European Journal of Information Systems (2009) 1–12

www.palgrave-journals.com/ejis/

Improving multiple-password recall: an empirical study

Jie Zhang[1],
Xin Luo[2],
Somasheker Akkaladevi[1] and
Jennifer Ziegelmayer[3]

[1]Department of Computer Information Systems, School of Business, Virginia State University, Petersburg, VA, U.S.A.; [2]Anderson School of Management, The University of New Mexico, Albuquerque, NM, U.S.A.; [3]Computer Information Systems, College of Business, Delta State University, Cleveland, MS, U.S.A.

Correspondence: Jie Zhang, Department of Computer Information Systems, School of Business, Virginia State University, Petersburg, VA 23806, U.S.A.
E-mail: jzhang@vsu.edu

Abstract
As one of the most common authentication methods, passwords help secure information by granting access only to authorized parties. To be effective, passwords should be strong, secret, and memorable. While password strength can be enforced by automated information technology policies, users frequently jeopardize secrecy to improve memorability. The password memorability problem is exacerbated by the number of different passwords a user is required to remember. While short-term memory theories have been applied to individual-password management problems, the relationship between memory and the multiple-password problem has not been examined. This paper treats the multiple-password management crisis as a search and retrieval problem involving human beings' long-term memory. We propose that interference between different passwords is one of the major challenges to multiple-password recall and that interference alleviation methods can significantly improve multiple-password recall. A lab experiment was conducted to examine the effectiveness of two interference alleviation methods: the list reduction method and the unique identifier method. While both methods improve multiple-password recall performance, the list reduction method leads to statistically significant improvement. The results demonstrate the potential merit of practices targeting multiple-password interference. By introducing long-term memory theory to multiple-password memorability issues, this study presents implications benefiting users and serves as the potential starting point for future research.
European Journal of Information Systems advance online publication,
31 March 2009; doi:10.1057/ejis.2009.9

Keywords: authentication; information security; memorability; memory theory; passwords

Introduction

Information security management has become one of the most pressing issues facing businesses in today's competitive information technology (IT)-driven world. User authentication serves as the first defense against security breaches. The prevailing authentication method involves the use of passwords which grant access only to authorized parties. It has been reported that 86% of U.S. companies use password authentication (InformationWeek, 2007) and, according to a Deloitte security survey (2007), 53% of surveyed organizations rely solely on password-based authentication for end-user Internet transactions. In the U.K., four-fifths of surveyed companies use passwords as the only authentication method (DTI survey, 2006). Since organizations widely adopt and heavily depend on password authentication methods, the issue of password management is of utmost importance.

In order to serve as an effective authentication method, passwords must be strong, secret, and memorable (Wiedenbeck *et al.*, 2005; Bellovin, 2006).

Received: 8 April 2008
Revised: 18 August 2008
2nd Revision: 31 January 2009
Accepted: 23 February 2009

'Strong' passwords are those that are difficult for others to guess; 'secret' passwords are hard for others to locate and obtain;
and 'memorable' passwords are those that users can easily remember. As a knowledge-based authentication mechanism, passwords depend on human memory. Yet, the increasing complexity and quantity of passwords make it nearly impossible for users to remember all of their passwords. Hence, users trade security for memorability. The effectiveness of password authentication can be jeopardized by end-users' mispractice, which is an inevitable consequence of human memory limitations.

Mispractice, including choosing weak passwords, writing passwords down, and using a common password for multiple accounts, has been widely reported in a variety of security surveys. User-created passwords are usually neither strong nor secret (Warkentin *et al*., 2004; Wiedenbeck *et al*., 2005; Vu *et al*., 2007). In fact, the top 10 passwords used on the Internet are all weak passwords (PC Magazine, 2007). When IT-enforced policies require users to choose strong passwords, users often write their passwords on a Post-it note stuck to the monitor, thereby compromising secrecy and defeating the purpose of having a password. Sixty-six percent of managers have observed employees writing passwords down on paper at work (RSA, 2006a). Furthermore, a recent Kaspersky security survey found that more than 50% of respondents use only one to four passwords, suggesting that password reuse is a common practice (PCPro, 2007). Users' mispractice is so common that passwords have become 'the weak link' in computer security.

The average employee must remember three different job-related user IDs and passwords. Some employees need to remember more than 10 passwords (DTI survey, 2006). In addition, they must recall many personal passwords for a variety of electronic systems including ATM machines, voice message systems, and websites. As the number of username/password pairs increase, the cognitive load creates 'access amnesia' resulting in confused or forgotten passwords. So many passwords are stored in human memory that they interfere with each other, and it is hard to separate one password from the others. Users are especially frustrated by the interference caused by having used a series of passwords for the same account. Requiring frequent password changes is a common security practice that contributes to interference. Massad & Beachboard (2008, p. 7) documented the frustration of one user who stated, 'because of the frequent password change requirements I was using the wrong password (had forgotten that I had changed it from my most commonly used password). My account locked up and I was not able to access it because of incorrect password [*sic*]'. According to the 2006 password management survey (RSA, 2006a), 39% of respondents in the Asia-Pacific region, 34% of users in Europe, and 23% of users in the U.S. are required to change their passwords on a monthly basis. However, these frequent password changes increase the burden on human memory and may encourage users to resort to writing down their passwords (Stanton *et al*., 2005).

Despite the drawbacks, passwords are likely to remain the dominant authentication technology (Wiedenbeck *et al*., 2005). While alternative authentication methods exist (e.g., public key encryption, one-time logon tokens, or biometric authentication), each would require widespread adoption of a variety of standards and hardware devices. Hence, the issues of reliability, privacy, and cost prevent these methods from being widely deployed. According to the 2007 Computer Security Institute (CSI) survey, only 18% of companies use biometric technologies and 35% use smart card/one-time tokens. On the other hand, 51% of companies use traditional password-based authentication. Furthermore, many other security-oriented technologies incorporate passwords to some extent, and, therefore, using them does not eliminate the issues related to memorability.

The interrelationship between text password security and memory theory has long been recognized. Previous studies relied on short-term memory theories and focused mainly on suggesting strong, yet easily recalled individual passwords (Smith, 2002; Carstens *et al*., 2004; Yan *et al*., 2004; Zviran & Erlich, 2006). However, improving the memorability of individual passwords helps only to a limited extent. In password practice, users are faced with multiple passwords. This poses different challenges from those of single-password management. No matter how easy passwords are to memorize, the real challenge is to memorize *and correctly match* numerous strong passwords to their corresponding accounts. Therefore, we believe a gap lies between password research and password practice.

