Access Management Using Knowledge Based Multi Factor Authentication In Information Security

Engr. Umar Iftikhar [1†] Engr. Kashif Asrar[2††], Engr. Dr. Maria Waqas[3†††], Engr. Dr. Syed Abbas Ali[4††††]
umariftikhar@neduet.edu.pk kashifasrar@neduet.edu.pk
Computer and Information Systems Engineering Department
NED University of Engineering and Technology
Karachi, Pakistan

Summary
Today, both sides of modern culture are decisively invaded by digitalization. Authentication is considered to be one of the main components in keeping this process secure. Cyber criminals are working hard in penetrating through the existing network channels to encounter malicious attacks. When it comes to enterprises, the company's information is a major asset. Question here arises is how to protect the vital information. This takes into account various aspects of a society often termed as hyper connected society including online communication, purchases, regulation of access rights and many more. In this research paper, we will discuss about the concepts of MFA and KBA, i.e., Multi-Factor Authentication and Knowledge Based Authentication. The purpose of MFA and KBA its utilization for human to everything interactions, offering easy to be used and secured validation mechanism while having access to the service. In the research, we will also explore the existing yet evolving factor providers (sensors) used for authenticating a user. This is an important tool to protect data from malicious insiders and outsiders. Access Management main goal is to provide authorized users the right to use a service also preventing access to illegal users. Multiple techniques can be implemented to ensure access management. In this paper, we will discuss various techniques to ensure access management suitable for enterprises, primarily focusing/restricting our discussion to multifactor authentication. We will also highlight the role of knowledge-based authentication in multi factor authentication and how it can make enterprises data more secure from Cyber Attack. Lastly, we will also discuss about the future of MFA and KBA.
Keywords: *Cyber security, evolution, vision, SFA, 2FA, MFA, data breach, KBA.*

1. INTRODUCTION

Constant rise of the volume of smart device usage, associated networking aspects have the impact on the mobile networks across the globe. Authentication is the enabler that keeps the transmission of such huge volume of data protected in closely knitted environment.

Authentication is often referred to as a mechanism in which the system computes the values being sent by the user and match it against the existing value. This is also known as the process of user's identification. It is a fundamental safeguard against unauthorized entry, whether offline or online, to the computer or some other sensitive application

Initially, to authenticate the subject, only one factor was used. Single-Factor Authentication (SFA) was being commonly used because of its user friendliness and simplicity. For example, it is plausible to consider using a password or a PIN to validate a user's identity. This is obviously the lowest authentication standard. One will automatically compromise the account by exchanging the password. Additionally, by using social engineering strategies, rainbow table or the dictionary attack, an unauthorized user may still try to obtain entry. The minimum prerequisite of password sophistication is usually to be considered when using this form of authentication. Keeping in view all the associated risks of authentication with a single factor, the SFA was considered a weak method of protection. In addition, owing to a variety of security risks, validation within a single factor wasn't known to be reliable in providing of adequate protection. The overcoming process of the shortcomings faced by SFA, Two-Factor Authentication (2F) was introduced which combined username/password with the personal ownership factor, i.e., a card or phone number. With the advent of this new type of authentication, factor groups are now classified into 3 types:

1. *SOMETHING YOU KNOW:* As the name suggests, it is something that user already knows. That can be anything such as a password or any "secret".
2. *SOMETHING YOU HAVE*: This is related to what user possesses that includes tablets, cards, tokens, etc.
3. *SOMETHING YOU ARE:* This is the Biometric factor, and can also be explained as the physical aspect of the individual. For example, thumb impression, facial recognition etc.

Multi-Factor Authentication (MFA) quickly became famous because of the extra layer of security that it offered using multiple types of credentials. Using MFA offered seamless protection of hardware as well as other important facilities against unauthorized access. For the most part, MFA is focused on biometrics, in which people are instantly identified on the basis of their behavioral and

Manuscript received July 5, 2021
Manuscript revised July 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.7.15

biological characteristics. As users were expected to show proof of their identification, which is dependent on two or three different factors, this move provided an enhanced degree of security.

