Helping Users Create Better Passwords: Is this the right approach?

Alain Forget
School of Computer Science
& Human-Oriented Technology Lab
Carleton University
aforget@scs.carleton.ca

Sonia Chiasson
School of Computer Science
& Human-Oriented Technology Lab
Carleton University
chiasson@scs.carleton.ca

Robert Biddle
Human-Oriented Technology Lab
Carleton University
robert_biddle@carleton.ca

ABSTRACT

Users tend to form their own mental models of good passwords regardless of any instructions provided. They also tend to favour memorability over security. In our study comparing two mnemonic phrase-based password schemes, we found a surprising number of participants misused both schemes. Intentional or not, they misused the system such that their task of password creation and memorization became easier. Thus, we believe that instead of better instructions or password schemes, a new approach is required to convince users to create more secure passwords. One possibility may lie in employing Persuasive Technology.

1. INTRODUCTION

Users tend to form their own mental models of security and what makes good passwords, which typically results in the creation of insecure but easily recalled passwords [1,2]. Therefore, assisting users in forming proper mental models is crucial to achieve greater security. Many approaches have been suggested to increase both password security and usability, such as password managers, graphical passwords, and phrase-based passwords; but none have proven widely acceptable.

Despite their usability and security limitations, there is incentive to ameliorate upon standard text-based passwords since they remain the most prevalent form of authentication. One suggested improvement is the use of mnemonic phrase-based passwords (herein called "*mnemonic passwords*") [5,6], where a password is based upon a memorable phrase. For example, the phrase "I have ten fingers and toes" could give "Ih10f&t" as a password. These offer a potential solution that requires little or no change in existing systems while promising increased memorability and security. We conducted a user study to evaluate the usability and security of two different mnemonic password schemes.

We discovered that while those participants who successfully created mnemonic passwords appeared to have stronger passwords, a large portion of participants opted for significantly weaker question-and-answer based passwords, reflecting inaccurate mental models of the system. Users tried to create the easiest-to-remember passwords, regardless of any instructions.

Submitted to the Symposium On Usable Privacy and Security (SOUPS) 2007, July 18-20, 2007, Pittsburgh, PA, USA

Version: May 24, 2007

2. BACKGROUND

In a study with 400 students, Yan et al. [6] found that mnemonic passwords were as secure as random passwords and more secure than standard passwords. Their evaluation was limited to guessing passwords using a standard password cracking dictionary and did not examine the mnemonic phrases chosen by participants.

Kuo et al. [5] collected survey data comparing standard passwords versus mnemonic passwords from 290 individuals. They found that the majority of mnemonic passwords were based on external sources, such as famous movie quotes or song lyrics. Thus, the passwords were found to be only as secure as regular passwords, if not less, since it would be trivial for attackers to build an attack dictionary based on such external sources.

Jeyaraman and Topkara [4] developed a system that would generate a fictitious news headline as a mnemonic phrase to assist users in remembering their password. Unfortunately, the system was only tested with randomly generated lowercase passwords, for which it managed to create mnemonic headlines for 80.5% and 62.7% of six- and seven-character passwords respectively. The usability and user acceptance of such a system was not evaluated.

3. STUDY METHODOLOGY

Sixteen university students, 8 male and 8 female, from various faculties and programs participated in our study, none specializing in computer security. A pre-test questionnaire revealed that approximately half of participants were concerned about the security of passwords yet all reported re-using passwords.

Participants were randomly assigned to either the self-constructed phrase group ("*Self*") or the pre-defined phrase group ("*Auto*"). For each trial, members of the Self group were required to create and input their own mnemonic phrase from which they then derived a password, whereas members of the Auto group were randomly given one of ten pre-defined phrases on which to base their password. Both groups created and confirmed their password, spent at least 30 seconds on a distraction task, and then logged in using their password without being prompted by the corresponding mnemonic phrase.

Participants received verbal instruction on how to create mnemonic passwords. They were also given a sheet of written instructions, including an example, and were advised to read the instructions before continuing with the experiment. Participants could refer to this sheet at any time during the session.

For each trial, the mnemonic phrase and all entered passwords were recorded. After successfully confirming their password, users answered two questions addressing the ease of password creation and perceived password memorability. Upon completion of ten trials, participants filled out a post-test questionnaire about their perceptions and attitudes on mnemonic passwords.

4. RESULTS AND DISCUSSION

Our experiment did not turn out the way we expected. Four of the eight participants in the Self group and two of the eight in the Auto group failed to use the mnemonic password system as intended. Instead of converting the phrase into a mnemonic, they interpreted their phrase as a question, giving their answer as their password. We identify this behaviour as question-and-answer or "*Q&A*". Conversely, those who used the system as intended are identified as the "*Mnemonic*" participants. During analysis, we discovered that this unexpected grouping of Q&A and Mnemonic better delineated behaviour than our intended experimental groups of Self and Auto. We hypothesise that Q&A participants formed inaccurate mental models of mnemonic passwords.

