Helping Users Create and Remember More Secure Text Passwords

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

ABSTRACT
This doctoral research aims to persuade users to choose and remember more secure text passwords. The first component involved user studies demonstrating that users can be persuaded to create more secure text passwords. Unfortunately, the stronger passwords were not as memorable as we had hoped. For the second component, we will attempt to improve password memorability by providing implicit feedback and cueing to users as they login. The third component involves developing password rehearsal games that persuade users to employ established memory aids to assist them in remembering more secure passwords.

Categories and Subject Descriptors
K.6.5 [**Management of Computing and Information Systems**]: Security and Protection – *authentication.*

General Terms
Security, Human Factors, Experimentation

Keywords
Authentication, computer security, games, memory, passwords, persuasion, usable security.

1. INTRODUCTION
Online privacy and security relies heavily on user-chosen text passwords. However, many users select weak passwords [2] that are vulnerable to systematic password guessing attacks, thereby compromising users' account resources, privileges, and data. It is crucial that users create secure passwords, lest their online bank accounts be stolen, their electronic communications (e-mail, messengers, etc.) become monitored and manipulated, and their personal information be used for identity fraud. Despite their weaknesses, text passwords are fast, easy, and inexpensive to implement. They are unlikely to be entirely replaced by other authentication mechanisms, such as physical tokens (which can be lost or stolen) and biometrics (which compromise privacy).

The following doctoral thesis plan for Alain Forget, working with PhD advisor Robert Biddle, consists of three components. First, we have developed and user tested the effectiveness of Persuasive Text Passwords (PTP) [3]: a text password creation scheme leveraging persuasive principles that were successfully employed in recent click-based graphical password work done in our group [1]. User studies revealed that PTP helped users create more secure passwords, but password memorability did suffer. Secondly, we are currently exploring how two properties of click-based graphical passwords, *implicit feedback* and *cueing*, can be applied to PTP, and text passwords in general, to improve the memorability of more random and secure passwords. The effectiveness of these properties applied to text passwords will be verified through user studies. Thirdly, we will examine and evaluate the effectiveness of password rehearsal games that leverage persuasive principles to encourage users to play simple but fun games that increase the memorability of more secure passwords.

2. BACKGROUND
Recent attempts to instruct users on creating strong but memorable text passwords have been in the form of *mnemonic passwords*: memorable phrases abbreviated into passwords. Yan et al. [5] found mnemonic passwords to be as secure as random passwords and more secure than normal passwords. Kuo et al. [4] found most mnemonic passwords to be based on external sources and only as secure as regular passwords. Our group has developed the click-based graphical password system Persuasive Cued Click-Points (PCCP) [1], wherein users click once on each of five images sequentially presented to them. Each shown image is determined by the click-point location on the previous image. To help users choose more random click-points, PCCP also presents a randomly-positioned viewport; a highlighted area of the image wherein users must choose a click-point. User studies showed that PCCP helped users to select more secure passwords.

3. PERSUASIVE TEXT PASSWORDS
The first main component of this doctoral research began with developing and testing a text password creation system analogous to PCCP. Persuasive Text Passwords (PTP) [3] improves users' password security by placing randomly-chosen characters into the password during creation. The user may accept this improvement or *shuffle* for an alternative improvement. This approach offers a middle ground between password advice and system-enforced rules.

Our 83-participant between-subjects user study tested one *Control* and four PTP variants. *Replace-2* substituted two randomly-selected characters in users' passwords with two other randomly-chosen characters. *Insert-2*, *Insert-3*, and *Insert-4* would respectively insert 2, 3, or 4 randomly-chosen characters at randomly-determined positions in users' passwords. See Figure 1 for an Insert-2 example.

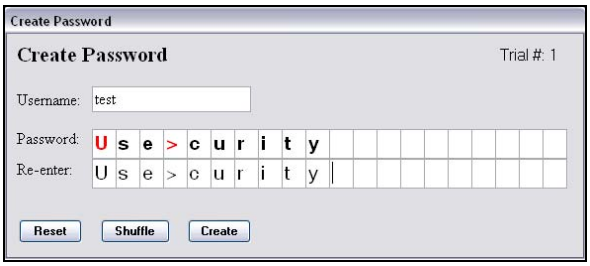

Figure 1. Screenshot example of inserting "U" and ">" into the user-chosen initial password "security".