Figure A. The Evolution of Authentication Methods

Today, in situations where protection standards are greater than normal, MFA is required to be used. As per SC Data UK 68 percent of European citizens wants to use biometric as a primary method of verification for their transactions. Consider the daily cash withdrawal routine. Over here, operator must deliver a token which is physical, i.e., card, and follow up with a PIN code. By incorporating the second channel, this method could easily be made more complex. It could be achieved with facial recognition approaches in a more interesting scenario. In addition, a new survey showed that in 2017, Thirty (30) % businesses expected adoption of the MFA resolution, with Fifty-one (51) % percent reporting that are now using MFA, and 38 percent stating they are using it in "some areas" of operation. These stats further validate that MFA is indeed the right step forward in the development of authentication. There are three applications of MFA: business applications including e-commerce, ATM etc. Government applications and investigative applications Currently, MFA is an incredibly critical vector for: The authentication of the user's identity and of the electronic computer (or its system); Infrastructure link confirmation; Linked IoT devices including, tablets, smartwatches, phones, should be validated. The MFA approach should be as user-friendly as possible, such as:

1. To enable and control resources they are able to use, consumer's first have to register themselves and then validate with SP (Service provider);

2. Upon accessing the service, the customer should provide a SFA with the finger print or token authorized by the service provider;

3. User authentication is done by log/sign via the matching credentials provided in the user portal until first approved by the device (or social login). For additional security, secondary authentication factors will be allowed by the managing framework. Once the customer successfully is done with the checks, the frame-work then gives access to the portal automatically;

4. Verification (secondary level) is executed by itself on the basis of bio-metric authentication or (MFA). In other words, operator will only have to provide an extra code or the token if the (MFA) is failed.

2. POTENTIAL SOURCES OF MFA

Currently, a large number of sensors are used in authentication mechanisms, allowing a user to be identified. In this section of the paper, we address the MFA-appropriate variables, what types of sensors are available on the market, and their associated challenges. Additionally, we will also talk about the steps to be taken in immediate future.

2.1 *PROTECTION USING PASSCODES:*

The traditional method to validate an operator stands by requesting password or a Personal identification number (PIN) code. Information factor historically reflects the hidden pass-phrase. To authenticate the user, it only takes a basic input system (at least one button).

2.2 AUTHENTICATION VIA TOKEN:

A physical token, such as a passport, which is suggested as a second factor party, should then be added to the password. A costumer can use a mobile, smartwatch, etc., which are more difficult to use from the hardware perspective.

2.3 BIOMETRIC USING VOICE:

Majority of current electrical devices now comes consisting of a mic which gives allowance to speech recognition which can be used as MFA factor. Unfortunately, downside of using speech recognition as method of authentication is that it might allow agencies to recognize speakers as well as imitate their voices.

2.4 FACE RECOGNITION:

At start of the development of face recognition method, the technology used image analysis which was quite easy to clone by supplying a picture to the system. The next stage was to enable three-dimensional identification of the face, by requesting the user to turn the head in a particular way during the authentication process. Lastly, development of the device has come up to the point where it is understanding the user's individual expressions.

2.5 IRIS RECOGNITION TECHNIQUE:

The methods for iris detection have been on the market for more than 20 years. When studying the color pattern of an individual's eye, this technique does not enable the consumer to be close to the capture system. Another enticing method is retina examination.

2.6 RECOGNITION VIA HANDS:

To authenticate the individual, certain programs employ the study of the actual form of a hand. Pegs were being

deployed for this purpose but the usability of such methodology was quite low.

2.7 RECOGNITION OF VEINS:

Fingerprint scanners provided the option to read even the finger's vein. To obtain and archive the movement of the whole hand, more complex systems use palm print recognition.

2.8 FINGERPRINT AUTHENTICATON:

The majority of mobile phone vendors are now moving to use fingerprint scanners as the main authentication mechanism. This approach is intuitive but is very simple to produce, primarily since our fingerprints can be acquired from nearly everything we touch.

2.9 AUTHENTICATION USING THERMAL IMAGE:

In this case, thermal sensors are used to recreate the unique thermal picture of the blood supply of one's body in the vicinity.

2.10 GPS BASED AUTHENTICATION:

A special case of position-based authentication is the use of the spatial location of the device and customer. Because of the transmission properties, the GPS signal may easily be jammed or deemed defective; it is thus advised to use a minimum of (2) Sources of location, such as Global positioning system (GPS) and the wireless network ID.

3. CHALLENGES ENCOUNTERED

For the implementation of secure identification and multi-factor authentication, user acceptance is a vital feature. Considering, it's very important to track a deliberate and detailed method when implementing and executing MFA solutions.

