



Romel Cabiling ▾



Home

Home > My courses > Network Attacks: Detection, Analysis & Counter... > 11 Browser Fingerprinting > Lesson Proper for Week 11

Lesson Proper for Week 11

BROWSER FINGERPRINTING

A **device fingerprint**, **machine fingerprint**, or **browser fingerprint** is information collected about a remote computing device for the purpose of identification.

That means that, when you connect to the internet on your laptop or smartphone, your device will hand over a bunch of specific data to the receiving server about the websites you visit.

Browser fingerprinting is a powerful method that websites use to collect information about your browser type and version, as well as your operating system, active plugins, time zone, language, screen resolution, and various other active settings.

Websites use the information provided by browsers to identify unique users and track their online behaviour. This process is therefore called “**browser fingerprinting.**”



The uniqueness of browser information is closely related to the investigation method of the police and forensic teams, who identify suspects and criminals based on fingerprints at the crime scene.

Browser fingerprinting works like that as well. Websites bulk-collect a large set of data of visitors in order to later use it to match against browser fingerprints of known users.

The data collected in browser fingerprinting includes;

1. Device model
2. Operating system (OS)
3. Screen resolution
4. Time zones
5. File format identifiers
6. Timestamp
7. User-agent (UA) string
8. Language settings
9. Plugins
10. Extensions

The pros of device fingerprinting are that it helps to prevent online fraud. For instance, it can help to identify whether the Web banking session has been intercepted.

What is more, the technique allows to track fraudsters who steal login and payment card numbers. Proceeding transactions, they face the repeating process of employing trial and error methods. Fraudsters are just not able to change devices so often and can be tracked.

CONS: DATA PRIVACY CONCERNS

Browser fingerprinting violates current privacy regulations as this way the users are not aware of the amount of their data transferred and who is getting hold of it. Users cannot simply clear their fingerprints like cookies, which poses concern even among the most privacy-conscious users.

PREVENTING DEVICE FINGERPRINT: RECOMMENDATIONS FOR USERS

Preventing device fingerprinting is not insurmountable. Besides, it is a very significant action to ensure safety while surfing the Internet. There are specific solutions, which make your personal web browsing information and your identity harder to trace.

a. Choosing the most popular browser: It's essential to download the latest version of your browser. Browsers are trying to keep their security solid and include improvements in each update, reducing the chances of becoming the target of device fingerprinting.

The latest version of the Mozilla Firefox browser claims to protect you against fingerprinting of devices. The browser blocks third-party requests to companies, which were caught red-handed in using device fingerprinting. Apple and Google also announced that they would restrict browser fingerprinting. Apple is going to hide the data, which can be fingerprinted, while Google made a draft of a "privacy budget" to limit the amount of data to fingerprint from the device by a certain company.

b. Private mode and incognito browsing: Another method to reduce device fingerprinting is to choose a private mode. This action doesn't stop the device fingerprinting completely, but it limits the general amount of data that is accessible to fingerprint.

In addition, we recommend the Tor browser for Incognito browsing, which is highly safe and confidential. Tor browser has anti-fingerprinting features, it aims to make all users unidentified, and reducing the possibility for you to be fingerprinted based on your browser and device information. The browser has the technology, which restricts the identification of your IP address. It hides your personal information, whether it's the language you prefer or the time zone you live in.

c. Flash and Java-script disablement: Device fingerprinting applications mostly operate on Java-script or Flash. The great news is that browsers block it themselves, so in some way, it shouldn't bother you. You can check if your browser is still operating with any of them and disable or completely uninstall all of the features.

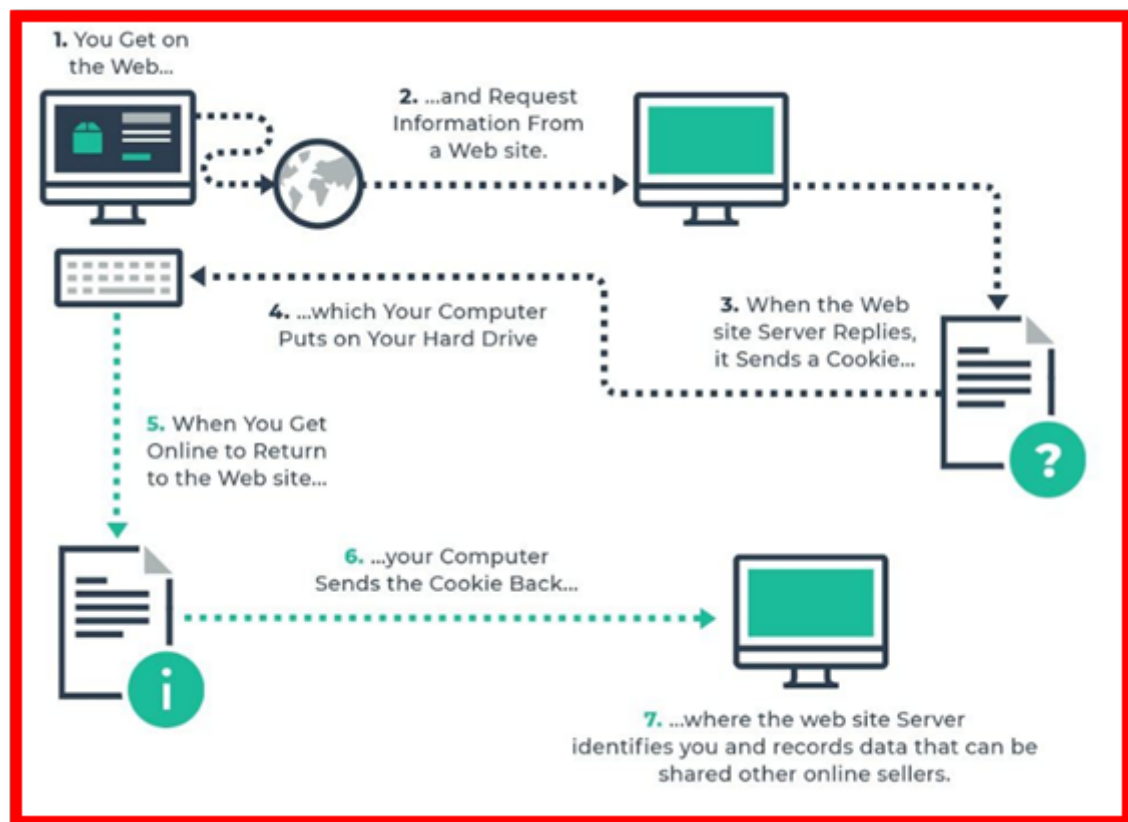
d. VPN use: A virtual private network or shortened VPN increases your safety, privacy, and security. It routes your traffic by third-party servers masking your actual location. You seem like you're using the Internet in some other place, country, or even continent. VPN creates a virtual IP address and efficiently masks user's information. Therefore, a device fingerprint will include a fake IP address.

