Persuasion for Stronger Passwords: Motivation and Pilot Study

Alain Forget[1,2], Sonia Chiasson[1,2], P.C. van Oorschot[1], and Robert Biddle[2]

[1] School of Computer Science, Carleton University, Ottawa, Canada
{aforget,chiasson,paulv}@scs.carleton.ca
[2] Human-Oriented Technology Lab, Carleton University, Ottawa, Canada
robert_biddle@carleton.ca

Abstract. Text passwords are the ubiquitous method of authentication, used by most people for most online services. Many people choose weak passwords that are vulnerable to attackers who simply guess all the passwords within the most probable password spaces. This paper describes a lightweight password creation mechanism that uses Persuasive Technology to influence users to create stronger passwords. Results from a pilot study show that our Persuasive Text Passwords (PTP) prototype system successfully influenced users to create and remember more secure passwords.

Keywords: authentication, computer security, passwords, Persuasive Technology, usable security.

1 Introduction

Online privacy and security relies heavily on authentication through textual passwords chosen by the users themselves. However, it is known that many users select weak passwords [5] that are vulnerable to automated attacks that systematically guess passwords and subsequently compromise 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.

Many security professionals have attributed the problem of weak passwords to a lack of user effort and motivation. However, Adams and Sasse [1] indicate that users create insecure passwords due not to a lack of motivation, but to misunderstanding the security threats, as well as how to effectively defend themselves with the provided mechanisms. Sadly, even when armed with such knowledge, limitations of human memory render users largely incapable of effectively using standard passwords [12].

In this paper, we consider how principles of Persuasive Technology (PT) [6] can help users create stronger text passwords that are nonetheless memorable. We first describe the background research on password choice and basic issues in evaluating password security. We present our Persuasive Text Passwords prototype system and explain how applied PT principles influence users to create more secure passwords. Finally, we describe our pilot study, report on the results, and offer our conclusions.

H. Oinas-Kukkonen et al. (Eds.): PERSUASIVE 2008, LNCS 5033, pp. 140–150, 2008.

2 Background

Some recent attempts to instruct users on creating strong but memorable passwords have been in the form of *mnemonic phrase-based passwords*: memorable phrases abbreviated into passwords. Yan et al. [18] found mnemonic passwords to be as secure as random passwords and more secure than normal passwords. However, Kuo et al. [9] found that most mnemonic passwords were based on phrases from external sources and were only as secure as regular passwords given the authors' attack model.

When creating accounts on the Internet, many websites offer advice on creating secure passwords through general suggestions or high-level feedback in the form of "strength meters". Furnell [7] discovered a lack of consistency and effectiveness across password requirements and advice provided by 10 popular websites. Apparently such advice has little effect, as recent findings by Florencio and Herley [5] show the majority of over 500,000 Internet users' online passwords (including for PayPal) consist solely of lowercase characters. Although memorability was not discussed, users created stronger passwords when one service provider imposed strength requirements. The authors also noted password re-use, averaging at about 3.22 website accounts per password. Thus, even when password instructions and memorability aids are readily available, users continue to behave insecurely.

Weirich and Sasse [16] assert that, for password security to be effective, users must exert extra effort in creating secure passwords. They further discussed reasons why conventional fear appeals fail to motivate users to behave securely. The authors propose *persuading* users to "buy-in" to a security-centred culture. They mainly employ user-centred design theory in their discussion of persuasion.

2.1 Persuasive Authentication Framework

More recently, Fogg [6] has presented Persuasive Technology (PT) as "interactive computing systems designed to change people's attitudes and behaviours". PT is a set of tools, media, and cues which technological solutions may implement to encourage users to behave in some desired manner. Persuasive tools assist users in accomplishing tasks more quickly and easily, persuasive media offer several representations by which messages are conveyed, and persuasive social cues endow products with friendly, knowledgeable, and trustworthy attributes.

Numerous persuasion strategies are associated with each of the three aforementioned persuasive roles. The persuasive goals, topic, medium, audience, and desired persuasive strength determine which persuasion strategies should be employed. PT has successfully produced desired behaviour changes in many domains, such as health [8, 15] and education [10].

PT is purposefully generalised so it may be used in any domain, but some PT theory does not readily apply to the unique challenges of usable security.