Visual inspection of the passwords revealed that those created through the Q&A method contained complete words and predictable numerical suffixes (such as "123"), and as such appear to be much weaker than those created using the intended Mnemonic method, which contained random parts of words, mixed cases, punctuation, and special characters.

Because our intention was for participants to choose mnemonic passwords, we investigated the prevalence of chatting acronyms in their passwords. We found that even when primed to use acronyms through an example in the instructions (and loading the phrases for the Auto group with commonly abbreviated words), only 36% of created passwords used chatting acronyms.

Despite this, letter sequences corresponding to chatting acronyms were common in all participants' passwords, even when participants were not intentionally using the acronyms as abbreviations. 95% of created passwords contained at least one such sequence of letters corresponding to an acronym found in Google's top ten search results containing lists of chat acronyms. The security impact of this finding may warrant further investigation.

Our small sample size meant that statistical significance was not reached on any of the following reported differences, but we believe that they are still worth noting and that a larger study would lead to statistically significant results. The post-test questionnaire showed that on a 10-point Likert scale rating the ease of logging into the system (where 1 represents very difficult and 10 represents very easy), Mnemonic participants reported a mean score of 3 (median of 4), while Q&A participants reported a mean score of 4.2 (median of 4). Mnemonic participants failed to login an average of 4.2 times throughout the session, compared to 1.2 times for Q&A participants. Typically, several login failures occurred on one trial, rather than being peppered across all trials.

When asked to compare the security of the new approach versus traditional text passwords on a 10-point Likert scale, participants who chose Mnemonic passwords felt that these were more secure than traditional passwords, reporting a mean score of 7.6 (median of 7). Participants who took the Q&A approach did not feel strongly one way or another, reporting a mean score of 5.7 (median of 6). When asked to compare the guessability of the new approach versus traditional passwords, neither group perceived much difference, with Mnemonic participants reporting a mean score of 6.2 (median of 7) and the Q&A participants reporting a mean score of 5.3 (median of 5.5), on a 10-point Likert scale. These responses raise some troubling questions about users' mental models of authentication. For example, why would users think that the mnemonic approach was more secure than traditional passwords, yet regard them as equally guessable?

What does this mean for mnemonic passwords? Do we recommend them? Our main feeling after conducting this study is that weak understanding of users' mental models of authentication makes it difficult to instruct users on their choice of password. The typical approach of instructing users was an ineffective way of influencing their behaviour as intended. We speculate that instead of instructing users and relying on their understanding, we should perhaps "persuade" them to behave in ways that lead to greater security. We propose that using Persuasive Technology [3] principles, interfaces could be designed to foster proper mental models and motivate users to behave more securely. We are currently investigating persuasive approaches to achieve this goal for both text-based and graphical passwords.

5. CONCLUSION

We conducted a study to explore the usability and security of mnemonic passwords. Despite the experimental setting and both verbal and written instructions, 6 out of 16 users did not create passwords using mnemonic phrases. This leads us to believe that the use of instruction was not effective and that the use of mnemonics as a viable way of improving memorability (and hence usability) is questionable. It was also apparent that users had incomplete or inaccurate mental models of authentication. In light of these facts, it is our belief that conventional approaches to bridging the gap between security and usability, such as improved instructions and new password schemes, may not be the solution. Rather than instruct or impose new password schemes, we propose that "persuading" users to choose better passwords, through the use of Persuasive Technology, may more effectively guide them to create more secure and more memorable passwords.

REFERENCES

[1] Adams, A., and Sasse, M.A. Users Are Not The Enemy. Communications of the ACM v.42(12) Dec.1999, 40-46.

[2] Florencio, D., and Herley, C. A Large-Scale Study of Web Password Habits. Proc. of WWW 2007, May 2007.

[3] Fogg, B.J. Persuasive Technology: Using Computers to Change What We Think and Do, Morgan Kaufmann Publishers, San Francisco, CA, 2003.

[4] Jeyaraman, S., and Topkara, U. Have the cake and eat it too – Infusing usability into text-password based authentication systems. Proc. of ACSAC '05, Dec. 2005.

[5] Kuo, C., Romanosky, S., and Cranor, L. F., Human Selection of Mnemonic Phrase-based Passwords, Proc. of SOUPS '06, July 2006.

[6] Yan, J., et al. Password Memorability and Security: Empirical Results. IEEE Security & Privacy Magazine, v.2(5), Sept-Oct 2004, 25-31.