Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.7778218

# STRENGTHENING AUTHENTICATION BEST PRACTICES FOR MULTI FACTOR AUTHENTICATION DEPLOYMENT

**H. Naga Chandrika & Dr. Pramod Pandurang Jadhav**

1.H. Naga Chandrika, Research Scholar , Dr. A.P.J. Abdul Kalam University University in Indore, Madhya Pradesh, India.

Mail id : nagachandrika87@gmail.com

2.Dr. Pramod Pandurang Jadhav,Associate professor, Dr. A.P.J. Abdul Kalam University University in Indore, Madhya Pradesh, India.

Mail id : ppjadhav21@gmail.com

**Abstract**

Multi-factor Authentication also known as Two-factor Authentication it is a security measure that involves using additional methods to authenticate a user identity beyond the standard username and password. Its purpose is data security by making it harder for unauthorized users to gain access.

This aims to explore the shortcomings of relying solely on username and password logins, the various types of authentication available, and the best practices for implementing multi-factor authentication. Additionally, we will discuss predictions for how this technology will continue to develop in the future.

## Introduction

Multi-factor authentication (MFA) is becoming a more prevalent security feature in online services, aimed at verifying the identity of users trying to access their content. In addition to the traditional username and password, MFA entails requiring the user to provide additional data or codes that only they possess. To ensure that higher level of security MFA protocols require two or more authentication methods .This can be applied to everyday activities such as using an ATM machine the user a bank card and knows a Personal Identification Number. This combination of something the user has and something the user knows is an example of MFA include various biometric data, such as fingerprints

There are various combinations of MFA that can be used to increase security . We had explore the various strengths and weaknesses of MFA. It is the best safe method to save our online accounts from attackers [1]. Enabling MFA on an account, even if a hacker manages to obtain the username and password they will not be unable to access the account without the MFA data. As a result, implementing MFA is a quick and effective way for a company to enhance the security of their users' accounts without requiring them to remember additional information .Despite the growing popularity of MFA so MFA will be the primary method.

However, relying solely on passwords poses two major challenges. Firstly, users often choose simple and easy-to-remember passwords, which can be easily cracked by attackers. Secondly, users tend to reuse passwords across multiple accounts with just one compromised password. These factors compromise the security of user accounts and leave them vulnerable to basic password cracking attacks. In fact, an analysis of commonly used passwords revealed the top ten most frequently used passwords, further highlighting the need for stronger authentication

measures.There are various patterns for creating passwords, including appending, prefixing, inserting, repeating, sequencing, replacing, reversing, capitalizing, using special formats, and mixing patterns [3]. when creating a password, as attackers often use dictionary attacks to crack passwords. In a basic dictionary attack, attackers attempt to use every word in the dictionary as a password. These attacks
utilize dictionary words, but also test against variations of those words using the ten common patterns for creating passwords. While pattern-based dictionary attacks are slower than simple dictionary attacks, they have the potential to crack a much greater number of passwords [3].

**Table 1. possible passwords per character in password**

| Number of Characters used | Number of password combinations |
|---|---|
| 1 | 69 (69^1) |
| 2 | 4761 (69^2) |
| 3 | 328509 (69^3) |
| 4 | 22667121 (69^4) |
| 5 | 1564031349 (69^5) |
| 6 | 107918163081 (69^6) |
| 7 | 7446353252589 (69^7) |
| 8 | 513798374428641 (69^8) |

A well-known approach to cracking passwords is through a brute force attack, where every possible combination of characters, starting with single letters, is attempted until the correct password is found. In many cases, machines that are compromised by brute force attacks become part of a botnet, a network of infected devices that can be controlled collectively by a single person, often referred to as the "bot master," to carry out distributed attacks. Brute force attacks come in different variations, just like dictionary attacks, and vary in complexity. For example, a standard botnet attack involves trying all possible character combinations, while letter frequency analysis uses the frequency of letters in words to guess the password. Another approach is the Markov model, which calculates the probability of two letters occurring together One type of brute force attack involves checking for characters that appear next to each other in a string.letter frequency analysis and the Markov model with additional external logic. The danger with a brute force attack lies in the fact that given the correct character set and an unlimited amount of time, it has the potential to crack any password. However, brute force attacks are highly inefficient as the time it takes to crack a strong password grows exponentially with every additional character, as illustrated in Table
1. Although brute force attacks can guarantee a 100% success rate, their inefficiency makes them a less than ideal approach for password cracking.Table 1 illustrates how the number of combinations increases exponentially with the addition of each character to a password, making the time required to crack the password increase at the same rate. Another method commonly