1. Security is a secondary task [17]; users will bypass any security measure which impedes them from completing their primary task.
2. Security systems are complex, making it difficult for users to form proper mental models [4]. Users may not even realise their behaviour puts them and others at risk or may underestimate the consequences of behaving insecurely.
3. Computer security must deal with the "barn door" property [17]; should private information be exposed even for a brief moment, it is impossible to guarantee that it has not been compromised by an attacker.

4. Users tend to concern themselves with privacy and security only when its impact on their lives is blatantly obvious [13]. Regrettably, this typically occurs no sooner than when users' security and privacy has already been breached.

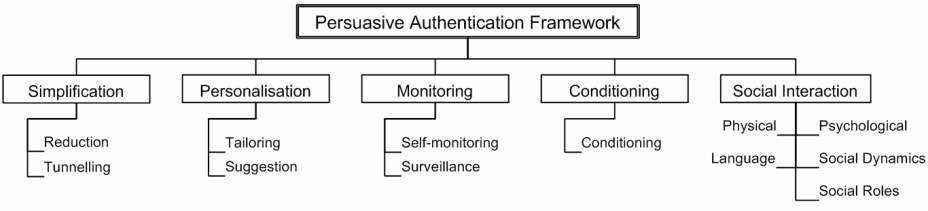

Fig. 1. The Persuasive Authentication Framework [3]

The Persuasive Authentication Framework [3] (Fig. 1) has recently been proposed. It condenses PT into five key principles that are applicable to the challenges of usable security and authentication. Each principle draws on various PT tools and cues.

Simplification. Authentication tasks should be made as simple as possible. This can be achieved by ensuring the authentication process is *reduced* to as few steps as possible and is *tunnelled* to ensure users make secure choices when using the system.

Personalisation. Since customised information is more persuasive than generic advice, *tailoring* the authentication process for users can persuade them to behave more securely. Greater persuasive power can result from offering personalised security *suggestions* at the most opportune moment.

Monitoring. Users may be more likely to behave securely if they know security administrators perform routine *surveillance* on their passwords. If the results of security analyses on users' passwords are visible to users (like password strength meters), they can *self-monitor* and adjust their behaviour to be more secure.

Conditioning. Users typically underestimate the threats and risks to their online accounts, and thus do not believe behaving securely is necessary. By applying various forms of reinforcement *conditioning* to synthetically encourage the correct behaviour, we can help shape the desired secure behaviour or turn existing behaviour into habits.

Social Interaction. Establishing a common rapport with users by emulating their *physical*, *psychological*, and *language* characteristics can make an authentication system more persuasive. Additional persuasion can be leveraged from *social dynamics*, such as thanking the user for behaving securely, and *social roles*, by using statements such as, "One weak link in the security chain is all it needs to break."

2.2 Password Space

Two fundamental concepts must be distinguished when evaluating the security of any authentication system. The first is the *theoretical password space* (TPS) size: the number of unique passwords users could theoretically choose in a given system. The TPS size is determined only by technical constraints independent of such factors as user-choice. Two main constraints in text passwords are the number of unique characters available on the keyboard, and any password character length limits.

The second concept is the *effective password space* (EPS): the number of passwords in the TPS that are likely to be chosen by real-world users. Clearly, the EPS can never be larger than the TPS. An ideal security system will have an EPS too large for an attacker to exhaustively guess in a reasonable amount of time.

Text passwords have a reasonably large TPS for passwords of sufficient length. They would be reasonably secure against guessing attacks if users chose passwords randomly and with equal probability. However, most users do not choose from the 95 English U.S. keyboard characters with equal probability. To simplify discussion, we consider 8-character passwords, since the arguments extend for longer passwords. The TPS size is the number of all possible 8-character passwords: $95^8 \approx 6.6 \cdot 10^{15}$.

Table 1 shows the growth in number of passwords as the password space character set becomes larger by using characters from different subsets, such as lower- and uppercase letters, digits, and symbols. We note Table 1 presents optimistic figures that do not account for biases towards dictionary words or commonly-used character patterns, which attackers readily exploit with cracking tools like John the Ripper [14].

Note the significant increase in password space size when all four character subsets are used. Such exponential jumps are well-recognized in the computer security field, and security estimates are typically expressed in base-2 logarithms [2], shown in the *estimated bits of security* column of Table 1. This security estimate naïvely assumes password characters are randomly chosen within their space. However, it is useful for coarse relative comparison. It is much harder to find a password amongst $95^8 \approx 6.6 \cdot 10^{15}$ others than it is to find amongst $26^8 \approx 2.0 \cdot 10^{11}$. Still, users continue to select passwords from small subspaces of the TPS, making attackers' guesswork less costly.

