METHOD OF PREVENTING LEAKAGE OF PERSONAL DATA THROUGH EYE-TRACKING MODULES OF USER DEVICES

DOI: 10.36724/2072-8735-2022-16-7-44-51

Mikhail Vyatkin,
Aleksei Potashnikov,
Vladimir Selivanov,
Igor Vlasuyk,
Ksenia Nezhivleva,
Moscow Technical University of Communications and Informatics, Moscow, Russia

Anastasia Mozhaeva,
Moscow Technical University of Communications and Informatics, Moscow, Russia;
The University of Waikato Hamilton, New Zealand,
anast.mozhaeva@gmail.com

Manuscript received 08 June 2022;
Accepted 30 June 2022

Keywords: *data personalization, data protection, machine learning, eye tracking, tracking protection, data anonymization, visuomotor system*

At the current stage of technology development, eleven billion records of personal data and payment information were compromised worldwide in 2022 as a result of leaks that became public knowledge, in particular, first and last names, email addresses, phone numbers, passwords, residency information, social security, bank card details and bank account information. Nowadays, with user computer data, personal information about a person can be collected through behavioural habits. Primary identifications by malicious software, such as identification by mouse cursor and sent requests, are already familiar to users and security services of specialized companies. However, the eye movement identification of users is a new and unresolved problem that threatens to cause major losses of personal data in the coming years. Manufacturers, with the exception of clauses in user agreements, do not solve the problem of tracking personal data using new devices. The article presents and analyzes modern eye tracking devices and the guarantee of user anonymity provided by the manufacturers. Proposed solution and method to prevent identity theft at the initial stage of identifying regions of user interest, which used a simulation of the visuomotor system as the horizontal and vertical movements of the human eye relative to a given activation.

Для цитирования:
Вяткин М., Поташников А., Селиванов В., Власюк И., Неживлева К., Можаева А. Метод предотвращения утечки персональных данных через модули отслеживания взгляда пользовательских устройств // T-Comm: Телекоммуникации и транспорт. 2022. Том 16. №7. С. 44-51.

For citation:
Vyatkin M., Potashnikov A., Selivanov V., Vlasuyk I., Nezhivleva K., Mozhaeva A. Method of preventing leakage of personal data through eye-tracking modules of user devices. *T-Comm*, vol. 16, no.7, pp. 44-51. (*in Russian*)

I. INTRODUCTION

Nowadays, many users and companies are expressing concerns about personal data on the Internet [1]. There is a problem with identifying a person on the Internet that is hard to deny. Users can be identified in various ways. Installing various identifiers, similar to cookies, which are stored on the computer and authenticate the user on websites, storing personal preferences and settings, tracking the status of the access session, and collecting all statistics about the users. The main disadvantage of the technology is that there is a possibility on the client side to replace or steal data fragments and obtain the necessary information or access to the data [2]. Also, with user computer information, the data can be identified from the HTTP headers of the requests sent. Eleven billion records of personal data and payment information were compromised worldwide in 2021 as a result of leaks that became public knowledge, in particular, first and last names, email addresses, phone numbers, passwords, residency information, social security, bank card details and bank account information [1].

A completely new way to determine personal data on the Internet, which is now gaining popularity: a so-called fingerprinting - identification of users by the behaviour and habits (movements of the cursor, typing speed on the keyboard, monitor resolution, favourite sections of the site, and the like). Future technologies are already being developed that allow the eye to interact with objects in games and commercial programs. Gamer eye trackers allow users to make the eyes an additional controller, to improve the experience in games such as Microsoft Flight Simulator, FarCry 6, Watch Dogs Legion, F1 2022, Euro Track Simulator, Figure 1 [2].

Fig. 1. Eye control in games

Another area, where eye tracking is used is AR/VR applications, in which the physical controller will gradually be supplemented or replaced by the user's glance. Televisions with eye tracking will be able to collect information about the user, offering preferred content [3], [4]. Considering the sales indices for recent years, about 6.65 million televisions were sold in Russia in just one year. Global statistics report that in 2021, manufacturers around the world shipped about 213.54 million televisions [5]. Assuming most television sets in the near future will be equipped with an eye-tracking system. The scale of the problem of saving the personal data of users is enormous. Televisions have already given rise to doubts about the security of personal data. The high-profile case of television manufacturer Vizio, which paid $2.2 million to settle a lawsuit after revealing that the company secretly collected and sold viewing data to third parties for years. Recorded data from shows that were viewed, the information was sold along with IP data and metadata such as MAC addresses, nearby Wi-Fi networks and so on. Although names could not be attached to the data, gender, age, income, marital status, household size, education and home ownership were included in the data archives sold [6]. With televisions being equipped with eye trackers, there will be more opportunities to collect and sell users' data. Under the law "on the protection of personal data", which describes the subjects of personal data, Article 7 of federal law № 152: "Operators and other persons who have access to personal data shall not disclose to third parties and shall not disseminate personal data without the consent of the subject of personal data, unless otherwise provided by federal law." Also, paragraph 9 of Article 6 states: "processing of personal data shall be carried out for statistical or other research purposes, except for purposes specified in Article 15 of this Federal Law, subject to mandatory depersonalization of personal data." The collection of human gaze data with subsequent identification is considered illegal.

