UDC 004.056.52: 004.942 **doi:** https://doi.org/10.20998/2522-9052.2022.2.02

Bohdan Rezanov, Heorhii Kuchuk

National Technical University "Kharkiv Polytechnic Institute, Kharkiv, Ukraine

MODELING THE PROCESS OF TWO-FACTOR AUTHENTICATION

Abstract. **The relevance of research.** Authentication is the process of confirming the authenticity of an object or subject of interaction in an information network by a presented identifier. Usually only one factor is used. However, most information security incidents occur due to the use of one factor. The easiest way to create an extra layer of security for accounts is to use two-factor authentication using 2FA programs. In this case, an additional step occurs, which increases the user authentication time and creates an additional load on the network. Thus, there is a need to create an additional layer of security for accounts in the "Active Directory" directory service without using an additional component on the target system and an additional step in the authentication process, thereby making the authentication process itself simpler and more responsive to the user. **The purpose of the article** is to develop a model of the two-factor authentication process, which will allow comparison of different approaches to its implementation. **Research progress**. The proposed model consists of three components: a system submodel, a threat submodel, and a security properties submodel. The analysis performed showed the advantages of using the PERT method for this problem. The simulation of the authentication process was carried out using a third-party service for checking the second factor (DUO) and the proposed method. The final PERT-diagrams are formed. A comparative analysis of these methods in terms of authentication speed was carried out. **Conclusion.** The developed model makes it possible to assess the quality of two-factor authentication by the selected parameter with a sufficient degree of accuracy. In particular, the proposed method showed more preferable results in terms of authentication speed compared to conventional methods.

Keywords: authentication, 2FA program, model, PERT method.

Introduction

Information security tools used by companies include authentication, identification, authorization, integrity checking. They are designed to protect legitimate users of the information system from illegal actions of intruders.

Authentication is the process of confirming the authenticity of an object or subject of interaction in an information network by a presented identifier. The main authentication method is single factor authentication. However, in a number of studies [1-4] it is noted that most incidents in the field of information security occur due to the use of one factor.

Studies have shown that the easiest way to create an additional layer of security for accounts is to use two-factor authentication [5-10]. The main types of two-factor authentication are:

- one-time passwords on paper (printable set of codes);
- sending a temporary code to an e-mail address;
- sending one-time password via SMS;
- OTP tokens (hardware one-time password generators);
- 2FA programs (Authenticator class applications).

A promising view is the use of 2FA programs, since it is possible to individually adjust the time interval for generating one-time passwords. For authentication and authorization of users, as a rule. directory service is used. A directory service is a network service that identifies all network resources and makes them available to users. The directory service centrally stores all the information required to use and manage these objects, simplifying the process of finding and managing these resources [11]. Examples of such services are Samba server, FreeIPA, Apache Directory Server, OpenLDAP, 389 Directory Server, Active Directory.

The Active Directory – directory service, unlike those listed above, is secure, distributed, segmented and replicated, which allows for simplified administration, scalability, support for open standards, and support for standard name formats [12]. This directory service uses LDAP [13], Kerberos [14] authentication protocols. Based on the RFC of these protocols, despite the security of the protocols themselves, they do not ensure the security of the authentication process itself on the part of the user, they do not support two-factor authentication, since authentication through these protocols occurs using one factor.

However, there are solutions to integrate the second factor into such directory services using third-party components on systems where authentication is required. An example of such solutions are the developments of Duo, Okta.

The works [15, 16] describe the authentication process using a third-party component. It is worth paying attention to the fact that in this approach, there is an additional step during authentication, which complicates the process. This increases the user authentication time and creates an additional load on the network.

Thus, there is a need to create an additional layer of security for accounts in the Active directory service without using an additional component in the target system and an additional step in the authentication process, thereby making the authentication process itself simpler and more responsive to the user. To solve this problem, it is necessary to resort to design, the initial stage of which is the development of a model. The model will allow us to study at each stage the effectiveness of the integration of two-factor authentication into authentication services with centralized user databases and evaluate the effectiveness of the work as a whole and at individual stages.

Therefore, **the purpose of this article** is to develop a model of the two-factor authentication process, which

will allow us to compare different approaches to its implementation.

At the first stage of research, a modeling method was chosen, at the second stage, a model of a standard authentication process based on the PERT method was developed, at the third stage, the proposed method was modeled.

At the final stage, using the developed model, a comparative analysis of these methods in terms of authentication speed was carried out.