Table 1. A comparison of password spaces across various 8-character password subsets

Password space subset	Passwords in subset	% of TPS	Estimated Bits of Security ($\log_2$)
Lowercase	$26^8 \approx 2.0 \cdot 10^{11}$	0.003	37.6
Lowercase & digits	$36^8 \approx 2.8 \cdot 10^{12}$	0.043	41.4
Mixed case	$52^8 \approx 5.4 \cdot 10^{13}$	0.806	45.6
Alphanumeric	$62^8 \approx 2.2 \cdot 10^{14}$	3.291	47.6
Alphanumeric & symbols	$95^8 \approx 6.6 \cdot 10^{15}$	100	52.6

We propose improving the security of passwords by increasing the probability that users will create passwords in larger password spaces, and therefore requiring much more effort for an attacker to guess. Although this would be an improvement, we must be clear that this approach only improves security against guessing attacks, and does not address attacks such as surreptitious installation of keyloggers, other "malware" on users' machines, or social strategies such as "phishing" whereby users are tricked into revealing their passwords. We also note that the strategy of increasing the effective password space is the basis for other existing strategies [9, 18]. The difference in our approach is that we propose to use Persuasive Technology.

3 Persuasive Text Passwords

Traditional approaches to increasing the effective password space for text passwords involve either advice or prescription. Password advice approaches include education

through the publication of guidelines, as well as general feedback on the user-chosen passwords' strength. Approaches using prescription include enforced rules for password creation and system-generated passwords with no user choice whatsoever. As discussed in Section 2 these approaches are problematic, as advice is often ignored and prescription leads to frustration and poor password memorability.

Our general approach is a password creation system involving both user choice and a persuasive system-chosen *improvement*. The user may accept the improvement or *shuffle* for an alternative improvement. Our approach uses Persuasive Technology (PT) as a middle path between advice and prescription. As an active part of the password creation process, we hope this approach will be more effective than mere passive advice. Additionally, user involvement in the creation process should result in memorable passwords. The amount of PT employed is admittedly modest, but we wish to assess its impact before incorporating any additional persuasive strategies.

3.1 Variations of Persuasive Text Passwords

To explore this password-improvement approach, we designed three Persuasive Text Passwords (PTP) mechanisms, which randomly place between two and four randomly-chosen characters in users' passwords. All three mechanisms allowed users to press a shuffle button, causing the system to assign a new set of randomly chosen and positioned characters to the users' passwords. All improved passwords contained at least eight characters. See Fig. 2 and Fig. 3 for an example of the PTP system. We developed and implemented the following three Persuasive Text Passwords variations.

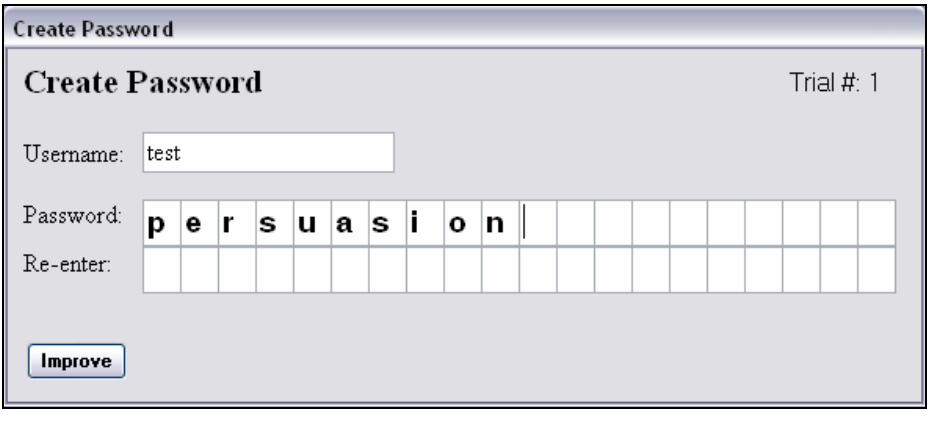

Fig. 2. A screenshot example of a user choosing "persuasion" as their original password in the Persuasive Text Passwords system

Preload. The system-assigned characters were randomly-chosen and positioned within the first eight character slots before the users began creating their password. In essence, the users created their password around the system-chosen characters.

