Enhanced Knowledge Based Authentication Using Iterative Session Parameters

Ali Alkhalifah, Geoff D. Skinner

***Abstract*—**Current Knowledge Based Authentication (KBA) schemes have been subjected to increasing criticism of late due to the realization that many of the secret questions being used are easily compromised. That is, normally a user's secret questions are based on personal details and personally related facts (which we term personal factoids). Often these facts are easily deduced by other entities that are able to gather information about the target user in question. Therefore, our research has been focused on enhancing the KBA process by using factoids not based on personal details. This paper provides the details of a novel scheme we have designed and tested that uses past session parameters in an iterative fashion as the basis for future KBA questions. To date the scheme has proved effective when used in conjunction with an initial registration process that verifies a user's trusted email address and mobile/cell phone number.

***Keywords*—**Knowledge Based Authentication, Information Technology Management, and Session Knowledge.

I. Introduction

TECHNOLOGY is advancing at a rapid rate and everything requires enhancement and innovation so that it becomes easily applicable for users of all kinds to have an access to the latest technology. The first and foremost thing for enhancing any technology is to make sure that it is secure and user friendly. The knowledge based authentication discussed in this paper highlights the innovations which it carries and how it would prove beneficial for the users if the use of the system is done in the required way. The concept of authentication may be taken as another aspect of the data security [5]. Some of the strong user authentication systems usually implement a method that is signing in a single process, but in this process the users may have to go through multiple levels of authentication. Some systems use the smart cards or images for authentication.

The traditional authentication method is one of the most commonly used methods by majority of the users and the system and it is one of the simplest methods too. Gradually with time the systems are trying to implement the latest user authentication systems. Passwords and PIN are common traditional authentication methods [6]. In the traditional authentication method the username and the password inserted by the user who is authorized is locally stored on the system of the server. The users when having access to the system enter their usernames and passwords in a plain form of text and then this text is sent system of the server. The server identifies and verifies if the username and password entered are correct or not and then allows access if the verification is successful. The username and password match with what was previously stored on the server and hence the user is authenticated.

Knowledge Based Authentication (KBA) has achieved importance as a customer authentication method for electronic transactions. [1]. It tries to authenticate the user on the basis of knowledge of some personal information, regularly throughout a real-time interactive question answer process. Most types of KBA are Personal Identification Numbers (PINs) and passwords. Password and PIN have some limitations, in spite of their wide usage [2]. The significant usability problem with passwords is that the user will forget it or it is hard to remember. Using challenge questions is the most accepted method to support recovery [3]. Security questions are usually used in e-commerce for fallback authentication. Financial institutions are encouraged to secure the accounts of their customers, to limit losses due to fraud as well as to meet the terms of regulations. Recent research has identified serious security weakness with common directorially chosen questions [4].

Knowledge based authentication system is an authentication system which requires the user to know something for getting the access into the system [6]. The secret questions one of knowledge based authentication techniques that are required by the user to answer may amount up to from one secret question till about usually four. It basically depends on the system of how many secret questions they require to be answered. One of the main purposes of using the knowledge based authentication system is to have the retrieval of passwords on a personal basis. The nature of the secret questions can be dynamic in nature or it could even be static in nature. By saying it as dynamic in nature, it may be considered that the user may have no clue as to what the system may ask the secret question as. The pairing of questions and answers is come upon by browsing through the data that are stored in the public records. By saying it as static in nature, it may be considered as that the user is given a choice from a range of questions. The user selects the questions he or she wants and gives the answer accordingly. This answer is stored by the system and asked for verification

G. D. Skinner is an academic with the Faculty of Science and IT at The University of Newcastle, NSW, 2308, AUSTRALIA (phone: +61-2-4985-4512; fax: +61-2-4921-5896; e-mail: geoff.skinner@newcastle.edu.au). A. Alkhalifah is a PhD research within the same Faculty.

at the time the user logs in.

The remainder of this paper details our innovative enhancements to Knowledge Based Authentication. Firstly, in the next section we provide background and related work that provided the knowledge and inspiration for our research. Section 3 details the initial conceptual design and methodological approach we have taken to derive our proposed solution. This is followed by Section 4 where we explain the implementation and testing of our solution. Section 5 provides the results of the testing, and is followed by Section 6 which discusses our conclusions and future work. The final section is a list of references we have used in our work and mentioned in this paper.