used by attackers for password cracking is through rainbow tables, which are representations of plaintext passwords and their hash values. Rainbow tables work by checking if the hash value from the table matches any of the final hash values. If a match is
found, the process begins by entering the plain text values for that hash, and if the hash produced by entering the plain text value matches, then the plain text password has been discovered. If not, the hash is reduced to a new plain text value and the process repeats until a successful password is found. Figure 1 depicts this process in the form of a block diagram. While rainbow tables are much faster than brute force attacks, they require a significant amount of disk space as the values are pre-stored. This is the trade-off for their efficiency.The use of password cracking techniques and other related methods highlights the inadequacy of relying solely on password authentication for online services. Since a computer cannot distinguish if a password has been cracked using any of the aforementioned techniques, any user entering a correct password is granted access.

Incorporating multi-factor authentication (MFA) alongside a username and password can address this issue by verifying the legitimacy of a user's identity (provided that their MFA methods have not been compromised), and mitigating some of the weaknesses of relying solely on passwords for authentication. Having discussed the limitations of relying on simple username and password systems, the report will now delve deeper into MFA itself, exploring its various types in the subsequent sections.The upcoming sections of this report will examine the various types of MFA used today, along with their respective advantages and drawbacks. Additionally, the report will highlight the best practices for implementing MFA into services, as well as current security concerns and adoption issues related to MFA. Furthermore, the report will discuss the future developments in MFA and draw conclusions based on the topics covered throughout the report.

**Types of Authentication**

Multi-factor authentication has three primary types, namely knowledge factors, possession factors, and inherent factors. The strength of MFA lies in the combination of two or more of these features, where each additional factor enhances the verification of the user's identity. This will examine each factor individually, analyzing their robustness, and providing real world examples to illustrate their effectiveness.

**Factors**

Knowledge factors refer to elements that only the user should be aware of, such as passwords, PINs, and security questions. Passwords have been extensively discussed earlier, and they are prone to numerous cracking methods. Additionally, users often reuse passwords, which makes them vulnerable if one service is compromised, and many passwords are not complex enough. However, if users opt for complex passwords, they tend to write them down or save them in files, which is also a security risk. To mitigate these issues, users can employ a password manager that generates robust passwords automatically and autofills them.Using a password manager eliminates the need for a user to remember multiple complex passwords, as they only need to recall one master password.

The password manager generates and stores strong passwords for each account, thereby reducing the risk of password reuse or weak passwords. However, if the user selects a weak

master password, it could be vulnerable to cracking, which may result in unauthorized access to all the user's accounts and login details.PINs, which stands for Personal Identification Numbers, are commonly used in card transactions or to unlock mobile phones and tablets. A PIN typically consists of four to twelve digits, but it is recommended that it
should not exceed six digits in length [7]. Similar to passwords, a PIN is entered into a system and compared with a reference PIN, and if the values match, access is granted. It is important to note that PINs used for different applications should be different, since using the same PIN across multiple platforms would make them only as secure as the weakest one [8]. Despite being shorter and easier to remember, PINs are less ideal for online activity as there are only 10,000 (10^4) possible combinations in a standard 4-digit PIN, which can be easily cracked by attackers.PINs or Personal Identification Numbers are commonly used in card transactions or to unlock mobile phones/tablets. A PIN should ideally be four to six digits in length [7]. PINs are used in the same way as passwords, where it is entered into a system and compared with a reference PIN. The advantage of a PIN is that they are shorter and therefore easier to remember. However, it is recommended that PINs used for different applications should be different since using the same PIN across multiple platforms makes them only as secure as the weakest one [8].

In physical use cases such as with ATM machines or mobile phones, a PIN is usually secure enough to prevent attacks. When the PIN is entered incorrectly a certain number of times, the mobile device will lock out for a period of time, or the card will get shredded by the ATM machine. This nature of PINs used in these examples makes them part of multi-factor authentication as an attacker will require both the bank card or phone and the PIN number to access the information [8]. However, for online activity, a PIN may not be ideal as it could easily be cracked by a brute force attack.However, despite these guidelines for creating good security questions, there are two main problems associated with them. Firstly, users often forget their answers. Studies have shown that users forget up to 16% [9]of their answers within six months. Secondly, answers to security questions can be guessed, especially given that people are sharing more personal information online than ever before. Many common answers to security questions can be found through a quick online search, making them public knowledge. Questions that are designed to fit a large number of people can also lead to problems, as common answers will occur. For instance, the question "What was the name of your first pet?" is likely to have common answers that can be found through a simple search of popular pet names. Just like with passwords and PINs, it is essential to limit the number of attempts that can be made to answer these questions to prevent such situations.


