

Comparison of the Effectiveness of Countermeasures Against Tracking User Browser Fingerprints

Alexander A. Salomatin*, Andrey Yu. Iskhakov**, Roman V. Meshcheryakov***

V.A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russia (e-mail: karateka30@mail.ru, iskhakovandrey@gmail.com**, mrv@ieee.org***)*

Abstract: The current paper examines the impact of countermeasures against tracking user browser fingerprints on user uniqueness. The measures investigated are changing browsers and installing special plugins that allow blocking access to browser attributes or replacing their values with random ones. Browser fingerprints are obtained using a tool written in the JavaScript programming language with the "fingerprint3.js" library connected. The experiment is conducted, as a result of which, the conclusion is made about the variability of the user's browser fingerprints and the degree of effectiveness of the proposed measures to counteract the tracking of browser fingerprints.

Copyright © 2022 The Authors. This is an open access article under the CC BY-NC-ND license (<https://creativecommons.org/licenses/by-nc-nd/4.0/>)

Keywords: Cybersecurity, information security, browser fingerprint, identification, browser attributes

1. INTRODUCTION

Nowadays the problem of cybersecurity is attracting more and more attention. A high level of information security is becoming necessary not only for ordinary people - users of Internet networks, but also for critical government infrastructures. For the latter, there are privacy risks, since most web servers collect information about the users who interact with them. Thus, despite the seeming advantage of ensuring the security of the web server itself, the security of users is threatened (Parfenov D., Torchin V., Zabrodina L., Parfenov A. (2019), Strukov A., Vetlugin K. (2017)).

The main actual form in which the collected information about users is stored is a digital footprint - a set of data on static and dynamic behavioral traits of the user in the network (Agafonov. U.M. (2018), Feher K. (2021), Iskhakov A. (2014), Iskhakova A., Iskhakov A., Meshcheryakov R., Bendrau R., Melekova O. (2018), Tsvirkun A., Platonov T., Malkina N. (2019)). Calculating a digital footprint does not always take a long time. This is the case when the digital footprint is represented by a browser fingerprint that contains data about the user's browser attributes (Nair K., RoseLalson E. (2018), Laperdrix P., Rudametkin W., Baudry B. (2016), Ivanov A., Zhukov V., Maslova O. (2014)).

Browser fingerprinting takes place in two steps (Bujlow T., Carela-Español V., Solé-Pareta J., Barlet-Ros P. (2017), Luangmaneerote S., Zaluska E., Carr L. (2017), Iskhakov A., Salomatin A. (2020)). The first step is to retrieve user trait data through various channels (e.g., using JavaScript or plugins). The second stage is combining all the trait values into a single string and then calculating the identifier - the user's digital footprint. In this regard, countermeasures against tracking user browser fingerprints can be applied as early as the first stage.

These ways of dealing with browser fingerprint tracking themselves can be different (Choi S., Yun J., Kim S. (2018), ElBanna A., Abdelbaki N. (2018)). The easiest ones are changing the browser and changing its settings. More

complicated are the development and use of special software tools, including plugins, that allow you to block access to user data or reduce the uniqueness of the browser fingerprint by substituting values of browser attributes.

However, despite the available set of different measures to counteract browser fingerprinting, the development and search for the most effective approach remains open. The problem is complicated not so much by the number of measures, as by the fact that due to the scientific and technological progress new technologies appear, which entail the emergence of new values of browser attributes, as well as new ways of calculating them (Antonio E., Fajardo A., Medina R. (2020), Efremov E., Kovalevsky A., Ershova, Y. (2018)). Moreover, approaches being developed that calculate user browser fingerprints can take into account and even bypass countermeasures, which makes the problem even more difficult to solve (Jiang W., Wang X. (2020), Laperdrix P., Rudametkin W., Baudry B. (2015)).

The purpose of the study is to propose an actual effective way to counteract browser fingerprint tracking by providing greater uniqueness of the user identifier. To fulfill the purpose, a theoretical review of main modern countermeasures against tracking user browser fingerprints is performed and an experiment is conducted to show the workability of the measures and to compare them to determine the most effective ones.

