KNOWLEDGE-BASED AUTHENTICATION USING TWITTER CAN WE USE LUNCH MENUS AS PASSWORDS?

ManabuOkamoto[1]

[1] Kanagawa Institute of Technology, Kanagawa, Japan

ABSTRACT

The vast majority of online servicesrequire some form ofpersonal authentication. Unfortunately, standard password authenticationstrikes a poor balance between security and convenience, whereas strongerauthentication schemes,such as those involvingbiometrics, one-time passwords, and electronic certificates, depend on specialized hardware and/orhardware tokens. To achieve convenience, robustness, and cost-effectiveness together, we propose a scheme for dynamicknowledge-based authentication in which Twitter direct messaging is used to collectsimple, memorable question/answer pairs. We also conduct a user study to evaluate the proposed scheme.

KEYWORDS

Authentication, Knowledge-based authentication, Password, Twitter

1. INTRODUCTION

The vast majority of web services usesome form of password authentication, mainly due to its familiarity and easeof use. Unfortunately, theauthenticating strength of a password is generally opposed to its memorability, and writing down or otherwise storing a password makes it easier to compromise. To address these deficiencies, many developers have turned to knowledge-based authentication (KBA).Broadly described, KBA [1]-[4] is a method ofidentifying usersbased on their personal knowledge. In a typical KBA scheme, a user isasked to answer one or more secret questions, as part of a multifactor authentication or self- service retrieval of a forgotten password. In this paper, we describe an innovative scheme forKBA that usesTwitter to issue questions to, and receive answers from, a given user. Specifically, the service provider asks the user a dynamic question in the form of a Twitter message, responds to the question in the form a Twitter response message. For our target domain, we have chosen information that is commonly available, yet personalized: the user's most recent lunch menu. The effectiveness of the proposed system is demonstrated via user study and analysis.

DOI : 10.5121/ijnsa.2013.5501

2. WHAT IS KBA?

KBA schemes can be divided intotwo basic categories: static anddynamic. In static KBA, the user typically selects the questionss/he would like to be asked (e.g. 'What city were you born in?', 'What colour is your car?', 'What is your favourite food?', etc.)and provides the answer(s) to these questionsin advance—i.e.during registration with a givenservice provider (SP). The question/answer pairs are stored and used by the SP to verify the user's identity when necessary. Whilestatic KBAis relatively convenient for users, it poses distinct risks. For example,if an attackersomehow acquires the question/answerpairs for a givenaccount, s/he can use them to impersonate the user indefinitely. For this reason, users are urgednot to retain thesame question/answer pairsover a long period.

In a dynamic scheme, the questionsasked by the SP are different each time. While this is generally safer than static KBA, it imposes an additional burden on both the SP and the user. The only way toreduce this burden is for the dynamic KBA scheme toobtain some subset of user-specific information automatically.

3. RELATED WORK

KBA has been successfully applied to a number of real services.For example, many on-line banking systemsask users toregister question/answer pairs beforehand, and then pose one or all of these questions to the user when strong authentication is needed. If the usercorrectly answers all of the questions posed, s/he is allowed to use the service.

Figure 1 shows a typical UI for KBA. Note that in this case, the question/answer pairs are fixed around date of birth,favouritecolour, andfavourite animal. Although an attacker may have access to the user's date of birth, s/he is unlikely to know the answers to the other two questions. Thus, the SP will typically ask for data of birth and one of the remaining questions, reserving the third question in case the user gets an answer wrong. It is unlikely that the user will fail to answer both of the remaining questions, since they target relatively simple and memorable information.

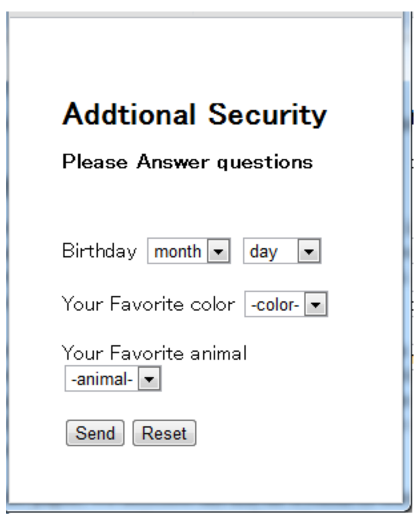

Figure1. A typical KBA UI

When the number of question/answer pairs is small, as in the case above, there is not much additional burden to the user. Unfortunately, the smaller the number of pairs, the easier it will be for attackers to acquire the necessary information. One can easily imagine that if Alice attends Bob's birthday party, and manages to strike up conversations about favourite animals and colours, Bob's bank account may soon be at risk. To mitigate this risk, we need a dynamic KBA scheme in which personalized question/answer pairs are obtained automatically.

