Possibilities of Improving the Cyber Security of Mobile Devices Based on the Integration of Dynamic Biometric Methods*

Aleksandra V. Vlasenko [1][0000-0002-4134-4980], Mikhail M. Putyato [1][0000-0003-0414-6034] and Aleksandr S. Makaryan [1][0000-0002-1801-6137]

[1] Kuban State Technological University
alex_vlasenko@list.ru
putyato.m@gmail.com
msanya@yandex.ru

Abstract. The article discusses the possibilities of using biometric authentication methods to improve the cybersecurity of the infrastructure of mobile devices and wearable electronics. It has been established, that approaches for collecting and analyzing parameters are also suitable for the formation of authentication systems for the Internet of things. Analysis and selection of characteristics required for identification are carried out. Biometric methods are based on identifying a person according to his inherent characteristics. The main advantage of biometric methods is that such signs cannot be stolen or transferred to another person. Biometric authentication does not identify a user with absolute precision. There is always a possibility of errors of the first (access denial) and second kind (false access).To solve the problem of providing an additional intermediate layer of data protection and encryption on a physical device, a mobile client-server application has been developed based on the technology of using dynamic biometric authentication methods.

Keywords: Cybersecurity, Forensics, Biometric Authentication Methods, Mobile Devices, Messengers.

1 Introduction

The widespread use of mobile devices and wearable electronics, as well as the high pace of changing trends in mobile applications, make the issue of security of stored data's security highly important. The decentralized nature of the information distribution environment poses more and more challenges for security professionals. And new approaches are not long in coming, for example, the decentralized nature of the IoT environment requires support for multi-entitlement attribute-based encryption (ABE) to implement granular access control [7], and experts are already working on implementing protocols with ABE support.

Messenger developers tend to go for tricks when implementing applications' security. They often claim their applications to contain certain security mechanisms, which are aimed to make users feel protected. However, practical researches of such implementations do not always confirm the declared safety.

In one of our articles [4], we studied an example of a "safe" messenger and demonstrated that it has been implemented with violation of the data protection system's integrity. The protection mechanisms function on open, accessible, software infrastructures of mobile devices: databases, transmission facilities, event logs, etc. In this regard, it is necessary to ensure the security of applications using the following approaches:

- encryption of attachments;
- removing all data from user-accessible memory space to the closed storage of the application;
- use of confusing names for file system elements;
- encryption of critical data stored in databases;
- use of an additional layer of encryption, which is critical for data, provided that the add-on is enabled, which enforces the need to enter a passphrase when opening an application on a smartphone;
- encryption of databases.

The purpose of the article is to study the implementation of an additional encryption layer and the possibilities for implementing additional data protection on mobile devices.

2 Materials and Methods

Some sources describe the advantages of network coding with its inherent algebraic structure and the maximum stream performance achieved with the multicast transmission. With network coding, content can be requested through multiple interfaces, greatly improving the efficiency of information delivery [8].

In our opinion and according to studies of other authors, the use of dynamic methods of biometric authentication is one of the most promising methods of protecting data on mobile devices. These and other methods of preventing and eliminating cyber threats are combined into the concept of cybersecurity.

When a malefactor gets access to a device, there is a threat of leakage of important information during the entire period of interaction.

Modern biometric authentication is based on two methods [3]:

- the static authentication method, which is based on recognizing the physical parameters of a person: fingerprints, distinctive characteristics of the iris, drawing of the eye retina, thermogram, face geometry, hand geometry, or even a fragment of the genetic code;
- the dynamic authentication method, which is based on the analysis of a user's behavior’s features that appear in the process of performing everyday activities, such as signature, keyboard handwriting, voice, and others.

Biometric authentication cannot guarantee absolute accuracy when identifying a user. Despite that, users' biometric characteristics will continue playing the main role in authentication, until a strong theoretical basis and a sufficient amount of practical usage experience is obtained for other authentication mechanisms, for instance, the algorithms based on post-quantum cryptosystems [2,4]. Another crucial obstacle to using such alternative mechanisms is that the problem of encryption key leakage doesn't have a generalized description [9]. Therefore, it is overcome with local solutions countering access to secret databases, for example, through the development of "evil" IBE schemes. A comparison of existing methods is presented in Table 1.

