Passwords and Perceptions

Gilbert Notoatmodjo and Clark Thomborson
Department of Computer Science
The University of Auckland
Auckland, New Zealand
gilbert@595lab.com
clark@cs.auckland.ac.nz

Abstract

The security of many computer systems hinges on the secrecy of a single word – if an adversary obtains knowledge of a password, they will gain access to the resources controlled by this password. Human users are the 'weakest link' in password control, due to our propensity to reuse passwords and to create weak ones. Policies which forbid such unsafe password practices are often violated, even if these policies are well-advertised.

We have studied how users perceive their accounts and their passwords. Our participants mentally classified their accounts and passwords into a few groups, based on a small number of perceived similarities. Our participants used stronger passwords, and reused passwords less, in account groups which they considered more important. Our participants thus demonstrated awareness of the basic tenets of password safety, but they did not behave safely in all respects. Almost half of our participants reused at least one of the passwords in their high-importance accounts. Our findings add to the body of evidence that a typical computer user suffers from 'password overload'. Our concepts of password and account grouping point the way toward more intuitive user interfaces for password- and account-management systems.

Keywords: Identity Management and Identity Theft, Password Practices, Security, Authentication.

1 Introduction

On any computer system that controls resources for more than one user, the ability to authenticate different users is imperative. A password has long been the most common way users prove their identity to a computer. The attractiveness of password based authentication lies not in its security, but in its simplicity, practicality, ease of use, and low cost. Although biometrics and multifactor authentication can provide a greater degree of confidence, they require more costly infrastructure or user training, which deter most service providers from requiring their use except when required by legislation (Rejman-Greene 2001; O'Gorman 2003).

In password based authentication, the identity of an individual is verified solely by his/her ability to present a previously agreed word. This results in a significant vulnerability. Security is compromised if an adversary learns a single word. The adversary who knows a user's password will be able to impersonate this user, and to access the resources to which this user is entitled.

An adversary may mount several types of attacks on password authentication systems. We identify three main categories, based on the target of the attacks.

1. **Attacks on the system end**
   This type of attack is targeted at the passwords stored in the system. An example of this type of attack is *password guessing attack* (Ding and Horster 1995; Halevi and Krawczyk 1998; Pinkas and Sander 2002).
2. **Attacks on the communication channel**
   These attacks target any communication channel through which passwords are transmitted. Our definition of communication channel includes all devices, media and protocols which connect the user to the system which stores the password (or its hash). Examples are *replay*, *eavesdropping*, and *man-in-the-middle* attacks.
3. **Attacks on the user end**
   These are directly targeted at the user. Examples are *social engineering*, *shoulder surfing*, *dumpster diving*, and *phishing*.

Of the three categories, attacks on the user end are perhaps the most alarming, for these attacks require only a minimal level of technical or specialist knowledge, and yet they may have a high chance of success. Furthermore, although cryptographic devices and protocols can protect the system and the communication channel, users are often protected only by security policies and guidelines. These security measures may be unknown, neglected, or avoided by many users.

Most users have a low awareness of their vulnerability and of the scope of damage that can be inflicted if their passwords are compromised (Adams and Sasse 1999; Weirich and Sasse 2001; Gaw and Felten 2006). The infamous hacker Kevin Mitnick, in his testimonial before the US Congress, stated that he obtained passwords more often by exploiting users than by using technical means.

> I was so successful in [the social engineering] line of attack that I rarely had to resort to a technical attack... Companies can spend millions of dollars on firewalls, encryption, and secure access devices, and its money wasted, because none of these measures address the

weakest link in the security chain (Poulsen 2000).

Previous studies have shown that users often write their passwords down, and post them in obvious locations (Barton and Barton 1984; Adams and Sasse 1999; Dhamija and Perrig 2000; Horowitz 2001). Users often create weak passwords based on obvious dictionary words or personal information, which can be guessed by people who know enough about them. These weak passwords include birth dates, personal names, nicknames, names of partners or favourite celebrities, and even the word 'password' (Riddle, Miron et al. 1989; CentralNic 2001; Sasse, Brostoff et al. 2001; Brown, Bracken et al. 2004). Password sharing between friends and work colleagues has also been noted as a common practice. Many users do this because of convenience and practical reasons (Adams and Sasse 1999), or as a result of social pressure.

