

Password Policy Effects on Entropy and Recall: Research in Progress

Jim Marquardson

Center for the Management of Information, University of Arizona, Tucson, AZ, United States.,
jmarquardson@cmi.arizona.edu

Follow this and additional works at: <http://aisel.aisnet.org/amcis2012>

Recommended Citation

Marquardson, Jim, "Password Policy Effects on Entropy and Recall: Research in Progress" (2012). *AMCIS 2012 Proceedings*. 20.
<http://aisel.aisnet.org/amcis2012/proceedings/ISSecurity/20>

This material is brought to you by the Americas Conference on Information Systems (AMCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 2012 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

Password Policy Effects on Entropy and Recall: Research in Progress

Jim Marquardson
University of Arizona
jmarquardson@cmi.arizona.edu

ABSTRACT

Passwords are commonly used for authentication. System architects generally put in place password policies that define the required length of a password, the complexity requirements of the password, and the expiration (if ever) of the password. Password policies are designed with the intent of helping users choose secure passwords, and in the case of password expiration, limit the potential damage of a compromised password. However, password policies can have unintended consequences that could potentially undermine their security aims. Based on the theory of cognitive load, it is hypothesized that password policy elements increase extraneous load, which can result in high entropy passwords, but to the detriment of recall. It is further hypothesized that certain password policy elements can still help increase entropy, while minimizing the negative impact on recall. An experiment to test the hypotheses and determine both a secure and user friendly password policy is put forward.

Keywords

Password policy, password selection, password entropy, password recall, cognitive load theory

INTRODUCTION

Passwords are a common form of authentication in many systems today. In the future, biometric devices, secure tokens, or other schemes might take hold and change the landscape for authentication, but when it comes to authentication in today's world, the password reigns supreme. However, passwords have their shortcomings. Strong passwords are hard to remember, and weak passwords are easy to guess and therefore do not provide sufficient security. Problems with passwords for authentication have led some people to call for their abolishment in favor of different authentication methods (Farrell & College, 2008). Despite the weaknesses that passwords exhibit, we argue that sound password policy can help alleviate many of the problems with password strength and recall.

Common sense security says that users should choose secure passwords when creating accounts or resetting their passwords. The definition of a secure password, however, seems to differ from password policy to password policy. Most password policies enforce certain requirements such as password complexity, length, and expiration period. Password complexity and length help contribute to the password entropy. Entropy is used estimate the number of attempts it would take somebody to determine the password using a brute force search. Instructions displayed at the time of password selection about selecting a secure password influence password selection, at least to the point of satisfying the minimum requirements. Traditional password policies and password instructions may influence users to select weaker passwords because they influence users to select passwords that satisfy the minimum policy requirements that they can still remember.

Selecting a strong password that is memorable can take a non-trivial amount of effort. It might be feasible to remember a handful of strong passwords. But in today's world, people have to remember many passwords (Zhang, Luo, Akkaladevi, & Ziegelmayer, 2009). When counting websites, personal identification numbers of bank cards, wireless routers, and home computers, the average person clearly needs many passwords. One researcher did a thorough count and discovered that he personally has to manage 61 distinct passwords (Farrell & College, 2008). Logically, it becomes increasingly difficult to remember all passwords as the number of passwords increases.

Added to the fact the people have many passwords, many systems require that those passwords be changed periodically. Even if password changes are not required by systems, they are frequently recommended as best practices for managing personal computer security. However, to reduce the burden of password management, one strategy that many people adopt is to simply never change their passwords when it is optional. Then, passwords only have to be created and memorized once. When users know that a password will need to be changed because of a password expiration policy, users may anticipate the need to have to re-memorize a password, and therefore choose passwords that are simpler.