Table 1. Comparison of biometric authentication methods.

Biometric authentication method	FAR (false acceptance rate)	FRR (false reject rate)	Falsification	User comfort	Cost
Fingerprint	0,001%	0,6%	Possible	Average	Low
Face recognition 2D	0,1%	2,5%	Possible	Average	Average
Face recognition 3D	0,0005%	0,1%	Problematic	Average, lower than average	High
Iris	0,00001%	0,016%	Impossible	High	High
Retina	0,0001%	0,4%	Impossible	Low	High
Palm veins	0,0008%	0,01%	Impossible	Average	Average
Voice	0,75%	0,75%	Possible	Average	Low
Keyboard handwriting	0.01%	0,01%	Possible	High	Low

The provided comparison shows that biometric authentication methods are suitable for the implementation of an intermediate protection layer for mobile applications.

There are two main mathematical approaches to solving the problem of recognizing the keyboard handwriting of a device user:

- probabilistic-statistical;
- based on neural network algorithms.

Classic statistical approaches to user identification by keystroke handwriting are not able to provide reliable continuous user recognition. Also, statistical methods for recognizing keyboard handwriting are based on the fact that the input values are subject to the normal distribution law, although the incoming data stream does not always correspond to such a distribution.

According to the studies [5], key holding time - at a small sampling step - is described by the intersection of two normal distributions. As a result, large errors occur when calculating a user's reference characteristics.

The approach based on neural networks helps solve some problems that arise when using standard statistical methods for processing the input data stream. Analysis of such

deep learning models as recurrent neural networks, deep neural networks, bounded Boltzmann machines, deep belief networks, convolutional neural networks, deep Boltzmann machines, and deep autoencoders raises the question of studying performance in two categories of classification: binary and multiclass [10]. The ability to filter random noise is one of the important neural networks' properties. It makes them preferable to algorithms for smoothing the experimental dependencies, which are used for statistical data processing. However, the use of methods based on trained neural networks causes new problems:

- undefined length of the learning process, the appearance of dead ends, and the state of "paralysis" of the neural network;
- training for all possible "alien" users (it is impossible to form a representative training sample for all possible "alien");
- it is impossible to solve the problem with a given error by training a network for a specified period.

In our opinion, the third approach, based on the construction of nonlinear dynamic models, is optimal. This approach is largely based on the ideas and methods of nonlinear dynamics. The construction of nonlinear dynamic models will not be problematic, provided that there is a sufficient amount of guaranteed true information about the real system, which makes it possible to define the fundamental relations and obtain the necessary equations.

The probability of correct user recognition with established keyboard skills is 98%, which satisfies the successful practical applicability of such systems completely [6].

Figure 1 depicts the principle of operation of the biometric user authentication system with the integration of technologies for active deception of intruders when managing IoT devices (see Fig. 1).

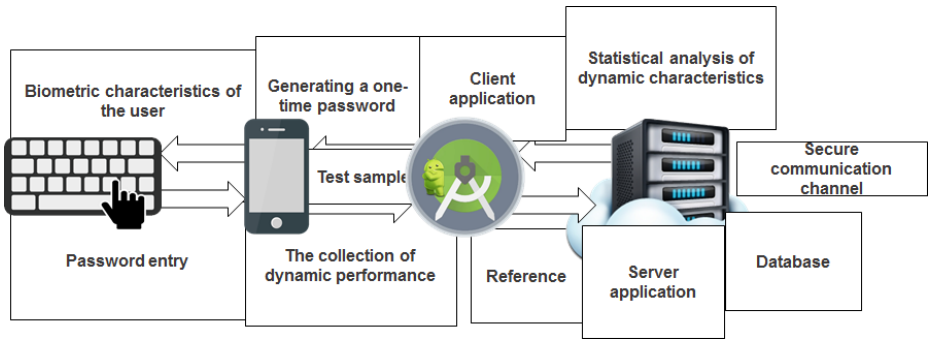

Fig. 1. The principle of operation of the biometric user authentication system with integration of technologies for active deception of intruders, when managing IoT devices.

