Improving the Password Selection Mechanism

Richard M. Conlan
Northeastern University CC&IS
360 Huntington Ave, 202WVH
Boston, MA 02215 USA
(617) 373-5280
kaige@ccs.neu.edu

Peter Tarasewich
Northeastern University CC&IS
360 Huntington Ave, 202WVH
Boston, MA 02215 USA
(617) 373-2078
tarase@ccs.neu.edu

ABSTRACT

Conventional wisdom seems to have concluded that traditional passwords are inherently insecure. We feel that these conclusions are premature. Our current research is reexamining the problem of password selection and memorability through the exploration of password selection mechanisms with novel interface designs. During the spring of 2006 we did work that was published as a CHI2006 work-in-progress paper summarizing the initial study. This poster is intended to extend upon that by further defining the methodology of that work, presenting preliminary results motivating further study, and by soliciting participation in the next phase of the study. The goal of this research is develop both principles and designs that help users to choose passwords that are secure and memorable.

1. INTRODUCTION

Conventional wisdom seems to have concluded that traditional passwords are inherently insecure. This argument has been adopted by major organizations such as Microsoft [3] and RSA Security [4], and is reflected in much of the literature. The argument is usually that users choose bad passwords and cannot be expected to remember strong passwords.

We feel that these conclusions are premature and that this argument is flawed. At present most password selection mechanisms (PSMs) are not designed according to basic HCI principles and we believe that this is highly responsible for the above conclusions. Our current research is reexamining the problem of password selection and memorability through the exploration of PSMs with novel interface designs.

1.1 Analysis of Current Selection Mechanisms

PSMs such as the applet depicted in Figure 1 are incredibly common, and yet they violate basic tenets of human computer interaction (HCI) and well-known design principles. The purpose of the PSM is to allow the user to select a new password. It could be argued that it is designed well for this purpose since it is obvious where to enter the old password, the new password, and what button to select. However, as corporations and individuals have become more concerned about security the PSM has gained the additional purpose of ensuring that the user selects a *secure* password.

Unfortunately, the standard PSM is not well suited to this task – a simple PSM offers no security context at all. To address this shortcoming, password complexity constraints were added to the simple PSM model. But these merely create a security threshold – they do not help the user to choose a good password. In fact, passwords that fail to meet the threshold often result in a response such as “The password failed to meet complexity requirements,” which offers so little information that the user does not necessarily know how to proceed. This is a clear violation of the third golden rule of interface design – *offer informative feedback* [6].

The current design of PSMs does little to help the user choose a good password. At best the user can keep trying passwords until they find one that works, but has no sense of progress from one attempt to the next. The findings in [1] and [5] support the claim that current PSMs have failed to adequately incorporate usability principles into their design.

2. METHODOLOGY

During the spring of 2006 we did work that was published as a CHI2006 work-in-progress paper summarizing the initial study. Here we present the methodology in much more detail than was included in the CHI paper.

We designed four PSMs to evaluate different user interface approaches. Each was implemented as a Java applet and subject to internal review and refinement. We then implemented the Dropbox-Online homework submission system, which was designed to be a simple but usable homework submission system which incorporated the applets when prompting users for password changes.

2.1 Applets

Each of the applets presents a different user interface notion, though we attempted to keep them as similar as possible besides the method of interface. When the user is selecting a new password each applet is driven by the same Password Quality Score algorithm and the interface elements are updated according to the same threshold levels. In addition to submitting the chosen password and the PQS, each applet also keeps track of whether the user clicked the Help button.

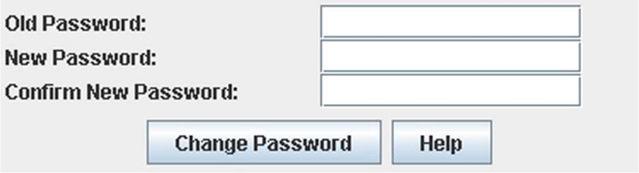
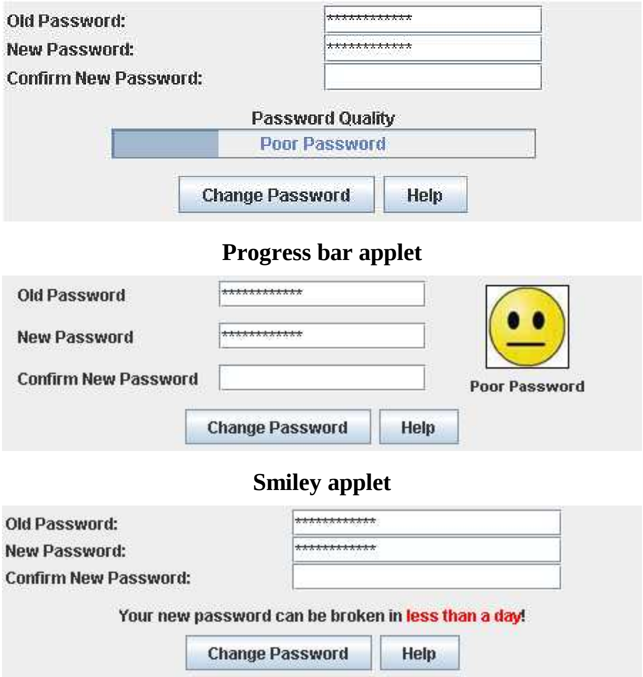


Figure 1. Control applet.