Figure 1. Apple ID Security Questions

**Inherent Factor**

The inherent factors of authentication refer to features and commonly use biometric or behavioral methods. Biometric authentication allows users to authenticate the remember anything or carry anything with them. Some common biometric methods include fingerprint scanning, face recognition, and retina scans, with mobile devices being the most common example of their use.The use of fingerprint authentication has become increasingly popular and is considered the most widely used biometric authentication method. In 2018, over one billion smartphones shipped with fingerprint scanners, as shown in Figure 2.

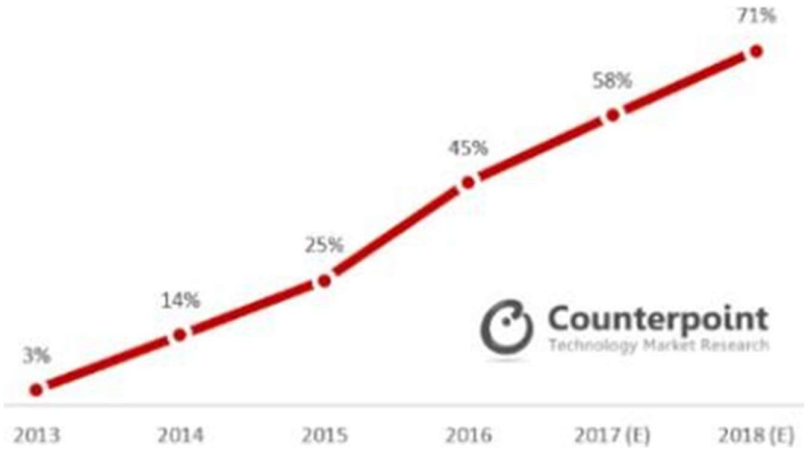


Figure 2. Fingerprint Sensor Penetration

Fingerprint authentication employs the minutiae algorithm, which involves storing the ridges of fingerprints as dots in a coordinate system. Users first scan their fingerprints, ensuring to cover as many areas as possible. During authentication, the user places their registered finger on the scanner. If the ridges match up with the coordinate system, the user will be authenticated and granted access. Compared to other biometric authentication methods, fingerprint scanners have a high level of reliability. This is likely because the technology has been established for longer, and no two people have identical fingerprints. Fingerprint authentication is widely used, with over one billion smartphones containing fingerprint scanners shipped in 2018 as shown in Figure 2.

The face recognition method is similar to the minutiae algorithm, but instead of plotting ridges, it analyzes the facial features (as shown in Figure 3). Two features that are considered important are the distance between the eyes and the distance from the forehead to the chin [10]. Facial authentication also serves as a contactless authentication method, as the user does not need to make physical contact for authentication. Instead, a camera captures the user's facial features and compares them to an internal database of features. If there is a match, authentication is verified. Face recognition is also highly reliable, with Apple stating that the likelihood of a stranger being able to unlock a device using Face ID is approximately one in one million.

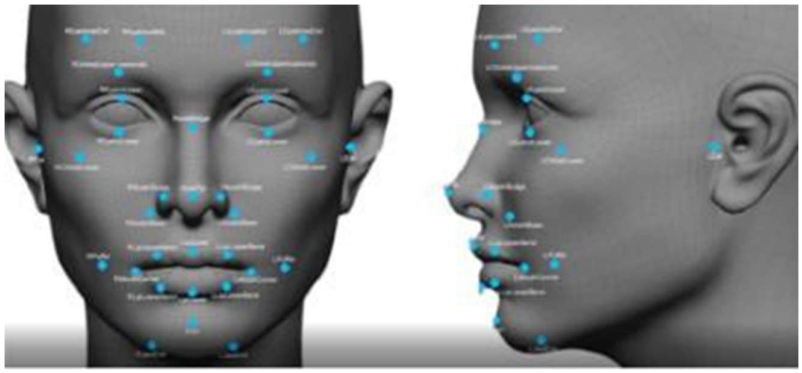

Figure 3. Fingerprint Sensor Penetration

**Future Development of MFA**

As outlined in the best practice section of this report, a key area for future development is to increase the adoption of multi-factor authentication (MFA) as a standard approach for user identification and security. One potential solution could be to make MFA mandatory for accessing online services that store sensitive data, such as email accounts or social media platforms. While many of these services offer the option to activate MFA, it is typically left to the user to take the initiative to do so. For instance, to enable MFA on a Facebook account, a user must navigate to their settings, select "security and login," and manually activate the feature. To improve security, websites could implement a policy that either requires or strongly encourages users to enable MFA for their accounts.As mentioned in the best practice chapter of this report, one of the key future developments in security and user identification will be the increased adoption of multi-factor authentication. This could involve making multi-factor authentication a mandatory security measure when accessing online services that contain a lot of private data, such as email services or social media. Although many online services offer the ability to activate MFA, it is often up to the user to manually enable it. For example, activating MFA on a Facebook account requires navigating to the settings, going to "security and login," and manually enabling MFA for the account. In the future, it could become standard for websites to either enforce the use of MFA or to regularly remind users of the functionality and benefits of using it. Additionally, new users to such services could be prompted to activate MFA upon account creation.

