Human-Computer Interaction -- INTERACT'03
M. Rauterberg et al. (Eds.)
Published by IOS Press, (c) IFIP, 2003, pp. 821-824

Managing Multiple Passwords and Multiple Logins: MiFA Minimal-Feedback Hints for Remote Authentication

Bo Lu and Michael B. Twidale

Graduate School of Library and Information Science
University of Illinois at Urbana-Champaign
Champaign, IL 61820
{bolu, twidale}@uiuc.edu

Abstract: Web-based accounts, services and subscriptions often require a login and a password. Users can easily accumulate a bewildering array of logins and passwords to remember on security systems where usability design was often an afterthought. In this paper we describe our conceptual system for Minimal-Feedback Hints for Remote Authentication (MiFA), which we hope will help alleviate this problem. In addition, we hope MiFA will improve the tenuous security currently on the web by improving the way users work with authentication systems.

Keywords: Security, passwords, logins, remote authentication, authentication, word association, minimal feedback

1 Introduction

Web-based accounts, services and subscriptions often require a login and a password. Users can easily accumulate a bewildering array of logins and passwords to remember on security systems where usability design was often an afterthought (Adams & Sasse, 1999; Adams et al., 1997; Davis & Price, 1987; Hitchings, 1995; Sasse et al., 2001; Whitten & Tygar, 1998). The same dilemma faces users who must log into multiple networks during the workday. Users often find themselves staring at the login page to a site they haven't visited in a while, trying valiantly to remember which of their many logins and passwords they used when registering an account months ago. Users are then apt to try a multitude of solutions, from trial-and-error to sometimes the tedious task of re-registering. These situations lead users to resent websites that force registration in order to gain access to content, because it forces users to remember yet another password.

In an effort to combat login name and password overload, users have devised their own solutions – like writing down passwords or using the same login and password for all their accounts. Even when forced to change their passwords at intervals, users often adapt by making simple, easily guessable changes like changing MyPassword1 to MyPassword2. Strong passwords are hard to remember, and users don't want to change their passwords unless they really have to (DeAlvare & Schultz, 1988; DeAlvare, 1990). Behavior like this inevitably raises security concerns (Davis & Price, 1987; Gordon, 1995).

Previous work in novel authentication systems has tried to address this problem (Smith, 1987; Zviran & Haga, 1993). We present MiFA as a method that is evolutionary rather than revolutionary, and would be more practical to implement widely. MiFA is currently in its conceptual design stages, with development ongoing in C++ to create prototype MiFA software, some of which was used for the preliminary pilot studies.

Note that the authors are HCI researchers and do not claim in-depth knowledge of security issues. Thus we present MiFA mainly as a tool to improve the user experience of logging in, with its possible contributions to security as a secondary feature.

2 Design Issues

The challenge is to design a system and interface with two potentially contradictory goals:

(1) Make it easy for legitimate users to create, and then remember and use a login name and password.
(2) Make it difficult for anyone else to guess another's login name and password.

Designs that over-emphasize (2) at the expense of (1) may appear to be more secure, but in actual use are at risk from compensating user behavior that can subvert the intended level of security. For example, requiring long passwords enhances (2) but degrades (1). Users may react by methods such as refusing to create long passwords, or if coerced, writing them down or subverting their length (by repetition of characters).

With the accumulation of large numbers of online accounts, a common user solution is to use a single login and password. The consequence is to enhance (1) and degrade (2). If users are to be encouraged to generate different logins and passwords, we need to design to lower the cost of this desirable behavior, as a complement to endeavors to persuade people to be more security conscious (Weirich & Sasse 2001).

2.1 Minimal Feedback Authentication

Current remote user authentication systems found on most intranets and on the Internet have an all-or-nothing authentication strategy, either you are right or you are wrong. We offer minimal-feedback interaction as an alternative. We adopt the idea of minimal-feedback authentication 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.

At the time of registration or new login creation, a new user will select which letters of his or her password should be made semi-public – up to a set number of characters. MiFA will then take a snapshot image of the login and password with semi-public letters revealed and the other characters replaced with stars (Figure 1). The image will then be alerted to slightly "smudge" the readability. This was inspired by software-thwarting methods currently employed by Yahoo and MSN in which a user must enter a word he or she sees embedded in a picture. We hope that by adopting this feature, MiFA will provide additional security against password-cracking software. The MiFA hint image will then be stored on the local machine and on the host server. While this is not fully secure, it is not fully public information either (thus the phrase "semi-public"). Even this is much more secure than current browsers, which may prompt users to store their entire login and password combination on a local machine. Furthermore it is also more secure than users immediately adding the login and password in plain text to a crib sheet of logins that they may maintain. If users are logging in from a machine other than their own, they will of course have to remember their login – from which the system will retrieve their password MiFA hint. And, if a user is using a friend's machine to log in and sees that friend's MiFA hint, it won't constitute a security break since the user doesn't know the rest of the password.