Another risky password practice is reuse. The risk of password reuse is that if a password is compromised, all other accounts which share the same password are also compromised. Unlike the other risks discussed above, password reuse is almost inevitable for most users, due to the proliferation of e-commerce and other services requiring password authentication. While human memory capacity seems unlikely to increase, the rising number of online services seems to force users to reuse their passwords. A recent study (Gaw and Felten 2006) showed that password reuse tends to increase as people accumulate more accounts. Ives, Walsh et al. (2004) described the 'domino effect' of multiple systems being susceptible to attacks because of password reuse.

Many service providers attempt to minimize the risk of password reuse by forcing users to change their passwords on a regular basis, and by prohibiting them from reusing their passwords on other accounts. These policies seem to cause difficulties for many users. Adams and Sasse (1999) discovered that having a large number of passwords reduces their memorability. Users who comply with a directive against password use may attempt to minimise the resulting cognitive burden by choosing easier-to-remember but weaker passwords, by writing them down, or by engaging in other insecure password practices. It is clear that password reuse is a non-trivial problem which will only worsen over time unless we provide users with appropriate password- and account-management assistance.

In order to be able to objectively evaluate existing password systems, or to develop systems which remain within their users' cognitive abilities, we must investigate the factors which influence users' password usage behaviour, and we must understand who users would like to organize their accounts and passwords. In this paper, we describe an exploratory survey which investigated how users' perceptions of their accounts and passwords influence the way in which they classify and associate their accounts and passwords.

This paper is structured as follows. Section 2 describes several related studies which have been previously discussed in literatures. Section 3 describes the motivation of our survey based study and details the procedures of our survey. Sections 4 and 5 present our findings and our conclusions, respectively.

2 Related Studies

Morris and Thompson (1979) studied a corpus of 3,289 passwords from many users over a long period of time and discovered that 86% of these passwords were extremely weak. Riddle, Miron et al. (1989) analyzed 6226 user generated passwords from IBM CMS environment used by students and staff at Syracuse University in 1987, finding that many passwords were extremely short and consisted of English words or persons' names.

Adams and Sasse (1999) conducted a study of password related user behaviors, including password construction, frequency of use, password recall and work practices. They concluded that their participants lacked security motivation and understanding of password policies, and tended to circumvent password restrictions for the sake of convenience. Dhamija and Perrig (2000) conducted an interview-based study involving 30 participants. Similar to Adams and Sasse, they concluded that participants tended to find 'workarounds' to circumvent system restrictions, which often resulted in insecure password practices. Moreover, they discovered that the level of security training did not appear to have any impact on participants' password practices – even trained participants often viewed secure password practices as being too cumbersome and impractical.

Brown, Bracken et al. (2004) conducted a survey involving 218 college students at Southern Methodist University to evaluate their password generation and usage behavior. On average, their participants maintained 8.18 accounts which require a password (S.D. = 2.81, Range = 3 to 20), while only having 4.45 passwords (S.D. = 1.63, Range = 1 to 11). The majority of participants (92.9%) reused their passwords on at least one account. Most of their participants drew heavily upon themselves and others close to them as inspirations for creating passwords.

Riley (2006) conducted a survey of password generation practices and usage behaviour involving 315 undergraduate and graduate students. Participants were instructed to complete a self-report questionnaire. Although the majority of the participants were able to identify most of the recommended password practices, most of them, even the ones who successfully identified recommended practices admitted to be doing things differently from what they believed they should do.