Main material

1. Choice of modeling method. The security model should consist of three components [17]:

system sub-model that clearly defines the system of interest in order to understand how it behaves during operation, as well as unintentional changes in operating conditions;

threat sub-model to clearly define the computing resources of attackers and their ability to access the system;

sub-model of security properties, in which properties must be clearly defined to prevent malicious actions.

There are many methods and approaches to modeling various systems. To model our system, the following methods were considered.

GERT (*Graphical Evaluation and Review Technique*) is an alternative probabilistic method for network planning. The method is used in the organization of work, its main principle is that subsequent tasks can begin after the completion of only a certain number of previous tasks. However, not all tasks presented on the network model must be completed to complete the project.

CPM (*Critical path method*) is a method based on determining the longest sequence of tasks from the beginning of the project to its completion, taking into account all the relationships of the project, which is called the critical path. Tasks that lie on the critical path (*critical tasks*) have zero lead time, and if their duration changes, the timing of the entire project changes. For other tasks, a possible reserve of time is calculated.

PERT (*Program Evaluation and Review Technique*) is a project evaluation and analysis method used in project management. The method is aimed at analyzing the time required to complete each individual task. It also determines the minimum time required to complete the entire project.

In the PERT method, projects are viewed as a network of individual events and activities. Work in them is any element of the project that takes time to complete, and which can suspend the start of other work. The method is based on the idea of determining and controlling the probable terms of the critical path of the entire complex of works (or a probabilistic approach using the average value of the β-distribution). The PERT method allows for possible fluctuations in the timing of each operation and analyzes their impact on the completion of the project as a whole.

Benefits of the PERT method:

- provides a graphical representation of the project and its main activities;
- allows you to set the duration range for each activity;
- makes it possible to obtain information about the expected completion time of the project, provides an estimate of the probability of completing the project before the specified date;
- identifies activities that have slack time and therefore their delay will not affect the duration of the project as a whole;
- identifies activities on the critical path that need close monitoring, as they affect the overall time to complete the project [18].

Using the PERT method, one can analyze the time required to complete each individual task and determine the minimum time required to complete the entire project [19].

Disadvantages of the PERT method:

- human factor, subjective analysis and inaccurate estimates may affect the timing;
- updating and maintaining the calendar requires a lot of time and money;
- complexity of management, there is no guarantee that the schedule will remain the same throughout the project.

The GERT method [20] is an alternative probabilistic method for network planning. The basis of the application of the GERT method is the use of alternative networks, called GERT networks. These networks can adequately define complex production processes in cases where it is difficult to clearly define what work and in what order must be done to achieve the goal of the project.

The basis of the application of the GERT method is the use of alternative networks, called GERT networks in terms of this method.

They allow you to more adequately set complex project processes in cases where it is difficult or impossible (for objective reasons) to unambiguously determine what kind of work and in what sequence should be performed to achieve the intended result (i.e. there is a multivariant implementation of the project).

The GERT-based modeling method is based on the use of weights, and is especially useful in work organization cases where subsequent tasks can start after only a certain number of predecessor tasks have completed. One of the significant disadvantages of GERT networks is their high computational complexity [21, 22]. Given that for the system being developed, the process that needs to be modeled has a clear sequence, we can give preference to the PERT method.

2. Modeling the Authentication Process. Let's simulate the authentication process using a third-party second factor verification service (DUO). A general view of the process in the form of a diagram is presented in Fig. 1.

The following steps are performed (Fig. 1):

1) user enters login, password, OTP into the user system (Windows);

2) user system (Windows) sends the user's login and password to Active Directory for verification;

3) Active Directory returns a response to the user system (Windows);

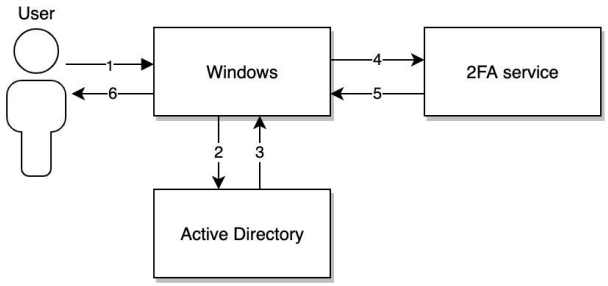

Fig. 1. Standard scheme of the authentication process using a third-party second factor verification service

4) user system, with a satisfactory response, sends the user's login and OTP for verification to the second factor verification service (DUO);

5) second factor check service returns a response to the user system (Windows);

6) user system (Windows) with a satisfactory response grants access to the user.

