THE NECESSITY AND BENEFIT OF MULTI FACTOR AUTHENTICATION

Rajabboyeva Surayyo Baxrom qizi
Xalmuratov Omonboy Utamuratovich
Trainee-teacher of UbTUIT, surayyobaxromqizi@gmail.com
Deputy direktor of UbTUIT, omonboyx@gmail.com
https://doi.org/10.5281/zenodo.7882398

Abstract: One of the safest authentication techniques is multifactor authentication (MFA). It includes a wide variety of subjects in a cyber-connected environment, including control of access rights, communications, and online payments. Due to the extra step the user must do, multifactor authentication is typically a little difficult. With two-factor authentication, in addition to the user ID and password, the user must also enter a unique code, often sent to them through SMS or one they have already obtained. This essay will discuss the idea of MFA, the main distinctions between MFA and two-factor authentication (2FA), the advantages of MFA, and the need of using it

Keywords: Security, Multi Factor, Authentication, Tokens, Security Protocols.

INTRODUCTION

Since ancient times, humans have been using authentication. Personal recognition is the simplest and oldest kind of authentication [1]. Meeting someone requires authentication, which takes place when you recognize their face and agree to speak with them. Additionally, if you are waiting for documents at work, you will accept them depending on the approvers' signatures. The outcome of approving someone or something is the same regardless of the authentication technique used. It is essentially a two-way channel with nodes A and B. A will challenge B in order for B to be approved.

Humans knows the authentication and have been utilizing it for ages. The simplest and oldest authentication method is personal recognition [1]. If you are going to meet someone, an authentication process will happen during the meeting, by recognizing the face and accept the person. Moreover, in workplace, if you are waiting documents, you will accept them based on the signature of approvers on them. Regardless of authentication methods, the result of accepting someone or something is the same. It's basically two ways channel that has two nodes A & B, while B will be challenged to be accepted by A. With the fact that nowadays our life has been changed and full with network and computer and cyber spaces, personal recognition is not valid any more. Authentication methods were evolved to fulfil recent complex life requirements to ensure the availability, confidentiality and integrity of the information. Recently an authentication method showed which is Multifactor authentication (MFA). At the present time, hackers have approximately 15 billion records from stolen credentials in different sectors, such as Banks, Healthcare, Institutes and many other different organizations. The importance of MFA came to prevent stealing information and protect organization's systems in stronger technique [2]. Previously, a known authentication method is Two Factor Authentication (2FA), which requires only two steps of verification. And here is the main difference between 2FA and MFA, where the last one requires at least 2 steps of

verification, if not more. This paper will illustrate the concept of MFA, the difference between 2FA and MFA, types, and benefits.

MULTI FACTOR AUTHENTICATION (MFA)

Nowadays, information is the most important asset in any organization. Therefore, securing the environment and apply the needed controls become a mandatory to assures business sustainability. Many security companies offer several solutions to secure systems, such as encryption, passwords, certificates and authentication. A new concept raised recently which is Multi Factor Authentication (MFA).

Multifactor authentication (MFA) is a security technology used to verify user's identity to access a system or application which requires multiple steps to validate user's credentials. Multifactor authentication combines two or more selfgoverning credentials: what the user knows, such as a password; what the user has, such as a security token; and what the user is, by using biometric verification methods [3]. The objective of MFA is making it more difficult to compromise the system. In case a hacker knows the credential for a system or application and tried to login, he will be challenged against another factor to satisfy it before successfully login to it. An authentication method is used with user's credentials to guarantees identity verification. Each additional authentication method in MFA is intended to challenge the user of the system in several ways such a who, or what it says it. Several authentication questions will help complicate hacker's job [3].

Many firms are utilizing MFA; as an example, Google encourages various MFA techniques among their services. Ultimately, this will assist organizations in securing their services by making it difficult for attackers to access services or control user accounts on Google [4].