The results of the study make it possible to highlight the following advantages of using biometric authentication methods in mobile devices in general and in mobile applications in particular:

- no additional equipment required;
- no additional user skills or actions required;
- the possibility of hidden authentication is provided. A user may not even be aware of the fact that additional verification is enabled, thus he will not be able to inform the attacker about it.

User recognition efficiency based on dynamic methods of biometric user authentication reaches 92.14%.

3 Results

An application prototype for the Android operating system has been created. The main stages of the application are shown in the figure (see Fig. 2).

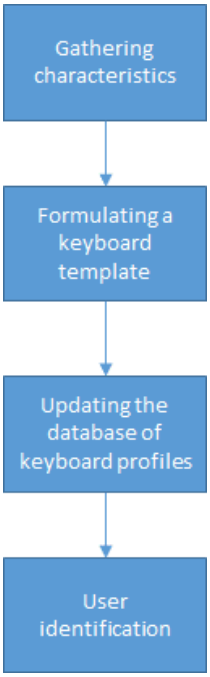

Fig. 2. Application stages.

The stage of collecting characteristics/training includes obtaining the values of the parameters described above. The creating of a keyboard template includes the analysis of the obtained parameter values and the formation of a reference template, with which the values obtained when trying to log into the system will be compared in the future.

Updating the database of keyboard profiles consists of updating the templates stored in the database. User identification is confirmation of a user's identity and then obtain-

ing permission or denying access. The developed application is intended for the continuous collection of information about keystrokes in Russian / English and the identification of an authorized or unauthorized user. The system implements a client-server architecture. There is a Java application that can read biometric data on the client side. The test sample contains the entered password and dynamic characteristics, as well as the name of the authentication profile (see Fig. 3).

Fig. 3. Application stages.

The software product implements 3 operating modes of the application and keyboard handwriting recognition:

- training;
- generating a threshold value;
- recognition.

The essence of continuous monitoring is that it can be used during authentication and after it has passed:

- monitoring all keyboard user activity. Quite resource-intensive for the solver, since the reference database requires storing the time-stamps of all characters that the user once entered;
- approach, based on frequent bigrams. Less resource-intensive, as only pairs of the most common letters, are used [1]

The application builds a reference template based on one parameter - the key hold time and a given passphrase known to both the legitimate user and the attacker. Table 2 shows the results obtained.

Table 2. Testing results.

The number of iterations of entering a password phrase at the training stage	Time-parameter value for symbol "r", ms	Time-parameter value for symbol "f", ms	Time-parameter value for symbol "n", ms	Time-parameter value for symbol "e", ms	Time parameter value for symbol "c", ms
20	User1: 80.5	User1: 75	User1: 97	User1: 79	User1: 60
	User2: 89	User2: 94.5	User2: 96.4	User2: 87.5	User2: 86.5
40	User1: 86	User1: 96	User1: 84	User1: 87.5	User1: 88.5
	User2: 102	User2: 101	User2: 88.5	User2: 86	User2: 78
60	User1: 85	User1: 83.5	User1: 91.5	User1: 92	User1: 69.5
	User2: 95	User2: 80.5	User2: 81.5	User2: 90.5	User2: 103.5

Based on the information presented in Table 2, the following conclusions are reached:

- not a single value of the parameter of the reference template of keyboard handwriting coincided among users, therefore, it can be concluded that each person has his unique keyboard handwriting;
- for the first test of the system, the smallest difference is observed for holding the "n" key (0.6ms), the largest for the "f" key (19.5ms);
- for the second test of the system, the smallest difference is observed for holding the "e" key (1.5ms), the largest for the "r" key (16ms);
- for the third test of the system, the smallest difference is observed for holding the "e" key (1.5ms), the largest difference for holding the "c" key (34ms).

