ACM Interactions, vol. 13, no. 3 (2006), pp. 38-40
Preprint version

Minimal-Feedback Hints for Remembering Passwords

Morten Hertzum
Computer Science, Roskilde University, Roskilde, Denmark
Phone: +45 4677 3077, email: mhz@ruc.dk

Passwords are a widely used mechanism for user authentication and thus critical to the security of many systems. To provide effective security, passwords should be known to the password holder but remain unknown to everybody else. While personal information and real words are relatively easy for a user to remember they make weak passwords from a security point of view because they are vulnerable to informed guessing and dictionary attacks. Strong passwords (e.g., b5j#Kv!8N) are less vulnerable to attack but at the same time more difficult to remember. However, the sheer number of passwords people must have to accomplish their day-to-day activities exceeds most humans' capacity for remembering meaningless strings of characters [1]. Most users handle the ensuing conflict between security and ease of use by choosing passwords that are easy to remember, writing down their passwords, using the same password for multiple systems, or in other ways giving ease of use priority over security.

Minimal-feedback hints are introduced to support users in remembering their passwords and thereby enable them to choose stronger passwords. Whereas most password mechanisms leave it entirely to users to be able to remember their passwords, minimal-feedback hints aid users' memory by providing them with a couple of the password characters when prompted for their password, see Figure 1. Minimal-feedback hints were first suggested by Lu and Twidale [3] with the thinking that "a few carefully revealed hints will jog an authorized user's memory, but will be of insufficient help to an unauthorized user who does not know the password in the first place".

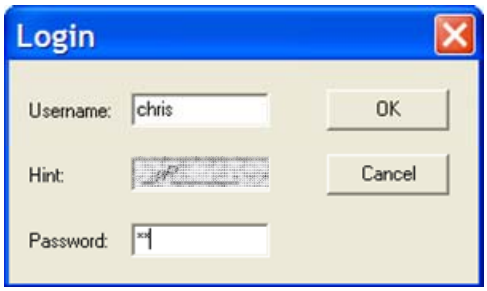

Figure 1. Password dialogue with minimal-feedback hint.

At password creation, users select the password characters that should be provided as hint. Then, the password with the hint characters revealed and all other characters replaced by, for example, underscores is converted to an image and slightly distorted. This conversion and distortion is done to provide additional security against password-cracking software. At login, the image is presented to users who will be able to determine which of their passwords must be the right one for this particular system, or to narrow down the set of likely passwords based on the hint. That is, the hint reveals the hint characters and their approximate position:

___ b _____ 8

In the example the first hint character, 'b', is preceded by one or more characters but is closer to the beginning of the password than to its end and the second hint character, '8', is the final character of the password.

A study was conducted to assess whether minimal-feedback hints (1) aid users' memory of their passwords, (2) make users more confident in the correctness of their memory of their passwords, and (3) coincide with password-creation strategies that yield strong passwords.

Fourteen users' ability to remember five passwords was assessed one week after creating them and four weeks after creating them. After one week, users remembered an average of 4.10 (*SD* = 1.52) passwords with the aid of hints. This was 1.70 passwords more than users remembered without hints, a significant improvement (all tests of significance were performed at the 0.05 level). After four weeks, users remembered an average of 3.36 (*SD* = 1.75) passwords with the aid of hints; 1.63 passwords more than without hints, again a significant improvement. Between the first and the fourth week users' ability to remember their passwords decayed slightly but not significantly. Thus, four weeks after creating their passwords the users remembered 67% of them correctly when aided by minimal-feedback hints (compared to 35% without the aid of hints). This success rate measures users' ability to remember their passwords in their first attempt. Given more than one attempt users will also succeed if the hints enable them to restrict the set of candidate passwords to a small number of alternatives.