PERT chart consists of separate typical blocks (Fig. 2). Each block contains seven sections with such information about the task [12]:

- in the Master password generator section, the number or name of the task is displayed;

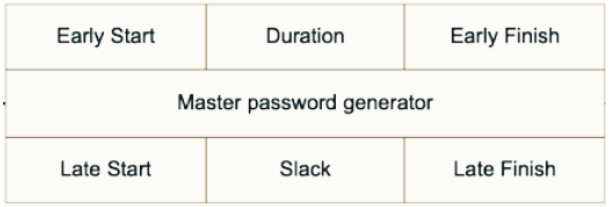

Fig. 2. View of a typical block of PERT charts

- Early Start section displays the earliest start, the earliest start date for the task;
- Duration section displays the duration of the task, calculated using the PERT method;
- in the Early Finish section, the earliest finish, the earliest deadline for completing the task, is displayed;
- in the Late Finish section, the late finish is displayed, the latest deadline for completing the task;
- Slack section shows the amount of time left to complete the task without affecting the end date of the project;
- in the Late Start section, the late start is displayed, the latest start date for the task.

An example of a PERT diagram for the considered process is shown in Fig. 3.

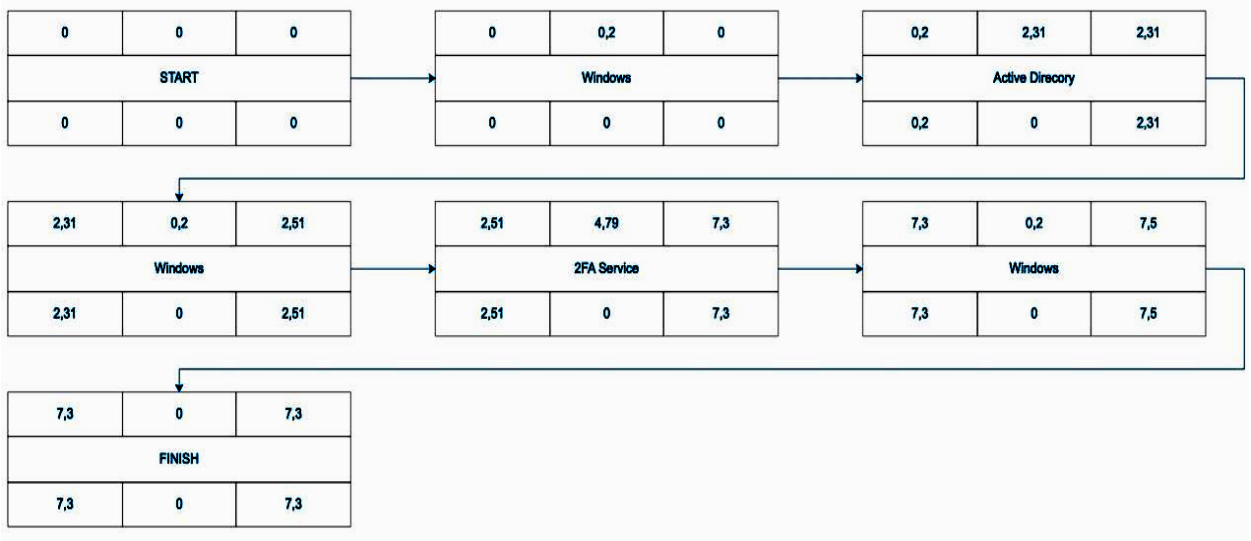

Fig. 3. An example of a PERT diagram of the authentication process using a third-party second factor verification service

3. Suggested method. Consider the proposed approach to the authentication process using a third-party service for checking the second factor. A sequence of actions is proposed, shown in Fig. 4.

