Online Journal of Applied Knowledge Management
A Publication of the International Institute for Applied Knowledge Management

Volume 4,Issue 1, 2016

Empirical results of an experimental study on the role of password strength and cognitive load on employee productivity

Stephen Mujeye, McHenry County College, USA, smujeye@yahoo.com

Yair Levy, Nova Southeastern University, USA, levyy@nova.edu

Herbert Mattord, Kennesaw State University, USA, hmattord@kennesaw.edu

Wei Li, Nova Southeastern University, USA, lwei@nova.edu

Abstract

The demand for information system authentication has significantly increased over the last decade. Research has shown that the majority of user authentications remain to be password-based, however, it is well documented that passwords have significant limitations. To address this issue, companies have been placing increased requirements on the user to ensure their passwords are more complex and consequently stronger with little consideration on the impact on employee productivity. Thus, this study was set to determine the effects of changing the password strength (cognitive load) over time and its impact on employee productivity. An experiment with two experimental groups and one control group was conducted. Data was collected on the number of failed operating system logon attempts, users' logon times, task completion times, and number of reset requests. The data collected from 72 participants was analyzed for group differences and when controlling for computer experience, age, and gender. Our results showed significant differences on all measures between the three groups. However, no significant differences were observed when controlling for computer experience, age, and gender. Furthermore, the results indicated a significant difference between the user's perceptions about passwords before and after the experiment. Our results may help organizations to realize the point at which increasing authentication places a higher cognitive load on the users, which in turn affects their productivity.

Keywords: *Access control in organization, passwords vs. organizational productivity, password strength, authentication in organization, password complexity paradox, cognitive load theory.*

Introduction

Authentication of users is an important security concern within any type of information system (IS), be it a Web-based or corporate network. Ren and Wu (2012) defined authentication as "the act of confirming that the communicating entity is the one claimed" (p. 714). Authentication ensures that only legitimate users are allowed to gain access into a system or a network. One of the most widely used methods of user authenticate is through the use of passwords (Chiasson, Forget, Stobert, van Oorschot, & Biddle, 2009). In order for passwords to be effective, it needs to be complex enough and resist several types of password attacks (Tsai, Lee, & Hwang, 2006).

Passwords by their nature are vulnerable to attacks like “dictionary attacks” and “brute force attacks” (Molloy & Li, 2011).

It appears that a need exists to better understand the balance between improving password security and its complexity requirement placed on users (Carstens, McCauley-Bell, Malone, & Demara, 2004). Moreover, it is evident that when passwords are too complex, users may forget their passwords, while it can have negative effects on productivity and task completion time. In situations where employees forget their passwords, time and resources are wasted while employees seek assistance in resetting their passwords. As such, the focus of our research was aimed at uncovering the point at which raising the authentication strength for passwords becomes counterproductive.

Theoretical Background

A significant increase has occurred in the number of ISs developed, implemented, and used by organizations (Erlich & Zviran, 2010). One of the challenges that accompanies are faced in the need for increased reliance on IS, is the security via enforcement of strong authentication methods. One of the branches of information security is access control, which governs who gains control to the IS. Kumari and Chithraleka (2012) mentioned that the main objective of access control is to protect resources from unauthorized access at the same time ensuring authorized access. One of the prerequisites of access control, at the foundation of security, is authentication. According to Levy, Ramim, Furnell, and Clarke (2011), “User authentication is the process of verifying an attempted request of an individual (i.e. ‘the user’) to gain access to a system” (p. 104). Menkus (1998) stated that methods of user authentication can be further dichotomized into three categories:

- Knowledge-based authentication – what the user knows
- Possession-based authentication – what the user has
- Biometric-based authentication – what the user is

Combination of two or three categories from the above (i.e. multi-factor authentication), is also valid when strong authentication measures needed, however, adding more complexity and outside the scope of this study. From these three categories, the most widely used method of user authentication is knowledge-based authentication. According to Erilich and Zviran (2009), knowledge-based user authentication can be further divided into different categories, which include: character-based, image-based, and question/answer-based.

In the categories above, the password method, a character-based method is the most widely used authentication method. In order for passwords to be effective and to reduce the problem of dictionary attacks or brute force attacks, some rules must be followed (Tsai, Lee, & Hwang, 2006). The rules include:

- Reduce or eliminate the use of dictionary words
- Increase password strength by increasing complexity (which includes minimum length, use of special characters/symbols, inclusion of numbers, & uppercase letters)

As noted above, passwords are the most-used method of user authentication in all types of computing environments (Kim, 2012). Oreku and Li (2009) also referred to the password as the frontline of defense against attackers and that virtually every system uses password as a method of authenticating users. Despite this, passwords have many limitations. Meng (2012) pointed out that passwords suffer from security and usability problems. Because users have limitations in long-term memory, they tend to use short passwords that are easy to remember. Password policies dictate the minimum number of characters, complexity, expiration limits, and/or the number of times a user can reuse the same password. To ensure different passwords are being used when the time to change comes, the Levenshtein distance can be used as it measures the extent to which two strings differ (Rane & Sun, 2010). Bard (2007) recommended a distance of five or greater in the Damerau Levenshtein distance metric to be considered for maximum strength. The characteristics of a password policy with some examples are noted in Table 1 (Inglesant & Sasse, 2012).

Table 1: Characteristics and Examples of Password Policy

Characteristic	Example
Length	At least eight (8) characters
Character Sets	At least one character from three of four classes; Character classes are uppercase letters, lower case letters, digits, and non-alphanumeric characters
Expiry	180 Days
History	Must not be similar to previous 12 passwords

Shay et al. (2010) also pointed out that while strong password policies improve security, those users may have difficulty remembering the passwords. Novakovic, McGill, and Dixon (2009) claimed that the use of strong passwords and constantly changing them can have counterproductive effects, as it places too much cognitive load on the users. As the cognitive load increases, it may result in users taking time away from performing their job functions, as well as increasing helpdesk and support requests to reset passwords (Brostoff & Sasse, 2000).

The cognitive load theory (CLT) is a seminal work based on cognitive science that equates the human mind to a processing system with working memory and storage memory (Sweller, 1988). Information that humans receive is stored in the long-term memory after working memory processes it. Miller (1956) found that the working memory is limited in such a way that the human mind can only hold seven items simultaneously. Hogg (2007) further stated that working memory is limited, which makes it difficult for humans to process complex tasks. He further defined cognitive load as “the processing of information that occurs in working memory” (p. 188). The limitations of the user’s memory can affect the ability to remember complex passwords (Boechler, 2006). Novakovic et al. (2009) also pointed out that requiring users to constantly change strong passwords places a high cognitive load on them.