In an effort to fill the void, this paper targets the multiple-password management crisis and treats it as a search-and-retrieval problem that involves humans' long-term memory. Cognitive psychology provides the theoretical foundation of this research. As the password problem is due to human memory limitations, it is appropriate to use memory theory to analyze the problem. While previous studies applied short-term memory theory to the individual password problem (Warkentin *et al*., 2004; Yan *et al*., 2004; Carstens *et al*., 2006), the uniqueness of the multiple-password problem and the application of long-term memory in password management have not been examined. Recognizing that the password problem is by nature a human memory problem, this study endeavors to examine the memory mechanism involved in recalling properly associated passwords. This research further explores memory issues related to password systems from a theoretical and experimental viewpoint. It breaks new ground by incorporating Atkinson & Shiffrin's (1968) Stage of Memory Theory (SMT) from applied psychology into password studies. We employ this classic theory to identify the distinction and connection between short-term and

long-term memory and to form the theoretical foundation for scientific investigation of long-term memory theory and password management. Based on the SMT and password-related literature, we contend that the interference among different passwords is one of the major challenges to multiple-password recall. As such, our research question is 'can interference alleviation mechanisms significantly improve multiple-password recall?' We propose two interference alleviation methods: the list reduction method and the unique identifier method. These were operationalized as the 'First Letter' treatment and the 'Password Rules' treatment, and an experiment was conducted to empirically evaluate their efficacy.

This research is the first attempt to apply a theoretical lens to the intriguing phenomenon of interference in multiple-password recall. The contribution of this paper is three-fold: first, it identifies multiple-password management (*vs* human memorability) as a separate aspect of the existing password predicament; second, it extends previous studies in the domain of theoretical application of memory in password problems from short-term memory theory to long-term memory theory; and third, it specifically investigates the efficacy of interference reducing techniques in improving password recall in multiple-password situations.

The remainder of this paper is organized as follows. A recap of the multiple-password problem and theoretical bases of the study are described next. The experiment section describes how data were collected, followed by data analysis and results. The details of the two suggested techniques are also explained in the experiment section. The paper concludes with a discussion of results, implications to academia and practice, limitations, and suggestions for future research.

Literature review

The multiple-password problem

Currently, the use of passwords is the most popular authentication method. Many organizations use passwords to secure computer systems, limit access to sensitive information, and safeguard remote or online transactions. More than 25% of end-users reported managing more than 13 passwords at work alone (RSA, 2005). In addition, many people also create passwords for other purposes such as personal finance, online shopping, gaming, and online communication. Users are advised to use unique passwords for different accounts, implement strong passwords, and change passwords from time to time. However, if end-users follow this advice, they will be required to memorize more passwords than human memory capacity permits.

A recent survey conducted by Kaspersky Lab (PCPro, 2007) found that 62% of users had up to 10 password-protected online accounts and 23% of users had more than 20 password-protected accounts. Password overload forces users to develop techniques to manage multiple passwords. Some rely on technological aids (e.g., removable storage devices, encrypted spreadsheets, or databases) as security vehicles to track their passwords. This, however, requires physical security measures and the fragility of the hardware creates a point of failure with potentially catastrophic consequences. Password reuse is another technique users employ. Fifty-one percent of users used common passwords for multiple accounts. Such behaviors raise security risks that could lead to identity theft. Hackers could obtain a password from a less secure application and use that password to access more sensitive accounts such as banking or shopping accounts. Hence, having multiple passwords decreases memorability and harms the password mechanism (Adams & Sasse, 1999; Ives *et al*., 2004).

Pure technical solutions are already in place. Enterprise single sign-on (ESSO) technology allows end-users to automatically logon to all authorized applications using a single user ID and password combination, thereby reducing the number of work-related passwords to remember. According to a Deloitte security survey (2007), 28% of organizations had already implemented single sign-on systems and 25% expected to implement it in the next 12 months, indicating wide adoption and growing acceptance of such technology. However, user control over each application, which sometimes functions at different levels, is traded for convenience. Furthermore, there is a tremendous potential for the misuse of data in malicious ways. If this single password is compromised, multiple applications are subject to unauthorized access and abuse. The potential loss is huge. On the other hand, ESSO in conjunction with a secondary authentication method, for example, smart cards, may offer enough security assurance while alleviating the password burden for work-related accounts. Yet, only 10% of companies that implemented ESSO adopted such strong authentication (RSA, 2006b).

In addition to work-related accounts, end-users also need to keep track of numerous personal accounts such as personal finance accounts, e-commerce accounts, communication accounts for email or instant messaging, gaming accounts, and social networking accounts. Various password management systems (PMSs) are available to deal with personal logon tasks, but each has limitations and disadvantages (Mulligan & Elbirt, 2005). Microsoft Internet Explorer and Mozilla Firefox both offer password storage mechanisms. Online account passwords are stored on local computers and can be automatically retrieved when users revisit the websites through that computer. Other software, such as PasswordSafe and KWallet, can be used to store multiple passwords on a local computer as an encrypted file, which in turn is protected by a master password. Users are only required to memorize that master password. However, PMSs are not a panacea. Current PMSs replace rather than facilitate human memory. Owing to the lack of repeated password entry, users are likely to forget their passwords when they need to login from a different computer.

Furthermore, PMSs do not increase security in the authentication process but rather increase user convenience. In actuality, PMSs simply move the point of failure to the single password on the local computer (Mulligan & Elbirt, 2005). Hence, users and organizations need to ensure that PMSs are both properly implemented and used, maintaining an awareness of risk factors that may be involved (PistolStar, 2006). In addition, users must overcome uncertainty and distrust in using the application to perform its role. If end-users forget the master password, they will be denied access to multiple applications. When the local computer is a laptop, accidental loss of the laptop may also put the stored passwords into the wrong hands. If attackers have access to either the master password or the encrypted password file, they could gain access to all the passwords. Also, the potential for a virus specifically targeting these systems may pose severe security problems (Mulligan & Elbirt, 2005). This risk can be substantial, considering the widespread and increasingly destructive impact of malware.

Another mechanism to alleviate the password recall problem is minimal-feedback hint systems (Lu & Twidale, 2003; Hertzum, 2004; Hertzum, 2006). Intended to jog users' memories, these systems offer users partial hints about their user IDs and passwords. However, such systems also rely on storing account information on local computers and therefore have similar drawbacks.

In terms of password design, the multiple-password problem is subject to the longstanding debate about password usability and security. The more secure the password mechanism is designed to be, the less usable it is. Strong and proactive password restrictions only make the password problem worse (Proctor *et al*., 2002) and enforcing password rules makes passwords more difficult to remember (Campbell *et al*., 2007). No amount of training or awareness can change the basic cognitive limitations which make it impossible for users to simultaneously accommodate the security recommendations of multiple systems. As the number of passwords increases, the password mechanism does not work due to these human memory limitations. Conklin *et al*. (2004) pointed out that, from the engineering point of view, software development focuses on a single password but ignores the scalability problem. Hence, they proposed that engineers should approach the password problem using a new mindset.