MFA is essential since it will increase security for all enterprises, regardless of size. Applications, services, or systems will have more security layers added so that an attacker would have to put up more effort to find a different way to effectively take over the system. Additionally, MFA support digital transformation by facilitating e-commerce, cloud computing, and remote workforce. In the contemporary digital world, each of them needs a secure environment. Additionally, MFA can be a crucial strategy for ensuring the longevity of online interactions.

Users must simplify their tasks in order to ensure easy access to the system. Additionally, system administrators and/or application developers work to entice users and guarantee a user-friendly environment. The MFA technique, however, will complicate the use of any system by adding an extra layer and process. Implementers and cybersecurity experts should thus examine the following issues [3]:

- Push Authentication. A mobile authentication technique which will push a code to the user through SMS or Authentication application to gain access.
- Adaptive MFA. A technique for utilizing relevant data and business rules to control the authentication factors to apply to a particular user in a particular situation. For example, an employee utilizing corporate VPN from home it's much safer than coffee shop, which will raise a flag and require the employee to provide MFA credentials.
- Single Sign-On. One step configuration on relevant system and its application, where the user is required to authenticate one time to access the system. After that the system will share the information with related application to ease the access.

CORE DIFFERENCE BETWEEN MFA AND 2FA

MFA is the combination of two or more authentication methods; two factor authentication (2FA) is the use of just two strategies [5].

Even while both 2FA and MFA provide updated security measures in addition to usernames and passwords, they each provide different levels of assurance that the person visiting the record is who they represent. Is MFA overall safer than 2FA? It depends, is the simple response.

As part of the MFA technique, more than one mechanism can be used to authenticate the system, such as a password and a one-time password (OTP). However, the security of both of these methods is unavailable. On the other hand, employing 2FA strong authentication techniques such location behavior and mobile push will be taken into consideration.

MULTIFACTOR AUTHENTICATION TYPES

There are several categories for MFA, and the most common three factors are:

1. Knowledge factor: something you know, such as Password or Pin.
2. Possession factor: and something you have, such as Smartcard or token.
3. Inherence factor: something you are, such as fingerprint or face or other biometric.

As mentioned in the second part of this paper that MFA works by joining at least two factors from above categories.

BENEFITS

The primary advantage of MFA over 2FA is that it adds more security levels throughout the authentication process.

MFA uses a broad range of authentications, including PINs, security questions, USB drives, voice, and fingerprints, as opposed to the typical method of 2FA, which uses the username and password combination together with a one-time password delivered over the phone. Because it is so difficult to copy or steal a person's unique features, biometrics play an essential part in MFA [7].

The majority of programs now are using biometrics to minimize the risk of intrusion, including behavior and face recognition. Because of this, even if 2FA authentication strengthens security by taking ownership parts into account when authenticating users, the security layers are still insufficient, which raises the risk of successful breaches.

By making it hard for hackers to avoid authentication, the use of MFA helps a company to safeguard networks, applications, and data. The more levels of protection are in line with the recommended industry practice of guaranteeing security throughout. The majority view in cybersecurity is that many safeguards are required to offer high enough levels of security. In other words, every layer includes weaknesses that may be used by hackers to compromise systems. For instance, brute force attacks might be used by attackers to access the system. Users commonly set passwords that are too simple or don't update them often, among other problems. Similar to 2FA, just introducing a second layer of authentication does not completely remove common flaws. For instance, the hacker can take the victim's smartphone in addition to the password in order to get the one-time password required to access into the system. Theft of the smartphone and password, however, are enough with MFA because biometrics will be required.

