PRIVACY Affairs

Menu

A Complete Guide to Browser Fingerprinting – What It Is and How It Affects You

By **Shanika W.** . 8 August 2022
Cybersecurity Analyst

Miklos Zoltan
Fact-Checked this

In this guide we will discuss what browser fingerprinting is and how it can affect your online privacy, as well as how you can avoid it.

This article will address the following questions:

- What is browser fingerprinting
- How browser fingerprinting works
- Browser fingerprinting techniques
- What are the purposes of browser fingerprinting
- How to test your browser fingerprinting
- How to prevent browser fingerprinting

Quick Summary

Browser fingerprinting generates a unique fingerprint of users enabling websites to track them among millions of others.

The most dangerous part of fingerprinting is websites' ability to collect extensive information to generate a unique browser fingerprint for every user.

The major techniques used for this purpose are Javascript and Flash and Canvas, WebGL, Media devices, and Audio fingerprinting.

Even though browser fingerprinting's main purpose is targeted advertising, you can use them for better fraud detection and botnet identification.

Several websites provide consumers the facility to check what kind of information websites can track about them.

As always, prevention is better than the cure; there are several ways you prevent websites from acquiring information to create your browser fingerprint.

Chapters

What is Browser Fingerprinting?

A fingerprint is unique to every person, and so is the browser fingerprint, a unique profile websites use to identify and track you among many users.

Browser fingerprinting, also referred to as device fingerprinting or online fingerprinting is an online tracking technology initially used for security purposes. Still, now it has become more privacy-invasive than browser cookies.

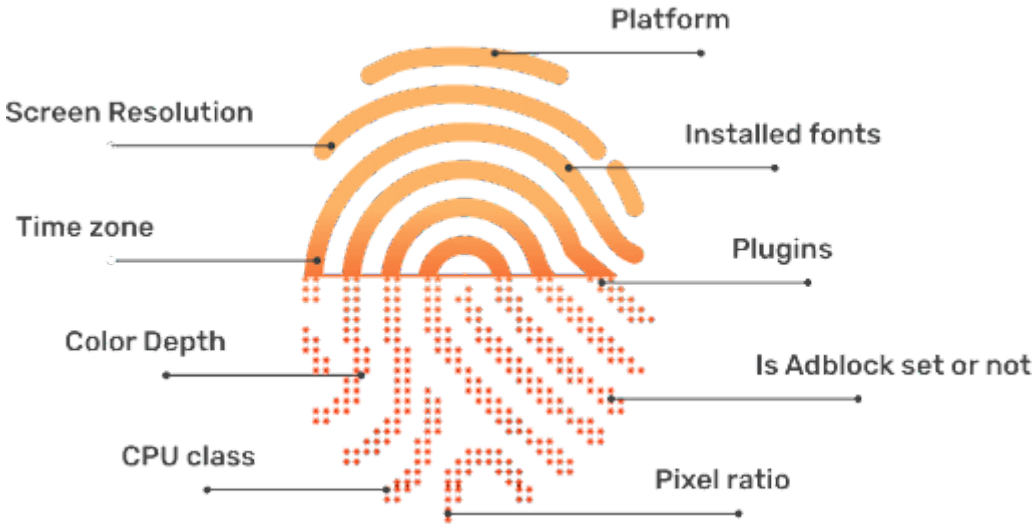
Websites create this digital fingerprint by collecting your device's different hardware and software settings. In that case,d browser settings.

For example, operating system, user agent, number of CPU cores, supported languages, your time zone, whether you have enabled cookies, screen resolution, plugins, use of an ad blocker, fonts, and many more.

These data make a unique digital fingerprint that browsers can identify you among millions of users, and its accuracy lies between 90 to 99%.

Unlike cookies, this technique does not store any information regarding the fingerprint in the users' device, making it stateless. The more unique these data become, the easier websites to create this fingerprint.

The fingerprint creation is usually done by a script that works silently in the background without your knowledge and consent. Browser fingerprinting makes you trackable for longer, even if your device, software, or browser configuration changes. Research proves that long-term tracking is possible even if your data changes frequently.



How Browser Fingerprinting Works?

This is how browser fingerprinting works:

Browser fingerprinting techniques

Javascript and Flash

There are different ways websites collect information about your device. When you visit a website, they use scripts with javascript to gather information about your device to correctly display the content in your browser.