Users can remember only five unrelated passwords (Adams & Sasse, 1999). Hence, managing multiple accounts decreases password recall accuracy (Vu *et al*., 2007). Furthermore, multiple passwords become more problematic over time as people have more and more accounts (Gaw & Felten, 2006). With increasing numbers of passwords and accounts, association – relating a correct password to the wrong account – becomes a common type of password recall error. When using related passwords, users are frequently troubled by within-list interference and have difficulty in accurately recalling any specific one. These related passwords are often linked by some common element and only differ slightly, for example, password1, password2, password$, etc. (Adams & Sasse, 1999). Hence, it is easy to confuse the password for one account with those for other accounts. This memorization burden results in a trade-off between the ease of use and the effectiveness of password systems (Warkentin *et al*., 2004). Brown *et al*. (2004) surveyed 218 students and 22.5% of them experienced password mix-ups. RSA (2005) found that 90% of the respondents expressed frustration with multiple-password management. Despite the evidence of a multiple-password problem, no systematic approach to the solution in terms of human cognition and behaviors has been explored.

Previous studies have applied memory theories to individual password problems (Warkentin *et al*., 2004; Yan *et al*., 2004; Carstens *et al*., 2006), focusing primarily on short-term memory theories such as chunking theory (Miller, 1956; Simon, 1974). According to Simon (1974), information is not processed in single strands or discrete entities but as 'chunks' of similar or equivalent data. Furthermore, Bishop (1990) indicated that, for easier memorability, passwords should ideally be composed of chunks that have psychological significance to the passwords' creator. Several smaller chunks can then be grouped into fewer larger ones through semantic encoding. While passwords consisting of fewer 'chunks' may be easier to remember individually, they may not necessarily be easy to pair with their specific accounts. Such pairing information requires extra effort to index and memorize (Simon, 1974). Short-term memory theories are therefore not adequate to explain multiple-password recall problems. The unique challenge of multiple-password management calls for memory theories that target the storage and retrieval of multiple account-password pairs.

The stage of memory theory (SMT)

The multiple-password problem can be considered an information retrieval problem related to long-term memory. In order to answer the question of why passwords cannot be recalled accurately, we need to understand how they are stored in the long-term memory in the first place. When we turn to cognitive psychology for information transition and storage theories, we find an old, simple, yet popular multi-store theory: Atkinson & Shiffrin's (1968) SMT. This classic theory's approach to human memory is supported by psychological research (Davelaar *et al*., 2005; Talmi *et al*., 2005) and forms the foundation of this study.

SMT postulates that information is processed and stored at three stages (Figure 1). First, a stimulus-response pair, also called external input, enters the sensory register. This piece of input information is then either lost in a very short period of time or it enters the next stage – the short-term store. Information in auditory-verbal-linguistic format may stay in short-term

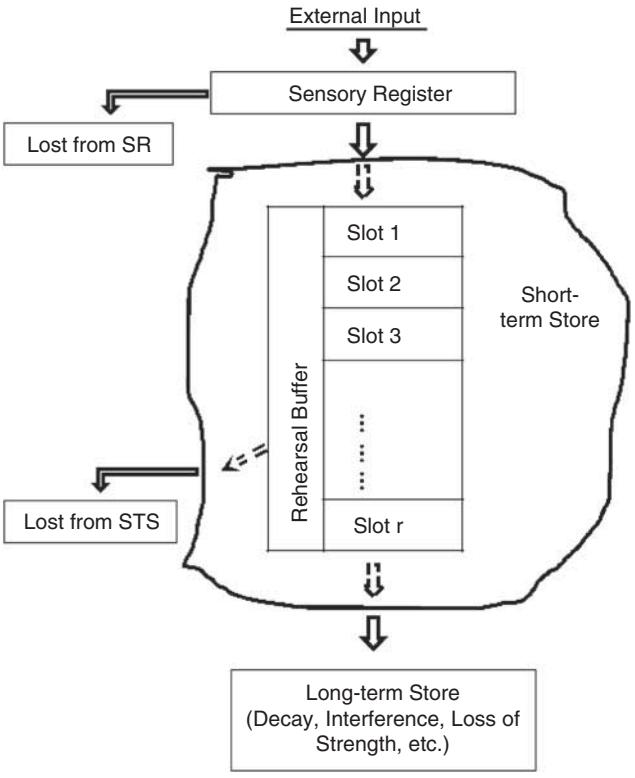

Figure 1 Human memory: a proposed system by Atkinson & Shiffrin (1968, p. 113).

store for about 15–30 s. The longer the information stays in the short-term store, the more likely that it enters long-term store and the stronger its trace in the long-term store. Trace measures the strength of information stored in the memory. Rehearsal, a control process, may prolong the stay of the input information and thereby make it more likely to enter the long-term store. Finally, the information is either lost or it enters the long-term store and becomes part of long-term memory. Decay, interference, and loss of trace strength all hinder the successful recall of the information that resides in the long-term memory. Interference is chiefly due to the intervention of similar information. In the multiple-password context, different account-password pairs interfere with each other, thereby making it difficult to accurately recall any specific account-password pair.

Atkinson & Shiffrin (1968) proposed that both search and retrieval are determined by the trace of the information. When the trace is strong and complete, related information is expected to be easier to locate and recall. The trace can be diminished by interference. Thus, search and retrieval processes can benefit from techniques that help avoid interference and thereby retain trace.

When we apply SMT to the multiple-password problem, we consider account-password pairs to be stimulus-response pairs that must be remembered. Since a user deliberately creates and memorizes passwords and their corresponding accounts, it is reasonable to conclude that these account-password pairs will eventually transfer from short-term store to long-term store and become part of long-term memory. Using SMT, we can investigate the storage, search, and retrieval process of these account-password pairs. We may also explore the interference effect among these account-password pairs. Finally, we can discover effective triggers for the recall of such account-password pairs.

Our research attempts to answer the question 'can interference alleviation mechanisms significantly improve multiple-password recall?' This study tests two possible methods to alleviate password interference. The first method is to help users limit their search to a specific password list. We do this by providing the user with the first letter of their password. This reduces their search to only their passwords beginning with that letter. This 'First Letter' hint was suggested as being effective by Norma Graham's experiment (as cited in Atkinson & Shiffrin, 1968, p. 120), in which the subjects were asked to recall the names of state capitals. The second method is to remind the user of the distinctive characteristics of the password. We do this by displaying the rules the user was required to follow in creating the password. Password rules usually specify characteristics of an acceptable password, for example, length, valid characters, required characters, or prohibited characters. These password format restrictions often force end-users to create unique passwords that are not particularly memorable to the user (Gaw & Felten, 2006). Such unique passwords distinguish themselves from other passwords due to the restrictions specified in the password creation rules. Since distinctiveness facilitates the retrieval of items from a search set in memory (Schmidt, 1991), we propose that the same password rules that compel the creation of unique passwords will assist users in recalling those passwords. An experiment was conducted to test the effectiveness of these two interference-reducing methods.