Results showed that the Insert variants helped users create the most secure passwords. Surprisingly, Insert-4 users made fewer errors than Insert-3 users, despite our hypothesis that memorability would decrease as more characters were inserted. Insert-4 users performed better for two reasons. Firstly, Insert-4 users spent a mean of 30 extra seconds memorising their password. Secondly, participants would compensate for the added memory load by choosing less secure initial passwords when PTP inserted more characters. Thus, although Insert-4 users committed less errors than Insert-3 users, they expended unrealistic effort to so. Furthermore, the compensatory behaviour resulted in Insert-2, -3, and -4 improved passwords to all be of equivalent strength, despite our hypothesis that passwords with more inserted characters would be more secure. We concluded that PTP shows promise in helping users create more secure passwords, but more must be done to improve their memorability.

4. CUEING AND IMPLICIT FEEDBACK

PCCP has two noteworthy properties lacking in text passwords and PTP. The first is *cueing*; users' memory of their click-point's location is cued by the image's appearance. The second is *implicit feedback*; since each image shown is determined by the previous click-point, should users select the wrong point, they will not recognise the next image. They will then realise what happened and may try again. Seeing the correct image tells users they are on the right path. Furthermore, without knowledge of the correct picture sequence, malicious attackers trying to guess legitimate users' passwords receive no meaningful information.

The current component of this doctoral research consists of examining ways in which cueing and implicit feedback can be applied to PTP and general text passwords. As users receive feedback and a cue after each click in PCCP, we believe the same should occur with each keystroke. Rather than display asterisks when logging in, a more meaningful cue could be shown, such as a different character, a symbol, and/or an image. These cues could be shown from left to right (like asterisks) or one at a time (like PCCP images). Displaying characters could be problematic, since users may simply choose a memorable first character and then use a simple and predictable character mapping, such as typing the shown character or the next letter in the alphabet. Images may have a similar drawback; users may choose the first letter an object in the image, such as "a"' for an airplane. However, users may choose "f"' for flying, "b" for big, or "!" for a fear of heights. Arbitrary symbols may have little intrinsic meaning, but when linked to keystrokes during password creation, they are given meaning and may cue users' memory when logging in.

5. PASSWORD REHEARSAL GAMES

Although not our current focus, the aim of the third doctoral research component is to design and test several *password rehearsal games* (PRGs) to help users remember their password through the use of cueing, recognition, rehearsal, mnemonics, and narratives. One such PRG could be *Mix-up*, wherein users are shown their password with the characters jumbled, and they must place their password's characters in the proper order. Another PRG example emulates *Hangman*, wherein users must correctly guess the characters of their password (preferably in the proper order). A third example is *Wordsearcher*, where users are presented with a 2-D grid of characters wherein the password is hidden and must be found. These games can also be generalised to help users remember multiple passwords. PRGs may use context-based cues to assist users in identifying to which account (bank, work, e-mail, messenger, etc.) each password belongs.

6. CONCLUSION AND FUTURE WORK

For the first doctoral research component, we employed persuasion to influence users to create more secure text passwords. User studies demonstrated that the persuasion was effective in guiding users to create more random and secure passwords, at the cost of some memorability. The second and current doctoral research component aims to improve the memorability of more secure text passwords by providing users with *implicit feedback* and *cueing* similar to click-based graphical passwords. For the third doctoral research component, we will examine *password rehearsal games* that encourage users to employ known memory aids with stronger and more random passwords. We thank Sonia Chiasson, Paul van Oorschot, and Robert Biddle for their contributions to this doctoral work.

7. REFERENCES

[1] Chiasson, S., Forget, A., van Oorschot, P.C., Biddle, R. Influencing Users Towards Better Passwords: Persuasive Cued Click-Points. *ACM BCS HCI 2008*.

[2] Florencio, D. and Herley, C. A Large-Scale Study of Web Password Habits. *ACM WWW 2007*. 657-666.

[3] Forget, A., Chiasson, S., van Oorschot, P.C., and Biddle, R. Improving Text Passwords Through Persuasion. *ACM SOUPS 2008*. (to appear in July)

[4] Kuo, C., Romanosky, S., and Cranor, L.F. Human Selection of Mnemonic Phrase-based Passwords. *ACM SOUPS 2006*. 67-78.

[5] Yan, J., Blackwell, A., Anderson, R., and Grant, A. Password Memorability and Security: Empirical Results. *IEEE Security & Privacy Magazine 2*, 5 (2004), 25-31.