3.1 COMPATIBIITY:

Three viewpoints could describe the key usability problems that arise in the authentication process. Availability of the task: time to register and time for device authentication. Effectiveness of the task: attempts to login for authentication and User personal opinion.

INCORPORATION:

In spite of all the usability problems being implemented, integration raises more concerns together within technical in addition human viewpoints. Majority solutions of MFA in relation to the market are hardware-based.

3.2 PROTECTION:

A digital infrastructure consisting of essential elements, such as sensors and computing units is any MFA platform. Both of these are usually vulnerable at completely different levels to a range of threats, reaching from repetition of attempts toward enemy outbreaks. Protection is therefore critical instrument for privacy towards being allowed also protected. During transmission between the sensor and the computation device, sensitive data breach is a possibility. Such robbery can occur primarily because of transmission which is unsafe through the input device respectfully to the database also there is a potential for an attempt. Danger is also associated with attacks in relation to the locations. The global positioning system (GPS) signals might be inclined to the location locking and feeding incorrect information to the receiver so that an inaccurate time or location is measured. For cellular- and WLAN-based location services, related strategies can be applied. The MFA architecture should provide comparatively high "throughput" ratios, representing a system's capacity to satisfy its operators' expectations in regards attempts of inputs amounts per time extent. A penetration assessment panel may also be sponsored by the MFA security platform to determine the possible vulnerabilities.

3.3 DURABILITY:

Even if the protection and privacy issues are thoroughly addressed, from the very beginning of their journey, biometric devices, mainly fingerprinting, have fallen short of achieving the "robustness" criterion. This was primarily due to operational experiments being carried out instead of field tests in the laboratory setting.

4. KNOWLEDGE BASED AUTHENTICATION

Knowledge Based Authentication is another strong measure to prove that the person who is providing the authentication information is truly that person. As its name clearly states KBA uses the knowledge possessed by the individual.

These four requirements should comply with a successful KBA query:

- The question should be appropriate for a large segment of the population.
- Easy answer.
- The answer to the argument should be one.
- Difficult retrieval of answer.

It is categorized into three forms with noticeable differences: a) Static KBA, b) Dynamic KBA, c) Enhanced KBA

a) Static KBA

Static KBA can be explained is shape of set of secrets that are pre agreed and that allows operators in picking safety questions also to deliver answers to which remain logged by the organization to be accessed later. Organizations are moving away from this method because questions are too generic and can be easily hacked.

b) Dynamic KBA

These are referred to as "out of the wallet" questions that are not pre-defined but created using a variety of data sources in real time.

c) Enhanced Dynamic KBA

Enhanced dynamic KBA goes one step further and makes the authentication process more secure, as it uses proprietary data stored behind firewalls and creates authorized question for relevant users, ensuring end to end authentication.

4.1 KBA CHALLENGES

Fig. 2 specifies the difficulties of KBA, it talks about fundamental issues, security and ease of use, however it incorporates the attributes that are separated into six categories. The Challenge of security contains safety problems, accessible individual information, and the confidentiality.

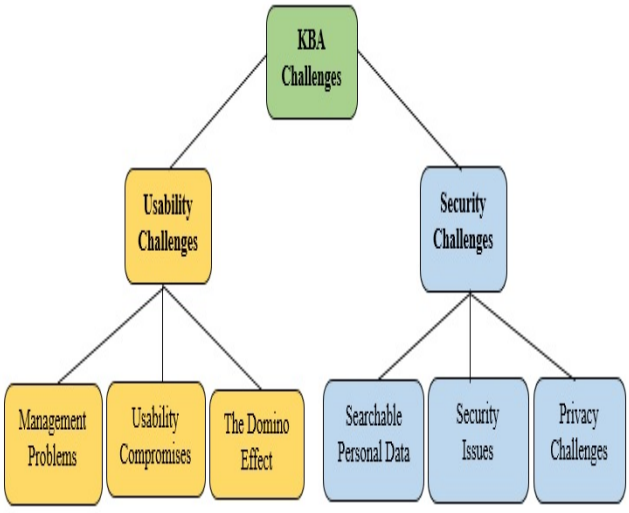

Figure 2. The challenges of KBA

4.1.1 Security / Confidentially Challenge

It is by which individual information is saved, in different domains. This classifies into three sections: attack types, searching about individuals' data or recognition, and confidentiality in regards to the client account.

