ISSN 2320-2602

International Journal of Advances in Computer Science and Technology (IJACST), Vol.3 , No.1, Pages : 16-19 (2014)
Special Issue of ICACSET 2014 - Held during 13-14 January, 2014 in Royal Orchid Sheraton Hotel & Towers, Bangkok

Authentication Using Private Weighted Questioning

Dr. Abdulameer Khalaf Hussain[1] , Dr. Hider Al-Lami[2]
[1]Jerash University , Jordan , abdulameer.hussain@yahoo.com
[2]College of Science and Humanity Studies,Saudi Arabia, allami69@yahoo.com

Abstract: This paper presents a strong authentication method by examining each user with certain private information related to that user. The proposed method constructs a database for all authenticated users .Each record in this database is assigned to individual users . Some of the fields of user's record are subjected to the user as private questions and he/she must answer these questions randomly with a suitable weight assigned to each question. The most important property of this method is that the user for certain privileges must answer some selected candidate questions private to a system group.To get more advanced privileges the user must answer a global question (GQ) in the form of passphrase supplied by the system manager .

Key words : Authentication , Knowledge Based Authentication , Passphrase ,Global Questions.
.

INTRODUCTION

One of the common sensitive application widely used is the controlling of personal finances. In these applications there are some security risks . In addition , there exist large criminal networks [1]. To overcome this threat , banks had studied to use sophisticated authentication mechanisms .The most effective solution used by many banking sites had been rely on security questions . These questions are divided into two types . The first sort asks about sensitive (private) information such as social security and bank account numbers, and ATM PIN codes and so this type of questions is referred as sensitive security questions. The other type of security questions (which is called personal security questions) in which the user is asked about personal history, and family background, such as one's mother's maiden name. These have also been referred to as "Personal Verification Questions". On the other hand , personal security questions can be divided into those selected by the user, perhaps from a menu of choices, and those specified entirely by the institution, such as ZIP code, mother's maiden name, or date of birth. Both sorts of security questions differ in a crucial respect from passwords. The ideal password is a high entropy string of characters, and is chosen entirely by the user, and then memorized. However, users are not expected to memorize answers to security questions. Instead, the answer should already be part of a user's long-term memory (or, in the case of a bank account number, be written down and readily accessible) [2].

A commercial authentication technique that had been analyzed in the academic literature is email -based authentication. This techniques has the ability to receive mail at a prearranged email address and is used as proof of identity. This security analysis of this approach was presented by Garfinkel. Garfinkel observes that emailing users a link to retrieve new password is often a secure technique [3].

There are six possible weaknesses in personal security questions. These weakness are inapplicability, ambiguity, and lack of memorability — diminish the usability of the question, guessability, attackability, and automatic attackability — reduce the security provided by a question. [4]. In the context of question authentication we must refer to knowledge based authentication which is used to verify user's identity on the basis of "what you know". This method requires personal knowledge to authenticate individual in order to access to the online environment. One example of such method is a user-id and password scheme. This example is a popular authentication method, because passwords are key to authentication and memorable. As analyzed in [5], low entropy passwords are prone to dictionary attacks. Another example of knowledge based authentication is challenge questions or security questions.[6] .This scheme is generally used in the banking sector [7] for authentication, and corporate email service providers for credential recovery [8].

Another authentication scheme is Profile Based Authentication Framework (PBAF) for student authentication in online examinations. This framework uses a multi-modal authentication approach to secure online examination. The solution comprises of two layers of authentication i.e. user-id and password, and challenge questions. Initially, a user-id and password can be used to login into the online learning environment to carry out regular learning activities [9] .

There is another significant method which is Knowledge Based Authentication (KBA) comes from the need of electronic transactions by customers . It tries to authenticate the user on the basis of knowledge of some personal information, regularly throughout a real-time interactive question answer process. [10].

Most types of KBA are Personal Identification Numbers (PINs) and passwords but these have some limitations, in spite of their wide usage [11].The most common problem with passwords is that the user will forget it or it is hard to remember. Instead we can use challenge questions which is the most accepted method to support recovery [12]. 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 [13].

The authentication system which requires the user's knowledge of something to get an access into the system is referred as knowledge based authentication system [14]. This needs secret questions to be answered by the user and depends on the type of the application of how many secret questions they require to be answered. The secret questions can be dynamic in nature or dynamic. The dynamic secret questions mean that they may be considered that the user may have no clue as to what the system may ask the secret question as whereas in static nature the user is given a choice from a range of questions [15].