Gaw and Felten (2006) conducted a survey to investigate how users manage passwords for their online accounts, involving 49 participants from Princeton University. They discovered that number of accounts increased by years in school, and concluded that people accumulate more online accounts as they get older. The number of unique passwords, however, was found not to increase with the years of study. Gaw and Felten defined password reuse as the ratio between the number of accounts and the number of unique passwords. The majority of users had three or fewer passwords and passwords were reused twice. The number of accounts increased by year in school, but the total number of passwords did not increase; leading Gaw and Felten to conclude that password reuse will become a bigger problem over time. "Ease to remember" was the most popular reason for reusing passwords. "Security" and

"Protecting private information" were the most frequent reasons cited for *not* reusing passwords. Users tended to vary the complexity of their passwords depending on the account's importance. They reused passwords less on accounts which contained private and valuable information. Many participants agreed with the statement "I reuse a password when there isn't much financial information (bank account, credit card number, etc.) about me on a website." Gaw and Felten also asked some open-ended questions, eliciting such responses as "for less important accounts, I use an easy password for simplicity."

Florencio and Herley (2007) from Microsoft Research conducted a large scale study of password usage and reuse practices which involved half a million participants. Data was collected by means of client software, which was shipped as a component of Windows Live Toolbar. Florencio and Herley discovered that participants seem to assign passwords of different strength based on the value of information related to the accounts – there is a considerable difference in bitstrength between passwords used to protect newspaper accounts (New York Times) and passwords used to protect financial related accounts (PayPal and Fidelity). Moreover, Florencio and Herley also discovered that weaker passwords tend to be shared at more sites, while stronger ones at fewer.

The corpus of existing password research can be broadly summarized as follows. The earliest studies were analyses of large collections of passwords. Through these studies, it was discovered that users tend to choose weak passwords. Later studies were based on surveys of users, resulting in better understanding of users' password practices. Left to their own devices, most users tend to employ insecure password practices, and they tend to circumvent security measures in favour of convenience and practicality. Although insecure passwords were found to be common, Dhamija and Perrig (2000) and Riley (2006) discovered that such insecure practices were not caused by the users' lack of security knowledge. Gaw and Felten (2006) and Florencio and Herley (2007) found that accounts which are considered to be of high importance tend to have passwords which are stronger, and which are not reused as much, as those on low-importance accounts.

3 Our Study

In contrast to previous studies, we focused our investigation on how users' perceptions of their passwords and accounts affect the way in which they manage their accounts and passwords. We hypothesized that users manage their passwords and accounts by mentally classifying their accounts and passwords using various perceived similarities, such as importance, length of passwords, and so on. This hypothesis was used as an organising idea for our exploratory study.

3.1 Survey Procedures

We advertised our survey by means of posters which were posted on notice boards within various departments in two main campuses of our university, as we intended to obtain sample data which is representative of our university's student population with diverse majors and degrees. The survey was conducted on one-to-one basis in a tutorial room within the Computer Science Department at The University of Auckland.

We used a coding scheme in order to allow participants to describe their passwords, accounts and associations between them without revealing their actual passwords and accounts. This was done to minimize the ethical hazard of our study. A potential drawback of this approach is that participants might find it very difficult to describe their passwords and accounts without writing them down. We decided to allow participants to write down their passwords and accounts during the procedure, on separate worksheets, during the survey procedure. At the end of each interview, the worksheets containing the sensitive information (user IDs and passwords) were destroyed using a commercial grade strip-cut paper shredder.

Our survey consisted of two main parts. In the first part, the participants were asked a few general questions about their background information (degree pursued, major of study, number of years spent at the university), and experience with computers and the internet. The second part consisted of a guided exercise, which was performed using the worksheets that we provided. This guided exercise had six steps.

1. Participants were asked to write all their passwords in a piece of paper.
2. We explained our hypothesis regarding how people organize their passwords by mentally grouping them.
3. Participants were asked to complete a table, by assigning numbers and codes to their passwords according to the way they group their passwords based on their perceived similarities. We also instructed the participants to describe the similarities that they use as a basis for grouping their passwords together. The worksheet containing this table was used only during the next step.
4. Participants were instructed to describe each of their passwords by completing the following columns:
   - **Length**
     The total number of characters in each password).
   - **Perceived security level**
     Measured on a five point Likert scale, from one (least secure) to five (most secure).
   - **Difficulty of recall**
     Measured on a 5 point Likert scale, from one (least difficult) to five (most difficult).

