Advances in Computer Science Research, volume 89
2019 International Conference on Wireless Communication, Network and Multimedia Engineering (WCNME 2019)

Two-factor Authentication Algorithm Implementation with Additional Security Parameter Based on Mobile Application

O. Ussatova[1,*], S. Nyssanbayeva[2] and W. Wojcik[3]
[1]Al-Farabi Kazakh National University, Almaty, Kazakhstan
[2]Institute of Information and Computational Technologies, Almaty, Kazakhstan
[3]Lublin Technical University, Poland
[*]Corresponding author

***Abstract*—The article describes the results obtained during the development of the two-factor authentication (2FA) model to protect data based on the application using your smartphone. The following example was considered - two-factor authentication using a smartphone as identifiers and one-time password generation based on the hash function of encryption standards. Software implementation was performed in the programming language JavaScript and the software implementation of the proposed algorithm was analysed.**

Keywords—two-factor authentication; data security; one-time password (OTP) generation; security methods; mobile application; smartphone

I. Introduction

The number of crimes committed in the digital environment and cases of Internet fraud is an ever-growing trend in the modern world. Online security, safety of logins, usernames and passwords are extremely important for many users.

This article discusses a two-factor authentication model based on a mobile application and authentication program.

Two-factor authentication, also known as 2FA, has become very popular in the current digital age. When choosing two different authentication channels, it is possible to protect user logins from remote attacks, the purpose of which is to use someone else's personal or identity data [1]. It requires not only a user name and password, but also the use of information that only the author knows or that will be immediately available only to the author [2]. More than 5 billion mobile devices are used in the modern world, and the use of the phone as an authentication tool helps to quickly solve the problems of enhanced protection, reduce additional costs and delays in delivery. The analysis showed that information leakage problem is relevant worldwide and the use of two-factor authentication to protect data will serve as an additional barrier for attackers. Two-factor authentication methods are considered as mechanisms to enhance the strength of authenticators.

II. Research goals and objectives

This article describes the results obtained during the development of a two-factor authentication model to protect data based on the application using a smartphone. The following studies were carried out:

- The analysis of the security procedures and information leakage;
- Developed a model of two-factor authentication based on the application using a smartphone;
- The algorithm of the application-authenticator using a smartphone for two-factor authentication and software implementation of the algorithm.

III. Ease of Use Research Analysis

In accordance with the security incident studies of Verizon's Data Breach Investigations Report (DBIR) in 2018, 95% of violations include the use of stolen personal data [3]. Standard security procedures (especially online) require the simple entry of a user name and password, and criminals can easily take possession of the user's personal data – personal and financial information – for the purpose of its further use for fraud, mainly in the field of Finance.

According to the reports of « SearchInform » company in 2018, 66% Russian companies have experienced information leakage and 70% of foreign ones [4]. A large percentage of the leakage concerns customer information and transactions, technical information, as well as personal data. One of the means of data security is password protection using the second factor.

Two-factor authentication from Infobip solves this problem with the help of SMS messages sent to a mobile phone and Voice technologies [5]. Using such message as a second authorization factor is not the safest solution. There may be problems with the authorization during foreign trips. SMS message is a payable service, which is also not quite relevant solution.

The proposed authentication method is an authenticator application that runs on a mobile device that is connected to the server. In this method the mobile device will be connected to the server by a unique MAC address of the phone. The MAC address will allow identifying the user in this system. This type of authentication is the most secure one, convenient and cost-effective to use.

IV. 2FA IMPLEMENTATION SYSTEM MODELING

The proposed authentication method is implemented using the client-server network architecture. The considered client-server application is developed on the Node.js software platform using JavaScript programming language, as well as frameworks and connected system libraries. The Node.js software platform was chosen to implement this application, as it is a server platform for JavaScript through the V8 engine. To implement the application, you need a smartphone that will display the generated one-time password to identify the user in the system. The application is designed for the Android operating system. According to statistics, 85.9 % of users are Android OS users [6], which determined its choice for the implementation of the proposed method. The scheme of the proposed method is shown in figure 1.

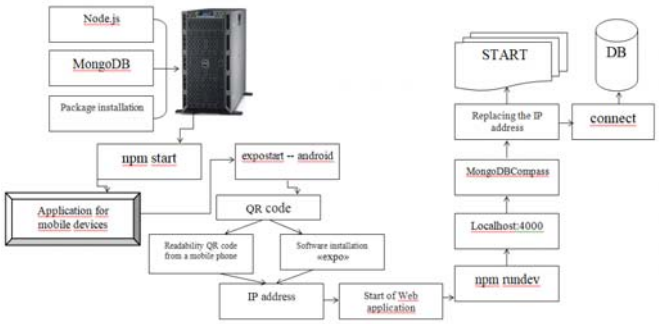

FIGURE I. SCHEME OF THE TWO-FACTOR AUTHENTICATION METHOD

The developed model is based on two types of two-factor authentication: application-authenticator and login verification using a smartphone.