The paper consists of three sections. The first section contains the theoretical part of the research. Groups of relevant measures are described, which make it difficult to obtain correct browser fingerprints identifying users. Examples of measures are given, as well as the principles of their work. The practical part of the study is located in the second and third sections. In order to better understand how the use of countermeasures affects the formation of the browser fingerprint, the article proposes to refer to an experiment in which the browser attributes will be calculated without the use of add-ons and together with them. The second section

describes in detail the experiment conducted and shows the results obtained. In the last section, the applied countermeasures against tracking user browser fingerprints are compared with each other in order to determine the most effective one.

2. AN OVERVIEW OF COUNTERMEASURES AGAINST BROWSER FINGERPRINTING

Countering the tracking of browser fingerprints makes it difficult to correctly identify the user, which can be useful in certain situations. In this case, the identifier, which is the element on the basis of which the user is recognized, becomes less important. In total, we can distinguish four main groups of measures aimed at preventing the calculation of correct browser fingerprints, identifying the user (ElBanna A., Abdelbaki N. (2018), Fiore U., Castiglione A., De Santis A., Palmieri F. (2014), Salomatin A.A. (2021)):

- Measures blocking access to obtaining user's browser attributes;

There are two main ways to block access to user data: disabling JavaScript and using the activated HTTP header Do Not Track (Fiore U., Castiglione A., De Santis A., Palmieri F. (2014)). As it is known, JavaScript is the main actual mechanism of user data retrieval and is used in almost every browser when visiting sites. In turn, Do Not Track header, although not a frequent measure, but the principle of its operation is simple, which provides ease of use. The header takes a numeric value that determines the user's tracking preferences and is sent along with the request message. The main disadvantage of measures belonging to the group is that blocking access to data can lead to loss of functionality of the site, and much of the information on the site may not be displayed at all.

- Measures to create identical browser attributes;

The idea behind these measures is that a user's browser fingerprint is less unique the more users have similar browser attributes. In such a situation, distinguishing two or more users from each other becomes more difficult, so user identification may not occur correctly. An example of a measure belonging to this group is the widespread use of the Tor browser by users. This browser specifies a limited set of many browser attributes, so there is little variability in the browser fingerprints of users in such a browser.

- Measures that reduce the uniqueness of the identifier without superstructures;

As an add-on is understood some third-party software (plugin) that allows you to influence the values of the user's browser attributes. If the plan is to reduce the uniqueness of the user ID, then as a simple but effective measure of this group is to expand the number of browsers used, the number of languages used, the number of devices, etc., or to reduce the number of values in those traits (browser attributes) that most users have the same.

- Measures to reduce the uniqueness of the identifier with add-ons.

The main principle of the measures is the formation of new values of browser attributes. The way values are generated is different for different plugins. Some plugins (for example, Privaricator) change browser attribute values by generating random values for significant attributes. In this case, the significant attributes are those browser attributes that are the most informative and describe the user better, more accurately than others. For example, canvas, font list, plugin list, WebGL. There are other add-ons that allow you to change the values of any other attributes, not just significant attributes. For example, RubberGlove. It allows you to find navigator and screen objects within a web page, and replace their values with null values. Thus, it is possible to change the values of such browser attributes as screen resolution, color depth, platform and some others.

The success of one method or another depends on many factors: the browsers used, the devices used, the sites visited, so to determine the effectiveness of the measures it is better to refer to an experiment. Given the large number of measures to counteract the tracking of user browser fingerprints, in the experiment it is planned to consider only some of the measures above.

3. EXPERIMENT ON THE USE OF COUNTERMEASURES AGAINST TRACKING USER BROWSER FINGERPRINTS

First, the original user's browser fingerprint is computed, then add-ons are applied and new browser fingerprints are computed.

