Journal of Information, Information Technology, and Organizations Volume 1, 2006

Applying Chunking Theory in Organizational Password Guidelines

Deborah S. Carstens
Florida Institute of Technology, Melbourne, FL, USA

carstens@fit.edu

Linda C. Malone and Pamela McCauley-Bell
University of Central Florida, Orlando, FL, USA

lmalone@mail.ucf.edu; mcbell@mail.ucf.edu

Abstract

This research evaluates the human impact that password authentication issues have on the security of information systems within organizations. This research resulted in the creation of password guidelines for authentication with passwords based on Miller's (1956) and Cowan's (2001) chunking theory research and a model for predicting the vulnerability that a particular set of conditions have on the likelihood of error in an information system. The findings indicate that human error associated with password authentication can be significantly reduced through the use of passwords that are composed of meaningful data for the user and that meet technical requirements for strong passwords.

Keywords: Chunking Theory, Human Error, Human Factors, Information Security, Information Technology, Passwords

Introduction

With the increasing daily reliance on electronic transactions, it is essential to have reliable security systems for individuals, businesses, and organizations to protect their information (Vu, Bhargav & Proctor, 2003; Vu, Tai, Bhargav, Schultz & Proctor, 2004). Computer security is largely dependent on the use of passwords to authenticate users of technology (Wiedenbeck, Waters, Birget, Brodskiy & Memon, 2005). However, users are challenged to remember long and random passwords and therefore too often choose passwords that may have low security strength or be difficult to remember (Wiedenbeck et al., 2005; Yan, Blackwell, Anderson & Grant, 2004). As the number of individuals using computers and networks has increased, so has the level of threat for security breaches against these computers and networks. Carnegie Mellon's Computer Emergency Response Team (CERT) (2006) has collected statistics showing that 6 security incidents were reported in 1988 compared to 137, 529 in 2003. Furthermore, CERT (2006) reported that 171 vulnerabilities were reported in 1995 in comparison to 5,990 in 2005 and already 3,997 in the first and second quarter of 2006. In addition, the Federal Bureau of Investigation (FBI) conducted a survey in which 40% of organizations

Accepting Associate Editor: Christopher Lueg

claimed that system penetrations from outside their organization had increased from the prior year by 25% (Ives, Walsh, & Schneider, 2004).

The rapid expansion in computing and networking has thus amplified the need to perpetually manage information security within an organization. Events such as 9/11 and the war on terrorism have also underscored an increased need for vigilance regarding information security. Organizations, government, and private industry are currently trying to adjust to the burden of this heightened need for information security, and, as an example of this, the U.S. Department of Homeland Security (2002) has focused particular efforts on ensuring information security. In light of the current context of universal computing and the realistic threats that exist to organizations' information systems, there is a strong need for more research in the field of information security.

In this world of ever increasing technological advances, users of technology are at risk for developing information overload as the number and complexity of passwords and other electronic identifiers increase. Previous investigations of the National Institute of Standards and Technology (NIST, 1992) have suggested that over 50% of incidents that occur within government and private organizations have been connected to human errors. The role that people play in maintaining information security is an important one that the literature has only begun to address. As researchers improve their understanding of how human factors limitations affect information security, they can provide organizations with insight into improving information security policies. Passwords adopted by users are too easily cracked (Proctor, Lien, Vu, Schultz & Salvendy, 2002). In particular, organizations can benefit from research revealing how best to minimize the demands that passwords place on the human memory system while maintaining the strength of a password (Carstens, McCauley-Bell, Malone, & DeMara, 2004).

The application of human factors and specifically cognitive theory principles can be used to positively influence system security when organizations follow password guidelines that do not exceed human memory limitations. Ultimately, user memory overload can be minimized when all aspects of a password authentication system have been designed in a way that capitalizes on the way the human mind works and also recognizes its limitations. As Hensley (1999) wrote, "Password(s) do little good if no one remembers them." Nevertheless, the exponential growth in vulnerabilities and security incidents as suggested by the CERT (2006) underscores that the design of password guidelines should be part of a comprehensive approach that still maintains strength of passwords as necessitated by the information technology (IT) community.

Because the impact of human error on information security is an important issue that left unresolved can have adverse effects on industry, the research presented focuses on (a) measuring the impact of password demands on the success of password authentication and (b) mitigating the risks that result when these demands exceed human capabilities. The research adds value to information security literature through testing the usefulness of chunking theory in the application of password development. The research presented is an expansion of preliminary research efforts conducted by Carstens and colleagues (2004) which statistically corroborates some of the preliminary findings.

Literature Review

Information Security

Ensuring effective information security involves making information accessible to those who need the information while maintaining the confidentiality and integrity of that material. There are three categories used to classify information security risks: (a) confidentiality, (b) integrity, and (c) accessibility or availability of information (U.S. Department of Homeland Security, 2002). A security breach in *confidentiality* can be defined as occurring when sources not intended to have knowledge of the information have been provided with this knowledge. Sending sensitive data to the wrong person is an example of this category. A security breach in *integrity* is an incident where there is an unauthorized or incorrect change made to an information source, such as a financial accounting error that causes the information in the database to be inaccurate. A security breach in *accessibility* occurs when either access for those entitled to a system is denied or access is given to those who are not authorized to access the system. An example of this category would be an authorized user of a system who is unable to access a system due to forgetting his or her password. Given the above definitions, a *human-error security incident* is defined as any human-error-related event that compromises information's confidentiality, integrity, or accessibility (Carstens et al., 2004).

Human Error in Information Security

Research has indicated that human error makes up as much as 65% of incidents that cause economic loss for a company and that security incidents caused by external threats such as computer hackers happen only 3% or less of the time (Lewis, 2003; McCauley-Bell & Crumpton, 1998; NIST, 1992). However, there is only a minimal effort to address the human error risks in information security, which is among the highest cause of information security incidents (McCauley-Bell & Crumpton, 1998; Wood & Banks, 1993). A common challenge faced by individuals today is the need to simultaneously maintain passwords for many different systems in their work, school, and personal lives. Research conducted by Wiedenbeck et al. (2005) suggests that stringent rules for passwords lead to poor password practices that compromise overall security. Human limitations can compromise password security because users are unable to remember passwords and therefore keep insecure records of their passwords such as writing a password down on paper (Yan et al., 2004).