To implement the system, you must use Node.js. This software platform is responsible for writing the server side in the JavaScript programming language. It also comes with an npm package manager, which is used to install various libraries and frameworks. Additionally, you need to install MongoDB-a document-oriented open source database management system that does not require a description of the table schema. When complex queries occur, they are typically resolved on the application side, making it easier to work with data and links to it. MongoDB is the most popular non-relational database. The choice of using the MongoDB database management system (DBMS) is due to the fact that this system is built quite simple scalability using sharding technology [7]. For the mobile application to work, it is necessary to read the QR code, which can be made using the installed scanner on the mobile device by default or install additional software "EXPO". To start the smartphone and personal computer, the local network is configured so that they are in the same network. Next step is - the launch of the web site to work. Next, open the console and run the command "npm rundev". This application uses "localhost: 4000". To view the database contents, use MongoDBCompass. After saving all settings, parts of the project will restart - the project is ready to work. The project works according to the algorithm described below.

V. IMPLEMENTATION SCHEME OF TWO-FACTOR AUTHENTICATION ALGORITHM

Let's consider an example of the proposed data security system using a combination of two factors: permanent and one-time temporary passwords [8]. Permanent password (the first factor) the user chooses and uses when registering an account (account). You must register in the application before automation.After that, the application is launched to enter user data (login and password), which must correspond to the registered data. Next you need to enter the application on your smartphone and enter the initial data to generate a temporary password. A temporary or one-time password is generated on the server according to a certain algorithm and is valid for a specific period of time for one authentication session [8]. The advantage of a one-time password is that the password is not reused. Generation of a temporary password is possible online. Additional software described in the system model above is used to obtain a temporary password. The software sends a request to the authorization server to generate a temporary password. A temporary password is generated on the server and displayed to the user in the optional software on the smartphone. This temporary password will have a short duration of 20 seconds. The generation of a temporary password is based on the result of the selected specific trigonometric function, which will have a number of variables. The choice of the function and its initial parameters is based on the result of the SHA256 hash function [9,10]. The input string for the hash function is a combination of user credentials, the current Greenwich mean time (GMT), and an additional secret string. A secret string is a required field that will be randomly selected from the array. The secret string will change at each input, making it much more difficult to open the initial input string, which allows you to strengthen the protection. The software implementation of the algorithm is shown in figure 2.

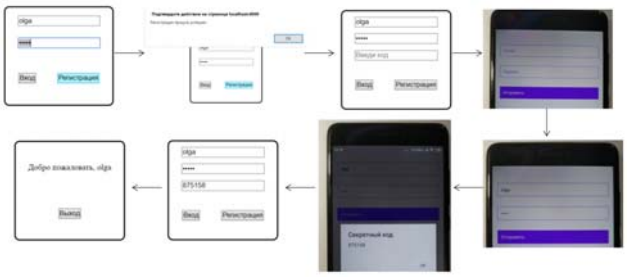

FIGURE II. SOFTWARE IMPLEMENTATION

VI. CONCLUSION

Studies show that the use of two-factor authentication can enhance the data protection. The proposed approach eliminates the existing drawback of using two-factor authentication based on SMS messages, as the proposed method uses two types of two - factor authentication: application-authenticator and login verification using a smartphone based on client-server application work. The software implementation of the proposed method shows that the algorithm works correctly and corresponds to the above beliefs.

REFERENCES

[1] Wang, D., Wang, P., Ma, C.G., Chen, Z.: iPass: Robust smart card based password authentication scheme against smart card loss problem. Cryptology ePrint Archive, Report 2012/439 (2012), full version: http://eprint.iacr.org/2012/439.pdf.

[2] Wang, D., He, D., Wang, P., Chu, C.H.: Anonymous two-factor authentication in distributed systems: Certain goals are beyond attainment. IEEE Trans. Depend. Secur. Comput. (2014), http://dx.doi.org/10.1109/TDSC.2014.2355850.

[3] Data Breach Investigations Report 2018. https://www.verizonenterprise.com/ resources/ reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf (last accessed January 10, 2019 г.).

[4] Providing information security. https://searchinform.ru/research-2018/ (last accessed January 25, 2019 г.).

[5] Two-factor authentication. https://www.infobip.com/ru/glossariy/ dvukhfaktornaya - autentifikatsiya (last accessed January 10, 2019 г.).

[6] iOS and Android already occupy 99.9% of the market for mobile operating systems. https://www.ixbt. com/news/2018/02/24/ios-android-99-9.html (last accessed January 27, 2019 г.).

[7] MySQL and MongoDB - when and what is better to use. https://habr. com/ru/ post/ 322532/ (last accessed February 02, 2019 г.).

[8] S. Nyssanbayeva, O. Ussatova "Two-factor authentication in the automated control system"//the III International scientific conference "Information Science and Applied Mathematics" - Almaty, 2018, volume No. 2, 448 -pp 239-242.

[9] National Institute of Standards and Technology (NIST) // https://www.nist.gov/ (last accessed September 02, 2018).

[10] FIPS 140-2 standard and self-encryption technology //https://www.seagate.com/files/ www-content / solutions-content / security-and-encryption / id / docs / faq-fips-sed-lr- mb-605-2-1302-ru.pdf / (last accessed November 12, 2018).