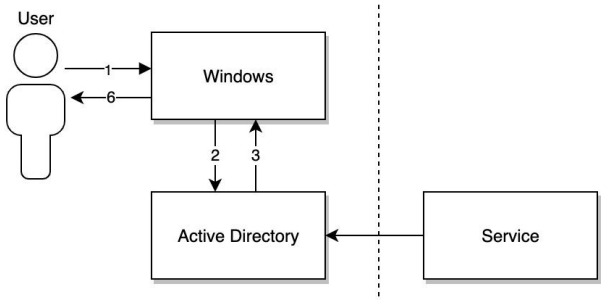

Fig. 4. Proposed Scheme for the Authentication Process

The proposed method performs the following actions (Fig. 4):

1) user enters the login, password, OTP into the user system (Windows)

2) user system (Windows) sends the user's login and password to Active Directory for verification

3) Active Directory returns a response to the user system (Windows)

4) user system (Windows) if the answer is satisfactory, the system grants access to the user

Note that the operations

Service –> Active Directory

does not affect the user authentication process.

An example of a PERT chart based on this process is shown in Fig. 5.

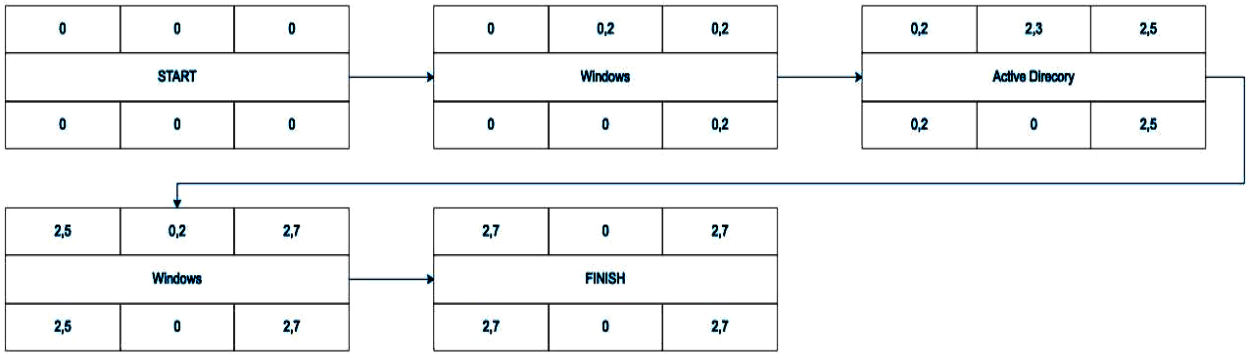

Fig. 5. Example PERT Diagram for the Proposed Authentication Process Method

4. Case study. To compare services, you need to test the authentication speed.

The following stand was prepared for testing. Oracle VM VirtualBox was taken as the basis for virtualization. For the server part, Windows Server 2019 is used, as well as Active Directory, a Microsoft directory service for operating systems of the Windows Server family.

For the client part, Windows 10 is used, an operating system for personal computers and workstations developed by Microsoft as part of the Windows NT family.

Test bench host machine: CPU 6-Core Intel Core i7, 2.2 GHz; RAM 16GB 2400Mhz DDR4; SSD 256 GB RAM; LAN 1GBps; Internet 1GBps.

Test bench virtual machines: Windows Server 2019 (CPU 4 Core; RAM 8GB; Drive 64GB; LAN 1GBps); Windows 10 (CPU 2 Core; RAM 4GB; Drive 64GB; LAN 1GBps).

Communication between virtual machines is provided through a bridge connection with the host machine.

The difference between the compared systems is that in the case of DUO, it is necessary to install an additional component in the client part, Winlogon is a component of Microsoft Windows operating systems that is responsible for processing the sequence of safe attention, loading the user profile at logon and, if necessary, locking the computer when the splash screen is running (another authentication step is required).

The actual retrieval and validation of user credentials is left to other components.

No additional components are needed for the developed system.

Testing will be done with a base of 1000 users. Before testing, 1000 accounts were created in Active Directory, 1000 accounts were created in the DUO system and 1000 TOTP tokens were issued.

The results of authentication testing using the second factor verification service are shown in Table 1 and Fig. 6.

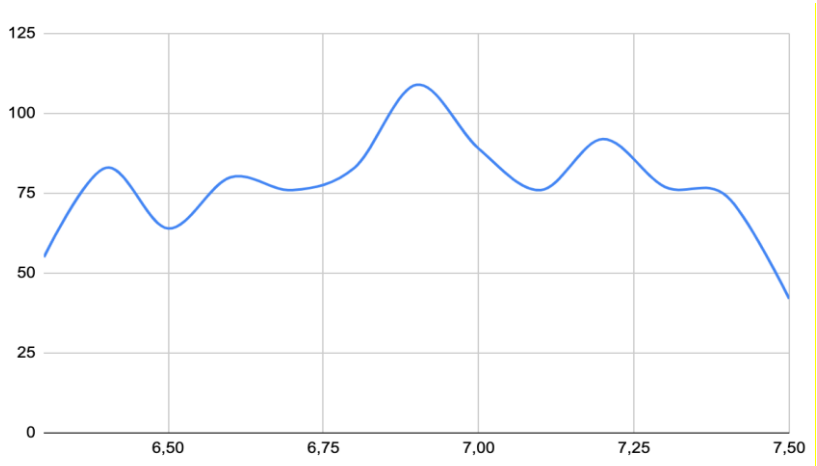

Fig. 6. Test results (standard method)

