Ensuring Information System Security by Selective Multi-factor Authentication

Margarov Gevorg I.
National Polytechnic University of Armenia, Institute of ITTE, Head of ISSD Department, Ph.D. in Technical Sciences, Professor (Yerevan, RA)
mgi@polytechnic.am
Naltakyan Narek L.
National Polytechnic University of Armenia, ITTE Institute, ISSD Chair, master's student (Charentsavan, RA)
nareknaltakyan1@gmail.com
Gishyan Vahagn A.
National Polytechnic University of Armenia, ITTE Institute, SAED, master's student (Noyemberyan, RA)
vahagn.gishyan.a@gmail.com
Seyranyan Aghasi T.
National Polytechnic University of Armenia, ITTE Institute, ISSD Chair, master's student (Hrazdan, RA)
aghasi.seyranyan@gmail.com

UDC: 004.056; **EDN:** JHMTZB;
DOI: 10.58587/18292437-2023.2-100
Keywords: security, multi-factor authentication, cybersecurity, information protection, personal information

Տեղեկատվական համակարգի անվտանգության ապահովումը ընտրովի բազմագործոն նույնականացման միջոցով

Մարգարով Գևորգ Ի.
Հայաստանի ազգային պոլիտեխնիկական համալսարան, ՏՀՏԷ ինստիտուտ, ՏԱԾԱ ամբիոնի վարիչ, տ.գ.թ, պրոֆեսոր (Երևան, ՀՀ)
mgi@polytechnic.am
Նալթակյան Նարեկ Լ.
Հայաստանի ազգային պոլիտեխնիկական համալսարան, ՏՀՏԷ ինստիտուտ, ՏԱԾԱ ամբիոն, մագիստրանտ (Չարենցավան, ՀՀ)
nareknaltakyan1@gmail.com
Գիշյան Վահագն Ա.
Հայաստանի ազգային պոլիտեխնիկական համալսարան, ՏՀՏԷ ինստիտուտ, ՍԱՈւԴ, մագիստրանտ (Նոյեմբերյան, ՀՀ)
vahagn.gishyan.a@gmail.com
Սեյրանյան Աղասի Թ.
Հայաստանի ազգային պոլիտեխնիկական համալսարան, ՏՀՏԷ ինստիտուտ, ՏԱԾԱ ամբիոն, մագիստրանտ (Հրազդան, ՀՀ)
aghasi.seyranyan@gmail.com

Ամփոփագիր. Բազմագործոն նույնականացումը (Multi-factor Authentication կամ MFA) ի հայտ է եկել որպես անվտանգության կարևոր միջոց՝ պաշտպանելու զգայուն տեղեկատվությունը և կանխելու չարտոնված մուտքը ավելի ու ավելի փոխկապակցված աշխարհում: Այս հոդվածում ներկայացրել ենք մեր կողմից մշակված բազմագործոն նույնականացման համակարգը, որը անվտանգության մեխանիզմ է, և ոչ միայն օգտատերերին առաջարկում է նույնականացման բազմաթիվ ձևեր՝ իրենց ինքնությունը ստուգելու համար, այլ կատարել այդ ամբողջը հստակ ֆիքսված հերթականությամբ, որը բարձրացնում է անվտանգության մակարդակը խոցելի կայքերում և նվազագույնի հասցնում օգտատերեի հաշիվների կորուստը: Այս գործիքակազմը իր կառուցվածքով ճկուն է, և կարող է կիրառվել ինչպես առանձին, այնպես էլ որպես ներդրված համակարգ: Առավելություններից է հանդիսանում նաև այն, որ օգտատերերը իրենք են ընտրում նույնականացման համակարգը, և դրանց հերթականությունը: Այս ամենը փոքր ինչ բարդացնում է նույնականացման գործընթացը, սակայն երաշխավորում է ապահովությունը կիբերհարձակումներից:
Հանգուցաբառեր՝ անվտանգություն, բազմագործոն վավերացում, կիբերանվտանգություն, տեղեկատվության պաշտպանություն, անձնական տվյալներ

Обеспечение безопасности информационных систем с помощью выборочной многофакторной аутентификации

Маргаров Геворг И.
Национальный политехнический университет Армении,
Институт ИТТЭ, Заведующий ИБПО Кафедрой, к. т. н., профессор (Ереван, РА)
mgi@polytechnic.am
Налтакян Нарек Л.
Национальный политехнический университет Армении,
Институт ИТТЭ, Кафедра ИБПО, магистрант (Чаренцаван, РА)
nareknaltakyan1@gmail.com
Гишян Ваагн А.
Национальный политехнический университет Армении,
Институт ИТТЭ, САУД, магистрант (Ноемберян, РА)
vahagn.gishyan.a@gmail.com
Сейранян Агаси Т.
Национальный политехнический университет Армении,
Институт ИТТЭ, Кафедра ИБПО, магистрант (Раздан, РА)
aghasi.seyranyan@gmail.com