Replace. As per a typical password system, users first chose their own password. The system then replaced two to four random characters in the password with new randomly-chosen ones.

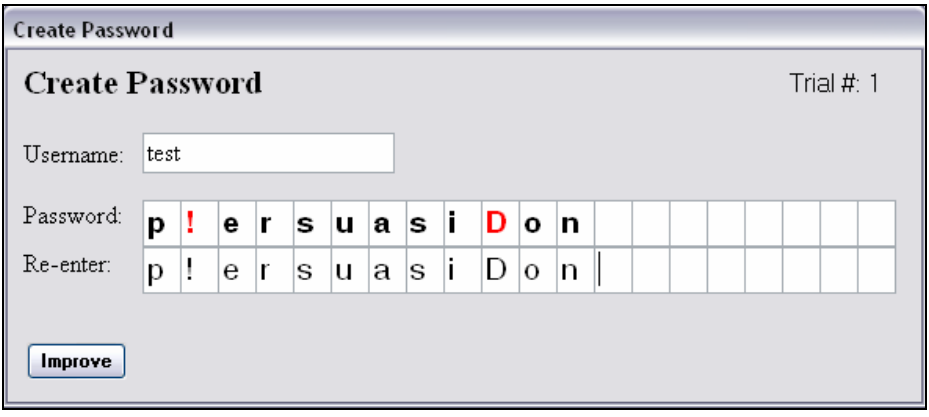

Fig. 3. A screenshot example of a user re-entering their Insert-improved password into the Persuasive Text Passwords system

Insert. After users chose their password, two to four random characters were inserted into the password at random positions**.** A screenshot of the Insert condition is shown in Fig. 3.

All 3 variations leverage these Persuasive Authentication Framework [3] principles.

Simplification. Since the PTP system takes on the responsibility of ensuring the password is secure, users can focus on making their password memorable, thereby simplifying the password creation task. Furthermore, the users' "path-of-least-resistance" is to comply with the system's initial suggestion, which is more secure than shuffling until a weaker set of characters (such as all lowercase characters) are found. Thus, when creating a new password, PTP makes the most secure choice the least burdensome; many other password schemes lack this property.

Conditioning. Shuffling repeatedly to find a specific set of system-assigned characters can be tedious. The PTP system makes less secure choices less attractive, hence guiding users away from poor security decisions.

Personalisation. Since the system-assigned characters are placed in a user-chosen password, users are likely to feel a kinship towards their password and thus are more likely to comply with the system's suggestions. Furthermore, we expect users are most likely to be open to password suggestions when creating one. Thus, PTP applies its persuasion at the most opportune moment. The persuasion may also develop their mental model of secure passwords, potentially leading them to apply the PTP random-character placement scheme to their other passwords.

3.2 Usability Pre-testing

Before conducting the pilot study, we first performed some informal usability pre-tests with six participants to uncover the most prominent usability issues. The following list describes the identified problems and the solutions we adopted.

Repeating Characters. Users would often repeat the system-assigned characters when creating a Preload password. For example, if the system presented the users with "_ _ B _ _ # _ 8", they were likely to choose a password similar to "BBB###88". Since the lack of distinct characters makes such passwords very insecure, we chose not to test the Preload variant in this pilot study.

Character Minimisation. Users would shuffle until the system placed only two randomly chosen characters into the password. Memorability seemed to suffer the few times users created passwords with three or four system-assigned characters. Therefore, we chose to examine only placing two characters for this pilot study.

Indistinguishable Characters. Certain system-chosen characters were difficult for users to tell apart, such as the grave accent (`) and the apostrophe (‘), or the lowercase "L" and the vertical line (|). To avoid such confounds in our pilot study, we removed the uncommon characters (the grave accent and vertical line) from PTP's set of system-selectable characters. The small loss in security due to removing the characters is worth avoiding possible user error, confusion, and frustration.

Character Memorability. Users had difficulty identifying the position and case of their password's system-chosen characters when confirming and logging in. Although their password was visible during creation, it was masked with asterisks (*) when confirming and logging in. To assist users in learning their passwords, the pilot study asks user to re-type their password unmasked (shown in Fig. 3) during the password creation phase. This additional step allows users to practice typing their entire password while visually verifying that the characters they type are correct. This assumes PTP passwords are created only in environments free of shoulder-surfing, where potential attackers can observe users entering their passwords**.**

3.3 Pilot User Study

The following pilot lab study procedures were evaluated and approved by our University's Ethics Committee for Psychological Research. We used a between-subjects design; 7 participants tested the Replace PTP variant and 8 others tested Insert. All were university students; 8 studying Computer Science and others from various disciplines. All used computers, the Internet, and passwords regularly. Data was collected from a total of 154 trials. Each participant completed 10 or more trials, each consisting of creating, confirming, and logging in with a password. Users also filled out a demographics and user-opinion questionnaire during the session.