The users indicated their confidence in the correctness of their memory of the individual passwords on a five-point scale from very uncertain (a rating of 1) to very certain (a rating of 5). Users were significantly more confident in the correctness of passwords recalled with the aid of minimal-feedback hints than without such hints. After four weeks, users' confidence averaged 4.04 (*SD* = 0.81) when they recalled passwords with the aid of hints. This was 1.33 more than their confidence without hints, a significant difference and consistent with their improved performance. The users' high level of confidence suggests that they considered minimal-feedback hints useful and may adopt them if introduced in operational systems.

With respect to password-creation strategies the users reported having applied several strategies to make their passwords memorizable. For example, an average of 2.21 of the five passwords created by each user contained one meaningful word and an additional 1.21 of each user's passwords contained two concatenated words. Five users created their passwords around words related to the topic of the service to which the password provided access, for example 'money' for the e-bank. On average, 1.71 of each user's passwords contained such a topical word. Only two of the users included characters other than letters and digits in their passwords. For each password the users selected one, two, or (in a few cases) three characters as their minimal-feedback hint. Users exploited the hints to amplify their password-creation strategies. This was mainly done by having the hints signal the start of the chunks of which passwords were constructed:

- The initial letter of every meaningful word contained in a password was often included in hints. On average, each user created 3.42 passwords containing meaningful words and for 2.29 of these passwords the hints included the initial letter of each of these words. Five users used this method for all their passwords.
- Often passwords ended in a number, and the initial digit of this number was included in the hint. On average, each user created 4.21 passwords ending in a number and for 2.29 of these passwords the first digit of the number was part of the hint. Four users used this method for all their passwords.

Without aids such as hints it is unrealistic to require that users always choose strong passwords, change them frequently, and never write them down. Weaker passwords and procedures for handling them are more vulnerable to various types of attacks. A frequent characteristic of the passwords created by the users was that they had one or more digits appended at the end. This is known as salting and incorporated in many password-cracking algorithms. The users' frequent use of topical words makes the passwords more vulnerable to informed guessing. Further, their use of real words, whether topical or not, increases the vulnerability of their passwords to dictionary attacks. This vulnerability is, however, partly mitigated when passwords contain two concatenated words. Finally, the vulnerability of passwords toward dictionary attacks will increase as still more powerful computers make it feasible to test passwords against still larger dictionaries [5]. While humans' capacity for memorizing passwords is not going to change appreciably over the next decades, still longer passwords will be needed to prevent password-cracking algorithms from brute-force testing all possible character strings.

While the users succeeded in using minimal-feedback hints to amplify their password-creation strategies, it appears that this amplification has been used primarily to make the passwords more memorizable and less to make them stronger. This suggests that minimal-feedback hints are most readily suitable for the diverse range of systems for which user authentication is necessary but of low to medium severity, including access to the members-only facilities of various associations' web sites, reviewer logins for journals and conferences, temporary access for customers to systems providing information about the delivery of their purchases, and so forth. It also suggests a supplementary need for user-authentication mechanisms that focus primarily on strength. Such mechanisms may, for example, include graphic challenges [4] and dynamic identity verification by means of keystroke characteristics [2].

REFERENCES

[1] Adams, A., and Sasse, M.A. Users are not the enemy. *Communications of the ACM*, 42, 12 (1999), 40-46.

[2] Leggett, J., Williams, G., and Usnick, M. Dynamic identity verification via keystroke characteristics. *International Journal of Man-Machine Studies*, 35, 6 (1991), 859-870.

[3] Lu, B., and Twidale, M.B. Managing multiple passwords and multiple logins: MiFA – minimal-feedback hints for remote authentication. In *Proceedings of the IFIP INTERACT 2003 Conference*. IOS Press, Amsterdam, 2003, 821-824.

[4] Pinkas, B., and Sander, T. Securing passwords against dictionary attacks. In *Proceedings of the 9th ACM Conference on Computer and Communications Security*. ACM Press, New York, 2002, 161-170.

[5] Schneier, B. *Secrets and Lies: Digital Security in a Networked World*. Wiley, New York, 2000.