Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2010 Proceedings

Americas Conference on Information Systems (AMCIS)

8-2010

User Acceptance of Multiple Password Systems: A Proposed Study

Christopher Kreider
University of Texas at San Antonio, Christopher.Kreider@utsa.edu

User Acceptance of Multiple Password Systems: A Proposed Study

Christopher Kreider
University of Texas at San Antonio
Christopher.Kreider@utsa.edu

V. Srinivasan Rao
University of Texas at San Antonio
Chino.Rao@utsa.edu

ABSTRACT

The traditional means of user authentication based on usernames and passwords is subject to a number of behavioral concerns that can significantly reduce the security provided. As such, an important part of proposing a new authentication scheme should involve careful consideration of behavioral factors. Little research has actually examined the role user acceptance plays in different authentication schemes. Our research in progress proposes the investigation of user acceptance of a cognitive password system comprised of multiple authenticators. Specifically we will investigate the role that password characteristics, such as number of passwords and password complexity, coupled with frequency of use, play in users' perceptions and overall willingness to faithfully adopt an alternative authentication system.

Keyword

Authentication, Associative Passwords, Cognitive Passwords

INTRODUCTION

The most common form of authentication in use today is the username/password combination. Over the years, good password practices have been established for this authentication scheme. For instance, it is recommended that strong passwords should be used, i.e., the password should be of a minimum length, include lower case and upper case letters, numbers and non-alphanumeric characters. Such passwords are generally difficult for others to discover by guessing. However, they are also difficult for the user to commit to memory and subsequently recall from long-term memory (Adams et al. 1997; Brown et al. 2004). This problem is exacerbated by the increasing number of passwords that users are required to remember. The ever increasing number of passwords, coupled with the recommendation that the same password not be used for more than one system, leads to the "password overload syndrome" (Furnell 2005; Hovav and Berger 2009). Additionally, it is recommended that passwords be changed periodically. The collective burden, of having to remember so many frequently-changing strong passwords, causes most users to adopt insecure coping mechanisms. Primarily, this takes the form of writing passwords down or maintaining a file on the computer with the passwords, which are subject to discovery by physical and electronic intruders respectively. Alternately, users may use the same password for multiple systems despite rules advising against such a practice (Ives et al. 2004; Smith 1987; Zviran and Haga 1999). Further, passwords, no matter how strong they are, are subject to discovery by others by practices such as phishing and spoofing. In effect, existing username/password authentication systems have weaknesses, which could compromise the overall security of personal and organizational information assets.

Variations of the username/password authentication systems have been proposed. These include the use of longer easier-to-remember passphrases (Porter 1982), and the use of multiple easily-remembered passwords (Zviran and Haga 1990). Zviran and Haga, and later Bunnell et al. (1997), have shown that the cognitive password system based on the use of multiple question and answer passwords reduce the load on memory, and can also yield an acceptable tradeoff between memorability and guessability. Despite such encouraging results, these variations have not been used in developing primary authentication systems.

Our longer-term research goal is to examine the merits of a cognitive password system as a universal alternative to the current strong password system. Many questions have to be answered to determine if the proposed system provides significant advantages over the traditional system. For instance, Zviran and Haga (1990) have studied memorability and guessability for a specific set of parameters. However, there is no research to indicate whether the results are robust over a broader range of parameters. To provide an example, they test the ability of subjects to remember the full set of passwords after three months. One could argue that memorability may suffer more over longer periods of time, or that memorability for frequently-used passwords may be higher than memorability of infrequently-used passwords. Further, Zviran and Haga have not examined user response to such systems. Users may be able to remember the multiple passwords, but may be resistant to

entering five passwords (Zviran and Haga's recommendation) each time to gain access to a computer system. Thus, much research has to be done to progress the idea beyond the preliminary work that has been done so far.

The current article describes a proposal to test user response to a multi-password system to access an experimental site that provides task-relevant information. Thus, the study is expected to provide results that would be relevant to access task-relevant sites, such as user accounts in organizations.