   Participants were asked to replicate their numbering scheme and their reasons for grouping which they had completed in the previous step, using the previous worksheet as a reference. However, this time, they were instructed not to write down their passwords.
5. As in Step 3, participants were told to list their accounts in a table and assign numbers and codes to them, following the manner in which they organise their accounts using mental groups according to their similarities as perceived by themselves. The sheet used in step 5 was used only during the next step.
6. Finally, participants were asked to collate all the previous information together by completing the following columns for each of their accounts:

- **Value of information**
  Measured on a 5 point Likert scale from 1 (least valuable) to 5 (most valuable).
- **Frequency of use**
  Measured on a 5 point Likert scale from 1 (least frequent) to 5 (most frequent).
- **Password (Number and code only)**
  Password assigned to the account. We instructed participants to not to write their actual passwords, but only the number and code they had assigned to their passwords in Step 3.
- **Password reuse (Y/N)**
  Participants were asked to choose 'Y' if the password which is used on this particular account is also used on at least one other account or 'N' if the password used on this particular account is unique.
- **Reason why password is reused/not reused**
  A brief explanation of why they decided to reuse or not to reuse passwords on a particular account.

After all the steps were completed, participants were instructed to separate and destroy the sheets containing their actual passwords and accounts from Steps 1, 3, and 5, using the paper shredder. We retained their sheets from Steps 4 and 6.

4 Results

We recruited 26 participants. All were students at the University of Auckland at the time of the survey; 14 were male and 12 were female. Our participants came from a range of faculties and departments across our university and were pursuing different degrees and majors.

4.1 Password Properties

We are interested to investigate whether there are any relationship between length, perceived security level and difficulty of recall of passwords as reported by our participants. Our test indicated that there was no evidence that there is a significant correlation between length and perceived security level of passwords (Kendall's Tau = 0.106, P-value = 0.471; Spearman's Rho = 0.165, P-value = 0.442). There was also no evidence of a significant correlation between length of password and difficulty of recall. (Kendall's Tau = -0.062, P-value = 0.673; Spearman's Rho = -0.089, P-value = 0.680).

There is, however, some evidence that there is a significant correlation between perceived security level and difficulty of recall of passwords (Kendall's Tau = 0.278, P-value = 0.059; Spearman's Rho = 0.359, P-value = 0.085). Visual observation of the scatter plot (refer to Figure 1. above) has also shown that there is an indication of a positive trend between these two variables, although there one possible outlier (participant 24). Further investigation suggests that most of this participant's passwords (6 out of 9 passwords declared), were 13 to 14 characters long, which are reasonably lengthy compared average length of passwords declared by our participants, which is only 8.6 characters. Excluding participant 24 from our analysis resulted in highly significant evidence of a correlation between perceived security level and difficulty of recall (Kendall's Tau = 0.372, P-value = 0.014; Spearman's Rho = 0.503, P-value = 0.014).

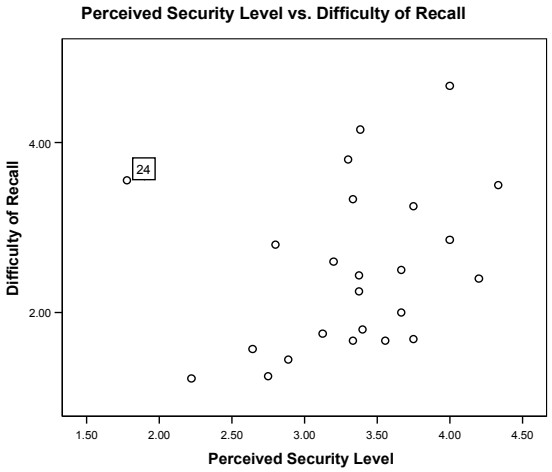

Figure 1: A scatter plot showing a positive relationship between perceived security level and difficulty of recall of passwords.

4.2 Growth of Accounts and Passwords

Due to the increase of the number of online services requiring password based authentication from time to time, we would expect the number of accounts and passwords of computer users to correlate with the amount of computing and internet experience, i.e. longer exposure to computers or the internet would translate into more accounts.