Research Problem and Hypotheses

The research problem that this study addressed was the obstacle of password memorability, which is further complicated by the fact that users have many passwords to recall for computers, networks, and Websites among other systems (Wiedenbeck, Waters, Birget, Brodskiy, & Memon, 2005). Wiedenbeck et al. (2005) further noted that passwords have to be constantly changed in order to improve security, which increases the burden on the human mind and makes it difficult for users to remember their passwords. Henry (2007) pointed out that an infrequently used password that must be changed constantly, along with other security countermeasures, increases the cognitive load on users. Kinsbourne and George (1974) determined limitations to the human memory that affect humans' ability to recall complex passwords that must be constantly changed. Thus, the need for this work is demonstrated by the work of Novakovic, McGill, and Dixon (2009). In their work, Novakovic et al. (2009) acknowledged that passwords are the main way of authenticating users, and that it needs be complex enough to prevent easy guessing. They also pointed out the challenge of increasing password security, which results in a negative impact on usage. Cahill, Martin, Phegade, Rajan, and Pagano (2011) also demonstrated how increasing password complexity requirements can lead to problems when users have hard times remembering the requirements. The main goal of this study was to assess the effects of raising the cognitive load of the authentication strength for users upon accessing a system. This study also assessed the point at which raising the authentication strength for passwords becomes counterproductive. There were three groups as shown in Table 2a and 2b. Group A was the increase-decrease password strength group, Group B was the decrease-increase password strength group, and Group C was the fixed password strength group. Based on the literature, we have the drafted the following hypotheses for this research study (noted in null layout):

H1: There will be no significant differences on the *number of failed OS logon attempts* between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C).

H1a: There will be no significant differences on the *number of failed OS logon attempts* between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) *when controlling for computer experience*.

H1b: There will be no significant differences on the *number of failed OS logon attempts* between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) *when controlling for age*.

H1c: There will be no significant differences on the *number of failed OS logon attempts* between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) *when controlling for gender*.

H2: There will be no significant differences on the *average logon times* between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C).

H2a: There will be no significant differences on the *average logon times* between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) *when controlling for computer experience*.

H2b: There will be no significant differences on the *average logon times* between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) *when controlling for age*.

H2c: There will be no significant differences on the *average logon times* between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) *when controlling for gender*.

H3: There will be no significant differences on the *average task completion times* between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C).

H3a: There will be no significant differences on the *average task completion times* between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) *when controlling for computer experience*.

H3b: There will be no significant differences on the average *task completion times* between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) *when controlling for age*.

H3c: There will be no significant differences on the *average task completion times* between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) *when controlling for gender*.

H4: There will be no significant differences on the *number of requests for assistance (unlock and reset account)* between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C).

H4a: There will be no significant differences on the *number of requests for assistance (unlock and reset account)* between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) *when controlling for computer experience*.

H4b: There will be no significant differences on the *number of requests for assistance (unlock and reset account)* between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) *when controlling for age*.

H4c: There will be no significant differences on the *number of requests for assistance* (unlock and reset account) between the increase-decrease password strength group (A), decrease-increase password strength group (B), and fixed password strength group (C) *when controlling for gender*.

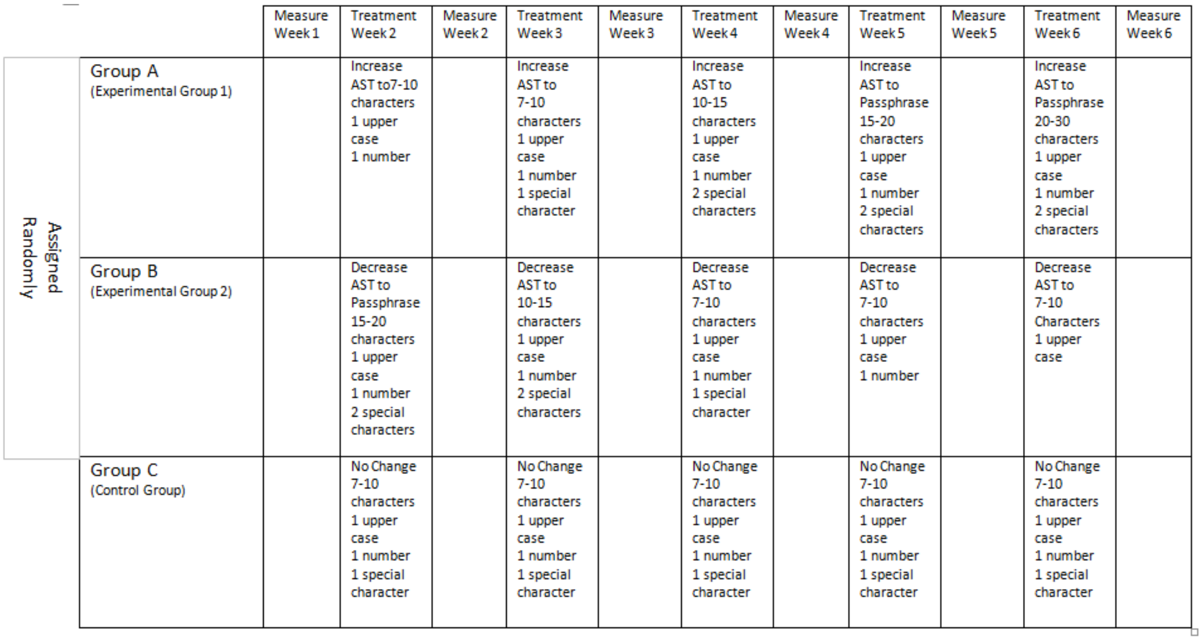
Methodology

To investigate the effects of increasing password strength, a lab experiment was used. Three random groups, two experimental and one control were used (Ellis & Levy, 2011). This research investigated the point at which passwords become too complex for users and become counterproductive. Two experimental groups (Group A & Group B) were constructed with 24 users in each group. A third group (Group C, fixed password strength) was constructed as the control group, and it had 24 users. The study participants in the three groups came from a local college in different majors at different levels in their academic levels. Lutu (2005) confirmed that a sample size is considered statistically valid if it has a true representation of the database from which it was selected. All users in the three groups were randomly assigned to one of the groups. The experiment was conducted over a period of 11 weeks. To test the effects of increasing password strength, a system was be set up and all three groups were asked to logon to the system. Once logged in, the users were asked to perform specific tasks. The system tracked the average number of failed logon attempts, average logon times, average task completing, and number of requests for assistance (unlock & resent account). These were tracked for all the three groups. The system had auditing mechanisms built in to track and measure all the tasks above. The users had different password strengths required based on the group membership and time within the experiment. The first experimental group (Group A, increase-decrease password strength) began with a password that was at least seven characters long, with one uppercase letter, in week one. As listed in Table 2a, the authentication strength increased in week two through week six, and their performance was measured during each week based on:

- Average number of failed OS logon attempts (NFOLA)
- Average logon times (ALT)
- Average task completion times (ATCT)
- Number of requests for assistance (unlock and reset account) (ARA)

