CERIAS

the center for education and research in information assurance and security

Memorability Issues Associated with Updating Passwords

Devin G. O'Brien and Robert W. Proctor, Department of Psychological Sciences
Kim-Phuong L. Vu, Department of Psychology, CSU Long Beach

Introduction

- The username-password method is the most common technique used for authenticating users.
- However, if users generate passwords that are easy to crack, then unauthorized users can gain access to personal and organizational information.
- This can cause serious damage to property and could produce personal and financial costs.
- By filtering out poorly constructed passwords through a process known as *proactive password checking*, users are prevented from selecting insecure passwords (Vu et al., 2007).
- Proactive password generation with a first-letter mnemonic technique, in which users generate a sentence and then form a password using the first letters of the words, results in secure passwords when a digit and special character are included (Proctor et al., 2002).
- Recent security practices have users update their passwords after a specified time period. How the memorability of the passwords is affected by this updating procedure is an important issue that is examined in this study.

Method

Participants

18 students from Purdue University's Introductory Psychology Subject Pool participated in the experiment.

Design and Procedure

- Participants were asked to generate passwords for 5 fictitious accounts (Amazon, Bank, Ebay, Email and Facebook).
- A set of proactive checking guidelines was used to decrease password crackability. This method required that the password be at least 6 characters long, contain an uppercase letter, contain a lowercase letter, contain a digit, contain a special character (e.g., $, or *), be unique from the passwords they use for their real accounts and not contain the person name or variation of it.
- ***Generation:*** Participants had to generate an acceptable password for each account using the first-letter mnemonic technique, and the generation times and number of attempts required to generate an acceptable password were measured.
- ***Short-term Recall:*** 5 minutes after generating the passwords, participants were given a short-term recall test.
- ***Long-Term Recall and Update:*** Two days later, participants returned and engaged in long-term recall of their passwords. Afterwards, they were asked to update their passwords and engage in short-term recall 5 minutes later. This procedure was repeated after another two days.
- ***Final Recall:*** a final session for recall of the last set of generated passwords was held one week later.

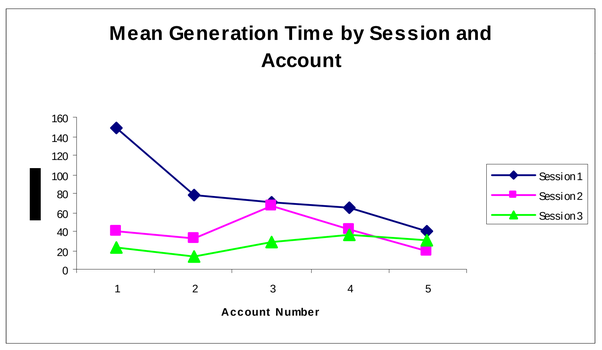
Memory Dependent Measures

- The number of recall attempts and time to accurately recall the passwords for each account were measured
- The number of passwords forgotten by participants for each session.

Results

Generation

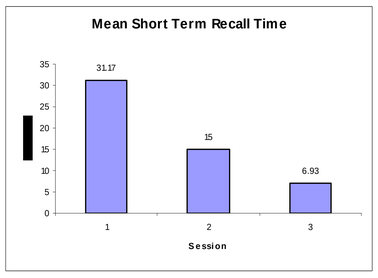
- Mean generation time for each account was submitted to a 3 (Session) x 5 (Accounts) ANOVA.
- All effects were significant. Participants took longer to generate the passwords in the first session than to update them in the subsequent sessions, $F(2,34) = 3.28$, $p < .001$.
- Generation time became shorter as participants generated the password for the first to fifth account, $F(4,68) = 4.51$, $p = .003$. The Session x Account interaction showed that the decrease in generation time for the first to fifth account was larger in Session 1 than in Sessions 2 and 3, $F(8,136) = 7.85$, $p < .001$.

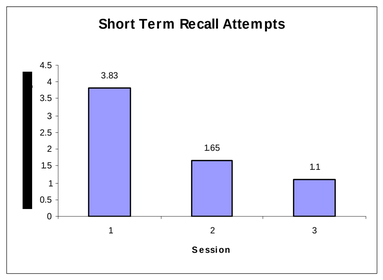


- For number of generation attempts, only the main effect of Session was significant, $F(2,34) = 5.28$, $p = .010$: Participants took more attempts when having to update their passwords in Session 2 ($M = 4.27$) than for generating their passwords in Session 1 ($M = 1.61$) and updating them in Session 3 ($M = 2.62$).

Short-term Retention

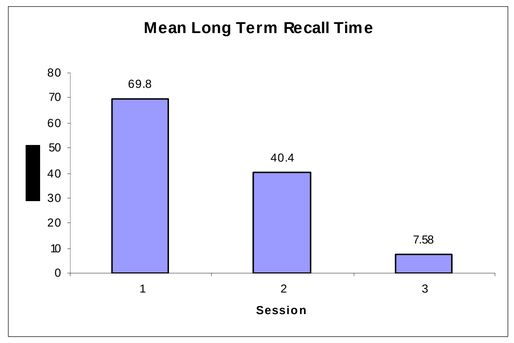
- Mean short-term recall time and number of attempts were submitted to 3 (Session) x 5 (Accounts) ANOVAs. For both analyses, only the main effect of Session was significant, with participants taking less time to recall their generated passwords in the second and third sessions, $F(2,34) = 3.28$, $p = .001$, and making fewer attempts, $F(2,34) = 3.28$, $p = .001$.





Long-term Retention

- For correctly recalled trials, mean long-term recall time and number of attempts were submitted to 3 (Session) x 5 (Accounts) ANOVAs. For recall time, only the main effect of Session was significant, $F(2,2) = 19$, $p = .013$, where recall time decreased across sessions.
- The number of long-term recall attempts showed no significant effects.
- When the number of passwords forgotten was analyzed as a function of short- and long-term retention, there was a main effect of retention interval, $F(1,17) = 4.45$, $p < .001$. No participants forgot any of the passwords tested after the 5-minute interval, though participants forgot roughly 1 password (20% of the passwords) for each of the long-term sessions.



How Participants Update Passwords

- The first analysis looked at how many characters of the password changed from the original password when participants updated the password. Participants showed a decrease in the number of changes made from 62% in the first to second generation to 49% from the second to third generation, $F(1,17) = 4.45$, $p = .017$. These results imply that the first time that users had to update their password, they put more effort into changing the password than they did for the subsequent update.
- The second analysis looked at how the password length changed across the original generation and the subsequent updates. Participants reduced their average password length across updates from 7.7 in session 1 to 7.1 in session 2 and 6.8 in session 3, $F(2,34) = 3.28$, $p < .001$.

Conclusions

- Generating a password for the first account on the first day took the longest, with generation time decreasing across accounts in that session and in succeeding sessions. This effect can be attributed to participants' inexperience with use of proactive password checking schemes.
- Allowing participants to engage in short-term recall showed a decrease in time and the number of attempts to correctly recall one's password. These effects can be attributed to gaining familiarity with mnemonic based passwords.
- When participants have to update their passwords, they often modify old ones.
- Participants who forgot passwords did so after a long-term interval (2 days or 1 week) and showed no forgetting after the short term 5 minute interval. Participants forgot 20% of their passwords on average for each session.

References

Proctor, R. W., Lien, M. C., Vu, K.-P. L., Schultz, E. E., & Salvendy, G. (2002). Improving computer security for authentication of users: Influence of proactive password restrictions. *Behavior Research Methods, Instruments, & Computers, 34*, 163-169.

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

We thank Abhilasha Bhargav-Spanzel for her programming assistance with this project.

PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center