Memorability of Persuasive Passwords

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

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

CHI 2008, April 5 – April 10, 2008, Florence, Italy
ACM 978-1-60558-012-8/08/04.

Abstract
Text passwords are the primary authentication method used for most online services. Many online users select weak passwords. Regrettably, most proposed methods of strengthening passwords compromise memorability. This paper explores a lightweight password creation mechanism's effect on password memorability. Our system employs Persuasive Technology to assist users in creating stronger passwords. Results show that our improvement scheme affected password memorability only for users who created secure passwords before the system applied its improvement. This result warns researchers to not alienate users who are already security-aware when trying to assist security-unaware users to behave more securely.

ACM Classification Keywords
K.6.5 Management of computing and information systems: Security and protection: Authentication

Keywords
Authentication, chunking, computer security, memory, passwords, Persuasive Technology, usable security

Introduction
User-chosen text passwords are the authentication method of choice for most online systems that require privacy and security. However, many users select weak passwords [4] that are vulnerable to automated attacks

that systematically guess passwords, resulting in users' account resources, privileges, and data being compromised. Although many methods have been suggested for improving the security of users' passwords, these tend to sacrifice memorability. In this paper, we discuss the memorability of passwords created with a prototype system that employs Persuasive Technology to assist users in creating stronger text passwords. We begin by summarising related research, and then introduce our prototype persuasive password system. We then describe our experimental study, report results on the passwords' memorability, and discuss the implications thereof.

Background

In the computer security field, security strength is usually measured on an exponential scale and thus is typically expressed in logarithm base-2, called *bits of security*. Menezes et al. [11] describe password security in terms of *password spaces*; the total number of distinct passwords that can be created with a given set of characters. The 95 English US keyboard characters are usually split into four such password spaces: lowercase letters (26), uppercase letters (26), digits (10), and symbols (33). A password's security can be measured by its length in characters and the number of password spaces wherein at least one of the password's characters is a member. For example, the password "fluffy" is 6 characters long and contains only lowercase letters, and thus offers $26^6 \approx 3.1 \times 10^8 \approx$ 28.2 bits of security. Similarly, "fluffy123" has 9 characters, either lowercase letters or digits, offering $36^9 \approx 1.0 \times 10^{14} \approx 46.5$ bits of security. Subsequently, capitalising an "f" for "Fluffy123" boosts the security to $62^9 \approx 1.3 \times 10^{16} \approx 53.6$ bits. Note however that these passwords are in fact very insecure not only because secure passwords should provide more bits of security, but dictionary words and predictable number sequences are easily guessed by most types of password attacks.

Security professionals often attribute weak password use to a lack of user effort and motivation. Adams and Sasse [1] instead argue that users misunderstand the security threats and how to effectively defend themselves with the given mechanisms. Sadly, human memory limitations further prevent users from utilising passwords' full theoretical security potential [15].

Bishop [2] has suggested that passwords should ideally be composed of *chunks* that have meaning only to the password's creator. Chunking is a well-recognised strategy people use to remember information by grouping several smaller chunks of information into fewer larger ones through some semantic encoding. The number of short-term memory chunks a human can retain is debatable, as Gobet & Clarkson [8] show Miller's 7±2 chunks [12] is an overestimate.

Mnemonic phrase-based passwords, which are passwords derived from abbreviated memorable phrases, have been proposed to assist users in creating both memorable and secure passwords. Yan et al. [18] found mnemonic passwords to be better than both normal user-created passwords and randomly-generated passwords. This aligns with Ericsson's explanation of expert memory [3], how rich semantic encoding is the principle underlying chunking in other domains, such as chess playing. However, Kuo et al. [9] discovered most user-chosen mnemonic passwords to be based on phrases easily found on the Internet, thus being only as secure as regular passwords.

Vu et al. [16] ran four usability studies where users had to create several passwords, recall them after five minutes, and again after one week. Each study tested a different set of enforced password creation requirements. The authors found the most secure and memorable passwords were created by using the first letter of each word in a sentence and inserting a digit and symbol. Other methods that have been studied include word association passwords [14] and random password generation [10], both of which were found to have memorability problems.

General advice on creating secure passwords and high-level feedback in the form of "password strength meters" abound on the Internet. Furnell [7] found password advice and criteria imposed by 10 popular websites largely lacked consistency and effectiveness.

Fogg [5] defines the new field of Persuasive Technology (PT) as "interactive computing systems designed to change people's attitudes and behaviours". Many domains, particularly health and education, have benefited from PT theory guiding users to behave in the desired manner. However, PT must be adapted to address the unique challenges of usable security [17]. We recently proposed the Persuasive Authentication Framework [6] as five principles which condense the key portions of PT theory best suited to address issues in usable authentication.

