In J. Kjeldskov, M.B. Skov, and J. Stage (eds.), *Proceedings of the Fourth Danish Human-Computer Interaction Research Symposium* (Aalborg, November 16), pp. 21-24. HCI Lab Technical Report No. 2004/1. Aalborg University, Aalborg, Denmark.

Remembering Multiple Passwords by Way of Minimal-Feedback Hints: Replication and Further Analysis

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

ABSTRACT

Passwords are a prominent mechanism for user authentication but entail a conflict between ease of use and security in that passwords must be both easy to remember for the password holder and difficult to guess for everybody else. To support users in remembering their passwords minimal-feedback hints for remote authentication (MiFA) provide users with a couple of the password characters when users are prompted for their password. In this study MiFA hints, originally devised by Lu and Twidale (2003), were evaluated by having 14 participants create five passwords each and prompting them for these passwords after one week and after four weeks. With the aid of MiFA hints participants remembered significantly more passwords and were significantly more confident in the correctness of their memory of their passwords than without hints. However, many of the passwords created by the participants were weak, for example a word followed by one or more digits, and vulnerable to dictionary attacks.

Categories and Subject Descriptors

K6.5 [**Management of computing and information systems**]: security and protection – *authentication*

General Terms

Experimentation, Security, Human Factors.

Keywords

Security, ease of use, user authentication, passwords, MiFA.

1. INTRODUCTION

Passwords are a widely used mechanism for user authentication and thus critical to the security of many systems [1, 11, 12]. To provide effective security, passwords should be known to the password holder but remain unknown to everybody else. While passwords such as personal information and real words are relatively easy for a user to remember they are weak 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].

Lu and Twidale [8] suggested a technique, minimal-feedback hints for remote authentication (MiFA), for supporting users in remembering their passwords. The distinguishing characteristic of MiFA is to aid users' memory by providing them with a couple of the password characters when prompted for the password. This study replicates the study by Lu and Twidale [8] to assess whether MiFA 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.

2. MINIMAL-FEEDBACK HINTS

Most user-authentication mechanisms present users with a blank password field and leave it entirely to users to be able to remember their passwords. MiFA hints introduce minimal feedback 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" [8].

At the time of password creation, users will select which characters from their newly created password should be provided as hint. Then, the password with the hint characters revealed and all other characters replaced by, for example, asterisks 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 account, or to narrow down the set of likely passwords based on the hint. Lu and Twidale's [8] exploratory study indicates that with MiFA hints users remember 75% of their passwords correctly in their first attempt. Their study involved five users who were prompted for their passwords ten days after creating them.

3. METHOD OF REPLICATION STUDY

The participants in this study were 16 graduate students in Computer Science, seven female and nine male. Their age ranged from 21 to 42 years with a median of 24 years. All participants had years of experience creating and remembering their personal passwords.

During an initial session the participants were asked to create passwords for five imagined web services: a bank, a book store, a university portal, an email account, and a travel site. Participants were provided with a form for writing down their passwords. This form also summarized the instructions given to participants before the form was handed out. Participants were instructed that the passwords had to be at least eight characters long and include both letters and digits, as is common practice in many systems, and that the five passwords had to be different but were allowed to be related. Further, participants were instructed not to use any of their real passwords but asked to use their normal strategies for creating passwords. Participants were also told that each password could have one, two, or three hint characters, which would be revealed to them when they were subsequently prompted for the password. Then, participants were asked to choose hint characters for each of their passwords and indicate them by underlining. Finally, participants were asked to write down any strategies they had applied in trying to create passwords that were memorizable.

On two subsequent occasions participants were prompted for their passwords. These password-prompting sessions took place one week and four weeks after the participants had created their passwords, and they proceeded in the same way. First, participants were asked to provide their passwords without the support of hints. For each password participants were also asked to indicate on a five-point scale from very uncertain to very certain how confident they were that they remembered the password correctly. Second, participants received their MiFA hints and were again asked to provide their passwords and indicate their confidence in the correctness of the provided passwords. The MiFA hints were provided to participants in a format that gave the hint characters and their approximate position in the passwords. Examples:

___ b _____ 8

__ a s _____

In the first example the hint characters are 'b' and '8'. The 'b' is preceded by one or more characters but is closer to the beginning than to the end of the password. The '8' is the final character of the password. In the second example the hint characters are 'a' and 's', and they appear next to each other near the beginning of the password.

Participants spent about 20 minutes creating their passwords and about 10 minutes on each of the two sessions where they were prompted for their passwords. Two participants failed to create passwords that were at least eight characters long and contained both letters and digits. These participants were excluded from the data analysis, leaving 14 participants.