People do not use systems simply in order to practice security. People use systems because they create value in some way. In many instances, the security hoops that users have to jump through just to use systems are perceived as an impediment to getting things done and accomplishing the real work that they have to do. To some extent, those complaints are understandable. Research has shown that people have limited capacity for processing information (Miller, 1956). For example, users might be frustrated when they simply want to login to a system to check the status of an order, only to be told that their password has expired and they now need to select a new one. The effort of having to split cognition between two activities causes cognitive resources to be applied in ways that distract users from achieving their goals in using systems (Ginns, 2006). Ideally, people could devote all of their energies to the tasks that create value. Some users try to accomplish this by doing the absolute minimum possible to satisfy security requirements. For example, if a password policy requires numbers in addition to letter, the user might meet the requirement simply by adding a "1" to the end of a common word in a dictionary.

In this paper, entropy and recall are being analyzed because they represent two important factors when discussing systems: security and user satisfaction. If passwords are being used to help secure the system, high entropy passwords will strengthen security. Low entropy passwords can more easily be cracked or guessed, opening the underlying system to various exploits. Recall is related to user satisfaction because if users are unable to remember their passwords because they are too complex or change too frequently, they will be dissatisfied. This dissatisfaction could lead to insecure practices such as writing down the password. In one study, 55% of end users reported writing down their passwords (Summers & Bosworth, 2004). Making passwords easier to remember, and therefore eliminating the need to write them down, would improve overall system security. With this in mind, clearly the goals of security and user satisfaction are not mutually exclusive, but necessary complements to each other. A password policy must seek to attain high entropy of passwords that users can still recall.

This paper seeks to analyze how users react to various password policies and establishes a theoretical framework for analyzing password policies. The main elements of a password policy that will be addressed in this paper are the password length requirement, password complexity requirement, and password expiration. An experiment is proposed in which participants are given different password policies, and the entropy and recall of the passwords are tested. It is critical that more research be done on password policies and their effects on system security since poor password policies and potential misunderstandings about passwords may lead to less secure systems and more security breaches.

LITERATURE REVIEW

Password Problems

Several studies have analyzed password selection and password policies. This section of the paper addresses research regarding password policies, password recall, and password strength. Cognitive load theory, which provides the theoretical framework for the model put forth in this paper, is also addressed. Finally, the research opportunities are set forth.

Password Policy

A password policy can be defined as the required characteristics that a password must contain and the processes around password management. The most commonly adopted password policy elements are required password length, password complexity, and password expiration period. Password length is simply the minimum and maximum number of characters that a password must contain. Some policies only publish a minimum length, since it is assumed that most users will never choose passwords that reach the maximum storage limit set by the system. Password complexity is the required mix of alpha, numeric, and symbols required in a password. The most basic password complexity is a password comprised solely of lower case alpha characters. Some password policies require upper case letters, numbers, and symbols. Password expiration is the timer period for which a password can be used until the system forces the users to change their passwords. Length and complexity combine to make a password harder to guess or crack. Password expiration exists as a safeguard to limit damage for a password that might already be compromised.

Though internal organization password policies are seldom made public, websites often publish their password policies. Several top websites were analyzed, and the results showed that some allow very short passwords (as few as five characters), and only one surveyed required any non-alpha character (Furnell, 2007). Experience has shown that traditionally, corporations have much more stringent password policies. For example, the University of Cincinnati published its password policy online (Director, 2008). Amongst other requirements, their password policy states that, "No more than 4 characters from the existing password can be re-used in the new password you are creating." No doubt, that password policy causes many cognitive resources to be expended during the password change process. Researchers have issued their own guidance on elements of good password policy. For example, it has been suggested that passwords be between 6 and 10 characters long (Summers & Bosworth, 2004). The SysAdmin, Audit, Networking, and Security group (SANS) recommends that passwords be a minimum of 15 characters ("SANS Password Policy," 2011). Other research has assigned various levels of security

depending on the length of the password, where a password 4 characters or fewer is Level 1, and a password 16 characters or greater is Level 5 (Villarrubia, Fernandez-Medina, & Piattini, 2006). No justification for assigning specific password lengths to their respective levels was given. Unfortunately, the conflicting recommendations indicate uncertainty in the basis for the policies. It seems that most password policies have evolved over time by adopting a mix of current industry best practices. To our knowledge, no study has undertaken an effort to provide a theoretical basis for evaluating individual elements of password policy in order to maximize password policy effectiveness.