II. Background and Related Work

Knowledge based authentication is a method of verifying the identity of a user through matching at least one piece of information (factoids) by a claimant against the source of information associated with him [29]. In this system, no prior relationship establishment is required between the verifier and the claimant. It is also relatively easy to recall as opposed to strong password. The research was directed towards providing a randomization challenge through feature selection of subset factoids. This makes it is easy to identify an attacker from a legitimate user. This method was found to be significantly outperforming the commonly employed random selection method. This method lowers guessability consequently reducing attackers' vulnerability.

Markus Jakobsson and Liu Yang [30] explained the vulnerability within many online services in the password reset process. They noticed that the small number of questions provided for users to choose from if they lose or forget their pass words can be derived via data-mining techniques. In resetting of passwords, by many sites share the few questions which create common Meta pass-word. To curb this problem user preference question was suggested. The challenge in this is that very many questions are required to make this possible. Redesigning user interface of set-up phase can lower the number of questions required. Interaction with users is reduced while maintaining error rates. An attacker will have to interact with the targeted site in order to succeed in drawing any information; such reduces user's interest in that particular site.

Rabkin [4] observed from a survey that the questions that are asked in fallback authentication were found to be surprisingly weak. Many on-line financial institutions find it hard to design secure authentication questions. He noted that most of the questions asked are guessable, not memorable and lacking unique answers and automatically attackable. Jakobsson, Stolterman and Yang [31] argued that many questions asked after passwords are forgotten are vulnerable because they are based on publicly available information. They argued that good security questions ought to be based on long-lived personal questions.

The preference based security approach functions in 2 phases: setup phase and authentication phase. During the opening of an account (setup phase) a user is asked several questions relating to music, T.V programs, sports and food. During authentication the user should give answers that are closely related to the answers given during opening. These kinds of questions have a lower error rate and are more difficult for attackers to guess. In concert with the observations of Jakobsson, Stolterman and Yang [31], Bonneau [32] argued that personal knowledge questions (PKQs) are better in reduction of questions guessability weakness. He observed that the questions that are sent by web-mail providers also typically have poor security. Most of the questions from his study on banks' websites proved to have poor usability or vast vulnerability to mining data which is readily available over the web. He argued that the use of preference based authentication lowers vulnerability based on publicly available information. He also argued that having a pass word backup system enhances the security of user's account.

Toomim et al., [40] conducted a study on the current set of questions that are used so as to bar some people from accessing information (black book list) while allowing some others (white list) to access the same information. They identified that the current systems are tedious, rude and lacking necessary social nuance, complicated and above all not absolutely tamper resistant. From this study they concluded that if users are to design questions that do not directly relate to them such as family names, friends names or more personal information that is retrievable form the source, they would reduce vulnerability of their information and their accounts. By lowering threshold to access control, tests on shared knowledge could enable wider types of information to acquire internet collaborative value.

According to a study that was conducted by Just and Aspinall [41, 2] the challenge questions asked in account retrieval upon forgetting a password are more vulnerable to attackers as they are based on common information in the public domain. They suggested the use of user chosen challenge to overcome this challenge. Data security would be enhanced if challenge questions would be formulated by the user, and sent to the server without answers so that the user would do personal evaluation. The answer ought to be combined consequently producing a single hash value making it harder for attackers to break-through. Wu et al., [42] proposed a recursive protocol to be used in group oriented authentication. The group members are supposed to share a group session key. The protocol has rounds of messages, waiting time, completion time, and communication overhead for the recursion completion. The protocol also manages to achieve properties such as independency, non-disclosure and integrity. It also has a use-only-once property consequently counteracting interleaving attacks. Any attempt to modify group's session key would require the use of the secret key agreed upon by the users and with the consent of group members.

Schecheter, Egelman and Reeder [23] pointed out that the

use of backup authentication mechanisms to regain accounts is wanting in terms of user's ignorance. There are so many users who do not even know that their information can be intercepted on transit. They designed a backup system that appears as part of Window Live ID. The system uses voice and facial appearance to validate the user's identity. Upon verification, the user is provided with account recovery code. It's required that an account holder provide a sufficient number of the codes for authentication. The researchers also argued that upon opening an account, the account holder should reply to the mail sent to him and engage in several communications with the web-mail provider so that upon forgetting the password, the communications that took place could act as a source authentication and verification.