It is important to use passphrase for ensuring more authentication and granting high levels of privileges . A passphrase is a sequence of words or other text used to control access to a computer system, program or data. A passphrase is similar to a password in usage, but is generally longer for added security. Passphrases are often used to control both access to, and operation of, cryptographic programs and systems. Passphrases are particularly applicable to systems that use the passphrase as an encryption key. The origin of the term is by analogy with password [16]. In this paper we use passphrase as private secure sentences to represent global questions.

RELATED WORKS

O'Gorman, Bagga, and Bentley had proposed a group of question-based protocol called Query-Directed Passwords (QDP). These questions are joined with other techniques (such as PIN, address of physical devices, and client-side storage device or wallet card). The aim of this procedure is to hide the questions from attackers [17] . Another scheme is called preference-based technique proposed by Jakobsson et al. [18]. In this scheme the users are subjected to question in order to make a series of preference judgments, and if their answers are related or close enough to the user's previously-established preferences, then the users are authenticated.

In most of the security question systems , the users have to specify the correct answers in advance. Another scheme which is called Adaptive Challenge Question which can avoid this by asking users about their browsing history in the recent past [19]. Security questions as used today have been studied in the past . A set of criteria for evaluating personal security questions, and has sketched a number of possible design alternatives [20]. In addition to the academic researches , the government of Canada has published guidelines for security questions in authentication [21].

One of the most important of the past studies is that of Haga and Zviran, published in 1991 [22].This system is used to ask users some personal security questions and these are measured as successful answer rate for the user.

The recent study of commercial authentication technique is that of Mannan and van Oorschot, which examined the websites of six financial institutions [23]. The websites they observed had surprisingly weak security models, and fairly loose length and complexity requirements for both passwords and personal security questions.

Another method by Griffith and Jakobsson who had demonstrated that mother's maiden name, perhaps the canonical example of a personal security question, can be deduced with significant probability via public records [24]. The authors suggested different techniques for deriving mothers' maiden names from public records . In addition the user subjected to a number of other security questions about names of family members.

PROPOSED SYSTEM

First we need to construct a database containing the use's information . The table inside the database contains a record for each user . The fields are filled with different questions and each question has a different weight . The questions are classified to two classes . The first class contains private data for that user and the second class contain private data related to the database manager . The aim of this classification is that to check the weights for the answered question . The weights of user's private information take weights different from that of the database private data. This can be used to organize the privileged granted to the user . This database is illustrated in Table 1.

Table 1: Database containing secure questions.

User	Question	Question	Question	Question	
U1	QU1	Q2M	… ..	QU1	
U2 . . .	Q1M	Q2M	… …	QU2	QU2
Un	QUn	Q1M	… … .		

Where Qui represents user's questions and QM represents manger questions.

Each question is assigned a weight . Suppose that wu1,wu2,….,wun are the weights assigned to each user's questions and wm1 , wm2, ….wmm are the weights for the manager questions . The threshold for each user's records can be computed according to the weights sum of each record . This sum of the answered questions are compared with this threshold . The system must determine authenticated ranges of the answered question in order to determine the class of the privileges granted to each user. Another important point , the system must determine a low weight sum that can be used to reject the user if that sum lies in this low level range. The scores gained by each user is used to grant him the corresponding privileges of that score. So we design a privilege table like access control matrix as shown in table 2.

Table 2: Scores and the Related Privileges

Score	Privileges type
10-20	Read Only (RO)
20-30	Write Only(WO)
30-40	Execute Only(EO)
40-50	Append Only (AO)
50-60	RO+EO
60-70	WO+AO
70-80	RO+AO
80-90	RO+WO+EO
90-100	RO+WO+EO+AO

In addition to these questions there is global question (GQ) submitted by the system manager . This type of question is also private and takes the form of passphrase instead of password because of the security strength of the passphrase . So each user desires to get more privileges than other must give the right passphrase related to him . The score of this passphrase is added to the high scores imposed in table 2 and the user is granted other sensitive accesses such accessing some secure fields which are not included in the privileges types of table 2.