Personal data protection measures are needed. Without proper protection, all users, who use eye tracking technology on devices, will be at risk. At present, there are no statistics on the number of users already using eye tracking technology, or, in other words, the number of citizens' personal data at risk right now. The solution to the problem of user identification is considered to be online and offline personal data depersonalization programs. However, data depersonalization programs often fail to meet the challenge. Problems arise with both primary user identification by malware and the depersonalization of databases collected by specialized agencies and made available to the public. For instance, in the mid-1990s, Massachusetts published medical records resuming the medical histories of every state employee. The governor publicly assured that the information was anonymous, removing all identifying information – names, addresses, and social security numbers. Soon the governor received by mail his own medical records (which included a lot of private information)! People could be re-identified by the information that was left.

Considerable research on re-identification methods has been made. Using publicly available Internet records, 50% of people can be identified by city, date of birth, and gender. 85% can be identified if given a zip code as well. Another interesting example of user identification that is not imagined in everyday lives is working with a movie database. Netflix released a database of 100 million movie-rating records, where people were asked to rate movies [on a scale] of 1 to 5, and had a whole group – 100 million records total. What appeared was that 99% of the people in the database could be identified by knowing the ratings for the 6 movies and about the time that a person had been watching. Even if for only 2 movies the ratings are known, 70% of the people can be

identified [7]. Re-identification is extremely effective and anonymizing data is incredibly difficult to achieve effectively.

The hunt is on for user data. For example, in 2020, hackers were on the network of the National Bank of Denmark for 7 months [8]. In November 2019, the attack on Alibaba began, secretly be collected more than 1.1 billion instances of user information [9]. In 2021, malefactors were exposed to more than 60 GB of data, including customer bases, retailer and distributor accounts, as well as financial information of the Acer Company [10]. Gaming industry giant EAgames lost 750 GB of data as a result of the server hack [11]. In the same year, a huge database of users appeared on the malefactors' forums [12].

Thus, the concerns of users and companies about the protection of personal data on the Internet are comprehensible. This problem is already crucial at the moment. All current research and software products do not consider the user's eye position, while more and more products are being released. The widespread introduction of eye tracking technology into mass and business segments is planned. In the near future, eye tracking devices appearing in sufficient supply could pose a threat in the area of personal data retention. One of the solutions for identifying and re-identifying users on the Internet is algorithms for primarily hiding information about user actions, such as cursor movements, eye tracking, and the preferred sections of the site, anonymized data is of no value to intruders and prevents the possibility of re-identifying the user.

The work is organized as follows. Section II provides an overview and analysis of existing data protection in the use of eye trackers by Internet users today. Section III proposes one of the possible solutions for personal data protection when using the new eye tracking feature, namely a new method of primary hiding information about user actions, which does not require significant resources and demonstrates high stable results of depersonalizing the user's screen.

II. DATA PROTECTION USING THE EYE TRACKER TODAY

Nowadays, using data about personal computers, information can be collected through behavioural habits. Primary user identifications by malware, such as identification by mouse cursor and sent requests, are already familiar to users and security services of specialized companies. However, user identification by eye movement is a new and unresolved problem that threatens to cause major personal data loss in the coming years.

Large corporations, such as Google, are developing eye tracking methods using new pupil detection equipment. Moreover, even without an eye tracking device, relying only on external camera readings, Google Glass already collects information about the user online and reveals personal data. Existing methods for eye tracking in Google Glass are used to position the pointer and area of interest in AR applications on the glasses. Google Glass is a headset for Android smartphones developed by Google, Figure 2. Google is currently selling to developers only, about 250,000 units worldwide.

Fig. 2. Smart glasses "Google Glass"

Google software can determine where a person is looking, often by where the outdoor camera is pointing. The scene details and regions of interest of the user can be more specifically identified. Such areas (regions) are samples from streams or sets of gaze data that show the user's object of interest in the presence of any content, Figure 3. If in Google an eye-tracking camera connection is added, even changes in pupil size can give information about emotional state or arousal in real life, Figure 4 [13].