The rest of the article is organized as follows. The next section provides a review of the relevant literature. The following section articulates research questions. Then the theoretical basis of the study is discussed and hypotheses developed. A proposed study is described, followed by a few concluding remarks.

LITERATURE REVIEW

Weaknesses of Traditional Password Systems

We use the term traditional password system to refer to the authentication system based on single user-generated password systems, which require strong passwords. In the past decade or so, with the increasing potential for online hacking, password policies, which guide the creation and use of passwords, have become commonplace. Some policies can be enforced through technical means. For instance, systems can force a user to create a strong password, but such technical enforcement is not always implemented. Even if implemented, users may find ways to violate the spirit of the rule by choosing easily guessed passwords that still meet strength requirements (e.g. P@55w0rd)(Keith et al. 2009). Other policies are entirely dependent on user compliance. For instance, users are advised not to write their passwords down and put them in places where they may be easily found. Such policies cannot be technically enforced. In summary, the traditional password system, despite its widespread adoption and use, has a variety of shortcomings that leave perceptions of its reliability and security unsurprisingly low (Furnell 2005).

A password is compromised when it is no longer a secret only known to the user, and can occur when an attacker guesses the password, gains access to the password, or a combination of both. Guessing attacks occur online, and generally consist of an attacker repeatedly guessing commonly used passwords (Ding and Horster 1995; Keith et al. 2009). Attackers may also gain access to the password, either in its plaintext or encrypted form in a variety of ways including phishing attacks (Hovav and Berger 2009), man-in-the-middle attacks(Schneier 2005), Trojans/keyloggers (Schneier 2005) dictionary attacks (Keith et al. 2009) and knowing where an user wrote his/her password down (Keith et al. 2009; Porter 1982). Research into problems with the traditional password systems has resulted in the development of several variations, such as associative passwords (Smith 1987), cognitive passwords (Haga and Zviran 1989; Haga and Zviran 1991; Zviran and Haga 1990) passphrases (Porter 1982) and graphical passwords (Xiaoyuan et al. 2005). Associative passwords are based on user-generated word association cue/response pairs, instead of the cue being only "password" (Smith 1987). Cognitive passwords are an extension of associative passwords in which the cue, instead of being a word, takes the form of a question based on personal facts or opinions (Zviran and Haga 1990). Passphrases are based on using an existing password system, but encourage significantly longer passwords, of up to 80 characters, by having users select passwords consisting of many words (a phrase) instead of a single word (Porter 1982). Graphical passwords use an image as the cue, and the response requires the user to click the appropriate places on the image, in the appropriate order (Xiaoyuan et al. 2005). What these alternative methods have in common is that they attempt to increase overall security while decreasing memory load on users. Of specific interest to us is the cognitive password system proposed and researched by Haga and Zviran (1989; 1991), Zviran and Haga (1990) and subsequently covered by Bunnell et al. (1997).

Cognitive Passwords

Cognitive passwords are a form of associative password system, in which, instead of the traditional name and password prompt, users are prompted with a question whose answer is known to the user but presumed to be unknown to outside parties. Cognitive questions fall into two categories as either being fact or opinion based. An example of a fact based question would be "What is the name of the last grade school you attended?" and an example of opinion based question would be "Who is the greatest President of all times?"

Haga and Zviran (1989) proposed that, in lieu of the single password required in traditional password systems, a cognitive password system would require a fixed number of questions (20) to be answered by the user at enrollment. To gain access to the system, the authentication process would require the user to answer five randomly selected questions from the set of twenty answered at enrollment. If a user answers one of the questions incorrectly, then the user would be presented with another set of random questions. The second set would be generated by sampling with replacement.

The empirical studies by Haga and Zviran focus on demonstrating two points (Haga and Zviran 1991; Zviran and Haga 1990a). First, they demonstrate that cognitive passwords are easier for users to remember than user- or system-generated single passwords with user recall of passwords being tested after a lapse of three months. Second, they demonstrate that while single cognitive passwords of a user may be guessed, certain cues when used appropriately could yield improved memorability/guessability ratios. They replicated their study with different subject pools to establish the validity of their results under the same set of conditions. Bunnel et al.'s (1997) replication over a shorter period of two weeks also supported the increased memorability of this type of system.

