International Journal of Engineering Research and Technology. ISSN 0974-3154, Volume 12, Number 12 (2019), pp. 2396-2402

Developing Knowledge based Authentication Mechanisms in Governmental Organization

Ali Alkhalifah† and Saleh Albahli††

Department of Information Technology, College of Computer, Qassim University, Saudi Arabia.

†ORCID: 0000-0001-6317-4313

Abstract:

More corporate applications and information nowadays have been accessible through the Internet. Users are concerned about their security of their activities that they apply on implement in the cyber world or any other place where authentication is required The importance of Information security realm have been increased these days. The new wave of attack (Shamoon virus) in Saudi Arabia have an impact on different organizations. Many governmental organizations suffered from the huge cyber-attacks since more than 35,000 computers were wiped and destroyed. Authentication is an im-portant part when we interact with different technologies and online systems. The au-thentication is an aspect of data security, its current scheme used nowadays in the sys-tems is depend on the login by user name and password in addition to one-time pass-word or traditional secret question, which in turn is usually easy to predicate. The con-cept of knowledge based authentication (KBA) is gaining wide acceptance gradually with time. It gives the user an authentication on the basis of knowledge of some secret information, regularly via a real-time interactive question and answer process. Our methodology identifies drawbacks in the existing mechanisms of knowledge-based au-thentication systems and enhances its security by adding extra layers including end-user training, password chunking and secure password usage policies. The aim of this pro-ject is to provide enhanced knowledge based authentication solution which ensures and provide more security and usability levels for both individuals and governments.

Keywords: KBA, Password Chunking, End-user Training, Saudi Arabia vision 2030.

I. INTRODUCTION

Security is an important aspect of business model. Every organization takes users personal data on first priority and make policies in order to protect their data from being leaked. The most important aspects of security are confidentiality, integrity and availability which is also called CIA triad. There are several mechanisms to provide these security services in order to protect data from security breaches. Confidentiality can be achieved by strong encryption mechanisms using public key cryptography. Integrity can be achieved by using hash mechanisms. Availability can be achieved by using backups, load balancers, firewall rules and RAID. Authentication can be achieved by Digital signatures, passwords and other similar mechanisms.

Basically, authentication can be achieved by using three ways which are [1]:

1- Token-based authentication.

2- Biometric-based authentication.

3- Knowledge-based authentication.

These methods are further classifier into sub categories which is illustrated in the figure 1 given below:

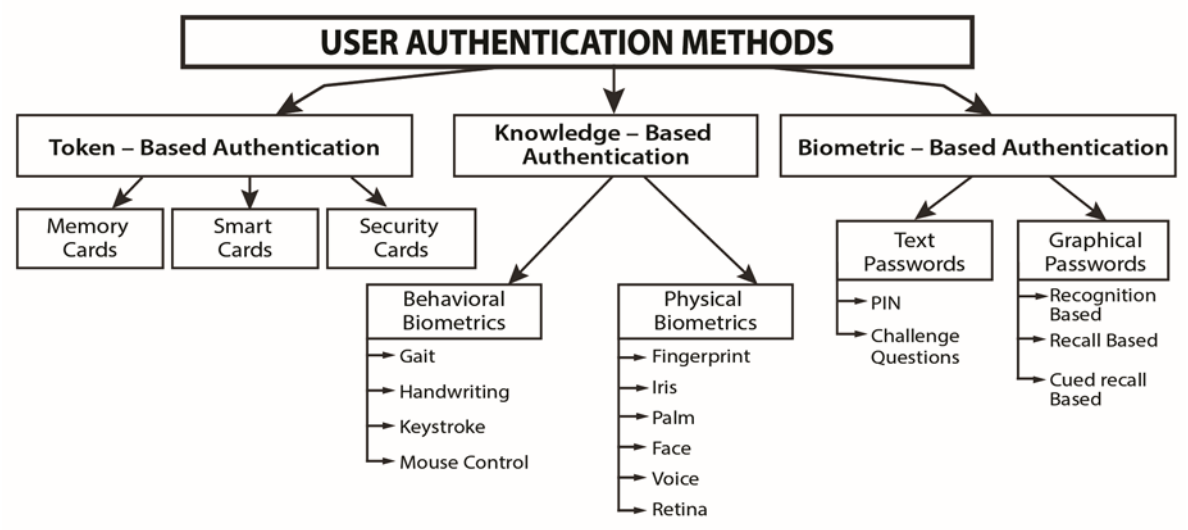

Figure 1: Methods of Implementing User Authentication

Knowledge-based authentication is one such mechanism in which user's personal information is asked from the user in order to authenticate and access the resources. Authentication may be done by asking password or security questions. KBA by using security questions tends to authenticate users by asking security questions related to that person. The simplest form of knowledge-based authentication works by asking secret question at the time of sign-up and then this question is asked when the user logs in to the system. In case of correct answer, the user is given access to the system. This mechanism assumes that only the authorized person will be able to answer the secret question since it is related to person's personal information or memories.

Types of Knowledge-based Authentication:

There are three types of knowledge-based authentication mechanisms that can be implemented in any organization. These three types are listed below [2]:

Table 1: Types of Knowledge-based Authentication

S. No	Type	Definition
1	Static-based KBA	Works by using pre-shared secret answer to the question between the client and server. At the time of authentication, user is asked that question and the answer is compared with the provided answer. If the provided answer matches with the database, user is authenticated to the system.
2	Dynamic-based KBA	By asking questions on real time based on user's demographic data or credit information. The questions are random and unknown which are presented in real time.
3	Customer-based KBA	These questions are related to customer historical data and interactions which are more relevant and safer to use by using multiple type questions. This type is also known as enhanced KBA and the questions are similar to Dynamic KBA.

Earlier KBA uses static-based authentication that works by using shared secret answer to the questions between the system and user at the time of signing up for application. Static KBA is easy to set up and does not require utilize more processing power.

The secret question can take variety of parameters including the following:

1- What is your favorite place?
2- Who is your favorite teacher?
3- What is the first school you attended?
4- Who is your best friend?
5- What is your birthplace?
6- What is the last name of your best friend?
7- Which is the first place you visited?

The overall mechanism of Static-based Authentication is illustrated in figure 2.

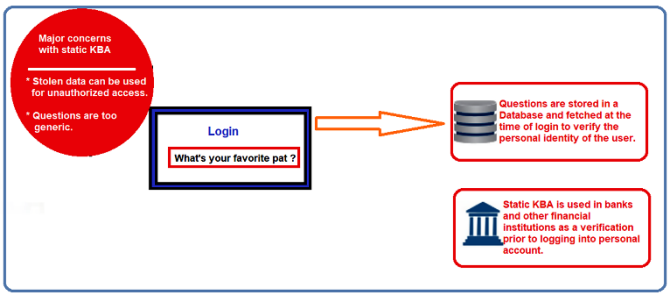

Figure 2 Working mechanism of Static-based Authentication

The figure 2 shows the login where of the e-commerce website where users are authenticated using static-based authentication. The question "What's your mother's maiden name?" is asked by the user and the answer is checked by comparing results with the database results. If the answer matches the stored result, the user is authorized and given access to the system. In case of incorrect answer, the user is given chance of few attempts and then blocked if user is unable to answer the secret question [3].

On the other hand, Dynamic-based authentication works by generating questions in real-time using information from various sources like user's past transactions and history, demographic data and other sources that can be helpful to verify the user. Dynamic-based authentication is more secure and user-friendly than static-based authentication since it does not require to memorize the answer. The questions in this mechanism keeps changing with time and they are generated in real-time after collecting data from different sources.

Figure 3: Methodology of Dynamic-based Authentication

Figure 3 shows the overall structure of the Dynamic-based authentication cd. The figure shows that in this mechanism,

the user is provided with real-time questions after extracting data from several sources. The sources in figure 3 show the following records.

1- **Public records**: This records includes general information about the user which is publicly available like from social media and other known facts.

2- **Marketing Data**: This information is extracted from the marketing stats and history.

3- **Credit Reports**: This information contains user's credit records and transactions.

4- **Other recorded facts**: Other recorded facts that are known by the system.

The third type is **customer-based KBA** in which multiple choice questions are asked by the user with only one correct answer. This type, also known as enhanced KBA is more user-friendly than other types discussed above. This type is mostly preferred by the users since the user does not require any type of memorization or hard work. The questions asked are similar to Dynamic-based authentication which consists of user's historical data, transactional data and other demographic data.

