A Framework for Creating Secure and Memorable Passwords

Emergent Research Forum (ERF)

Martha Wagner McNeil
Dakota State University
Martha.McNeil@trojans.dsu.edu

Omar El-Gayar
Dakota State University
Omar.El-Gayar@dsu.edu

Cherie Noteboom
Dakota State University
Cherie.Noteboom@dsu.edu

Abstract

Despite their pitfalls, passwords remain ubiquitous. Users are encouraged to make passwords that are easy to remember and hard to guess, but as the number of information systems (IS) accounts per user proliferates, this is easier said than done. We tackle the competing goals of security and memorability, applying design science to create a framework for producing personalized algorithms which users may then use to create passwords that are both secure and memorable.

Keywords

Password, information security, identification, authentication, design science.

Introduction

Passwords remain the most widely used authentication mechanisms deployed in information systems (IS) today because they are inexpensive to implement, uncomplicated for users to operate, commonly accepted, and levy no special hardware requirements on users (Bonneau et al. 2012). While individuals cope with proliferating passwords, few studies have focused on ways to balance password usability and security. We propose a framework to help users create passwords that are both secure and memorable.

Many password issues result from human frailties that pose obstacles to making strong passwords, including issues of memory, ability, and understanding. Sometimes users create weak passwords that they think are strong while others fail to understand the threat. Most people can create and remember a few strong passwords; however, with the explosion of internet-based services, users have an ever-growing number of IS accounts. These conditions lead to insecure behaviors which undermine IS security. Most users want to create strong passwords because it is in their own best interests (Mwagwabi et al. 2014). To promote strong passwords and improve IS security, a method is needed to lower password usability hurdles, while supporting the security intent of passwords, accounting for human memory limitations, and accommodating portability and trust concerns.

The remainder of this paper is organized as follows. First, we discuss related research. Specific to design science, we enumerate the objectives of an effective solution and discuss plans for the design, development, and evaluation of the framework. Finally, we summarize and discuss limitations and future work.

Related Research

Alternatives to the framework. Other techniques, including biometrics, hardware tokens, visual/auditory cues, and even Choose Your Own Authentication (CYOA) have been proposed as alternatives to passwords. While many of the alternatives may alleviate password memorability and strength issues; none has been shown to stand out from all the others on various important measures (Bonneau et al. 2012; Forget et al. 2015). In particular, many of the proposed password alternatives

require change on the system-side of the password equation, a situation which individual users are powerless to affect. Thus, we focus on approaches that reside entirely on the user-side.

A commonly-used strategy for remembering passwords is to write them down on paper. Some experts advise against this; however, when stored securely, writing passwords down supports memorability, allowing users to make more secure passwords and limit password reuse. Moreover, such lists are not susceptible to malware (Reeder and Consolvo 2015). Unfortunately locking a list in a safe is the antithesis of portability. Some users maintain a digital list of passwords, which is more portable in some ways and can be stored securely via encryption. But this approach is more vulnerable to hacking than its paper counterpart and both the file format and encryption method used may affect portability.

Password manager applications allow the user to make many strong and unique passwords, while only remembering one secure master password. The manager stores all the user's passwords within, usually protected by encryption. Unfortunately, portability and trust issues hamper acceptance of password managers. Notably, if the master password or the manager itself is compromised, all of the user's passwords are at once exposed. In addition, managers may not work across all of the user's devices (Gasti and Rasmussen 2012; Hayashi and Hong 2011; Li et al. 2014; McCarney et al. 2012; Silver et al. 2014). Finally, they may be counterproductive to password self-efficacy (Zhang et al. 2009).

Versipass addresses the main trust issue with password managers, exposure of the user's passwords due to compromise of the manager. Versipass stores password cues rather than passwords. A cue helps the user remember an associated password, but does not immediately reveal the password (Stobert and Biddle 2014). Versipass stores information necessary to generate the associated passwords. If compromised, this raises privacy concerns and could simultaneously lock the user out of all his accounts requiring many password resets. Moreover, as implemented, Versipass does not support all platforms.

Mnemonic strategy is an approach in which the user selects a memorable phrase and compresses it into a password (e.g. by taking the first letter of each word). (Wright et al. 2012) found that passwords created this way can be stronger if the user is coached on secure phrase selection and transformation. Absent adequate guidance, users often select common phrases and follow predictable rules leading to crackable passwords. According to (Kuo et al. 2006) mnemonic passwords based on common phrases may become susceptible to dictionary attack as cracking tools improve. A mnemonic strategy algorithm can be produced from our proposed framework using a single phrase and rule. But this algorithm will yield just one password. In order to have unique passwords for multiple accounts, the mnemonic strategy algorithm alone is not enough.