Table 1 – **Testing the Standard Method**

Time	6,3	6,4	6,5	6,6	6,7	6,8	6,9
Frequency	55	83	64	80	76	83	109
Time	7	7,1	7,2	7,3	7,4	7,5	
Frequency	89	76	92	77	74	42	

The table shows that the minimum time to complete the login operation with this approach is 6.3 s.

The maximum is 7.5 s., And the average authentication time is 6.9 s.

The results of authentication testing using the proposed method are given in Table 2.

Authentication testing results using the developed system:

Table 2 – **Testing the proposed method**

Time	2,1	2,2	2,3	2,4	2,5	2,6
Frequency	56	96	123	118	93	100
Time	2,7	2,8	2,9	3,0	3,1	
Frequency	91	95	88	95	45	

From the obtained results, it follows that the minimum time to complete the login operation is 2.1 s., the maximum is 3.1 s., and the average authentication time is 2.6 s.

Let's combine the data of tables 1 and 2 on one diagram (Fig. 7, blue color on the left - Table 1, red color on the right – Table 2).

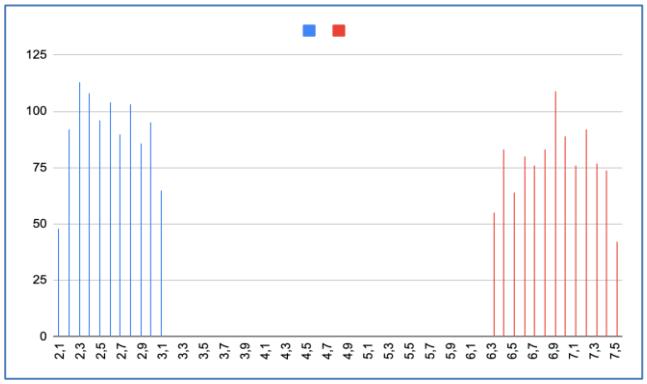

Fig. 7. Authentication Time Analysis

From the diagram in Fig. 7, it is obvious that the proposed method in terms of the proposed parameter is significantly more efficient than the standard one (almost 3 times).

Conclusions

The article presents a model of the two-factor authentication process, which made it possible to compare different approaches to its implementation. The proposed model consists of three components: a system submodel, a threat submodel, and a security properties submodel.

The analysis performed showed the advantages of using the PERT method for this problem. The developed model made it possible to assess the quality of two-factor authentication by the selected parameter with a sufficient degree of accuracy.

In particular, the simulation of the authentication process was carried out using a third-party second factor verification service (DUO) and the proposed method.

The final PERT-diagrams are formed. A comparative analysis of these methods in terms of authentication speed was carried out.

The proposed method showed more preferable results in terms of authentication speed compared to conventional methods.