These results provide a good starting point to argue the merits of a multiple password system based on cognitive passwords. However, they leave several questions unanswered. First, all passwords are not used with the same frequency. Some accounts are accessed daily, while others may be accessed monthly and still others annually. In our experience, complex strong passwords are difficult to commit to memory initially, but once memorized are recalled with ease if used daily, but more difficult to recall if used infrequently. Second, Haga and Zviran (1989) suggest five random cognitive passwords out of a set of twenty. This raises the questions, are five passwords to access a system too many or too few, and, is a set of twenty enough to safeguard against accidental guessing? Third, user acceptance of this variation of the traditional password system has not received much attention.

User Acceptance Studies

Faithful adoption of mandated systems, i.e., the use of systems as intended by the designers, requires an understanding user acceptance. Zviran and Elrich (2006) have recently emphasized the importance of user acceptance in selecting appropriate authentication systems.

Earlier, Zviran and Haga (1993) investigated five different authentication systems, focusing on memorability. They asked their subjects to rank the systems, first according to ease of recall, and then according to how much they liked them. The ranking results were compared to the objective measures of recall taken in the experiment, and suggested there was no relationship between the two (e.g. users ranked self-generated passwords first for ease of recall, however the study's results showed that this type of password was actually third when measured objectively with recall rates of 27.2%). This study provides information on preference, which may be argued to be a surrogate for user acceptance.

A key study of user acceptance of authentication systems is Keith et al.'s (2009) investigation of user acceptance of passphrases. Their research not only focuses on memory and typographical errors, but also on users' perceptions of ease of use, and usefulness from the perspective of the technology acceptance model. Their model shows that the login failure rate is influenced by perceived ease of use, which influenced perceived usefulness, which in turn led to an intention to adopt. No other study has examined user acceptance, and its role in adoption of an authentication system.

RESEARCH QUESTIONS

In general, we are interested in understanding user response to a multi-password system. There are two key issues that need to be clarified. First, we need to compare user responses to the multiple cognitive passwords system to the user responses to the traditional single strong password system. Second, we need to shed light on user responses to the multiple password system for the various combinations of parameters. Broadly, the research questions are:

a) Are multiple password systems based on easily remembered cognitive passwords preferred to single password systems based on more difficult to remember strong password systems?

b) To what extent does the number of cognitive passwords used in a multiple password system affect user perceptions of the ease of use and usefulness of the system?

c) To what extent does the frequency of use of the system affect the perceived ease of use and perceived usefulness of the system?

Single strong passwords may be user-generated or system-generated. User-generated passwords allow the users to choose whatever combination of characters they like, within system constraints, to be their authenticator where system generated passwords are based on randomly generated characters and are assigned to users without giving them a choice. Keith et al. (2007) did not find any support for the hypothesis that user generated passwords will lead to fewer memory errors than system generated passwords. On that basis, we will test only user generated strong passwords. We opt for user generated passwords rather than the system generated to stay consistent with the idea that cognitive passwords will be user generated.

THEORETICAL BASIS and HYPOTHESES

Technology acceptance model (TAM) is the generally used basis for studying acceptance of technologies. In its simplest version, TAM states that perceived ease of use and perceived usefulness of a technology will influence the adoption of the technology (Davis 1989). In applying this model to the study of cognitive passwords, one needs to examine the relationship between the characteristics of the password systems to perceived ease of use and perceived usefulness of system, such as was done by Keith et al. (2007). We adapt the model tested by Keith et al. for our study (see Figure 1).