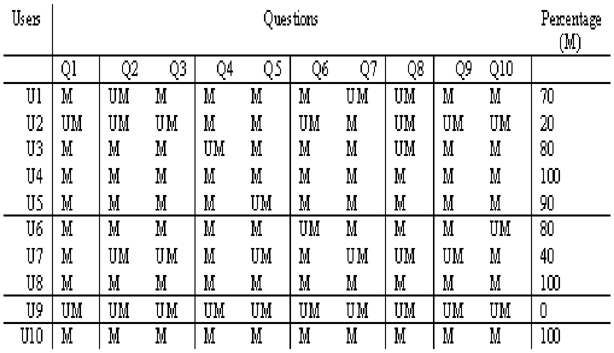
Some of the important private secure questions that can be used to authorize the users are found in [15, 2 5] as follows:
Q1: What is your birth date?
Variations: What is your year of birth?
Q2: What is your social security number?
Variations: What are the last four digits of your social security number?
Q3: What is your mother's maiden name?
Variations: What is your father's middle name? What is your spouse's middle name? What is your first child's middle name? What is your youngest sibling's middle name?
Q4: What was the total on your most recent bill?
Variations: What was the account balance on your most recent statement?
Q5: What high school did you attend?
Variations: What middle school did you attend? What grade school did you attend? What was the name of your high school mascot?
Q6: Where were you born?
Variations: In what city were you born? In what state were you born? Where did you live when you were age 14?
Q7: What is your favorite TV show?
Variations: Who is your favorite TV character? Who is your favorite TV actor?
Q8: What is your favorite book?
Variations: Who is your favorite character in a book? Who is your favorite author?
Q9: What is your favorite animal?
Variations: What is your favorite type of mammal? What is your favorite type of fish? What is your favorite type of bird?
Q10: What is your pet's name?
Variations: What is your favorite pet's name? What was the name of a childhood pet?
Q11: Who is a memorable person from your childhood?
Variations: Who was your childhood hero? Who is a memorable person to you?
Q12: What is your father's surname?
Q13: What is best friend's surname?
Q14 : Who is the favorite hero of your childhood?
Q15: What was your dream job as a child?
Q16: What is your home address house name or number?
Q17: What is your home address town?
Q18: What is your home telephone number including country and area code?
Q19: What is your mobile number including country code?

Each of these secure questions has a score depending on the degree of privacy of the question . To ensure more security and more privilege grant , the user asked to answer global question (GQ) . This question has the property of perfect security because it is in the form of passphrases private to each authenticated user granted from the manager.

RESULTS

Table 3 gives some different users without global questions for the first trial which asked the numbered questions sequentially .

Table 3 : Different responses of 10 users .

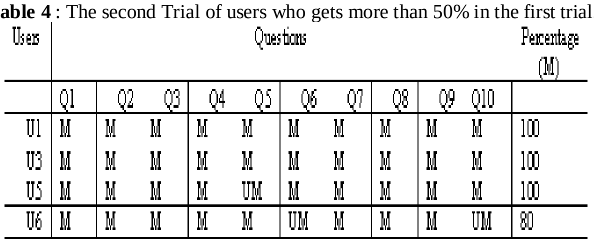


Users	Questions										Percentage (M)
	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	
U1	M	UM	M	M	M	M	UM	UM	M	M	70
U2	UM	UM	UM	M	M	UM	M	UM	UM	UM	20
U3	M	M	M	UM	M	M	M	UM	M	M	80
U4	M	M	M	M	M	M	M	M	M	M	100
U5	M	M	M	M	UM	M	M	M	M	M	90
U6	M	M	M	M	M	UM	M	M	M	UM	80
U7	M	UM	UM	M	UM	M	UM	UM	UM	M	40
U8	M	M	M	M	M	M	M	M	M	M	100
U9	UM	UM	UM	UM	UM	UM	UM	UM	UM	UM	0
U10	M	M	M	M	M	M	M	M	M	M	100

Note : M stands for matched answer and UM stands for unmatched answer

From this table we see that there are 4 full authenticated users (100%) and 3 users are considered unauthenticated . The users that must subjected to second trial to prove their partial or full authentication are 4 users who get answer percentage larger than 50% . Table 4 illustrates the results of testing the unmatched answers of those users .

Table 4 : The second Trial of users who gets more than 50% in the first trial.

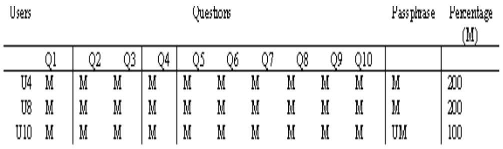


Users	Questions										Percentage (M)
	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	
U1	M	M	M	M	M	M	M	M	M	M	100
U3	M	M	M	M	M	M	M	M	M	M	100
U5	M	M	M	M	UM	M	M	M	M	M	100
U6	M	M	M	M	M	UM	M	M	M	UM	80

The authenticated users are granted privilege according to their answer percentage .

To get advanced privileges the manger asks the users to provide their global questions in the form of passphrase .The score of each global question is 100. Table 5 explains two users who wants such privileges .

Table 5 : Results of answering global questions .



