LANQUETIN Alexis
GONZALEZ Jules
INFO5
06/12/2021

Web Browser Fingerprint

- VT -

Résumé

Mots clefs : Web, Anonymat, Sécurité informatique

Les WebBrowser Fingerprint sont un moyen d'identifier les utilisateurs sur internet à l'aide des données "laissées par le navigateur et device", au lieu des données de l'utilisateur en questions. Cette approche a plusieurs avantages, notamment celui de ne rien stocker sur le PC, d'utiliser des informations sur le device et non l'utilisateur (aucune lois sur la vie privées ne peut-être violée) et il est difficile voir impossible de supprimer/masquer ces informations, contrairement aux moyens tels que les cookies, qui peuvent être bloquer ou supprimer.

I - What is it ?

Le Web Browser Fingerprinting est une méthode utilisée par les sites web afin d'identifier les utilisateurs à travers leur navigateur et leur device. D'après une étude de l'Electronic Frontier Fundation menée sur 3 mois consistant à tenter de reconnaître les utilisateurs d'un site web en utilisant leur Fingerprint, cette technique d'identification serait fiable à 99%. Les Fingerprints se basent sur le contenu des requêtes HTTP, la configuration du navigateur, la configuration machine ainsi que l'adresse IP de l'utilisateur.

Cookies & Tracking

Les cookies sont actuellement la méthode d'identification la plus prisée pour l'identification sur les sites web, ils sont utilisés pour récolter des données personnelles et faciliter le ciblage pour les publicitaires, mais avec les controverses concernant le respect des données privé auxquelles ils font fasse, le besoin d'un nouveau moyen d'identification est né.

Les Fingerprints, contrairement aux cookies, ne permettent pas d'accéder à des données personnelles de l'utilisateur mais seulement à des données matérielles et logiciels. À l'inverse des cookies, elles ne sont pas stockées sur l'appareil. Enfin, contrairement à ces derniers, les fingerprints ne peuvent pas être bloquées, mais nous évoquerons des méthodes pour les limiter dans la partie IV.

II - How does it work ?

Passif Fingerprinting

Le Fingerprinting passif utilise les entêtes des requêtes HTTP pour récolter des informations sur l'appareil de l'utilisateur. Les données accessibles dans ces entêtes sont initialement utilisées par les sites web pour fournir des pages lisibles, elles contiennent notamment le système d'exploitation, le format d'encoding supporté, l'adresse IP de la machine. Cette technique pour accéder aux données est difficilement contrôlable, puisque ces données sont nécessaires aux requêtes HTTP pour un bon fonctionnement

Actif Fingerprinting

Plusieurs techniques permettent d'accéder à d'autres données de l'appareil de manière active.

Une de ces techniques consiste à utiliser les Canvas, un élément de Javascript conçu pour avoir un comportement dynamique. L'utilisation des Canvas laisse une trace contenant notamment des informations sur les paramètres graphiques de l'utilisateur, qui peuvent être utilisées dans la création de Fingerprints.

Des scripts JavaScripts peuvent être utilisés également pour vérifier la présence d'extensions et de plugins sur le navigateur, les formats de fichier supportés, la timezone de l'utilisateur…

Les sites web peuvent également accéder aux paramètres du navigateur, comme les autorisations sur les cookies ou l'activation du mode DoNotTrack. Il peuvent de plus vérifier quels périphériques (microphone,speaker, webcam, …) et capteurs (utilisés pour les appareils mobiles) sont connectés à l'appareil.

Une dernière méthode consiste à lancer des médias audios et, à l'instar des Canvas, regarder la trace laissée par la lecture de ces derniers pour extraire des paramètres audios de l'utilisateur.

Les données récoltable par le fingerprinting actif peuvent être limitées, mais cette limitation est souvent accompagnée d'une baisse d'utilisabilité, que nous détaillerons dans la partie IV.

III - Cas d'utilisations

Les WebBrowser fingerprint ont une seule utilisation : traquer et identifier des utilisateurs lorsque ceux-ci parcourent internet. Il y a cependant quatre raisons principales de vouloir utiliser ce traçage et de surveiller l'activité sur internet.

La première est une utilisation dans un but commercial et publicitaire. En effet, c'est un moyen de récolter des informations différentes et précise que celles déjà stockées dans les cookies (qui peuvent être désactivées par l'utilisateur). Ainsi, tracer les utilisateurs et récolter leur données est très intéressant pour les annonceurs car cela leur permet de créer des profils personnalisés plus précis. Et plus les données sur l'utilisateur sont précises, et plus précises

seront les annonces, et par conséquent les revenus de l'entreprise.