In [5], researchers proposed a partial solution to this problem.Their system sends personal emails about which the user can be subsequently questioned.The system asks the user whether s/he has recently received e-mail from a specified sender. If s/he answers correctly, s/he is authenticated. The problem with this scheme is that it depends upon granting an e-mail server purview over personal e-mail data, and so may compromise security in other ways.

4. PROPOSED METHOD

In this paper, we propose use of Twitter [6] to store personal information for dynamic KBA. Twitter is a social networking and micro-blogging service. Userscan send short, timestampedmessages (of up to 140 characters) called tweets. These tweets aresimpler and more user-friendly than e-mail, and can be composed and read using either a PC or mobiledevice. It is noteworthy that, in Japan, when the earthquake of March 2011 knocked out many other services (including many email servers), Twitter continued to function for nearly all users. As a result, the service was used to exchange information in the most stricken areas. For this reason, we consider Twitter to be a robust choice for KBA communication.

For our information domain, we have chosento target personal lunch menus. This choice has two distinct advantages. First, almost all users in Japan consume lunch on a daily basis, irrespective of variations in breakfast and dinner plans.Second, because lunch menus tend to be simple, users generally remember the mover the course of several days. Assuming that both the SP and user have Twitter accounts, and that each 'follows' the other (i.e. is subscribed to the other's Twitter message stream), the two parties will be able tocommunicate directly through tweets, for the purpose of KBA. Figure 2 illustrates how this communication will proceed.

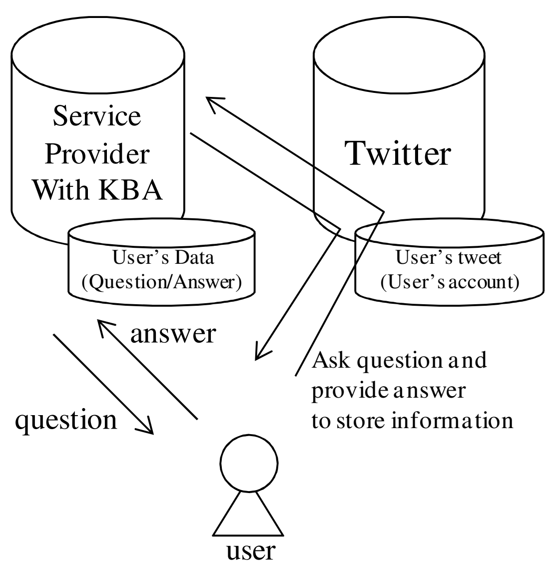

Figure 2. KBA scheme usingTwitter

The steps involved in this scheme are as follows:

1) SP sends user Alice a direct message containing a simple question,namely'What did you have for lunch today?'
2) Alice replies with a direct message containing her answer:'Cheeseburger'. Because the question and the answer are both direct messages, other Twitter users cannotread them.
3) SP stores the question-answer pair, in this case: 'Lunch on February 15'– 'Cheeseburger'– 'Alice'. SP repeats step 1-3.
4) When Alice wants to access the SP, she sends her ID.
5) In return, the SP asks a question based on theinformation stored in Step 3: 'What did you have for lunch on February 15?'To prevent attackers from discovering and using the answer in Alice's stead, the SP sets a brief window of time during which the answer will be accepted.
6) Alice answers the question promptly and the SP confirms heranswer. Steps 5 and 6 may be repeated several times. Alice must answer all questions correctly.
7) SP authenticates Alice based on her confirmed answers and grants her access to services on the SP.

Note that, in Step 5, SP can also ask questions via direct message on Twitter, in which case the SP must alert Alice accordingly: 'We have sent a question to your Twitter account. Please read this question and enter your answer here'. This strategy is more secure since it uses multiple channels of personal communication,and requires that the user also have access to her Twitter account.Figure 3 provides a sequence diagram for this strategy.

