December 2004

Password Composition and Security: An Exploratory Study of User Practice

John Campbell
Griffith University

Kay Bryant
Griffith University

Password Composition and Security: An Exploratory Study of User Practice

John Campbell
Kay Bryant

Department of Management
Griffith University
Brisbane, Australia
J.Campbell@griffith.edu.au
K.Bryant@griffith.edu.au

Abstract

User authentication is a vital element in ensuring the secure operation of computer-based systems. The most common control mechanism for authenticating user access to computerised information systems is the use of passwords. Password-based systems remain the predominant method of user authentication despite the many sophisticated and viable security alternatives that have emerged from research and development. However, evidence suggests that this method is often compromised by poor security practices. This paper presents the results of a survey that examines user practice in creating and using password keys. This paper reports the findings from a pilot study examining user password composition and security practices for e-mail. Despite a greater awareness of security issues, the results show that an improvement in user password management practice is required.

Keywords

Password composition, password security, email

INTRODUCTION

User authentication is an essential first line of defence in the security of computer-based systems. There are three main approaches to user authentication: something the user knows (password or PIN), something the user has (a smart card or other token) and something the user is (a biometric characteristic) (Furnell et al. 2000). Password systems are the most commonly used means of authentication in computer-based systems. Passwords are conceptually simple for both system designers and end users, and can provide effective protection if they are used correctly. Unfortunately, users can compromise password security by forgetting passwords, writing them down, sharing them with other people and selecting easily guessed words.

Due to the predominance of password authentication systems, many users are required to remember passwords for a range of different systems and applications. The requirement to remember such a large number of passwords can cause a major problem for users. It is, therefore, no surprise that users frequently select dictionary words or personal names as the basis for their passwords, as these are easier to remember. Not only can users choose insecure and easily guessed passwords, they may also select the same password for multiple accounts. As such, should an intruder gain access to one protected account, it is quite likely that he or she will be able to reuse that same password to gain access to other devices or applications. Once a password is compromised, an intruder may remain unnoticed for some time unless passwords are changed frequently.

PASSWORD SECURITY ISSUES

The password approach has a number of shortcomings, which can undermine the effectiveness of the approach (see for example Furnell et al. 1999, Jobusch and Oldehoeft 1989). Several studies have examined the ease with which passwords can be determined. In one of the earliest empirical studies, Morris and Thompson (1979) found that a personal computer could guess 86 percent of passwords in less than one week. Subsequent replications of this study by Klein (1990) and Spafford (1992) found that password selection had improved over time with only 21 percent being able to be guessed in a week. Unfortunately, the software tools that can be used to deduce passwords have become even more powerful and seditious in recent years. The major strategies for overcoming the inherent weaknesses in password usage include the following:

- Non-Dictionary words: selecting non-dictionary passwords prevents the use of dictionary-based attacks. Such attacks can identify a password in less than 20 minutes even on dictionaries with up to one million words. The only way to identify non-dictionary passwords is using a brute-force approach (testing every combination of characters for every length of password).
- Passwords with mixed case/symbols: Including both upper/lower case and symbols (!#$% etc.) in passwords requires any attack to use a brute force method and increases the number of character permutations that must be tried.
- Password ageing: Should an intruder obtain a valid password, most systems will allow them to continue to access the system until the intrusion is noticed. Users need to change their passwords regularly, thus forcing the intruder to identify the new password.

While these strategies may help improve password security, these restrictions make the composition and memorising of passwords a complex and unintuitive exercise.

A PRELIMINARY SURVEY OF E-MAIL PASSWORD SECURITY

Most research on e-mail has concerned itself with the issues of media choice and media effects (see Lee 1994, Markus 1994). E-mail is one of the most successful Computer Supported Cooperative Work (CSCW) applications to date and affects the daily life of almost every working person in the industrialised world (Rudy 1996, Bälter 2000).