Research shows that compared to no password complexity requirements at all, implementing password complexity requirements does help users create stronger passwords (Campbell, Kleeman, & Ma, 2006). However, that same research showed that people have trouble remembering those passwords as early as a week later. Rather than focusing on no password policy versus a password policy, this research will compare the effects of password strength and recall among various different password policies.

Password complexity requirements still have limitations when it comes to password strength. A password can be technically complex, but still contain information that is easy to guess. For example, many users include information from their name and date of birth in their passwords (Campbell, Ma, & Kleeman, 2011). Passwords that simply satisfy the complexity requirements, but use user identifiable information might be relatively safe from dictionary attacks, but the password is much more likely to be guessed. This would especially be true for high value, public targets where a lot of information is known about them. Some have proposed using cognitive passwords that prompt users to enter information presumed to be known only to them, thereby eliminating the need to memorize a password which is a new piece of information (Kreider & Rao, 2010). However, just like traditional password schemes, cognitive password schemes could suffer from guessing attacks.

Password Recall

Since people have trouble remembering passwords, research identified ways to help users remember passwords. The mnemonic password technique (e.g. turning “My dog loves to chase cats” into the password “Mdlccc”) has been suggested as a way to create strong, yet memorable passwords. Unfortunately, research shows that prompting users to use mnemonic passwords does not help improve password security (Yan, Blackwell, Anderson, & Grant, 2004). Also, users typically choose convenience over security (Tam, Glassman, & Vandenwauver, 2010). For password policies to be truly effective, they must align with the user interest of permitting memorable passwords.

Some researchers have suggested *Password Rehearsal Games* as a means for helping users memorize passwords (Forget, Chiasson, & Biddle, 2008). While one can reasonably believe that a game could help improve password recall, in an ideal setting the cognitive effort to memorize the password and the time used to play the game could be put to better purposes.

Password Strength

Several studies have focused on detecting and encouraging password strength. For example, Spafford 1992 deemphasizes user education and encourages use of a custom dictionary scan to determine if a password is weak or strong, and whether or not the system should allow it. Another study looked at passwords from a historical University student database and analyzed them for strength. The study showed that 45% of passwords used were easy to crack using automated tools (Weber, Guster, Safonov, & Schmidt, 2008). To make passwords harder to guess and crack, some researchers have put forth the idea that strong passwords rely more on special characters and randomness rather than length (for example Riley, 2006). An additional study was done that required participants to satisfy seven different password criteria in order to make the passwords resilient against attacks (Vu et al., 2007). However, approximately half of the passwords could be cracked within four hours. Clearly, password complexity is not a silver bullet for password strength. It is interesting to note that in that research, passwords only had to be six characters long. The shortness of the passwords could have contributed greatly to the ability of the computers to crack the passwords so quickly. Other research has indicated that longer passwords may be more resilient against dictionary attacks and brute force attacks because of their higher entropy (Yan et al., 2004).

Cognitive Load

Cognitive load theory helps explain how cognitive resources are used when individuals learn and solve problems (Chandler & Sweller, 1991). This theory can also be applied to how people select and memorize passwords, as password selection and memorization is a form of learning. Three categories of cognitive load are described by cognitive load theory: intrinsic load, extraneous (or ineffective) load, and germane load (Paas, Renkl, & Sweller, 2003).

Intrinsic Load

Intrinsic load is the inherent difficulty in learning something. For example, learning a new word in a foreign language, or solving a calculus problem both have intrinsic cognitive load that cannot be reduced. Instructional materials cannot be redesigned to reduce intrinsic load.

Extraneous Load

Extraneous load detracts from intrinsic load by the nature of the way information is presented to the learner. When extraneous load is high, learners must expend cognitive resources on activities not directly related to understanding a concept or schema generation. For example, extraneous load would be high if an instructor tried to explain the concept of a triangle using descriptive words and technical language. A more effective approach that would reduce extraneous load would be simply to draw a triangle and then describe the important elements. Learning happens effectively when intrinsic load is high, and extraneous load is minimized. It has been theorized that user password training would help reduce extraneous load for password selection and memorization (Horcher & Tejay, 2009).