Experiment

The experiment was comprised of two stages: (1) multiple-password creation, and (2) multiple-password recall. In the first stage, the participants were asked to create unique passwords for four separate accounts: shopping, finance, communication, and travel. This number of accounts was chosen because users can only memorize up to four or five unrelated passwords (Adams & Sasse, 1999). One week later, Stage two was conducted. In this stage, the participants attempted to login to all four accounts using the passwords they had created the week before.

Participants

Ninety-three students from a university in the southern U.S. participated in the experiment for bonus points. Only students who participated in Stage one were permitted to participate in Stage two. Subjects were

students enrolled in introductory microcomputer applications courses. All of them used computers on a regular basis and had generated accounts with passwords before. In addition to any non-school-related accounts, each of them had at least four school or class-related accounts that required passwords.

Using student samples is appropriate for password studies. College students are frequent Internet users and active participants in online activities, most of which require creating password-protected accounts. It is reported that on average, college students have more than eight password-protected accounts (Brown *et al*., 2004; Riley, 2006). Furthermore, current password practices of college students are likely to be carried on into their future employment (Campbell *et al*., 2007). While this study, along with much previous password research (e.g., Proctor *et al*., 2002; Yan *et al*., 2004; Gaw & Felten, 2006; Vu *et al*., 2007), uses student samples, the results can be generalized to employee populations.

Stage one

The experiment was conducted in the classroom environment. The participants were directed to a webpage designed for this experiment. They were asked to generate unique passwords for four accounts: shopping, finance, communication, and travel. Because this research focuses solely on password recall, the students were instructed to create a common user name for all four accounts. By choosing the accounts from a drop-down list, they were able to create the four accounts in any order. Each password had to satisfy different specific password rules, most of which are common password rules found on popular websites (see Table 1). Students were instructed to create passwords that were easy for them to remember but hard for other people to guess. They were explicitly told not to write down the passwords and that they would need to login to those accounts in the future using the passwords created. During the experiment, their instructors walked around in the classrooms, proctored, and assisted the students in accessing the website.

Passwords for all accounts had to meet the minimum length requirement of eight characters. Another rule shared by all accounts was to 'use a password with the first two letters different from your other accounts'. This rule forced participants to create unique passwords for each account. All rules were enforced automatically using a JavaScript program. If an entered password did not meet the requirement, a pop-up window would display the rule(s) violated and instruct the user to re-enter a password.

Once an account was successfully created, the participant would see a confirmation page displaying the user name and password for that account on the screen. Figure 2 depicts an example of a confirmation page. A shopping account was created for demonstration. The user name was 'Testusername' and the password was

Table 1 Password rules

Account	*Password rules*
Shopping	1. Contain at least eight characters 2. Use at least one number (0–9) 3. Use at least one lower case letter (a–z) 4. Use at least one UPPER case letter (A–Z) 5. Use a password with the first two letters different from your other accounts
Finance	1. Contain at least eight characters 2. Use at least one number (0–9) 3. Use at least one letter (a–z, A–Z) 4. Use at least one special character from @ $ & # _- 5. Use a password with the first two letters different from your other accounts
Communication	1. Contain at least eight characters 2. Use both numbers and letters (0–9, a–z, A–Z) 3. Use a password with the first two letters different from your other accounts
Travel	1. Contain at least eight characters 2. Use at least one number (0–9) 3. Use at least one letter (a–z, A–Z) 4. Use at least one special punctuation mark from, ; ? ! 5. Use a password with the first two letters different from your other accounts

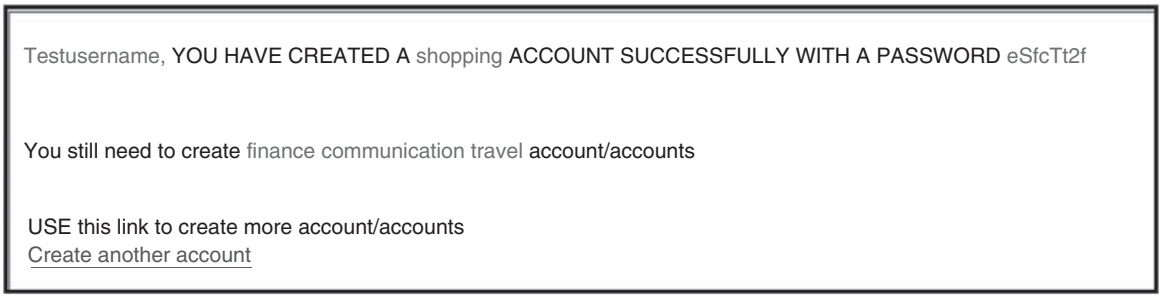

Figure 2 Confirmation page for account creation.

'eSfcTt2f'. All important information, including the account type and password, was highlighted in red to draw more attention. The participants were instructed to rehearse the password to help memorize it. The confirmation page also instructed the participants to continue creating other accounts. After all four accounts were created, a confirmation summary page displayed all four passwords along with the specific account to which each belonged. Participants were instructed to take the opportunity to rehearse more. The experiment was designed in this way because the focus of this study is password recall from long-term memory. Rehearsal is an effective method to help new passwords enter long-term memory (Atkinson & Shiffrin, 1968; Rundus, 1971) . Because it is uncommon for a user to create four accounts at one time, rehearsal was necessary in the current experimental design to avoid the loss of passwords in short-term memory.

Stage two

In this stage, only students who had completed Stage one were permitted to participate. At the beginning of Stage two, the participants were directed to a second website designed for this experiment. On the website, participants were asked to type in their user names. Without their knowledge, the participants were randomly assigned to three groups, including one control group and two treatment groups. After entering the username, the subject was automatically directed to one of three login screens according to the assigned group.

If a participant was assigned to the control group, he/she would see a typical login page with a textbox to enter the password. However, the screens displayed for participants in the treatment groups contained supplemental information about their passwords. In the so-called 'First Letter' treatment group, the login screen displayed the first letter of the password for the account selected. In the so-called 'Password Rules' group, the login screen displayed the password rules applied to the account selected.

Participants could choose any of the four accounts from a drop-down list and thereby login to their accounts in any order. They were instructed to attempt to login as many times as they might do with real accounts, subject to a time limit of 10 min for the four accounts. Setting unlimited attempts for login can prevent preempting memory search, thereby allowing login behaviors to be examined more thoroughly.