Chen and Liginlal [43] presented a Bayesian Network KBA model that is grounded on information theory and problematic reasoning that was geared towards addressing the two major problems of KBA metrics: memorability and guessability. The BN-KBA is usable in making decisions on authentication. The model facilitates the development of a closed-form solution that allows estimation of guessing entropy metrics and guessability. The factoids used are personal reducing guessability even further. The authors argued that use of information that is based on personal knowledge than public knowledge increases security through reduced guessability.

To critically address the issues in security issues in online transactions, it is important to understand how the concepts of data security, authentication, and knowledge based authentication interrelate. Knowledge based authentication is a method of verifying the identity of a user through providing secret knowledge (factoids) associated with him/her such as password and personal questions [29]. This is done in an effort to increase the security of data in any online transaction. Due to the vulnerability of personal information that is increased by the nature of questions asked, it is important to note that data security would be enhanced if challenge questions would be formulated by the user, and sent to the server without answers so that the user would do personal evaluation. The answer ought to be combined consequently producing a single hash value making it harder for attackers to break-through. Several studies have been conducted that are aimed at increasing the security of online transactions.

Wu et al., [42] proposed a recursive protocol to be used in groups' oriented authentication. The group members are supposed to share group session key. The protocol has rounds of messages, waiting time, completion time, and communication overhead for the recursion completion. Schecheter, Egelman and Reeder [23] pointed out that the use of backup authentication mechanisms to regain accounts can increase vulnerability of online transactions. This is partly attributed to user's ignorance. The authors designed a backup system that appears as part of Window Live ID. The system uses voice and facial appearance to validate the user's identity. Upon verification, the user is provided with account recovery code. It is required that an account holder provide a sufficient number of the codes for authentication. The researchers also argued that upon opening an account, the account holder should reply to the mail sent to him and engage in several communications with the web-mail provider so that upon forgetting the password, the communications that took place could act as a source authentication and verification. The above analysis indicates that data security can only be increased if knowledge based authentication is augmented. The user should be in a position to choose the right authentications. This will help to reduce the vulnerability of any personal information.

III. Conceptual Design and Methodological Approach

User authentication is one of the most critical aspects of information systems today. Traditional techniques for user authentication involves the use of text based authentication techniques such as the use of passwords. With the growing need for high security, especially in business critical systems, text based authentication techniques have been found to be ineffective and unreliable. One of the biggest challenges with text based authentication techniques are that password authentication required the use of complex passwords to complicate security bleaches. Complexity in passwords lead to high needs for memorization by system users which is usually hard as users keeps forgetting. To overcome this, end users end up writing their complicated password on papers or even files in their computers. If someone gets access to such password either through paper or files inside computers, systems security can be easily compromised.

Knowledge based authentication is the latest techniques that security managers are using to maintain complicated and hard to breach security policies. The use of secret questions and companion technology is especially critical in knowledge base authentication as it allows user to securely gain access to information system with a simple task on the appropriated peripheral device. There are three kinds of authentication systems that can be used to trust users; nevertheless, tokens and biometric schemes are not investigated in this study. A decision was made to carry on this research using the knowledge based authentication system particularly personal secret questions. Previous research papers have been pointed out various knowledge based techniques; but, not any of the research we found had studied user acceptance of using those methods for online banking.

Our research carries out a new knowledge based authentication technique that applies user iterative activities for personal secret question retention. The prototype developed in our research is for showing new KBA system to users. Our work aims to identify the appropriateness of login methods for online banking and to investigate user preferences in a challenge question authentication system. Another aim of our research is to evolve more secure and usable knowledge based authentication techniques alternative to traditional authentication methods (PIN and Password), difficult to guess by the attacker and easy to remember by the user.

Several tests were conducted on user authentication.

Various secret personal question techniques have been analyzed to determine their effectiveness in critical data security. Experiments were based on existing information systems and security technologies. Test applications and systems were selected for the experiments. The test applications used included application software such as a website that provided the login interface while the systems used included SMS and E-mail. These systems and applications were selected due to their availability and affordability. Systems such as biometric systems are not applicable for this research since they are very expensive and therefore not readily available for everyday use.

Several Knowledge based authentication levels were tested, one at a time so their strengths and weaknesses could be identified. It is on the basis of the weaknesses identified from various existing knowledge based authentication techniques that appropriate measured for security enhancements were identified. Once testing had been conducted on the existing technique, evolutionary prototypes of the proposed enhancements were continually evolved and tested.