Using regression, we obtained very strong evidence that years of internet experience is positively correlated to the number of online accounts ($F = 7.696$, Adj. $R^2 = 0.211$, P-value = 0.011). This suggests that the number of online accounts maintained by our participants increases as they gain more internet experience, confirming earlier findings by Gaw and Felten (2006). Our regression model explains 24% of the variation in the number of online accounts, and therefore is not suitable for prediction. Holding everything else constant, the number of online accounts maintained by our participants changes by 1.2 accounts per year of internet experience. We also confirmed another prior finding by Gaw and Felten (2006), that there is no correlation between the number of passwords and the number of years of internet experience ($F=-0.027$, Adj. $R^2 = 0.337$, P-value=0.567).

4.3 Password Reuse Statistics

It is certain that if the number of passwords does not keep up with the increase in the number of accounts, people will have to reuse their passwords. We investigated whether our participants reused more passwords as they accumulated more accounts.

We measured number of password reuse occurrences, i.e. the number of accounts on which our participants reused their passwords, from each participant's data, and plotted our result against the total number of accounts. It is evident in the scatter plot below that our participants reused more as they accumulate more accounts.

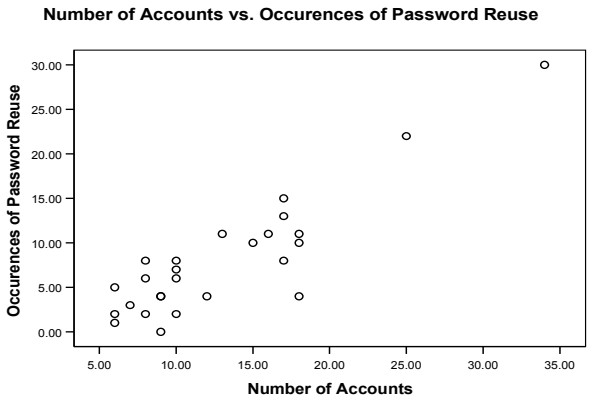

Figure 2: A scatter plot showing the relationship between number of accounts and number of password reuse occurrences.

We then constructed a linear regression model, using number of accounts as a predictor for number of password reuse occurrences. We obtained very strong evidence that the increase in number of password reuse occurrences is related to the increase in the number of accounts ($F = 87.465$, $R^2 = 0.799$, Adj. $R^2 = 0.790$, P-Value < 0.001).

We had asked our participants to choose the statement, from a list we provided, which best represents the reason for their password usage practices (whether or not they reuse this password) for each of their accounts. The frequency of how many times each statement selected by our participants is presented in Tables 1 and 2.

Reasons cited for not reusing passwords	Frequency	Percentage
The information stored under this account is of high value/importance.	**38**	**28.4%**
I try to avoid password reuse because I believe it is not secure.	21	15.7%
The password was assigned by the account provider.	18	13.4%
The account provider has password format restrictions, so I had to change my password to meet their restrictions.	18	13.4%
I created a unique password to avoid confusion with my other account(s).	18	13.4%
Other	11	8.2%
I created a random password for this account.	10	7.5%

Table 1: Reasons cited for not reusing passwords (sorted by frequency).

Reasons cited for reusing passwords	Frequency	Percentage
I reuse password for this account because it is easy to remember.	**72**	**35.1%**
The information that is stored under this account is of similar value/importance to the information stored under the other account(s) which use the same password.	39	19%
This account belongs to the same category as the other account(s) which use the same password.	38	18.5%
This account belongs to the same domain (leisure/work/family) as other account(s) which use the same password.	27	13.2%
I use this account in the same frequency as the other account(s) which use the same password.	16	7.8%
I have several passwords and I randomly assigned them to my accounts.	7	3.4%
I only have one password and I use it for all my accounts.	3	1.5%
Other	3	1.5%

Table 2: Reasons cited for reusing passwords (sorted by frequency).