REFERENCES

1. (2021), *Two-factor authentication*, available at: http://www.aladdin- rd.ru/solutions/authentication.
2. (2021), *Setting up two-factor authentication*, available at: http://support.citrix.com/proddocs/topic/web-interface- imping-ton/nl/ru/wi-configure-two-factor-authentication- gransden.html?locale=ru.
3. (2020), *Seven Methods for Two-Factor Authentication*, available at: http://www.infosecurityrussia.ru/news/29947.
4. (2020), *Two-factor authentication for remote access*, available at: http://itc.ua/articles/dvuhfaktornaya_autentif-ikaciya_pri_udalen nom_dostupe_23166.
5. Evseev S.P. and Korol, O.G. (2014), "Study of two-factor authentication methods", *Information processing systems*, No. 2(118). pp. 81–87.
6. Belov, V.N. and Pushkova, K.S. (2017), "User account protection in modern gadgets", *Scientific trends: Issues of exact and technical sciences*, 12 MC, MOAN, St. Petersburg, pp. 8-9.
7. Uskova, S.I. and Kamshilov, S.G. (2018), "Ensuring information security in the interaction of business entities with banking structures", *XVII All-Russian Scientific and Practical Conference of Students, Postgraduates and Young Scientists*, ChGU, Chelyabinsk, Vol. 2, pp. 190-195.
8. Claudia, Ziegler, Acemyan, Philip, Kortum, Jeffrey, Xiong and Dan S., Wallach (2018), "2FA Might Be Secure, But It's Not Usable: A Summative Usability Assessment of Google's Two-factor Authentication (2FA) Methods", *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Vol 62, Issue 1, DOI: https://doi.org/10.1177/1541931218621262.
9. (2020), *Methods Departments of Psychological Sciences1 and Computer Science*, Rice University 6100 Main Street, MS-25, Houston, Texas 77005, USA.
10. Kulikova, O.V. (2010), "Methods and means of authentication in the tasks of ensuring information security in corporate information systems", *Information technology security*, Volume 17, No. 3, pp. 85-91.
11. Ivanova, A.S. and Gazizov ,A.R. (2018), "Methods of authentication and identification of information systems of educational organizations" *Scientific vector*, Issue 4.
12. Chizhikov, Dmitry (2021), "Lecture 1: Introduction to Active Directory", *Microsoft Active Directory Implementation Methodology*, available at: https://intuit.ru/studies/courses/1068/259/lecture/6608.
13. (2015), "Directory Service", *Information system administrator functions*, available at: https://helpiks.org/5-87570.html.
14. Sermersheim, J. (2006), *Lightweight Directory Access Protocol (LDAP)*: The Protocol, Ed. Novell, Inc., June 2006.
15. (2021), *RFC4120*, available at: https://datatracker.ietf.org/doc/html/rfc4120.
16. Derek, Simmel and Shane, Filus (2017), "Flexible Enforcement of Multi-factor Authentication with SSH via Linux-PAM for Federated Identity Users", *PEARC17: Proceedings of the Practice and Experience in Advanced Research Computing 2017 on Sustainability, Success and ImpactJuly 2017*, Article 10, pp. 1–9, DOI: https://doi.org/10.1145/3093338.3093392.
17. Wenyi, Liu, Selcuk Uluagac, A. and Raheem, Beyah (2020), "MACA: A Privacy-Preserving Multi-factor Cloud Authentication System Utilizing Big Data", *The School of ECE Georgia Institute of Technology Atlanta*, GT CAP Group, GA 30332, USA, available at: https://cap.ece.gatech.edu/papers/1569883983.pdf.
18. Jason, Bau and John C., Mitchell (2011), "Security Modeling and Analysis", IEEE Security & Privacy, May-June 2011, Vol. 9, Is. 3, hh. 18-25, DOI: https://doi.org/10.1109/MSP.2011.2.
19. Fridlyanov, M.A. (2017), "Methods and techniques of project management in the sphere of industrial production", *Problems of market economy*, No. 3, pp. 17–24.
20. Murtuzov, G.A. (2020), "Methods for determining the timing of construction", *Alley of Science*, No. 5 (44), available at: https://alley-science.ru/domains_data/files/4May2020/METODY%20OPREDELENIYa%20SROKOV%20STROITELSTVA.pdf

21. Antonova, A.S. and Aksenov, K.A. (2014), “Comparative analysis of subcontracting work planning methods”, *Modern problems of science and education*, No. 3, pp. 88-97, available at: https://science-education.ru/ru/article/view?id=13388.
22. Panfilova, T.A. (2017), *Stochastic adaptive algorithms for improving software*, diss … cand. tech. sciences: 05.13.01 Krasnoyarsk, 160 p.
23. (2021), *Method GERT*, available at: http://www.topknowledge.ru/investmen/3187-metod-gert.html&sa=D&source=docs&ust=1638475515309000&usg=AOvVaw1Yhcjwrn-h7852e944lhZR

Received (Надійшла) 19.03.2022
Accepted for publication (Прийнята до друку) 25.05.2022

ABOUT THE AUTHORS / ВІДОМОСТІ ПРО АВТОРІВ

Резанов Богдан Михайлович – аспірант, кафедра комп’ютерної інженерії та програмування, Національний технічний університет “Харківський політехнічний інститут”, Харків, Україна;
Bohdan Rezanov – PhD Student of Computer Engineering and Programming Department, National Technical University «Kharkiv Polytechnic Institute», Kharkiv, Ukraine;
e-mail: brezanov@gmail.com, ORCID ID: http://orcid.org/0000-0002-4113-8781.