Thus, these scripts are mostly legitimate, and blocking them will not properly render the content. In addition, the Adobe Flash plugin installed in your browser can provide so much information like your operating system, time zone, screen resolution, etc.

The website generates a hash or a unique fingerprint from all this data.

Canvas fingerprinting

This technique exploits the HTML5 canvas element to secretly gather information about the user's graphic card, drivers, and GPU. When you visit a website that contains the canvas fingerprinting script, it forces the browser to draw an image or a text with a random font and size.

The rendering of that image is slightly different in every device since they have different graphics hardware, software, and drivers.

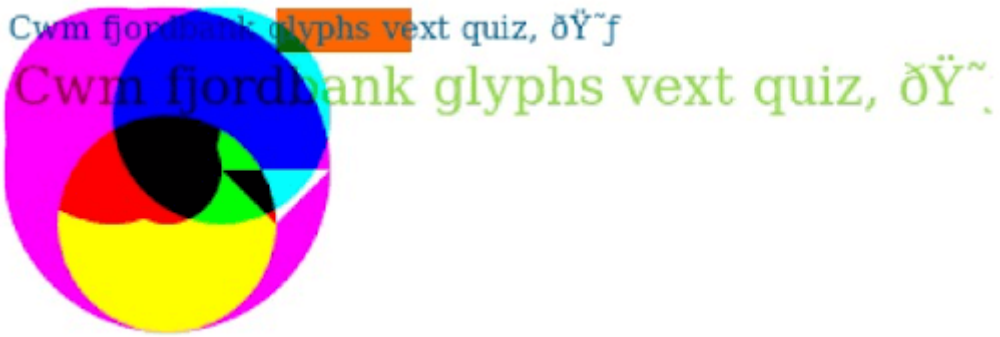
The fingerprinting script then identifies how your browser has rendered that image, and through that, it deduces detailed information about your device's graphics, GPU model, and other information.

Then the fingerprinting script converts the data into Base64 encoded format and computes the canvas fingerprint hash.

This technique is accurate and does not take too much time to process, making it one of the most widely used fingerprinting techniques.

WebGL Fingerprinting

WebGL fingerprinting works very similarly to Canvas fingerprinting, which forces the browser to render an image or text. Then it uses these images to retrieve information like device screen resolution, graphic cards, etc.



Media Device fingerprinting

Device fingerprinting uncovers information about all the media devices, especially their IDs on your device, which means that it can reveal both internal media components like audio and video cards and external media components like headphones, mikes, and external speakers.

But this technique is not widely used because the fingerprinting script requires user permission to access media devices like the camera and the microphone.

Audio Fingerprinting

This technique uses the same approach for fingerprinting that canvas printi utilizes. But rather than creating an image, this technique test how your dev plays sound.

The sound waves generated from the sound are different because of the variations in the browsers and the devices' audio configurations. Thus, this method can decipher the devices' information like sound hardware and software, CPU architecture, etc.

AudioContext Fingerprinting

AudioContext fingerprinting is comparatively a new technique identified by researchers at Princeton University, based on AudioContext API in modern browsers. It uses the characteristics of the audio signature of devices rather than the sound played on them.

Websites can identify variations in audio waveforms using this AudioContext API to extract a fingerprint, which is a property of machines' audio stack.

There is a test page from Princeton University to test the browser fingerprinting Using the AudioContext and Canvas API. You can see an image of the audio context fingerprint and the properties used to generate it.

The uses of Browser Fingerprinting

- **Targeted Advertising** – The main purpose of browser fingerprinting is tracking users secretly without the user's consent. Several industries, from advertising to fraud detection companies, take these fingerprints to understand customer behavior. Online advertisers and marketing industries use them to serve personalized advertising.
- **Dynamic Pricing** – Fingerprints also help to achieve dynamic pricing. For example, suppose you visited another country with a different price for your favorite product, based on the location settings given by the browser fingerprinting data. In that case, advertisers can adjust the prices accordingly.
- **Identifying Potential Fraudsters** – Banks can probe into the suspicious online behavior of their accounts; for example, when the user accesses the account through multiple locations within a short period, they can use this

unique fingerprint to identify if this is the usual user that accesses the account. So, they can identify and flag any hacker trying to gain access to the account from a machine with a different configuration.