A pilot study was conducted to assess the attitudes and awareness of the general public so as to gain insight into password composition and management practice. The study assessed the following issues:

- Profiling e-mail account usage (purpose, number of accounts, frequency of access)
- Password practice (reuse, composition, disclosure, backup)

A questionnaire was designed to elicit responses about student use and management of e-mail passwords. The first section of the questionnaire collected demographic data and information as to their computer and e-mail usage. The second section focused specifically on password use and management practices. The survey was administered to the students in the second last week of semester.

Students who had enrolled in a second-year information systems course participated in the study. All students had undertaken at least one year of study within the Business School. Participation in the survey was entirely voluntary with 82 students volunteering to participate. The gender breakdown was 49 males and 31 females with 2 students not responding to this question. The majority of students were aged between 16 and 25 (63), 12 were between 25-35 and the remaining 7 students were between 36-45. All but 9 of the students were enrolled at University on a full time basis. One of the nine was not actually enrolled; only auditing the course. Half the students were not employed, 29 were employed on part-time and 9 were full-time employees; 3 students did not respond to this question.

The majority of students had used computers for more than 5 years; 42 had used computers between 6-10 years and 22 for longer than 10 years. Only 2 students had used computers for less than 2 years. Students were asked to indicate what they used computers for. Approximately 80 percent of students indicated their main use was for Internet, e-mail and home use. Bank and work use formed a second grouping of between 42-50 percent and Other areas of use (eg studies, games and watching videos) accounted for less than 20 percent. The number of e-mail accounts varied; 5 had only one; 22 had 2; 29 had 3, 25 had 4 or more e-mail accounts and 2 students did not respond to the question. Personal e-mail use was most prevalent (94 percent), followed by University use (83 percent) and Work-related use (31 percent). Students were asked whether they used the same password for all e-mail accounts. Of the 80 students responding, 23 used the exact same password, 35 had passwords with a slight variation and 22 used completely different passwords.

RESULTS & DISCUSSION

This section reports the results of the data analyses from the second section of the questionnaire. This section focused on e-mail password practices – length and composition in the first instance and then on self-management of passwords. The results of the pilot study are shown in diagrammatic form as histograms – Figures 1-8.