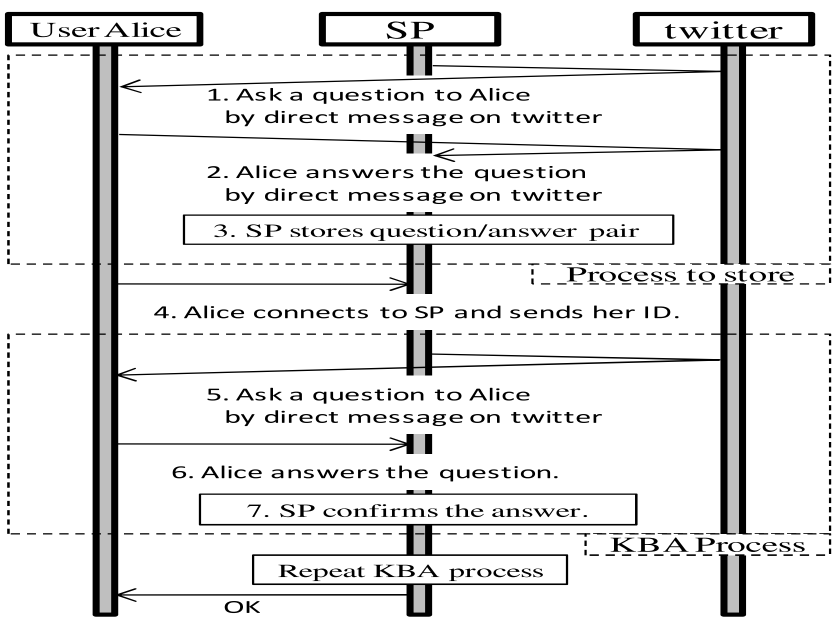

Figure 3. KBA sequence.

5. CAN WE USE A LUNCH MENU AS A PASSWORD?

The frequency and regularity of lunchtime dining make it an ideal target for dynamic authentication questions. The simple question, 'What did you have for lunch today?' will have an answer that tends to vary from day to day, yet remains relatively easy to remember.

Consider the simple interactions depicted in Figures 4–9. First, Alice is asked via direct message what she had for lunch today (Figure 4).

Figure 4. Tweet for a question.

She replies with a direct message (Figure 5), resulting in a parsable answer tweet (Figure 6).

Figure 5. Reply for a question on Twitter.

Figure 6. Answer tweet.

When Alice wants to accessthe SP, she logs in at the website (Figure 7).

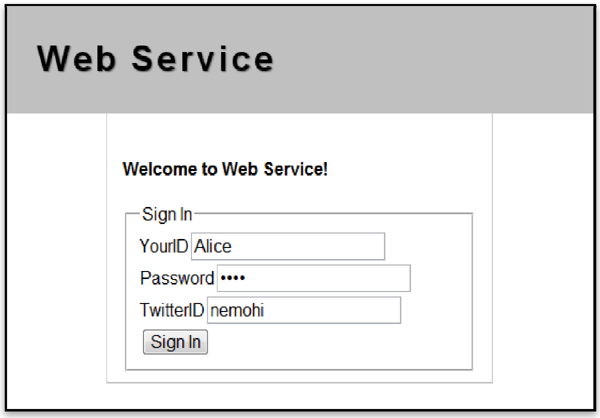

Figure 7. SP login

Finally, the SP sends the dynamic authentication question 'What did you have for lunch on January 17?' to Alice (Figure 8).

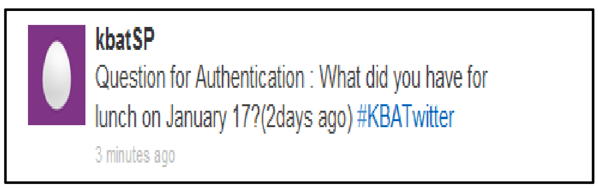

Figure 8. Authentication question tweet

Alice answers by inputting'Cheeseburger'into the web form provided (Figure 9).

