DOI: https://doi.org/10.30837/csitic52021232202

Analysis of Variations in Biometric Authentication Methods in Mobile Devices

Oleksandr Sievierinov[1]

[1]*Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, e-mail: oleksandr.sievierinov@nure.ua*

Lesia Bilan [2]

[2]*Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, e-mail: lesia.bilan@nure.ua*

Abstract. *The analysis of variability of biometric authentication methods was carried out, the classification of biometric methods was examined. To ensure the required level of protection, it is recommended to use rich-factor authentication.*

Keywords: *authentication, biometric authentication, mobile device, fingerprints, Face ID.*

I. Introduction and Problem Statement

To solve the problem of information security, biometric is now increasingly used to replace password authentication. Password authentication has a number of obvious disadvantages, the main of which is that it is difficult to ensure that the password is left unnoticed by others, it is difficult to keep the code word or phrase secret. Therefore, most devices have changed the standard passwords and codes for biometric methods during authentication. Biometric authentication is fully used in mobile devices. More and more mobile devices are using fingerprint scanning and Face ID technology to protect corporate and personal data. But the issue of security remains an important factor. Therefore, the analysis of vulnerabilities of biometric authentication methods in mobile devices is very relevant.

II. Problem Solution and Results

Biometric authentication is based on a set of automated methods and devices for identifying people using their physiological or behavioral characteristics [1]. Biometric authentication is a way to confirm a person by recognition and combination of biometric data (eye color, eye contour, fingerprints, hand geometry, facial features, etc.), which are recorded by these data, with the owner's personal data.

The aim of the work is to analyze the methods of biometric authentication to determine the reliability of these methods of protection of information.

There are many methods of biometric identification, which can be divided into two main groups: statistical and dynamic. Statistical methods are based on the physiological (statistical) characteristic of a person, i.e. a unique characteristic given to him/her by birth and not inimitable by him/her. Statistical methods include fingerprints, shaped bones, eye line, color of the rheumatic membrane of the eye, ear shape, etc. [1, 2]. Their main disadvantage is that the data required for each of these authentication methods can be easily created. They are in open access, because every day we leave behind a lot of our own data which can be removed using special devices.

Another group - dynamic methods of biometric authentication. These include methods based on the behavioral characteristics of people, their handwriting, keyboard handwriting, voice, etc. These methods are also not 100% reliable, because if necessary, a well-trained person can repeat your behavioral characteristics and other necessary data [1-3].

Biometric data are considered the most secure method of authentication, but they can be stolen or changed, and sensors of mobile devices can be manipulated, reproduced or disabled.

It should also be borne in mind that when using mobile devices, the lack of the necessary capacity and the lack of memory capacity makes it necessary to consider the authentication algorithms. Therefore their efficiency suffers and there are more and more possibilities for bypassing the protection system, which makes the task easier for crackers [3, 4].

Moreover, regardless of the type of biometric system in many mobile devices, if the user is not recognized, the system requires entering a password. So, the system can be forced to disable biometric authentication.

The analysis showed that for biometric authentication devices based on fingerprint readers in iPhones and Samsung hackers have learned to create pre-dropped fingerprints for unlocking. Also in 2019, a number of applications were presented that showed how 3D-rule can be used to create a plastic replica of fingerprints or a "primitive" face that can bypass the mobile device's security system [1-4].

Moreover, it is possible to compromise biometric data if access is granted through a mirror. Therefore, one of the most important security measures for biometric authentication is the protection of biometric information. Samsung and Apple devices store the mathematical representation of the bit instead of the bit itself in a separate protected location. This protected location is not synchronized with either the darkroom or the backups.

Thus, since the analysis showed the existence of differences in the methods of biometric authentication in mobile devices, two-factor or three-factor authentication is recommended to ensure the required level of protection.

III. Conclusions

In view of the above disadvantages, we can conclude that for a more reliable protection of information it is more appropriate to use the methods of luggage factor authentication. If only biometric authentication is used, two methods from different groups should be used, i.e. one from static and one from dynamic.

REFERENCES

[1] Мироненко Є.В., Сєвєрінов О.В. Біометрична ідентифікація і автентифікація особи за геометрією обличчя. – НТУ «ХПІ», 2020. – С. 96.

[2] Biometrics: definition, use cases and latest news, Available at: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics (accessed 11 April 2021).

[3] Нечволод К. В., Сєвєрінов О. В., Власов А. В. Аналіз безпеки в даних ЕММ системах // Системи управління, навігації та зв'язку. Збірник наукових праць. – 2019. – Т. 3. – №. 55. – С. 131-134.

[4] Сєвєрінов О.В., Федорченко В.М., Перепадя В.І. Аналіз загроз персональним даним в мобільному пристрої під час використання різноманітних додатків // Системи озброєння і військова техніка. – 2016. – № 4. – С. 42-45.