II LIMITATIONS OF EXISTING TECHNIQUES

All types of KBA works by assuming that if the correct answer is given, the identity of the user has been confirmed and given internal access to the system for which he is authorized. Each type of KBA has its own limitation which is illustrated in the table 2.

Table 2: Limitations of KBA

S. No	Type	Limitations
1	Static KBA	- Easy to guess secret answer. - Requires users to memorize things.
2	Dynamic KBA	- Difficult to set up. - Requires much more processing. - Time consuming.
3	Enhanced KBA	- Requires more processing power. - Time consuming. - Information can be collected by hacking user's social media accounts or social engineering.

Apart from these limitations, the latest studies show that each type of KBA is breakable if proper enumeration is done by the Hackers. Hackers can steal personal information by hacking into Gmail, facebook and other accounts and get a lot of information. From where, it becomes easy to guess the right answer. With the enhancement of technology, Biometric factors are also used as an alternative to KBA in order to access the system. However, biometric features can also be stolen like iris and fingerprints by using advanced social engineering techniques [6].

Graphical passwords or security questions on the other hand having advantages over textual based passwords are rarely used because of its high cost and other issues. Figure 4 shows the pros and cons of using graphical password over text-based password [7].

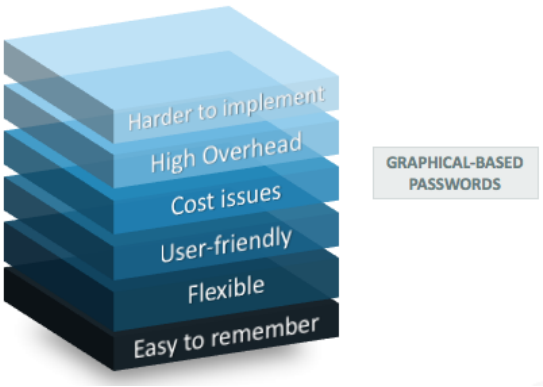

Figure 4: Pros and Cons of Graphical Passwords

This paper aims to solve the issues in these types of knowledge based authentication mechanisms by proposing a new prototype that can solve the usability issues in text-based knowledge based authentication mechanisms.

III. RELATED WORK

In order to identify gaps in current knowledge-based authentication mechanisms, we studied the similar work done in the past and give a brief introduction related to KBA. Kraus [8] performed a survey on user experiences in authentication mechanisms. The author addressed several issues in knowledge-based authentication including password handling practices of users, managing high number of passwords, strategies for password creation and password sharing. The author also addressed how positive feelings can impact on security behavior when choosing questions for authentication. Furthermore, the use of biometrics also seems to be influenced by positive and negative emotions of the users. Therefore, it is very important to consider flexibility and usability when implementing security controls.

Karim [9] conducts research on authentication methods used in online examination. The author also highlighted the threats that may occur during online examination systems. The authentication mechanisms are classified into four categories namely knowledge-based (What you know?), biometric (What you are?), Token (what you have?) and other mechanisms (physical location of the user i.e. where are you, timestamp, IP address etc.). The main threats in online examination systems are mainly because of impersonation that affects credibility of the examination authority. The author suggests various ways to improve online examination systems including merging biometric-based authentication and traditional password-based mechanisms.

Hong [10] conducted a research on whether combining more than one biometric factor can increase performance or not. The author by conducting and performing empirical study shows that performance can be significantly improved by using multi-biometric. The results from his experiments shows that by merging facial and fingerprints, performance can be increased significantly.

Saudi Arabia Vision 2030:

According to Saudi Arabia vision 2030, more IT infrastructure will be developed and everything will be digitalized. With more digital infrastructure, it attracts financial sector including Banks, insurance companies, investment companies and real estate firms. However, it imposes more threats if proper authorization is not present in the digital systems. In order to make sure that only authorized persons get access to the system, the knowledge-based authentication mechanisms should be properly analyzed before implementing it.

Our research is focused on improving knowledge-based authentication mechanism by providing a prototype for Banking sector.