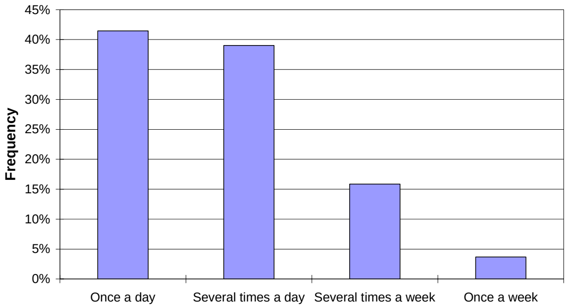

Figure 1. Frequency of Email Account Access

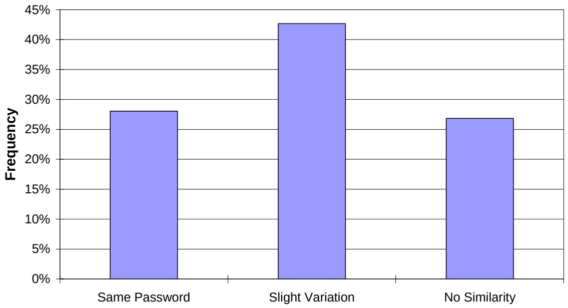

Figure 2. Password Similarity Between Accounts

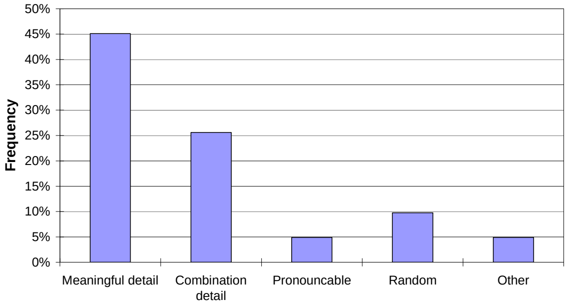

Figure 3. Password Composition

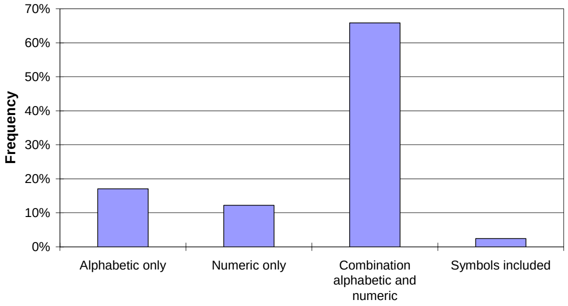

Figure 4. Type of Characters in Password

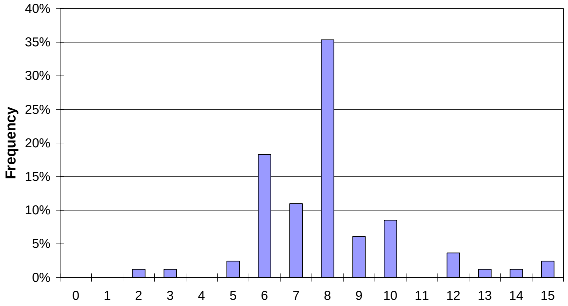

Figure 5. Characters in Email Password

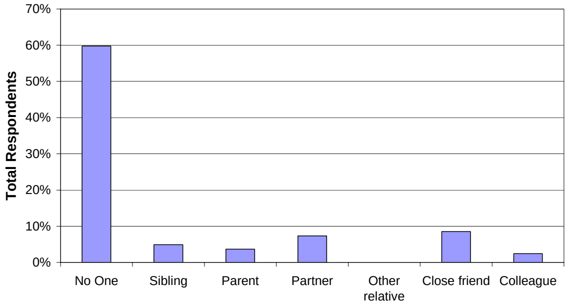

Figure 6. Password Sharing

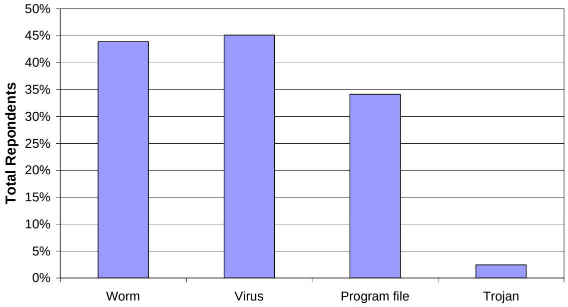

Figure 7. Password Cracking Techniques

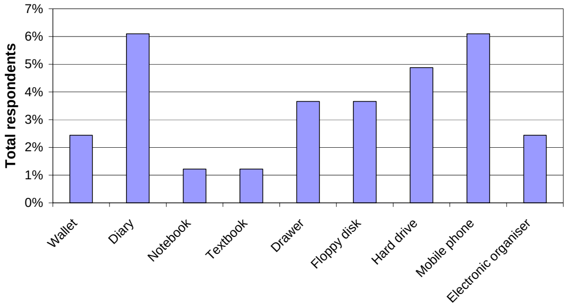

Figure 8. Methods used to Store Passwords

E-mail accounts are heavily used as shown in Figure 1 since at least 80 percent of students check their e-mail one or more times a day. This result could well be expected given that the subjects participating in this pilot study were students enrolled in a course involving online resources.