Previous research studies have suggested diverse knowledge based authentication techniques which have enhanced security and usability evaluate to existing used techniques (passwords, PINs and challenge questions). Those suggested techniques propose the use of secret questions to improve password memorability and system login. In this research project, we have derived our solutions from those proposed techniques. In addition, we designed an authentication technique that is based on previous login data as secret question retention. The research design idea was implemented as a prototype. The reason of prototyping is to test our concepts and to show new idea to users [53]. The prototype is a helpful when examining concepts, and it is an effective method to test out ideas [54]. Prototyping can engage both high-fidelity stage and low-fidelity stage.

A low-fidelity prototype uses resources which are very diverse from the final result; it is proposed to be simple, cheap and quick to construct [54]. The principle of low-fidelity prototyping is for theoretical design, to discover new concepts, and it facilitates designers to decide the merits of new ideas. We utilize low-fidelity prototyping to investigate secret questions for login techniques. High-fidelity prototyping uses resources that are expected to be in the final result and create a prototype that seems much like the final product [54] .For our purpose; we applied a website that simulates our knowledge based authentication system based on the concepts from the low-fidelity prototype.

Deciding what to test and what not to test is a big part of prototyping. Therefore, prototyping needs intelligent settlements to be made [55]. The settlements direct to two types of prototyping which are horizontal and vertical. A horizontal prototype gives a wide range of functionalities through little details, whilst a vertical prototype presents a lot of details for a few functions. The idea of authentication needs only a single function which verifies users; so, we implemented vertical prototyping for the high-fidelity prototype.

IV. Implementation and Testing

Knowledge based authentication should involve the use of secure authentication techniques such secret questions which are sent by companion technology such as email and short message service (SMS). Answers to secret questions are sent to the user's subscription mobile phone number or email, and entered upon requests during authentication. This technique should be used carefully as the information cannot be guaranteed to be a secret. In our proposed knowledge based authentication technique, the verifier programmer asks the claimant a series of questions that they should be able to answer from the answers sent to them via companion technology. The questions depend on the user activity so that only the real user would know the correct answers. The information could be of any of the following:

- Last login date
- Last login session
- Last login time
- Last login transaction details

This authentication system does not involve the use of PINs and passwords. While they may also be classified as knowledge, they are excluded from the scope of this security mechanism because they must be memorized for the purpose of authentication. Knowledge based authentication techniques leverages the user's recollection of information that is not specifically learned for authentication. This technique has some features that are different from another Knowledge based authentication (KBA) system as following:

- Can be used to for users, authentication over the telephone, and mobile phone in person or online.
- Can be used for authentication of users who have forgotten their password or lost other types of authentication credential.
- Answers sent over companion technology are less likely to be forgotten than an infrequently used password. Handling large number of passwords reset requests may add significant cost. This mechanism can be effective in any online authentication settings such as online banking as an alternative to passwords, particularly where service use is infrequent.

The user activities used for secure authentication must be simple activities with distinctive authentication features. Users can for instance authenticate through answering a simple question that requires entry of an answer sent by the service provider via mobile phone, e.g. last login session ID. This is an intelligent technique which can be complicated for higher security through the use questions. Companion technology is critical and must be emphasized in knowledge based authentication due to availability of intelligent features that are found in modern technology devices such as sensitive screens and other biometric systems. Knowledge based techniques that are based on insecure hardware and software technologies should not be used for security compliance in

modern information systems. The user activities chosen and the companion technology in adopted must have high reliability metrics. At the same time, application of knowledge based authentication must consider various classes of users.

Our knowledge based authentication technique which uses personal knowledge questions proposes some assurance levels. These security levels are dependent on user choices and each level requires at least one data login. These levels as following:

Level 1: when used as a single authentication factor. Answering one secret question that is not based on fixed personal data, e.g. last login session ID must be included. This level is very simple system.

Level 2: when used as a couple authentication factors while questions based on previous data login. In this level, which is simple system, two of challenge question must be answered such as last login time and session ID.

Level 3: When used three of authentication factors. Providing three questions must be answered by the user, these include for instance last login time; date and session ID. We can call this level the intermediate system.

Level 4: When used all authentication factors. This level requires from the user to answer all questions that are offered in the interface. In this classification, variable data derived from prior service delivery events e.g. last login time and transaction details such as payment information are included. For that reason, this level is called the advance system.

