Multi-factor authentication. An extended overview

Matei-Dimitrie TIȚA
National Institute for Research and Development in Informatics - ICI Bucharest
B-dul Mareșal Alexandru Averescu, Nr. 8-10, 011455, București, Romania
matei.tita@ici.ro

Abstract: This paper presents in a more detailed manner some of the techniques that can enforce the security of data by using a multi-factor authentication. Cyberattacks target vulnerable systems by exploiting their weak authentication procedures and the validation process. An additional method of authentication is supposed to help the users secure the access to their information by presenting something more than just a password. The most well-known factors are biometrics, cards and authentication applications. By adding more than one factor for authentication, the possibility of a security breach is diminished. Moreover, we discuss the importance of using a multi-factor authentication, as well as some advantages and some drawbacks for each of these methods.
Keywords: security, multi-factor authentication, cyberattacks, password, biometrics, breach

INTRODUCTION

On a day to day basis, we face situations where we are requested to prove our identity in order to access some personal belongings. This helps keep the data stored confidential, so that any unauthorized attempts to reach it will be dismissed. The most renowned procedure used for user verification is a password. We can see it mostly everywhere from a simple e-mail account to the more serious savings account in a bank.

However, this can a be a shortcoming due to the possibility of an individual getting in possession of the credentials of someone else. This event is not so unlikely as you may think, giving the fact that more and more threats arise in the internet as days go by. Even from a simple incident such as losing a piece of paper that had the password written down for remembering, this can turn into a serious problem. Mostly, this is due to the fact that, for easy access, people tend to use the same password when registering for different accounts and, consequently, it can lead to disastrous outcomes.

This article intends to assist those that use a variety of applications and, therefore, need to secure their personal data. To that end, the paper highlights several proposals meant to block any malicious action performed by people who are not supposed to get hold of the information contained. Thus, the readers will become more self-aware of the importance of employing as many methods of verification as possible, in order to avoid an unwanted access to their restricted content.

So, how can we avoid such an unfortunate event? We can simply start by being more careful with manoeuvring pass codes. It seems decent and safe, but can we try to improve the method of authentication? This is where multi-factor authentication comes into play. It adds an extra layer of security to our personal data, preventing any illegitimate attempt on accessing some piece of information, but what is it really?

CLARIFICATION OF THE TERM

Multi-factor authentication, in short MFA, represents a system which uses not only one method of authentication, but rather two or more, in order to validate the identity of the user. The additional action required for a successful login can be either something the user knows, such as an answer to a secret question, something the user possess, like a security token or it might as well be what the user inherits, found in biometric verification.

According to (Margaret Rouse, 2015), MFA has the objective of creating a stronger and more complex defence, so that in the case of one factor of authentication being compromised, there will be at least one more hurdle to jump before the target could be accessed. This target can be a device, a network, a database holding crucial information, or even a physical location.

We may not realize, but this authentication is integrated into our daily activity in various forms, the most notable one being the act of swiping a card and entering the PIN in order to complete a particular transaction. Two or more factors of authentication would be beneficial in not just mailing services, but also banking, governmental and medical domain. These mostly contain sensitive data that directly impact the lives of people and because of that, it is recommended that precautionary measures are taken for securing information.

THE FACTORS FOR USER AUTHENTICATION

An authentication factor embodies a group of credentials, which is needed to confirm the identity. The multi-factor authentication has several elements, each additional one having a purpose of reassuring the system that an individual requesting the access to a sensitive piece of data is in fact authorized to proceed.

These factors can be classified in many ways, but there are three main categories which we will discuss in particular: the possession factor, the knowledge factor and the inherence factor.

Possession factors can be anything that the user own for logging in to a certain service. In this category we can enumerate some such as a key, a bank card or a one-time password (OTP). An OTP token is represented by a hardware device or even a software program with the ability to provide a PIN or password for only one login session or transaction. This single-use characteristic represents the fundamental advantage of tokens. Assuming that an unapproved user manages to record an OTP used for a past login process, he will not be able to abuse it because it will be invalidated after its unique usage.