To calculate the browser fingerprints of users, there are already ready-made resources (Laperdrix P., Rudametkin W., Baudry B. (2016)). On the one hand, it is possible to use specialized sites. On the other hand, creating your own server and your own methods can also be effective. This approach can be done with the "fingerprint3.js" library, which is actively updated, extending the functionality, fixing bugs and considering the actual necessary data to be retrieved. Moreover, this library is publicly available, so it can be used by anyone.

There are also other ways to calculate browser fingerprints that are in the public domain. For example, there are web sites like amunique.org, with which the users are provided with some basic information about their configuration and how trackable it is. However, the authors of the paper don't use these sites because the authors strive for their own program and their own conclusions about the increasing the effectiveness of countermeasures in the absence of information about the browser fingerprints of millions of users.

In the current study, the browser fingerprint consists of the browser attributes shown in Table 1.

Table 1. Browser user attributes calculated in the experiment

Attribute	Value
-----------	-------

Fonts	["Agency FB", "Arial Unicode MS", "Calibri", "Century", "Century Gothic", "Franklin Gothic", "Haettenschweiler", "Leelawadee", "Lucida Bright", "Lucida Sans", "MS Outlook", "MS Reference Specialty", "MS UI Gothic", "MT Extra", "Marlett", "Microsoft Uighur", "Monotype Corsiva", "Pristina", "Segoe UI Light"]
DomBl	false
FontPref	"default": 149.3125, "apple": 149.3125, "serif": 149.3125, "sans": 144.015625, "mono": 121.515625, "min": 9.34375, "system": 147.859375
Audio	124.04347527516074
ScreenFr	[0, 0, 40, 0]
OsCpu	false
Language	["ru-RU"]
ColorDep	24
DevMem	8
ScreenRes	[1920, 1080]
HardwareConcurrence	6
Timezone	Europe/Moscow
SessionStorage	true
LocalStorage	true
IndexedDB	true
OpenDatabase	true
CpuClass	false
Platform	"Win32"
Plugins	["PDF Viewer", "Chrome PDF Viewer", "Chromium PDF Viewer", "Microsoft Edge PDF Viewer", "WebKit built-in PDF"]
Canvas_Wind	true
Canvas_Geom	"data:image/png;base64,iVBORw0KGgoAAAAN..."
Canvas_Text	"data:image/png;base64,iVBORw0KGgoAAAAN..."
TouchSupport	"maxTouchPoints": 0, "touchEvent": false, "touchStart": false
Vendor	"Google Inc."
VendorFlavors	["chrome"]

CookiesEnabled	true
ColorGamut	"srgb"
InvertedColors	false
ForcedColors	false
Monochrome	0
Contrast	0
ReducedMotion	false
Hdr	false
Math	[1.4473588658278522, 709.889355822726, ..., 1.9275814160560204e-50]

Then the countermeasures against tracking browser fingerprints are applied. The choice of measures was based on their availability and customizability, and they should not be time-consuming. Each of the measures related to add-ons or browser changes allows you to change the values of browser attributes, so below, in addition to the list of measures themselves, is a brief description of the attributes whose values are changed.

- Canvas Blocker (Fingerprint Protect)

The values of Canvas_Geom, Canvas_Text change. The beginnings of the identificatory-strings are the same, but their values are different from the rest. The plugin itself generates their values randomly. This can be checked by running the test again and comparing the Canvas values with each other.

- DoNotTrack Header

Turning on the HTTP header in the Google Chrome browser does not change the values of the browser fingerprint attributes.

- CyDec Security Anti-FP

It changes the value for the list of received plugins. The new value is as follows: ["Chrome PDF Plugin", "Chrome PDF Viewer", "Native Client"]. Thus, some plugins are hidden, and new plugins are added.

- Changing the browser to a new standard one

The list of the changed values can be seen in Table 2.