Apparatus

For this experiment, software was developed for account creation and login. Java server pages (JSP) and an Oracle database residing on an Apache Tomcat server were used for development. HTML was used for designing all the experiment web pages. JavaScript was used for validation and processing. When the subjects created their accounts, the passwords for each account were stored in the Oracle database. When participants attempted to login to their created accounts, the number of login attempts and information about successful or unsuccessful attempts were tracked by the software. The passwords typed in, whether correct or not, were also recorded.

Data analysis and results

In total, 70 students participated in both stages. Fifty-nine students successfully created all four accounts and attempted to login to all of them. Demographic information of these participants is reported in Table 2. Among the 59 students, 22 were assigned to the control group, 21 were assigned to the 'First Letter' group, and 16 were assigned to the 'Password Rules' group. Eleven students either failed to create or failed to attempt login for all four accounts and therefore were excluded from the data analysis due to missing data.

All participants were required to recall four unique passwords. Participants in the 'First Letter' group demonstrated the best recall performance ($M = 3.3$, SD = 1.1), followed by the 'Password Rules' group ($M = 2.9$, SD = 1.3). Participants in the control group displayed the lowest mean recall rate ($M = 1.8$, SD = 1.7). A one-way ANOVA, with group (control group, 'First Letter' group, and 'Password Rules' group) as the independent variable, was conducted on the performance measure: mean successful recall rate. The effect of interference alleviation methods was significant with $F(2, 56) = 7.115$ and $P < 0.01$ (Table 3). Power analysis was carried out to examine the reliability of the ANOVA result. Assuming a large effect size (Cohen's $f = 0.4$), Cohen's power table (1988) shows a power of 0.78, given alpha = 0.05 and a pooled sample size of 20, which is equal to the average sample size of the three groups. While the power is an increasing function of effect size, a small change in the estimated effect size will change the power remarkably. In this study, the observed effect size is substantially large (Cohen's $f = 0.45$), indicating the ANOVA test is sufficiently powerful.

Table 2 Demographic data

Gender		*Race*		*Class status*	
Male	27	White	36	Undergraduate	48
Female	28	Black	19	Graduate	3
Non-reported	4	Non-reported	4	Other	4
				Non-reported	4

Table 3 ANOVA results for successful recall rates

	Sum of squares	*d.f.*	*Mean square*	*F-ratio*	*Sig.*
Between groups	27.516	2	13.758	7.115	0.002
Within groups	108.280	56	1.934		
Total	135.797	58			

Table 4 *Post hoc* **pairwise comparisons (Based on Games-Howell comparisons)**

Comparison	*Mean difference (Sig.)*
'First Letter' *vs* Control group	1.5606 ($P=0.002$)
'Password Rules' *vs* Control group	1.1023 ($P=0.071$)
'First Letter' *vs* 'Password Rules' group	0.4583 ($P=0.507$)

Since ANOVA F is significant, we conducted *post hoc* analysis to examine which group means are different from the others. A summary of the result is presented in Table 4. For multiple comparisons, the Bonferroni adjustment (Abdi, 2007) on the significance level was applied to increase the rigor of each individual comparison. To obtain an overall significance level of 0.05, the Bonferroni adjusted level of significance is 0.0167. The average successful recall rates in both treatment groups are higher than the control group. However, the difference is only statistically significant for the 'First Letter' group ($P<0.0167$). The result offers evidence of the effectiveness of the 'First Letter' treatment. The effectiveness of the 'Password Rules' method is still subject to further investigation. With a larger sample, the mean difference between the 'Password Rules' group and the control group may be statistically significant.

On the account creation page, the four accounts were offered as a drop-down list with a default order of shopping, finance, communication, and travel. Users could create accounts in any order by selecting the corresponding account. While most users followed the default order, some did not. The order of password creation may have had a confounding effect on the complexity and memorability of the passwords created. Since the experiment required the subjects to create four completely unique passwords, the last password tended to be more complex and difficult to memorize. Owing to the random assignment of participants to the three experimental groups, order effect, if any exists, is expected to affect all groups equally and lead to limited impact on the results, which are based on the comparison of group means. For more rigorous analysis addressing this issue, we conducted a complementary experiment to test whether the order of password creation has an impact on recall performance.

In this new round of the experiment, the accounts on the password creation page were randomized. All other settings were the same as in the original experiment. Another cohort of students was recruited from the same university. While nearly 90 students participated in Stage one of this complementary study, only 76 of them also completed Stage two. In the end, 49 usable data points were obtained. The recall performance in this complementary experiment ($M=2.12$, $SD=1.54$) was compared with that of the original experiment ($M=2.63$, $SD=1.53$). There was no significant difference ($t(106)=1.703$, $P>0.05$), indicating that the order of password creation has no significant impact on recall performance. Hence, the complementary experiment provided further evidence that our findings are valid, despite the possible order effect.

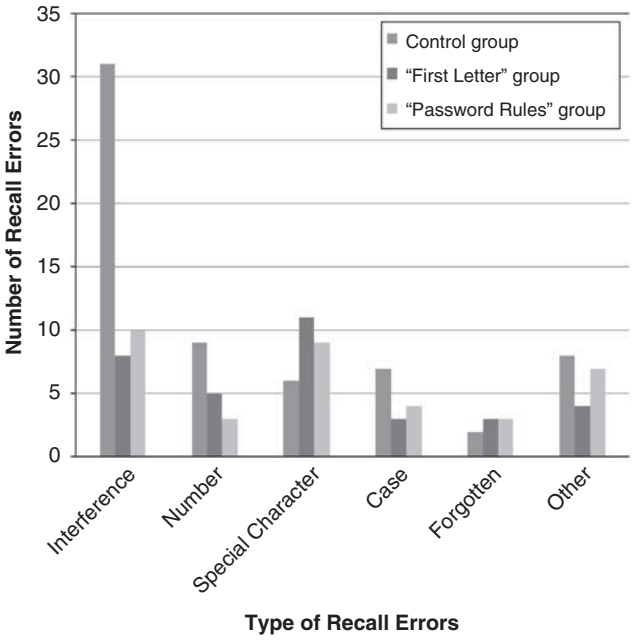

Figure 3 Password recall errors.

Discussion and conclusion

Reasons for recall errors

Since all the entered passwords were recorded, we were able to examine the types of errors the subjects made in recalling their passwords. As reported in Figure 3, the major types of errors include interference errors, number requirement errors, special character requirement errors, case errors, and forgotten passwords. The categorized error counts confirm that interference is the major reason for multiple-password recall errors, and the two treatments do help reduce the interference effect.