What is interesting is the similarity between passwords for different e-mail accounts (Figure 2). Of the 80 students responding to this question, 23 used the exact same password, 35 had passwords with a slight variation and 22 used completely different passwords. One promising factor was that most passwords were a combination of alphabetic and numerical characters and were on average 8 characters in length. With the exception of 2 students whose passwords were 2 and 3 characters long, password length ranged between 5 and 15 characters (Figure 5). An interesting follow-up on this would be to determine whether this was required by their e-mail provided or whether this was by their own choice. However, while this result is positive, the fact that just under half of the passwords contained meaningful detail or a combination of meaningful detail is of some concern. This outcome coupled with the fact that respectively, 35 percent and 44 percent of respondents never changed their password or changed it no more than twice a year, indicates a serious lack of concern with password security. On the whole, respondents appear to be unconcerned about the risks associated with poor password composition. It would appear there is a need for a better education process on password composition for users. The education process should also stress the wide variety of programs able to crack passwords relatively easily. Just under 38 percent of respondents were not aware of these types of programs.

Along with questions about password composition, respondents were also asked about sharing and remembering their passwords. The results are slightly more positive with regards to revealing their password to others. Almost 60 percent of respondents (49) said they had not shared their password. Of the 15.9 percent who had shared, it was with a close relative such as partner (6), sibling (5) or parent (2). Only 8.5 percent of respondents had shared with non-family members such as a close friend (6) or colleague (1). Respondents were evenly divided with respect to admitting whether they had forgotten their password; 8 chose not to answer this question. The following question asked where respondents had kept written versions of their passwords either in electronic or hard copy format. As shown in Figure 8, a wide array of places was listed. However, over 70 percent of respondents said they did not keep copies of their password regardless of the media. It would appear that, for the most part, respondents are reacting positively towards messages about password practices of sharing and remembering.

CONCLUSION

This study has briefly explored aspects of user practice in password composition and security management within the context of e-mail usage. A major objective of this study was to design and pilot a survey instrument for a more comprehensive study to be undertaken at a later date. However, the results from this pilot are revealing in itself and provide important insight into ongoing issues relating to the creation and management of user-based password management systems. The survey results support our initial focus on e-mail account management as an important end-user application context. E-mail usage was found to be very high with around one-third of all respondents using three or more e-mail accounts. As anticipated, this creates password management difficulties for users and encourages password reuse across different e-mail accounts and/or their storage on paper or in an electronic device for later reference. The password composition practices adopted by respondents further compound this situation. Our results show that the vast majority of users are choosing passwords that are based on meaningful personal details that can be more readily guessed by others.

The password practices of users is an under researched area. Our results, while only preliminary, show that many users have not adopted secure management practices. Our ongoing research will build upon this understanding and aim to gain further insight into how user practices can be improved.

REFERENCES

Adams, A. and Sasse, M.A. (1999) Users Are Not the Enemy, *Communications of the ACM*, 42:12, 41-46.

Bälter, O. (2000) How to replace an old email system with a new, *Interacting with Computers*, 12:6, 601-614.

Furnell, S.M., Dowland, P.S., Illingworth, H.M. and Reynolds, P.L. (2000) Authentication and Supervision: A Survey of User Attitudes, *Computers & Security*, 19:6, 529-539.

Sherman, R. (1992) Biometrics Futures, *Computers & Security*, 11:2: 128-133.

Jobusch, D.L. and Oldehoeft, A.E. (1989) A Survey of Password Mechanisms: Part 1, *Computers & Security*, 8:7, pp. 587-604.

Klein, D. (1990) A survey of, and improvements to, password security, *Proceedings of the USENIX Second Security Workshop*, Portland, Oregon, August 1990: 5-14.

Lee, A.S. (1994) Electronic Mail as a Medium for Rich Communication: An Empirical Investigation Using Hermeneutic Interpretation, *MIS Quarterly*, 18:2, June, 143-157.

Markus, M. L. (1994) Electronic Mail as the Medium of Managerial Choice, *Organization Science*, 5:4, November, 502-527.

Morris, R. and Thompson, K. (1979) Password Security: A Case History, *Communications of the ACM*, 22:11, 594-577.

Rudy, I.A. (1996) A critical review on research on electronic mail, *European Journal of Information Systems*, 4, 198-213.