This system does not involve traditional authentication method (PIN and password) due to its complexity in memorizing and it is guessable by the attacker. Further, we are trying to find an alternative KBA method to provide more secure and usable system based on personal knowledge questions. Therefore, we used four levels in order to test the security level of our prototype. These levels include answering one personal knowledge question (very simple system), answering two PKQs (simple system), answering three PKQs (intermediate system) and answering four PKQs (advance system). We developed four security criteria during the implementation which are guessability, independence, and observation and secure communication. These criteria helped to test the security level during the experiment and the simulation.

Guessability is the most important security criteria that make the system very secure [59]. The numerousness is an important factor in the guessability which determines the number of secret questions provided in the system. In addition, the independence is another factor in deterring how the system is difficult to guess, this factor measures while the answers are changed with time. The changed with time factor plays an important variable in measuring the guessability and the independence factors. We proposed a formula to quantify the rate of changing the answers with time as following:

*The number of Times = (the number of questions) *)the number of iterative logins)*

For example, according level 3 and the third iterative login, the number of answers changed will be 9 times.

Observation is a critical issue in the security of challenge system [59]. Observation is more subjective for the reason that the difficulties of determining the answers depend on several factors such as individuals that have relationship with the user. In our study, for instance providing one question related to time could be recognized by user's relations who were with the user when he logs in. Variance is one of the most important factors in the observation. The variance means that factors belong to different scales and are not related. Communication is an important factor for protecting data that is sent to online users. The user does not need to write the answer in paper or keep them in a file that are subjected to theft or damage, but he can find the answers any time in his email inbox or SMS folder as the security feature with these technologies is high. After the user logs out from the system, he will receive a message on his email and mobile phone. This message contains data about the answer of the questions.

A web site was built and designed in ASP.NET with VB (visual basic language) as the user interface. Through the web site pages, we were able to test our knowledge based prototype. The pages include user login page as home page, registration page, data recollection page and the user page. Internet Information system (IIS) is a web server application and set of feature addition modules created by Microsoft for use with Windows. In our experiment, we used IIS to provide SMTP (Simple Mail Transfer Protocol) to enable the system to send an email or SMS message.We built database for our experiment by Microsoft SQL server 2008 Management Studio. This includes creation of tables, storing procedures and executing some quires that are needed to verify the users and implement the system. We used ADO.NET technique to access and update database.

The proposed Knowledge based authentication contains three phases: Registration, First Iterative and the 1...N ongoing iterations. The user is not required for answering a secret question during registration phase to access and getting to login. During first iterative phase the user is required to answer at least one secret question to authenticate, and these answers along with time, date, session ID and other transaction details are sent to the user's email or SMS. In addition, the user requires answering also at least one question to get login during 1…N iterative phase. This answer depends on iterative phase.

The registration stage in this experiment needs the registration of user name, account, e- mail and mobile number. After the registration, the user will receive a message by his\her e mail and mobile phone. This message contains data such as time, session ID and date logout. These data must provide for first time authentication to help answering the secret questions. The user needs to register once, that means; each user will visit the registration page just when he needs to register in the system. The system provides recollection of data if the user needs the message that is sent to him again, but the content of data is same as data on the first message. The

user needs to provide his /her email and SMS that is registered in the user table, otherwise the user can not retrieve the login data and he will receive a message such as "Your Email or mobile phone number is incorrect". However, the user will have a message such as "Your data has been sent to your Email & Mobile" if he entered the correct email and mobile phone number.

After registration and logging out, the system sends massage to the user's email and mobile phone. This message contains data that are reacquired to answer the secret questions to login again. These Data contain last time, date and the account details that are entered during registration phase. When the user logs out, the system sends message by the companion technology and the user table in the data base will be updated. The content of this message is different than the message sent in the registration phase. For example, the user may register in the system at 4th of May and he can login in 10th of May. Because the answers will be changed with time, the attacker feels difficult to guess the answer.

The final phase indicates the re-authentication process. In this phase the answer for the challenge questions will be changed in each iterative, and the user will receive different messages with different data. For instance, if the user logged in the system 5 times, then he is provided five different answers in all questions. After the user logs out, the data in the user table will be updated. This phase presents how secure the system is because it offers same question but with different answers for every time the user is authenticating. So, this indicates the guessability and the observation. This helps the user to remember the answer in every authentication attempt, and he does not need to keep the answer for long time. Our KBA system design also considers some security considerations to determine how much information to protect in case of authentication failure. The user has limited number of attempts to get login, in our design we allow the user to have 3 attempts to provide the right answer or his/she account will be locked out.