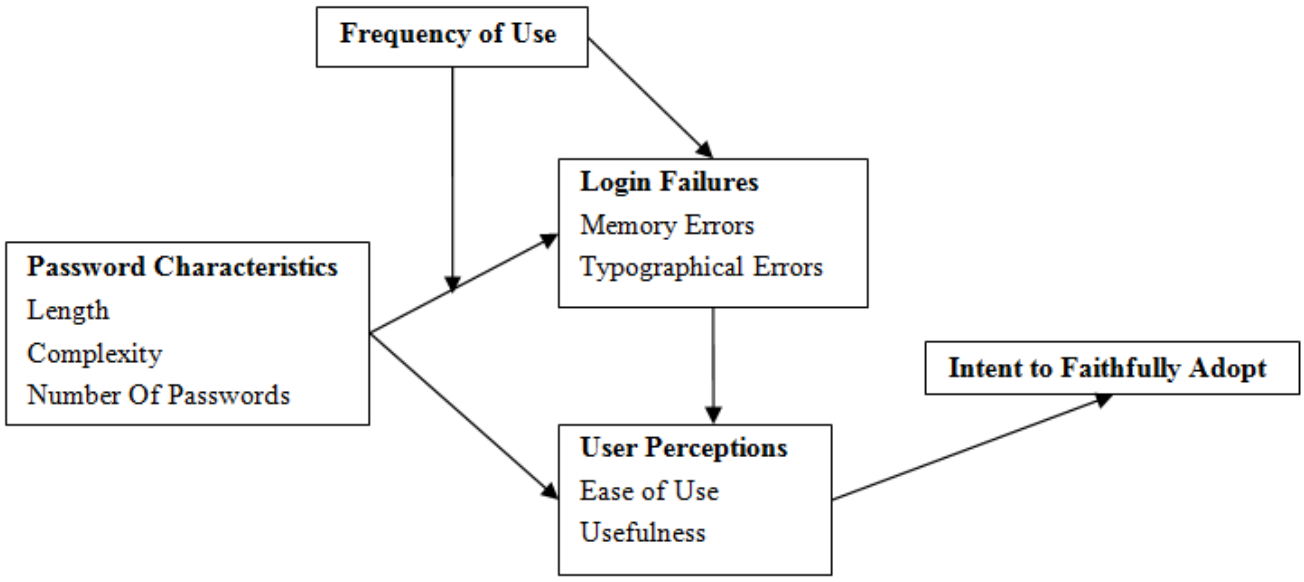

Figure 1 Proposed Theoretical Model

Our theoretical model deviates from that of Keith et al. in some respects. First, once an organization adopts a password system, users are compelled to use it. However, users do have the choice to adopt a system faithfully or not, i.e., use the system in the spirit in which it was designed rather than use the system in ways which subvert the intent of the designer. So, we have modified their dependent variable intent to adopt to intent to faithfully adopt.

Second, Keith et al. (2007) studied the differences between passphrases, user generated passwords and computer generated passwords. They indicate that these differ along the dimensions of password length, password complexity (randomness of characters) and source of password (user-generated or system-generated). The proposal to use multiple passwords brings in an additional dimension, i.e., the number of passwords. This will constitute one of the key variables in our theoretical model. Further, in our study, users will generate their own passwords, so source has been removed from the list of password characteristics. We will measure length of passwords to examine if it explains variances in dependent variables.

Third, the Keith et al. model indicates that the effect of login credentials (password characteristics) on perceived ease of use will be mediated by the number of memory and typographical errors. We believe that, in addition to the mediated relationship, there is also a direct relationship between password characteristics and the perceived ease of use.

Fourth, frequently used passwords are easier to remember than infrequently used passwords. We have included frequency of use as a variable that will influence login errors.

Fifth, we argue that simple cognitive passwords are easier to remember than complex strong passwords because they have already been committed to long term memory in the users' mind and are therefore not subject to short term memory limitations. Complex strong passwords, when used repeatedly can also get imprinted in the users' minds when used repeatedly and frequently. Our model indicates that frequency of use moderates the relationship between password characteristics and login errors. In other words, for frequently used passwords, cognitive passwords and strong passwords are likely to lead to same number of errors, whereas, for infrequently used passwords, strong passwords will lead to greater number of errors than cognitive passwords.