METHODS USED FOR (FINGERPRINT) TRACKING

1. Cookies & Tracking

Websites remember and track individual computers and devices by loading the cookies (small data packets) onto your computer.

Every time you visit a website, your browser will download cookies. When you visit the same website at a later time, the website will assess the packets of data and provide you with a personally customized user experience.



2. Canvas Fingerprinting

A type of "browser fingerprinting" techniques of tracking online users that allow websites to uniquely identify and track visitors using HTML5 canvas element instead of browser cookies or other similar means.

Canvas fingerprinting works by exploiting the HTML5 canvas element: when a user visits a website their browser is instructed to “draw” a hidden line of text or 3D graphic that is then rendered into a single digital symbol, a potentially unique identifier to track users without any actual identifier persistence on the machine.

For the record, canvas fingerprinting focuses on the graphics aspects only. The data it relies on includes:

- o Operating system
- o Browser
- o Graphics card
- o Graphics card driver
- o Installed client fonts

USES OF CANVAS FINGERPRINTING

1. Preventing Abuse

A key reason is to prevent abuse. Identifying computers associated with spam or malicious activity makes it harder for them to cause problems. You can block potential bad actors or limit their access to your site.

2. Secure User Accounts

You can also use fingerprints to identify legitimate users. If a user’s fingerprint is identical, or at least similar from session to session, you can be reasonably confident the user is legitimate. If you detect a change, you can take steps to verify their identity. This could take the form of an email confirmation, a captcha, or contacting them via a device if two-factor authentication is available.

You can also detect people accessing your site repeatedly to make sure paywall and rate limits are respected. Gaming or e-commerce sites can use fingerprints to help confirm users are who they say they are.

3. Site Personalization

Like cookies, fingerprints can be used to identify users and give them content that their previous behaviour suggests they will like. This could mean showing them ads for products or services they have expressed an interest in before.

BENEFITS OF CANVAS FINGERPRINTING

1. Content Personalization. Marketers understand just how important personalization is. That's why all the big content hubs such as Netflix, Spotify, and even ecommerce sites rely on web tracking methods such as canvas fingerprinting. Content personalization translates to a better user experience for surfers and more revenue for

brands.

2. Targeted Ads. A good example is when advertising computers for gaming and gaming hardware. Advertisers have a list of users who have previously visited similar listings, so they target the ads to them.

3. Online Fraud Prevention. With canvas fingerprinting, for example, fintech can detect when an online banking session is a threat. As you may be aware, the devices you normally use to log in to e-Wallets and other online banking platforms have a specific footprint. Any log-in via a device with a new footprint indicates that the account may be under attack.

◀ Preliminary Activity for Week 11

Jump to...



Analysis, Application, and Exploration for Week 11 ▶



Navigation

Home



Dashboard

Site pages

My courses

Capstone Project 1

Network Attacks: Detection, Analysis & Counter...

Participants

General

06 - Preliminary Examination

10 Internet Cookies

11 Browser Fingerprinting



Preliminary Activity for Week 11



Lesson Proper for Week 11



Analysis, Application, and Exploration for Week 11



Generalization for Week 11



Evaluation for Week 11



Assignment for Week 11

Ojt/Practicum 1

Social And Professional Issues

System Integration And Architecture 2

Courses





Fair Warning

NOTICE: Please be reminded that it has come to the attention of the Publishing Team of eLearning Commons that learning materials published and intended for ***free use only by students and faculty members within the eLearning Commons network were UNLAWFULLY uploaded in other sites without due and proper permission.***

PROSECUTION: Under Philippine law (Republic Act No. 8293), copyright infringement is punishable by the following: Imprisonment of between 1 to 3 years and a fine of between 50,000 to 150,000 pesos for the first offense. Imprisonment of 3 years and 1 day to six years plus a fine of between 150,000 to 500,000 pesos for the second offense.

COURSE OF ACTION: Whoever has maliciously uploaded these concerned materials are hereby given an ultimatum to take it down within 24-hours. Beyond the 24-hour grace period, our Legal Department shall initiate the proceedings in coordination with the National Bureau of Investigation for IP Address tracking, account owner identification, and filing of cases for prosecution.

Activities

-  Assignments
-  Forums
-  Quizzes
-  Resources