Аннотация. Многофакторная аутентификация (MFA) стала важной мерой безопасности для защиты конфиденциальной информации и предотвращения несанкционированного доступа. В этой статье мы представили разработанную нами систему многофакторной аутентификации, которая является механизмом безопасности и не только предлагает пользователям несколько методов аутентификации для подтверждения своей личности, но и делает все это в четко определенном порядке, что повышает уровень безопасности на уязвимых веб-сайтах и сводит к минимуму потерю учетных записей. Этот инструментарий гибок по своей структуре и может использоваться как отдельно, так и как целостная система. Одним из преимуществ является то, что пользователи сами выбирают систему аутентификации. Все это немного усложняет процесс аутентификации, но гарантирует безопасность от кибератак.

Ключевые слова: безопасность, многофакторная аутентификация, кибербезопасность, защита информации, личная информация

Introduction

Computer security, cyber security, or information technology security (IT security) is the protection of computer systems, their hardware, software, or electronic data from theft, as well as from disruption or error in the services they provide [**1**]. The role of cyber security in this digital age is increasing as organizations and individuals interact more with technology and the Internet in their daily activities. The rapid growth of Internet-connected devices, digital services, and data has led to an increase in cyber threats, and as a result, the need for cybersecurity has increased. The main goal of cybercriminals is to take over the accounts or personal data of users or organizations. Currently, to avoid this problem, many people use multi-factor authentication to avoid similar attacks, but these methods also have their drawbacks and are vulnerable [**2**].

The main security components are authorization and authentication, but they are different from each other.

Authorization is the process of granting or denying access to specific resources or actions based on the identity of the authenticated user or device [**3**]. Authorization determines what a user is allowed to do or access within a system or application.

Authentication is the process of verifying the identity of a user, typically through the use of a username and password, biometric factors such as fingerprints or facial recognition, or other authentication methods such as security tokens or smart cards [**4**]. The goal of authentication is to ensure that only authorized users or devices are granted access to a system or application.

Authentication can also be used to enforce access controls, which dictate what information or systems a user is allowed to access based on their role or privileges. For example, a user with administrative privileges may be granted access to more sensitive information or systems than a regular user, and authentication can help ensure that these access controls are enforced.

Here are some of the most common authentication methods:

- Passwords: Passwords are one of the most widely used authentication methods. Users are required to enter a username and a secret password to access the system or information.
- Biometric authentication: Biometric authentication uses physical characteristics of the user, such as fingerprints, facial recognition, or iris scans, to verify their identity [**5**].

- Two-factor authentication: Two-factor authentication requires the user to provide two forms of authentication to access the system or information, such as a password and a one-time code sent to their mobile device [**6**].
- Multi-factor authentication: Multi-factor authentication requires the user to provide multiple forms of authentication, such as a password, biometric verification, and a security token [**7**].
- Smart cards: Smart cards contain a microchip that stores encrypted authentication information. Users must insert the smart card into a reader and enter a PIN to gain access.
- Security tokens: Security tokens generate a unique, one-time code that the user must enter along with their password to gain access.
- Certificate-based authentication: Certificate-based authentication uses digital certificates to verify the user's identity. The user's private key is stored securely and is used to decrypt information sent by the system.

But authentication has some common problems, such as weak passwords, identity theft, brute force attacks, authentication delays, complexity, false positives, and exploiting vulnerabilities. Overall, these authentication issues highlight the need for organizations to carefully consider their authentication methods and take steps to ensure that they use the most secure and effective methods available. These issues can compromise the security of systems and information, and organizations need to think carefully about their authentication methods to make sure they are secure and effective. To solve these problems and raise security, a new authentication system was proposed in this article.

Selective Multi-Factor Authentication Toolkit:

The article presents a selective multi-factor authentication toolkit, which can act both as a separate system, if the microservice architectural model is used, and as a functional part of the complete system, if the monolithic architectural model is used.

The working principle of the authentication algorithm consists in making a choice: the user has N number of independent and different authentication mechanisms for authentication. From the given set of mechanisms, the user must choose the M number preferred for him during registration, where M>0 && M<=N.

Authentication mechanisms.

There are two types of authentication mechanisms in the proposed toolkit:

- Static. The mechanisms by which the user must remember what he chose or entered during registration or when changing them in order to pass verification. For example: pin code, secret question, etc.
- Dynamic. Those mechanisms are connected with external providers, and a new code is generated for each verification. For example: email, sms, whatsapp.

While choosing the preferred M number of identification methods preferred, the user must also indicate their sequence, for example:

1. Sms
2. Email
3. Pin

After selecting M number of mechanisms and specifying their sequence, the user registers on the platform.