Confidential/Security challenge is classified into further types:

a) Searchable personal

It becomes simple for users when the password they use is same across multiple social networks, but such scenario is considered a challenge due to login circulation and redundancy. That may be activated by simple guessing or attacks.

b) Security / Confidentially Issues

Many kinds are present if we talk about threats and hacking that include a false account or data theft. Security's biggest obstacle is guessing passwords for the account. There are numerous online and offline methods for guessing passwords that are being used. Inclusion of CAPTCHA in programs is the popular solution to avoid guessing when online.

The offline technique needs no computing resources, but it is based on guessing passwords multiple times while lettering them in such way that it is known to be repetitive.

c) Privacy / Confidentiality challenges

In order to ensure privacy, policies and regulations are often devised the aim of which is to regulate access to consumer data.

Thus, to diffuse attacks, a need in creating security enquiries that shall be neither confidential to operators nor biased against individual users.

4.1.2 Usability Challenge

Due to the convenience of using the same password in different domains and programs, accessibility is considered a key difficulty in handling user accounts. Yet it is a challenge that endangers personal protection and secrecy.

a) Problems Related to management

It consists many issues, like organizational security many people whom, owing similarity of passwords and verification concerns, wish to use the system. They dont comprise of values that are default, texts, also companies consist of fast retrieval strategies for unexpected outbreaks.

b) Usableness compromises

Opportunity to question usableness offers some capacity for the individual. Audio and Graphical trials somehow be acquired. Use of the similar key is a concern for user accounts on many platforms. Users are targeted by attackers

without the user's knowledge by guessing user identities and passwords. Such password guessing has many policies to mitigate the difficulty of memorability of passwords.

c) The domino effects

A group of identical events are introduced as a result of this accumulative impact. It's a sequence of dominoes crashing, also best described as mechanical influence.

5 ACCESS MANAGEMENT TECHNIQUES

5.1 Centralization

An enterprise primary technique towards data breach is to deploy a solution to centralize views, controls and authority over user's identities. Any organization's network primary comprises of applications, databases, portals, data traffic flows, recommended measure to keep an eye on all the moving parts.

5.2 Role Based Access Control

The purpose of this type of access control is to restrict user's permission to their roles inside the infrastructure for example, an old employee of a firm should not have access to digital financial account. Any enterprise foremost security measure should be to assign clear and designated roles to users. RBAC helps in facilitating, Cyber Security Visibility, Business Processes, Identity Security is also of immense importance not to grant relaxations to users outside their roles, temporary privileges should expire in under a certain timeline.

5.3 Zero Trust Identity Security

Incorporation of multiple checkpoint to get your identity authenticated and is called zero trust identity security. In a nutshell, any organization should never trust anyone under any circumstances. They should not allow anyone to get connected to your database and network. It should first undergo a series of steps to authenticate.

5.4 Principle of Least Privilege

This technique parallels RBAC as they both work to limit privilege being granted to users. This highlights that users should only be granted those permissions which are necessary for their specific job or role.

5.5 Automated Onboarding

Automated onboarding process ensures that the users get started just with the right permissions.

5.5 Orphaned Account Detection and Removal

Failure in the process of employees off boarding results in management failures and allows the cyber criminals to use these accounts as gateways to breach into the system and result in cyber-attack.

Techniques should be implemented to mandate and automate the process of off boarding to make sure that no orphaned accounts have slip pass identity security.

5.7 MFA

Single factor authorization hasn't proven to be reliable barrier various vulnerabilities. Cyber criminals can easily guess password-based logins systems or applications etc. Moreover, user's repetitively using username passwords for multiple sites for their ease has made it easier for cyber scams.

5.8 KBA

Asking the right questions with the right data is not enough to refine the KBA tool for reliable, efficient and stable identity authentication. Although various research suggest consuming a graphical or image authentication mechanism, yet Textual KBA is still a widely used authentication method. The method has its own downside which makes it challenging to protect against attackers. Therefore, there is no single sustainable model that fits all organizations' needs.