La seconde raison à un but sécuritaire. En effet, certains site web utilisent les web browser fingerprints pour détecter une potentiel fraude ou usurpation d'identité. Cela est aussi utile pour identifier les botnets, puisque les botnets vont établir une connexion via des devices différents à chaque fois.

La troisième raison est un but statistique. En effet, cela permet d'avoir des statistiques de fréquence de visite pour les sites (savoir si un utilisateur "anonyme" revient ou non…)

Et pour finir, ces fingers prints peuvent aussi être utiliser par les agences de surveillances gouvernemental ou non, car puisqu'il est impossible de ne pas avoir de fingerprint (bien qu'il soit possible de diminuer son unicité) il est possible de tracer des personnes qui utilisent d'autre moyens pour renforcer leur intimité (VPN, TOR network…).

IV - Protection

Contrairement aux cookies que l'on peut désactiver, aux scripts que l'on peut bloquer, aux adresses IP que l'on peut changer, il est impossible de se protéger entièrement des Web Browser fingerprint. Cela vient du fait qu'une fingerprint est calculée à partir de la configurations du navigateur et PC, et donc l'utilisation d'un plugin spécial pour bloquer un contenu laisse une trace de son fonctionnement. On peut y voir un paradoxe dans le sens où un utilisateur extrêmement protégé, avec une configuration optimale, le rend unique. Aux yeux de internet, cet utilisateur bien protégé apparaît comme un utilisateur "anormalement protégé", ce qui le rend paradoxalement unique. Cependant, il est possible de limiter l'unicité de sa fingerprint. En effet, l'idée va être de bloquer assez d'informations pour que la votre fingerprint soient trop pauvre en informations et donc assez commune pour ne pas arriver à vous identifier clairement.

Pour se protéger de ce traçage, il faut mettre en place différents moyens. A garder à l'esprit que l'anonymat est question d'équilibre. En effet, la majorité des sites ont besoin d'informations, de scripts, de fonctionnalités pour fonctionner efficacement. Bloquer ces éléments en vue d'intimité peut dégrader la navigation et l'utilisation d'internet. C'est donc un équilibre entre l'utilisabilité (l'expérience utilisateur du web) et d'anonymat.

A ce jour, voici les différents moyens pour se protéger des fingerprints :

- Utiliser la navigation privée : En effet, celle-ci a pour but de créer un profil utilisateur "standard" sans stocker d'informations sur le PC. Il est important de noter que toutes les navigations privées ne fonctionnent pas de la même manière, et la plupart se contentent juste de ne rien garder en historique, ce qui n'offre aucunes protections.
- Utiliser des bloqueurs de trackers : Ce sont des plugins (AdBlock, Disconnect..) qui s'ajoutent au navigateur afin de bloquer des scripts qui se lancent automatiquement afin de récolter des informations sur vous.
- Désactiver les scripts JavaScript et Flash : Ceux-ci offrent de nombreuses fonctionnalités aux sites, mais permettent de faire tourner de tracker (script).
- Utiliser des navigateurs résistants aux fingerprints (Tor, Brave) : Ces navigateurs ont mis l'accent sur l'anonymat, en utilisant un configuration par défaut, des plugins puissant et tous autres mécanismes pour assurer l'anonymat. Brave va générer des informations et données aléatoires.
- Utiliser un VPN : Un VPN permet de masquer son adresse IP et sa localisation en passant par un serveur sécurisé pour accéder à internet.
- Utiliser une virtual machine (VM) différentes à chaque fois : C'est peut-être une des méthodes les plus efficaces contre les fingerprints, puisque l'idée est de changer l'environnement de navigations a chaque fois, et donc les informations du système, et donc sa fingerprint.

Conclusion

Les WebBrowser Fingerprint sont un moyen d'identifier les utilisateurs efficacement sur internet. Le fait qu'elles utilisent les données du device et non les données de l'utilisateurs est très interessantes car rien n'est stockée sur le PC, aucune loi sur la vie privée ne peut-être violées, et il est difficile voir impossible de supprimer/masquer ces informations, contrairement aux moyens tels que les cookies, qui peuvent être bloquer ou supprimer.
Il est cependant possible de diminuer son efficacité en bloquant l'accès à certaines informations, et en mettant en place différentes techniques vues précédemment. Mais l'anonymat reste un équilibre entre l'utilisabilité et la sécurité : il faut connaître son combat et savoir ce que l'on veut.

Sources

https://restoreprivacy.com/browser-fingerprinting/
https://fr.wikipedia.org/wiki/Empreinte_digitale_d%27appareil
https://pixelprivacy.com/resources/browser-fingerprinting/
https://coveryourtracks.eff.org/learn
https://amiunique.org/fp
https://coveryourtracks.eff.org/
https://www.deviceinfo.me/
https://uniquemachine.org/