Lastly, it should also be noted that security technologies are different from technologies that are primarily designed to improve productivity. With productivity technologies, such as a payroll application or an enterprise resource planning application, users may perceive the immediate efficiency or effectiveness with which a user can execute tasks related to his/her primary responsibilities. This ability to assess whether a technology improves efficiency or effectiveness helps influence perceived usefulness. With security technologies, the real usefulness is in the improved overall security. To most users, their responsibilities are of primary concern and security requirements are of secondary concern. Based on this argument, perceived usefulness may not be easily influenced by changes in the characteristics of the password systems (Liang and Xue 2009).

Password Characteristics and Login Failures: Keith et al. (2007) demonstrated that use of passphrases led to fewer login errors than complex single passwords, both user-generated and computer-generated. In the current study, the individual cognitive passwords are not longer than the user-generated strong password, but there are more of them. The lower complexity of the cognitive passwords suggests that users of multiple cognitive passwords will make fewer login errors (both typographical and memory). The larger number of cognitive passwords will not cause any increase in memory errors, because each password is easily remembered. It is unclear whether the larger number of cognitive passwords users are required to enter will cause more typographical errors.

Cognitive passwords are easier to recall because they are embedded in the user's memory and as such should be not be affected by short term memory failures. It is argued that complex passwords, if used frequently can also get embedded in the user's memory and be recalled easily, i.e., if a password is being used frequently, there should be no difference between the login errors of cognitive passwords and strong passwords. On the bases of these arguments, it is hypothesized:

H1a: For infrequently used (sets of) passwords, users of multiple cognitive passwords will make fewer total login errors than users of single strong passwords.

H1b: For frequently used (sets of) passwords, there will be no difference in the number of errors made by users of multiple cognitive passwords when compared to the number of errors made by users of single strong passwords.

Password Characteristics and Perceived Ease of Use: It is believed that complex passwords following random patterns that are harder to recall will be perceived as more difficult to use than cognitive passwords that follow familiar patterns that are used regularly. Based on this, it is hypothesized:

H2a: The perceived ease of use of cognitive passwords will be higher than the perceived ease of use of strong passwords, for the same number of passwords.

It is argued that users will find it annoying to enter multiple passwords. In fact, the larger the number of passwords that have to be entered to gain access to a system, the more likely it is that users will be annoyed. Based on this, it is hypothesized:

H2b: The perceived ease of entering multiple cognitive passwords will be negatively correlated to the number of passwords that have to be entered.

Login Errors and Perceived Ease of Use: Login errors will slow the user down in their effort to start using a system. The greater the number of login errors the greater will be the user annoyance, and consequent perception that the system is not easy to use. So, it is hypothesized:

H3a: The perceived ease of use will be negatively correlated to the number of login errors made by the user.

Keith et al (2007) have reported a significant correlation between login errors and perceived usefulness (correlation coefficient = -0,14, $p<0.05$). Based on that, it is hypothesized:

H3b: The perceived usefulness of the password system will be negatively correlated to the number of login errors made by the user.

Password Characteristics, Login Errors and Perceived Usefulness: The usefulness of a password system lies in the increased security that it provides the information assets. Experiential use of a test system does not provide any connection to possible real improvement in security. Hence, it is argued that password characteristics will not be correlated to perceived usefulness.

H4a: Password characteristics will not be correlated to perceived usefulness.

PROPOSED METHODOLOGY

We propose to conduct a longitudinal experiment to assess user response to multiple password systems. In this section, we describe the planned experiments.

Experimental Design: There are three parameters that will be manipulated: (a) complexity of password, (b) number of passwords, and (c) the frequency of use.

Complexity of passwords will be either simple or complex. Simple passwords will consist of cognitive passwords, which will primarily be common facts that are a part of a user's life. Such facts are presumed to be deeply ingrained in the memory of the user, unlikely to be forgotten. Complex passwords, which are usually referred to as strong passwords in the traditional password systems are random combinations of upper and lower case characters, digits and non-alphanumeric characters. Greater effort is presumed to be needed to retain in memory and recall when needed.