Кучук Георгій Анатолійович – доктор технічних наук, професор, професор кафедри комп’ютерної інженерії та програмування, Національний технічний університет “Харківський політехнічний інститут”, Харків, Україна;
Heorhii Kuchuk – Doctor of Technical Sciences, Professor, Professor of Computer Engineering and Programming Department, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine;
e-mail: kuchuk56@ukr.net; ORCID ID: http://orcid.org/0000-0002-2862-438X.

Моделювання процесу двофакторної автентифікації

Б. М. Резанов, Г. А. Кучук

Анотація. Актуальність дослідження. Автентифікація – процес підтвердження справжності об'єкта або суб'єкта взаємодії в інформаційній мережі за пред'явленим ідентифікатором. Зазвичай при цьому використовується один чинник. Проте, більшість інцидентів у сфері інформаційної безпеки трапляються внаслідок використання одного фактору. Найбільш простим способом створити додатковий рівень безпеки для облікових записів є використання двофакторної автентифікації з використанням 2FA-програм. При цьому виникає додатковий крок, який збільшує час автентифікації користувача, створює додаткове навантаження на мережу. Таким чином, виникає необхідність створити додатковий рівень безпеки для облікових записів у службі каталогів Active directory без використання додаткового компонента в цільовій системі і додаткового етапу в процесі аутентифікації, тим самим роблячи сам процес аутентифікації більш простим і доступним для користувача. **Метою статті** є розробка моделі процесу двофакторної аутентифікації, яка дозволить провести порівняння різних підходів для його реалізації. **Хід досліджень**. Пропонована модель складається з трьох компонентів: підмодель системи, підмодель загрози та підмодель властивостей безпеки. Проведений аналіз показав переваги використання для даного завдання методу PERT. Проведено моделювання процесу аутентифікації з використанням стороннього сервісу перевірки другого фактору (DUO) та запропонованого методу. Сформовано підсумкові PERT-діаграми. Проведено порівняльний аналіз даних методів за швидкістю автентифікації. **Висновок.** Розроблена модель дозволяє з достатнім ступенем точності оцінити якість двофакторної автентифікації за вибраним параметром. Зокрема, запропонований метод показав кращі результати за швидкістю автентифікації порівняно з загальноприйнятими методами.

Ключові слова: автентифікація, 2FA-програма, модель, метод PERT.

Моделирование процесса двухфакторной аутентификации

Б. М. Резанов, Г. А. Кучук

Аннотация. Актуальность исследования. Аутентификация – процесс подтверждения подлинности объекта или субъекта взаимодействия в информационной сети по предъявленному идентификатору. Обычно при этом используется один фактор. Однако, большинство инцидентов в сфере информационной безопасности случаются вследствие использования одного фактора. Наиболее простым способом создать дополнительный уровень безопасности для учетных записей является использование двухфакторной аутентификации с использованием 2FA-программ. При этом возникает дополнительный шаг, который увеличивает время аутентификации пользователя, создает дополнительную нагрузку на сеть. Таким образом, возникает необходимость создать дополнительный уровень безопасности для учетных записей в службе каталогов Active directory без использования дополнительного компонента в целевой системе и дополнительного этапа в процессе аутентификации, тем самым делая сам процесс аутентификации более простым и отзывчивым для пользователя. **Целью статьи** является разработка модели процесса двухфакторной аутентификации, которая позволит провести сравнение различных подходов к его реализации. **Ход исследований**. Предлагаемая модель состоит из трех компонентов: подмодель системы, подмодель угрозы и подмодели свойств безопасности. Проведенный анализ показал преимущества использования для данной задачи метода PERT. Проведено моделирование процесса аутентификации с использованием стороннего сервиса проверки второго фактора (DUO) и предложенного метода. Сформированы итоговые PERT-диаграммы. Проведен сравнительный анализ данных методов по скорости аутентификации. **Вывод.** Разработанная модель позволяет с достаточной степенью точности оценить качество двухфакторной аутентификации по выбранному параметру. В частности, предложенный метод показал более предпочтительные результаты по скорости аутентификации по сравнению с общепринятыми методами.

Ключевые слова: аутентификация, 2FA-программа, модель, метод PERT.