Valeology: International Journal of Medical Anthropology and Bioethics
(ISSN 2995-4924) VOLUME 02 ISSUE 11, 2024

TEACHING METHODOLOGY FOR USING PASSWORD-BASED AUTHENTICATION IN INFORMATION SECURITY

Vohidov Dilshod Alikulovich
Assistant of Samarkand State Medical University

Abdukhalilova Sabina Farrukh qizi, Khushmurodova Gulasal Anvarbek qizi
Student of Samarkand State Medical University, 108 – group of the medical faculty

Abstract:

The main objective is to study the theoretical and practical aspects of computer security, knowledge of password protection methods, as well as the formation and development of skills and abilities to use them in practice.

Keywords: *identification, permission control, authentication, authorization, smart card, token.*

Introduction

Introduction: For the security problem associated with the management of system resources, the term "permission control" will be used as a general term. When conducting explanations related to this area, 3 main important areas are distinguished: identification, authentication and authorization.

Identification is the process of treating a person as someone. For example, when you identify yourself on the phone, you can say that you have been identified. In this case, you introduce yourself, for example, as "I am Sherzod." In this case, Bokhodir serves as your identity. Thus, identification - the identification of a subject - is the process of presenting to the system or the requesting subject. In addition, a postal address can be considered as an identifier in an e-mail system. The process of providing a postal address can be considered an identification process. In an e-mail system, a postal address is unique. It can be assumed that the user identifier is unique and cannot be repeated in the system.

Authentication is the process of verifying that a user (or party) is authorized to use a system. For example, let's take the process of using a user from a personal computer. When the user initially logs into the system, he or she enters his or her ID (i.e., user name) and through it, he or she is presented to the system (undergoes the identification process). The system then asks the user for a password to verify the identity provided. If the ID contains the appropriate password (i.e., is authenticated), the user will be able to access the computer. In other words, we can say that authentication is the process of verifying the identity of a user or entity.

Once authenticated, the user is granted access to the system resource. However, the authenticated user is not allowed to perform unnecessary actions in the system. For example, requiring that a user with authentication privileges be given the ability to install applications. So, how do you restrict the permissions of an authenticated user? These are the questions that the field of authorization deals with.

Authorization is the process of authorizing the actions that a user who has passed the authentication processes can perform in the system.

In the field of security, terms are used separately from their standardized meanings. In particular, permission control is often used as a synonym for authorization. However, in this course, permission control is considered more broadly. That is, the authorization and authentication processes are considered as parts of permission control.

Summarizing the definitions given to the above terms, the following conclusion can be drawn:

Identification - who are you?

Authentication: are you who you really are?

Authorization - do you have permission to do this?

Literature Review and Methodology: In authentication or identification processes, subjects can take the form of a person or a device (computer). That is, a person can authenticate a person, a machine can authenticate a person, or a machine can authenticate a machine. This lecture will focus on the human or machine authentication scenarios. An example of a “something you know” state is a password. On the other hand, an example of a “something you have” state is a smart card, token, remote control, or car key. The “something you have” state is usually considered as a synonym for biometrics. For example, right now you can buy a laptop and authenticate yourself through a fingerprint scanner on it.

Password is some information known only to the user and ensures the authentication process in the system. Password is a widely used parameter in the authentication process in practice. For example, we will need to enter the password required to obtain rights to use our computers. This case can also be used for mobile phones. An overview of the authentication process in a password-based state is shown in Figure 3.1.

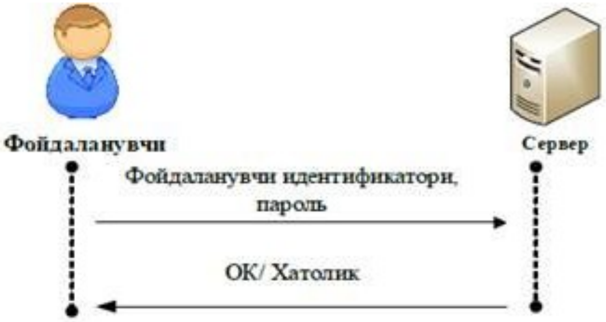

Figure 3.1. Machine and human authentication process based on password

Password-based authentication has the following features:

- ✓ easy to implement password-based authentication (low cost, easy to replace);
- ✓ the user's password usually contains information about the alocador (for example, his favorite football team, phone number, and Hack.) (123456, 12345, DM > yeg (U) and is therefore "easily identified by intruders;
- ✓ remembering complex passwords is difficult (for example, }De}(43}Yett+U);
- ✓ a widely used password-based authentication method in practice.