The knowledge factors consist of the information which the user is requested to provide to the system for a login attempt. Usernames, as well as passwords, PINs or certain answers to some secret questions can all be considered part of this group of factors. By default, an individual will be asked to provide a password or a PIN code when creating a user for future uses of a service, but an additional information needed for confirmation would come in handy. This is where we introduce the term KBA, short for Knowledge-based authentication. This represents a scheme that prompts the user to answer one or more secret questions (Margaret Rouse, 2015). Of course, these questions should not be easily guessed by researching or by deducing and it is advised that the information demanded could be remembered without a particular effort from the authorized user.

These KBA questions can be viewed as static or dynamic. For the static ones, the user selects some questions for which he will need to enter the right answers. These pair of questions and answers are verified by the hosting side in order to confirm the identity. An example would be asking about the name of the owner's pet or favourite music genre. A downside of this scheme refers to the possibility of finding the information needed by the secret questions on the social media.

Dynamic questions, on the other hand, would not let the users select whichever query they like. The pairs are gathered from data present in public records, and therefore the entity trying to login would not have any clue about what question might be requested. What also differs

Fig. 1: *Biometrics assure the identity of a user (Credit Rawpixel)*

from static questions is the fact that these generated questions refer to a specific event in a time period rarely known by anyone else but the real user. Asking for a past street address from when the owner of the account was a child might be a good case. This information can still be found; however, it would most certainly take significant time. Given the fact that there is surely a time limit set for giving the correct answer, the dynamic scheme will succeed in identifying forbidden access to data.

The third type of factors are the inherence factors. These include the physical characteristics of the user, or as people know them, biometrics. Some commonly known methods are the fingerprint scan, that even for identical twins differs, retina scan, facial or voice recognition. These last two are accomplished with the help of artificial intelligence, or more concretely, machine learning.

Besides these three categories, we can also mention two supplementary types of factors that can be used for authentication: location and time. Smartphones, for instance, have GPS tracking, so by using its position determined by satellites and radio waves, the location from which the login is registered can be verified for potential abnormality. Furthermore, time can be checked in order to hider the possibility of account hijacking. Take for instance an ATM card access in Europe at a certain hour in the day. The same card is then used in no more than several minutes on a different continent. A well-maintained system would be aware of this anomaly and would prevent these types of frauds.

MOTIVATION FOR MFA

The basic method in which usernames and passwords are stored is through a password database. While it is rather easy to maintain, it has a major drawback. Even if an encryption algorithm is used in conjunction with the information saved in the database, it can still fail to keep the data confidential. Suppose that the database is snatched. This event will give the attacker the possibility to start working on solving the users' credentials. In time and with some rather high computation speed, the information in the database will be compromised and the hacker will have total control over the data within it.

This is due to the improvement in CPU speed, and because of that, attacks that rely on a straightforward brute force or credential-stuffing can rise many threats. There have been many cases in the past where companies have become victims of credential-stuffing, like Apple with their iCloud accounts or GitHub.

Fig. 2: Phishing attack (Credit Pixabay)

Phishing emails can also be prevented by a using the MFA. These types of attacks target users and persuades them into giving sensitive information such as the login username and password to a fraudulent website, as depicted in Fig. 2. If the site is not a genuine one, then it could not send a proper code for access.

In order to prevent these scenarios, a multiple factor authentication should be adopted. People are starting to take cyber security more seriously than before when designing websites or storing information online, an issue referenced in (Nitin Sharma, 2018).

TECHNOLOGIES USED IN MULTIPLE FACTOR AUTHENTICATION

Implementing the MFA can be done in different ways, some of them being more preferred than others due to their effectiveness. We will go through all the main types of multiple factor authentication providing a brief use-case, together with some characteristics regarding their functionality, as presented in (Australian Cyber Security Centre, Australian Government, Australian Signals Directorate, 2014).

1. **SMS, emails and voice calls**

This technique is based upon receiving a unique password or PIN passcode valid for a limited amount of time that is intended for a single use. As mentioned, a SMS, electronic mail can be handed over, or through a call to the person initiating the request. Choosing between any of these methods can be up to the user during the process of his registration. After one of these options is chosen, the password is sent though to verify the authenticity of the request and complete the enrolment process.

At a later authentication attempt, the service that handles logins will send the requesting side of the connection, using one of the previously selected method, the additional passcode or password. After this step, it will validate the information provided and based on that data, it will decide whether to proceed to give the user access to future operations or reject it.