Vision specialist Michael Dorr, head of an international junior research group at the Technical University of Munich in Germany, in conjunction with Scientific American MIND magazine, provides information that users are already concerned about the implications of the unclassified front-facing cameras in Glass. The cameras in Glass are able to record pictures and videos of crowds of oblivious passersby every day. Google can learn about users based on their gaze, and this raises concerns about a potential invasion of privacy. The Google patent number 8611015 was issued on December 17, 2013, and describes a number of new features, including eye tracking. Brandin White, the developer of Google Glass, believes the worst thing to happen today is that user data is being sold. Google wants people to have apps on their devices, which know everything about their lives. Corporation has the position that personal device keeps track of the user's life and helps with daily routine, Figure 4 [14]. The question remains open as to how willing people are to trust the identification of personal data for eye tracking. To what extent user data will be protected.

Nowadays, eye tracking technology is actively used in games, with Tobii being the leader in gaming eye trackers. Tobii solutions allow gamers to use their gaze as an additional controller in games. For instance, the aiming position follows the user's gaze or highlights additional actions in the virtual world without pointing to the cursor. Tobii introduces Tobii Pro Glasses. The discreet device and simple design, similar to ordinary glasses, increase the possibility of natural behaviour, especially in public places or during face-to-face communication [15]. In the Windows 10 operating system, Microsoft has implemented the Windows Hello biometric unlock technology. Since Windows Hello is built directly into the operating system, it allows you to identify a user by face or fingerprint to unlock users' devices. The system supports embedded and external devices. There are more than 1.4 billion active devices running Windows 10 or Windows 11 with Windows Hello technology [16]. Tobii with its eye-tracking devices is the first company to start collaborating with Microsoft. Today developers have access to collect users' data based on this technology. The technology allows Windows Hello to work in various lighting conditions, even in the dark [17], [18].

At the current moment, there is no software for anonymizing and preventing user identification based on gaze data in the mass segment. Major manufacturers of eye tracking devices offer to rely on a policy of "data transparency". For example, Tobii, on its official website under Transparency writes: "The data generated by eye tracking technology can inform a lot about a person. The reactions in certain situations, the feelings, the identification and even suffering from specific diseases. Classified as personal data, eye tracking information must be handled accordingly. Tobii is committed to protecting the data integrity and privacy of every person who interacts with eye tracking. But we cannot do this alone. We rely on every product to respect users by being very clear about whether their eye tracking data is being stored or transferred to another system and, more importantly, why. To help us realize this aspiration, we created the Tobii EyeTracking Data Transparency Policy" [19].

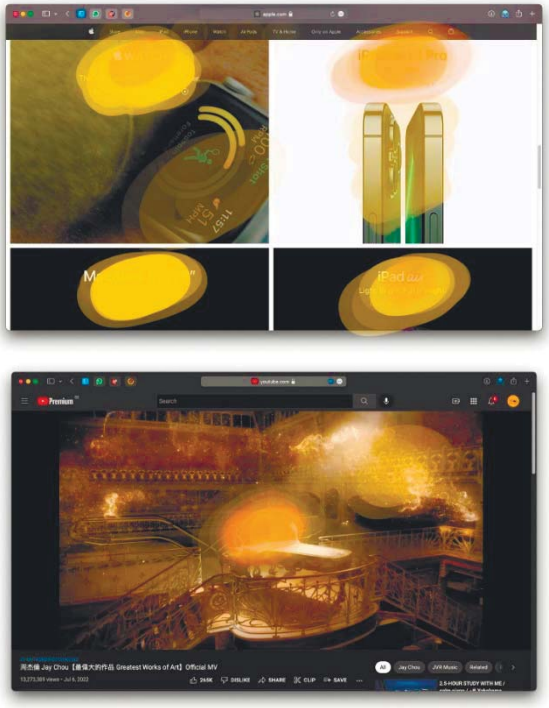

Fig. 3. Regions of interest during viewing of the website and video content

Fig. 4. Regions of interest in real life

The company claims that developers must adhere to licensing conditions when creating their products, one of the conditions being the above-mentioned policy of data transparency. Nevertheless, developer licensing does not protect against malicious unlicensed software, hacker attacks, and the threat of infecting the device to collect user information. Also, the Eye Tracking Data Transparency Policy policy only protects software users from trusted developers, who license the products from Tobii. While many products exist and are being developed that are too small or highly specialized for Tobii licensing, as well as malware and computer viruses. The situation is similar (almost identical) to other manufacturers of eye-tracking devices.