The Persuasive Text Passwords system logged users' actions and passwords. When introducing participants to the system, they were told to pretend the passwords they created would be protecting their online bank accounts, and therefore to choose passwords that would be hard for others to guess but were still memorable. They were told the password system's improvements would help them create more secure passwords, but that they may shuffle as often as they liked to find system-chosen character combinations they preferred. Participants performed a practice trial to familiarise themselves with creating passwords in this new way. These practice trials are not included in the 154 total trials. Each trial consisted of the following phases.

Create a Password. Users would compose a password of at least 8 characters according to their randomly-assigned condition (Insert or Replace). Users then re-typed their improved password (with the system-assigned characters) to ensure they could correctly identify the characters in their password. In this phase, the password was visible in order for users to identify the system-assigned characters and accurately re-type them. Users could press a shuffle button to randomly change the system-assigned characters and positions. See Fig. 3 for a password creation example.

Confirm a Password. Users re-entered their password, improved with the previously system-chosen characters. The echoed password was visually masked by asterisks (*). If they were unsuccessful, they could try to confirm again. If they could not remember their password, they could move on to the next trial and create a new password.

Answer Two Questions. Users answered two 10-point Likert scale questions gauging the perceived password creation difficulty and predicted memorability after one week.

Distraction Task. For 45 seconds, users counted backwards in threes, beginning from a randomly-chosen four digit number (e.g. 4372, 4369, 4366, etc.). This was intended to clear their textual working memory [11] and simulate a longer passage of time.

Log In. Users logged in by retyping their improved password. The echoed password was again visually masked by asterisks (*). Similar to the Confirm phase, they could retry if they were unsuccessful. If users could not remember their password, they could skip this trial and begin creating a new password for the next trial.

3.4 Results

In considering the pilot study's results, we adhere to the twin goals of usable security. We must care for usability; the system should be easy to use for the purpose intended. In this case, created passwords must be memorable, and the creation process should not be time-consuming. However, the system should also accomplish the security goals. In this case, the resulting passwords should be sufficiently stronger than those originally chosen by the user. We now address both these issues.

Memorability. How memorable were the passwords?
Out of the 154 total trials where users created passwords, 145 (94%) resulted in a successful confirm, of which 132 (86%) was on the first attempt. Of the former 145 successful confirmations, 141 (97%) also resulted in a successful login, of which 128 (88%) were on the first attempt. Pearson's chi-squared tests revealed no significant distinction between the Insert and Replace conditions. Although our method did not test long-term memorability, the cognitive load was substantial due to the many passwords being created. Overall, we feel these results suggest a reasonable level of memorability, but warrants further testing.

Times. How long did it take to create passwords, confirm them, and login?
To create a password, users took a mean and median of 66 and 58 seconds, with a standard deviation of 31 seconds. This includes the time to construct an initial password, shuffle as much as desired, and re-enter the improved password. The mean times to confirm and login were 15 and 14 seconds respectively. A regression analysis showed login times became shorter as users completed more trials. Two sample t-tests revealed no significant distinction between Insert and Replace. We believe these times are acceptable as a starting point and are likely to decrease with daily use.

Shuffles. How often did users shuffle improved password suggestions?
Over all 154 trials, the mean number of shuffles per trial was 8, and the median was 3. Our observations suggest that most users shuffled until they found an improved password they felt was memorable. However, users were often persuaded to comply with the first system-suggestion, as they did not shuffle at all in 41 of 154 trials. T-tests revealed no significant distinction between Insert and Replace.

Perception. What opinions did users report about the usability and security of PTP?
Our post-test user-opinion questionnaire asked users to answer several questions, some reversed to avoid bias, on 10-point Likert scales. The main results are as follows, showing median responses. Users felt the new system was slower (4), that they would prefer a normal system if they were in a hurry (4), and that they would find the passwords more difficult to remember (4). However, they did feel the system was more secure than ordinary passwords (8), led to passwords that would be more difficult to guess (8), and with practice, they could get used to the system (8). These results seem reasonable for a new authentication system, and reflect a trade-off we would expect. We note that participant responses may be biased from being told the system's improvement would make their password more secure. Although we believe such a statement would be made if the system were deployed, we plan to test user acceptance of PTP when it is not introduced as a security improvement. Chi-squared tests revealed no significant distinction between Insert and Replace.