We found that no single reason explained why people reused passwords on some accounts and not for the others. However, our results did show that the highest proportion (28.4%) of the reasons cited for not reusing password was the value or importance of the accounts, followed by "I try to avoid password reuse because I believe it is not secure" (15.7%). This shows that our participants are aware that password reuse is not a secure practice which can put their valuable accounts at risk. Our participants chose the statement "I reuse password for this account because it is easy to remember" most often (35.1%) as their reason for password reuse. This suggests that "password overload" is a major contributor to unsafe password practice.

4.4 Account and Passwords Groupings

Our results indicated that all participants used some form of similarities to group their accounts. All participants except one also grouped their passwords using some form of similarities. Further investigation indicates that the non-grouping participant only had 3 passwords, which was the smallest amount of passwords among all our participants. Most of our participants provided colloquial descriptions of the similarities they used to group several accounts together, such as 'school stuff', 'e-mail accounts', and 'online banking'. We performed a bottom up analysis to categorise these reasons. Our analysis is necessarily subjective, because some of the descriptions were vague and developing a new set of categories

always involves some heuristic decisions. We settled on five categories.

1. **Type of service (72%)**
   Grouping based on the type of service or usage associated with accounts, e.g. financial, communication, and education.
2. **Risk (18.6 %)**
   Grouping based on the level of importance and risk of the information stored under the accounts, as well as the level of security measures assigned to the accounts.
3. **Frequency (5.2%)**
   Grouping based on frequency of usage of the accounts, where accounts with the same frequency of usage are grouped together.
4. **Alias (2.5%)**
   Grouping based on alias or login names associated with the accounts.
5. **Sharing (1.7%)**
   Grouping based on parties with which the account usage and credentials are shared, such as friends, work colleagues and family members.

We also performed a bottom-up analysis on the low level descriptions given by our participants of their password groupings, creating six categories.

1. **Semantic (44.4%)**
   Grouping based on similarities in semantic properties of the passwords, such as length, number of letters, number of words, permutation around similar phrases, pronunciation and so on.
2. **Inspiration (15.3%)**
   Grouping based on the inspiration used to create passwords.
3. **Accounts (15.3%)**
   Grouping based on types or categories of accounts for which the passwords are used.
4. **Perception of Security (12.5%)**
   Grouping based on users' perception of how secure the passwords are, where passwords that are considered to provide similar security levels are grouped together.
5. **Creation (6.9%)**
   Grouping based on who created the passwords, when and how the passwords were created, e.g. assigned by service providers during registration, created by own, and so on.
6. **Recallability (5.5%)**
   Grouping based on the ease of recall of passwords.

We were somewhat surprised by these statistics, having expected that the most common password grouping strategy would be by a perception of security.

4.5 Account and Passwords Groupings

We investigated whether account groups which are considered of high importance are managed differently from other account groups. Before any further investigation could be done, we first needed to separate the high importance account groups from the other, less important account groups. In our survey, we had asked the participants to assign a 'value of importance' score to each of their accounts using 5 point Likert scale. We used these scores to distinguish the groups which are considered of high importance in the following way. For each participant, we selected the account group which had the highest average (arithmetic mean) of 'value of importance' scores among all their account groups. In cases where there are several groups having the same highest average score, we selected all of these groups. Two participants failed to describe the associations between their passwords and accounts according our instructions, making it impossible to extract the information needed to perform this analysis. Consequently, we did not include their responses in this part of our analysis. Our selection process identified 37 account groups as being of high importance. The remaining 93 account groups were classified as low importance account groups, and were used as controls.

The main differences that we found between the high importance account groups and the low importance account groups are listed below.

4.5.1 Size

We found the high importance account groups to be of smaller size (in terms of number of accounts per group) on average (Mean = 1.84, SD = 1.28), compared to the low importance account groups (Mean = 2.78, SD = 2.21).