As far as we know, there is currently no eye depersonalization program in the world, which in turn puts users of eye tracking devices at risk right now. In Q1 2022 report, Tobii announced negotiations with Sony to become the supplier of eye tracking technology in PlayStation VR 2. As of 2020, 5 million first-generation PS VR kits have been sold. Persons should expect the popularity of these devices to grow when the second generation with eye tracking technology is released. The audience of such devices is constantly growing, analysts suggest that by 2024 a quarter of virtual and mixed reality devices will have eye tracking technology. Meanwhile, as described above, these companies, except as clauses in user agreements, are not addressing the problem of tracking users.

III. POSSIBLE WAYS OF SOLVING THE PROBLEM

One possible way to solve user identification on the Internet is to develop methods to anonymize user personal data in streaming data using eye tracking and machine learning. In this article, we propose a methodology for anonymizing user gaze data that will be able to hide and anonymize the information reliably enough. This methodology will make it much more difficult to de-anonymize a user on the Internet.

To create the method a database of average content should be used, which includes the maximum number of real scenes of the person's computer use while browsing the content with marked regions of interest. The database should simulate the personal data received by Toby, Google and other devices, from real users while browsing ordinary content like Internet sites, paid TV, etc. Visual perception is burdened with a highly discontinuous input stream arising from saccadic eye movements. For successful imitation, the methodology used a simulation of the visuomotor system that successfully simulates the horizontal and vertical movements of the human eye relative to a given activation. It has been repeatedly proved that algorithms built on models that take into account the characteristics of the human visual system give higher and more stable results [22, 23,24]. The scheme of the method is shown in Figure 5.

The average content database block contains an entire user database containing ordinary user content. The Regions of Interest block includes user regions of interest and the direction of real users' gaze. These regions show the zones of interest of the user while consuming and interacting with the content. We remind to the readers, that the regions of interest obtained through eye tracking are the users' personal data.

In the virtual area block, a virtual area is created programmatically, with a resolution several times greater than the real size of the main monitor. Content from the average content database, previously selected by the model, is broadcast onto the virtual area (virtual monitor) and is as similar as possible to the content. The installed eye-tracking system captures the user's eye point and transmits the data to the coordinate displacement block.

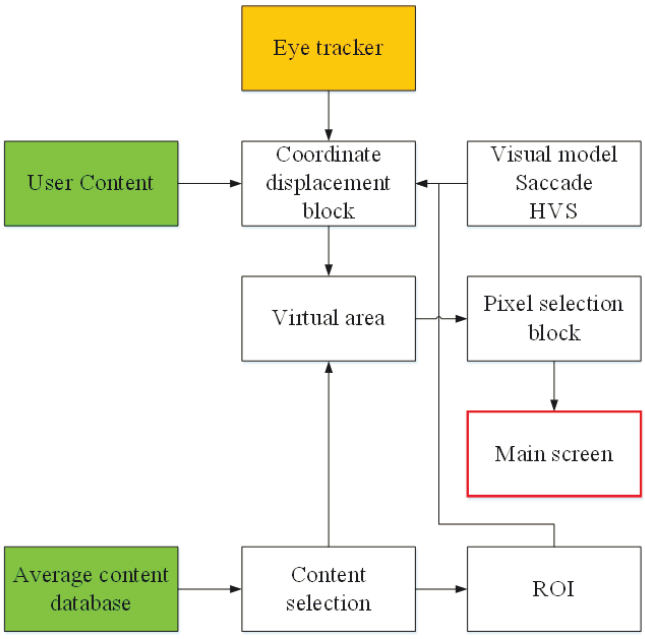

Fig. 5. Scheme of the presented method

The visual model block is needed to generate points and saccades of the human eye, considering the physiological features of vision. The eye movement modelling procedure was carried out using geometric modelling of binocular vision. Used the saccade model formula [20]:

The relationship between peak saccadic angular velocity and saccadic amplitude can be approximated by the exponential function:

$$V_p(A;\eta,c) = \eta\left(1 - e^{-\frac{A}{c}}\right) \quad (1)$$

where V_p is peak saccadic angular velocity, A is saccadic amplitude, η is parameter representing the maximum attainable peak angular velocity of any saccade made by the individual, c is parameter determines the proportionality constant between V_p and A for small saccades. Model of saccadic waveform $s(t)$ determined as the sum of a soft ramp function $f(t)$ and a shifted negated soft ramp function $-f(t-\tau)$,

$$s(t;\eta,c,\tau) = cf(\eta t/c) - cf(\eta(t-\tau)/c) \quad (2)$$

where

$$f(t) = \begin{cases} t + 0.25e^{-2t}, & t \geq 0 \\ 0.25e^{2t}, & t \leq 0 \end{cases} \quad (3)$$

and η, c, and τ are parameters. Amplitude of the saccade model $s(t)$ is given by $\eta\tau$,

$$A = \lim_{t\to\infty} s(t) - \lim_{t\to-\infty} s(t) \quad = \eta t = \eta(t-\tau) = \eta\tau. \quad (4)$$