4. FINDINGS

Table 1 shows the participants' ability to remember the five passwords one week after creating them and four weeks after creating them. After one week, participants remembered an average of 4.10 passwords with the aid of hints. This is 1.70 passwords more than participants remembered without hints, a significant improvement (T-test, p=0.022). After four weeks,

Participant	Remembered after 1 week		Remembered after 4 weeks	
	No hints	Hints	No hints	Hints
P1	5	5	5	5
P2	2	5	0	5
P3	5	5	0	5
P4	-	-	0	5
P5	0	4	4	4
P6	-	-	4	4
P7	-	-	2	3
P8	-	-	0	3
P9	1	4	2	2
P10	2	4	2	1
P11	0	0	0	0
P12	5	5	-	-
P13	0	5	-	-
P14	4	4	-	-
Average	2.40	4.10	1.73	3.36

Table 1. Number of passwords remembered by the participants ('-' indicates a missing value). Each participant was prompted for five passwords one week after creating them and four weeks after creating them.

Participant	Confidence after 1 week		Confidence after 4 weeks	
	No hints	Hints	No hints	Hints
P1	4.8	5	5	5
P2	1	3.6	1	3.4
P3	5	5	1	5
P4	-	-	1.6	4.4
P5	4	4.2	4.2	4.2
P6	-	-	3	4.2
P7	-	-	3	3.6
P8	-	-	1	2.8
P9	2	5	4	4
P10	4.8	4.8	5	5
P11	1.4	2.2	1	2.8
P12	5	5	-	-
P13	2	4.2	-	-
P14	-	-	-	-
Average	3.33	4.33	2.71	4.04

Table 2. Participants' confidence in their memory of their passwords ('-' indicates a missing value). Each number is the average of five password-confidence scores on a scale from 1 (very uncertain) to 5 (very certain).

participants remembered an average of 1.63 passwords more with hints than without hints, again a significant improvement (T-test, p=0.046). Between the first and the fourth week participants' ability to remember their passwords decayed by 0.67 for recall without hints and by 0.74 for recall with hints. This decay is, however, not significant (T-test, no hints: p=0.793, hints: p=0.182).

Table 2 shows the participants' confidence in the correctness of their memory of their passwords. After one week, participants' confidence averaged 4.33 when they recalled passwords with the aid of hints. This is 1.00 more than their confidence without hints, a significant difference (Wilcoxon test, p=0.028). After four weeks, participants were an average of 1.33 more confident in the correctness of passwords recalled with hints than without hints, again a significant difference (Wilcoxon test, p=0.018). Between the first and the fourth week participants' confidence dropped slightly but not significantly (Wilcoxon test, no hints: p=0.917, hints: p=0.855).

Password-creation strategies were provided by 12 of the 14 participants. The contents of these strategies included:

- Eight participants' passwords consisted of a sequence of letters followed by one or more digits. For six of the participants this property was an explicit part of their password-creation strategies. On average, 3.07 of the five passwords created by each participant had this property.
- Six participants created only passwords that were the minimum of eight characters long, and four participants explicitly mentioned this as one of their password-creation strategies. On average, 3.29 of the passwords created by each participant were eight characters long.
- Five participants 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 participant's passwords contained such a topical word.
- Four participants had password-creation strategies involving the concatenation of two meaningful words, typically their name (see below) and a topical word. On average, 1.21 of each participant's passwords contained two concatenated words. An additional 2.21 of each participant's passwords contained one meaningful word.
- Three participants incorporated their own name (i.e., first name, middle name, last name, or userid) in their passwords. On average, 1.50 of each participant's passwords contained the participant's name. In addition, one participant used the names of friends' children and pets in his passwords.
- Two participants created passwords that corresponded to memorizable patterns on the keyboard (e.g., the two leftmost columns of keys). One of these participants consistently included special characters (i.e., neither letters nor digits) in his passwords, but apart from the five passwords created by this participant only one password contained a special character.

For each password the participants selected the one, two, or three characters they wanted as their MiFA hint. The distribution across one-, two-, and three-character hints was 29%, 66%, and 6%, respectively. Participants used the hints to amplify their password-creation strategies. This was mainly done by having the hints signal the start of the chunks of which the passwords were constructed:

- The initial letter of every meaningful word contained in a password was often included in hints. On average, each participant created 3.42 passwords containing meaningful words and for 2.29 of these passwords the hints included the initial letter of each of these meaningful words. Five participants used this method for all their passwords.
- Often passwords ended in a number external to the main password-creation strategy, and the initial digit of this number was included in the hint. On average, each participant 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 participants used this method for all their passwords.