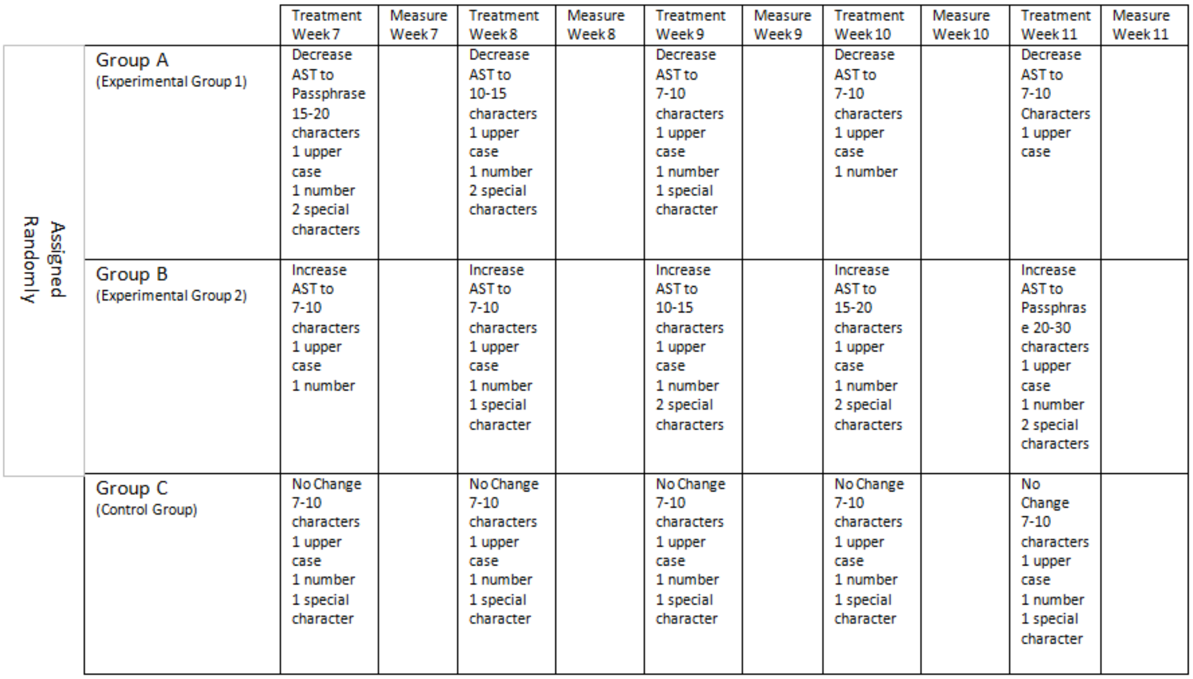
The authentication strength was the strongest in week six, when it increased to include a passphrase with 20-30 characters, one uppercase letter, one number, and two special characters. After the performance was measured, it began to decrease in weeks seven through week 11 and the performance was measured in each of those weeks as well. The second experimental group (Group B, decrease-increase password strength) began in week one with a password that included a passphrase with 20-30 characters, one uppercase letter, one number, and two special characters. As listed in Table 2a, it decreased each week until week six when it was 7-10 characters with one uppercase letter. The performance for Group B was measured during each week based on the same criteria that was used for Group A. As listed in Table 2b, the password strength for Group B began to increase in week seven through week 11 and the performance was measured each week as well. Figure 1 illustrates how the password strength was manipulated throughout the experiment.

Table 2a: Experimental Design – Authentication Strength (AST) – Week One to Week Six



		Measure Week 1	Treatment Week 2	Measure Week 2	Treatment Week 3	Measure Week 3	Treatment Week 4	Measure Week 4	Treatment Week 5	Measure Week 5	Treatment Week 6	Measure Week 6
Assigned Randomly	Group A (Experimental Group 1)		Increase AST to7-10 characters 1 upper case 1 number		Increase AST to 7-10 characters 1 upper case 1 number 1 special character		Increase AST to 10-15 characters 1 upper case 1 number 2 special characters		Increase AST to Passphrase 15-20 characters 1 upper case 1 number 2 special characters		Increase AST to Passphrase 20-30 characters 1 upper case 1 number 2 special characters	
	Group B (Experimental Group 2)		Decrease AST to Passphrase 15-20 characters 1 upper case 1 number 2 special characters		Decrease AST to 10-15 characters 1 upper case 1 number 2 special characters		Decrease AST to 7-10 characters 1 upper case 1 number 1 special character		Decrease AST to 7-10 characters 1 upper case 1 number		Decrease AST to 7-10 Characters 1 upper case	
	Group C (Control Group)		No Change 7-10 characters 1 upper case 1 number 1 special character		No Change 7-10 characters 1 upper case 1 number 1 special character		No Change 7-10 characters 1 upper case 1 number 1 special character		No Change 7-10 characters 1 upper case 1 number 1 special character		No Change 7-10 characters 1 upper case 1 number 1 special character	

Table 2b: Experimental Design – Authentication Strength (AST) – Week Seven to Week 11



		Treatment Week 7	Measure Week 7	Treatment Week 8	Measure Week 8	Treatment Week 9	Measure Week 9	Treatment Week 10	Measure Week 10	Treatment Week 11	Measure Week 11
Assigned Randomly	Group A (Experimental Group 1)	Decrease AST to Passphrase 15-20 characters 1 upper case 1 number 2 special characters		Decrease AST to 10-15 characters 1 upper case 1 number 2 special characters		Decrease AST to 7-10 characters 1 upper case 1 number 1 special character		Decrease AST to 7-10 characters 1 upper case 1 number		Decrease AST to 7-10 Characters 1 upper case	
	Group B (Experimental Group 2)	Increase AST to 7-10 characters 1 upper case 1 number		Increase AST to 7-10 characters 1 upper case 1 number 1 special character		Increase AST to 10-15 characters 1 upper case 1 number 2 special characters		Increase AST to 15-20 characters 1 upper case 1 number 2 special characters		Increase AST to Passphrase 20-30 characters 1 upper case 1 number 2 special characters	
	Group C (Control Group)	No Change 7-10 characters 1 upper case 1 number 1 special character		No Change 7-10 characters 1 upper case 1 number 1 special character		No Change 7-10 characters 1 upper case 1 number 1 special character		No Change 7-10 characters 1 upper case 1 number 1 special character		No Change 7-10 characters 1 upper case 1 number 1 special character	