V. Analysis of Results

The evidence got from the implementation of the guessability factor and changing the answers variable in each authentication attempt proved to be the most essential and effective one. The performance goal achieved from the performance metric was that there was successful authentication with difficult question to guess. The observation has a more technical glitch which makes it difficult for the hackers to identify what the answer to the secret question could be. All the above mentioned metrics (in chapter 4) have their own reliability and validity reasons. The most feasible metric that we have reached to during our study is the criteria of guessability. This method seems more reliable than the others and more difficult for the hackers to figure out the answers of the users who have logged into the system. All the other metrics have resulted in somewhat similar results but due to more authenticity and the formula being more technical, the observation metric seems to be the most feasible for the system which wants to have authentication for the user logins.

The usability metrics needs to be given due consideration too as the factors on which it depends is very critical for the whole procedure to take place systematically. The time to learn, the speed of performance, and the error rates by the user or the system cannot be overlooked under any circumstances. If the users take time to learn and then speed of performing is slow then the required results may not be achieved and hence undue problems may arise hence it is very important to keep the rate of error to the minimum and to do the tasks with speed and accuracy.

From the results of the prototype simulations, the objectives of this research were achieved. This study was aimed to find the appropriateness of login methods for online banking and to evolve secure knowledge based authentication technique alternative to traditional authentication methods. In addition, it aimed to find alternative secret questions based authentication method that are weak and lack of the security and the usability stages which have been identified in many studies. The findings of testing and simulations shows that answering secret questions from data that belong last login and received by email and SMS provided an authentication method alternative to other knowledge based authentication options. As the results of the evaluation presents that PKQ prototype of this study meets the criteria of security, it could be argued that our system enhanced and improved knowledge based authentication.

Through the testing and the evaluation processes, we found that personal knowledge questions method that were developed and reviewed in this research study enhanced knowledge based authentication and improved the security level. This system could authenticate the users the entire time while they are logging in to the system. Knowledge based authentication means that you need to know some data that relate your online activity before you use the system.

The testing was expected to test and evaluate the usability level, as the testing of the usability would provide more accurate results. In addition, measuring the system against both the security and the usability levels would benefit from providing an efficient authentication method. In this phase of the study, we focused on implementing the security criteria in order to simplify and shorten the experiment time. Therefore; the experiment was conducted without testing the usability level, although this study put our metrics for testing the usability level in for the next phase of the study.

Another limitation of the results is that all the measures and the testing of this system were observed and conducted by the researcher. Testing the system by participants with different experiences related to knowledge based authentication methods and from different ages would offer more accurate results. We could analyze and investigate more data and look for unforeseen patterns through larger sample sizes. To measure the performance of the system and then determine which knowledge based authentication options is the best one

in the real world , the results needs to be compared with other authentication methods. The results show the best level of answering secret questions in our proposed knowledge based authentication. This study compared different levels of this system against each other rather than compared against other knowledge based authentication methods. This indicates that this system could not be the best alternative to another authentication method, but the results confirmed that this system provided an alternative method and solved the problems of secret questions based authentication that have been identified previously in different literatures.

VI. Conclusion and Future Work

This study aimed to find knowledge based authentication solution that would be suitable for online banking. Secret questions authentication is one of the most common methods of verification for online businesses and very useful for online banking. However, many studies reviewed in this research have confirmed that this technique has some limitations. They revealed that at times it is easy for others to guess the answers of the user's personal information because the one who guesses may be linked to the users. Hence they may have considerable and usable knowledge about the target user to comprise the secret personal questions. Further, it was discovered in the literature that the majority of other people trying to access a user's account are most often their spouses, parents, siblings or friends that are very close to the user.

Therefore, as part of our enhanced KBA proposal we developed a set of security criteria to measure our novel new system against. They are the guessability, the independence, the observation and the communication. They were used to find solutions for the highlighted limitations, and we tested and measured the performance of our proposed system against these criteria. To adapt these mechanisms to a conceptual generic computer system, we built and designed a prototype. Using our prototype we simulated four levels of implementation in the study so as to further determine the performance of our proposed enhanced knowledge based authentication scheme.