Germane Load

Germane load is the required mental load to acquire a new schema, or process information into a schema. As with extraneous load, germane load can be manipulated through the instructional design process. Prior training about password selection practices could contribute to lower germane load, but this potential effect is not treated in this paper.

Research Opportunities

There is a lot left to be researched regarding password selection and security. No research found has examined the effect of password expiration on password selection. No research found has strictly tried to determine memorability and security of password policies that focus on length rather than complexity. Prior research has established a link between passwords and cognitive load theory (Horcher & Tejay, 2009). However, this paper will look at the effects of extraneous load by means of password policy rather than through user training. This research could have significant impacts on organizational password policies. Organizations could be encouraged to drop the requirement to periodically reset passwords, increase the password length requirement, and reduce the password complexity requirements. The end result could be more secure and memorable passwords.

THE RESEARCH MODEL

The basis of the research model is cognitive load theory. Cognitive load theory suggests that people have limited working memory, but a virtually unlimited long-term memory (Paas, Tuovinen, Tabbers, & Gerven, 2003). Selection and memorization of a password fits into the working memory portion of cognitive load theory. In addition, it is theorized that more complex password policies increase extraneous load, thereby reducing the cognitive resources that people can apply to picking and recalling passwords.

In the process of selecting and memorizing a password, the password policy adds extraneous load. Not only do people have to select a password, but they have to expend mental effort ensuring that the password meets the requirements of the password policy. The more complicated a password policy is, the higher the extraneous load will be, and the less cognitive resources people will be able to apply to selecting and memorizing a password. People realize their own weaknesses in memorizing passwords, so if they are presented with an opportunity to reduce cognitive load on a less important task, they will take it in order to focus cognitive energy on a more important task. For example, if password policy increases extraneous load by requiring many special characters in a password, the user will have less cognitive resources available, and would compensate by choosing a shorter password. Also, a password policy requiring a password to be reset periodically also adds extraneous load. In this situation, the user will compensate by choosing a simpler password because it is easier to remember. Researchers have observed that people have difficulty remembering passwords (for example Zhang, Luo, et. al., 2009). It is hypothesized that all password policies add extraneous load to some extent. However, extraneous load should be minimized by choosing policies that minimize extraneous load while still maintaining high resulting password entropy and recall. As extraneous load decreases, more cognitive load can be applied to the intrinsic activity of selecting and memorizing a password. A user will be able to select passwords with more entropy and be able to memorize the passwords easier. In this way, the two goals of increasing user satisfaction and system security can both be attained.

Based on the theory of cognitive load, complexity, length, and expiration are expected to affect the entropy of selected passwords and the ability of users to recall those passwords. A more complex password policy will increase germane load, which will negatively affect password entropy and recall.

The password policy itself will also directly affect entropy and recall. Password policies that require a certain number of special characters and a minimum password length will directly influence password entropy. Also, complex password policies will result in passwords that are harder to remember compared to password policies with simple requirements.

The diagram in Figure 1 summarizes the research model. It is hypothesized that compared to a control, every password policy that establishes a length, complexity, or expiration requirement will increase extraneous load. However, the way the extraneous load is manifested in the resulting entropy and recall is hypothesized to be different based on the different

password policies. See Table 1 for a detailed explanation of the different hypotheses and the components of their password policies.

Examining Individual Password Policy Elements

Entropy is calculated using the formula $Entropy = \log_2 C * L$ where C is the number of characters in the potential character set, and L is the length of the password. Therefore, increasing C or L will have a positive impact on password entropy. Adding one bit of entropy doubles the number of possible passwords, and would therefore double the time it would take a brute force search to discover the password.

- *Length.* Longer passwords greatly increase the entropy of passwords. Essentially, the entropy of the password scales linearly with the length of the password.
- *Complexity.* Increasing the character set increases password entropy, but to a lesser degree than password length as demonstrated in the equation above. Essentially, there is a diminishing rate of return on entropy when increasing password complexity.
- *Expiration.* Whether or not a password expires should have no effect on the entropy of a password.