Human memory. The average human can learn seven plus or minus two items (Miller 1956) with some improvement gained by chunking and coding (Clark and Paivio 1991; Gobet et al. 2001). Recall is also aided when information can be organized in multiple ways and/or linked to images. Memory depends on learning, a process that encompasses sensory input, attention, and processing (Wesson 2017). Mnemonics are a form of elaborative processing which has been shown to improve password recall by encoding the information into an organizational structure (Wright et al. 2012; Yan et al. 2004). Depth of processing (i.e. drawing relationships between items) can also improve recall. Prior password research has applied memory theory to password recall. (Camp et al. 2016) found that linkage to episodic memory, a person's memory of past experiences, supported recall in context. (Stobert and Biddle 2013) investigated memory retrieval, finding that combining cued recall with recognition produced good password recall with faster login time. (Vu et al. 2007) observed that recall is improved when users actively generate their own passwords. Proactive interference can prevent a user from remembering a particular password because they have many other passwords (Bunting 2006).

Objectives of a Solution

A viable solution to the password issues discussed will satisfy the following objectives: (1) support creation of passwords that are both secure and memorable, (2) accommodate common password policies, (3) accommodate at least 20 passwords per user, (4) improve the user's overall self-efficacy in the password process, (5) accommodate user preference in the items and methods used to create the passwords, (6) require that the user learn no more than 7-9 items of information, (7) use only information from the user's memory (i.e. not require digital storage of either the passwords or the facts/rules used to generate them), and (8) be accessible across all platforms for which the user requires passwords with no implied

authentication system changes. Objectives 1-4 support the intent of passwords as a viable access control mechanism, 5-6 account for human memory limits, and 7-8 accommodate portability and trust concerns.

Research Method and Design

We align our research with the design science research method (DSRM) (Peffers et al. 2007), consisting of six key activities: identify and motivate the problem, define objectives of a solution, design and develop an artifact, demonstrate, rigorously evaluate, and communicate results.

The Framework

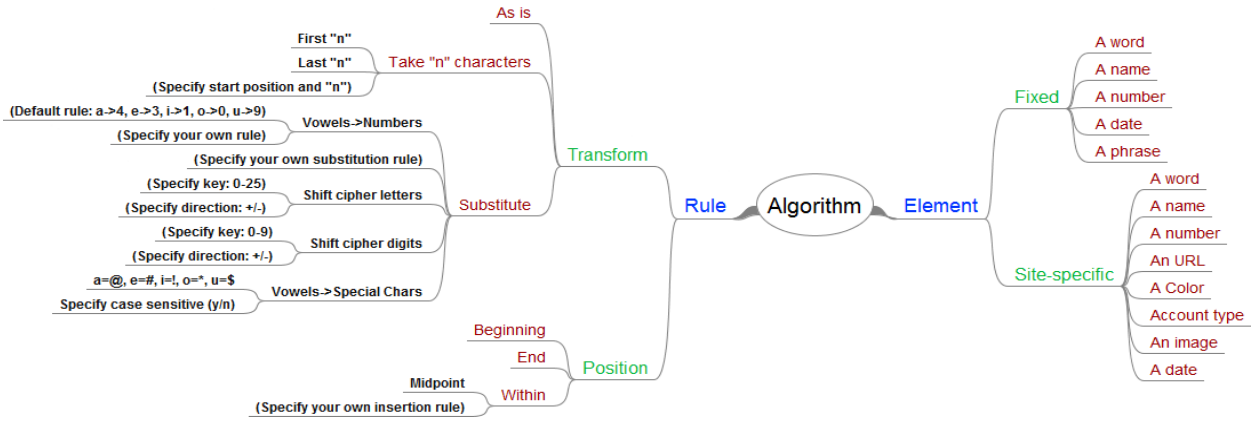

Figure 1. Notional Design of the Framework

We propose to develop a framework which can be used to generate personalized password algorithms. A notional design for the framework is shown in Figure 1. Our concept is to devise an extensible framework composed of sets of password elements and composition rules. The initial sets of elements and rules will be derived from prior password research and our creativity, but the framework will accommodate the addition of new elements and rules. Some example elements and rules are shown in Figure 1. The user will select a small, easily remembered, and personalized subset of the available elements and rules. In conjunction with human memory and password strength heuristics from the literature, the framework will help the user incorporate his selected elements and rules to yield a password creation algorithm that is uniquely his own. Then, instead of remembering and keeping secret a long list of passwords, the user will only have to remember, apply, and guard the algorithm. We anticipate that the algorithm will be easier to remember than the set of passwords generated from it because instances of the selected elements will be derived from information the user intrinsically knows (i.e. episodic memory), and the number of choices made to construct the personalized algorithm (the new information the user has to learn) will be within the bounds of Miller's "magic number" 7. In addition, the framework leverages elaborative processing, depth of processing, and active generation. Figure 2 illustrates an example application of the framework to create an algorithm. In the example, the user must learn four element/rule pairs.