Consequently:

$$V_p == \eta(1 - e^{-A/c}) \quad (5)$$

Then the movement of pixels in the proposed method is defined as

$$\frac{\partial r_p}{\partial t} = \frac{(D^2 + \frac{h^2}{h_p^2}(x^2+y^2))h_p}{Dh} V_p \quad (6)$$

where x, y is the current coordinates of the center of the region of interest relative to the center of the image, measured in pixels; D is the distance from the image to the person, measured in measured in pixels and meters respectively; h, h_p, is the height of the image, respectively.

$$\frac{\partial x}{\partial t} = \frac{y_2 - y_1}{(x_2 - x_1)\sqrt{1 + \frac{y_2 - y_1}{x_2 - x_1}}} \frac{\partial r_p}{\partial t} \quad (7)$$

where (x_1, y_1) and (x_2, y_2) are the coordinates of the initial and final position of the center of the region of interest relative to the center of the image, respectively, measured in pixels.

$$\frac{\partial y}{\partial t} = \frac{1}{\sqrt{1 + \frac{y_2 - y_1}{x_2 - x_1}}} \frac{\partial r_p}{\partial t} \quad (8)$$

The coordinate displacement block takes the original resolution of the monitor with the content currently being broadcast and viewed by the user on it; a model of the human visual system with the number and direction of user saccades read by the eye tracker; and regions of interest for the content being broadcast in the virtual area. Then, in the coordinate displacement block, an allowable displacement coordinate at a given moment is created and transmitted to the virtual area.

The pixel selection block moves the original resolution main content over the virtual area by the coordinate calculated by the displacement block. Thus, making it impossible to distinguish user regions of interest from those marked in the average content. The user, meanwhile, sees the main content on the device's monitor. When data is stolen, attackers will get a mixture of average and real gaze data, with real data being a small fraction of the total mass and impossible to distinguish from, visualization of the method's operation is shown in Figure 6.

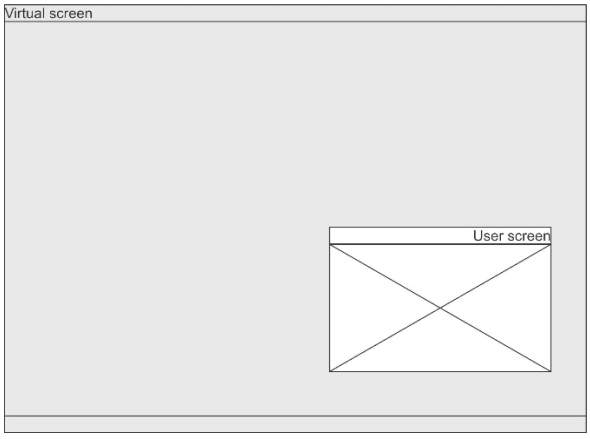

Fig. 6. Visualization of the presented method's operation

The presented method can be used to create software for eye tracking devices. This software can be installed on any PCs and smart wearable devices when gaze anonymization is necessary. According to the U.S. Patent and Trademark Office, Google has patented the eye tracking technology in next-generation Google Glass [21]; the Google itself reports that "about 21.6 million people would buy Glass if it went on sale today. Thus, according to the Law "On Personal Data Protection" of the Federal Law 152, article 11, paragraph 1: “Information which characterizes the physiological and biological characteristics of an individual and

which can be used by the operator to identify the subject of personal data (biometric personal data) can be processed only with the written consent of the subject of personal data, except in cases provided by the part 2 of this article.". Based on the above, in the near future there will be the need to install the anonymization software of personal data, namely the regions of interest of users, on more than 20 million devices with the ability to track the eye.

IV. CONCLUSION

At the current stage of technology development, there are more than 11 billion personal data of users in the public domain, obtained without their consent. New technologies on the market today make users' lives more comfortable, but allow the illegal collection of personal data through behavioural habits. These technologies include user identification by eye movement, which is an unsolved problem at the moment and threatens to cause great losses of personal data in the coming years. Manufacturers, with the exception of clauses in user agreements, do not solve the problem of tracking personal data using new devices. The article presents and analyzes modern eye tracking devices and the guarantee of user anonymity provided by the manufacturers. We propose the solution and the method to prevent identity theft at the initial stage of identifying regions of user interest.

The data, presented in the article, can be useful for creating new ways of solving personal data protection or the initial hiding of information about users' actions when using the eye tracking feature that has appeared on the market.