Recall is the ability to remember a password. Chunking theory is used to help determine how password policy elements would affect recall.

- *Length.* Longer passwords should still be memorable if there is no expiration requirement, and if it is devoid of special characters and numbers. Recall of longer passwords will be more difficult than shorter passwords simply because there are more characters to memorize. However, the detrimental effects of increasing password length are expected to be minimal, and significantly less than those of increasing password complexity and introducing an expiration requirement.
- *Complexity.* Requiring complex passwords that include capitalization, symbols, and numbers will harm recall. This is because it is easier for people to create a memory unit using words rather than with numbers and symbols (Baddeley, 2000).
- *Expiration.* It is hypothesized that introducing an expiration requirement will impede recall because of higher conflict between previous passwords that have been memorized (Stanton, Stam, Mastrangelo, & Jolton, 2005).

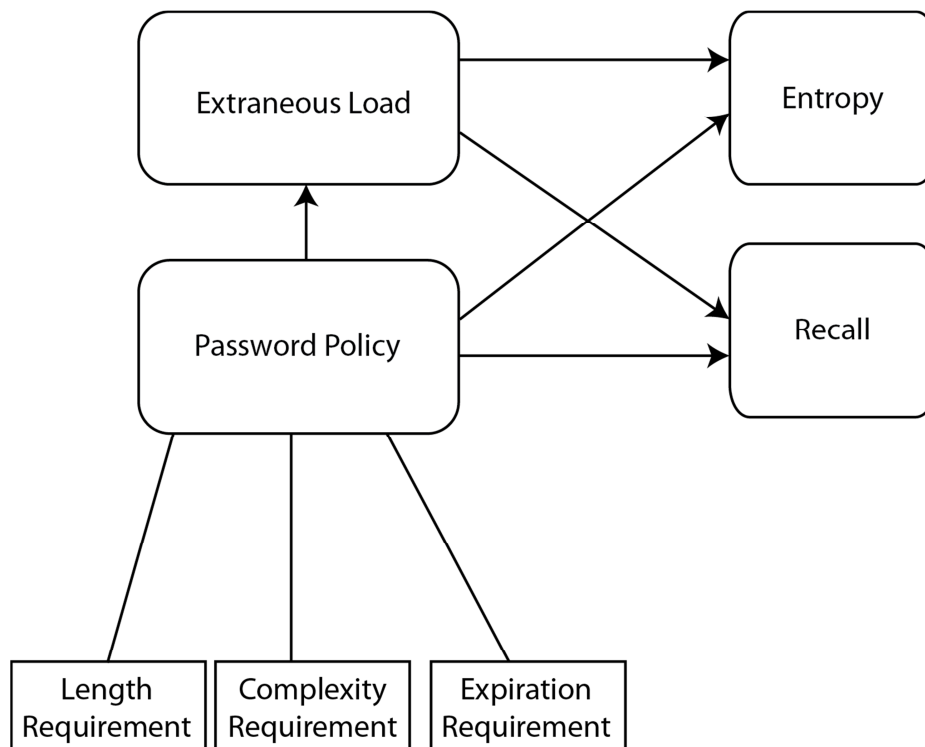
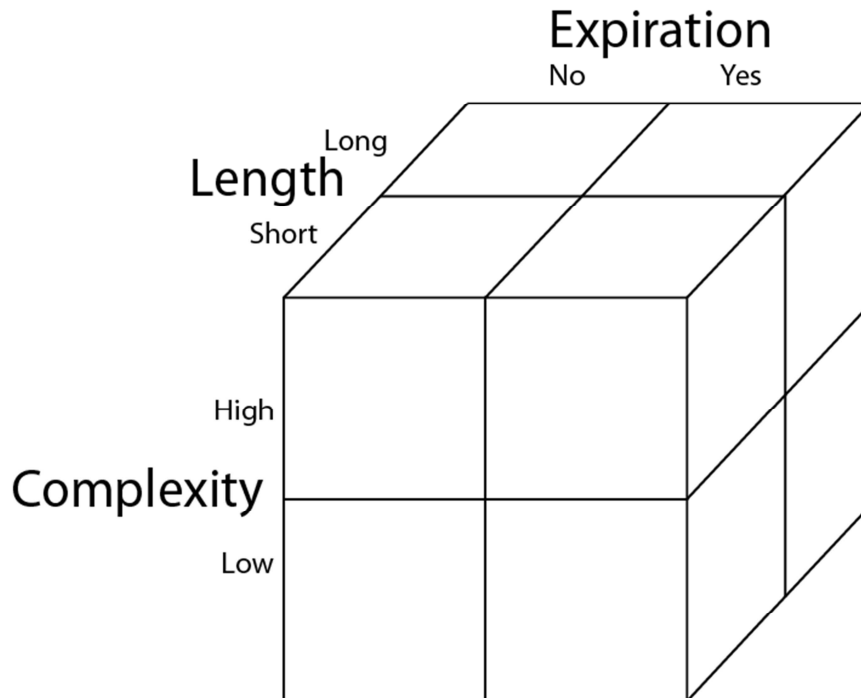