Based on the test results, it can be concluded that a large percentage of errors of the first and second kind occur due to an insufficient amount of data received on the server to form a standard keyboard handwriting. It is also concluded that using a single parameter (key holding time) is not enough to form a standard keyboard handwriting. It should be noted that testing was carried out continuously for three experiments, i.e. users were entering a well-known phrase monotonously during a certain period. Since it is uncomfortable for a user, further testing should be carried out intermittently for a long period (at least for a day) to track the trend of changing the keyboard handwriting of different people over the same period. Moreover, the monotonous input of a non-changing phrase causes results distortion, which leads to the conclusion that it is more beneficial to use the input of free text for testing purposes.

Conclusion

As a result, an additional intermediate stage of protecting mobile application data is proposed. It is expected to provide efficient defense from potential intruders' attacks. The new security level has the following features:

- independence from other protection methods;
- the possibility of independent usage as the only means of organizing information security;
- the possibility of a complex application in conjunction with other tools with the help of advanced integration and interaction tools;
- the prospects of using the direction of dynamic biometric methods in conjunction with the technological development of mobile devices and wearable electronics;
- presence of infrastructure for further research.

References

1. Golub, K.: Deception of Intruders Using Traps TrapXDeceptionGrid. URL: https://www.anti-malware.ru/practice/methods/TrapX-DeceptionGrid, last accessed 2020/09/03
2. Vlasenko, A., Evsyukov, M., Putyato, M., Makaryan, A.: Research on the Implementation of Key Encapsulation Mechanisms for Post-Quantum Cryptographic Methods. Caspian journal: Management and high technologies, Astrakhan, 121-127 (2019) DOI: 10.21672/2074-1707.2019.48.4.121-127
3. Gorelic, A.: Methods of Recognition. Moscow: Higher school (1984)
4. Putyato, M., Makaryan, A.: Classification of Messengers Based on Analysis of the Security Level of Stored Data. Caspian journal: Management and high technologies, Astrakhan, 121-143 (2019) DOI: 10.21672/2074-1707.2019.48.4.135-143
5. Bragina E.K., Sokolov S.S.: Modern Methods of Biometric Authentication: Review, Analysis, and Definition of Development Prospects URL: https://cyberleninka.ru/ article/n/sovremennye-metody-biometricheskoy-autentifikatsii-obzor-analiz-i-opredelenie-perspektiv-razvitiya/viewer

6. El-Hadidi Kamal M.: Biometrics. What and how. URL: http://www.net-security.org/dl/articles/Biometrics.pdf, last accessed 2020/09/03
7. Xiong, Hu, Wu, Yan, Su, Chunhua, Yeh, Kuo-hui: A Secure and Efficient Certificates Batch Verification Scheme with Invalid Signature Identification for the Internet of Things. Journal of Information Security and Applications. Article 102507 Volume 53 August 2020 (2020) DOI: 10.1016/j.jisa.2020.102507
8. Boussaha, R., Challal, Y., Bouabdallah, A., Bessedik, M.: Optimized in-Network Authentication Against Pollution Attacks in Software-Defined-Named Data Networking. Journal of Information Security and Applications Article 102409 Volume 50 February 2020 DOI: 10.1016/j.jisa.2019.102409
9. Hou, H., Yang, B., Zhang, M., Zhou, Ya., Huang, M.: Fully Secure Wicked Identity-Based Encryption Resilient to Continual Auxiliary- Inputs Leakage. Journal of Information Security and Applications Article 102521 Volume 53 August 2020 DOI: 10.1016/j.jisa.2020.102507
10. Ferrag, M. A., Maglaras, L,. Moschoyiannis, H., Janicke S.: Deep Learning for Cybersecurity Intrusion Detection: Approaches, datasets, and comparative study. Journal of Information Security and Applications Volume 50, February 2020, 102419 DOI: 10.1016/j.jisa.2019.102409