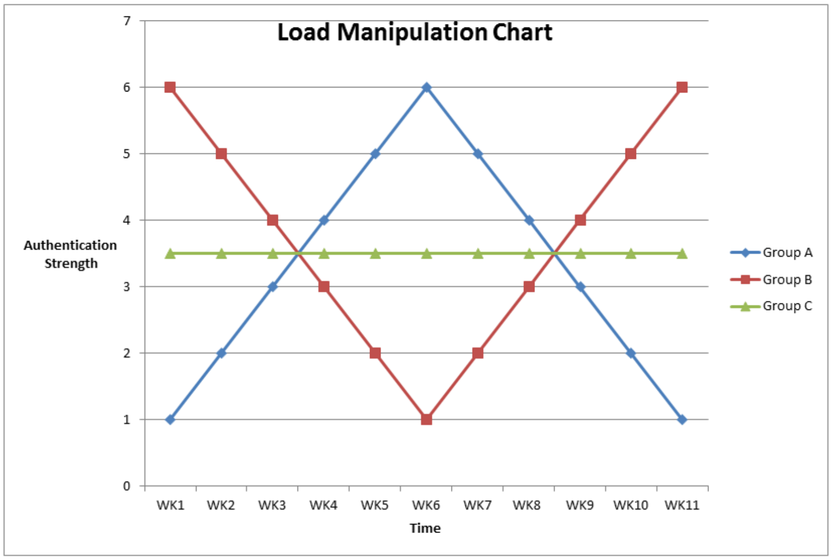


Figure 1: Load Manipulation Chart of the Authentication Strength for the Three Groups

Instrument Validity and Reliability

Trochim and Donnelly (2008) defined validity as the best available approximation to the truth of a given proposition, inference, or conclusion and reliability as repeatability and consistency. In this study, the pretest-posttest with control group design was used because of its strength in controlling threats to internal validity (Campbell & Stanley, 1963). Straub (1989) mentioned internal validity as one that asks the question whether observed effects or results could have been caused by unmeasured variables. Campbell and Stanley (1963) defined internal validity as “the basic minimum without which any experiment is uninterpretable: Did in fact the experimental treatments make a difference in this experimental instance?” (p. 5). There were several threats to internal validity that were addressed in this study. The first one had to deal with users selecting the option of saving their passwords or writing them down. Measures were put in place to ensure participants did not have the ability to save passwords or write them down. The use of notebooks or any electronic devices was prohibited during the experiment. For the average logon times and average task completion times variables, a program called Vision was used to block access to desktops before tasks are given so that participants begin at the same time. Interruptions during task could also affect the results and, therefore, measures will be put in place to control every interruption. The network was fully tested to ensure the Active Directory authentication server was available during the experiment time. The fact that the sample size in this study was homogeneous was important as it provided additional validity for the measured effect of the treatment (Levy & Ellis, 2011).

Data Analysis

Before the collected data could be analyzed, a pre-analysis data screening was conducted. Levy (2006) has identified some reasons for the pre-analysis data screening to take place. The process of pre-analysis data screening was helpful in increasing the validity of the results as well as the accuracy of the data being analyzed. A visual inspection on the data was conducted to make sure that there was no missing data. The Mahalanobis Distance analysis was carried out on the data to identify any multivariate outliers. One case was identified as a multivariate outlier, and was removed from the data set prior to further analysis. Mertler and Vannatta (2010) noted the multivariate analysis of covariance (MANCOVA) as a test that investigates group differences when there is one independent variable affecting two or more dependent variables. The MANOVA test was used to assess group differences for the four variables of NFOLA, ALT, ATCT, and ARA (H1, H2, H3, & H4). These tests were helpful in determining if there were any differences between the control group (C) and the increase-decrease password strength group (A), as well as the decrease-increase password strength groups (B). Additionally, the MANCOVA was used to test the group differences on NFOLA, ALT, ATCT, and ARA when controlling for computer experience, gender, and age. The main difference between the multivariate analysis of variance MANOVA and MANCOVA is that the latter allows for adjusting with one or more covariates (Mertler & Vannatta, 2010), thus, it was used on the hypotheses for the covariate analysis (H1a-H1c, H2a-H2c, H3a-H3c, & H4a-H4c).

Results

The results of this study are three folds. First, the pretest-posttest experiment surveys were administered to reveal if there were any differences in the users' perceptions about passwords before the experiment as well as after the experiment. Second, after data collection from 72 users, our results revealed if there are statistical differences between group A, groups B, and group C for the four variables of NFOLA, ALT, ATCT, and ARA. These tests were helpful in determining if there were any differences. Last, the results revealed if there were any significant differences on the measured variables when controlling for computer experience, age, and gender. The MANOVA was conducted on the data collected from the pretest-posttest experiment surveys. The results from the MANOVA test indicated that there is a statistical difference between the user's perceptions about passwords before the experiment and after the experiment (F = 1.210, p = 0.029) among the groups. Figures 2a, 2b, and 2c show the both the mean and standard deviation (SD) results for both the pretest and posttest questions. Furthermore, Tables 3a and 3b show the mean (M) of all the eight questions given to students during the pretest surveys and the posttest surveys.

