The Agony of Passwords: Can We Learn from User Coping Strategies?

Elizabeth Stobert
School of Computer Science
Carleton University
Ottawa, Canada
estobert@scs.carleton.ca

CHI 2014, April 26–May 1, 2014, Toronto, Ontario, Canada.
ACM 978-1-4503-2474-8/14/04.

http://dx.doi.org/10.1145/2559206.2579421

Abstract
Users are burdened by having to keep track of many accounts and passwords. We conducted a series of interviews to investigate how users cope with these challenges, and found that most users have developed personal strategies involving password reuse and writing passwords down. These strategies have their limitations, but they are rational and could serve as the basis for a new user-centred approach to security.

Author Keywords
Authentication; usable security

ACM Classification Keywords
K.6.5 [Computing Milieux: Security and Protection]: Authentication.

Introduction
Everyone hates passwords. When we talk to users about passwords, people are quick to share their opinions. Passwords are bothersome, unavoidable, and present a complicated task. Users have trouble choosing secure passwords, and they know that easily memorized passwords are often also easily guessed by attackers [1]. In addition, users are burdened with many accounts, each of which is expected to have a strong, unique password. Finally, the user must keep track of which password

corresponds with which account. Although everyone hates passwords, most users are somehow coping with the problem. We are interested in how they are coping, and the kinds of tools and strategies they are using to handle passwords. We speculate that users' coping strategies might show how to relieve the agony of passwords.

Alternative solutions to the password problem exist in the form of biometrics, security tokens, and single sign-on, but these present issues with privacy, theft, and the huge infrastructural costs of deployment and maintenance [8]. Deployed solutions to the password problem consist mainly of password managers, which store and enter users' passwords, thus saving the user from remembering their passwords or which passwords are associated with which accounts. Browser-based password managers save passwords when they are typed into the appropriate fields, and then automatically input them when the page is visited again (often without authentication). Dedicated password managers typically work in one of two ways: they either generate a password at login by hashing the user's master password together with information from the website, or they store the user's passwords in a password "wallet" which is protected by a master password [3].

An alternative technique for managing passwords is to reuse passwords across multiple accounts. This strategy is widely employed by users [6, 5, 7], but has security risks. If a reused password is discovered (e.g., through a leaked password set), an attacker may be able to gain access to several accounts. Das et al. [4] found that 43% of all passwords in their data set were reused across multiple accounts, and showed that password reuse can be leveraged for more efficient password attacks.

A number of studies have investigated the number of passwords and accounts that users possess. Gaw & Felten [6] found that undergraduates had an average of about 12 accounts, but they had fewer unique passwords and password reuse was commonplace. The study also found that most participants cited easier memorability as their reason for password reuse, and that participants classified their accounts by the desired level of privacy and security. Florencio & Herley [5] conducted a large scale study of password use through the six-month deployment of a Microsoft toolbar. They collected data from more than 250,000 users, and found that the average user had 6.5 passwords, each of which was shared across 3.9 websites. They found that the average user accessed 25 accounts over the six month period, and logged into eight accounts per day. A 2011 diary study of password use by Hayashi & Hong [7] collected detailed records of password entries over a two-week period. They found that users accessed a mean of 8.6 accounts over two weeks, and estimated that most participants had about 11 accounts in total. Although they did not study password reuse directly, all of their participants reported reusing passwords.

The purpose of our study was to conduct a qualitative investigation into the coping strategies that users develop to handle the ever-increasing demands of passwords. We are interested in whether users' coping strategies can form a user-centred basis for a new approach to password management.

Study

To investigate how users manage and keep track of their passwords, we conducted a series of interviews about password habits. The interviews were facilitated by the researcher, who asked the questions, recorded answers, and encouraged participants to discuss or give fuller answers. The password interview was audio-recorded to facilitate further note-taking and analysis. We also

conducted a brief self-administered demographics questionnaire that collected basic information including age, gender and occupation, and was mostly intended to give a better understanding of the interview sample.

The password interview included a series of questions about the number of passwords and accounts, password reuse, password managers, and how participants kept track of their passwords. We also asked about how they would behave when creating new accounts, and when changing or resetting the password on an existing account. We did not ask participants what their passwords were, and we specifically told participants that they should never reveal their passwords to us.

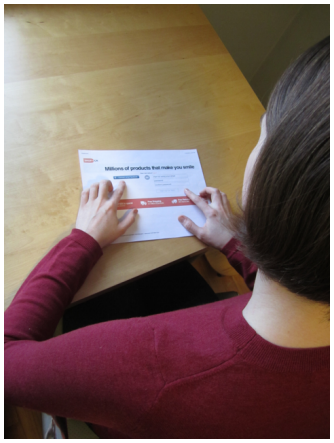

Figure 1: Participants used website screenshots to situate themselves in the password creation task.