Choice 1 - Fixed element: value "@9$" - Transform: as-is Choice 2- Site-specific element: Account name - Transform: drop non-alphas, first 6, shift +2 - Position: beginning Choice 3 - Fixed element: value "Moody Blues" - Transform: drop spaces, first 5, replace vowels with digits - Position: beginning	Choice 4 - Site-specific element: Account type [Financial, Other, Medical, Shopping, Social] - Transform: first character of - Position: beginning An example password generated from the algorithm for Shopping.com --> `SM00dyUjqrrk@9$`.

Figure 2. Example Application of the Framework

An initial instantiation of the artifact will be a document that describes example elements and rules, steps the user through the workflow, and includes detailed instructions to help the user distinguish choices that

may lead to weak vs. strong passwords per the findings in (Wright et al. 2012). While the framework is intended to facilitate the creation of strong passwords, it does not guarantee this outcome. It is primarily a tool to help the user organize his thoughts in the password creation process and must be used in conjunction with password strength guidance. Instantiation as an application is left to future work, pending successful evaluation of the framework under manual operation.

Demonstration and Evaluation

The effectiveness of the framework will be demonstrated and evaluated by utilizing it in an experimental situation to measure how well it solves the problem. Two treatments (framework and control) are envisioned with random assignment of subjects. The former will create passwords using their personalized algorithms while the latter will create passwords in an ad hoc process. We plan to use an evaluation strategy based on several techniques discussed in (Wright et al. 2012). To compare the usability of passwords derived via the framework versus the control, we will measure password creation time, short- and long-term recall success, and the cognitive loads imposed during password creation and recall. Cognitive load will be measured using the instrument described in (Hadie and Yusoff 2016; Leppink et al. 2013). To objectively assess password strength we will compare the probability distributions of passwords produced by the two treatments, utilizing automated password guessing and the β-guess-rate statistic (Bonneau 2012) which measures the expected success rate of a guesser when given a finite number of guesses per account. Finally, per Wright's observation that contemporary guessing tools are inherently disadvantaged against novel password strategies, we will tune the guessing method based on the framework.

Summary, Limitations, and Future Work

Our contribution is a theoretical framework for creating secure and memorable passwords to reduce the costs associated with forgotten passwords, improve password usability, and support IS security. A limitation of the framework, mentioned above, is that it does not guarantee strong passwords in the absence of password strength guidance. A future instantiation as a software tool could guide the user through the workflow, present element/rule templates, coach the user towards secure selections, account for common password policies, visualize the algorithm, and provide a password strength meter. Future work could also include adding new elements and composition rules and evaluating the framework under a variety of password policies and contexts.

REFERENCES

Bonneau, J. 2012. "The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords," *Proceedings - IEEE Symposium on Security and Privacy*, pp. 538–552.

Bonneau, J., Herley, C., Van Oorschot, P. C., and Stajano, F. 2012. "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes," *Proceedings - IEEE Symposium on Security and Privacy*, pp. 553–567.

Bunting, M. 2006. "Proactive Interference and Item Similarity in Working Memory," *Journal of Experimental Psychology: Learning Memory and Cognition* (32:2), pp. 183–196.

Camp, L. J., Abbott, J., and Chen, S. 2016. "CPasswords: Leveraging Episodic Memory and Human-Centered Design for Better Authentication," *Proceedings of the Annual Hawaii International Conference on System Sciences* (2016–March), pp. 3656–3665.

Clark, J. M., and Paivio, A. 1991. "Dual Coding Theory and Education," *Educational Psychology Review* (3:3), pp. 149–210.

Forget, A., Chiasson, S., and Biddle, R. 2015. "Choose Your Own Authentication," *Proceedings of the 2015 New Security Paradigms Workshop*, pp. 1–15.

Gasti, P., and Rasmussen, K. B. 2012. "On the Security of Password Manager Database Formats," in *European Symposium on Research in Computer Security*, Springer Berlin Heidelberg, pp. 770–787.

