The Necessity of Multi Factor Authentication

[1]Norah Alyousif, [2]Sultan Alhabis

Saudi Aramco, Dhahran, Saudi Arabia

DOI: https://doi.org/10.5281/zenodo.6472757

Published date: 20-April-2022

Abstract: **Multifactor authentication (MFA) is one of the most secure authentication methods. It covers a wide range of topics in a cyber-connected environment, such as online payments, communications, and access right management, among others. Multifactor authentication is usually a little complicated because it necessitates an extra step on the part of the user. With two-factor authentication, in addition to the user ID and password, the user must additionally input a special code that they usually receive through SMS or a special code that they have received in advance. This paper will explore the concept of MFA, key differences between MFA and two facto authentication (2FA), MFA benefits, and the necessity of utilizing it.**

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

I. INTRODUCTION

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.

II. 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 self-governing 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].

A lot of organizations are using MFA, as an example, Google supports different kinds of MFA methods among its services. Which eventually will help them to secure their services by challenging attackers to access services or take over user accounts in Google [4].

The importance of MFA is intangible, as it will improve the security for any organizations. It will add additional security layers in applications, services, or systems to require the attacker to give more effort to search for another way to successfully take over the system. In addition, MFA support digital transformation through supporting remote workforce, cloud, and e-commerce. all of them requires secured environment in the current digital era. Moreover, MFA can be vital method to assures the sustainability of online interactions and secured transactions [5].

Simplifying the work is an essential need by users to assure accessing the system easily. As well as application's developers and/or system administrators to entice users to assures providing user friendly environment. However, MFA method will add additional layer and extra step, which will complicate the utilization of any system. Therefore, implementers and cybersecurity specialist need to take into consideration below points [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.

III. CORE DIFFERENCE BETWEEN MFA AND 2FA

A combination of two of more authentication methods can be considered as MFA, however using only two methods can know as two factor authentication (2FA) [5].

Despite the fact that both 2FA and MFA add upgraded security efforts additionally to username and passwords, they each give various degrees of assertion that the individual getting to the record is authentic. All in all, is MFA safer than 2FA? The short response is, it depends.

More than one method can be used as MFA approach to authenticate the system, for example using password and one-time password (OTP). However, both of these methods are weak in security. In another hand, utilizing strong authentication methods in term of 2FA such as, location behaviour and mobile Push will be considered as strong types of authentication and hard to crack, which eventually will be more secured. For that reason, any MFA technique is just pretty much as solid as the strategies utilized [6].

IV. MULTIFACTOR AUTHENTICATION (MFA) 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.

V. BENEFITS

The main benefit of MFA over 2FA is that it integrates additional layers of security into the authentication process. Instead of using the username and password combination together with a one-time password sent through the phone, which is the default approach in 2FA, MFA makes use of a wide variety of authentications, including PINs, security questions, USB drives, voice, and fingerprints. The utilization of biometrics in MFA is particularly important as it is almost impossible to steal or replicate person-specific features [7].

Today, most applications make use of biometrics including behaviour and face recognition to eliminate the risk of intrusion. Therefore, although 2FA authentication improves security by considering ownership factors when authenticating users, the layers of security as still inadequate, which increases the possibility of successful breaches. Implementing MFA enables an organization to secure networks, applications, and data by making it difficult for hackers to breach authentication.

The increased number of security layers aligns with the industry best practice of ensuring security in-depth. The overarching view in cybersecurity is that a single safeguard is not adequate to provide sufficient levels of security. In other words, each layer has vulnerabilities that hackers can leverage to breach systems. For instance, attackers can execute brute force attacks to gain access to the system. At the same time, users tend to make passwords mistakes such as setting weak passwords or failing to change them frequently. Likewise, simply adding a second layer of authentication – as is the case in 2FA – does not eliminate common vulnerabilities. For example, in addition to obtaining the password, the hacker can also steal the victim’s smartphone to receive the one-time password needed to log into a system. However, with MFA, the theft of the password and smartphone are not adequate as biometrics would be required.

Another benefit of MFA is that it enhances regulatory compliance. In the recent past, regulators have been adopting security and safety standards to secure data and protect consumers. In the health care sector, for instance, covered entities such as hospitals, insurance firms, and health providers are expected to implement strong security safeguards to limit the theft of personally identifiable information. Likewise, in the banking and financial services industry, players are expected to ensure strong authentication to protect financial information and eliminate risks such as credit card fraud [8]. Although the regulations might not specifically stipulate the need for MFA, the security posture expected can only be attained by adopting MFA. Also, the area of cybersecurity is an active area of legislation, which means that the compulsory implementation of MFA is likely to be a requirement across industries and sectors. Certainly, as the adoption of information systems increases, the need for robust security safeguards becomes a priority for governments.

MFA is also beneficial in situations where an organization intends to enable a single sign-on (SSO) system. One of the key challenges associated with the utilization of passwords is that users are expected to have strong passwords for different applications and accounts. Indeed, this is a major reason why users tend to have one password for multiple services, which is a highly insecure practice. However, the adoption of multi-factor authentication allows one to confirm the identity of a user in a single sign-on (SSO) setting [9]. By streamlining signing in across different applications and accounts, single sign-on solutions save time without adversely affecting the security of the system. Google’s diverse solutions today utilize single sign-on (SSO) by leveraging MFA.

VI. 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 self-governing 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=2ahUKEw ifpceW9eD1AhVDyxoKHeARCZ44FBDoAXoECAoQAg#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/the-authentication-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.