REFERENCES

1. A. T. Tunggal (2022), "The 65 Biggest Data Breaches", UpGuard, June 2022, [online] Available: https://www.upguard.com/blog/biggest-data-breaches

2. Tobii Gaming "Enhance PC games with eye tracking", [online] Available: https: // gaming. Tobii.com/games/

3. H. Lee, W. Oh Lee, C. Cho, S. Gwon, K. Park, H. Lee, J. Cha (2013), "Remote Gaze Tracking System on a Large Display", *Sensor*, (Basel), [online] Available: https://www.researchgate.net/publication/257534510_Remote_Gaze_Tracking_System_on_a_Large_Display

4. W. Oh Lee, Y. G. Kim, K. Y. Shin, D. T. Nguyen, K. W. Kim, K. R. Park, C. In Oh (2014), "New method for face gaze detection in smart television," *Opt. Eng.*, no. 53(5) 053104, Available: https://doi.org/10.1117/1.OE.53.5.053104

5. "Televisions Global Market Report 2021: COVID 19 Impact and Recovery to 2030", 2021, [online] Available: https://www.reportlinker.com/p06072066/Televisions-Global-Market-Report-COVID-19-Impact-and-Recovery-to.html?utm_source=GNW

6. D. Coldewey, "Vizio settles for $2.2 million in FTC suit over snooping on consumers viewing habits", *TechCrunch*, [online] Available: https://techcrunch.com/2017/02/06/vizio-settles-for-2-2-million-in-ftc-suit-over-snooping-on-consumers-viewing-habits/

7. Ian H. Witten, E. Frank, M.A. Hall (2016), "Data Mining: Practical Machine Learning Tools and Techniques", Elsevier Science & Technology, Available: https://doc.lagout.org/Others/Data%20Mining/Data%20Mining%20Practical%20Machine%20Learning%20Tools%20and%20Techniques%20%283rd%20ed.%29%20%5BWitten%2C%20Frank%20%26%20Hall%202011-01-20%5D.pdf

8. M. Lorenzen (2021), "Central bank of Denmark hacked as part of 'the world's most sophisticated hacker attack", [online] Available: https://www.version2.dk/artikel/central-bank-denmark-hacked-part-worlds-most-sophisticated-hacker-attack

9. Y. Jie, L. Lin (2021), "Alibaba Falls Victim to Chinese Web Crawler in Large Data Leak", *The Wall Street Jornal*, [online] Available: https://www.wsj.com/articles/alibaba-falls-victim-to-chinese-web-crawler-in-large-data-leak-11623774850

10. C. Climpanu (2021), "Acer confirms second security breach this year", *TheRecord*, [online] Available: https://therecord.media/acer-confirms-second-security-breach-this-year/

11. S. Gatlan (2021), "Hackers breach gaming giant Electronic Arts, steal game source code", *BleepingComputer*, [online], Available: https://www.bleepingcomputer.com/news/security/ hackers-breach-gaming-giant-electronic-arts-steal-game-source-code/

12. B. Meyer (2021), "COMB: largest breach of all time leaked online with 3.2 billion records", *Cybernews*, [online] Available: https://cybernews.com/news/largest-compilation-of-emails-and-passwords-leaked-free/

13. L. Granka, M. Feusner, L. Lorigo (2008), "Eyetracking in Online Search", *Passive eye monitoring*, pp. 283-304. Available:https://static.googleusercontent.com/media/research.google.com/en//pubs/archive/34378.pdf

14. J. Calderone (2015), "Eye Tracking in Google Glass: A Window into the Soul?", *Scientific American*, [online] Available: https://www.scientificamerican.com/article/eye-tracking-in-google-glass-a-window-into-the-soul/

15. Tobii Pro Glasses (2021), [online] Available: https://www.tobiipro.com/product-listing/tobii-pro-glasses-3.

16. Microsoft story labs, "Microsoft By The Numbers: adding up the stories that make Microsoft", [online] Available: https://news.microsoft.com/bythenumbers/en/windowsdevices.

17. Microsoft Windows App Development, "Windows Hello", [online] Available: https://docs.microsoft.com/en-us/windows/uwp/security/microsoft-passport.

18. Tobii Eye Tracking, "Powering facial recognition for Windows 10", [online] Available: https://www.tobii.com/xperience/hello/

19. Tobii Eye Tracking Data Transparency Policy, 2022, [online] Available: https://transparency .tobii.com

20. Dai Weiwei, Selesnick Ivan, Rizzo John-Ross, Rucker Janet, Hudson Todd (2016), "A parametric model for saccadic eye movement", *IEEE Signal Processing in Medicine and Biology Symposium (SPMB)*, [online] Available: https://www.researchgate.net/publication/313539565_ A_parametric_model_for_saccadic_eye_movement

21. Google patents: "Gaze Tracking System", 2013 Available: https://patents.google.com /patent/US8510166B2/en

22. A. Mozhaeva, L. Streeter, I. Vlasuyk and A. Potashnikov (2021), "Full Reference Video Quality Assessment Metric on Base Human Visual System Consistent with PSNR," *2021 28th Conference of Open Innovations Association (FRUCT)*, pp. 309-315.