Preliminary research conducted in the area of the human impact on information security indicated that 37% of survey participants never change their work and/or school passwords and that 69% of survey participants never change their personal passwords (Carstens et al., 2004). The same research indicated that when prompted to replace a current password, 43% of survey participants changed their work and/or school passwords back to a password they had used in the past; 33% of survey participants indicated changing their personal passwords back to an old password as well. The survey research suggests that with the IT community stressing the importance of using secure passwords, not writing passwords on paper, changing passwords often, and using different passwords for all systems, a person may compromise the strength of their password due to human information processing limitations. Proctor et al. (2002) performed experiments testing passwords between five-character and eight-character in length. The research suggests that increasing password character length to a minimum of 6 to 8 characters reduces crackability and therefore password strength in terms of security. Another study conducted suggests that crack-resistant passwords were achieved through the use of a sentence-generation password method including the user to embed a digit and special character into the password (Vu et al., 2004). However, memorability issues occurred with users from adding the digit and special character to the password.

Short-term Memory

Miller's (1956) Chunking Theory and Cowan's (2001) research is useful to consider when developing a model for password guidelines. This theory classifies data in terms of chunks and indicates that the capacity of working memory is 7±2 chunks of information. More recent research suggests that a mean memory capacity in adults is only three to five chunks with a range of two to six chunks as the real capacity limit (Cowan, 2001). A chunk of data is defined as being a letter, digit, word or different unit, such as a date (Miller, 1956). A chunk is further described as a set of adjacent stimulus units that are closely tied together by associations in the user's long-term memory. Miller suggests that merely turning information into a meaningful chunk of data can increase a person's short-term memory capacity. This occurs because chunking data places the input into subsets that are remembered as single units. A person's short-term memory capacity is reduced if a person tries to remember isolated digits or letters rather than grouping or recoding the information into chunks of data. Chunking then becomes useful in creating a meaningful sequence of stimuli within the total string of data; that is, chunks serve as an integral representation of data that are already stored in a person's long-term memory.

Similar to Miller's Chunking Theory, Newell, Shaw, and Simon (1961) suggest that highly meaningful words are easier for a person to learn and remember than less meaningful words, with *meaningful* being defined by the person's number of associations with the word. Vu et al. (2003) suggest that passwords could be more memorable if users comprised their passwords with familiar characters such as phone numbers. Memorizing a string of words that represent complete concepts is easier to remember than an unrelated list of words suggests Straub (2004). Building on Miller's work, Golbeck (2002) suggests that schemas can serve as the basis for chunks because they provide a meaningful method for grouping information. A schema is defined as a mental model that makes recall of an item easier for users. Mental models are sets of beliefs that a person has on how a system works and therefore interacts with a system based on these beliefs (Norman, 1988).

Research suggests that turning information into a meaningful chunk of data can increase a person's short-term memory capacity. For example, a study conducted by Loftus, Dark, and Williams (1979), which tested short-term memory retention among ground control and student pilots through an examination of communication errors, found that recall was better when material was chunked. In addition, Preczewski and Fisher (1990) studied the format of call signs made up of any series of letters and digits used by the military in secured radio communications. The findings indicate that the size of the chunks influenced the accuracy of short-term retention. Furthermore, mixing letters and digits within one-chunk was more difficult to recall than just having letters or digits make up the chunk because the mixed chunk of letters and digits lacked meaning. This research therefore suggests that memory is enhanced when the person can make meaning of the data string.

Wickens (1992) suggests that chunking should be used whenever possible because of people's working memory limitations. Further, he describes chunking as a strategy or mnemonic device that may be taught. This mnemonic aspect is what makes chunking a helpful way for organizations and individuals to develop passwords that do not exceed human memory limitations. Therefore, system designers, or in this case, system password guideline designers, should not exceed the low end of Miller's 7±2 chunk scale. Proctor et al. (2002) performed research where Miller's Chunking Theory (1956) was a consideration in testing different length passwords between five-characters to eight-characters due to Miller's 7±2 chunk scale. In a study conducted by Vu et al. (2004), a sentence-generation method was utilized to produce a crack-resistant password through the user being required to embed a special character and digit into the sentence. User memorability of these generated passwords declined as it took users two times longer to recall the passwords, made users perform twice as many errors in recalling the password, and result in users forgetting the password twice as often. The researchers suggest that the errors occurred due to users forgetting the sentence generated and the special character and/or digit embedded in the sentence. Furthermore, participants experienced difficulty with remembering the digit and/or symbols which researchers attributed to the symbols and/or digits not being meaningfully related to the sentence. Vu et al. (2003) conducted a different study to analyze the effects of password generation and recall utilizing multiple accounts suggesting that increasing demands on human memory leads to the level of remembrance of the password to be decreased. The research presented in the next section is an expansion of their research through gathering more data in the area of human memory limitations through testing longer passwords than those tested in their study as well as utilizing Chunking Theory to aid the user in remembering their passwords.

Methodology

The purpose of the research was in evaluating the impact of password demands as a means of authentication and to mitigate risks that result when these demands exceed human capabilities. The intent was to develop password guidelines that don't exceed human memory limitations yet that maintain strength of passwords. The password guidelines developed in this research had individuals compose their passwords of relevant and meaningful data that aren't accessible to the public. Some industries do suggest to system users to compose passwords of meaningful data. However, specific guidelines or password training have not been established to aid users in how to comprise a password that is both secure and meaningful.

The research adds value to information security literature through the testing the usefulness of chunking theory being applicable to the development of passwords.

The research addressed in this section is summarized in Table 1. The study consisted of two experiments performed at a large federal agency to determine whether a difference exists in people's ability to remember complex passwords with different difficulty levels. The hypothesis tested for the two Federal Agency experiments presented in this section is below:

Ho: There is no difference in people's ability to remember complex passwords with different difficulty levels.