A plus for this method is reducing the cost of the administrating system, as it delivers its passcodes to its users using a receiving device which they already possess, such as mobile phones. It is one of the most common form of multi-factor authentication primarily thanks to its simplicity and easiness. Although it does not require much effort to set-up and operate with, this technique has some downsides as well. By using a phone for obtaining the second item needed for authentication, it is dependent on the service provided by telecommunication networks. Therefore, the location from where the user issued the login request can directly influence the process of fetching his limited passcode.

Another aspect that can be mentioned is that these telecommunication networks do not assure the end-to-end security of the connection. This can lead to messages being leaked by getting in the hands of potential unlawful entities. Moreover, the usage of devices over the internet may result in data theft, mainly if the passcodes are delivered via platforms built for internet messaging or for calls, such as Voice Over Internet Protocol.

An action that may help in securing this multi-factor authentication is setting an appropriate expiry time for the single-use passcode. This will minimize the chance that an interceptor would have a sizable span of time to enter the code sent to the user. It is also highly recommended that if a particular device, such as the phone, is no longer in the possession of the owner, it should be reported as soon as possible, in order for the systems to invalidate any MFA method assimilated to that device.

Fig. 3: *Mobile Payments with Biometric ID System (Credit Stockvault)*

It can be used in applications that perform card payments for securing transfers directed by an individual (Fig. 3). By introducing this further verification of identity, abusing a stolen credit card would be quite impossible. Another case in which this method can be effective is when a particular user register for the first time on a domain or creates an app account. This will aid the system in discovering any malicious activity that may want to flood a server with requests for registering fake accounts.

2. **Mobile app**

Much like the technique using the messaging or calling system of a device, this method implies that a key such as passcode is dispatched to a software application on a device that the user carries. One difference would be the requirement of an installation for a particular app. This application will only be useful for logins and identity verification in case the system detects suspicious activity (Australian Cyber Security Centre, et. al., 2014).

The idea behind this multi-factor authentication approach is thoroughly straightforward. When a request for an authentication is received by the system tasked with granting access to data within a server, an automatic message will be sent to the application. The contents of the message can be a numeric code, a password composed of alpha-numeric characters or it can just be a notification. This notification, commonly referred to as a "push" notification, alerts the user of the device that someone tried to access his or her account remotely. From this point, the user must confirm whether the request was intentional or not by choosing between two options. If the answer is positive, then the authentication process ends successfully and the personal information on the account is now visible to the requesting side. As it may be intuitive, a negative response will alert the system that the request was not intended to be issued, cutting off the connection with the unauthorized entity.

The advantage that mobile apps have over the SMS and voice calls is the usage of a secure channel. The request and response are transmitted utilizing a HTTPS (Hypertext Transfer Protocol Secure) connection. This extension over the internet transfer protocol guarantees privacy as well as integrity of the data that is being exchanged. These days most of the requests on the internet are made with this protocol. Because of this extra layer used for securing information the chance someone will be able to steal the code and use it is rather slim (Zack Whittaker, 2018).

A problem that may arise is the potential existence of a malware on the device that receives the code or notification. In this case, even if the code is not used by the true owner of the account, the malicious software can still harvest this sensitive data and utilize it. Losing the physical device on which the notification for the login attempt is sent is also disastrous for the user. In this instance, any link from the device which holds the application to a multi-factor authentication should be nullified in order to prevent any further theft.

The mobile application version of the MFA can be found in mail services such as Yahoo, or it can be used for securing access to a multitude of websites, a function that Google Authenticator provides.