Figure 1. The research model.

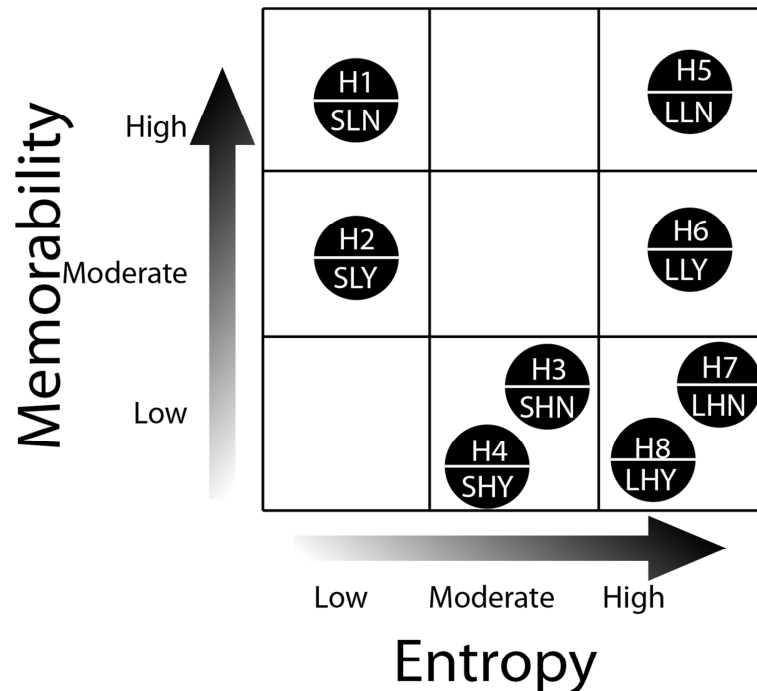
The following figure shows how the different password policy elements combine to create the different hypotheses which will translate into the different treatment groups.

**Figure 2. The password elements being hypothesized.**

The following table shows the different password policy hypotheses. Each hypothesis will correspond to a different treatment group. The length, complexity, and expiration are the elements of the password policy that compose each treatment.

	Minimum Length	Complexity Requirement	Expiration
H1	Short	Low	No
H2	Short	Low	Yes
H3	Short	High	No
H4	Short	High	Yes
H5	Long	Low	No
H6	Long	Low	Yes
H7	Long	High	No
H8	Long	High	Yes

The hypothesized entropy and hypothesized recall are low, moderate, or high. Entropy will be the number of calculated bits of entropy. Recall will be the percentage of people in the treatment who were able to successfully remember their passwords to login. A summary of the hypothesized results are shown in Figure 3. As it can be seen in the figure, H5 is the only treatment that is hypothesized to result in both high entropy and high recall. If the hypothesis is supported by the data, this is the type of password policy that should be encouraged and adopted by policy makers.



* The password policy code is length ([S]hort, [L]ong), complexity ([H]igh, [L]ow), and expiration ([Y]es, [N]o).

Figure 3. Summary of the hypothesized results.