Users	Questions										Passphrase	Percentage (M)
	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10		
U4	M	M	M	M	M	M	M	M	M	M	M	200
U8	M	M	M	M	M	M	M	M	M	M	M	200
U10	M	M	M	M	M	M	M	M	M	M	UM	100

ANALYSIS and CONCLUSION

The authenticated method using the private secure questions is considered a strong method for proving the authenticity of the users. Our scheme is designed in a different way in that it contains global question for each user which is in the form of the passphrase in addition to the personal questions . We use the passphrase because of the high security of this structure with relative to other pieces of secure information such as password. Also this method is implemented for different users to answer questions both sequentially and randomly for selecting the available questions in the database of the system .

If we examine the results of this method for the authenticated users we get 95% responding to their questions because some of the authenticated users may forget the correct answer for the first trial , but those when examined for the second trial to provide the correct answers we get about 99.7 %. These results are obtained after examined 200 users.

REFRENCES

[1] J. Franklin, V. Paxson, A. Perrig, and S. Savage" An inquiry into the nature and causes of the wealth of internet miscreants" Proceedings of the 14th ACM conference on Computer and Communications Security, 2007.

[2] Social Security Administration. RSA Identity Verification. Available online. http://www.rsa.com/node.aspx?id=3347, 2008.

[3] S. Garfinkel " Email-based identification and authentication: an alternative to PKI" , IEEE Security & Privacy Magazine, 1(6):20–26, 2003.

[4] M. Just" Designing and evaluating challenge-question systems" , IEEE Security and Privacy Magazine,
2(5):32–39, Sept.-Oct. 2004.

[5] J.Huiping ,"Strong password authentication protocols", 4th International Conference on Distance Learning and Education (ICDLE), 2010, IEEE.
[6] A. Moini, A.and M.Madni, "Leveraging Biometrics for User Authentication in Online Learning: A Systems Perspective", *IEEE Systems Journal*, 2009,3(4),469-76.

[7] A. Rabkin "Personal knowledge questions for fallback authentication: Security questions in the era of
Facebook", In SOUPS 2008: Proceedings of the 4th Symposium on Usable Privacy and Security, 2008, 23,New York, NY, USA, ACM.

[8] S.Schechter, A,Brush, and S.Egelman "It's No Secret. Measuring the Security and Reliability of Authentication via", 30th IEEE Symposium on Security and Privacy, 2009, IEEE.

[9] C.Shaver, and J.Acken "Effects of equipment variation on speaker recognition error rates", International Conference on Acoustics Speech and Signal Processing (ICASSP), 2009, IEEE.

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

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

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

[13] 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.

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

[15] U . Abrar , X. Hannan , L. Mariana and B. Trevor, "Using Challenge Questions for Student Authentication in Online Examination", International Journal for Infonomics (IJI), Volume 5, Issue 3/4, September/December 2012

[16] [http://en.wikipedia.org/wiki/Passphrase]

[17] L. O'Gorman, A. Bagga, and J. Bentley, "Call Center Customer Verification by Query-Directed Passwords.
In Financial Cryptography" , 8th International Conference, FC 2004, Key West, FL, USA, February 9-12, 2004: Revised Papers. Springer, 2004.

[18] M. Jakobsson, E. Stolterman, S. Wetzel, and L. Yang , " Love and authentication", In CHI '08: Proceeding of
the twenty-sixth annual SIGCHI conference on Human factors in computing systems, pages 197–200, New York, NY, USA, 2008. ACM.

[19] F. Asgharpour and M. Jakobsson , " Adaptive Challenge Questions Algorithm in Password Reset/Recovery",In First International Workshop on Security for Spontaneous Interaction: IWISSI '07, September 2007.

[20] M. Just, " Designing and evaluating challenge-question systems", IEEE Security and Privacy Magazine,
2(5):32–39, Sept.-Oct. 2004.

[21] Office of the Privacy Commissioner of Canada. "Guidelines for Identification and Authentication".
Available Online. http://www.privcom.gc.ca/ information/ guide/ auth 061013 e.asp, October 2006.

[22] W. Haga and M. Zviran, " Question-and-answer passwords: an empirical evaluation",Information
Systems, 16(3):335–343, 1991.

[23] M. Mannan and P. van Oorschot, " Security and usability: The gap in real-world online banking", In
New Security Paradigms Workshop (NSPW'07), September 2007.

[24] V. Griffith and M. Jakobsson, " Deriving mothers maiden names using public records", In Applied Cryptography and Network Security (ACNS). Springer, 2005.

[25] K. Bruce , "Tips for Avoiding Bad Authentication Challenge Questions", Security Professional Services , 2007