6. CONCLUSION

The protection of data is crucial to maintain critical operational information for a company. The use of additional resources like MFA has been utilized to establish control over data. Not only does Multi Factor Authentication (MFA) add an additional step when authenticating users but also adds another layer of assurance and security. Logging of MFA attempts can be viewed and used in security analyst work. Knowledge Based Authentication (KBA), even with all enhancements and improvements remains an imperfect authentication method if independently introduced. KBA may be used as a wide spectrum approach to authentication if used as a component in Multi Factor Authentication (MFA). Hackers will still be able to get their hands on the data, but further effort is required than searching up public information or collecting aggregated data. In contextual based systems, KBA can be used as a contingency approach when users fail to meet the requirements for other forms of authentication.

References

[1] VNI Ciso Global Mobile Data Traffic Forecast 2016–2021. White Paper, 2017.

[2] Lamport, L. Password authentication with insecure communication. Commun. ACM 1981, 24, 770–772.

[3] Benarous, L.; Kadri, B.; Bouridane, A. A Survey on Cyber Security Evolution and Threats: Biometric Authentication Solutions. In Biometric Security and Privacy; Springer: Berlin, Germany, 2017; pp. 371–411.

[4] Boyd, C.; Mathuria, A. Protocols for Authentication and Key Establishment; Springer: Berlin, Germany, 2013.

[5] Mohsin, J.; Han, L.; Hammoudeh, M.; Hegarty, R. Two Factor vs. Multi-factor, an Authentication Battle in Mobile Cloud Computing Environments. In Proceedings of the International Conference on Future Networks and Distributed Systems, Cambridge, UK, 19–20 July 2017; ACM: New York, NY, USA, 2017; p. 39.

[6] Konoth, R.K.; van der Veen, V.; Bos, H. How anywhere computing just killed your phone-based two-factorauthentication. In Proceedings of the International Conference on Financial Cryptography and Data Security, Christ Church, Barbados, 22–26 February 2016; Springer: Berlin, Germany, 2016; pp. 405–421.

[7] Kim, J.J.; Hong, S.P. A method of risk assessment for multi-factor authentication. J. Inf. Process. Syst. 2011, 7, 187–198.

[8] Dasgupta, D.; Roy, A.; Nag, A. Toward the design of adaptive selection strategies for multi-factor authentication. Comput. Secur. 2016, 63, 85– 116.

[9] Grassi, P.A.; Fenton, J.L.; Newton, E.M.; Perlner, R.A.; Regenscheid, A.R.; Burr, W.E.; Richer, J.P.; Lefkovitz, N.B.; Danker, J.M.; Choong, Y.Y.; et al. NIST Special Publication 800-63B. Digital Identity Guidelines: Authentication and Lifecycle Management; Technical Report; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2017.

[10] Gunson, N.; Marshall, D.; Morton, H.; Jack, M. User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. Comput. Secur. 2011, 30, 208–220.

[11] Schneier, B. Two-factor authentication: Too little, too late. Commun. ACM 2005, 48, 136.

[12] Petsas, T.; Tsirantonakis, G.; Athanasopoulos, E.; Ioannidis, S. Two-factor authentication: Is the world ready?: Quantifying 2FA adoption. In Proceedings of the 8th EuropeanWorkshop on System Security, Bordeaux, France, 21 April 2015; ACM: New York, NY, USA, 2015; p. 4.

[13] Wang, D.; He, D.; Wang, P.; Chu, C.H. Anonymous two-factor authentication in distributed systems: Certain goals are beyond attainment. IEEE Trans. Dependable Secur. Comput. 2015, 12, 428– 442.

[14] Sun, J.; Zhang, R.; Zhang, J.; Zhang, Y. Touchin: Sightless two-factor authentication on multi-touch mobile devices. In Proceedings of the Conference on Communications and Network Security (CNS), San Francisco, CA, USA, 29–31 October 2014; pp. 436–444.

[15] Bruun, A.; Jensen, K.; Kristensen, D. Usability of Single- and Multi-factor Authentication Methods on Tabletops: A Comparative Study. In Proceedings of the International Conference on Human-Centred Software Engineering, Paderborn, Germany, 16–18 September 2014; Springer: Berlin, Germany, 2014; pp. 299–306.

[16] Harini, N.; Padmanabhan, T.R. 2CAuth: A new two factor authentication scheme using QR-code. Int. J. Eng. Technol. 2013, 5, 1087–1094.

[17] Scheidt, E.M.; Domangue, E. Multiple Factor-Based User Identification and Authentication. U.S. Patent 7,131,009, 31 October 2006.