METHODOLOGY

An experiment will be performed to test the hypotheses. Individuals participating in the research will be told that they need to create a username and password in a system. The participants will be told that for the purposes of the research, their passwords must be stored in clear text, but that they will not be revealed outside of the research. The participants will randomly be assigned into one of eight different treatment groups. A control group will not be given any password policy. Each treatment group will have a unique password policy composed of the complexity requirement (low or high), length (short or long), and expiration (no expiration or a defined expiration period). The password policy elements will be presented to the user at the time of password creation, and the system will enforce the password requirements. The passwords will be stored in clear text for analysis. After a week, the participants will be asked to login to the system again in order to test their recall. Invalid login attempts will be recorded. Even though some participants will be told that their password will expire, it is not necessary for this experiment to have them reset their password after the specified expiration period. We are only interested in how merely stating that a password will expire affects their initial password selection.

The entropy of the passwords created for the control and treatment groups will be analyzed. The entropy will be created using the following formula: $Entropy = \log_2 C * L$, where C is the character set and L is the length of the password. The character set will be inferred from the plaintext password. For example, a password containing only lower case letters will have a character set of 26. A password containing lower case letters and a number will have a character set of 36. Additionally, the ability to recall the passwords will be analyzed for the control and treatment groups. Whether or not the user was able to recall the password will be recorded as a Boolean value. A user will be given three chances to login, and if the password is entered correctly in those three attempts, recall will be considered successful.

It is acknowledged that using the character set and password length alone is not sufficient to measure password strength. For example, a user could select a very long word in a dictionary for a password. To account for this possibility, in addition to the calculated entropy, analysis will be done to determine if the participants' passwords are found in common password cracking dictionaries. Also, it would be helpful to ascertain if the participants wrote down the passwords that they created for the experiment. A follow-up survey would need to be administered to ask them about their password practices during the

experiment. The participants will need to be asked if they wrote the password down, and if so, how they wrote it down. For example, some participants might choose to record their password in a secure password manager, such as KeePass or LastPass. The results of that analysis might point to future research needs about the way users manage their passwords.

CONCLUSION

Passwords are fundamental to the security of many systems both on the internet and within organizations. Several studies have been done that look at different methods for memorizing passwords, ways to encourage users to select appropriate passwords, and factors that inhibit secure password practices. However, no research found has specifically looked at how password policy affects password entropy and recall through the lens of cognitive load theory. I believe that the insights gained from the proposed experiment would provide password policy makers with more useful information when creating password policies. For example, instead of requiring overly complex passwords, password policy makers should simply require longer passwords. This research would be relevant because it is hypothesized that user satisfaction through easier recall of passwords and higher system security through higher entropy passwords can be achieved simultaneously through better password policy. Since users are often considered the weakest link in the security chain, satisfying the users while promoting secure behavior is critical. This work could also lead future researchers to analyze other common security policies and their effects on user behavior and the resulting security implications.

ACKNOWLEDGMENTS

I would like to thank Dr. Alex Durcikova and Dr. Sue Brown for their generous guidance and feedback during the writing of this paper.