23. A. I. Mozhaeva, I. V. Vlasyuk, A. M. Potashnikov, L. Streeter, (2021), "Reference objective metric for assessing video quality compatible with PSNR, taking into account the frequency and peripheral characteristics of human vision," *DSPA: Issues of using digital signal processing*,
vol. 11, no. 2, pp. 44-54.

24. A. M. Potashnikov, V. A. Mazin, N. S. Stepanov, A. P. Smirnov and A. I. Mozhaeva (2022), "Analysis of Modern Methods Used to Assess the Quality of Video Sequences During Signal Streaming," *2022 Systems of Signals Generating and Processing in the Field of on Board Communications*, 2022, pp. 1-4.

МЕТОД ПРЕДОТВРАЩЕНИЯ УТЕЧКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ЧЕРЕЗ МОДУЛИ ОТСЛЕЖИВАНИЯ ВЗГЛЯДА ПОЛЬЗОВАТЕЛЬСКИХ УСТРОЙСТВ

Вяткин Михаил, *Московский технический университет связи и информатики, Москва, Россия*
Поташников Алексей, *Московский технический университет связи и информатики, Москва, Россия*
Селиванов Владимир, *Московский технический университет связи и информатики, Москва, Россия*
Власюк Игорь, *Московский технический университет связи и информатики, Москва, Россия*
Неживлева Ксения, *Московский технический университет связи и информатики, Москва, Россия*
Можаева Анастасия, *Московский технический университет связи и информатики, Москва, Россия;*
Университет Вайкато Гамильтон, Новая Зеландия, ***anast.mozhaeva@gmail.com***

Аннотация
На текущем этапе развития технологий в открытом доступе, в результате утечек, ставших достоянием общественности за 2022 год, во всем мире оказались скомпрометированы одиннадцать млрд записей персональных данных и платежной информации, в частности, имена и фамилии, адреса электронной почты, номера телефонов, пароли, сведения о постоянном месте жительства, номера социального страхования, реквизиты банковских карт и данные о банковских счетах. В настоящее время используя данные о компьютере, используемом пользователем, можно собрать личные данные о пользователе с помощью поведенческих привычек. Первичные идентификации пользователей вредоносным программным обеспечением, как идентификация по курсору мышки и отправленными запросами уже знакомы пользователям и службам безопасности специализированных компаний. Однако, идентификация пользователей по движению глаз является новой и не решенной проблемой, которая грозит большими потерями личных данных в ближайшие годы. Проблема отслеживания персональных данных пользователей с помощью новых устройств не решается компаниями производителями, кроме как пунктами в пользовательских соглашениях. В статье представлены и проанализированы современные айтрекеры и гарантии анонимности пользователей, предоставляемые производителями. Предложено решение и способ предотвращения кражи личных данных на начальном этапе выявления областей интереса пользователя, с использованием моделирование зрительно-моторной системы как горизонтального, так и вертикального движений глаза человека относительно заданной активации.

Ключевые слова: *персонализация данных, защита данных, машинное обучение, отслеживание взгляда, защита от слежения, анонимизация данных, зрительно-моторная система.*

Литература

1. *A. T. Tunggal*. The 65 Biggest Data Breaches // UpGuard, June 2022, [online] Available: https://www.upguard.com/blog/biggest-data-breaches.
2. *Tobii Gaming*. Enhance PC games with eye tracking", [online] Available: https: // gaming. Tobii.com/games/
3. *H. Lee, W. Oh Lee, C. Cho, S. Gwon, K. Park, H. Lee, J. Cha*. Remote Gaze Tracking System on a Large Display // Sensor, (Basel), 2013, [online] Available: https://www.researchgate.net/publication/257534510_Remote_Gaze_Tracking_System_on_a_Large_Display
4. *W. Oh Lee, Y. G. Kim, K. Y. Shin, D. T. Nguyen, K. W. Kim, K. R. Park, C.* In Oh, "New method for face gaze detection in smart television // Opt. Eng., 53(5) 053104, 2014, Available: https://doi.org/10.1117/1.OE.53.5.053104
5. Televisions Global Market Report 2021: COVID 19 Impact and Recovery to 2030, 2021, [online] Available: https://www.reportlinker.com/p06072066/Televisions-Global-Market-Report-COVID-19-Impact-and-Recovery-to.html?utm_source=GNW
6. *D. Coldewey*. Vizio settles for $2.2 million in FTC suit over snooping on consumers viewing habits, TechCrunch, [online] Available: https://techcrunch.com/2017/02/06/vizio-settles-for-2-2-million-in-ftc-suit-over-snooping-on-consumers-viewing-habits/
7. *Ian H. Witten, E. Frank, M.A. Hall*. Data Mining : Practical Machine Learning Tools and Techniques, Elsevier Science & Technology, 2016 Available: https://doc.lagout.org/Others/Data%20Mining/Data%20Mining_%20Practical%20Machine%20Learning%20Tools%20and%20Techniques%20%283rd%20ed.%29%20%5BWitten%2C%20Frank%20%26%20Hall%202011-01-20%5D.pdf
8. *M. Lorenzen*. Central bank of Denmark hacked as part of 'the world's most sophisticated hacker attack, 2021, [online] Available: https://www.version2.dk/artikel/central-bank-denmark-hacked-part-worlds-most-sophisticated-hacker-attack