Ha: There is a difference in people's ability to remember complex passwords with different difficulty levels.

Table 1: Summary of Experiments

Research Activity	Password Length in Characters	Password Guidelines	Participants	Study Length	Participants' Training
7-Character Password Level (Experiment 1)	7	(a) Password must be at least 7 characters in length. (b) Password must have a combination of symbols and letters. (c) Password can't use the same term more than twice. (d) Password must not spell out a dictionary word or proper noun. (e) Password can't be relevant data such as individual's social security number, street address, birth date, etc.	30	5 days for one week	None
Two-Chunk Password Level (Experiment)	10	(a) Participants' first and last initials formatted using a combination of both uppercase and lowercase letters (first chunk). (b) Participants' federal agency start date using different types of symbols as day, month, and year separators (second chunk).	30	5 days for one week	None
Three-Chunk Password Level (Experiment 1)	12	(a) Participants' first and last initials formatted using a combination of both uppercase and lowercase letters (first chunk). (b) Participants' federal agency start date using different types of symbols as day, month, and year separators (second chunk). (c) Participants' mother's first name initial in uppercase and maiden name initial in lowercase (third chunk).	30	5 days for one week	None
Four-Chunk Password Level (Experiment 2)	20-22	(a) Participants selected two meaningful dates that weren't easily accessible to the public using a symbol of choice to be used as day/month/year separators (2 chunks). (b) Participants selected two sets of initials that contained at least one uppercase and one lowercase letter (2 chunks).	30	5 days for one week	15 minute training session on creating a meaningful password.

Experiment 1

The experimental design for Experiment 1 consisted of three levels of password strength passwords tested for five days each with matched samples across each level of password strength tested. The participants for the study were 30 federal agency employees that volunteered for the study through an e-mail request announcement sent out to all employees within two departments. The employees that participated in the study ranged in age from 20 to 50 and consisted of personnel in the fields of engineering, science, and business within different organizational levels ranging from clerical staff to managerial staff. Data was collected through electronic dissemination of questions. The response rate was 100% as participants that were away from the office were still able to be responsive to the study as access to their work e-mail was readily available. The results were interpreted through utilizing a Chi-square ($\chi 2$) goodness of fit test.

Experiment 1 involved participants opening three password-protected Microsoft Word™ 97 documents five days a week for three weeks, with each week representing a different level of password strength password in the experiment. For each level of password strength in Experiment 1, the password recall rate was determined through participants' responses to questions sent electronically regarding if the participant remembered all three passwords and whether the participant had to look at paper to remember their passwords. Each of the three levels tested different password difficulty levels. Password strength for each level in the experiment was measured through the amount of meaningful data that was contained in participants' passwords as well as participants' ability to chunk the data for ease of remembrance. Level 1 referred to as the "7-Character Password Level" required participants to choose their own passwords that satisfied stringent password guidelines as noted in Table 1 without any training on how to best select a password.

Level 2 referred to as the "Two-Chunk Password Level" required participants to utilize 3 two-chunk passwords totaling ten-characters that followed the guidelines as displayed in Table 1. An example of a Two-Chunk Password Level is "Rs#08-2193" with the first chunk being "Rs" that stands for Ryan Smith and the second chunk being "#08-2193" that stands for his federal agency start date of August 21, 1993. Level 3 referred to as the "Three-Chunk Password Level" had participants utilize 3 three-chunk passwords that were the same as the passwords utilized in the Two-Chunk Password Level but with two additional characters consisting of their mother's first name initial in uppercase and maiden name initial in lowercase (third chunk). An example of a Three-Chunk Password Level password is "Rs#08-2193Nj" with the first and second chunk remaining the same as the example previously stated, and the third chunk being "Nj" that stands for "Norma Jones." Measurement of participant's performance was determined through asking each participant five days a week to answer the exact same questions regarding password recall rate. A $\chi 2$ goodness of fit test was used to determine which set of password guidelines were easiest for participants to remember and which passwords required participants to refer to paper for recall.

Experiment 2

Design for Experiment 2, which is referred to as the "Four-Chunk Password Level Experiment," consisted of a five-day experiment that involved 30 federal agency employees. The participants for the study were 30 federal agency employees that volunteered for the study through an e-mail request announcement sent out to all employees within two departments. The employees that participated in the study ranged in age from 20 to 50 and consisted of personnel in the fields of engineering, science, and business within different organizational levels ranging from clerical staff to managerial staff. Data was collected through an electronic survey. The response rate was 100% as participants that were away from the office were still able to respond via e-mail. The results were interpreted through calculating 95% confidence intervals for the three levels in Experiments 1 as well as the Four-Chunk Password Level Experiment to determine significant differences in the password guidelines tested.

The Four-Chunk Password Level Experiment involved participants who were tested on their ability to recall a password composed of four-chunks of meaningful and unique data, where each password contained 20 to 22 characters depending on individual preferences for using or not using middle initials. The Four-Chunk Password Level Experiment differs from the levels of password strength tested in Experiment 1 not only in testing longer passwords with more chunks of data but in a training component: the experimenter met with each participant to provide a 15 minute training session on how to select meaningful passwords. Guidelines for these passwords are also displayed in Table 1. An example of a Four-Chunk Password Level Experiment password is "08#11#71Lg12#11#81kd." The first chunk is "08#11#71" which stands for "August 11, 1971." The second chunk is "Lg" which stands for "Laura Green." The third chunk is "12#11#81" which stands for "December 11, 1981." Lastly, the fourth chunk is "kd" which stands for "Kyle Doyle." The Four-Chunk Password Level Experiment utilized a different set of participants than those in the three levels affiliated with Experiment 1 in order to test individual capability to recall lengthy passwords without previous practice. In this way, the Four-Chunk Password Level Experiment could serve as a validation experiment to back up the results of Experiment 1.