Table 2. Changed values of browser attributes in new browser

Attribute	Value
Fonts	["Agency FB", "Arial Unicode MS", "Calibri", "Century", "Century Gothic", "Franklin Gothic", "HELV", "Haettenschweiler", "Leelawadee", "Lucida Bright", "Lucida Sans", "MS Outlook", "MS Reference Specialty", "MS UI Gothic", "MT Extra", "Marlett", "Microsoft Uighur",

	"Monotype Corsiva", "Pristina", "Segoe UI Light", "Small Fonts"]
FontPref	"default":149.35000610351562, "apple":149.35000610351562,"serif":149.35000610351562, "sans": 144.01666259765625, "mono": 136, "min": 9.366668701171875, "system": 147.89999389648438
Audio	35.7383295930922
OsCpu	Windows NT 10.0; Win64; x64
Language	[["ru-RU"], ["ru-RU", "ru", "en-US", "en"]]
DevMem	false
Plugins	false
Vendor	false
VendorFlavors	false
ColorGamut	false

New values for Fonts, FontPreferences, Audio, OsCpu, Language are obtained. For some attributes, on the contrary, the values are not calculated, in the table they are shown as "false".

- Chaging the browser to Tor Browser

Tor Browser shows that no connection to the server can be established, so no fingerprints are retrieved. However, the tool itself can be an effective countermeasure against tracking browser fingerprints under other conditions.

- NoScript

Connecting the plugin in Google Chrome does not let getting fingerprints because the site linked to the artificially created server is not fully loaded.

- Disconnect

There are no changes in the browser fingerprint due to the installation of the plugin.

It is also possible to install plugins on another browser. Consider the last one and the two types of plugin used: Canvas Fingerprint Defender and Font Fingerprint Defender.

- Canvas Fingerprint Defender (for the new browser)

Compared to the original fingerprint in the new browser, the values of Canvas_Geom and Canvas_Text change, similar to the application of the plugin in Google Chrome. However, there is one advantage associated with receiving a notification that the browser fingerprinting is going on and therefore the plugin is currently being used for its intended purpose.

- Font Fingerprint Defender (for the new browser)

Changes the list of used fonts for the browser attribute Fonts. New fonts are added.

There are other measures to counteract the tracking of user browser fingerprints, but this set of measures may be sufficient to analyze the results of the experiment, since there is a change in the important informative attribute Canvas, as well as the addition or removal of other browser attributes.

4. EXPERIMENT RESULTS ANALYSIS

To evaluate the effectiveness of the measures used, the calculation of the statistical parameter - Shannon entropy will be used by (1):

$$H(x_i) = -\sum_j P(x_{ij}) \log_2 P(x_{ij}), 1 \leq i \leq n, i \in Z, \quad (1)$$

where:

n is a number of browser attributes,

x_i is the random variable associated with the value of the i -th characteristic,

x_{ij} is the j -th value of the i -th characteristic,

$P(x_{ij})$ is the probability that the i -th characteristic will take a new j -th value.

In practice, the normalized Shannon entropy is used more often. It is calculated by (2):

$$H_n = \frac{H(x_i)}{H_M}, \quad (2)$$

where:

H_M is the maximum entropy at which all values of the j -th characteristic are unique, i.e. $H_M = \log_2(n)$.

It is assumed that the higher the entropy value, the more the characteristics change and the better the countermeasure against tracking user browser fingerprints works. However, it is worth noting that decreasing entropy can also be useful, as it allows to achieve identity for characteristics and in some cases also contribute to an effective countermeasure.

There is a total of 34 browser attributes. Assume that each attribute can change with equal probability 0.029, and that all attributes have the same value in composing the user's browser fingerprint. Let us calculate the entropy for all applied measures and enter the values in the resulting Table 3.

Table 3. Comparative analysis of the effectiveness of countermeasures against browser fingerprint tracking in the experiment

Measure	Changeable attributes	Entropy
Canvas Blocker (Fingerprint Protect)	Canvas_Geom, Canvas_Text	0.059