3. **Biometrics**

As the name itself suggests, this multi-factor authentication method is relying on metrics associated to human characteristics. There are a lot of modes in which an individual will be identified by the biometrics, but the most notable ones are fingerprint, iris recognition,

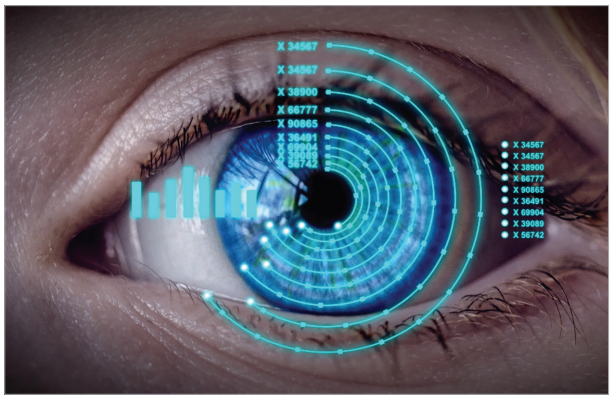

Fig. 4: *Iris recognition used for biometric identification (Credit Stockvault)*

presented in Fig. 4, face recognition, palm geometry and DNA. It can be mentioned that behavioural attributes such as the voice or typing rhythm can also be tested against a match for a more secured operation.

Whenever a certain person registers for a biometric verification, the system will demand a scan for the specific biometric in order to use it for future authentication as a reference point. At a later attempt at logging into the system, the user will be asked for the standard password in partnership with the biometric that was set-up beforehand. The service in charge of authentication will be verifying both the data provided by the biometric and the password with the ones presented at the sign-up phase. Based on calculations conducted for checking the legitimacy of the information received, the access is given or not.

Such a method can be presented with some security vulnerabilities that could be exploited if not acted upon. This happens because biometric characteristics do not resemble confidential information to a software designed to capture biometrics. In the case of hashing the output data provided by a biometric reader, the matching done for authentication is heavily dependent on the software tasked with capturing the flow of data. Assuming that the device is compromised by a mischievous program, the services encapsulated by the biometric software can be used to intercept data or even replay rightful authentications from before. It can lead to deceptive requests, seen as the user's initiative, dismantling any privacy for the owner's content (Australian Cyber Security Centre, et. al., 2014).

In addition to these aspects, the quality of the biometric capture software is playing an important role in determining the performance of the technique. It needs to deal with the case of a potential false positive or a false negative error. The false positive error is coming from a decision where the condition is satisfied, although it should have not been. In this case it is crucial that the malevolent individual should not be granted access from a bad match on the biometric data. False negatives are not as harmful as the positives, but they still represent a problem to be dealt with. They indicate that a condition did not hold, even though the biometric reading was an appropriate one. As in the example mentioned, the actual owner will not be able to authenticate successfully (Nbarth, 2014).

There are some ways to improve the security of this technique. One of these is providing a notification to the user that can be easily viewed every time a request for authentication is detected. This way any replication of the biometrics in a harmful manner will be logged. Another way is to use an additional authentication method as an alternative. This will not only increase the security of the process of logging in, but it can also resolve any false negatives given by the biometric reader by changing the way of identity verification.

Fig. 5: *Fingerprint scan (Credit Pixabay)*

Most smartphones now come with a fingerprint sensor. These scanners can be used to configure biometric signatures for online transactions, or they can offer restriction to certain files and applications. Furthermore, some mobile phone front cameras are able to use the image captured to run an iris scan or face recognition process. The technology behind these two is based on artificial intelligence with the help of some graphic processing to identify plausible matches.

4. **Smart cards**

A smart card is essentially a physical card that has a chip integrated within, which plays a role similar to a token (Margaret Rouse, 2018). It can have the dimensions of a credit card and it is usually made of plastic. These cards store a private key, which can be a PIN passcode or a standard password containing numbers, letters and symbols.

The chip located in the card can be a microcontroller, which is a compact circuit with a specific function, or an embedded memory chip. The confidentiality is assured by using encryption for the data located in its memory and information integrity is also strongly enforced by its hardware design.

Smart cards rely on a system that reads its contents, such as a card reader, to function properly. The microprocessor or memory chip integrated in the card interact through an interface with these systems either by direct contact or by a wireless connection. The user can be asked to provide the passcode to unlock the smart card, thereby unlocking the smart card and signing the authentication request with the user's unique private key. After the reader passes the received data from the card to a system, most of the time using the network, the intended system verifies the user's identity by looking at the signature. Based on that signature, the individual that initiated the request will be given a pass or not.