Security. Did the system help users create more secure passwords?
Table 2 shows the system's effect on password security by describing the nature of both the pre- and post-improvement passwords. For example, our improvement process reduced the proportion of very weak lowercase alphabetic passwords from 20.8% to 4.5%. The proportion of very strong passwords that included lowercase, uppercase, numeric, and special characters rose from 14.3% to 29.9%. Most passwords were improved to include characters from additional character subsets.

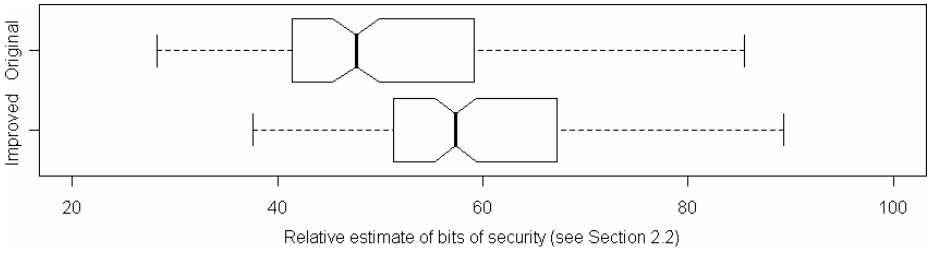

Fig. 4. Box plot of a relative bits of security estimate of users' original and improved passwords

Fig. 4 compares the distribution users' original and improved passwords' estimated bits of security (see Section 2.2). Each box denotes the 2nd and 3rd quartiles, divided by the bold line noting the median. The whiskers at each of the boxes' extremities show the 1st and 4th quartiles. The groups are statistically different if the notches in both boxes do not overlap. T-tests confirm the improved passwords were statistically stronger across all participants ($t(306) = -5.0532$, $p < .001$), and within both the Insert ($t(164) = -4.7548$, $p < .001$) and Replace ($t(140) = -2.5138$, $p < .05$) conditions. Thus, PTP influenced users to create passwords more difficult for attackers to guess.

Our user sample consisted of approximately half Computer Science (CS) students, and it appears these participants formed a distinct group. For example, 12% of CS students chose original passwords in all lowercase, while 30% of the other students did the same. The possibility for improvement was therefore reduced for CS students. Since such technical expertise was over-represented in our sample, we expect that the general impact of our approach would likely be greater than our study results suggest.

Table 2. Proportions of users' original and improved passwords across four character subsets

Character Subsets	% of Original Passwords	% of Improved Passwords
All lowercase	20.8%	4.5%
All uppercase	0.6%	0.0%
All numeric	0.0%	0.0%
All special	0.0%	0.0%
Lowercase & uppercase	1.3%	5.8%
Lowercase & numeric	26.6%	5.8%
Lowercase & special	5.9%	7.2%
Uppercase & numeric	2.0%	0.0%
Uppercase & special	2.6%	0.0%
Numeric & special	0.6%	0.0%
Lowercase, uppercase, & numeric	14.3%	16.9%
Lowercase, uppercase, & special	3.2%	9.7%
Lowercase, numeric, & special	7.8%	16.9%
Uppercase, numeric, & special	0.0%	3.3%
All four character subsets	14.3%	29.9%
Passwords in 1 subset	21.4%	4.5%
Passwords in 2 subsets	39.0%	18.8%
Passwords in 3 subsets	25.3%	46.8%
Passwords in 4 subsets	14.3%	29.9%

4 Conclusion

In this paper, we have outlined how Persuasive Technology can be used to improve passwords by reducing the likelihood that passwords can be guessed systematically, and thus increasing the security of users' online accounts (and the accompanying resources and capabilities thereof). Although the approach described in this paper uses a modest number of PT strategies, it yields a useful improvement in password strength, and we therefore believe the approach is worth further study.

Generalised advice and feedback have had limited success in helping users create more secure passwords. The main advantage of our approach is that it increases password strength while promoting password memorability through user involvement.

