УДК - 004.056

М.С. Павлюк

DEVICE TRACKING

Vinnytsia National Technical University

Анотація

Стаття досліджує технології відстеження пристроїв. Вона охоплює технічні аспекти, вплив на приватність та безпеку, соціальні та етичні наслідки, використання в різних сферах та правові аспекти. Надає загальний огляд цих напрямків досліджень, що можуть служити основою для подальших робіт у цій області.

Ключові слова: технічні пристрої, конфіденційність, технології відстеження, захист інформації, інформація, пристрій, приватність, безпека.

Abstract

The paper explores device tracking technologies. It covers technical aspects, influence and security implications, social and ethical implications, applications in various fields, and legal aspects. It provides a general overview of these areas of research that can serve as a basis for further work in this area.

Keywords: technical devices, confidentiality, tracking technologies, information security, information, device, privacy, security.

Introductoin

In the digital world, where technical devices have become an integral part of everyday life, theft or loss can significantly impact our confidentiality. However, modern smartphones are equipped with tracking functionality, which allows for quick device location, albeit not always by benevolent individuals [1].

The use of technologies such as IP addresses, MAC addresses, Bluetooth, hardware indicators, or phone signals can aid in locating a device in case of loss. However, it's important to consider that location information gathered this way may be subject to misuse. Additionally, other data such as browser history, GPS coordinates, DNS servers, cookies, metadata, and FingerPrint can also be used for user tracking and privacy breaches. Therefore, it's crucial to exercise caution and discretion regarding the disclosure of personal information and the use of tracking features.

Research results

It's important to use devices where you disclose confidential information with caution and care. Technical devices can be tracked using various elements, such as photos and videos, communication circles, assets, and location. Many cameras add technical information to the image file properties. From a photo posted on social media, one can often determine where and when it was taken. There are special services that provide this information to anyone interested. Since there is no perfect world and not everyone adheres to strict confidentiality, the research highlights popular elements such as:

- **IP (Internet Protocol)** is essentially a digital address assigned to your device by your provider. There are different types of IP addresses: internal, external, dynamic, static. 80% of Internet users utilize an external static IP address assigned by their provider. Knowing your IP address, one can determine the provider, as well as the city you live in, postal code, and even your home.
- **MAC address** is a unique identifier for network equipment, allowing devices to access the Internet. Routers, phones, computers, and other gadgets capable of connecting to a network have MAC addresses. For example, when Wi-Fi is enabled, any device (laptop, tablet, or smartphone) reveals its MAC address. This information is publicly available and cannot be hidden without disabling the Wi-Fi module in your device. Some visitor analysis systems, such as Wi-Fi radars, are built upon this data, collecting information on how long, how often, and which locations a person visits. This data is then used to build popular routes and gather statistics on visit times and frequencies [2].