Persuasive Text Passwords

A solution to the problem of password security versus memorability has yet to be found. Meanwhile, users are required to remember an ever-growing number of passwords. We decided to try utilising our Persuasive Authentication Framework to develop and implement several variations of a Persuasive Text Password (PTP) prototype system. By randomly placing a few randomly-selected characters into users' passwords during password creation, the PTP system *improves* the security of user-chosen passwords. Users may *shuffle* for an alternative improvement until they find one they feel is memorable. The random nature of the system-chosen characters is unpredictable to malicious attackers attempting to systematically guess users' passwords, and thus we believe PTP will increase the security of users' passwords. We also believe the system will be usable and users' passwords will be memorable since they mostly consist of user-chosen content.

Persuasive Text Password Variations

We first conducted informal usability pre-tests to uncover and correct major usability issues. Of all the variants evaluated, we chose to test the following two in our formal usability study:

- *Insertion*: Once users had chosen their own password, the system would *insert* two characters into the users' password. See figure 2 for an example.
- *Replacement*: Identical to Insertion, except the two system-chosen characters *replaced* two user-chosen characters, rather than inserted in between.

In this study, we wanted to focus on exploring as many alternatives as possible to find the best among them. An upcoming study will compare our final design against a control group using regular passwords.

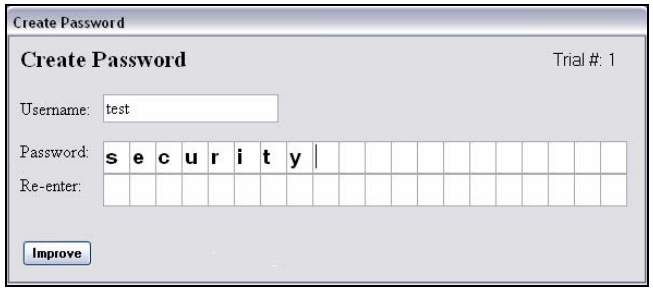

figure 1. An example user choosing the password "security" in the Persuasive Text Password system

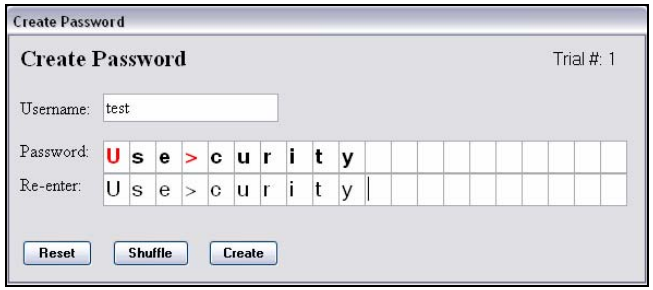

figure 2. An example user re-entering their password, improved by the Persuasive Text Password Insertion variant

User Study

Our University's Ethics Committee for Psychological Research approved the following formal usability study procedures. 15 university students took part in individual one-hour sessions, testing one of the two PTP variations (Insertion or Replacement). 8 participants studied Computer Science, 3 studied Psychology, and the others from various disciplines. All participants used the Internet and passwords regularly. We ran a total of 154 trials, wherein each consisted of the following:

- *Create*: Users composed a password of 8 or more characters (see figure 1) with their randomly-assigned variation. Users then re-entered their password (with the system-chosen characters) to ensure they could recognise their password's characters (see figure 2). The password was visible so users could identify the system-chosen characters and re-enter the password.
- *Confirm*: Users re-typed their password, masked by asterisks (*), including the previously system-selected characters. If they were unsuccessful, they could re-attempt to confirm. If they forgot their password, they could skip the current trial and create a new password.
- *Distraction*: To clear their textual working memory and simulate the passage of a longer amount of time [13], users counted down in threes starting from a four digit number (e.g. 4372, 4369, 4366) for 45 seconds.
- *Login*: Users retyped their masked improved password to login. As in the Confirm phase, if they were unsuccessful, they could retry to login or skip.

Results

Since placing randomly-chosen characters into passwords is almost certain to make them more secure, we were mainly interested in evaluating the passwords' memorability. In an attempt to devise a formula to score a password's memorability, we found that the *recall time*, the sum of time taken to confirm and login, was a suitable password memorability measure since a linear regression test revealed a strong correlation with the number of confirm and login errors ($F(1, 152) = 339.3$, $p < .001$), and the linear model showed the recall time increased as the confirm and login errors increased.

Since the random characters will come from varying password spaces, the security gain will also vary. Thus, we first examined whether the amount of shuffling had any effect on the difference in bits of security between their original and improved passwords. A linear regression test found no correlation ($F(1, 152) = .04914$, $p = .8249$). We also found no correlation between the amount of shuffling and recall time ($F(1, 152) = .3144$, $p = .5758$). These results show that users could chose memorable improvement characters without sacrificing their password's security.

We next compared recall time to the difference in bits of security between the improved and original passwords, finding no correlation ($F(1, 152) = 1.011$, $p = .3164$). We also found no strong correlation between recall time and the improved passwords' bits of security ($F(1, 152) = 3.532$, $p = .06211$). These results suggest PTP's security improvement did not affect the memorability of their improved passwords.