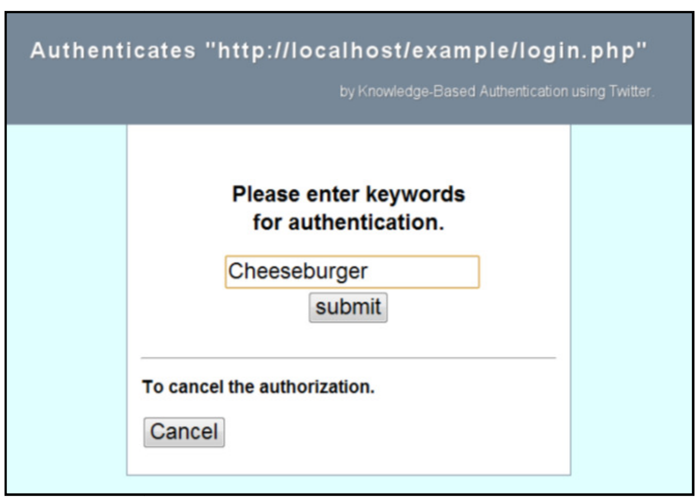

Figure 9. Input answer.

If this answer is confirmed, Alice is authenticated. The question/answer process can be repeated as many times as the SP deems necessary for authentication.

6. SECURITY ANALYSIS

The multi-channel nature of our authentication strategy, coupled with Twitter's support for SSL communications, make for a highly secure system. Even if an attacker, Bob,gains regular knowledge of Alice's lunch menus, he will need to have access to her Twitter account to make any use of his knowledge. Without knowing what day the question is targeting, he will not be able to retrieve the correct answer.

7. USER STUDY

We conducted a user study often test subjects. The details of this study were as follows:

Testers: 10university students, 21-22 years of age.

Test Period : 6 weeks:2 weeks for collection of question/answer pairs,and 4weeksof authenticated SP access, using the proposed strategy.

Test Method: Our server automatically sentquestions via twitter direct message to all test subjects at lunch time (13:00) each day. The test subjects either ignored or answered these questions via twitter direct message. Each answer resulted in storage of a question/answer pair on the server. The users were then asked to login at the server three times per week, each time answering 3 authentication questions.

Question for KBA: Everyday

SP logins per tester:12 (Every Tuesday , Wednesday , and Friday for the final4 weeks)

Authentication questions at login: 3

- What was one of your lunch menus for the period beginning 3 days ago and ending yesterday?
- What was one of your lunch menus for the period beginning 7 days ago and ending four days ago?
- What was one of your lunch menus for the period beginning 14 days ago and ending 7 days ago?

Time window for each question:10 seconds

The results of our study are given in Table 1.

The [Received] column is the rate at whicha subjectansweredthe questions sent viatwitter direct message ('What did you havefor lunch today lunch?'). Note that all test subjects answered all of the sent questions. In a real-world scenario, this rate would tend to be lower than 100%.

The [Correctness]column is the rate at which a subject answereda given set authentication questions correctly. A value of lower than 100 indicates that the givenuser gave at least one wrong answer.

Finally, the [Attacker] column is the rate at whichan attacker answered a given set of authentication questions correctly. Attackers and their targets are chosen at random from the existing group of subjects. If the attackeranswersall of thequestionsin a challenge set correctly, the value will be higher than 0, indicating a successful breach of security.

Note that when question scope included only the three preceding days, successful attacks did occur, and when authentication scope covered the entire two weeks, subjects found it difficult to remember the correct answer. Although the subjects can retrieve a complete record of their answers from their Twitter message feed, doing would likely take more time than is permitted by the answer window. Our tentative conclusion is that the middle scope, one week, produces the best balance between authentication strength and the user memory span.Figure 10 shows the challenge UI that would be used in this case.

It should be noted that our attackers benefited from a worst case security scenario. Many of our subjects lunched together on a regular basis, and so had partial knowledge of one another's lunch menus.This, coupled with their prior knowledge of the attack opportunity, resulted in predictable security breaches. In a real-world scenario, gaining such advantages would require dedicated social engineering.

Table 1. Result of our KBA.