Errors were classified as interference errors if a partial or complete password associated with a different account was recalled instead of the correct password. The control group, without any interference alleviation mechanism, displayed the most frequent occurrences (31 occurrences) of interference errors. Both the 'First Letter' group and the 'Password Rules' group displayed fewer interference errors compared to the control group. In the 'First Letter' group, interference occurred eight times, but further investigation indicated that six out of the eight occurrences were due to common first-letter passwords. In these cases, users had multiple passwords with the same first letter. This happened because (1) although, according to the enforced password rules, the first two letters of their passwords must be different from each other, users were permitted to use the same first letter for all

their passwords if they used a different second letter; and (2) users did not know in advance that they would be provided the first letter of their passwords. Without this knowledge, they did not create their passwords in a way that would take advantage of the extra help during login. In these cases, the interference alleviation mechanism may not have been effective because it may not have reduced the search list.

Numbers and special characters are also major reasons for recall failure. Common mistakes include omitting number(s), adding extra number(s), omitting or adding special character(s), and using the wrong special character(s). This observation is consistent with previous research that suggests it is hard to integrate numbers and special characters into meaningful passwords (Warkentin *et al.*, 2004). While using the wrong case (uppercase/lowercase), completely forgetting the passwords, and several other errors are observed, none of them are as predominant as the previously listed types.

Implications for research

As stated by Dennis & Valacich (2001), the best research designs tend to openly accept their flaws and aggressively play to their strengths. The goal of our study was to isolate the function of accessing and retrieving information from long-term memory in order to observe the impact of interference reducing techniques. This isolation required the precision and control of the experimental methodology. Our methodological approach diverges from other quantitative studies because we were interested in gaining the precision, which is the *raison d'être* of experimental research (Dennis & Valacich, 2001), that would allow us to effectively conduct these experiments in a controlled environment. Our contrived settings were successfully established with this precision to allow us to test and extend long-term memory theory (i.e., SMT) in the new domain of multiple-password management.

While the primary strength of experimental research is precision and control, they are gained at the expense of realism and generalizability. We do not suggest that the treatments used in this study should necessarily be applied in practice. They are artifices that we have used to observe the cognitive process. We believe that the empirical evidence from this experimental research is of interest and relevant to the IS community at large in that understanding how users recall passwords can help us develop more effective password mechanisms and thereby reduce user mispractice associated with the multiple-password problem.

To the best of our knowledge, this research may be the first theory-based empirical research targeting the multiple-password problem. While previous research has suggested methods to address the individual password problem, those methods may not be adequate to assist in multiple-password recall. In the multiple-password context, easy-to-remember passwords are not necessary easy to recall. For example, it was observed in the experiment that one participant used '@1password' as the finance account password. As an individual password with only three chunks, '@' + '1' + 'password' is easy to remember. However, when the participant tried to login to the corresponding account, the recorded attempts showed that he/she tried passwords related to other accounts but did not even relate the word 'password' to his/her accounts. Other similar observations show that multiple-password management involves unique obstacles and more challenges than individual password management. Thus, this phenomenon calls for new views and theoretical exploration.

This research serves as an innovative starting point to apply long-term memory theory to multiple-password research. Based on the SMT, we proposed that interference alleviation methods may be effective in improving multiple-password recall. Experimental results provide statistical evidence to support this proposition. There is a rich body of literature that examines effective methods of improving single-password recall (Warkentin *et al.*, 2004; Yan *et al.*, 2004; Carstens *et al.*, 2006). The findings of this research can be integrated with those of previous studies to help extend the domain. Interference alleviation methods can be used to help separate a password for a specific account from other passwords, at which point methods improving single-password recall can come into play. Combining interference alleviation methods with existing single-password creation and recall methods, end-users are more likely to accurately recall the requested password.

Implications for practice

Interference is one of the major reasons for multiple-password recall errors. The results of this study demonstrate the effectiveness of interference alleviation methods in improving multiple-password recall. The implications for practice are two-fold: for end-users and for IT professionals. For end-users, improving multiple-password memorability and recall is the key. This study supports the effectiveness of finding ways to reduce interference by limiting the search list or by identifying unique characteristics of the correct password when recalling the password. One way is suggested by the treatment used in the 'First Letter' group. End-users might construct their passwords in a manner in which the first letter of the password is easily associated with its corresponding account and thereby more easily recalled. For example, they might relate the first letter to the website URL. A password starting with 'y' could be used for a Yahoo email account, a password starting with a 'g' for a Google account, etc. A similar approach has been suggested by Craig Busse as cited in Gehringer (2002). Alternately, users might relate the first letter to the type of accounts. For example, they might use passwords starting with 'e' for all email accounts, 'b' for all bill-paying accounts, etc. Each user could build his or her own secret 'First Letter' password pattern. Once the first letter is accurately recalled, the interference effect is

significantly reduced. However, this method of alleviating interference would not be restricted to techniques involving the first letter. Any password construction system that helps the user easily reject passwords for other accounts and thereby reduce the number of passwords that might be the correct password will improve recall.

For IT professionals, supporting multiple-password recall is the key. Upon acknowledging the fact that end-users have difficulty dealing with multiple passwords, IT professionals should take the initiative to facilitate multiple-password recall. Between the user ID and password input, another logon layer that carries some password-related information may be necessary. IT professionals may want to experiment with various vehicles that can serve as such a layer. For example, displaying a user-selected picture upon input of user ID, a practice already in place for anti-phishing purposes, could serve a dual function. These images could serve as an inconspicuous prompt to users to remind them of their password. Users could select images embedded with password-related information and use it as a vehicle to identify the password for that specific account. For example, an image of an office might remind the user that his password includes his office number. An image of a book might remind the user that the password contains her favorite author's initials. Hence, even though the hint is displayed, it is only meaningful to the user.

Limitations and directions for future research

Benbasat (1984) stated that research on Information Systems can be carried out in a wide range of settings and by a variety of strategies. There is no perfect research because different strategies carry comparative strengths and weaknesses (Dennis & Valacich, 2001). This research is no exception as it suffers from several limitations.

First, laboratory experimentation, by its nature, tends to limit the external validity of its results. According to McGrath's (1982) argument in respect to research dilemmas in three dimensions, we are aware that, as our objective is to gain precision and control in the artificial settings, there is a corresponding loss of generalizability and realism. As such, these experiments were conducted in contrived settings with carefully constructed tasks that may not match everyday experience. For example, in order to observe multiple-password creation and recall performance, the experiment designed for this research required participants to create four passwords under different password rules in the same session. While all four passwords were created at the same time and were recalled one week later without any login in between, this design helped control for the confounding effect of the life span and recall frequency of the passwords. However, realism is sacrificed for control. In real practice, the average end-user has many password-protected accounts that are created at different times with different login frequency. Under these conditions, the interference effect is much more complicated than in the laboratory setting. Many factors may influence recall performance. For example, passwords recalled more frequently tend to be recalled correctly because performance in a memory task improves with repetition of the material (Raaijmakers, 2003). Future research may attempt to improve generalizability of the results from the laboratory setting by replicating this study in field settings which are embedded with richer realism and provide a deeper understanding of the participants involved. Existing accounts, rather than experimentally created accounts, could be used to test recall performances. We may further investigate how quantity, life span, and recall frequency of those passwords impact interference level and recall performance.