Since the Four-Chunk Password Level Experiment tested a password of 20–22 characters in length, the experiment could not utilize password-protected documents, as the software wouldn't accommodate a password of this length. Therefore, e-mail was sent out to each participant during the five days of the experiment asking individuals to answer the same two questions enabling the researchers to calculate each participant's password recall rate: (a) Please type in your password below (if it is incorrect, I will resend this message to you asking you to try again), and (b) Did you have to refer to paper to recall your password (please answer yes or no)? The e-mail message also informed individuals that if a new e-mail message was not sent to them later the same day; it meant that they had typed the password correctly on the first try. The e-mail message alternately indicated that if the individual had incorrectly entered the password, another e-mail message would be sent later in the day, asking the individual to try again. Finally, the e-mail indicated that this process would be repeated until the participant typed in the correct password either from memory or from referring to paper.

Statistical Analyses

A $\chi 2$ goodness of fit test was conducted to determine statistical differences in the three password levels of password strength tested in Experiment 1. A 95% confidence interval for the true proportion of recall rates and looked-at-paper rates for each password level tested in both experiments was also constructed to determine significant differences. Conducting the 95% confidence interval test enabled the fourth password level tested in the Four-Chunk Password Experiment to be part of the analysis.

Findings

The results are presented in Tables 2, 3 and 4. Tables 2 and 3 display the percentages from the answers to the questions regarding recall rates from both experiments. Additionally, Table 2 displays the results of the three levels of password strength of Experiment 1 in which a $\chi 2$ goodness of fit test was performed in the analysis regarding the question "Did you remember all 3 passwords?" The results indicate a statistical difference in that the Two-Chunk Password Level and Three-Chunk Password Level passwords had a significantly higher level of remembrance than the 7-Character Password Level.

Table 3 displays the results of performing a $\chi 2$ test for the question of "Did you have to look at paper to remember the passwords?" The results indicate a statistical difference in that individuals referred to paper to recall a password significantly more in the 7-Character Password Level than in the Two-Chunk Password Level and Three-Chunk Password Level, which points to the difficulty individuals experienced in recalling the 7-Character Password Level passwords. The reduction in the number of the Two-Chunk Password Level participants referring to paper for password recall as compared with the Three-Chunk Password Level participants may be attributable to a learning curve. That is, the Two-Chunk Password Level and Three-Chunk Password Level passwords were similar, which enabled participants to utilize the Two-Chunk Password Level as training for the Three-Chunk Password Level.

Table 2: Recall Rates

Experiment and Level	% Days Remembered All Passwords (Recall Rates)
7-Character Password Level (Experiment 1)	50.7
Two-Chunk Password Level (Experiment 1)	66.7
Three-Chunk Password Level (Experiment 1)	72.7
Four-Chunk Password Level (Experiment 2)	76.0

Note: $\chi 2$ test performed in Experiment #1 indicated that the 7-Character Password Level password strength versus the Two-Chunk Password Level password strength resulted in $p<0.01$; 7-Character Password Level password strength versus the Three-Chunk Password Level password strength resulted in $p<0.001$; Two-Chunk Password Level password strength versus the Three-Chunk Password Level password strength resulted in p= NS.

Even though there were an increased number of characters in the Three-Chunk Password Level passwords, the Three-Chunk Password Level individuals experienced an increased level of remembrance with less referral to paper in comparison to the Two-Chunk Password Level participants. The results suggest that passwords in the Three-Chunk Password Level may be as easily recalled as those in the Two-Chunk Password Level (without a learning curve). Table 4 displays the results of the researchers having performed interval comparisons that utilize the percentages found in Tables 2 and 3.

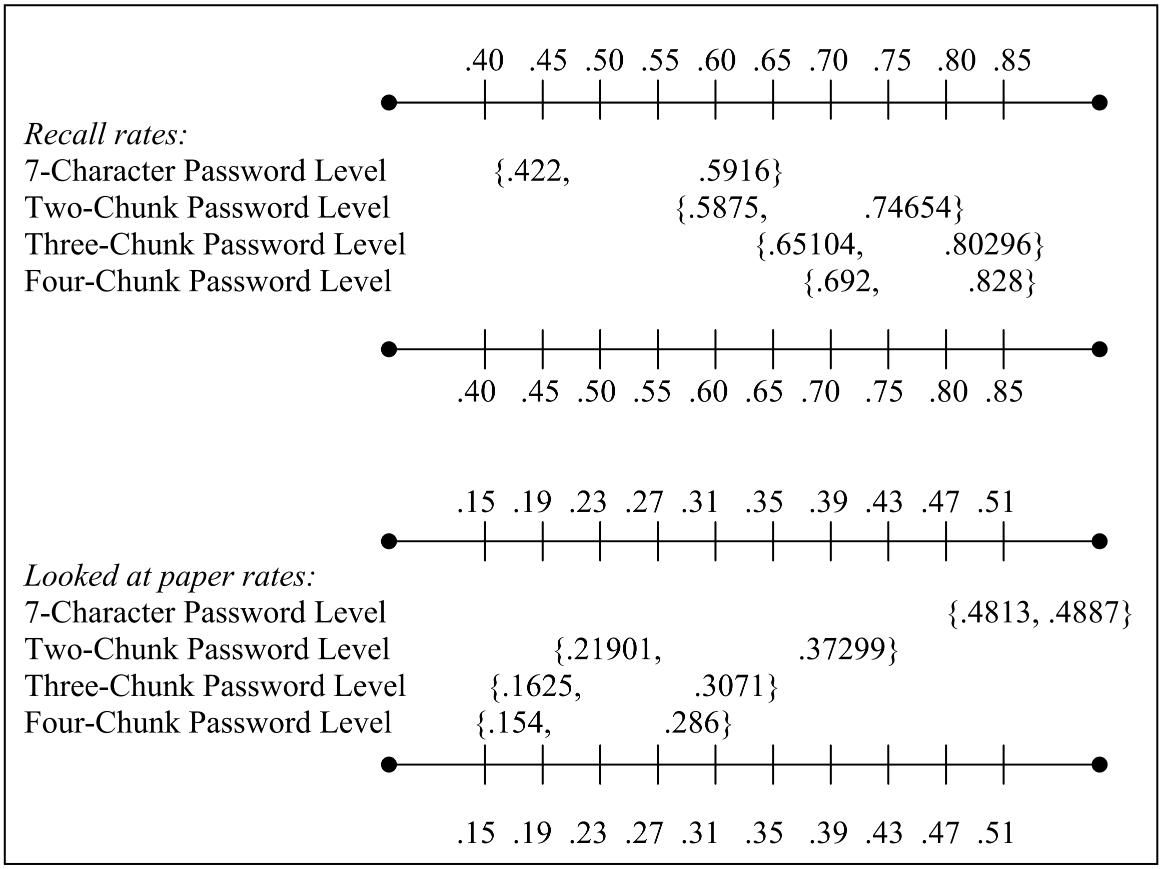
Table 3: Rates at Which Individuals Looked at Paper to Assist Password Recall