We chose our methodology to encourage participants to discuss thoughtfully the ways in which they approach the task of password management. We used a guided interview to give participants an opportunity to explain how and why they make their decisions, and to avoid having participants rush through the questions. We provided users with props in the form of cards with website screenshots (figure 1) to situate themselves in the password creation and reset tasks, and to encourage them to consider their real life behaviour.

Fourteen people took part in the study, and all were recruited using posters, mailing lists, and word-of-mouth from the university community. The majority of participants (85%) were female, and ranged between 17 and 65 years of age (median 25 years). Most participants (79%) were students, from a range of programs including the humanities, sciences, and social sciences. Several participants worked in the university community, mainly in administrative roles.

Results

The first part of the interview investigated how many accounts and passwords users have. We divided questions into multiple parts to encourage participants to closely reflect on their answers. For example, in a question about number of accounts, we identified 14 account categories where participants might have accounts, and asked about each category individually. In this, as in all our study, we reflected carefully on the words participants used and how they chose to describe their experience and this was the basis for our thematic analysis. Space limitations prevent us from including illustrative quotes.

Participants reported having between 9 and 51 accounts in total, with a median of 27 accounts. Most participants' accounts were for email, school- or work-related activity, and social networking. Participants reported using a median of 11 accounts in an average week, with a range of 3 to 14 accounts.

Participants reported having between 2 and 15 unique passwords, with a median of 5 passwords. All of the participants in the study reported reusing passwords between accounts. Most participants (79%) reported reusing more than one password, and all participants reported reusing passwords either "always" or "frequently". Participants described different strategies for reusing passwords. Some described using the same password for all accounts, and others described linking passwords with usernames. Participants also reported using different passwords for different online contexts, such as at work or school. Several participants mentioned that they were more careful not to reuse passwords on "financial" or "important" accounts. Conversely, many participants also mentioned having a specific password

that they reused widely on accounts of low interest, low importance, or infrequent use.

We were interested in whether participants considered context of use in their password management strategies. Participants reported entering their passwords on a range of devices including desktop computers, laptop computers, tablets, e-readers, and smartphones, but the most commonly reported context was a computer (laptop or desktop) as well as a smartphone. Most participants (79%) said that they did not consider device constraints when choosing passwords. Participants who said they did consider device constraints mentioned that they considered the availability of apps (i.e., whether they would have to type the password frequently) and the different security requirements of different devices. All participants reported that they enter their passwords on computers that do not belong to them. Several participants mentioned that they were more careful about logging out on these computers, and about not saving passwords in the browser. One participant mentioned that they sometimes changed their passwords after entering them on computers belonging to other people.

The next set of questions addressed the coping strategies that users develop to keep track of passwords and accounts. We asked participants if they used any kind of password manager (including the browser-based managers), and 64% of respondents said that they saved their passwords in some kind of password manager. All of these 64% went on to clarify that they saved passwords in their browser or in the Apple keychain. No one reported using dedicated password management software.

Eleven participants reported writing down at least some of their passwords. Of these participants, all referred to the recorded passwords as a backup for memory, and not a resource used at every login. Participants reported different recording strategies – some recorded only part of the password, or a hint to the password, while others were more methodical about recording all of every password. Participants reported using both physical and digital media to store passwords, but specified that the recorded passwords were easily accessible from their regular computing context.

The final part of the interview included questions about password changes and resets of forgotten passwords. Only a minority of participants (14%) reported ever changing passwords of their own volition (we specifically excluded situations where a website enforces a password change), and these participants remarked that they changed passwords rarely, and only under special circumstances. Participants evidently did not consider situations where they changed forgotten passwords, because all participants reported having done this. Most participants reported resetting forgotten passwords once per month or less, and most people said that their strategy in that situation was to change the password to what they thought it might have been (often reusing a password).

Discussion & Interpretation

Our study confirmed that users have many accounts and passwords, and are clearly burdened by the management task. However, all of our users described functional coping strategies that allowed them to have effective online experiences.

Security Tools: Although a wealth of password management tools are available, few of our users reported using them. Participants in our study were unfamiliar with tools and techniques that could help them manage their passwords and accounts. None of our participants used a

dedicated password manager, and no one mentioned using services such as single sign-on that allow users to log into multiple sites with one account (Google and Facebook both provide single sign-on services). The high cost of adoption and a poor understanding of how these services work can prevent users from setting them up. Even for low cost solutions, such as the browser-based password managers, security advice can be conflicting – several participants mentioned that they had been discouraged from using tools like browser-based password managers and were avoiding or had stopped using such tools because they had heard they were insecure. These stories point to a failure in the security community. When we tell users that they should *not* do something, we must give them feasible advice about what they *should* do instead.