DoNotTrack Header	Doesn't change attributes	Isn't calculated
CyDec Security Anti-FP	Plugins	0.029
Changing the browser	Fonts, FontPref, Audio, osCpu, Language, DevMem, Plugins, Vendor, VendorFlavors, ColorGamut	0.294
Changing the browser to Tor Browser	Attributes cannot be obtained	Isn't calculated
NoScript	Attributes cannot be obtained	Isn't calculated
Disconnect	Doesn't change attributes	Isn't calculated
Canvas Fingerprint Defender (for the new browser)	Fonts, FontPref, Audio, osCpu, Language, DevMem, Plugins, Vendor, VendorFlavors, ColorGamut, Canvas_Geom, Canvas_Text	0.354
Font Fingerprint Defender (for the new browser)	Fonts, FontPref, Audio, osCpu, Language, DevMem, Plugins, Vendor, VendorFlavors, ColorGamut	0.294

Fig. 1 shows the diagram of the entropies of available countermeasures against tracking user browser fingerprints in the experiment.

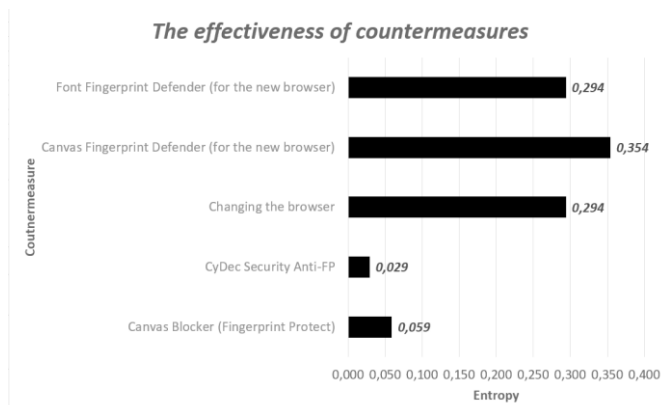


Figure 1. Diagram of the effectiveness of countermeasures against tracking browser fingerprints in the experiment

The highest value of entropy corresponds to the fact that the applied countermeasure is the most effective. Thus, the most

effective ways are the combined use of the plugin and a change of browser. Changing the browser from Google Chrome to a new standard one and installing the Canvas Fingerprint Defender plugin allows you to change 12 browser attributes and achieve an entropy value of 0.354.

5. CONCLUSIONS

This paper examines the effectiveness of countermeasures against tracking user browser fingerprints. The second chapter describes the classification of the main countermeasures against tracking user browser fingerprints. The third section conducts an experiment that produces different browser attributes, taking into account the browser and plugins used, or lack thereof. To obtain browser fingerprints consisting of browser attributes, Javascript code is written with the "fingerprint3.js" library connected. In the fourth part of the work is a comparative analysis of the measures used. Entropy metrics and modifiable attributes are determined, based on which a table is compiled and the conclusion is made about the most effective means of combating the tracking of user browser fingerprints. The main result of the experiment is that the combined use of countermeasures, such as changing browsers and installing a special plug-in for a new browser, is most effective. It provides the highest entropy value and changes 12 browser attributes; therefore, the user will be the hardest to correctly identify because his browser fingerprint will be strongly different from that of other users. The results of the study can be used both for practical purposes to reduce the probability of correct identification of users, and in the further works to study in more detail the proposed measures to counteract the tracking of browser fingerprints of users. In addition, the study can be expanded with the study of other characteristics of browser fingerprints, which can be obtained through the use of other resources.

Funding: This research was partially funded by Russian Science Foundation, project No 22-21-00846.

REFERENCES

- Agafonov. U.M. (2018). Deanonymization of users based on digital, fingerprint, *Information Space Security: Collection of Proceedings of the XVI All-russian Scientific and Practical Conference of Students, Young Scientists. Ekaterinburg: Ural Federal university named after the first President of Russia B.N. Elcin*, pp. 3-5.
- Antonio E., Fajardo A., Medina R. (2020). Tracking browser fingerprint using rule based algorithm, *Proc. of the 2020 16th IEEE Int. Colloquium on Signal Processing & Its Applications*, pp. 225–229.
- Bujlow T., Carela-Español V., Solé-Pareta J., Barlet-Ros P. (2017). A Survey on Web Tracking: Mechanisms, Implications, and Defenses, *Proceedings of the IEEE*, vol. 105, № 8, pp. 1476-1510.
- Choi S., Yun J., Kim S. (2018). A comparison of ICS datasets for security research based on attack paths, *Int. Conf. on Critical Information Infrastructures Security*, pp. 154–166.