Spafford, E.H., (1992) Opus: Preventing Weak Password Choices, *Computers & Security*, 11:3: 273-278.

Zviran, M. and Haga, W.J., (1999) Password Security: An Empirical Study, *Journal of Management Information Systems*, 15:4. 161-185.

APPENDIX

Survey on Password Practice

Security is of concern for users of computerised information systems. The most common control mechanism for authenticating user access to computerised information systems is the use of passwords. The purpose of the research study is to examine user practice in creating and using passwords. This questionnaire is designed to investigate user email account password usage and practice.

The survey is voluntary and anonymous. Individual responses will not be identified. Please do not identify yourself in any way, write your password(s) or e-mail address anywhere on this survey.

Please tick the box that best applies to you.

What is your age group?
□ 16-25 years □ 26-35 yrs □ 36-45 yrs □ 46-55 yrs □ More than 56 yrs

What is your gender? □ Male □ Female

Are you enrolled at university? □ Full time □ Part time □ Not enrolled

Are you employed? □ Full time □ Part time □ Not employed

How long have you been using a computer?
□ 0 - 2 years □ 3-5 years □ 6-10 years □ More than 10 years

What do you use a computer for? *Tick all that apply.*
□ Home use □ Work □ Banking □ Email □ Internet access
□ Other use, please specify ____

How many email accounts do you currently have? □ 1 □ 2 □ 3 □ 4 or more

If you have more than one email account, do you use the exact same password for each email account?
□ Same password □ Slight variations of the same password □ No similarities between passwords

What is your email use? *Tick all that apply.*
□ Personal □ Work □ University
□ Other, please specify____

Besides email, do you use any other computer-based applications that require the use of a password?
Please specify____

Please apply the following questions to your most frequently used email account.

How often do you check your emails?
□ Once a day □ Several times a day
□ Once a week □ Several times a week
□ Once a month □ Several times a month
□ Never

How many characters are in your password? Please specify ________

Does your email password contain?
□ Alphabetic characters only (eg. abcd, ERTIS)
□ Numeric characters only (eg. 1234, 5579)
□ Combination of alphabetic and numeric characters (eg. a34d, Fo67Y1)
□ Combination of characters including symbols (eg. @sad1&%*_)
□ Other

How did you choose your password?
□ Meaningful detail (eg. name, date, street, registration number)
□ Combination of meaningful details (eg. Bill2000, 4jun84)
□ Pronounceable password (eg. one4you, 2Bfree)
□ Random combination of characters (eg. car8&t, CoLL186+)
□ Other, please specify __________________

Have you ever forgotten your password? □ No □ Yes

I keep a hand-written copy of my password in my: *Tick all that apply.*
□ Wallet □ Diary □ Notebook □ Textbook □ Desk □ Drawer □ Computer keyboard
□ Computer monitor □ Other, please specify ____
□ I do not keep a hand-written copy of my password

I keep an electronic copy of my password on my: *Tick all that apply.*
□ Floppy computer disc □ File on computer hard drive □ Mobile phone
□ Electronic Organiser □ Other, please specify _________________________________
□ I do not keep an electronic copy of my password

How often do you change your password?
□ Never
□ Less than once a year
□ 1 - 3 times a year
□ 4 - 6 times a year
□ Once a month
□ More than once a month

With whom do you share your email password? *Tick all that apply.*
□ No other person
□ A sibling
□ A parent
□ Partner
□ Other relative
□ Close friend
□ Colleague
□ Other, please specify ________________

Have you ever changed your password because you felt that someone else had guessed it?

□ No □ Yes

If so, what led you to believe it had been guessed? ________________________________

Are you aware of password cracking techniques? *Tick all that apply*.

□ Worm
□ Virus
□ Program file
□ Other, please specify____

What do you consider are the major problems with password security? ________________________________

____

____

____

Thank you for your participation.

COPYRIGHT