Password Reuse: For the users in our study, their primary compensatory strategy for passwords was reusing passwords. Participants reported widely reusing a small number of passwords. There are security risks to reusing passwords, but it can be a sensible and intuitive way of relieving the burden of passwords. Participants described a variety of reuse techniques, including algorithmic strategies that recombined different password elements for different accounts, linking passwords with usernames, and linking passwords with specific contexts. A number of participants remarked on having separate passwords for financial accounts, such as their online banking. This provides a good example of a way in which users are coping and sensibly reusing passwords.

In the interviews, a number of participants referenced having to try all of their passwords at every login (in effect, mounting a guessing attack on themselves). If an attacker records all attempted passwords on a single website, they can quickly learn all of a user's passwords, which can endanger all of a user's accounts. If reusing passwords is to be a viable strategy, users need to be cued about which account goes with which password.

Frequency of Use vs. Need for Security: Participants often made the mistake of conflating frequency of use with the need for security. Many participants mentioned a set of accounts that they did not care about and used infrequently (and conversely, associated frequent use with a need for high security). While these factors can be correlated, they are often unrelated, and it is dangerous to assume that an account is secure with a weak password if you do not use it often. A better guideline for users might be to consider the consequences of security breaches, and to reuse passwords where similar information is shared; it does not make sense to protect the same information with a strong password in one place and a weak password in another.

Writing Passwords Down: The majority of our participants reported writing down at least some of their passwords. Most participants reported it as a backup strategy, and that they referred to the recorded passwords only in unusual circumstances. Participants reported writing down assigned passwords, passwords that could not be reset, passwords for important accounts, and infrequently used passwords. One participant told us that she had begun writing her passwords down when she found that she was having to reset forgotten passwords too often.

Writing passwords down is conventionally understood to be insecure, but many security experts actually advocate writing passwords down [2] if they can be kept in a physically secure location. Writing passwords down is a sensible step, but the caveat about storage is poorly understood by users. In our study, participants reported

keeping their password lists in their email, in dropbox, saved on their cell phones, or saved on their computer desktops. While writing passwords down is an intuitive and reasonable way of handling security, users need helpful guidance on the right way to store these passwords.

Threat models: One of the emergent themes during the questionnaire discussions was confusion about the nature of the threat. Although worried about security, participants seemed unclear about the type of threats that concerned them. They did not differentiate between targeted personal attacks, anonymous large-scale password hacks, and the loss of private data, although they referenced all three during the discussions. Without a clear model for the type of threat they were facing, participants did not seem to appreciate that the defences for different attacks might vary based on the nature of the account in question.

Conclusion

Our study found that users' password management techniques are perhaps more extensive than we might guess. Participants have large numbers of accounts, and are desperately trying to find a way to protect and keep track of all of them. Although tools such as password managers and single sign-on can help users, few users are taking advantage of them. However, users are developing strategies that are helping them cope with the challenges of passwords. These strategies include reusing passwords and writing passwords down. Despite their limitations, these user-centred strategies are rational. Our contribution to HCI is that secure password authentication might be based on accommodating or improving these strategies rather than ignoring or advising against them. An approach that provided site-specific cues or facilitated reuse could help users leverage their current practices to make them more secure.

While research into strong, novel solutions is important, we have neglected the opportunities for significant harm reduction. There exist problems that cannot be easily solved: the growth in accounts, the inherent risks of passwords, and there may come a day where a new authentication system (such as biometrics, or universal single sign-on) provides the solutions to these problems. But in the meantime, we must adopt a philosophy of *user-centred security*, where we learn what people are doing to cope with security, and support those actions in our solutions.

References

[1] Adams, A., and Sasse, M. A. Users Are Not The Enemy. *Communications of the ACM 42*, 12 (1999).

[2] Cheswick, W. Rethinking Passwords. *Queue 10*, 12 (2012).

[3] Chiasson, S., Van Oorschot, P., and Biddle, R. A usability study and critique of two password managers. In *USENIX Security Symposium* (2006).

[4] Das, A., Bonneau, J., Caesar, M., Borisov, N., and Wang, X. F. The Tangled Web of Password Reuse. In *NDSS 2014* (2014).

[5] Florencio, D., and Herley, C. A Large-Scale Study of Web Password Habits. In *WWW '07* (2007).

[6] Gaw, S., and Felten, E. W. Password management strategies for online accounts. In *SOUPS '06*, ACM (2006).

[7] Hayashi, E., and Hong, J. A diary study of password usage in daily life. In *CHI '11*, ACM (2011).

[8] Herley, C., and van Oorschot, P. A Research Agenda Acknowledging the Persistence of Passwords. *Security & Privacy, IEEE 10*, 1 (2012), 28–36.