Experiment and Level	% Days Looked at Paper to Remember Password
7-Character Password Level (Experiment 1)	48.5
Two-Chunk Password Level (Experiment 1)	29.6
Three-Chunk Password Level (Experiment 1)	23.5
Four-Chunk Password Level (Experiment 2)	22.0

Note: For probability values see the note to Table 2.

Table 4 displays the statistical difference in the four different levels of password strength tested. Therefore, the overlapping intervals indicated that the different levels of password strength were the same. Whereas, the non-overlapping intervals indicated that the different levels of password strength had a statistical difference. Thus, research suggests that recall rates were better for the Three-Chunk Password Level versus the 7-Character Password Level and better for the Four-Chunk Password Level Experiment versus the 7-Character Password Level. It is important to note that since there is only minimal overlapping between the 7-Character Password Level and the Two-Chunk Password Level, the results suggest that the Two-Chunk Password Level passwords may be better recalled than those in the 7-Character Password Level, suggesting the same results as indicated in the $\chi 2$ test. Results also indicate that there was no statistical difference in individuals' ability to recall (a) the Two-Chunk Password Level passwords versus those in the Four-Chunk Password Level Experiment or (b) the Three-Chunk Password Level passwords versus those in the Four-Chunk Password Level Experiment.

Table 4: Comparison of Rates at the .95 Confidence Interval



Recall rates:		
7-Character Password Level	{.422,	.5916}
Two-Chunk Password Level	{.5875,	.74654}
Three-Chunk Password Level	{.65104,	.80296}
Four-Chunk Password Level	{.692,	.828}
Looked at paper rates:		
7-Character Password Level	{.4813,	.4887}
Two-Chunk Password Level	{.21901,	.37299}
Three-Chunk Password Level	{.1625,	.3071}
Four-Chunk Password Level	{.154,	.286}

Note: The four different levels of password strength were compared with each other at the .95 confidence interval. If the intervals overlap, then the two intervals are the same. If the two intervals are not overlapping then there is a statistical difference. Therefore, if the confidence intervals overlap, the two rates at the .05 level are not statistically significant but if they are non-overlapping, then the two rates are statistically different with $p \leq .05$.

In analyzing the looked-at-paper rates for the experiments, the results indicate that participants looked at paper to recall passwords less with the Two-Chunk Password Level than the 7-Character Password Level, less with the Three-Chunk Password Level than the 7-Character Password Level, and less in the Four-Chunk Password Level Experiment than the 7-Character Password Level. Findings indicate that passwords utilizing Chunking Theory required participants to look at paper the least. The intervals overlap (a) for the Two-Chunk Password Level in comparison with the Three-Chunk Password Level, (b) for the Four-Chunk Password Level Experiment in comparison with the Two-Chunk Password Level, and (c) for the Four-Chunk Password Level Experiment in comparison with the Three-Chunk Password Level. Therefore, findings suggest that there is no statistical difference in the number of times participants had to refer to paper to remember either a two-chunk, three-chunk, or four-chunk password.

The results indicate that a password comprised of meaningful chunks is easier to recall than a password with random data, even if the password contains additional characters. Research suggests that individuals were better able to recall the passwords in the Two-Chunk Password Level and Three-Chunk Password Level as well as in the Four-Chunk Password Level Experiment, which indicates that data in the actual passwords could be meaningfully chunked together for the individual. Furthermore, the results indicate that an individual is able to recall a two-chunk password as easily as a three-chunk or even a four-chunk password. Results further suggest that an individual is able to recall a password ranging from 7 to 22 characters in length without referring to paper, provided that Chunking Theory is utilized in composing individual passwords.

The findings of the interval-comparisons analysis were similar to the results indicated by the $\chi 2$ goodness of fit test conducted for all of the different level password strength passwords tested as part of Experiment 1. The Four-Chunk Password Level Experiment also served as a validation experiment to ensure that participants can recall more than two-chunks of data with ease. Since results suggested that participants in Four-Chunk Password Level Experiment were able to recall four-chunks of meaningful data that were unique to each individual and that they were able to do so without frequent referral to paper to aid in recall, the positive results affiliated with the Three-Chunk Password Level can be considered valid. Although the results of the Four-Chunk Password Level Experiment were positive, it is not feasible from an IT perspective to have passwords of that length. Nevertheless, passwords can still be composed of two-chunks to four-chunks of data because chunks of data can range in size (e.g., by selecting a one-character symbol rather than a more lengthy date). In other words, four-chunks in comparison to two-chunks doesn't necessarily equate to a longer password as suggested by the research. It is interesting that the results indicate that as long as information in a password is composed of meaningful information unique to an individual, human memory capabilities enable an individual to recall up to four-chunks of data consisting of up to 22-characters.

Discussion

The research findings are applicable to the study of information, information technology and organizations. Figure 1 is a vulnerabilities impact model developed to display how password issues could potentially contribute to vulnerabilities being present within organizations' systems. This impact has the potential to cause harm to information which is the core of any organization as knowledge is power. Without confidentiality, integrity, and accessibility of information within organizations' systems, an organizations' competitive advantage could be violated. Organizations still primarily utilize passwords as a means of user authentication for information technology. The password issues that were identified during the research consisted of an individual being expected to remember many different passwords, multiple systems that required different or similar passwords for an individual to obtain access, and the complexity of password guidelines that individuals are expected to follow in the development of their passwords. These issues produce system vulnerabilities, such as weak passwords (e.g., dictionary words), common passwords (e.g., using the same password for more than one system), visible passwords (e.g., an individual writing their password on a sticky note hanging on their computer), and security policies not being followed due to the complexity of the password guidelines. These vulnerabilities could result in the potential of insecure systems.