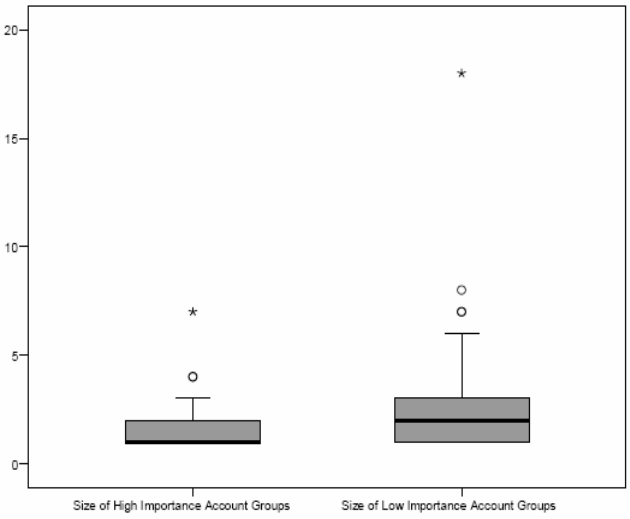

Figure 3: Box plot showing the differences in size of high importance account groups and low importance account groups.

4.5.2 Password Reuse Behaviour

In total there were 68 accounts in our high importance account groups, of which 43 (63%) were assigned passwords which were not used for any other accounts, whereas 25 (37%) had passwords which were reused. In contrast, of the 253 accounts in the low importance account groups, only 82 (32%) were given non-reused passwords, and 171 (68%) were given reused passwords.

Almost half (11/24) of our participants reused their passwords on at least one account in their high importance account groups, whereas nearly all participants (23/24) reused their passwords on at least one account in their low importance account groups.

Our analysis provided significant evidence that participants who reused their passwords on at least one account in their high importance account groups have, on average, a larger number of accounts compared to participants who did not reuse passwords on their high importance account groups (P-value = 0.020). We estimated the difference to be somewhere between 1.07 and 11.28 accounts. We also have significant evidence that participants who reused passwords on at least one account in their high importance account groups have on average longer internet experience than participants who did not reuse passwords in their high importance account groups (P-value = 0.028). We estimated the difference to be somewhere between 0.28 and 4.4 years.

4.5.3 Perceptions of Passwords Used

Our findings indicated that 17 of 24 (70%) of our participants have passwords that are exclusively used for accounts in high importance groups, and each participant has on average 2.9 of these passwords (S.D. = 1.9).

Using Student's t-test, we obtained significant evidence that passwords which are used exclusively on important account groups were considered to have significantly higher perceived security level (P-value = 0.017) and ranked as more difficult to recall (P-value = 0.02) compared to passwords which are used on less important account groups.

Our findings have shown that our participants have account groups which are considered more important than the others, and are managed differently. Compared to the other, less important account groups, these account groups tend to have reasonably less number of accounts. We also found that password reuse occurrences are significantly less in these groups. Furthermore, passwords which are used on accounts in these groups are perceived to be more secure and harder to recall.

5 Concluding Remarks

Before we proceed further, we would like to remind our readers that our results must be interpreted with extreme care. As we described in Section 3 and 4, our participants were all students at the University of Auckland, hence our results might not be the best representation of the general user population.

In contrast to previous studies on password usage practices, we investigated how a user's perceptions of their accounts and passwords influence their password selection. In accordance with our organising hypothesis, our results indicated that our participants did indeed mentally classify their accounts and passwords in groups based on various similarities.

Regardless of which similarities they used to classify their accounts, we found that our participants tended to use passwords which they perceived to be stronger, and that they did not reuse passwords as often, in account groups which they considered more important than their other account groups. This is unsurprising behaviour. By analogy, people will put their most valuable possessions in highly secure but inconvenient places, such as in safety deposit boxes. They are willing to go through the inconvenience because they understand the value of the possessions that they are trying to protect, and are aware of the risks associated with leaving their valuable possessions in easily accessible, obvious places. Our findings suggest that most of our participants have a similar sense of trading security for convenience, and that they understand that reusing passwords or using weak passwords on their important accounts could put their important information at risk. We thus believe that the underlying reasons for users' insecure password practices are their inability to remember more than a few passwords, and their failure to recognise the importance of some of their accounts. It may be helpful to teach users better ways of identifying their most important accounts.

Can users be prevented from reusing passwords? We think it unlikely, given the still-rapid rate of increase in online services. The relatively new phenomenon of single sign-on services does not seem to have significantly reduced the rate of increase in password reuse, although this could of course change if a small number of single-sign on services become wildly popular.