To our surprise, we found a strong correlation between recall time and users' original passwords ($F(1, 152) = 9.191$, $p < .005$). The linear model revealed that the stronger a user's original password, the longer the recall time, and thus the more their improved password's memorability suffered. This matches comments from the participants who created more secure original passwords. They stated the PTP system interfered with their password creation scheme, and made their passwords more difficult to remember.

Discussion

Although our data stems from only 15 participants and the prevalence of Computer Science students is disproportionate with the Internet population, our preliminary results suggest the PTP-improved passwords were memorable. To verify these trends, we are presently expanding the study with participants more typical of the online population, as well as introducing a normal password scheme control group.

Our best explanation for the original password's effect on the improved password's memorability involves chunking. When users who are unaware of password security threats originally choose simple (and insecure) passwords, such as a single word, they only have one chunk to remember. Once the PTP system thereafter improves the password by placing two random characters, users then have three chunks to remember; their original simple password and the two extra characters. Conversely, users who are aware of the threats to password security instead choose a more complex original password. These passwords are likely to be composed of semantically meaningful chunks that appear unpredictable to anyone but the password's creator. When the PTP system improves the security-conscious user's password, the two inserted characters are likely to be extra chunks unrelated to the user's semantic links, potentially severing them, thereby decreasing memorability. We believe this is why improved passwords that were originally secure were harder for users to recall than improved passwords that were previously very simple and insecure.

Conclusion

We have shown that user-chosen passwords can easily be strengthened, thereby better protecting users' online accounts (and the resources and capabilities therein) by lowering the chance malicious attackers guess the passwords through automated password attacks. Although PTP's security improvement did not affect

password memorability for users who originally chose weak passwords, more security-conscious users, who created secure passwords without aid from the system, had some trouble recalling their improved passwords. We used *chunking* theory to explain the surprising result, whereby users who choose weak passwords had fewer chunks to remember than users who choose more secure and complex passwords.

This phenomenon warrants further examination and testing, which we believe will uncover important implications for any system intended to assist users in creating more secure passwords or behaving securely in general. Although many people do not understand how to behave securely and why they should do so, when trying to help them, it is essential we not alienate users who already recognise the importance of security.

References

[1] Adams, A. & Sasse, M.A. Users Are Not The Enemy. *Communications of the ACM 42*, 12 (1999), 41-46.

[2] Bishop, M. A Proactive Password Checker. *Technical Report PCS-TR90-152* (1990), accessed Jan 2008, http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/19920018383_1992018383.pdf

[3] Ericsson, K.A., Charness, N., Feltovich, P.J., & Hoffman, R.R. *The Cambridge Handbook of Expertise and Expert Performance*. Cambridge University Press, Cambridge, UK, 2006.

[4] Florencio, D. & Herley, C. A Large-Scale Study of Web Password Habits. *Proc. WWW 2007*, 657-666.

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

[6] Forget, A., Chiasson, S., & Biddle, R. Persuasion as Education for Computer Security. *Proc. E-Learn 2007*, AACE, 822-829.

[7] Furnell, S. An assessment of website password practices. *Computers & Security 26*, 7-8 (2007), 445-451.

[8] Gobet, F. & Clarkson, G. Chunks in expert memory: Evidence for the magical number four…or is it two? *Memory 12*, 6 (2004), 732-747.

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

[10] Leonhard, M.D. & Venkatakrishnan, V.N. A Comparative Study of Three Random Password Generators. *Proc. IEEE EIT 2007*, 227-232.

[11] Menezes, A.J., van Oorschot, P.C. & Vanstone, S.A. *Handbook of Applied Cryptography*. CRC Press, 1996.

[12] Miller, G.A. The magical number seven, plus or minus two: some limits on our capacity for processing information. *Psychological Review 63*, 2 (1956), 81-97.

[13] Peterson, L.R. & Peterson, M.J. Short-term retention of individual verbal items. *Experimental Psychology 58*, 3 (1959), 193-198.

[14] Pond, R., Podd, J., Bunnell, J., & Henderson, R. Word Association Computer Passwords: The Effect of Formulation Techniques on Recall and Guessing Rates. *Computers & Security 19*, 7 (2000), 645-656.

[15] Sasse, M.A. Computer Security: Anatomy of a Usability Disaster, and a Plan for Recovery. *CHI 2003 Workshop on HCI and Security Systems*, ACM Press.

[16] Vu, K.-P.L., Proctor, R.W., Bhargav-Spantzel, A., Tai, B.-L., Cook, J., & Schultz, E.E. Improving password security and memorability to protect personal and organizational information. *International Journal of Human-Computer Studies 65*, 8 (2007), 744-757.

[17] Whitten, A. & Tygar, J.D. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. *Proc. USENIX Security Symposium 1999*, USENIX, 169-183.

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