Despite all the careful deliberations in the experimental design and construction, the experimental interface is not without flaw. In the account creation page, the four accounts were offered as a drop-down list in the default order of shopping, finance, communication, and travel. Users could create accounts in any order by clicking on the corresponding account. However, many used the default order. The order of password creation may have had a confounding effect on the complexity and memorability of the passwords created. Future research is suggested to more carefully look into the order effect.

Another limitation is that this study was conducted with a small sample. In this study, a participant had to create all four accounts at the first stage and attempt to login to all of them at the second stage to be included in the data analysis. Owing to the two-stage nature of the experiment and zero tolerance of missing data, the sample size is much smaller than ideal. While we conducted power analysis to ensure that the statistical tests had enough power despite the small sample, a more definite result may be obtained regarding the 'Password Rules' method. In future research, a larger sample should be obtained to examine the 'Password Rules' method and other potential interference alleviation methods.

This study provides a new perspective for future research in the password management area. By recognizing the uniqueness of the multiple-password recall problem, a better understanding of the recall failures can be developed. By introducing the multi-store memory theory SMT, this study bridges the research gap and further extends current studies, which mainly examine the relationship between individual-password management and short-term memory theories, to investigate the relationship between multiple-password management and long-term memory theories. While only two interference alleviation methods were examined in this study, the opportunity to discover other potential methods appears to be very promising.

Despite the innovative improvements made in the arena of authentication, text passwords continue to be the predominant authentication method. Although other methods have been proposed (e.g., graphical, passphrase, biometric), they have less usability (Proctor

et al., 2000) and their effectiveness has yet to be tested (Cranor & Garfinkel, 2004). Although human beings may inevitably encounter password loss due to memory limitations, we believe that, upon successful implementation of interference alleviation methods, end-users may improve their ability to manage numerous passwords.

About the authors

Jie Zhang is an assistant professor in the Department of Computer Information Systems at Virginia State University, U.S.A. She received her Ph.D. degree in Management Information Systems from the University of Mississippi. Her research interests include behavioral information security, privacy, and SMEs information systems management. She can be reached at jzhang@vsu.edu.

Xin Luo is an assistant professor of Management Information Systems and Information Assurance in Robert O. Anderson School of Management at The University of New Mexico, U.S.A. He is the Associate Director of Center for Information Assurance Research and Education at UNM. He received his Ph.D. in Information Systems from Mississippi State University. His research interests center around information security, E-commerce/M-commerce, and global IT adoption and management. He has published research papers in journals including *Communications of the ACM*, *Journal of the AIS*, *Communications of the AIS*, *Journal of Organizational and End User Computing*, *Cross-Cultural Management: An International Journal*, *Information Management & Computer Security*, *Journal of Information Privacy and Security*, *International Journal of Information Security & Privacy*, *Information Systems Security*, and *Journal of Internet Banking and Commerce*, etc. He can be reached at Luo@mgt.unm.edu.

Somasheker Akkaladevi is an assistant professor of Computer Information Systems at Virginia State University, U.S.A. He received his Ph.D. in Computer Science from Georgia State University. His research interests include Artificial Intelligence, Bio-Informatics, Computer Networks, Computer Architecture, Algorithms, Parallel and Distributed Computing. He has published research papers in journals and conferences including *The Journal of Cluster Computing*, *International Journal of Foundations of Computer Science*, *Soft Computing*, *21st IEEE International Parallel & Distributed Processing Symposium*, *Second International Conference on Neural Networks and Brain*, *IEEE International Midwest Symposium on Circuits and System*, *26th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, and *The Sixth IEEE International Workshop on Nature Inspired Distributed Computing*, etc. He can be reached at sakkaladevi@vsu.edu.

Jennifer Ziegelmayer is an Instructor of Computer Information Systems at Delta State University and a doctoral candidate at The University of Mississippi. Her research interests focus on IT personnel issues including counterproductivity, organizational citizenship behavior, and accountability. In addition, she studies information security, privacy, and the use of social networking applications. Her research has been published in journals including *the Journal of Computer Information Systems* and *Information Systems Frontiers*. She can be reached at jziegelmayer@deltastate.edu.

References

ABDI H (2007) Bonferroni and Sidak corrections for multiple comparisons. In *Encyclopedia of Measurement and Statistics* (SALKIND NJ, Ed), pp 103–107, Sage, Thousand Oaks, CA.

ADAMS A and SASSE MA (1999) Users are not the enemy. *Communications of the ACM* **42(12),** 41–46.

ATKINSON RC and SHIFFRIN RM (1968) Human memory: a proposed system and its control processes. In *The Psychology of Learning and Motivation* (SPENCE KW and SPENCE JT, Eds), pp 89–195, Academic Press, New York.

BELLOVIN S (2006) Unconventional wisdom. *IEEE Security & Privacy* **4(1),** 88.

BENBASAT I (1984) An analysis of research methodologies. In *The Information Systems Research Challenge* (MCFARLAND FW, Ed), pp 47–85, HBS Press, Boston.

BISHOP M (1990) A proactive password checker. Technical Report PCS-TR90-152. [WWW document] http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/19920018383_1992018383.pdf.

BROWN AS, BRACKEN E, ZOCCOLI S and DOUGLAS K (2004) Generating and remembering passwords. *Applied Cognitive Psychology* **18(6),** 641–651.

CAMPBELL J, KLEEMAN D and MA W (2007) The good and not so good of enforcing password composition rules. *Information Systems Security* **16(1),** 2–8.

CARSTENS DS, MALONE LC and MCCAULEY-BELL P (2006) Applying chunking theory in organizational password guidelines. *Journal of Information, Information Technology, and Organizations* **1,** 97–113.

CARSTENS DS, MCCAULEY-BELL PR, MALONE LC and DEMARA RF (2004) Evaluation of the human impact of password authentication practices on information security. *Information Science Journal* **7(1),** 67–85.

COHEN J (1988) *Statistical Power Analysis for the Behavioral Sciences* 2nd edn, Lawrence Erlbaum Associations, New Jersey.

CONKLIN A, DIETRICH G and WALZ D (2004) Password-based authentication: a system perspective. In *Proceedings of the 37th Hawaii International Conference on System Sciences*, IEEE Computer Society, Washington, DC.

CRANOR LF and GARFINKEL S (2004) Secure or usable? *IEEE Security & Privacy* **2(5),** 16–18.

CSI (2007) The 12th annual computer crime and security survey. [WWW document] http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf.