9. *Y. Jie, L. Lin*. Alibaba Falls Victim to Chinese Web Crawler in Large Data Leak // The Wall Street Jornal, 2021, [online] Available: https://www.wsj.com/articles/alibaba-falls-victim-to-chinese-web-crawler-in-large-data-leak-11623774850
10. *C. Climpanu*. Acer confirms second security breach this year // TheRecord, 2021, [online] Available: https://therecord.media/acer-confirms-second-security-breach-this-year/
11. *S. Gatlan*. Hackers breach gaming giant Electronic Arts, steal game source code // *BleepingComputer,* 2021, [online], Available: https://www.bleepingcomputer.com/news/security/ hackers-breach-gaming-giant-electronic-arts-steal-game-source-code/
12. *B. Meyer*. COMB: largest breach of all time leaked online with 3.2 billion records // *Cybernews*, 2021, [online] Available: https://cybernews.com/news/largest-compilation-of-emails-and-passwords-leaked-free/
13. *L. Granka, M. Feusner, L. Lorigo*. Eyetracking in Online Search // Passive eye monitoring, 2008, pp.283-304 Available:https://static.googleusercontent.com/media/research.google.com/en// pubs/archive/34378.pdf
14. *J. Calderone*. Eye Tracking in Google Glass: A Window into the Soul? // Scientific American, 2015, [online] Available: https://www.scientificamerican.com/article/eye-tracking-in-google-glass-a-window-into-the-soul/
15. Tobii Pro Glasses, 2021, [online] Available: https://www.tobiipro.com/product-listing/tobii-pro-glasses-3/
16. Microsoft story labs. Microsoft By The Numbers: adding up the stories that make Microsoft, [online] Available: https://news.microsoft.com/bythenumbers/en/windowsdevices
17. Microsoft Windows App Development. Windows Hello, [online] Available: https://docs.microsoft.com/en-us/windows/uwp/security/microsoft-passport
18. Tobii Eye Tracking. Powering facial recognition for Windows 10, [online] Available: https://www.tobii.com/xperience/hello/
19. Tobii Eye Tracking Data Transparency Policy, 2022, [online] Available: https://transparency .tobii.com
20. *Dai Weiwei, Selesnick Ivan, Rizzo John-Ross, Rucker Janet, Hudson Todd.* A parametric model for saccadic eye movement // IEEE Signal Processing in Medicine and Biology Symposium (SPMB), 2016, [online] Available: https://www.researchgate.net/publication/313539565_A_parametric_model_for_saccadic_eye_movement
21. Google patents: Gaze Tracking System, 2013 Available: https://patents.google.com /patent/US8510166B2/en
22. *A. Mozhaeva, L. Streeter, I. Vlasuyk and A. Potashnikov*. Full Reference Video Quality Assessment Metric on Base Human Visual System Consistent with PSNR // 2021 28th Conference of Open Innovations Association (FRUCT), 2021, pp. 309-315.
23. *А. И. Можаева, И. В. Власюк, А. М. Поташников, Л. Стритер*. Эталонная объективная метрика оценки качества видео совместимая с PSNR учитывающая частотные и периферическую характеристики зрения человека // DSPA: Вопросы применения цифровой обработки сигналов. 2021. Т. 11. № 2. С. 44-54. EDN TQJSHP.
24. *A. M. Potashnikov, V. A. Mazin, N. S. Stepanov, A. P. Smirnov and A. I. Mozhaeva*. Analysis of Modern Methods Used to Assess the Quality of Video Sequences During Signal Streaming // 2022 Systems of Signals Generating and Processing in the Field of on Board Communications, 2022, pp. 1-4.