Gobet, F., Lane, P. C. R., Croker, S., Cheng, P. C.-H., Jones, G., Oliver, I., and Pine, J. M. 2001. "Chunking

Mechanisms in Human Learning," *Trends in Cognitive Sciences* (5:6), pp. 236–243.

Hadie, S. N. H., and Yusoff, M. S. B. 2016. "Assessing the Validity of the Cognitive Load Scale in a Problem-Based Learning Setting," *Journal of Taibah University Medical Sciences* (11:3), Elsevier Ltd, pp. 194–202.

Hayashi, E., and Hong, J. 2011. "A Diary Study of Password Usage in Daily Life," *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 2627–2630.

Kuo, C., Romanosky, S., and Cranor, L. F. 2006. "Human Selection of Mnemonic Phrase-Based Passwords," *SOUPS '06: Proceedings of the Second Symposium on Usable Privacy and Security*, pp. 67–78.

Leppink, J., Paas, F., Van der Vleuten, C. P. M., Van Gog, T., and Van Merriënboer, J. J. G. 2013. "Development of an Instrument for Measuring Different Types of Cognitive Load," *Behavior Research Methods* (45:4), pp. 1058–1072.

Li, Z., He, W., Akhawe, D., and Song, D. 2014. "The Emperor's New Password Manager: Security Analysis of Web-Based Password Managers," *23rd USENIX Security Symposium (USENIX Security 14)*, pp. 465–479.

McCarney, D., Barrera, D., Clark, J., Chiasson, S., and van Oorschot, P. C. 2012. "Tapas: Design, Implementation, and Usability Evaluation of a Password Manager," *Proceedings of the 28th Annual Computer Security Applications Conference on - ACSAC '12*, pp. 89–98.

Miller, G. A. 1956. "The Magical Number Seven, Plus or Minus Two: Some Limits on Our Capacity for Processing Information," *Pyschological Review* (63), pp. 81–97.

Mwagwabi, F., McGill, T., and Dixon, M. 2014. "Improving Compliance with Password Guidelines: How User Perceptions of Passwords and Security Threats Affect Compliance with Guidelines," *Proceedings of the Annual Hawaii International Conference on System Sciences*, pp. 3188–3197.

Peffers, K., Tuunanen, T., Rothenberger, M. a., and Chatterjee, S. 2007. "A Design Science Research Methodology for Information Systems Research," *Journal of Management Information Systems* (24:3), pp. 45–77.

Reeder, R., and Consolvo, S. 2015. "'... No One Can Hack My Mind': Comparing Expert and Non-Expert Security Practices," *Symposium on Usable Privacy and Security*, pp. 327–346.

Silver, D., Jana, S., Boneh, D., Chen, E., and Jackson, C. 2014. "Password Managers: Attacks and Defenses," *Proceedings of the 23rd USENIX Security Symposium*, pp. 449--464.

Stobert, E., and Biddle, R. 2013. "Memory Retrieval and Graphical Passwords," *Proceedings of the Ninth Symposium on Usable Privacy and Security - SOUPS '13*, p. 1.

Stobert, E., and Biddle, R. 2014. "A Password Manager That Doesn't Remember Passwords," *Proceedings of the 2014 Workshop on New Security Paradigms Workshop*, pp. 39–52.

Vu, K. P. L., Proctor, R. W., Bhargav-Spantzel, A., Tai, B. L. (Belin), Cook, J., and Eugene Schultz, E. 2007. "Improving Password Security and Memorability to Protect Personal and Organizational Information," *International Journal of Human Computer Studies* (65:8), pp. 744–757.

Wesson, K. 2017. "Learning and Memory: How Do We Remember and Why Do We Often Forget?," *Brain World*. (http://brainworldmagazine.com/learning-memory-how-do-we-remember-and-why-do-we-often-forget/, accessed April 21, 2018).

Wright, N., Patrick, A. S., and Biddle, R. 2012. "An Empirical Study of Mnemonic Sentence-Based Password Generation Strategies," *Proceedings of the Eighth Symposium on Usable Privacy and Security - SOUPS '12*, p. 1.

Yan, J., Alan, B., Anderson, R., and Grant, A. 2004. "Password Memorability and Security: Empirical Results," *IEEE Security and Privacy* (2:5), pp. 25–31.

Zhang, J., Luo, X., Akkaladevi, S., and Ziegelmayer, J. 2009. "Improving Multiple-Password Recall: An Empirical Study," *European Journal of Information Systems* (January), pp. 1–12.