IV. METHODOLOGY

The security of the knowledge based authentication is still questionable since it requires a good question bank that can never be guessed by anyone. Generating such questions is always challenging since it requires questions with such answers that is easy to remember for users and hard to guess for Hackers.

Our proposed solution highlights the usability issue in text-based security questions in order to make it more interactive for users accessing and processing financial transactions. This project will help the security researchers and industries to interact with each other and implement this prototype in order to make this system more effective.

Our contribution in knowledge-based authentication mechanism to the community of banking sector in Saudi Arabia as per vision 2030 is as follows:

1- End-user training to choose complex security question.
2- Identifying gaps in text-based passwords.
3- Training to the user to choose an answer which is less likely spoken in daily life.
4- Enforcement by banking sector to generate strong security questions.
5- Choose easy to remember answer without compromising security threshold.

Our methodology starts by identifying issues in text-based passwords and answers to security questions.

Following issues are addressed by reviewing several literature papers in the past.

1- Password space:

When choosing a password as a PIN number, it is often assumed that user will choose a 4-digit pin which is secure enough to protect against PIN number guessing. Since the password space is only 4 digits which can only generate 10,000 unique numbers. It is easy for an Attacker to conduct password spraying attack on different accounts of the same user. It is the human nature to use same password for all accounts, Hacker can take this to his advantage and access the victim's account.

Our prototype can solve this issue by providing end-user training to the users by providing multiple choice questions which ensures that user has created strong and unique PIN number. The multiple choice questions for this issues are designed and listed under the table 4.

Table 3: Question bank to choose unique 4 digit PIN

S. No	Question to choose unique PIN number	Yes/No
1	Are all four numbers in the password unique?	-
2	Have you used this PIN number in other accounts?	-
3	Does anyone knows about this PIN number in your circle?	-

These questions will be asked at the time of choosing of the PIN number in order to train end-users and enforce them to use unique passwords. If all the questions are marked as **Yes**, it will redirect to the new page confirming that new password will be created. If any of the question is marked as **No,** it will ask user to fulfill the requirements.

2- Password Creation Policies:

Password creation policies is the major concern of the user's privacy since majority of the breaches are caused because of weak passwords. The following policies should be implemented by financial sector including bank to make sure that users are using the strong passwords for their accounts.

i- Password should be at-least 8 characters long.

ii- Password should contain one special character, one capital letter and one number.

iii- Password should not contain words used in dictionary.

iv- Password should not be distributed to anyone.

v- Password should not be stored in any digital device or physically without any protection.

vi- A single password should not be used for more than 3 different accounts.

These policies are the mandatory to implement and train users on how to choose complex passwords. Apart from these policies, there should be a password generation mechanism implemented in the website that generates unique strong passwords every time the user clicks on the generate password button.

3- Password Handling policies

Password handling is a major issue which a lot of users find it difficult task. A single user owns multiple accounts most of them with a same or similar password. This is a great threat since compromising

password of a single account can lead to the compromise of multiple accounts of the user. This issue can be addressed by multiple ways. One way is to check on the website "https://haveibeenpwned.com/" for a compromised account. The website takes email address and checks if the email has been compromised in the past or not. If the email is found to be compromised, then the user must change the password wherever this email has been used. The owner of the website Troy Hunt made it as open-source to be used for everyone.

Strong Password Creation using Password Chunking Technique:

Our Prototype includes Password chunking which is relatively new method used to create passwords by chunking different pieces of information. Our prototype will enforce users and suggest different items which they can select and create passwords by combining these pieces. Our prototype will automatically create and suggest password once the items from the list are selected by the user. An example of password chunking technique is given in figure 5:

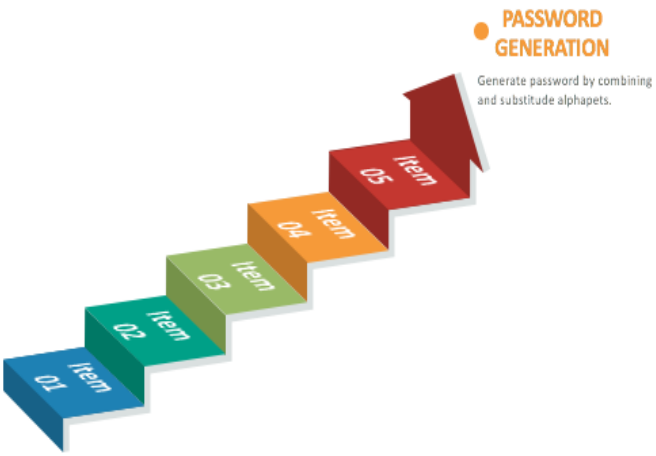

Figure 5: Prototype for password chunking

Our prototype will enhance user authentication mechanism since the password will be easy to remember by the users as well as complex to crack by the Hackers. The prototype for password chunking will not only generate passwords by combining selected words but also make it more complex by substituting some of the alphabets mentioned below:

i- "a" will change to "@".

ii- "i" will change to "!".

iii- "e" will change to "3".

iv- "o" will change to "0".

v- "j" will change to "7".

These substitutions will not place every time since it will become more predictable. The algorithm will randomly perform substitution in order to generate complex password. After the algorithm completes processing, it will ask user to pick suggested password or use their own password. If the user chooses to create his own password, then it will be compared against the checklist in Table 3.

Criteria for selecting static KBA Questions:

Our prototype meets the following criteria for selecting questions for authentication [5]:

1- The questions should be designed such that it is appropriate for large number of customers.

2- The answer should be something that users can easily remember.

3- The question should only have one correct answer.

4- The answer should be such that it cannot be guessed.

5- The answer should not be discovered through search engines.

6- Other parameters considering human interaction with the system in mind.

End-user training:

After suggesting and implementing strong password by using password chunking, our prototype has a module that will train end-users by explaining how passwords have been stolen in the past and how they can improve knowledge-based authentication mechanism to protect themselves from being hacked. Our training will be focused on these areas:

Table 4: Training Types to improve KBA

S. No	Training type	Purpose
1	MCQ's based training	To promote awareness by asking security questions in order to know how much they know about best security practices
2	Video tutorials	Providing video tutorials to make them aware about best practices of using knowledge based authentication mechanisms.
3	Slides	To provide knowledge about hacking incidents in the past due to weak password policy and end-user training.

The first type should be used to self-educate the users and the questions will be randomly selected from the pool of MCQ's questions. These questions will be based on self-awareness

and basic security questions as mentioned below.

Table 5: Question Bank for self-awareness

S. No	Question	Answer	Ranking
1	How often do you change password of a single account?	A- 1-3 months B- 3-6 months C- More than 6 months	High
2	Where do you store password if it seems complex to you?	A- Physical paper. B- Mobile with screen lock C- Other digital device with encrypted app?	High
3	How often do you feel comfortable if a friend asks your login information or asks you to login on your friend's system?	A- Not comfortable at all? B- Comfortable since I trust them? C- I don't provide this information to anyone	High

Our prototype saves the results and based on the ranking, it will suggest on which points you should work to improve your online security so that no one can get unauthorized access to the system.

The second training type covers video tutorials on several security topics including privacy and different scenarios on how a password can be stolen for example. The attacks are categorized into six classes as follows:

1- Using Shoulder surfing:

This type of attack involves the physical presence of the Adversary/Attacker where he observes the person behind the shoulder when he is typing the password. This attack can be prevented by making sure that no one else is behind a person or spying using CCTV cameras or any other medium.

2- Using key loggers installed in your friend's system:

This attack utilized the key logger software installed on someone else's system so that whatever keystroke is entered is saved in the Attacker's machine. This attack can be prevented by never typing sensitive information on any other system that you own.

3- Dictionary attack:

This is the type of attack where attacker uses the long dictionary containing common passwords and fuzz the login page with these passwords. Prevention to this attack can be achieved by using strong passwords that are not listed in any password dictionary.

4- Brute force attack.:

This attack is similar to Dictionary attack except that it uses all possible forms of combinations to fuzz the login portal and try luck of achieving the password. In order to protect this attack, it is recommended to use password of long length and use combination of special characters, capital letters and numbers.

5- Social engineering attack:

This attack involves understanding human psychology and exploit their trust to gain their password. An attacker can use tricks such that asking for help or providing help and build their trust. After building the trust, they exploit this relationship and extract sensitive information by talking to the victim or similar means.

