDuVwJfUXtKJMx7		
IP	INCOGNITO	BROWSER
109.54.221.114	Yes	Firefox on Linux

Why it is used: the constructive way

- combat fraud or credential hijacking



From comunicazioni@intesasanpaolo.com

To Me

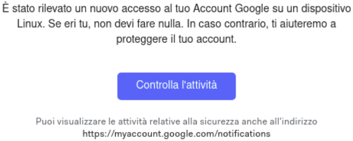
Subject **Intesa Sanpaolo: accesso da un nuovo dispositivo**

10/12/23, 12:48

Gentile Cliente,
ti informiamo che in data 12.10.2023 alle ore 12:48 è stato eseguito un accesso al sito Intesa Sanpaolo da un browser non utilizzato ultimamente.
Non sei stato tu?
Contatta la Filiale Digitale al numero 800.303.303.
Sei all'estero? Chiama il +390118019200.

Cordiali saluti
Intesa Sanpaolo

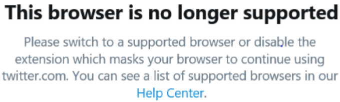
Questo messaggio è stato inviato da un indirizzo email di sola notifica ti preghiamo di non rispondere.



È stato rilevato un nuovo accesso al tuo Account Google su un dispositivo Linux. Se eri tu, non devi fare nulla. In caso contrario, ti aiuteremo a proteggere il tuo account.

Puoi visualizzare le attività relative alla sicurezza anche all'indirizzo https://myaccount.google.com/notifications

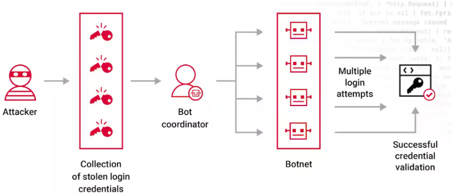
- suggest updates



This browser is no longer supported

Please switch to a supported browser or disable the extension which masks your browser to continue using twitter.com. You can see a list of supported browsers in our Help Center.

- bot detection



Attacker
Collection of stolen login credentials
Bot coordinator
Botnet
Multiple login attempts
Successful credential validation

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:

- **Advertising:** data collected allows advertising businesses to create a custom profile for targeted advertising
  - higher revenue for the company
  - user satisfaction (sometimes)

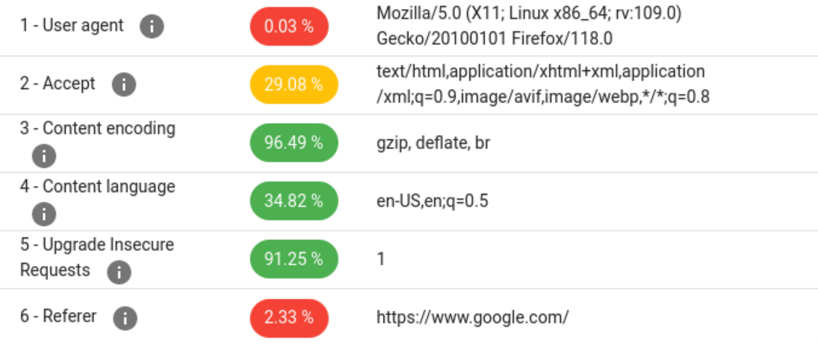
- **Dynamic content and pricing:** adapt content and prices due to users habits, status and location

Why it is used: the destructive way

Deliver exploits that are tailored for a specific user configuration:

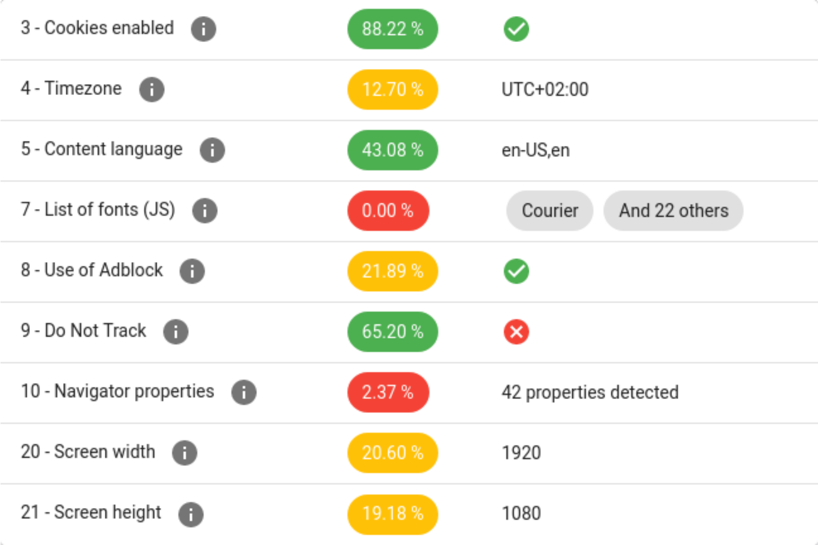
1. find a website vulnerability
2. use this vulnerability to inject a tracking script
3. collect user information
4. define an exploit for the user
5. send the exploit to the user the next time he visits the website