REFERENCES

1. Baddeley, A. (2000). The episodic buffer: a new component of working memory? *Trends in cognitive sciences*, 4(11), 417-423. Retrieved from <http://www.ncbi.nlm.nih.gov/pubmed/11058819>
2. Campbell, J., Kleeman, D., & Ma, W. (2006). Password Composition Policy: Does Enforcement Lead to Better Password Choices? *17th Australasian Conference on Information Systems* (pp. 1-9).
3. Campbell, J., Ma, W., & Kleeman, D. (2011). Impact of Restrictive Composition Policy on User Password Choices. *Behaviour & Information Technology*, 30(3), 379-388. doi:10.1080/0144929X.2010.492876
4. Chandler, P., & Sweller, J. (1991). Cognitive Load Theory and the of Instruction Format. *Cognition and Instruction*, 8(4), 293-332.
5. Director, U. of C. I. S. (2008). Password Policy. *Policy*. Retrieved from http://www.uc.edu/infosec/policy/Policy_Password_Policy_9_1_23.pdf
6. Farrell, S., & College, T. (2008). Password Policy Purgatory. *IEEE Internet Computing*, 12(5), 84-87.
7. Forget, A., Chiasson, S., & Biddle, R. (2008). Lessons from Brain Age on Password Memorability. *Future Play '08 Proceedings of the 2008 Conference on Future Play: Research, Play, Share* (pp. 262-263).
8. Furnell, S. (2007). An assessment of website password practices. *Computers & Security*, 26(7-8), 445-451. doi:10.1016/j.cose.2007.09.001
9. Ginns, P. (2006). Integrating information: A meta-analysis of the spatial contiguity and temporal contiguity effects. *Learning and Instruction*, 16(6), 511-525. doi:10.1016/j.learninstruc.2006.10.001
10. Horcher, A.-marie, & Tejay, G. P. (2009). Building a better password: The role of cognitive load in information security training. *2009 IEEE International Conference on Intelligence and Security Informatics* (pp. 113-118). Ieee. doi:10.1109/ISI.2009.5137281
11. Kreider, C., & Rao, V. S. (2010). User Acceptance of Multiple Password Systems: A Proposed Study. *AMCIS 2010 Proceedings* (pp. 1-8).
12. Miller, G. A. (1956). The Magical Number Seve, Plus or Minus Two: Some Limits on Our Capacity for Processing Information. *The Psychology Review*, 63(2), 81-89.
13. Paas, F., Renkl, A., & Sweller, J. (2003). Cognitive Load Theory and Instructional Design : Recent Developments. *Educational Psychologist*, 38(1), 1-4.

14. Paas, F., Tuovinen, J. E., Tabbers, H., & Gerven, P. W. M. V. (2003). Cognitive Load Measurement as a Means to Advance Cognitive Load Theory. *Educational Psychologist*, 38(1), 63-71.
15. Riley, S. (2006). Password Security : What Users Know and What They Actually Do. *Usability News*, 8(1).
16. SANS Password Policy. (2011, September). doi:10.1109/MIC.2008.108
17. Spafford, E. H. (1992). OPUS : Preventing Weak Password Choices. *Computers & Security*, 11(3), 273-278.
18. Stanton, J., Stam, K., Mastrangelo, P., & Jolton, J. (2005). Analysis of End User Security Behaviors. *Computers & Security*, 24(2), 124-133. doi:10.1016/j.cose.2004.07.001
19. Summers, W. C., & Bosworth, E. (2004). Password Policy : The Good , The Bad , and The Ugly. *WISICT '04 Proceedings of the winter international symposium on Information and communication technologies* (pp. 1-6).
20. Tam, L., Glassman, M., & Vandenwauver, M. (2010). The psychology of password management: a tradeoff between security and convenience. *Behaviour & Information Technology*, 29(3), 233-244. doi:10.1080/01449290903121386
21. Villarrubia, C., Fernandez-Medina, E., & Piattini, M. (2006). Quality of password management policy. *First International Conference on Availability, Reliability and Security (ARES'06)* (pp. 1-7). Ieee. doi:10.1109/ARES.2006.102
22. Vu, K.-P. L., Proctor, R. W., Bhargav-Spantzel, A., Tai, B.-L., Cook, J., & Eugeneschultz, E. E. (2007). Improving password security and memorability to protect personal and organizational information. *International Journal of Human-Computer Studies*, 65(8), 744-757. doi:10.1016/j.ijhcs.2007.03.007
23. Weber, J. E., Guster, D., Safonov, P., & Schmidt, M. B. (2008). Weak Password Security: An Empirical Study. *Information Security Journal: A Global Perspective*, 17(1), 45-54. doi:10.1080/10658980701824432
24. Yan, J., Blackwell, A., Anderson, R., & Grant, A. (2004). Password Memorability and Security: Empirical Results. *IEEE Security & Privacy*, 2(5), 25-31. doi:10.1109/MSP.2004.81
25. Zhang, J., Luo, X., Akkaladevi, S., & Ziegelmayer, J. (2009). Improving multiple-password recall: an empirical study. *European Journal of Information Systems*, 18(2), 165-176. doi:10.1057/ejis.2009.9