- **Botnet Identification** – Moreover, Browser fingerprinting also helps identify botnets because botnets use different devices for establishing connections with the target machines. Redware Bot Manager is one such example bot manager that utilizes fingerprinting as one of its detection techniques.

How To Test Your Browser's Fingerprinting?

Several websites are dedicated to checking your browser fingerprinting with a score of how unique it is and a breakdown of what kind of information they track with the fingerprint. Lets' see from this section such browser fingerprinting checkers.

Am I Unique

This open-source website amiunique.org lets you discover how identifiable you are on the internet.

Their main purpose is to "study the diversity of browser fingerprints and provide developers with data to help them design good defenses." It implements both canvas and WebGL fingerprinting to provide users with many global statistics and browser characteristics.

Go to its homepage and click on the "View my browser fingerprint." link. It will then generate the fingerprint and provide the list of data used to create it.

You can also download this fingerprint and use its browser extension to let it keep tracking your fingerprint.

The website will collect your browser fingerprint and put a cookie on your browser for four months to help with their purpose.

Am I Unique allows users to download their browser fingerprint and featur
browser extension for Chrome that will keep track of your fingerprint over time.

Cover Your Tracks

Cover Your Tracks is a website by the Electronic Frontier Foundation that allows you to understand the uniqueness of your browser fingerprint.

It is a research project that investigates the tools and techniques of online trackers. Once you click on the 'Test your Browser link on its home page, it will generate the following information.

- If the browser blocks tracking adds
- If the browser blocks invisible trackers
- If you protect from fingerprinting

In addition to that, it provides detailed information on the different tracking properties. This information also helps EFF to evaluate the third-party trackers and identify protection methods.

Privacy.net

Privacy.net gives you an idea of what information websites, advertisements, or widgets find about yourself when you visit them. The website has several tests which evaluate your browser privacy in steps.

- Basic Info Test reveals the basic information like your IP address, location, browser, screen resolution, operating system, and even the machine is a desktop or laptop and how much battery power is left in it.
- The autofill test reveals if you have enabled that feature
- User Accounts tests reveal the user accounts you have logged into
- Browser capability test provides your browser features, capabilities, request parameters, and plugins
- Fingerprint analysis generates the unique fingerprint based on the canvas fingerprinting technique and lists out the information used to generate

Device Info

Device Info is a browser security and privacy testing and troubleshooting tool that lists all the information the websites can gather about your device.

The list is so long that you may wonder how much information can be gathered and provided to outside parties. Following are some of the interesting information it can reveal.

- Accounts logged in
- Battery status
- Bluetooth
- Browser plugins
- Country
- CPU
- No of Webcams
- Memory (RAM)
- ISP
- Graphics Card Name
- If Canvas Fingerprinting Supported
- Microphones
- Mouse Position
- What is the last key pressed

Hidester

Hidester, a VPN company, also provides a free tool to test browser fingerprints. You can first see if your browser is Adblock enabled or not, do not track enabled via HTTP or navigator and the browser fingerprint.

Additional information reveals how much time it took to calculate the fingerprint and the basic information about your device and the browser.

How To Prevent Browser Fingerprinting?

Now that you know how much information websites use for browser fingerprinting, you must be wondering if you can completely prevent it. Browser fingerprinting is quite a powerful method; thus, challenging to stop completely.

You can take certain security and privacy measures to control it, but there are some downsides. So, here are some steps you can take to avoid this.

Disable JavaScript

The more information available, the more accurate the browser fingerprint can identify you. JavaScript in browsers are key techniques that extract such information.

Disabling JavaScript means websites won't get key information to create the fingerprint, such as your plugins, system fonts, languages, etc.

Browsers will have only a few information such as User-Agent name, HTTP access headers, etc. Therefore, disabling javascript on your browser is an effective method of protecting yourself from fingerprinting.

But on the other hand, it hurts accessing some sites since most sites heavily depend on javascript, impacting your browsing experience.

Use a common browser

Using a common browser is a simple hack to make your fingerprint as less unique as possible to reduce tracking. Because using a common or popular browser means many users are using it, you are less likely to become a target.

For example, Chrome and Safari are the most used web browsers worldwide according to browser market share statistics by 2021, and Microsoft Windows is the most used operating system.

However, always use the latest version of the browser or the OS you intend to use because each OS and browser can have the latest security updates for battling device fingerprinting.