5. DISCUSSION

Four weeks after creating their passwords the participants remembered 67% of them correctly when aided by MiFA hints. This is significantly better than the 35% they remembered without hints and comparable to the 75% remembered after ten days in the study by Lu and Twidale [8]. Both their study and this study concern 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.

Participants were also significantly more confident in the correctness of passwords recalled with the aid of MiFA hints than without such hints. Thus, participants' perception of the MiFA hints is consistent with their improved performance. The participants' high level of confidence suggests that they consider MiFA hints useful and may adopt them if introduced in operational systems. The decay in the participants' memory from one week after creating their passwords to four weeks after creating them was not significant but calls for testing MiFA hints longitudinally, if possible as an element of their introduction in an operational setting.

Without hints it is unrealistic to require that users always choose strong passwords, change them frequently, and never write them down. This entails a conflict between security and ease of use [e.g., 4, 5, 6, 9, 10, 12]. Passwords may be attacked by outsiders that aspire to gain access to systems. Such attacks can be broken into four types:

- *Informed guessing*: cracking a person's password by combining knowledge about the person with knowledge about frequently used password-creation strategies.
- *Social engineering*: persuading a person to reveal passwords by exploiting that humans are, in general, unsuspecting and want to help out if they can.
- *Dictionary attacks*: cracking passwords by trying a large number of candidate passwords in a brute-force manner.
- *Interception*: capturing passwords when they are entered by or echoed to legitimate users, for example by wiretapping data lines.

This simple typology serves to illustrate that unless users understand the different types of attacks they are likely to behave in ways that counter some types of attacks but remain vulnerable toward others. Further, the vulnerability of passwords toward

dictionary attacks is increasing as still more powerful computers make it feasible to test passwords against still larger dictionaries [6, 11]. 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.

A frequent characteristic of the passwords created by the participants 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 participants' frequent use of names and topical words make the passwords more vulnerable to informed guessing. Further, their use of real words, whether topical or not, increase the vulnerability of their passwords to dictionary attacks. This vulnerability is, however, partly mitigated when passwords are created by concatenating two words. The near absence of special characters in the participants' passwords is a serious weakness because it reduces the password space dramatically. Finally, the participants' marked preference for passwords consisting of exactly eight characters is a regularity that can be exploited by password-cracking algorithms.

While the participants have, at least to some extent, succeeded in using the MiFA 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 a need for supplementary user-authentication mechanisms that focus primarily on strength. Such supplementary mechanisms may include graphic challenges [2, 10], which exploit that humans read distorted text much better than computers, and dynamic identity verification by means of keystroke characteristics [7] or pointing characteristics [3].

6. CONCLUSION

This study replicates and confirms work by Lu and Twidale on minimal-feedback hints for user authentication. With the aid of hints the 14 participants in this study remembered significantly more passwords and were significantly more confident in the correctness of their memory of their passwords than without hints. Hints were frequently used to amplify password-creation strategies by revealing the initial character of the chunks of which passwords were constructed. However, many of the passwords created by the participants were weak in spite of the improved support for remembering passwords.

7. ACKNOWLEDGEMENTS

This work was funded in part by the IT University of Copenhagen. Special thanks are due to the students who participated in the study.

8. REFERENCES

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

[2] Ahn, L. von, Blum, M., and Langford, J. Telling humans and computers apart automatically. *Communications of the ACM,* 47, 2 (2004), 57-60.

[3] Barrelle, K., Laverty, W., Henderson, R., Gough, J., Wagner, M., and Hiron, M. User verification through pointing characteristics: An exploration examination. *International Journal of Human-Computer Studies*, 45, 1 (1996), 47-57.

[4] Dourish, P., and Redmiles, D. An approach to usable security based on event monitoring and visualization. In *Proceedings of the 2002 Workshop on New Security Paradigms*. ACM Press, New York, 2002, 75-81.

[5] Hertzum, M., Juul, N.C., Jørgensen, N., and Nørgaard, M. (forthcoming). Usable security and e-banking: Ease of use vis-à-vis security. To appear in *Proceedings of OZCHI 2004*.

[6] Klein, D.V. "Foiling the cracker": A survey of, and improvements to, password security. In *Proceedings of the Second USENIX Security Workshop*. USENIX, Berkeley, CA, 1990, 5-14.

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

[8] 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.

[9] Morris, R., and Thompson, K. Password security: A case history. *Communications of the ACM*, 22, 11 (1979), 594-597.

[10] 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.

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

[12] Schultz, E.E., Proctor, R.W., Lien, M.-C., and Salvendy, G. Usability and security: An appraisal of usability issues in information security methods. *Computers & Security*, 20, 7 (2001), 620-634.