Fig. 6: *Insecure transactions can lead to credit card fraud (Credit Pixabay)*

Similar to biometrics, this MFA technique might be vulnerable to attacks based on intercepting and reissuing phony requests, as they rely on readers to operate. These smart cards are especially susceptible to some attacks that may leak the stored data within. One of the attacks uses a differential power analysis – DPA and by interpreting the electricity usage of the chip, is able to deduce the private key. According to (Margaret Rouse, 2012), DPA attacks measure the level of power at different parts of the chip and uses a statistical analysis to identify what operations are done for the encryption. These types of intrusions are difficult to observe and therefore require careful attention from anyone using this method of authentication.

However, smart cards do offer some benefits, mainly compared to the classic magnetic stripe cards. One upgrade is of course the microprocessor that is integrated into the card, as it has the ability to process information without needing a remote connection. The memory chip can as well store in a tightly-secured manner the significantly more data required for authentication than a magnetic stripe card.

From the point of view of storing data on a smart card, it is difficult to modify its content once the store is performed. This represents another advantage over the standard cards, as the information located on the chip of smart cards has a low probability of being duplicated. The last issue that should be addressed in this comparison is the general immunity against a magnetic field or even an electronic interference, a characteristic not present in the magnetic stripe cards.

On the other hand, smart cards and also their corresponding readers are quite costly.

Moreover, there may be a compatibility issue that can arise from using smart cards with nonstandard protocols for storing data, as well as using software restricted to certain cards or readers.

Smart cards are found in various fields of activity. Some notable examples are payment cards, which are given by banks or credit card companies, ID cards issued by companies to control the access to their locations and also smart cards used by medical institutions to accumulate information about their patients.

5. **Software certificate**

This is a method of authentication that utilizes a certificate which is stored on a particular device. The software certificate can be either in a registry or in a file located in the gadget's local memory and is intended to guarantee the identity of its owner.

In a case where some user choses to authenticate, the system seeks to access the certificate and if it succeeds, the software existent on the device will sustain the owner to validate his or her identity. This verification is done with a signature attributed to a demand for authentication using the private key of the user. From here, the system responsible for approving the request is checking whether the signature is done by a valid and unaltered private key. If it passes the validation phase, the system can confirm that the request was not emitted fraudulently.

Similar to the methods presented above, this one can also have a risk of being exposed to vulnerability exploits. A major complication can come not just from the software used for signing the authentication request, but from the operating system found on the device too. There are malware programs that infect software applications present on a device which may or may not be traceable. If the malicious software gets in a position where it has elevated privileges, the certificate along with the keys used for identity verifications can be effortlessly taken. From this point on, remote accesses are likely to be initiated from the attacker's own devices with little chance to be uncovered.

Therefore, it is highly advised that these software certificates should only be used in transactions with reduced risk of data hacking and in systems that can guarantee the protection of the user's data. Another measure to be taken for securing the certificate is enabling a notification for every authentication request, which asks for a passcode in order to gain access to the certificate. If on the owner's device there is a Trusted Platform Module, which stores RSA encryption keys, then it can be utilized to enforce the security by storing the certificate within itself.

6. **U2F security key**

The universal second factor is a method of authentication which uses a physical token or a card, known as a U2F security key or authenticator. It uses special types of Universal Serial Busses or Near-Field Communication gadgets, that have technology like the smart cards presented before.

This USB token communicates with the aid of an interface that mimics a keyboard. Therefore, no additional software is needed to function properly on a particular system. When an individual requests access to a piece of data protected with this technique of authentication, the U2F security key verifies the identity of the initiator using public key cryptography methods, as well as a secret device key found on the device. Eventually, the key will sign a challenge-response type of request, which will be analysed for validation.

In order to improve their security, U2F security keys ought not to be stored with the owner's NFC devices as it can lead to data loss. In addition, it is recommended that only the security keys that have been approved by the most recent U2F specification version should be used for a secured experience.

U2F security keys are used as a supplementary method of two-step verification for online services such as Google, Dropbox, GitHub and even Facebook, having support in web browsers like Google Chrome and Firefox (Tony Tan, 2014).

7. **Physical one-time PIN token**

One-time passwords can improve protection of data access. They avoid the drawbacks of

standard static password authentication by having a limited time of validity to perform a request. Physical tokens are representing a mean of providing the user with a proper OTP by revealing it on its display.