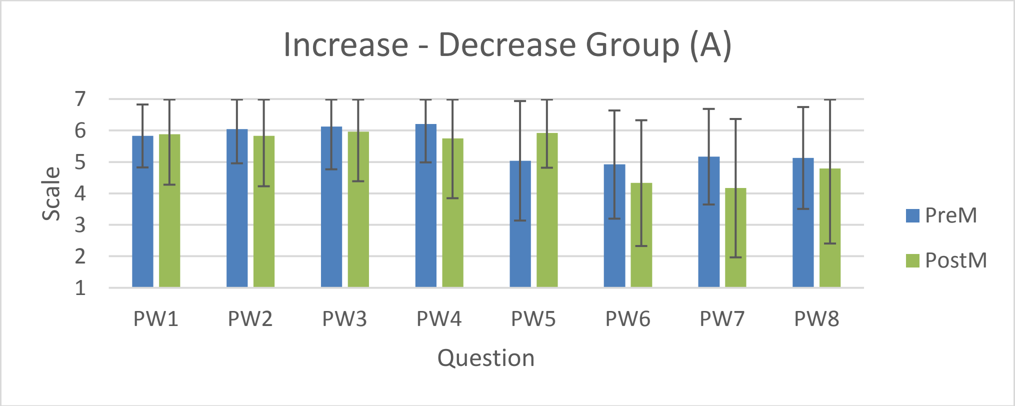


Figure 2a. Pretest-Posttest Experiment Survey Results (Mean & SD) – Group A

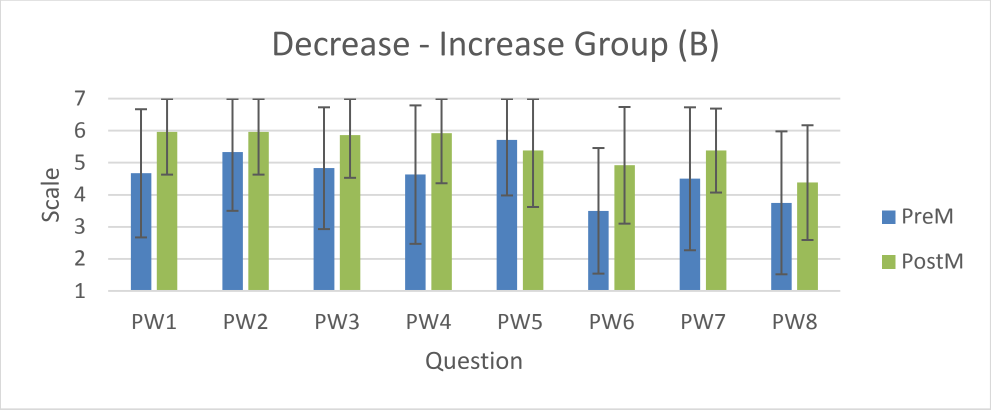


Figure 2b. Pretest-Posttest Experiment Survey Results (Mean & SD) – Group B

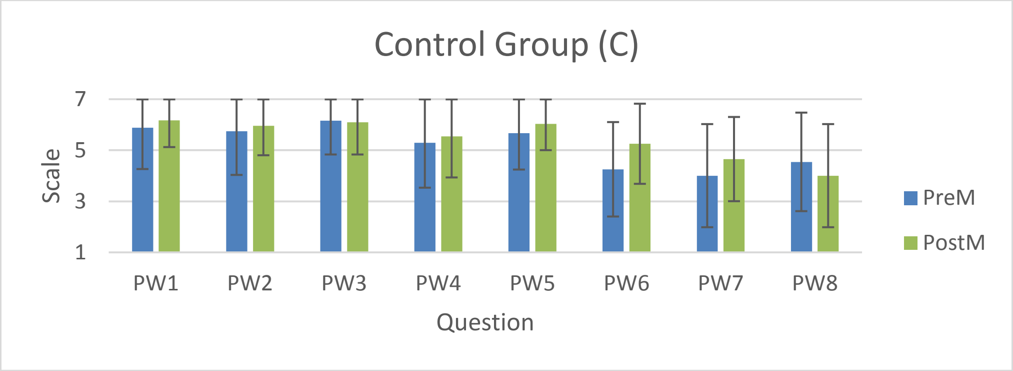


Figure 2c. Pretest-Posttest Experiment Survey Results (Mean & SD) – Group C

Table 3a. Pretest Mean and Posttest Mean for Survey Questions by Group

	PW1		**PW2**		**PW3**		**PW4**	
Group	**Pre M**	**Post M**	**Pre M**	**Post M**	**Pre M**	**Post M**	**Pre M**	**Post M**
A	5.83	5.88	6.04	5.83	6.13	5.96	6.21	5.75
B	4.67	5.96	5.33	5.96	4.83	5.86	4.63	5.92
C	5.88	6.17	5.75	5.96	6.16	6.10	5.29	5.54

Table 3b. Pretest Mean and Posttest Mean for Survey Questions by Group

	PW5		**PW6**		**PW7**		**PW8**	
Group	**Pre M**	**Post M**	**Pre M**	**Post M**	**Pre M**	**Post M**	**Pre M**	**Post M**
A	5.04	5.92	4.92	4.33	5.17	4.17	5.13	4.79
B	5.71	5.38	3.50	4.92	4.50	5.38	3.75	4.38

C	5.67	6.04	4.25	5.25	5.29	4.65	4.54	4.00

The MANOVA test was used to assess group differences for the four variables of NFOLA, ALT, ATCT, and ARA. These tests were helpful in determining if there were any differences between the increase-decrease password strength group (A), the increase-increase password strength groups (B), and the control group (C). When it comes to NFOLA, ALT, ATCT, and ARA between Groups A, B, and Group C, the MANOVA results indicated that there was a significant difference between the groups. The F test, which was used, was the Wilk's Lambda. The Box's Test was evaluated first as significant ($p < 0.001$, n=71). The Wilk's Lambda indicated a significant mean group differences in the three groups with respect to NFOLA, ALT, ATCT, and ARA, Wilks' $\Lambda = .889$, $F(8, 1570) = 11.88$, $p < .001$, multivariate .057. Table 4 presents means and standards deviations for NFOLA, ALT, ATCT, and ARA by the group category. Figures 3a-3d below also displays the graphs with the mean for NFOLA, ATL, ATCT, and ARA.

Table 4. Means and Standard Deviations for Variables by Group

	NFOLA		**ALT**		**ATCT**		**ARA**	
Group	**M**	**SD**	**M**	**SD**	**M**	**SD**	**M**	**SD**
A	.44	.90	1.27	.60	2.09	.53	.08	.27
B	.41	.96	1.39	.68	2.01	.63	.10	.30
C	.05	.28	1.07	.27	1.86	.41	.00	.60