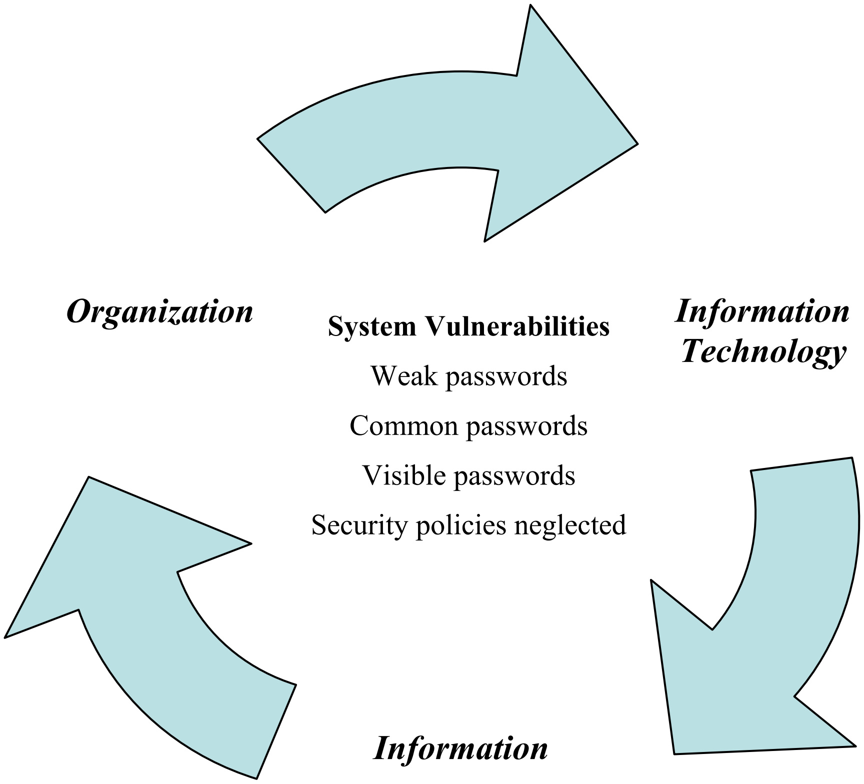


Figure 1: Vulnerabilities Impact Model

Several limitations of the study were present. The first limitation consisted of the research only being tested within a single organization. Secondly, the study only identified password issues; however other issues that have the potential to cause system vulnerabilities such as workload issues also need to be studied. The third limitation is that the study only utilized participants that were Americans. With the rise in globalization, a study with a more diverse participant base may have revealed different findings. The fourth limitation is that the study centered on the use of password authentication when other means of authentication such as bio-identifiers, smart cards, tokens and individual certificates are also utilized in society.

Conclusion

The research adds value to information security literature through testing the usefulness of chunking theory being applicable to the development of passwords. The research findings presented the researchers with several opportunities to expand their efforts to assist organizations to better guard against their system vulnerabilities. The findings resulted in practitioner implications, research implications, and guidelines for future research.

Practitioner Implications

Research on passwords is necessitated in spite of a movement to alternative security techniques, such as bio-identifiers, individual certificates, tokens and smartcards. For example, smart cards communicate directly with the target system and run the authentication procedure themselves. A survey of 4,254 companies in 29 countries was conducted by Dinnie (1999) to identify a global perspective of information security. The survey indicated that password authentication in the USA is the preferred security method utilized 62% of the time as opposed to smart card authentication only being used 8% of the time and certificates 9% of the time. In Australia, password authentication is used 67% as opposed to smart card authentication only being used 9% of the time and certificates 5% of the time. The remaining countries surveyed showed password authentication at 58% with smart card authentication at 4%. However, the problem with password authentication, smart cards and tokens is that these provide the ability to have the information that is requested but not the ability of identifying the person (Harris & Yen, 2002). Therefore, bio-identifiers will likely become increasingly popular as it is the only way to identify who the person is rather than what they have or know. Harris & Yen (2002) have noted the main problems of bio-identifiers are the cost, inconvenience of users needing to prepare to be scanned and needing to be enrolled at multiple computer systems, potential to fool systems leading to unauthorized access and fear individuals have with their biometric data being stolen. Therefore, password usage for both professional and personal use is still a common means of authentication necessitating the need to understand it better from the perspective of human memory limitations and security aspects.

The present research addressed the human side of information security through the results of the experiments suggesting that passwords can be developed that are both secure and easy to recall. This research offers guidance to those that design security policies, by providing practical and manageable password guidelines displayed in Figure 2. When followed, these guidelines result in (a) reduced vulnerability of information systems within organizations and (b) increased trust in the users of information technology. These guidelines provide users with a password that will be both secure and easy to recall (i.e., stored effectively in an individuals' long term memory). Password guidelines were created that do not exceed human memory limitations yet maintain strength of password as necessitated by the IT community. The password guidelines are based on the guidelines tested in the research and need to be further studied to validate use outside of a federal agency. There is a need to develop passwords that don't exceed human memory limitations yet that maintain strength of password as necessitated by organizations' IT communities. The two criteria for ideal password development are: (a) passwords contain meaningful and personally relevant data for the user: and (b) passwords are strong passwords in terms of the IT community's standards.

- Passwords contain two to four chunks of data and are 10 to 22 characters in length, depending on the character length capabilities of the given system.
- Passwords must contain a combination of symbols, numbers, and letters.
- Passwords cannot use the same term more than twice.
- Passwords must not spell out a dictionary word or proper noun (name of a person, pet, place or thing).
- Passwords can not contain information easily accessible to the public (social security number, street address, family members' birthdays, wedding anniversary date, etc.).