User	Received %	Correctness %			Attacker %		
		3days	1 week	2 weeks	3days	1 week	2 weeks
A	100	100	100	83	8	0	0
B	100	100	83	50	0	0	8
C	100	100	100	100	0	0	0
D	100	100	100	83	0	0	0
E	100	100	100	75	0	0	0
F	100	100	83	75	0	0	0
G	100	100	100	75	0	0	0
H	100	100	83	50	0	0	0
I	100	100	75	50	0	0	0
J	100	100	100	25	8	0	0

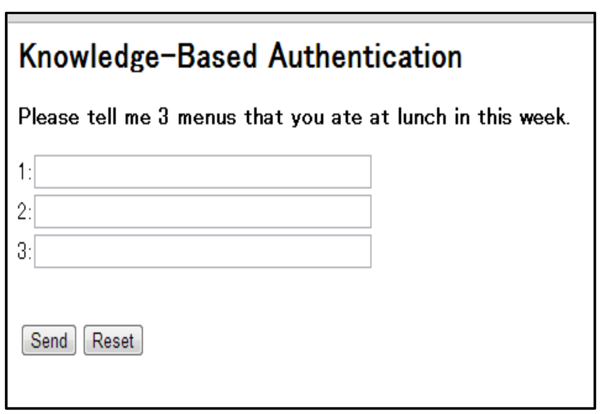

Figure 10. Appropriate question.

8. FUTURE WORK

Our experiments showed a clear need to normalize answer content. If, for example, Alice produces the answer ‘hamburger’ when the correct answer was in fact ‘cheeseburger’, the system should be able to judge her answer correct within some degree of tolerance.

We might also introducea special tag (e.g. ‘#kba’) to mark answers to implicit and/or anticipated questions.For example, if a subject uses the standard Twitter micro-blogging feature toreport that‘Today’s lunchwassushi. Delicious. #kba’, the system should be able to parse and store ‘sushi’ as today’s lunch menu, and thereby obviate the usual question/answer exchange. Since this information is public, we might then need to narrow the time windowfor answering (say, to 5 seconds), as an additional security measure against attentive attackers. Note that this constitutes a rather poor compromise, and could be used only in a relaxed security scenario.

9. CONCLUSION

In this paper, we proposed a knowledge-based authentication scheme that uses Twitter to obtain question/answer pairs for authentication. Although this scheme requires regular user responses to an on-going question (‘What did you have for lunch today?’), it has the potential to ease the overall security burden, for both users and service providers.

REFERENCES

[1] What is knowledge-based Authentication?, http://searchsecurity.techtarget.com/definition/knowledge-based-authentication.

[2] Knowledge Based Authentication, http://csrc.nist.gov/archive/kba.

[3] N. Asokan, V. Shoup, M.Waidner, (2004) “Quantifying assurance of knowledge based authentication,”Proceedings of the 3rd European Conference on Information Warfare and Security,pp109-116.

[4] Ye Chen, Divakaran Liginlal, (2008) “A maximum entropy approach to feature selection in knowledge-based authentication,”Decision Support Systems,Vol.46, Issue 1, pp388-398.

[5] Nishigaki Masakatsu, Koike Makoto, (2006) “A user authentication based on personal history: A user authentication system using e-mail history,”Transactions of Information Processing Society of Japan, Vol.47, No.3, pp945-956.

[6] Twitter, http://twitter.com/.

[7] M Sreelatha, M Shashi, M Anirudh, Md Sultan Ahamer, V Manoj Kumar, (2011) “Authentication schemes for session passwords using color and images,”IJNSA,Vol. 3, No. 3.

[8] Sreelatha Malempati, ShashiMogalla, (2011) “An ancient Indian board game as a tool for authentication,”IJNSA,Vol. 3, No. 41.

[9] B.Schneier, (1996) *Applied Cryptography*, John Wiley & Sons.

[10] Sreelatha Malempati, Shashi Mogalla (2011) “User Authentication using Native Language Passwords,”IJNSA,Vol. 3, No. 6.

[11] Lein Harn , Changlu Lin(2013) "An Efficient Group Authentication for Group Communications,"IJNSA,Vol. 5, No. 3.

Authors

Manabu Okamoto

Received hisB.S. and M.S. degrees in Mathematics from Waseda University in 1995 and 1997, respectively. In 2010, he received hisdoctorate degree inGlobal Information and Telecommunication from Waseda University. He is currentlyAssociate Professor at Kanagawa Institute of Technology.