In order to enter the platform, the user must go through the verification processes by the mechanisms of his choice. After passing through each authentication mechanism, the database indicates which mechanism the given user passed through and when it was passed. [Picture 1]

	id	userid	logintype	lastlogin
1	1	1	PIN	2023-03-23 08:43:40.879000
2	2	1	EMAIL	2023-03-23 08:44:26.010000
3	3	1	QUESTION	2023-03-23 08:45:06.636000

Picture 1: *View of the table in the database after verification by authentication mechanisms*

After everything has been done correctly, the user will be allowed to enter only if he/she has passed the authentication mechanism in the correct sequence as he/she indicated during registration. Even if the user went through all the authentication mechanisms he chose correctly, but in the wrong sequence, he cannot enter the given system, because the correct sequence of the algorithm of the given toolkit is a mandatory condition.

The mandatory condition in the form of a code looks like this [Picture 2]. In this code, it is clearly defined that the user must have gone through the authentication mechanisms chosen by him and in the correct sequence, the code part userLoginTypesService.checkUserLoginFlow(user) is responsible for this, which, by reading the information in the database, decides whether the user is authorized to enter the system or not.

```java
@Override
public ResponseEntity<AccessTokenDto> authenticate(final AuthenticationRequest request) throws Exception
{
    var principal = request.getUsername();
    var credentials = request.getPassword();
    final User user = userService.findByUsername(principal).orElseThrow();
    if (!userLoginTypesService.checkUserLoginFlow(user))
    {
        throw new InvalidLoginFlow();
    }
    authenticationManager.authenticate(new UsernamePasswordAuthenticationToken(principal, credentials));
    log.debug("Login successful");
    final String token = jwtTokenUtil.generateToken(createJwtUser(user));
    final var accessTokenDto = createAccessToken(user, includeRefreshToken: false, token);
    userService.updateLastLogin(user.getId());
    return ResponseEntity.ok(accessTokenDto);
}
```

Picture 2: *code snippet in the java programming language*

Advantages and disadvantages of the method

Some of the advantages and disadvantages of the method are listed below:

Advantages:

Improved Security: Authentication can help to improve security by ensuring that only authorized users or devices are granted access to sensitive information or systems.

Protection Against Cyber Attacks: By requiring users to authenticate themselves before accessing a system or application, authentication can help protect against cyberattacks such as hacking and phishing.

Reduced Risk of Insider Threats: Authentication can help to reduce the risk of insider threats by ensuring that employees only have access to the information or systems that they need to do their jobs.

Disadvantages:

Cost: Implementing authentication mechanisms can be costly, particularly if an organization is using advanced authentication methods such as biometric authentication.

Complexity: Authentication can add complexity to the user experience, particularly if multiple forms of authentication are required.

User Resistance: Some users may be resistant to the additional steps required for authentication, such as having to remember a complex password or using a security token.

Conclusion

Multi-factor authentication (MFA) has become an integral part of social platforms and many websites on the Internet. The article briefly presents its main problems and their possible consequences. A new multi-factor authentication system has been developed, which guarantees the safety of important information on the Internet. The advantage of the mechanism lies in the fact that in the event of an attack or failure of any security mechanism, other openers continue to function and ensure data confidentiality. The results of preliminary tests of the system are available in the article.

References

1. **Schatz, Daniel; Bashroush, Rabih; Wall, Julie** (2017). "Towards a More Representative Definition of Cyber Security". Journal of Digital Forensics, Security and Law. 12 (2). ISSN 1558-7215.
2. **Haider Mehraj, D. Jayadevappa, Sulaima Lebbe Abdul Haleem, Rehana Parveen, Abhishek Madduri, Maruthi Rohit Ayyagari, Dharmesh Dhabliya**, Protection motivation theory using multi-factor authentication for providing security over social networking sites : Pattern Recognition Letters Volume 152, December 2021, Pages 218-224
3. **Fraser, B.** (1997), RFC 2196 – Site Security Handbook, IETF
4. "What is Authentication? Definition of Authentication, Authentication Meaning". The Economic Times. Retrieved 2020-11-15.
5. **Brocardo ML, Traore I, Woungang I, Obaidat MS.** "Authorship verification using deep belief network systems Archived 2017-03-22 at the Wayback Machine". Int J Commun Syst. 2017. doi:10.1002/dac.3259
6. **Turner, Dawn M.** "Digital Authentication: The Basics". Cryptomathic. Archived from the original on 14 August 2016. Retrieved 9 August 2016.
7. European Central Bank. "Recommendations for the Security of Internet Payments" (PDF). European Central Bank. Archived (PDF) from the original on 6 November 2016. Retrieved 9 August 2016.

Сдана/Հանձնվել է 04.03.2023
Рецензирована/Գրախոսվել է 10.04.2023
Принята/Ընդունվել է 17.04.202