Number of passwords refers to the number of cognitive passwords that the user is expected to provide. Individual cognitive passwords are subject to discovery by guessing, spoofing or phishing. The requirement of multiple cognitive passwords for authentication reduces the likelihood of such discoveries. However, it is unclear how many passwords users would be willing to tolerate. While the research by Zviran and Haga (1990) used five, we will explore alternatives of one, three, five and seven.

Users in real life have multiple computer accounts. Some accounts are used daily, others once a week, and still others at longer intervals. For experimental purposes, expecting subjects to log onto a simulated site daily would be excessive. At the other end, most student subjects are available for a three to four month period, so required usage intervals of longer than a month would provide the subjects insufficient experience to assess ease of use. Based on these arguments, two levels of frequency of use will be used: weekly and monthly. Subjects will be emailed with instructions to access the website and retrieve information required for their classes.

In summary, a fractional factorial design is planned. For the complex password, the number of passwords will be one. For the cognitive password case, the number of passwords will be one, three, five and seven. For each of these cases, there will be two levels of usage frequency: weekly and monthly. All passwords will be user-generated. Subjects will not be able to change passwords during the experiment because of the relatively short span of the study.

	Weekly		Monthly	
Number of Passwords	Strong Password (complex)	Cognitive Password (simple)	Strong Password (complex)	Cognitive Password (simple)
1	X	X	X	X
3		X		X
5		X		X
7		X		X

X = subjects assigned to these cells.

Table 1. Fractional Factorial Design

Subjects: Students from the Introduction to Management Information Systems class will be solicited to volunteer as subjects. Students are appropriate, as they need to access multiple accounts on a variety of discrete systems.

Experimental Set Up and Procedures: Subjects will complete an online demographics questionnaire when they enroll. In addition to the demographics, initial information will be gathered on their current password needs and experiences. Questions would include: how many computer accounts does the subject have, do these accounts have strong password requirements, does the subject use strong passwords, does the subject use same password for multiple accounts, does the subject write down passwords and so on. Then they will be assigned at random to one of the experimental conditions. Based on the experimental cell that a subject is assigned to, he/she will be required to set up a password or set up passwords.

Subsequently, subjects will access the experimental web site when instructed by email to do so. Once they have logged in, a class related exercise or information will be provided. Specifically, the site will be designed to be a goal oriented site, that is a site they visit to perform a specific task, as opposed to generalized tasks such as social networking. When a subject logs in, the time, date of login will be recorded. The subject will be allowed to log in only when they have been requested to log in, to ensure that the frequency of usage is controlled.

At the end of a three-month period, the subjects will complete a questionnaire, which will include items for perceived ease of use, perceived usefulness and willingness to adopt. Additionally, subjects from each cell will be invited to volunteer for an

additional exit interview. In the interview, we will try to elicit reasons why they believe such a system would be beneficial or detrimental.

Measures: The variables in the study will be measured as follows:

Complexity of Password: For the experimental groups in which the subject are required to have a complex password, the password will be validated to ensure that it meets the requirements, i.e., the password includes upper and lower case letters, digits, and non alphanumeric characters, and is at least eight characters long. In the case of cognitive passwords, subjects may use simple passwords. The passwords will be scrutinized to see if complex passwords are being used.

Number of passwords: Subjects with complex passwords (traditional strong password) will have only one password, Subjects with cognitive passwords will have one, three, five or seven passwords.

Frequency of Password Use: Subjects will be required to access the target experimental website weekly or monthly, in response to an email request from the researchers. Subjects will not be allowed to access the site between email requests.

Number of Memory and Typographical Errors: Distinguishing between memory and typographical errors raises some issues. All password entries will be recorded. If more than one attempt was required to access the site, the subject will be asked to complete a short questionnaire to generate a self-report on why they failed to login correctly. The Levenshtein distance between the correct password and the passwords entered will be determined following procedures followed by Keith et al (2007; 2009) to validate the self-reported response. If after three attempts the subject is not able to get the password(s) correct, they will have an option to click on a button to indicate that they cannot remember the password. If they do so, they will be asked to complete the short questionnaire on why they failed to login correctly.

Perceived Ease of Use, Perceived Usefulness, Intent to Faithfully Adopt: The scales used by Keith et al. (2007) will be used with minor modifications.