Our approach involves altering only the password creation step in the authentication process. Thus, PTP should be easily integrated with most password systems since it only requires minor modifications to the end-user interface and no changes to the password server. Moreover, the visibility of how passwords are made more secure can help form users' mental models of stronger passwords, which may lead them to create stronger passwords where our approach is not built-in.

Our immediate future work involves three lines of inquiry. We wish to expand our study with participants more typical of the online population, compare our results to a

control group, and test password memorability over longer periods of time as well as with more system-assigned characters. Secondly, we wish to refine our improvement strategy with regard to well-known patterns of systematic guessing, such as words, names, and other character patterns. Finally, we plan to increase the level of persuasion involved, leveraging more PT strategies.

References

1. Adams, A., Sasse, M.A.: Users Are Not The Enemy. Communications of the ACM 42(12), 41–46 (1999)
2. Burr, W.E., Dodson, D.F., Polk, W.T.: Electronic Authentication Guideline. NIST Special Publication 800-63, Version 1, pp. 1–53 (2004)
3. Forget, A., Chiasson, S., Biddle, R.: Persuasion as Education for Computer Security. In: Association for the Advancement of Computing in Education (AACE) E-Learn, pp. 822–829 (2007)
4. Chiasson, S., van Oorschot, P.C., Biddle, R.: A Usability Study and Critique of Two Password Managers. In: 15th USENIX Security Symposium, pp. 1–16 (2006)
5. Florencio, D., Herley, C.: A Large-Scale Study of Web Password Habits. In: 16th International World Wide Web Conference (WWW), pp. 657–666 (2007)
6. Fogg, B.J.: Persuasive Technology: Using Computers to Change What We Think and Do. Morgan Kaufmann, San Francisco (2003)
7. Furnell, S.: An assessment of website password practices. J. Computers & Security 26(7-8), 445–451 (2007)
8. Gasser, R., Brodbeck, D., Degen, M., Luthiger, J., Wyss, R., Reichlin, S.: Persuasiveness of a Mobile Lifestyle Coaching Application Using Social Facilitation. In: IJsselsteijn, W., de Kort, Y., Midden, C., Eggen, B., van den Hoven, E. (eds.) Persuasive 2006. LNCS, vol. 3962, pp. 27–38. Springer, Heidelberg (2006)
9. Kuo, C., Romanosky, S., Cranor, L.F.: Human Selection of Mnemonic Phrase-based Passwords. In: 2nd Symposium on Usable Privacy and Security (SOUPS), pp. 67–78 (2006)
10. Lucero, A., Zuloaga, R., Mota, S., Muñoz, F.: Persuasive Technologies in Education: Improving Motivation to Read and Write for Children. In: IJsselsteijn, W., de Kort, Y., Midden, C., Eggen, B., van den Hoven, E. (eds.) Persuasive 2006. LNCS, vol. 3962, pp. 142–153. Springer, Heidelberg (2006)
11. Peterson, L.R., Peterson, M.J.: Short-term retention of individual verbal items. J. Experimental Psychology 58(3), 193–198 (1959)
12. Sasse, M.A.: Computer Security: Anatomy of a Usability Disaster, and a Plan for Recovery. In: ACM CHI 2003 Workshop on HCI and Security Systems (2003)
13. Shostack, A., Syverson, P.: What Price Privacy (and why identity theft is about neither identity nor theft). In: Camp, L.J., Lewis, S. (eds.) Economics of Information Security, pp. 129–142. Kluwer Academic, Norwell (2004)
14. Solar Designer: John the Ripper password cracker (2006) (accessed, March 2008), http://www.openwall.com/john/
15. Sterns, A., Mayhorn, C.: Persuasive Pillboxes: Improving Medication Adherence with Personal Digital Assistants. In: IJsselsteijn, W., de Kort, Y., Midden, C., Eggen, B., van den Hoven, E. (eds.) Persuasive 2006. LNCS, vol. 3962, pp. 195–198. Springer, Heidelberg (2006)
16. Weirich, D., Sasse, M.A.: Pretty Good Persuasion: A first step towards effective password security in the real world. In: 7th New Security Paradigms Workshop, pp. 137–143 (2001)
17. Whitten, A., Tygar, J.D.: Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In: 8th USENIX Security Symposium, pp. 169–183 (1999)
18. Yan, J., Blackwell, A., Anderson, R., Grant, A.: Password Memorability and Security: Empirical Results. IEEE Security & Privacy Magazine 2(5), 25–31 (2004)