In this research, the experimental evaluation and the simulation were conducted to answer the research questions. In the experiment, the personal knowledge question system were tested and observed by the researcher. We developed our metrics of evaluation based on other established and widely used authentication systems. The security metrics are used in the research for deriving the results. The results were discussed and analyzed to determine the performance of our proposed authentication technique. From analyzing the results we propose that our enhanced knowledge based system is practical and offers significant improvements over currently available KBA schemes.

References

[1] G. Di Crescenzo and A. Rubin, *Financial cryptography and data security*, Springer, Berlin Heidelberg, 2006, pp. 325.

[2] M. Schellekens, *Electronic signatures: authentication technology from a legal perspective*, The Hague: T.M.C. Asser Press, 2004, pp. 160.

[3] M. Just and D. Aspinall, "Personal Choice and Challenge Questions: A Security and Usability Assessment," in Proceedings of the 5th Symposium on Usable Privacy and Security, Mountain View, CA USA, July, 2009.

[4] M. Keith, B. Shao and P. Steinbart, "The usability of passphrases for authentication: An empirical field study," *International Journal of Human-Computer Studies*, Vol. 65, 2007, pp. 17–28.

[5] R. Kubera and W. Yu, "Feasibility study of tactile-based authentication," *International Journal of Human-Computer Studies*, Vol. 68, 2009, pp. 158–181.

[6] A. Rabkin, "Personal knowledge questions for fallback authentication: Security questions in the era of Facebook," *in Proceedings of the 4th symposium on Usable privacy and security*, Pittsburgh, Pennsylvania, USA, July, 2008.

[7] Y. Chen and D. Liginlal, "A maximum entropy approach to feature selection in knowledge-based authentication." *Decision Support Systems*, Vol. 46, 2008, pp. 388–398.

[8] M. Jakobsson and S. Wetzel, "Quantifying the Security of Preference-based Authentication," *in Proceedings of the 4th ACM workshop on Digital identity management*, Alexandria, Virginia, USA, 2008, pp. 61-69.

[9] M. Jakobsson, E. Stolterman and S. Liu Yang, "Love and Authentication," *in Proceeding of the twenty-sixth annual SIGCHI conference on Human factors in computing systems*, Florence, Italy, 2008, pp. 197-200.

[10] J. Bonneau, "Alice and Bob in Love: Cryptographic Communication Using Natural Entropy," *in Proceedings of the 17th International Workshop on Security Protocols 2009*, Cambridge, UK, April, 2009.

[11] M. Toomim, X. Zhang, J. Fogarty and J. Landay, "Access Control by Testing for Shared Knowledge," *in Proceeding of the twenty-sixth annual SIGCHI conference on Human factors in computing systems*, Florence, Italy, 2008.

[12] M. Just and D. Aspinall, "Challenging Challenge Questions," *presented at Trust 2009: Socio-Economic Strand*, Oxford, UK, 6-8 April, 2009.

[13] T. Wu, T. Huang, C. Hsu, and K. Tsai. "Recursive protocol for group-oriented authentication with key distribution," *The Journal of Systems and Software*, Vol. 81, 2008, pp. 1227–1239.

[14] S. Schecheter, S. Egelman and R. Reeder, "It's Not What You Know, But Who You Know: A social approach to last-resort authentication," *in Proceedings of the 27th international conference on Human factors in computing systems*, Boston, MA, USA, 2009..

[15] Y. Chen and L. Divakaran, "Bayesian Networks for Knowledge-Based Authentication," *IEEE Transactions on knowledge and data engineering*, Vol. 19, No. 5, 2007, pp. 695-710.

[16] A. Adams and M.A. Sasse, "Users are not the enemy," *Communication of the ACM*, vol. 42, no. 12, 1999, pp. 41-46.

[17] H. Sharp, Y. Rogers, and J. Preece, *Interaction Design: Beyond Human-Computer Interaction*, 2nd ed. John Wiley & Sons, Chichester, West Sussex, 2007.

[18] N. Heaton, "What's wrong with the user interface: How rapid prototyping can help," *In IEE Colloquium on Software Prototyping and Evolutionary Digest London*, IEE (1992), Digest No. 202, Part 7, pp. 1-5.

[19] M. Just, "Designing and evaluating challenge-question systems," *in IEEE Security and Privacy Magazine*, Vol. 2, No. 5, 2004, pp. 32–39.