CONCLUSION

This article describes research-in-progress. The concept of using multiple easily-remembered cognitive passwords in lieu of a single difficult-to-remember strong password has been around for many years. Earlier researchers have shown that users recall cognitive passwords more readily than strong passwords, and that it is difficult for others to guess sub-sets of cognitive passwords. For the concept to progress further, much research remains to be done. One issue that has to be addressed is the user response to multiple password system. In the current article, we have proposed an experimental study to examine user acceptance of the system. We invite feedback on the concept of multiple password authentication systems, and the details of our experimental design.

ACKNOWLEDGEMENTS

We thank the track chair, the mini-track chair and the reviewers for their constructive feedback. The article is greatly improved as a result of their suggestions.

REFERENCES

Adams, A., Sasse, M., and Lunt, P. 1997. "Making Passwords Secure and Usable," *People and Computers* (12), pp 1-20.

Brown, A., Bracken, E., Zoccoli, S., and Douglas, K. 2004. "Generating and Remembering Passwords," *Applied Cognitive Psychology* (18:6).

Bunnell, J., Podd, J., Henderson, R., Napier, R., and Kennedy-Moffat, J. 1997. "Cognitive, Associative and Conventional Passwords: Recall and Guessing Rates," *Computers & Security* (16:7), pp 629-641.

Davis, F.D. 1989. "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," *MIS Quarterly* (13:3), pp 319-340.

Ding, Y., and Horster, P. 1995. "Undetectable on-Line Password Guessing Attacks," *SIGOPS Oper. Syst. Rev.* (29:4), pp 77-86.

Furnell, S. 2005. "Authenticating Ourselves: Will We Ever Escape the Password?," *Network Security* (2005:3), pp 8-13.

Haga, W.J., and Zviran, M. 1989. "Cognitive Passwords:From Theory to Practice," *Data Processing & Communications Security* (13:3), pp 19-23.

Haga, W.J., and Zviran, M. 1991. "Question-and-Answer Passwords: An Empirical Evaluation," *Information systems* (16:3), pp 335-343.

Hovav, A., and Berger, R. 2009. "Tutorial: Identity Management Systems and Secured Access Control," *Communications of the Association for Information Systems* (25:1), p 42.

Ives, B., Walsh, K.R., and Schneider, H. 2004. "The Domino Effect of Password Reuse," *Commun. ACM* (47:4), pp 75-78.

Keith, M., Shao, B., and Steinbart, P. 2009. "A Behavioral Analysis of Passphrase Design and Effectiveness," *Journal of the Association for Information Systems* (10:2), pp 63-89.

Keith, M., Shao, B., and Steinbart, P.J. 2007. "The Usability of Passphrases for Authentication: An Empirical Field Study," *International Journal of Human-Computer Studies* (65:1), pp 17-28.

Liang, H., and Xue, Y. 2009. "Avoidance of Information Technology Threats: A Theoretical Perspective," *MIS Quarterly* (33:1), pp 71-90.

Porter, S.N. 1982. "A Password Extension for Improved Human Factors," *Computers & Security* (1:1), pp 54-56.

Schneier, B. 2005. "Two-Factor Authentication: Too Little, Too Late," *Commun. ACM* (48:4), p 136.

Smith, S. 1987. "Authenticating Users by Word Association," Human Factors and Ergonomics Society, pp. 135-138.

Xiaoyuan, S., Ying, Z., and Owen, G.S. 2005. "Graphical Passwords: A Survey," *Computer Security Applications Conference, 21st Annual*, pp. 10 pp.-472.

Zviran, M., and Haga, W. 1993. "A Comparison of Password Techniques for Multilevel Authentication Mechanisms," *The Computer Journal* (36:3), p 227.

Zviran, M., and Haga, W. 1999. "Password Security: An Empirical Study," *Journal of Management Information Systems* (15:4), pp 161-185.

Zviran, M., and Haga, W.J. 1990. "Cognitive Passwords: The Key to Easy Access Control," *Computers & Security* (9:8), pp 723-736.