The improvement of regulatory compliance is a further advantage of MFA. In order to secure data and safeguard customers, regulators are currently implementing security and safety rules. For instance, covered businesses in the healthcare industry, such hospitals, insurance companies, and healthcare providers, are required to have adequate security measures in

place to prevent the loss of personally identifiable information. Comparable requirements apply to the financial services and banking industry, where participants must guarantee demanding identification to safeguard financial data and avoid threats like credit card theft [8]. Although MFA may not be specifically required by the regulations, MFA is the only method available to achieve the required security posture. Additionally, as cybersecurity is a hot topic for legislation, MFA must be implemented voluntarily across all business sectors and industries. Undoubtedly, as the use of information technology develops, governments will focus on the need for strong security measures. Once an organization needs to set up a single sign-on (SSO) system, MFA is also beneficial. Users have to to have secure passwords for numerous applications and accounts, which presents one of the main challenges related with using of passwords. In fact, this is an important reason in why people frequently use the same password for many different services, which is a very unsafe habit. But using single sign-on (SSO), multi-factor authentication makes it possible to verify a user's identity [9]. By streamlining signing in across different applications and user accounts, single sign-on ideas save time without harming the security of the system. Single sign-on (SSO) is used by Google's many solutions nowadays using MFA.

CONCLUSION

This paper has analysed the concept of Multi Factor Authentication (MFA) and its benefits. Previous section has illustrated MFA as a security technique that needs numerous steps to validate a user's credentials in order to access a system or application. Multifactor authentication uses biometric verification methods to integrate two or more selfgoverning credentials: what the user knows, such as a password; what the user owns, such as a security token; and what the user is. The necessity of utilizing MFA cannot be overstated, as it will increase the security of any company. It will add additional security layers to apps, services, or systems to make the attacker work harder to find a different approach to gain control of the system. MFA also aids digital transformation by facilitating remote workforce, cloud, and e-commerce. Moreover, giving the fact of MFA benefit, where it wins on 2FA by adding third check in addition to user's credentials and PIN. Furthermore, applying MFA nowadays is mandatory to comply with regulations. Critical business such as hospitals and banks entail to secure their data to ensure sustainability and regulation compliance. Also, MFA helps end-users to access shared services easily through utilizing Sing sign on (SSO). User's will be able to login to several common services and applications by checking credentials one time and leveraging Multi Factor Authentication.

References:

[1] R. A. Grimes, Hacking Multifactor Authentication, John Wiley & Sons Inc., 2021.
[2] "Why Multi-Factor Authentication (MFA) Is Important," OKTA, [Online]. Available: https://www.okta.com/ identity-101/why-mfa-is-everywhere/.
[3] "What is multifactor authentication and how does it work?," [Online]. Available: https://www.techtarget.com /searchsecurity/definition/multifactor-authentication-MFA.
[4] "The Ultimate Chrome OS Guide For The Google Pixelbook Go," [Online]. Available: https://books.google.com.sa/books?id=rrw6EAAAQBAJ&pg=PT139&dq=Multi+Factor+authentication+(MFA)&hl=en&sa=X&ved=2ahUKEwifpceW9eD1AhVDyxoKHeARCZ44FBDoAXoECAoQAg#v=onepage&q=Multi%20Factor%20authentication%20(MFA)&f=false.

[5] “What is multi-factor authentication (MFA) and how does it work?,” SecurID, Oct 2021. [Online]. Available: https://www.securid.com/en-us/blog/what-is-mfa/.
[6] “What are the Key Differences between 2FA and MFA?,” [Online]. Available: https://www.incognia.com/theauthentication-reference/what-are-the-key-differences-between-2fa-and-mfa.
[7] A. C. S. S. M. M. Y. E. B. a. E. A. Bhargav-Spantzel, “Privacy preserving multi-factor authentication with biometrics,” Journal of Computer Security, vol. 15, pp. 529-560, 2007.
[8] F. C. R. C. G. &. Z. N. Sinigaglia, “A survey on multi-factor authentication for online banking in the wild.,” Computers & Security, 2020. [9] a. A. K. T. Bazaz, “A review on single sign on enabling technologies and protocols,” International Journal of Computer Applications, vol. 151, no. 11, pp. 18-25, 2016