There are many algorithms used for generating OTP, but for this particular technique of authentication, a time-synchronized algorithm is adopted. This method relies on a precise clock located inside of the token, that is synchronized with the authentication server's clock, as mentioned in (Dysprosia, 2004). It is essential that these are accurately configured in order for the password algorithm to work properly, as any new set of passwords generated is based on the current value of the time.

When users authenticate with a password of their choice, a one-time passcode is demanded by the system. A unique PIN is generated in conjunction with the synchronized clock shared between the token and the server and sent for submission. The authentication service will validate the information received and will decide whether to grant access.

For OTPs, the most noteworthy advantage over the classic passwords, which do not have a limited validity, is the immunity to replay attacks, commonly known as playback attacks. Because the generated password can only be used once within a time period, the attacker that obtained a previous OTP from that token would be restricted to enter the same passcode into the system.

Nonetheless, these time-synchronized tokens can in fact become unsynchronized. One way to deal with these unfortunate events is allowing the user to enter a few successive passcodes for the server to recalibrate.

Banks usually offer their customers these physical tokens for ensuring their transactions are conducted without any incidents. Other companies might opt for using security tokens for their employees if they want to safeguard access to some critical information.

CONCLUSIONS

Digital security is crucial nowadays and more vulnerable than before. By adding the multiple-factor authentication to any service that demands an identification phase from its users, the chance for cybercriminals to breach the security barrier will decrease substantially.

According to (Wireless friend, 2009), some supporters of this multiple-factor authentication claim that it can diminish the rate of online fraud, particularly identity theft. This is due to the fact that a stolen password would not be sufficient enough for an attacker to gain access to the victim's sensitive data. Cyberattacks can still be carried out against a MFA system, such as phishing and man-in-the-middle, but that would require more effort from the attacker.

In the past years, there have been reported an increasing number of successful breaches. Attackers, most of the time, do not just steal data, but rather alter or destroy it. A system which supports MFA will be able to restrict malicious programs from entering a critical zone, or at least slow them down until they can be discovered and eliminated.

In this context, it is highly recommended for every user to set-up at least a two-factor authentication method for all websites and applications which offer this feature. Sure, it will take some additional effort at the configuration phase and also at every attempt at an account login, but it pays off. The easiest method is configuring a multiple-factor authentication with SMS-based responses. For a better assurance, the physical key represents the most secure option for authentication, but requires the user to be more cautious.

All in all, multiple-factor authentication can be a life saver when it comes to securing the access to sensitive data. People are starting to realise the dangers of not rigorously securing their personal information and one method of overcoming this is through MFA.

REFERENCE LIST

Australian Cyber Security Centre, Australian Government, Australian Signals Directorate (2014) Implementing Multi-Factor Authentication, https://www.cyber.gov.au/publications/multi-factor-authentication

Dysprosia (2004) One-time password, https://en.wikipedia.org/wiki/One-time_password

Margaret Rouse (2012) differential power analysis (DPA), https://searchsecurity.techtarget.com/definition/differential-power-analysis-DPA

Margaret Rouse (2015) knowledge-based authentication (KBA), https://searchsecurity.techtarget.com/definition/knowledge-based-authentication

Margaret Rouse (2015) multifactor authentication (MFA), https://searchsecurity.techtarget.com/definition/multifactor-authentication-MFA

Margaret Rouse (2018) smart card, https://searchsecurity.techtarget.com/definition/smart-card

Nbarth (2014) False positives and false negatives, https://en.wikipedia.org/wiki/False_positives_and_false_negatives

Nitin Sharma (2018) What is 2-Factor Authentication and Why Should You Care?, https://hackernoon.com/what-is-2-factor-authentication-and-why-you-should-care-e8af5808d499

Tony Tan (2014) Universal 2nd Factor, https://en.wikipedia.org/wiki/Universal_2nd_Factor

Wireless friend (2009) Multi-factor authentication, https://en.wikipedia.org/wiki/Multi-factor_authentication

Zack Whittaker (2018) Cybersecurity 101: Two-factor authentication can save you from hackers, https://techcrunch.com/2018/12/25/cybersecurity-101-guide-two-factor/?guccounter=1&guce_referrer_us=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_cs=y7O8t7ciCc333VjnzpNKcw