Another area of future development will be in the form of inherent factors. While biometric forms of authentication, such as fingerprint scanning, are commonplace in modern mobile devices, they have yet to become widely used in desktop computers. Although the necessary

hardware and software technologies exist, they have not yet reached the mass market of users. A representative from Microsoft stated that although fingerprint scanning is present in enterprises, the main issue is that it is not prevalent [10].The primary means of implementing inherent factors for both consumers and companies is through incorporating scanning technologies in newly developed laptops and desktops. This is an emerging trend in the computer market with the introduction of Windows Hello for Windows-powered devices and Touch ID for MacBooks. However, currently, Windows devices that support this feature are limited, and only MacBooks produced after 2018 have Touch ID functionality. With
increased adoption of these features for new laptops and heightened awareness of how to activate them on existing devices using webcams and USB fingerprint readers, inherent factors of authentication are likely to gain in popularity due to their ease of use and fast authentication times.

## Conclusion

It is evident that employing multi factor authentication in some capacity is more secure than depends on a username and password. As users become more security concerns and the significance of safeguarding their online data, their initial step in enhancing the security of their accounts should be to activate multi factor authentication. The issues with username and password logins, the various authentication methods available, current best practices for multi-factor authentication, and predictions for how the technology will evolve in the coming years With the growing importance of security in protecting user data, companies are under increasing pressure to adopt measures such as multi-factor authentication to confirm a user's identity.

The implementation of MFA options is the first step in this direction. As the technology behind multi-factor authentication continues to evolve, becoming more reliable and secure, its adoption should increase year by year, eventually becoming as common among technology users as usernames and passwords are today. It is likely that, with government regulations and user awareness of the importance of security, multi-factor authentication will eventually become a standard security measure for online accounts.

## References

[1] Archana, B. S., Chandrashekar, A., Bangi, A. G., Sanjana, B. M., & Akram, S. (2017, May). Survey on usable and secure two-factor authentication. In 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT) (pp. 842-846). IEEE.

[2] Bošnjak, L., Sreš, J., & Brumen, B. (2018, May). Brute-force and dictionary attack on hashed real-world passwords. In 2018 41st international convention on information and communication technology, electronics and microelectronics (mipro) (pp. 1161-1166). IEEE.

[3]Tatlı, E. I. (2015). Cracking more password hashes with patterns. IEEE Transactions on Information Forensics and Security, 10(8), 1656-1665.

[4]Gautam, T., & Jain, A. (2015, November). Analysis of brute force attack using TG—Dataset. In 2015 SAI Intelligent Systems Conference (IntelliSys) (pp. 984-988). IEEE.

[5]Theocharoulis, K., Papaefstathiou, I., & Manifavas, C. (2010, August). Implementing

rainbow tables in high-end fpgas for super-fast password cracking. In 2010 International Conference on Field Programmable Logic and Applications (pp. 145-150). IEEE. [6]Kumar, H., Kumar, S., Joseph, R., Kumar, D., Singh, S. K. S., Kumar, A., & Kumar, P.
(2013, April). Rainbow table to crack password using MD5 hashing algorithm. In 2013 IEEE Conference on Information & Communication Technologies (pp. 433-439). IEEE.
[7]Williamson, J., & Curran, K. (2021). The Role of Multi-factor Authentication for Modern Day Security. Semiconductor Science and Information Devices, 3(1), 16-23.
[8]Williamson, J., & Curran, K. (2021). The Role of Multi-factor Authentication for Modern Day Security. Semiconductor Science and Information Devices, 3(1), 16-23. [9]Schechter, S., Brush, A. B., & Egelman, S. (2009, May). It's no secret. measuring the
security and reliability of authentication via “secret” questions. In 2009 30th IEEE symposium on security and privacy (pp. 375-390). IEEE.
[10]Williamson, J., & Curran, K. (2021). The Role of Multi-factor Authentication for Modern Day Security. Semiconductor Science and Information Devices, 3(1), 16-23.