Figure 2: Password Guidelines

It is important that these guidelines be utilized in conjunction with training that assists the user in creating a password composed of meaningful data chunks and in managing multiple passwords. Some degree of training is required to guide employees on how to compose passwords that are comprised of meaningful chunks of data unique only to that employee. Research by Yan and colleagues (2004) suggests that password security can be significantly improved through educating users on how to better comprise a password. First, the instructor should define what it means to compose a password of meaningful chunks and may discuss how many chunks of data can easily be recalled by users (i.e., two, three or four, as suggested in the current study). It would also be helpful if the instructor were encouraged to tell different employees to comprise their passwords of different lengths so that potential hackers would be unable to discover a consistent password length among employees. For example, an instructor might inform employees in one class to have a system specific password between 7-9 characters in length and in another class might recommend a password between 10-12 characters in length.

Instructors should also stress the importance to have the same password used for more than one system. Employees should also be encouraged to select one chunk of a password to be considered as a core of every password. The core or one-chunk would then be part of all passwords. For example, if a person wanted to create a two-chunk password, a person could select “Mb#=43” which translates to my basketball number equals 43 as one-chunk within their password. The person could then select the second chunk of data such as “iemf” which translates to industrial engineering major in Florida. The two chunks could be combined to form one password that an individual uses to access their university portal. Therefore, one-chunk of every password for an individual could remain constant. It is the second chunk of the password that could vary and be composed of information that is directly linked to the system or device where it is used. An individual could then have multiple passwords in both their professional and personal lives that have one familiar chunk which never varies. However, from a security perspective additional chunks used in the password should vary. From a human memory limitations perspective, linking the second chunk to the system being used in a unique and non-obvious matter would enable an individual to obtain a password that is strong yet easy to recall.

These guidelines are applicable to a variety of uses such as information systems, document passwords, corporate portals and mobile devices. However, the guidelines are not applicable to legacy systems due to the recommended character length. Although, the other aspects of the guidelines could aid legacy system users to better recall their passwords.

Research Implications

The world has been revolutionized by the amount of information that makes its way into the daily lives of individuals and ultimately organizations. It is therefore necessary that research continues to identify specific ways that assist individuals in handling the abundance of information. The guidelines detailed in the present research and displayed in Figure 2 reduce the information load faced by individuals trying to maintain numerous passwords for recall.

These guidelines propose a password-creation system that does not impose additional demands on a person’s attention capacities and short-term memory since passwords are composed of information that already exists in an individual’s long-term memory. When these guidelines are followed, employees can be trusted to follow organizational security policies because employees have been provided with clear instructions that enable them to form strong passwords that are easy to recall. The use of password guidelines reduces the likelihood of an organization being subject to a security breach since individuals would be less likely to engage in practices that render an organization vulnerable, such as using the same password for multiple systems or writing their passwords on paper. The present findings support the use of Miller’s (1956) Chunking Theory and Cowan (2001) when developing password guidelines and training on password development. Specifically, the findings suggest the benefits of utilizing two-chunks to four-chunks of data to increase password security while reducing the demand on the user. Through simple password guideline changes and employee password security training, organizations can better guard against human error while maintaining secure practices for user authentication that guard against external threats. The present research serves as a guide to organizations looking to strengthen their password-creation guidelines as well as a building block for future research that focuses on the human side of information security.

Future Research

Future research is needed to further validate the original findings of the research. The future research should consist of several components such as (a) continuously conducting surveys regarding individual password usage as new technology emerges thus increasing the amount of technology utilized daily by organizations; (b) expanding upon the model described in Figure 1 through surveys and experiments to identify issues beyond password issues that may cause system vulnerabilities such as the exploration of workload issues; (c) determining links between password issues and other newly identified issues on human memory limitations and strategies to reduce the potential for vulnerabilities produced; (d) apply the training concepts in utilizing the password chunk suggestions to different types of organizations such as non-government organizations consisting of universities, private-industry and virtual corporations to validate the findings through gathering before and after vulnerabilities statistics; and (e) conduct more literature reviews and experiments in the area of short-term memory to identify additional research studies on the human side of information security such as studying other authentication tools consisting of bio-identifiers, individual certificates, tokens and smartcards.

Future research in the human side of information security will further support the need for organizations to have password guidelines that do not exceed human memory limitations. Having password guidelines that do not exceed human memory limitations will enable organizational security policies to be better followed and eliminate the need for individuals to write their passwords on a piece of paper or use the same password for multiple systems. Identification of the links between password issues and possibly workload issues on human memory limitations will further educate organizations on the vulnerabilities present. Once the vulnerabilities are identified, organizations can better guard against the vulnerabilities present in systems and therefore positively contribute to impacting the security of information within systems.

Acknowledgements

Sincere appreciation is given to the US federal government agency for providing subjects and information security experts for the research. The following individuals are also acknowledged for their guidance in conducting the research effort: Dr. James T. Brown, SEBA Solutions, Inc., and Dr. Ronald F. DeMara and Dr. Lesia Crumpton-Young, from the University of Central Florida. Sharon Carnohan and Suzanne Murray are also appreciated for their editing support.

References

Carnegie Mellon Computer Emergency Response Team (CERT). (2006). Computer emergency response team statistics. Retrieved September 14, 2006 from http://www.cert.org/stats/cert_stats.html#incidents

Carstens, D. S., Mc-Cauley-Bell, P., Malone, L., and DeMara, R. (2004). Evaluation of the human impact of password authentication practices on information security. *Informing Science Journal, 7*, 67-85. Available at http://inform.nu/Articles/Vol7/v7p067-085-229.pdf

Cowan, N. (2001). The magical number 4 in short-term memory: A reconsideration of mental storage capacity. *Behavioral and Brain Sciences*, *24*(1), 87-185.