Smart card or token

Tokens in the form of smart cards or devices are used for authentication. A smart card is a credit card-sized device with a small amount of memory and computing capabilities. A smart card usually stores some secret size, key, or password, stores and even performs calculations. Figure 3.2 shows a special-purpose smart card and a device for reading it (a smart card reader).

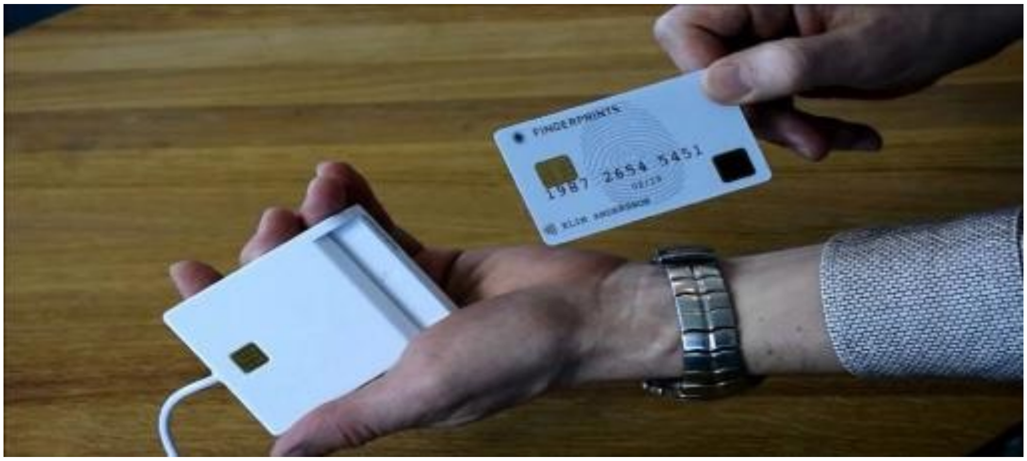

Figure 3.2. Smart card vs. smart card reader

Something-based authentication methods can be implemented in various forms. Take a password generator for example. A password generator is a small device that is used when logging into a system. Suppose Alice has a password generator and she wants to authenticate with Bob using it. To do this, Bob sends a random number k (—question—) to Alice. Alice enters the resulting number K and the PIN required to use the password generator into the password generator. The password generator, on the other hand, provides the answer to Alice, and it is passed to Bob. If the answer is correct, Alice is authenticated, otherwise she will not be able to pass. An overview of this scenario is shown in Figure 3.3.

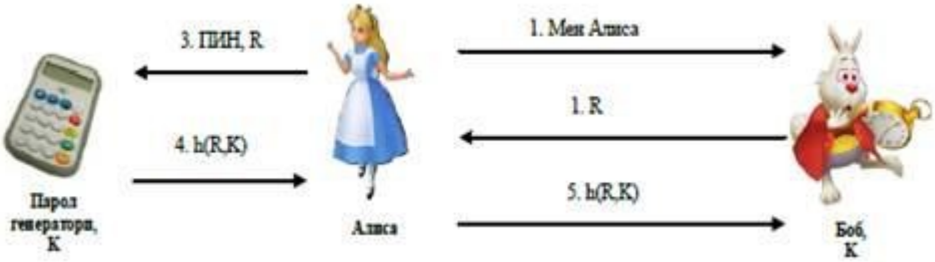

Figure 3.3. Token-based authentication process

According to the given scheme, the generator of heads and passwords must have a distributed key K. In this scheme, the question-answer mechanism was used. That is, Bob sends Alice a number R as a question and receives the corresponding answer - h(r, k). By checking the received information, Bob checks Alice for authenticity.