Drawing from our findings, we have a possibly provocative suggestion: reusing passwords on the less-important accounts should be encouraged rather than discouraged! Expecting users to create unique, strong passwords for all their accounts is just as unreasonable as expecting someone to place all of their possessions in a safe deposit box. Users should be taught how to identify which accounts are truly important, and deserving of strong and unique passwords.

By using passwords which they perceived to be more 'secure' on accounts that they considered important, our participants demonstrated their awareness of the importance of using strong passwords to protect their valuable information. As we did not measure the entropy strength of our participant's passwords, we are unable to make any assessment of the actual strength of their passwords. Previous studies (Adams and Sasse 1999; Gaw and Felten 2006) have shown that most users lack the knowledge of the capability of an attacker. The scale of an achievable dictionary attack is wildly underestimated. Passwords are often viewed as being secure if a typical human would not know the word being used as a password, or if a human could not easily guess it. Clearly, users still need education and assistance when choosing passwords for important accounts.

Our findings also opened a possibility to extend our concepts of password and account groupings to design more intuitive user interfaces for password and account management systems. However, this prospect still warrants future research.

6 References

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

Barton, B. F. and M. S. Barton (1984): User-friendly password methods for computer-mediated information systems. *Computer Security* **3**(3): 186-195.

Brown, A. S., E. Bracken, et al. (2004): Generating and remembering passwords. *Applied Cognitive Psychology* **18**(6): 641-651.

CentralNic (2001): Password clues, the CentralNic password survey report. http://www.centralnic.com/news/research. Accessed 5 December 2007.

Dhamija, R. and A. Perrig (2000): Deja vu: a user study using images for authentication. *Proceedings of the 9th USENIX Security Symposium*, USENIX Association.

Ding, Y. and P. Horster (1995): Undetectable on-line password guessing attacks. *ACM SIGOPS Operating Systems Review* **29**(4): 77-86.

Florencio, D. and C. Herley (2007): A large-scale study of web password habits. *Proceedings of the 16th International Conference on World Wide Web*, Banff, Alberta, Canada, 657-666, ACM Press.

Gaw, S. and E. W. Felten (2006): Password management strategies for online accounts. *Proceedings of the Second Symposium on Usable Privacy and Security*, **149**: 44-45, ACM Press.

Halevi, S. and H. Krawczyk (1998): Public-key cryptography and password protocols. *Proceedings of the 5th ACM Conference on Computer and Communications Security*, 230-268.

Horowitz, A. (2001): Top 10 security mistakes, Computerworld. http://www.computerworld.com/securitytopics/security/story/0,10801,61986,00.html. Accessed 30 September 2008.

Ives, B., K. R. Walsh, et al. (2004): The domino effect of password reuse. *Communications of the ACM* **47**(4): 75-78.

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

O'Gorman, L. (2003): Comparing passwords, tokens, and biometrics for user authentication. Proceedings of the IEEE **91** (12): 2019 - 2020.

Pinkas, B. and T. Sander (2002): Securing passwords against dictionary attacks. *Proceedings of the 9th ACM Conference on Computer and Communications Security*, 161-170.

Poulsen, K. (2000, March 2, 2000): Mitnick to lawmakers: people, phones are weakest links. http://seclists.org/politech/2000/Mar/0005.html. Accessed 10 July 2007.

Rejman-Greene, M. (2001): Biometrics — real identities for a virtual world. *BT Technology Journal* **19**(3).

Riddle, B. L., M. S. Miron, et al. (1989): Passwords in use in a university timesharing environment. *Computer Security* **8**(7): 569-578.

Riley, S. (2006). Password security: what users know and what they actually do. *Usability News* **8**(1).

Sasse, M. A., S. Brostoff, et al. (2001). "Transforming the 'weakest link' — a human computer interaction approach to usable and effective security." *BT Technology Journal* **19**(3): 122-131.

Weirich, D. and M. A. Sasse (2001): Pretty good persuasion: a first step towards effective password security in the real world. *Proceedings of the 2001 Workshop on New Security Paradigms*, 137-143, ACM Press.