Before accepting the user's choices for semi-public characters, MiFA will employ a back-end dictionary to verify that the password is not easily guessable, even given the semi-public characters. We hope that this prevents users from giving away characters in a password that would clearly indicate what the rest of the password would be (DeAlvare 1990). Both these measures will maintain a level of security, even when a small portion of the password is semi-public.

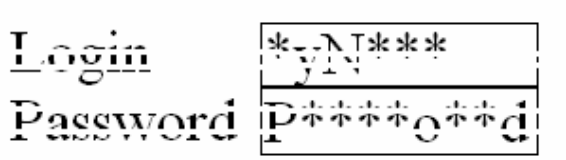

Figure 1: A MiFA snapshot image of the login "MyName" and password "Password".

The MiFA system also allows the user to mentally run through the possible login names and passwords before trying them. For most users, logging in to a rarely used system will require some level of trial-and-error. Instead of guessing and entering a password and waiting for all-or-nothing feedback via the network, users will be able to use the hint to narrow down the set of likely passwords, or to select which of their passwords must be the right one for this particular account. Many remote authentication systems today employ a maximum number of failed tries feature in an effort to thwart unauthorized entry. However, such an approach does not distinguish between selection errors, typos and hacking, and can easily lock out authorized users who simply did not type carefully enough, used an out of date password, or were trying out one of a handful of candidate passwords. With MiFA, at a glance users can discard many guesses. Our pilot studies indicate that usually users are able to narrow it to one guess, with first guesses right 75% of the time with MiFA hints.

2.2 Password-recovery systems

Current Login systems such as Yahoo! Mail™ and Microsoft .NET Passport™ have a feature for users who have forgotten their passwords. However, these

systems are insecure. These systems use easily accessible and oftentimes public information to authentic identity. For example, Yahoo! Mail™ asks for the user's birthday, zip code, and country of residence while Microsoft .NET Passport™ asks for state, country, and zip code. With an email address and a name in hand, anyone can easily use a telephone or web-based directory assistance service to gain this information. It is our hope that the MiFA system will reduce the need for password-recovery systems such as these, though we must keep in mind that some users will still forget their passwords, no matter what kind of system we provide.

2.3 Concerns

Of course, the system brings with it its own problems. For example, users will no longer be able to arrive at a website they use often and very quickly type in login and password on autopilot. That's why the Mifa system will be optional, but run on default if the user has not been to a website in a while.

3 Pilot Testing

The first step in evaluating the MiFA concept was to use small-scale pilot studies to glean insight into the premise of the MiFA solution. User tests were conducted with five volunteer users, three male and two female. One user was a faculty member, and the rest were undergraduate students – majoring in fields from music to linguistics. Each test subject was asked to provide four to five sets of unique login names and passwords. The login names and passwords were to be similar to, but for obvious security reasons different from logins and passwords these users would actually use. We did not put any size limitations on the login name, but we instructed each subject to provide passwords that were at least 8 characters long, as is common practice with many authentication systems today. Users were then allowed to choose two or three of the login and password sets that they had just created on which to apply the MiFA style hint. To create a MiFA-style hint, users were asked to choose two letters of their login name and three letters of their password to reveal, and to substitute stars in place of all other characters in their login and passwords. Around 10 days later, we returned to each user and asked them to login to the four websites they had previously registered for. For sites for which they had supplied a MiFA style hint, we supplied that hint to them at login.

The result was almost unilaterally in favor of the MiFA-style hinting of login names and passwords. The five test users combined for a total of 21 unique login-and-password pairs. Of the 21, 12 were MiFA-hinted and 9 were not. Of the 12 with MiFA hints, users 10 days later were able to correctly remember 8 on the first try. Of the 9 login-password sets without MiFA-hints, users were not able to remember any (Table 1).

	Logins and Passwords Created	Logins and Passwords remembered 10 days later
MiFA Hinted	12	8
No Hints	9	0

Table 1: Pilot test results.

Three of the five users told us as they logged in that they were confident in their answers. One notable quote from the study was a user who filled out her MiFA-hinted password letter-by-letter, then looked at the resulting password and said aloud "Why did I pick *that* as a password? But that's what it is." She was right.