How data is collected: HTTP request



1 - User agent	0.03 %	Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/118.0
2 - Accept	29.08 %	text/html,application/xhtml+xml,application /xml;q=0.9,image/avif,image/webp,*/*;q=0.8
3 - Content encoding	96.49 %	gzip, deflate, br
4 - Content language	34.82 %	en-US,en;q=0.5
5 - Upgrade Insecure Requests	91.25 %	1
6 - Referer	2.33 %	https://www.google.com/

How data is collected: JavaScript attributes



3 - Cookies enabled	88.22 %	✓
4 - Timezone	12.70 %	UTC+02:00
5 - Content language	43.08 %	en-US,en
7 - List of fonts (JS)	0.00 %	Courier And 22 others
8 - Use of Adblock	21.89 %	✓
9 - Do Not Track	65.20 %	✗
10 - Navigator properties	2.37 %	42 properties detected
20 - Screen width	20.60 %	1920
21 - Screen height	19.18 %	1080

How data is collected: Canvas fingerprinting

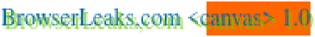
The way an image or text is rendered on a canvas can vary based on the browser, OS, GPU, font rendering settings and anti-aliasing algorithms, resulting in a unique image

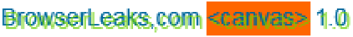
Steps to generate a fingerprint from the canvas:

1. get the image base64-encoded using `.toDataURL()`
2. compute a hash of the string

How data is collected: Canvas fingerprinting example

```
// text with lowercase/uppercase/punctuation symbols
var txt = "BrowserLeaks,com <canvas> 1.0";
ctx.textBaseline = "top";
// the most common type
ctx.font = "14px 'Arial'";
ctx.textBaseline = "alphabetic";
ctx.fillStyle = "#f60";
ctx.fillRect(125,1,62,20);
// color mixing to increase the difference in rendering
ctx.fillStyle = "#069";
ctx.fillText(txt, 2, 15);
ctx.fillStyle = "rgba(102, 204, 0, 0.7)";
ctx.fillText(txt, 4, 17);
```

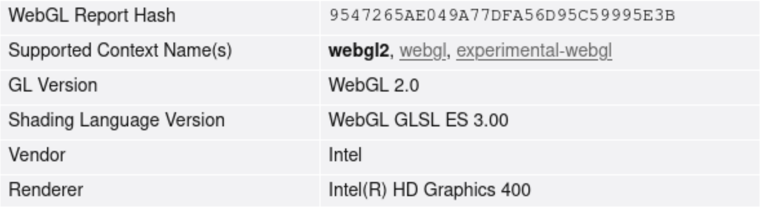




How data is collected: WebGL fingerprinting

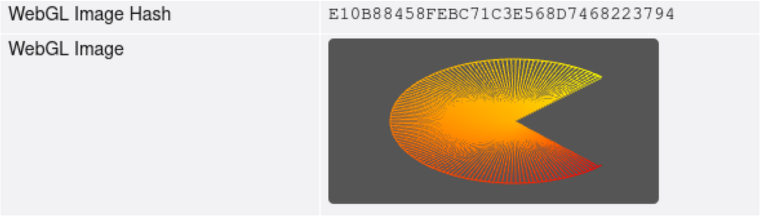
WebGL is a JavaScript API used to render 3D graphics within a web browser by utilizing the device's GPU:

- WebGL report:



WebGL Report Hash	9547265AE049A77DFA56D95C59995E3B
Supported Context Name(s)	**webgl2**, webgl, experimental-webgl
GL Version	WebGL 2.0
Shading Language Version	WebGL GLSL ES 3.00
Vendor	Intel
Renderer	Intel(R) HD Graphics 400

- WebGL image:



WebGL Image Hash	E10B88458FEBC71C3E568D7468223794
WebGL Image	

What about privacy: GDPR and ePrivacy Directive

Whether collecting personal data using browser fingerprinting companies must comply with the requirements of GDPR and ePrivacy Directive:

- the data collection process must be transparent to users
- companies must ask for consent when personal data is involved

Nevertheless companies rely on specialized companies in this field and their fingerprinting methods are hard to detect or avoid

Conclusions: prevention and mitigation

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

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

Any questions?