Smart card or authentication methods based on something you have have the following characteristics:

- smart card-based authentication does not require remembering anything;
- high cost of implementation and device (in particular, replacing a token in case of its loss is expensive);
- there is a problem with the loss of a token or smart card and burnout;
- provides a high level of security if the token is securely transferred.

Biometric-based authentication

In the biometric-based authentication method, the biometric parameter serves as a key to a person's ultrasound. There are many more biometric parameters, such as fingerprint, face image, pupil, voice, movement style, ear shape, hand shape, and hacking. In practice, the authentication method based on biometric parameters is widely used. For example, the fingerprint authentication method is widely used at the entrance doors of apartment buildings or at the entrance of organizations, and on laptops and mobile phones, it is based on face image or fingerprint authentication (Fig. 3.4).

Fingerprint Face image Pupil of the eye Voice

Figure 3.4. Examples of biometric samples

In the field of information security, biometric parameters are considered as an alternative to passwords, providing higher security. The authentication method based on biometric parameters has the following features:

- the method based on biometric parameters does not require the need to remember and carry;
- the implementation of authentication based on biometric parameters to a password
- is considered more expensive than the token-based method and cheaper than the token-based method (there are some exceptions);
- there is no way to replace the biometric parameter, that is, if the biometric parameter is fake, the authentication system is considered completely compromised for this user;
- authentication methods based on different biometric parameters are perceived by people to varying degrees.

The ideal biometric parameter for use in the field of authentication should correspond to:

- be universal - the biometric parameter is mandatory for all users;
- be different - the selected biometric parameter should be different for all people;

- property - the selected biometric parameter must remain unchanged over time;
- accumulability - the physical property must be easily accumulated.

Results: In practice, the concentration of the physical property will also depend on the person's attention to the process.

Biometric parameter is widely used not only in solving the problem of authentication, but also in identification. That is, ―who are you? can answer the question: "why?" For example, BI has fingerprint databases related to criminals. In this database, it is downloaded as a fingerprint (fingerprint image, username) and can be used to check a person for presence in the list of criminals. To do this, an image of a fingerprint is taken from the person being checked, and if it is present in the RV1 database, then the name of the person being checked matches the username corresponding to the fingerprint image.

Conclusion. If one of the parties verifies the authenticity of the other, this is called one-way authentication. If both parties authenticate each other, this is called two-way authentication. For example, when using email, only the server authenticates the user (using a password) and therefore can be called one-way authentication. However, when making electronic payments, both the server authenticates the user and the user authenticates the server. Therefore, this case can be called double authentication.

REFERENCES:

1. Вохидов, А. М., Вохидов, Д. А., Фармонова, Р. Ф., & Хафизова, Д. Ш. (2022). Разработка Графическим Пользовательским Интерфейсом-Программ В Пакете Tkinter С Использованием Современных Педагогических Технологий В Области Медицины. *Miasto Przyszłości*, *30*, 181-184.
2. Vohidov, D., Maxmudova, Z., & Sayfullayev, R. (2022). TIBBIYOT YO’NALISHIDA ZAMONAVIY PEDAGOGIK TEXNOLOGIYALARINI QO ‘LLAB TKINTER PAKETIDA GUI DASTURLARINI TUZISH. *Евразийский журнал математической теории и компьютерных наук*, *2*(12), 31-35.
3. Voxidov, A., Voxidov, D., Avazov, A., & To‘layev, A. (2023). TIBBIYOT UNIVERSITETI PEDIATRIYA FAKULTETI TALABALARI UCHUN TA'LIMDA ISHLAB CHIQISH AMALIYOTINING KONTEKST SIFATIDA TA'LIM. *Евразийский журнал академических исследований*, *3*(2 Part 4), 150-154.
4. Melitoshevich, V. A., & Alikulovich, V. D. (2023). Development by a Graphic User Interface-Programs in the Tkinter Package Using Modern Pedagogical Technologies in the Field of Medicine. *Miasto Przyszłości*, *32*, 13-17.
5. Вохидов, Д. А., Вохидов, А. М., Аминов, Ж., & Хабибжон, Л. (2023). Роль Информационных Технологий В Управлении Ресурсами Персонала Здравоохранения. *Miasto Przyszłości*, *34*, 299-305.
6. Voxidov, A. M., Malikov, M. R., Voxidov, D. A., & Nurmuxammadiyeva, L. A. (2022). Tibbiy-biologik tadqiqotlarda statistik tahlil jarayonlari. *Academic research in educational sciences*, *3*(3), 287-293.
7. Alikulovich, V. D., & Melitoshevich, V. A. (2023). Use of Interactive and Modern Pedagogical Software in the Process of Freelancing Sites in Medicine. *Eurasian Scientific Herald*, *17*, 1-6.
8. Voxidov, A. M., Malikov, M. R., & Voxidov, D. A. (2021). TIBBIYOTDA DIFFERENSIAL TENGLAMALARNI FARMATSIYA SANOATIDA QO’LANISHI. *Academic research in educational sciences*, *2*(12), 1096-1102.
9. Voxidov, D., & Voxidov, A. (2023). TIBBIYOT XODIMLARI RESURSLARINI