The control applet is depicted in Figure 1 and each of the experimental applets are depicted in Figure 2. The *Control applet* is intended to represent the typical situation at current, which is to offer no feedback at all on the password quality.



Old Password: *************
New Password: *************
Confirm New Password:

Progress bar applet

Old Password *************
New Password *************
Confirm New Password

Smiley applet

Old Password: *************
New Password: *************
Confirm New Password:

Your new password can be broken in less than a day!

Warning applet

Figure 2. Experiment applets.

The *Progress bar* applet offers feedback through progress bar, which reflects an approach seen in some existing software packages and is tempting because it relies on widgets available in many GUI frameworks. The *Smiley applet* is perhaps the most novel of the interfaces, expressing password quality by varying the perceived happiness of the avatar. The *Warning applet* attempts to motivate the user through fear by suggesting how long it would take an attacker to crack the password.

2.2 Dropbox-Online

The Dropbox-Online system was then used for homework submission by two CC&IS classes at NEU. The students were not told that a study was under way due to fear that foreknowledge of a study focused on password quality would skew the results. At the end of the semester we took a few minutes out of one of the final class periods to explain the study and its purpose to the students and solicit their permission to use their password data in the study. We offered two levels of participation– they could choose to participate by granting us access only to their Password Quality Score (PQS) data or they could grant us access to all of their password data.

The Dropbox-Online system also tracked how often users experienced erroneous logins and how many times each user had to reset their password during the course of the semester. It stored passwords using MySQL's password hash function for login purposes and using 4096-bit RSA encryption to enable password recovery in those cases that consent was received. The public key was stored off-site, and the password data of all non-participants was deleted without examination.

2.3 Participation

This was designed as a between-subjects study. Between the two classes there were 67 students. The applets were distributed evenly over the classes and assigned to individuals at random. Throughout the semester there were three mandatory password changes, though some students performed additional changes either of their own volition or because of a forgotten password.

Of the 67 students, 39 consented to be included in the study by granting access to at least their PQS data. Of these only 15 granted us access to their full password data. This suggests that the two-tiered approach may be appropriate for these sorts of studies where it is hard to know ahead of time how many participants will consent due to the sensitive nature of the data.

3. PRELIMINARY RESULTS

Results were not ready by the poster abstract deadline, but those resulting from our preliminary analysis would be included in the SOUPS poster.

4. FUTURE WORK

We are currently working to set up a larger study by involving students and faculty from other universities. Our intent is to open up the Dropbox-Online homework submission system for use by anybody willing to allow us to compile and examine the password quality data gathered through their usage of the system. Those interested will use the system throughout the coming fall semester and then solicit consent from subjects at the end of the semester in a similar manner to the preliminary study. We would then correlate results across all consenting subjects.

The Dropbox-Online homework submission system is online at https://www.dropbox-online.com. Demo accounts are available on request for anybody interested. The four applets are available for examination online at:

http://www.embracetherandom.com/changePasswordUIStudy/

This site is also intended to serve as a focal point for research done by ourselves and others into how user interface design affects password quality. If you are doing research in this field and would like it linked to from here, please let us know.

For more information please feel free to contact us.

5. REFERENCES

[1] Adams, A., Sasse, M. A. *Users are not the enemy*. In *Comm. ACM*, Vol. 42, No. 12, 1999.

[2] Conlan, R., Tarasewich, P. *Improving Interface Design To Help Users Choose Better Passwords*. CHI, April, 2006.

[3] Ilett, D. *Gates: Passwords passé*. CNET News.com. Nov. 16, 2004. Available at: http://tinyurl.com/bcqt5.

[4] *Passwords vs. Strong Authentication*. RSA Security. Available at: http://tinyurl.com/cru4a.

[5] Sasse, M.A., Brostoff, S., and Weirich, D. *Transforming the 'weakest link': a human-computer interaction approach to usable and effective security*. BT Technical Journal, Vol 19 (3), Jul. 2001, 122-131.

[6] Schneiderman, B. *Designing the User Interface: Strategies for Effective Human-Computer Interaction*. 4th Ed. Addison-Wesley, various locations, 2004