- **Bluetooth** operates similarly to a MAC address. All devices with active Bluetooth are constantly attempting to connect to something or someone. This can be exploited by malicious actors, often in crowded places. Scammers carefully plan their actions and prepare a device for hacking, typically a factory-reset tablet or smartphone. The only hindrance is the limited range (no more than 10-12 meters) required for a stable connection.
- **Hardware or phone indicators:** Basic VPN and proxy server programs help hide your location from prying eyes, but this isn't always sufficient. Some websites embed programs that read your hardware or phone system data: language, time, network name, and more.
- **Phone tracking:** Phones can be tracked using various identifiers, including Bluetooth and MAC addresses. Tracking a phone via IP is more challenging than a PC, as phone IPs are typically dynamic. IMEI and IMSI (the unique numbers of your phone and SIM card) are also used. With these identifiers, malicious actors can gain access to nearly everything on your phone: contacts, location, movements, address, account balance, and in some cases intercept calls or messages. They may also sign you up for paid services that deduct money from your account. However, the downside for attackers is that only you and your operator know your IMEI and IMSI [2].
- **Browser:** Carelessness is often the main reason browsers get hacked. Downloading files or installing extensions, and accidentally landing on phishing sites, can lead to the installation of malicious software on your hardware. After that, it depends on what was downloaded. Your system may be immediately locked, demanding ransom, or it may quietly track all your online activities in the background. Detecting malicious software is challenging; sometimes antivirus programs don't catch it, and it can remain unnoticed on your computer. A warning sign to watch for is an unusually heavy system load: if your hardware suddenly starts working slower and worse than before [2].
- **GPS:** Tracking methods using GPS are intuitively understandable even to users with limited cybersecurity knowledge. Most applications installed on phones or other devices continuously collect GPS data in the background. The phone's location is determined by satellite signal transmission, which provides precise geographical coordinates on Google Maps. Consequently, large corporations collect vast amounts of data and store them on their servers.
- **DNS servers:** DNS lookup allows tracking users on the network. Recursive domain servers have capabilities that jeopardize the confidentiality of users' personal data. Information obtained through DNS (Domain Name System - a computer distributed system for obtaining domain information) can be used to track users on the network and gather a "profile of their interests."
- **Cookies:** Some cookies are harmless, while others remain active even on sites they don't belong to, collecting information about your behavior. These are called persistent third-party cookies. Third-party cookies gather information for targeted advertising, analytics collection, or statistic tracking. Tracking cookies can be so aggressive that many antivirus programs classify them as spyware [2].
- **Metadata:** Metadata refers to data about data (composition, content, status, origin, location, quality, formats, volume, access conditions, copyrights, etc.). The National Information Standards Organization (NISO) offers a classification that can be applied to all types of data or data repositories, from libraries to websites, for textual and non-textual data, in digital or material form.
- **FingerPrint or device fingerprinting** is general information collected about a specific device for its subsequent identification. Fingerprints collect information even when cookies are disabled. If not listed, everything FingerPrint reads collects approximately information on 3 A4 sheets, including unique defects in your video card, screen diagonal, and much more. This technology is typically used by government agencies to apprehend cybercriminals [2].

The concept of device fingerprinting is associated with the practical value of human fingerprints. Ideally, all machines have a different fingerprint value (distinctiveness), and this value never changes (stability). In such a case, every machine on the network could be precisely identified without the user's consent. In reality, achieving full distinctiveness or stability is impossible. Improving one parameter leads to deterioration of the other. Protecting personal information online is extremely important. Tracking methods such as using IP addresses, cookies, and unique browser fingerprints allow providers to track user actions over time. To protect their privacy, users are advised to use VPNs, manage app permissions, be cautious with cookies, and regularly clear browser data. These measures can help maintain confidentiality and protect against tracking on the Internet [2].

Conclusion

The tracking technologies discussed are powerful tools that can have a significant impact on user privacy and security in the digital world. However, their potential benefits, such as locating lost devices and improving user experience, must be balanced with the risks of privacy and security breaches. Research into these technologies is necessary to understand their impact and develop effective protection measures. Special attention should be paid to privacy and security aspects, as they pose key challenges for modern tracking technologies.

REFERENCES

1. How to find and block a lost device? URL: https://news.samsung.com/ua/how-to-find-and-lock-a-lost-samsung-device-or-erase-all-data (date of access: 18.03.2024)

2. Tracking identifiers. URL: https://hackyourmom.com/pryvatnist/identyfikatory-vidslidkovuvannya/ (date of access: 18.03.2024)

Павлюк Марина Сергіївна – студентка групи УБ-22б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: pavlukmarina095@gmail.com

Науковий керівник**: Магас Людмила Миколаївна** – Викладач кафедри іноземних мов, Вінницький національний технічний університет, м. Вінниця

Pavliuk Maryna S. *- student of the group UB-22b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: pavlukmarina095@gmail.com*

Supervisor**: Magas Liudmyla M. -** Lecturer, Department of Foreign Languages, Vinnytsia National Technical University, Vinnytsia