DAVELAAR EJ, GOSHEN-GOTTSTEIN Y, ASHKENAZI A, HAARMANN HJ and USHER M (2005) The demise of short-term memory revisited: empirical and computational investigations of recency effects. *Psychological Review* **112(1),** 3–42.

DELOITTE (2007) The 2007 technology, media, and telecommunications security survey. [WWW document] http://www.deloitte.com/dtt/cda/doc/content/dtt_tmt_securitysurvey2007.pdf.

DENNIS A and VALACICH J (2001) Conducting research in information systems. *Communications of the AIS* **7(5),** 1–41.

DTI SURVEY (2006) DTI information security breaches survey. [WWW document] http://www.pwc.co.uk/pdf/pwc_dti-fullsurveyresults06.pdf.

GAW S and FELTEN EW (2006) Password management strategies for online accounts. In *Proceedings of the 2nd Symposium on Usable Privacy and Security*, pp 44–55, ACM Press, New York, USA.

GEHRINGER EF (2002) Choosing passwords: security and human factors. In *Proceedings of 2002 International Symposium on Technology and Society*, (HERKERT JR, Ed) pp 369–373, IEEE Computer Society, Washington, DC.

HERTZUM M (2004) Remembering multiple passwords by way of minimal-feedback hints: replication and further analysis. In *Proceedings of the Fourth Danish Human-Computer Interaction Research Symposium*, (KJELDSKOV J, SKOV MB and STAGE J, Eds) pp 21–24, Aalborg University, Aalborg, Denmark.

HERTZUM M (2006) Minimal-feedback hints for remembering passwords. *Interactions* **13(3),** 38–40.

INFORMATIONWEEK (2007) 2007 InformationWeek/Accenture Global Information Security Survey. [WWW document] http://www.informationweek.com/whitepaper/Security/ Privacy/2007-informationweek/accenture-global-information-wp1213826038953?articleID = 21800009.

IVES B, WALSH KR and SCHNEIDER H (2004) The domino effect of password reuse. *Communications of the ACM* **47(4),** 75–78.

LU B and TWIDALE MB (2003) Managing multiple passwords and multiple logins: MiFA minimal-feedback hints for remote authentication. In *Proceedings of the IFIP INTERACT Conference*, (RAUTERBERG M, MENOZZI, M and WESSON J, Eds) pp 821–824, IOS Press, Zurich.

MASSAD N and BEACHBOARD J (2008) A taxonomy of service failures in electronic retailing. In *Proceedings of the 41st Hawaii International Conference on System Sciences*, IEEE Computer Society, Washington, DC.

MCGRATH JE (1982) Dilemmatics: the study of research choices and dilemmas. In *Judgment Calls in Research* (MCGRATH JE, MARTIN J and KULKA RA, Eds), pp 69–102, Sage, Beverly Hills, CA.

MILLER GA (1956) The magical number seven, plus or minus two: some limits on our capacity for processing information. *Psychological Review* **63**, 81–97.

MULLIGAN J and ELBIRT AJ (2005) Desktop security and usability trade-offs: an evaluation of password management systems. *Information Systems Security* **14(2),** 10–19.

PC MAGAZINE (2007) 10 most common passwords. [WWW document] http://www.pcmag.com/article2/0,2817,2113976,00.asp, 8 May.

PCPRO (2007) Password reuse opens door to ID theft. [WWW document] http://www.pcpro.co.uk/news/106758/password-reuse-opens-door-to-id-theft.html.

PISTOLSTAR (2006) The myths and realities of domino R6/7 password management. [WWW document] http://managingautomation.bitpipe.com/detail/RES/1213377135_517.html.

PROCTOR RW, LIEN MC, SALVENDY G and SCHULTZ EE (2000) A task analysis of usability in third-party authentication. *Information Security Bulletin* **5(3),** 49–56.

PROCTOR RW, LIEN MC, VU Kpl, SCHULTZ EE and SALVENDY G (2002) Improving computer security for authentication of users: influence of proactive password restrictions. *Behavior Research Methods, Instruments, & Computers* **34(2),** 163–169.

RAAIJMAKERS J (2003) Spacing and repetition effects in human memory: application of the SAM model. *Cognitive Science: A Multidisciplinary Journal* **27(3),** 431–452.

RILEY S (2006) Password security: what users know and what they actually do. *Usability News* **8(1)**. [WWW document] http://psychology.wichita.edu/surl/usabilitynews/81/Passwords.asp.

RSA (2005) RSA security survey reveals multiple passwords creating security risks and end user frustration. [WWW document] http://www.rsa.com/press_release.aspx?id = 6095.

RSA (2006a) RSA security research shows volume of business passwords overwhelming end users and hindering IT security efforts. [WWW document] http://www.rsa.com/press_release.aspx?id = 7296.

RSA (2006b) Enterprise single sign-on solutions reduce IT helpdesk calls but raise concern amongst security experts, reveals RSA security. [WWW document] http://www.rsa.com/press_release.aspx?id = 6903.

RUNDUS DJ (1971) Analysis of rehearsal processes in free recall. *Journal of Experimental Psychology* **89(1),** 63–77.

SCHMIDT SR (1991) Can we have a distinctive theory of memory? *Memory & Cognition* **19(6),** 523–542.

SIMON HA (1974), How big is a chunk? *Science* **183(4124),** 482–488.

SMITH RE (2002) *Authentication: From Passwords to Public Keys*. Addison-Wesley, Boston, MA.

STANTON JM, STAM KR, MASTRANGELO P and JOLTON J (2005) Analysis of end user security behaviors. *Computers & Security* **24**, 124–133.

TALMI D, GRADY C, GOSHEN-GOTTSTEIN Y and MOSCOVITCH M (2005) Neuroimaging the serial position curve: a test of single-store versus dual-store models. *Psychological Science* **16(9),** 716–723.

VU Kpl, PROCTOR RW, BHARGAV-SPANTZEL A, TAI Blb, COOK J and SCHULTZ EE (2007) Improving password security and memorability to protect personal and organizational information. *International Journal of Human-Computer Studies* **65**, 744–757.

WARKENTIN M, DAVIS K and BEKKERING E (2004) Introducing the check-off password systems (COPS): an advancement in user authentication methods and information security. *Journal of Organizational and End User Computing* **16(3),** 41–58.

WIEDENBECK S, WATERS J, BIRGET JC, BRODSKIY A and MEMON N (2005) Passpoints: design and longitudinal evaluation of a graphical password system. *International Journal of Human-Computer Studies* **63**, 102–127.

YAN J, BLACKWELL A, ANDERSON R and GRANT A (2004) Password memorability and security: empirical results. *IEEE Security & Privacy* **2(5),** 25–31.

ZVIRAN M and ERLICH Z (2006) Identification and authentication: technology and implementation issues. *Communications of the Association for Information Systems* **17(1),** 90–105.