6- Phishing attack:

This attack involves technical knowledge where Attacker designs a page similar to a legitimate financial website and sends this page to victim. Victim thinking this as a legitimate page will provide login information in order to access his portal. Once the user sends login information, it will be sent Attacker hosting server where he will gain information to access the victim's portal.

Security Question for KBA

The last function of our prototype is a mechanism to provide multi-factor authentication by using security question. Security question is also taken as a complex thing to remember by end-users since they find it difficult to memorize. Our prototype will solve this issue by providing easy to remember security question without effecting its security threshold. Our security question mechanism should work on following criteria:

1- It easy for users to remember.

2- It should be difficult for Hacker to guess.

To answer the first criteria, our mechanism will use graphical based icons as an answer to security question. To answer the second criteria, our mechanism will use several security questions with only one correct answer. There will be a rate limit for incorrect guesses after which the account will be blocked for a certain period of time.

Survey for participants:

Every product has a door of improvements and getting feedback by the end-users is the best way for this purpose. By asking survey questions, there is a possibility to improve this prototype, the survey consists of the following questions:

1- Do you think it is easy to create your password using this prototype?
2- Do you think this mechanism is secure than other mechanisms out there?
3- Do you like this new prototype?
4- Do you think it will help you create strong passwords?
5- Do you think it will help you create memorable passwords?
6- Do you prefer this prototype for creating all your passwords?

V. CONCLUSION

Knowledge-based authentication mechanisms have become very popular now days to its ability to provide a secure mechanism to authenticate users. It can be used as a multi-factor authentication mechanism to provide defense-in depth mechanisms. Recently, graphical passwords and security questions are used but it has an overhead of cost. The issues with KBA are not new and the most serious concern over this system is that the passwords and security questions can be guessed to compromise victims.

We have a designed a more secure prototype of KBA that can help not only in multi-factor authentication but also to train end-users to minimize the risk of human hacking. Our prototype suggests and enforce strong passwords and train end users using several means including multiple choice questions, video tutorials and providing news about recent breaches by compromising weak passwords. Our prototype will help security researchers to study and implement this prototype in financial sector of Saudi Arabia so that the vision 2030 can be achieved without any security risks.

ACKOWLEDGEMENTS

The authors gratefully acknowledge Qassim University, represented by the Deanship of Scientific Research, on the material support for this research under the number 3864-coc-2018-1-14-S during the academic year 1439 AH / 2018 AD.

REFERENCES

[1] Ajzen, I. (1988). Attitudes, personality, and behavior. Milton-Keynes: Open University Press.

[2] Ajzen, I. (1991). The Theory of Planned Behavior. Organizational Behavior and Human Decision Processes, 50, pp. 179-211.

[3] Anderson, R. (1993). Why cryptosystems fail. In Proceedings of the 1st ACM Conference on Computer and Communications Security, pp. 215-227

[4] Bada, M. and Sasse, A. (2014). Cyber Security Awareness Campaigns: Why do they fail to change behavior?. Global Cyber Security Capacity Centre, University of Oxford, UK

[5] Barton, B. F. and Barton, M. S. (1984). User-friendly password methods for computermediated information systems. Computers & Security, 3(3), pp. 186-195.Bensinger, D., (1998), Human memory and the graphical password, Passlogix, White Paper.

[6] Bensinger, D., (1998), Human memory and the graphical password, Passlogix, White Paper. Bettinghaus, E. P. and Cody, M. J. (1987). Persuasive Communication (4th ed.), Holt, Rinehart & Winston, New York: NY.

[7] Bishop, M. and Klein, D. V. (1995). Improving system security via proactive password checking. Computers & Security, 14(3), pp. 233-249.

[8] Kraus, L.; Antons, J.N.; Kaiser, F.; Möller, S. User experience in authentication research: A Survey. In Proceedings of the PQS 2016, Berlin, Germany, 29–31 August 2016; pp. 54–58

[9] Karim, N.A.; Shukur, Z. Review of User Authentication Methods in Online Examination. Asian J. Inf. Technol. 2015, 14, 166–175.

[10] Abdelkarim, N., Shukur, Z. (2015) "Review of User Authentication Methods in Online Examination", Asian Journal of Information Technology, 14 (5), 166-175.