For example, the latest Mozilla browser can prevent fingerprinting by blocking any third-party requests by companies that have been identified as participating in fingerprinting.

Use TOR browser

If you're seriously concerned about preventing browser fingerprinting, using the TOR could be the best solution.

Because Tor has been designed to achieve maximum privacy for the user, it enters the Tor network when you connect to the internet with the Tor brow. It connects Tor nodes encrypting and privatizing your data.

This hides the source or destination IP addresses. It will further prevent browser fingerprinting by standardizing several browser characteristics.

When you use the Tor Browser with a VPN, it can further reduce the tracking ability. For example, you can select certain levels of security, which can disable javascript, restrict fonts options, disable HTML Canvas rendering, etc.

Some of the settings of Tor are identical for every user, which makes fingerprinting techniques generate unique browser fingerprints with the rest of the characteristics. However, using the Tor browser with a VPN may slow down your browsing speed.

Use of anti-fingerprinting browsers

Like the Tor Browser, anti-fingerprint browsers provide a lot of privacy than normal browsers, which block tracking by default. For example:

- Avast Private Browser can block online tracking and mask your digital fingerprint.
- Brave browser is an open-source browser based on Chromium that does not collect any information regarding your online activity. In addition, it automatically blocks trackers and makes the browser instances similar by adding or removing APIs and randomizing values.
- DuckDuckGo automatically blocks ads, third-party trackers, and uses HTTPS encryption on its browser, making the browsing experience as private as possible. With its chrome extension, now you can use it with Chrome as well.

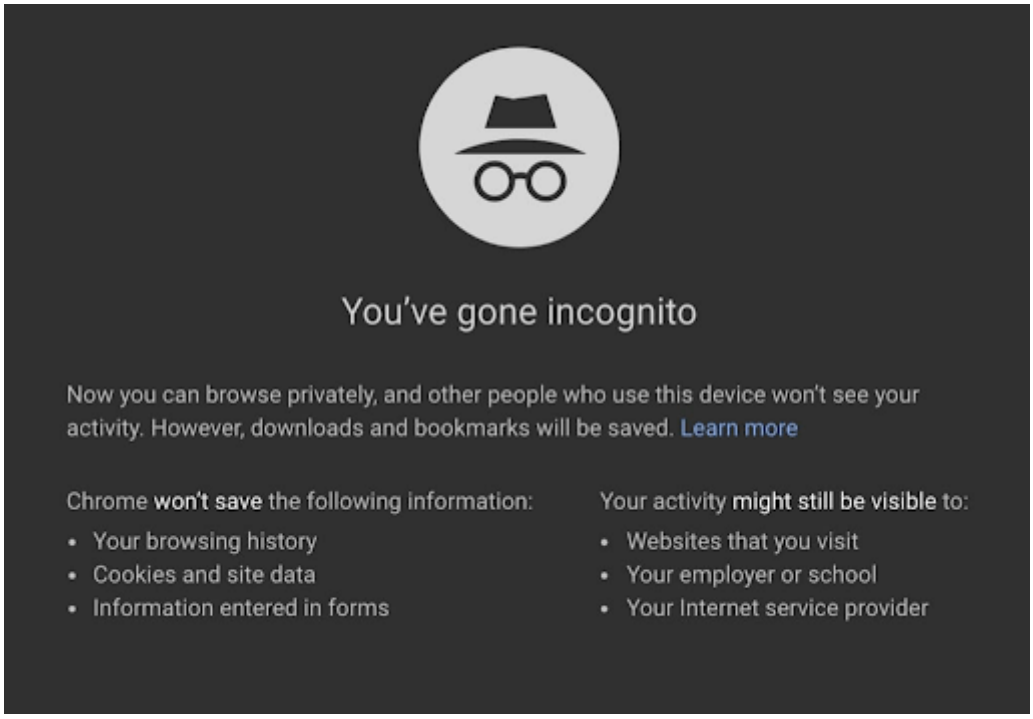
Use Incognito mode or private browsing

Using the Incognito or private browsing mode in browsers like Chrome, Edge, Safari, and Firefox is another simple way to reduce the chance of generating a unique fingerprint.

When you browse through incognito mode, it will not save your online activity like search history, passwords, and cookies. Once you close such a private

window, it will clear your browsing session.