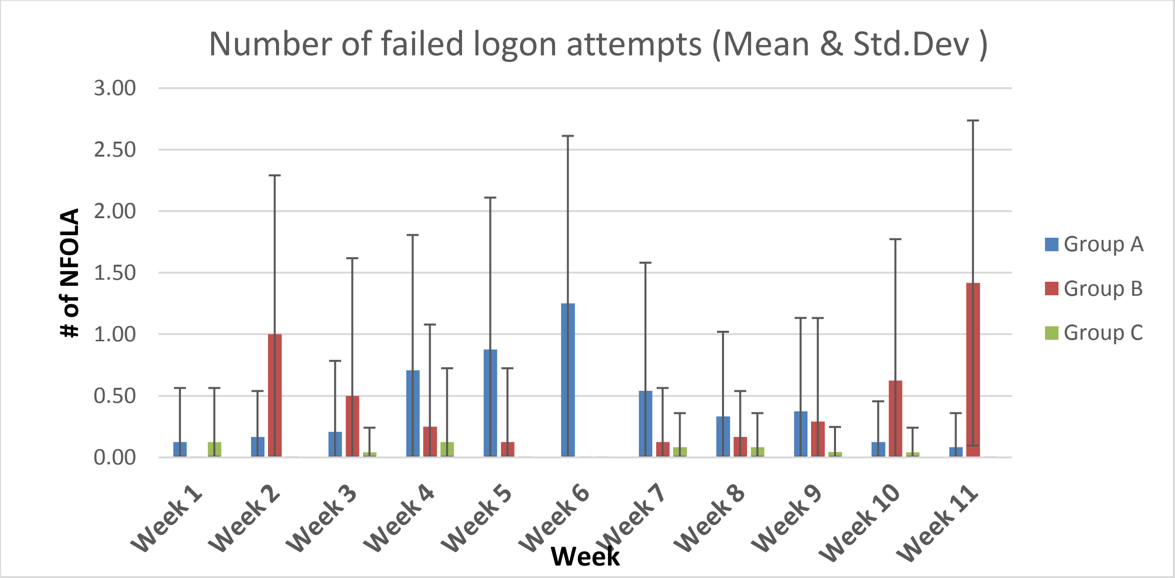


Figure 3a. Number of Failed Logon Attempts (NFOLA) Mean and SD

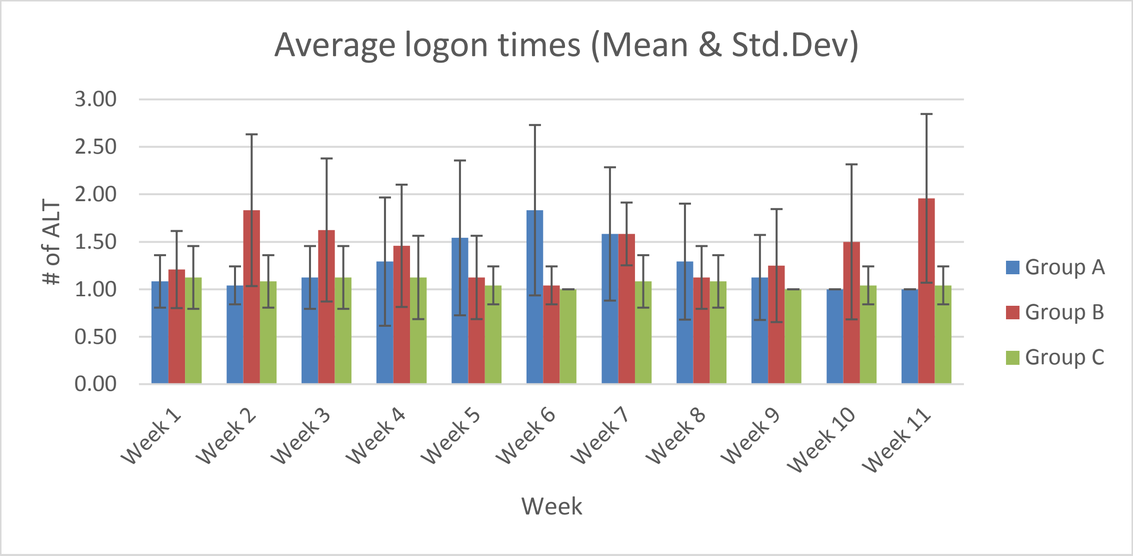


Figure 3b. Average Logon Times (ALT) Mean and SD

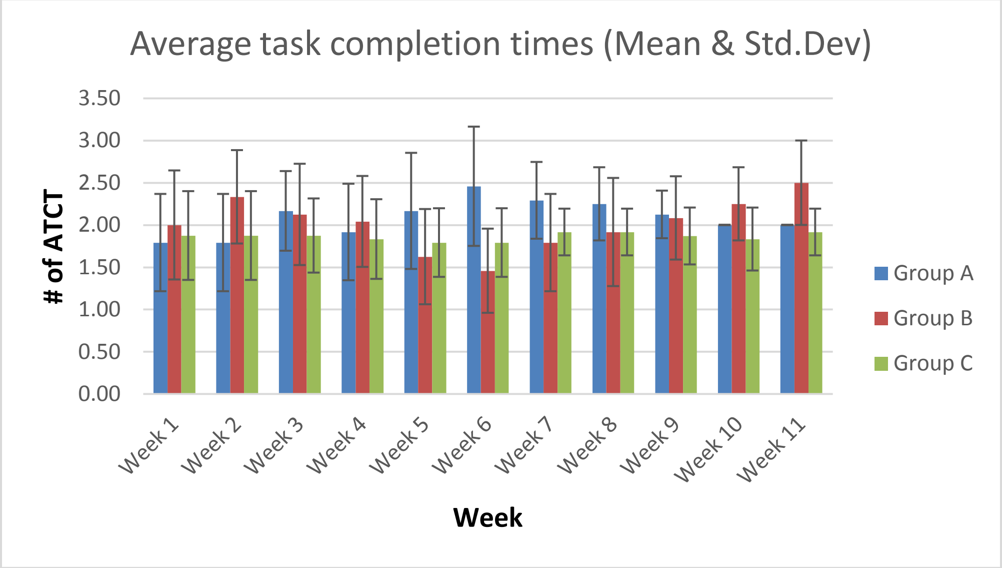


Figure 3c. Average Task Completion Times (ATCT) Mean and SD

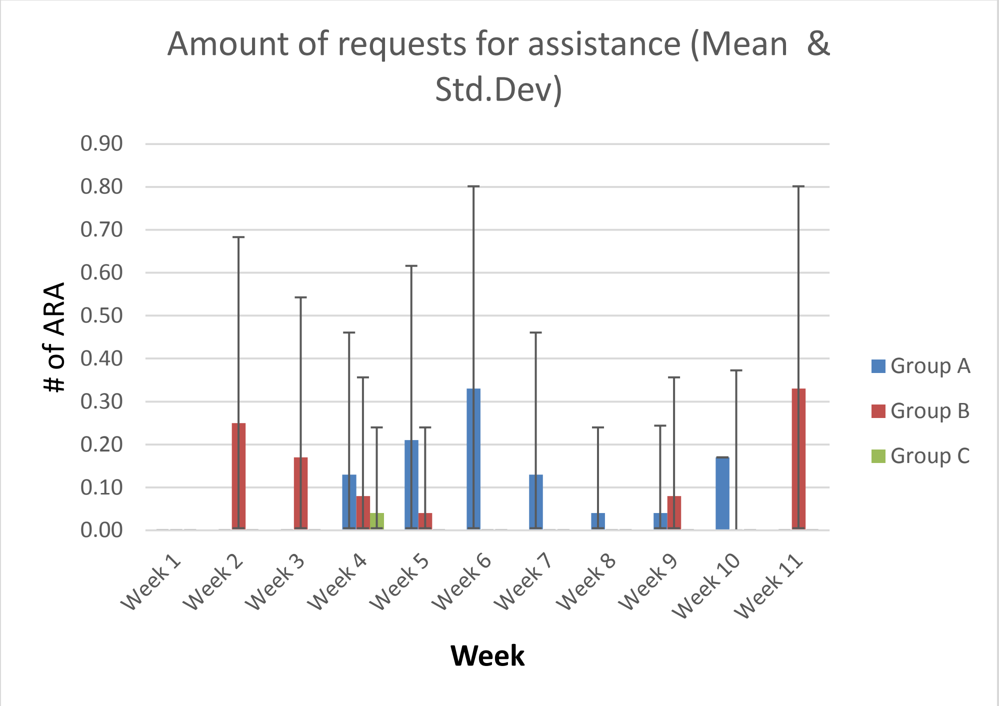


Figure 3d. Amount of Requests for Assistance (ARA) Mean and SD

Additionally, the MANCOVA was used to test the group differences on NFOLA, ALT, ATCT, and ARA when controlling for computer experience, gender, and age. The first covariate analyzed was computer experience. The MANCOVA results seem to suggest that the covariate of computer experience does not significantly influence the group differences, Wilks' Λ = .993, F (4, 784) = 1.36, p = .247, multivariate .007. When broken down by each variable, p = .17, .07, .96, .09 for NFOLA, ALT, ATCT, and ARA respectively. Table 5 shows the adjusted means (AM) and unadjusted means (UM) when controlling for computer experience.