Dinnie, G. (1999). The second annual global information security survey. *Information Management & Computer Security, 7(3), 112-120.*

Golbeck, J. (2002). Cognitive load and memory theories. Retrieved June 2, 2006, from http://www.cs.umd.edu/class/fall2002/cmsc838s/tichi/printer/memory.html

Harris, A.J., & Yen, D.C. (2002). Biometric authentication: Assuring access to information. *Information Management &Computer Security, 10*(1), 12-19*.*

Hensley, G.A. (1999). Calculated risk: passwords and their limitations. Retrieved June 2, 2006, from http://www.infowar.com/articles/99article_120699a_j.shtml

Ives, B., Walsh, K., & Schneider, H. (2004). The domino effect of password reuse. *Communications of the ACM, 47*(4), 75-78.

Lewis, J. (2003). Cyber terror: Missing in action. *Knowledge, Technology & Policy, 16*(2), 34-41.

Loftus, E. F., & Dark, V. J., & Williams, D. (1979). Short-term memory factors in ground controller/pilot communication. *Human Factors, 21*, 169-181.

McCauley-Bell, P.R., & Crumpton, L.L. (1998). The human factors issues in information security: What are they and do they matter? *Proceedings of the Human Factors and Ergonomics Society 42nd Annual Meeting*, USA, 1998, 439-442.

Miller, G.A. (1956). The magical number seven plus or minus two: Some limits on our capacity for processing information. *Psychological Review, 63*, 81-97.

National Institute of Standards and Technology (NIST). (1992). *Computer System Security and Privacy Advisory Board (Annual Report)*, 18.

Newell, A., Shaw, J. C., & Simon, H. (1961). *Information processing language V manual*. Edgewood Cliffs, NJ: Prentice-Hall.

Norman, D. A. (1988). *The psychology of everyday things.* New York: Harper & Row.

Preczewski, S.C., & Fisher, D.L. (1990). The selection of alphanumeric code sequences. *Proceedings of the Human Factors Society 34th Annual Meeting*, USA, 1990, 224-228.

Proctor, R.W., Lien, M.C., Vu, K.P.L., Schultz, E.E., & Salvendy, G. (2002). Improving computer security for authentication of users: Influence of proactive password restrictions. *Behavior Research Methods, Instruments, & Computers, 34*, 163-169.

Straub, K. (2004). Cracking password usability exploiting human memory to create secure and memorable passwords. *UI Design Newsletter*, Retrieved June 2, 2006, from http://www.humanfactors.com/downloads/jun04.asp

U.S. Department of Homeland Security. (2002). *Federal information security management act.* Retrieved June 2, 2006, from http://www.fedcirc.gov/library/legislation/FISMA.html

Vu, K.P.L., Bhargav, A., & Proctor, R.W. (2003). Imposing password restrictions for multiple accounts: Impact on generation and recall of passwords. *Proceedings of the 47th Annual Meeting of the Human Factors and Ergonomics Society,* USA, 2003, 1331-1335.

Vu, K.P.L., Tai, B.L., Bhargav, A., Schultz, E.E., & Proctor, R.W. (2004). Promoting memorability and security of passwords through sentence generation. *Proceedings of the Human Factors and Ergonomics Society 48th Annual Meeting*, USA, 2004, 1478-1482.

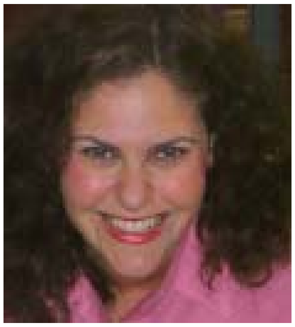
Wickens, C.D. (1992). *Engineering psychology and human performance* (2nd ed.). New York: Harper-Collins Publishers.

Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A., & Memon, N. (2005). PassPoints: Design and longitudinal evaluation of a graphical password system. *International Journal of Human Computer Studies, 63*, 102-127.

Wood, C.W., & Banks, W.W. (1993). Human error: an overlooked but significant information security problem. *Computers & Security, 12*, 51-60.

Yan, J., Blackwell, A., Anderson, R., & Grant, A. (2004). Password memorability and security: Empirical results. *IEEE Security and Privacy, 2*(5), 25-31.

Biographies



Dr. **Deborah Carstens** has a Ph.D. in Industrial Engineering and B.S. in Business Administration from the University of Central Florida as well as a M.B.A. from the Florida Institute of Technology. She is an Assistant Professor of Management Information Systems at the Florida Institute of Technology instructing courses in human-computer interaction, usability, and system design and development. Her research interests are in process and safety optimization, human error analysis and usability testing. She previously was employed for over ten years at the NASA Kennedy Space Center (KSC) where her work included being a principal investigator on human factors research projects, Industrial Engineering for Safety Program Study Manager over research studies conducted on space shuttle activities, and the Process and Human Factors Engineering (P&HFE) Roadmap Manager responsible for the identification of P&HFE technology needs at KSC up to year 2025. During her career at KSC, she was awarded a superior accomplishment award, NASA KSC Graduate Fellowship, and from the Society of Logistics Engineers a Logistics Specialty Award for exceptional achievement in Logistics Management Information Systems.

Linda C. Malone is a Professor in the Industrial Engineering Department at University of Central Florida. She got her B.S. and M.S. degrees in mathematics and her Ph.D. degree in statistics from Virginia Tech in 1975. She is the coauthor of a statistics text, has authored or coauthored 43 refereed papers, and has a patent pending. She is an associate editor of the Journal of Statistical Computation and Simulation. She has served in various offices in statistical organizations including service on the Board of Directors of the American Statistical Association. She was awarded the honor of Fellow of the American Statistical Association.

Pamela McCauley-Bell is an Associate Professor in the Industrial Engineering and Management Systems Department at the University of Central Florida. She has a Ph.D. in Industrial Engineering, M.S. in Industrial Engineering, and B.S. in Industrial Engineering from the University of Oklahoma. Dr. McCauley-Bell's primary teaching interests at the graduate level are human factors or ergonomics and intelligent systems development. Most recently, she developed an undergraduate course in information security that she taught at the Massachusetts Institute of Technology. She has developed courses in Biomechanics, Ergonomics, Expert Systems and Fuzzy Set Theory. Dr. McCauley-Bell's research interests bring together her background in physical ergonomics, human factors and intelligent system development with the modeling techniques of fuzzy set theory.