The pilot testing also indicated that even when users could not remember their passwords, MiFA improved the accuracy of second guesses. One user realized that her password ended with the name of a character from her favorite TV show, but she couldn't remember which character. She ended up writing down both and telling us "It's got to be one of these two" – indicating that even though her first guess was wrong her second would have been correct.

After 10 days, users were unable to remember any of the logins or passwords that did not carry MiFA hints. Users flat-out told us that they usually write down new logins and passwords at time of creation, and without their "cheat sheets" they quickly gave up (Wickens, 1992). However, because users were asked to supply previously unused logins and passwords for security reasons, and we anticipate that this contributed to the lack of recall for passwords without MiFA hints. Users in real life, security issues aside, would have likely used one of their existing passwords.

Several other variables likely contributed to MiFA's success in the pilot studies. Users were asked to register for four different sites simultaneously, which is an uncommon occurrence. Also, the "registration" was done either on paper or via command prompt to a simple C++ program instead of the usual graphical login web pages. The

"websites" themselves were only identified by number and carried none of the distinguishing and memorable characteristics like purpose, content, or context that can usually help to jog users memories.

4 Future Work

We feel that the results of the pilot studies show that the MiFA concept holds significant promise. We anticipate moving development of prototype MiFA software away from C++ and into web format. As we introduce the elements of color, layout, and content as additional means to help users remember, we anticipate that the gap between user memory of MiFA-hinted and non-MiFA hinted passwords will narrow.

Further work is required to determine whether the MiFA hints are too helpful – whether they make the name and password guessable by someone other than their creator. The rules for generating hints that maximize recognition by the creator but minimize the potential for guessing by others will need to be examined and refined. In addition, we would like to investigate how the MiFA concept scales. If only one site gives a MiFA hint, then the novelty of MiFA itself might play a factor in the gap between user recall of MiFA-hinted and non-MiFA hinted passwords. We plan on conducting longer-term user studies of MiFA whereby a group of users will interact with MiFA authentication on a regular basis and will have multiple logins and passwords that have MiFA hints.

Finally, the most significant test of MiFA is whether an implemented version changes those user behaviors that tend to degrade security, i.e. reducing the incidence of use of identical logins and passwords, encouraging the adoption of longer, harder to guess passwords, and discouraging the storing of those details in plain text records.

Acknowledgments

The authors would like to thank the test users who helped us assess the viability of the MiFA model. This work is supported by the National Science Foundation under Grant No. 0081112.

References

Adams, A. & Sasse, M.A. (1999), Users are Not the Enemy: Why users compromise computer security mechanisms and how to take remedial measures, *Communications of the ACM* 42(12), 40-46.

Adams A, Sasse, M.A. & Lunt, P. (1997), Making passwords secure and usable, *in* H. Thimbleby B. O'Conaill & P. Thomas (eds), *People and Computers XII: Proceedings of HCI'97*, Springer, pp.1-19 .

Davis, D. & Price, W. (1987), *Security for Computer Networks,* Wiley.

DeAlvare, A.M. (1990), How crackers crack passwords or what passwords to avoid, *in Proceedings of the 2nd Unix Security Workshop II*, pp.103-112

DeAlvare, A.M. & Schultz Jr., E.E (1988), A framework for password selection, *Technical Report UCRL-99382,* Lawrence Livermore National Laboratory.

Gordon, S. (1995), Social Engineering: Techniques and Prevention, Computer Security, in *Proceedings of the 12th World Conference on Computer Security, Audit & Control*, pp.445-451.

Hitchings, J. (1995), Deficiencies of the traditional approach to information security and the requirements for a new methodology. *Computers and Security* 14(5), 377–383.

Sasse, M.A., Brostoff, S., & Weirich, D. (2001), Transformng the 'weakest link': A human/computer interaction approach to usable and effective security. *BT Technology Journal* 19(3), 122-131.

Smith, S.L. (1987), Authenticating Users by Word Association. *in Proceedings of the Human Factors Society 31st Annual Meeting*, The Society Press, pp.135-138.

D.Weirich & M. A. Sasse (2001), Pretty Good Persuasion: A first step towards effective password security for the Real World. Proceedings of the New Security Paradigms Workshop 2001, pp. 137-143. ACM Press.

Whitten, A. & Tygar, J.D. (1998), Usability of Security: A Case Study. *Technical report No. CMU-CS-98-155*, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA.

Wickens, C.D. (1992), *Engineering Psychology and Human Performance, 2nd Ed.* Harper Collins.

Zviran, M & Haga, W.J. (1993), A comparison of password techniques for multilevel authentication mechanisms. *The Computer Journal* 36(3), 227-237.