BOSHQARISHDA AXBOROT TEXNOLOGIYANING O ‘RNI. *Евразийский журнал медицинских и естественных наук*, *3*(3), 114-120.

10. Вохидов, Д. А., Вохидов, А. М., Аминов, Ж., & Хабибжон, Л. (2023). Роль Информационных Технологий В Управлении Ресурсами Персонала Здравоохранения. *Miasto Przyszłości*, *34*, 299-305.

11. Вохидов, Д. А., Вохидов, А. М., Хайдарова, Х. Р., & Тураева, А. Б. (2023). Ключевые Особенности Learningapps В Повышении Знаний Студентов Медицины. *Miasto Przyszłości*, *42*, 607-609.

12. Melitoshevich, V. A., Alikulovich, V. D., Janaboyevna, A. A., & Baxtiyorovna, D. S. (2024). TIBBIY-BIOLOGIK MASALALANI CHIZIQLI KORRELYATSIYA USULIDAHISOBLASH. *BARQARORLIK VA YETAKCHI TADQIQOTLAR ONLAYN ILMIY JURNALI*, *4*(4), 1-6.

13. Alikulovich, V. D., Melitoshevich, V. A., & Kizi, O. F. O. (2024). KEY FEATURES OF LEARNINGAPPS IN IMPROVING THE KNOWLEDGE OF MEDICAL STUDENTS. *Eurasian Journal of Academic Research*, *4*(3-2), 142-145.

14. Voxidov, D., Voxidov, A., & Aminov, J. (2023). MAIN FEATURES OF TRAINING APPLICATIONS IN INCREASING THE KNOWLEDGE OF MEDICINE STUDENTS. *Modern Science and Research*, *2*(12), 226-229.

15. Jaloliddin, A., & Alikulovich, V. D. (2023). TIBBIYOT YO'NALISHIDAGI TALABALARNI BILIMINI OSHIRISHDA LEARNINGAPPS NING ASOSIY XUSUSIYATLARI.

16. Вохидов, А. М., Вохидов, Д. А., & Давронова, З. М. (2023). Статистического Анализа В Медико-Биологических Исследованиях. *Miasto Przyszłości*, *42*, 232-237.

17. Voxidov, D., & Voxidov, A. (2023). PEDAGOGICAL CONDITIONS FOR EFFECTIVE DISTANCE LEARNING IN THE SYSTEM OF TRAINING OF ENVIRONMENTAL SPECIALISTS. *Modern Science and Research*, *2*(10), 436-442.

18. Вохидов, А. М., Вохидов, Д. А., Фармонова, Р. Ф., & Хафизова, Д. Ш. (2022). Разработка Графическим Пользовательским Интерфейсом-Программ В Пакете Tkinter С Использованием Современных Педагогических Технологий В Области Медицины. *Miasto Przyszłości*, *30*, 181-184.