- Efremov E., Kovalevsky A., Ershova, Y. (2018). Effective ways of information collection from open sources in the Internet, *Theoretical and practical issues of integrated safety*, pp. 217-218.
- ElBanna A., Abdelbaki N. (2018). Browsers Fingerprinting Motives, Methods, and Countermeasures, *International Conference on Computer, Information and Telecommunication Systems (CITS)*, Colmar, pp. 1-5.
- Fehér K. (2021). Digital Identity and The Online-Self: Footprint Strategies, *Journal of Information Science*, vol. 47, pp. 192-205.
- Fiore U., Castiglione A., De Santis A., Palmieri F. (2014). Countering Browser Fingerprinting Techniques: Constructing a Fake Profile with Google Chrome, *17th International Conference on Network-Based Information Systems*, Salerno, pp. 355-360.
- Iskhakov A. (2014). User authentication schemes in ACS using QR codes and data transfer using NFC technology, *Information countermeasures against terrorism threats*, vol. 22, pp. 11–15.
- Iskhakov A., Salomatin A. (2020). Estimation of the time for calculating the attributes of browser fingerprints in the user authentication task, *Topical Problems of Agriculture, Civil and Environmental Engineering*, vol. 224, pp. 1–9.
- Iskhakova A., Iskhakov A., Meshcheryakov R., Bendrau R., Melekova O. (2018). Using a heatmap of user behavior in the problem of identifying the subject of an information security incident, *Proc. of the SPIIRAS*, vol. 6, pp. 147–171.
- Ivanov A., Zhukov V., Maslova O. (2014). Application of browser fingerprinting for identification of users in international information interchange networks, *Youth, society, modern science, technology and innovation*, no. 13, pp. 15-16.
- Jiang W., Wang X. (2020). Tracking your browser with high-performance browser fingerprint recognition model, *China Communications*, vol. 17, no. 3, pp. 168-175.
- Laperdrix P., Rudametkin W., Baudry B. (2016). Beauty and the Beast: diverting modern web browsers to build unique browser fingerprints, *Proc. of the 2016 IEEE Symposium on Security and Privacy*, pp. 878– 894.
- Laperdrix P., Rudametkin W., Baudry B. (2015). Mitigating browser fingerprint tracking: multi-level reconfiguration and diversification, *Proc. of the 2015 IEEE/ACM 10th Int. Symposium on Software Engineering for Adaptive and Self-Managing Systems*, pp. 98–108.
- Luangmaneeerote S., Zaluska E., Carr L. (2017). Inhibiting Browser Fingerprinting and Tracking, *IEEE 3rd International Conference on Big Data Security on Cloud*, Beijing, pp. 63-68.
- Nair K., RoseLalson E. (2018). The Unique Id's You Can't Delete: Browser Fingerprints, *International Conference on Emerging Trends and Innovations in Engineering and Technological Research (ICETIETR)*, Ernakulam, pp. 1-5.
- Parfenov D., Torchin V., Zabrodina L., Parfenov A. (2019). Approaches to vulnerability search and security in digital manufacturing Networks, *Proc. of Managing the Development of Large-Scale Systems*, pp. 1253–1259.
- Salomatin A.A. (2021). Methods to counteract the tracking of user browser fingerprints, *Proceedings of the 29th International Conference "Problems of Security Management of Complex Systems" (PUBSS'2021, Moscow)*, M.: ICS RAS, pp. 248-252
- Strukov A., Vetlugin K. (2017). On methods of quantitative analysis of the cybersecurity of technical systems based on a logical-probabilistic approach, *Science of Science*, vol. 9, pp. 1–7.
- Tsvirkun A., Platonov T., Malkina N. (2019). Detection of Internet fraud with some probability, *Information Security Questions*, pp. 8-13.