It is impossible to stop websites from assembling your fingerprint using this mode completely. However, you can still reduce the data points websites can obtain for fingerprinting by going incognito or private browsing.



Use a VPN

Using a virtual private network (VPN) every time you surf the internet is another way to reduce the effects of browser fingerprinting. VPNs create an encrypted tunnel between your device and the VPN server hiding your IP address.

Because of this, a browser fingerprint won't use any information related to the device's IP address. It is good to use a popular VPN and use it with other prevention techniques.

However, this is not the best method to avoid fingerprinting because much other information than the IP address is still accessible.

Use anti-malware software

Anti-malware software provides an extra layer of protection for browser fingerprinting and the devices' overall security. This software can prevent harmful scripts, ads, malware, or spyware directly linked to the browser's fingerprint.

They can scan the whole system and detect any downloaded files containing scripts.

Use security plugins

There are security plugins you can install which will prevent fingerprinting scripts or trackers. Plugins like Privacy Badger, Disconnect, AdBlock Plus, and NoScript can block any harmful ads spying on you and any third-party trackers.

Privacy Badger, for example, can learn automatically to block invisible trackers. Also, you can allow those security plugins to run scripts only on specific websites that may be essential to render smoothly.

Summary

Browser fingerprinting has become one of the threats to online privacy. Not only do websites collect usual information like your IP address, but browser fingerprinting uses a lot of data points to create your unique browser fingerprint.

With technological advancements, we will see more accurate methods evolve for browser fingerprinting, which means that it will be difficult to get away from it completely.

Thus, we recommend smartly using a combination of safe browsing methods discussed in this article to tighten your privacy and stop being a target of browser fingerprinting.

Frequently Asked Questions

Some people found answers to these questions helpful

Is browser fingerprinting similar to cookie-based tracking?

No. Cookies and browser fingerprinting are completely different. Cookies ge… stored on the users' devices, and users can delete them or expire. But browser

fingerprints do not remain on the user's devices. Moreover, fingerprints can update with the changes to the user devices and browsers. Thus, they are more reliable and stay longer than cookies.

Is browser fingerprinting legal?

Yes, it is legal in many areas of the world. For example, even though the General Data Protection Regulation (GDPR) of the European Union has regulations over cookie-based tracking, browser fingerprinting-related laws have not yet been in effect.

What is cross-browser fingerprinting?

A research paper (Cross-)Browser Fingerprinting based on OS and Hardware Level Features reveals browser fingerprinting works across multiple browsers with more accuracy than single-browser fingerprinting. Earlier, browser fingerprinting was limited to individual web browsers. It means If you switch to another browser regularly, your fingerprint cannot use with other browsers.

How can you block fingerprinting in Firefox?

Firefox has a new fingerprint blocker which you can enable in a few steps. Open Firefox and click on the settings and then Privacy & Security tab. Select the standard browser privacy option on the resulting page, which automatically blocks fingerprints.

Is browser fingerprinting reliable?

Studies have found that browser fingerprinting is a very accurate way of identifying unique users. For example, in a study that collected 3,615 fingerprints over three months, browser fingerprinting had a 99.2 percent success rate.

Trending

How to

How to Block Ads On All Your Devices With pfSense, Squid & SquidGuard

9 June 2022

How to

How to Set Up IP Filtering and DNS Blackholing on pfSense Using pfBlockerNG

10 June 2022

Privacy

A Complete Guide To Google FLoC - What it Does and How it Works

9 July 2022

Shanika Wickramasinghe is a software engineer by profession. She works for WSO2, one of the leading open-source software companies in the world. One of the biggest projects she has worked on is building the WSO2 identity server which has helped her gain insight on security issues. She is keen to share her knowledge and considers writing as the best medium to do so. Cybersecurity is one of her favorite topics to write about.

Being a graduate in Information Technology, she has gained expertise in Cybersecurity, Python, and Web Development. She is passionate about everything she does, but apart from her busy schedule she always finds time to travel and enjoy nature.

Shanika W. Connect with the author: in

Leave a Comment

Write Your Comments...

Name

Email

Website

Save my name and email in this browser for the next time I comment.

Leave a Comment

About Us

Terms & Conditions

Privacy Policy

Cookie Policy

Earnings Disclaimer

Contact

PRIVACY Affairs

Twitter