Table 5. Adjusted and Unadjusted Means for Variables (Computer Experience)

	NFOLA		**ALT**		**ATCT**		**ARA**	
Group	**AM**	**UM**	**AM**	**UM**	**AM**	**UM**	**AM**	**UM**
A	.43	.44	1.27	1.27	2.10	2.09	.08	.08
B	.42	.41	1.38	1.39	2.00	2.01	.10	.10
C	.47	.05	1.07	1.07	1.87	1.86	.00	.00

The second covariate analyzed was gender. The MANCOVA results seem to suggest that the covariate of gender does not significantly influence group differences, Wilks' Λ = .996, F (4, 820) = .82, p = .512, multivariate .004. When broken down by each variable, p = .32, .82, .91, .26 for NFOLA, ALT, ATCT, and ARA respectively. Table 6 shows the adjusted means (AM) and unadjusted means (UM) when controlling for gender.

Table 6. Adjusted and Unadjusted Means for Variables (Gender)

	NFOLA		ALT		ATCT		ARA	
Group	**AM**	**UM**	**AM**	**UM**	**AM**	**UM**	**AM**	**UM**
A	.44	.44	1.27	1.27	2.09	2.09	.08	.08
B	.41	.41	1.39	1.39	2.00	2.01	.10	.10
C	.05	.05	1.07	1.07	1.86	1.86	.00	.00

The third covariate analyzed was age. The MANCOVA results seem to suggest that the covariate of age does not significantly influence group differences, Wilks' Λ = .993, F (4, 784) = 1.34, p = .254, multivariate .007. When broken down by each variable, p = .53, .38, .03, .79 for NFOLA, ALT, ATCT, and ARA respectively. Table 7 shows the adjusted means (AM) and unadjusted means (UM) when controlling for age.

Table 7. Adjusted and Unadjusted Means for Variables (Age)

	NFOLA		ALT		ATCT		ARA	
Group	**AM**	**UM**	**AM**	**UM**	**AM**	**UM**	**AM**	**UM**
A	.44	.44	1.27	1.27	2.09	2.09	.08	.08
B	.41	.41	1.39	1.39	2.01	2.01	.10	.10
C	.48	.05	1.07	1.07	1.86	1.86	.00	.00

Discussions and Conclusions

The results of this study answered the main research question, which was: At what point does the increase of the cognitive load (via different password strengths) become counterproductive to the organization by causing an increase in number of failed OS logon attempts, users' average logon times, average task completion times, and number of requests for assistance (unlock & reset account)? Figure 3a reveal an increase in the number of filed OS logon attempts over the weeks with the highest in Week 5 and 6 for Group A as well a Week 10 and 11 for Group B. The mean for the mentioned weeks are also at their highest level. Table 2a shows that the authentication strength for Group A is a passphrase with 15-20, 1 uppercase, 1 number, and two special characters in Week 5. Group B has the same strength in Week 10 as revealed in Table 2b. The results, therefore, suggest this is the point where users start having a sharp increase in NFOLA. Weeks 6 and 11 in Groups A and B respectively have the same authentication strength except that the characters in the passphrase are increased to 20-30 characters. The NFOLA is at its highest point in those weeks.

Figure 3b reveal the average logon times increasing over the weeks as the authentication strength is raised for both Group A and B. The highest increase appear to be in Week 6 for Group A and Week 11 for Group B. The same pattern was also observed on the mean for ATCT and ARA. The mean for Group C which has an authentication strength of 7-10 characters, one uppercase, one number, and one special character stay about the same for NFOLA, ALT, ATCT, and ARA throughout the 11-week experiment time. It therefore appears that when the authentication strength is stronger than 7-10 characters, one uppercase, one number, and one special character it becomes counterproductive. The second question was: At what point does such increase become counterproductive to the organization when controlled for computer experience, age and gender? This study answered this question in that results did not show any differences when the controlled for computer experience, age and gender.

Recommendations and Future Research

This research study was conducted at a two-year college. Future studies will be required to replicate the findings at other organizations and government agencies. The majority of participants in this study were in the 18-25 age range, performing a similar study with a wider frequency age is recommended. As it relates to conducting this research over an 11-week period and changing the password every week, it may be meaningful to repeat the study over a longer period requiring users to change the passwords over a longer period than a week. Future studies could also explore the possibility of educating users on the benefits of security as it relates to passwords and authentication strength. While the pretest and posttest were used, there was no training or awareness about information security.

Acknowledgement

We would like to thank the anonymous referees for their careful review and valuable suggestions. We also would like to thank Dr. Nitza Geri, Co-Program Chair, for her recommendations and constructive comments.

References

Bard, M. (2007). Spelling-error tolerant, order-independent pass-phrases via the damerau-levenshtein string-edit distance metric. *Proceedings of the fifth Australasian symposium on ACSW frontiers*, Darlinghurst, Australia, pp. 117-124.

Boechler, P. (2006). Understanding cognitive processes in educational hypermedia. *In C. Ghaoui (Ed.), Encyclopedia on Human Computers Interaction*, (648-651). Hershey, PA: Information Science Reference. doi:10.4018/978-1-59140-562-7.ch097

Brostoff, S., & Sasse, M. (2000). Are passfaces more usable than passwords? A field trial investigation. *Proceedings of the Human Computer Interactions Conference 2000*, London, UK, pp. 405-424.

Cahill, C. P., Martin, J., Phegade, V., Rajan, A., & Pagano, M. (2011). Client-based authentication technology: user-centric authentication using secure containers. *Proceedings of the Seventh ACM Workshop on Digital Identity Management*, New York, NY, pp. 83-92.

Carstens, D., McCauley-Bell, P., Malone, L., & DeMara, R. (2004). Evaluation of the human impact of password authentication practices on information security. *Information Science Journal*, *7*(1), 67-85.

Chiasson, S., Forget, A., Stobert, E., van Oorschot, P. C., & Biddle, R. (2009). Multiple interference in text passwords and click-based graphical passwords. *Proceedings of the 16th ACM Conference on Computer and Communications Security*, Swinton, UK, pp. 500-511.

Erlich, Z., & Zviran, M. (2010). Goals and practices in maintaining information systems security. *International Journal of Information Security and Privacy, 4*(3), 40-50. doi: 10.4018/jisp.2010070103

Erlich, Z., & Zviran, M. (2009). Authentication methods for computer systems security. In Khosrow-PourM. *Encyclopedia of information science and technology*. (Vol. 1, pp. 288-293). Hershey, PA: Information Science Reference. DOI: 10.4018/978-1-60566-026-4.ch049

Henry. P. T. (2007). *Toward usable, robust memometric authentication: An evaluation of selected password generation assistance*. Dissertation Abstracts International, 68 (09), (UMI No. AAT 3282618). Retrieved March 31, 2013 from Digital Dissertations database.

Hogg, N. (2011). Measuring cognitive load. *Handbook of Research on Electronic Surveys and Measurements*, 188-194. Hershey, PA: Information Science Reference. DOI: 10.4018/978-1-59140-792-8.ch020

Inglesant, P., & Sasse, M. (2010). The true cost of unusable password policies: password use in the wild. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. New York, NY, pp. 383-392.

Kim, I. (2012). Keypad against brute force attacks on smartphones. *Institution of Engineering and Technology*. *6*(2), 71-76.

Kinsbourne, M., & George, J. (1974). The mechanics of the word frequency effect on recognition memory. *Journal of Verbal Learning and Verbal Behavior*, 13, 63-69.

Kumari, K., & Chithraleka, T. (2012). A comparative analysis of access control policy modeling approaches. *International Journal of Secure Software Engineering, 3*(4), 65-83.

Levy, Y. (2006). *Assessing the value of e-learning systems*. Hershey, PA: Information Science.

Levy, Y., & Ellis, T. (2011). A guide for novice researchers on experimental and quasi-experimental studies in information systems research. *Interdisciplinary Journal of information, knowledge, and management*, 6, 151-161.

Levy, Y., Ramim, M. M., Furnell, S. M., & Clarke, N. L. (2011). Comparing intentions to use university-provided vs. vendor-provided multibiometric authentication in online exams. *Campus-Wide Information Systems*, *28*(2), 102-113. doi:10.1108/10650741111117806

Lutu, P. E. (2005). Database sampling for data mining. In J. Wang (Ed.), *Encyclopedia of Data Warehousing and Mining* (pp. 344-348). Hershey, PA: doi:10.4018/978-1-59140-557-3.ch066

Menkus, B. (1998). Understanding the use of passwords. *Computers & Security*, *7*(2), 132-136.

Mertler, C. A., & Vannatta, R. A. (2010). *Advanced and multivariate statistical methods* (4th ed.). Glendale, CA: Pyrczak.

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

Molloy, I., & Li, N. (2011). Attack on the gridcode one-time password. *Proceedings of the 6th ACM symposium on information, computer and communications security*, New York, NY, pp. 306-315.

Novakovic, L., McGill, T., & Dixon, M. (2009). Understanding user behavior towards passwords through acceptance and use modeling. *International Journal of Information Security and Privacy*, *3*(1), 11-29.

Oreku, G., & Lin J. (2009). End user authentication (EUA) model and password for security. *Journal of Organizational and End User Computing*, *21*(2), 28-33.

Rane, S. & Sun W. (2010) Privacy preserving string comparisons based on Levenshtein distance. *Information Forensics and Security (WIFS), 2010 IEEE International Workshop,* Seattle, WA,pp.1-6. doi: 10.1109/WIFS.2010.5711449

Ren, X., & Wu, X. (2012). A novel dynamic user authentication scheme. *International Symposium on Communications and Information Technologies*, Gold Coast, Queensland, Australia, pp. 713-717.

Shay, R., Komanduri, S., Kelly, P., Leon, P., Mazurek, M., Bauer, L., Christin, N., & Cranor, L. (2010). Encountering stronger password requirements: user attitudes and behaviors. *Symposium on Usable Privacy and Security*. Redmond, WA, pp. 1-20.

Sweller, J. (1988). Cognitive load during problem solving: effect on learning. *Cognitive Science*, 12, 257-285.

Tsai, C., Lee, C., & Hwang, M. (2006). Password authentication schemes: current status and key issues. *International Journal of Network Security*, *3*(2), 101-115.

Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, A., & Memon, N. (2005) PassPoints: design and longitudinal evaluation of a graphical password system. *International Journal of Human-Computer Studies*, *63*(1-3), 102-127. doi:10.1016/j.ijhcs.2005.04.010

Authors' Biographies

Dr. Stephen Mujeye is a Networking instructor at McHenry County College, Crystal Lake, Illinois. He earned a Bachelor's degree with a double major in Business Management and Business Systems Support Specialist from Siena Heights University, Adrian, Michigan. He has a Master's degree in Information Resource Management from Central Michigan University, Mt. Pleasant, Michigan and completed his Ph.D. in Information Systems at Nova Southeastern University. He holds a number of industry certifications, including A+, Network+, Security+, and MCTS.

Dr. Yair Levy is a Professor at the Graduate School of Computer and Information Sciences at Nova Southeastern University and the director of the Center for e-Learning Security Research

(CeLSR). During the mid to late 1990s, he assisted NASA to develop e-learning systems. He earned his Bachelor's degree in Aerospace Engineering from the Technion (Israel Institute of Technology). He received his MBA with MIS concentration and Ph.D. in Management Information Systems from Florida International University. His current research interests include security issues with e-learning systems, cyber-security skills, and cognitive value of information systems. Dr. Levy is the author of 'Assessing the Value of e-Learning Systems' (2006). His research publications appear in numerous peer-reviewed journals and conference proceedings. Also, Dr. Levy has been serving as a member of conference proceedings committee for numerous scholarly conferences. Moreover, Dr. Levy has been serving as a referee research reviewer for hundreds of national and international scientific outlets. He is a frequent invited keynote speaker at national and international meetings on IS, Information Security, and online learning topics. Dr. Levy's teaching interests in the masters level include MIS, system analysis and design, information systems security, e-commerce, and Web development. His teaching interests in the doctoral level include Information Systems Development (ISD) and Advanced Multivariate Research Methods and Statistics. To find out more about Dr. Levy, please visit his site: http://scis.nova.edu/~levyy/

Dr. Herbert Mattord, CISM, CISSP completed 26 years of IT industry experience before joining the faculty at Kennesaw State University in 2002. He was the Manager of Corporate Information Technology Security at Georgia-Pacific Corporation, where much of his practical knowledge in information security was acquired. He is currently on the Faculty at Kennesaw State University with the rank of Associate professor where he teaches undergraduate courses in Information Security and graduate courses in Information Systems. He serve as the Assistant Chair of the Department of Information Systems and Associate Director of the KSU Center for Information Security Education. He is the co-author of several books published by Course Technology and an active researcher in information security management topics.

Dr. Wei Li is a professor in the College of Engineering and Computing at Nova Southeastern University. His research interests include attack modeling and simulation, intrusion detection, firewall management, role-based access control, and the application of AI techniques in various security problems. He is a senior member of IEEE and a member of ACM.