Password Composition Policy: Does Enforcement Lead to Better Password Choices?

John Campbell
Dale Kleeman
Wanli Ma
University of Canberra

School of Information Sciences and Engineering
University of Canberra
Canberra, ACT
Email: john.campbell@canberra.edu.au
Email: dale.kleeman@canberra.edu.au
Email: wanli.ma@canberra.edu.au

Abstract

The primary function of access controls is to restrict the use of information systems and other computer resources to authorised users only. Although more secure alternatives exist, password-based systems remain the predominant method of user authentication. Prior research shows that password security is often compromised by users who adopt inadequate password composition and management practices. One particularly under-researched area is whether formal password composition policies actually lead to more secure passwords and user security practices. Consequently, this study investigates empirically the efficacy of using password composition rules to improve password security. The results show that the enforcement of password composition rules does not significantly reduce the use of meaningful data. While the enforcement of rules does reduce password reuse, the overall incidence remains high. These passwords are also perceived by users as being more difficult to remember. Finally, the enforcement of password composition rules significantly increases the average Levenshtein's edit distance between the passwords and ordinary dictionary words indicating that enforcement does improve protection against dictionary-based attack.

Keywords

Password authentication, password policy, computer security

INTRODUCTION

Although better authentication systems exist (e.g., see Boukhonine et al. 2005), password-based authentication remains the most commonly used means of controlling access to computer-based resources. Passwords are conceptually simple for both system designers and end users, and can provide effective protection if they are used correctly. Unfortunately, users sometimes compromise password security through forgetfulness, by writing them down, sharing them with other people and by selecting easily guessed words. These weaknesses are known to seriously undermine the efficacy of computer system security (Conklin et al. 2004, Carstens 2004, Ives et al. 2004, Furnell et al. 1999, Jobusch and Oldehoeft 1989, Spafford 1992, Zviran and Haga 1999).

A consequence of these weaknesses is that organisations often rely on password composition policies to force users to create more secure passwords. This is usually implemented in such a way as to provide an explicit framework that constrains user choices during the password composition process. However, little is known about how user behaviours are changed except that it is difficult for users to create passwords that are both secure and easy to remember (Yan et al. 2004). To this end, our primary research question is: *Does the enforcement of password composition policy lead to better password choices?*

ASSESSING THE EFFICACY OF ENFORCED PASSWORD COMPOSITION RULES

Password authentication systems are commonly used for securing access to IT devices such as PDAs, laptop computers and desktop computers. These passwords are usually stored in a special secure storage space on the IT device itself and are also sometimes used to gain access to network resources. These passwords are vulnerable to attack in three ways:

- **Password guessing:** The weakest passwords are those that can be easily guessed. The easiest way to guess a password is to start with a dictionary of common words, slang, and popular phrases. It is then relatively easy to write a program to mimic a human logging on to a web-based application using combinations user logon codes and guessed passwords (Zhang 2005).
- **Social engineering:** Perpetrators will attempt to exploit the gullibility of users by pretending to be somebody trustable. Even the most careful user can be sufficiently lulled into a false sense of security to disclose personal information and sometimes even passwords (Adams and Sasse 1999, Haggerty and Taylor 2005). The impact of social engineering on password security is not the primary focus of this paper as weak and strong passwords are equally vulnerable to social engineering attack.
- **Password cracking:** password cracking requires the encrypted version of the password. The encrypted version can be accessed via network sniffing (especially in wireless networks), virus implanting (Bento and Bento 2004), and through Spy Ware such as *PPAuditor* or *RainbowCrack* (Symantec 2006a, 2006b). With the increasing prevalence of mobile devices, it is becoming easier for perpetrators to gain access to an encrypted password stored on a mobile device.

Password composition policies are meant to reduce the risk of attack by forcing users to compose passwords that are not easy to guess or that have similarities to common dictionary words (Piscitello and Kent 2003). Unfortunately, complex passwords are also more difficult to remember and users are sometimes tempted to write them down or to keep an electronic copy stored in a mobile phone, computer, or on other storage device. In terms of our research question, we assess the impact of password composition policy on the known weaknesses in user-defined passwords. These are: the use of meaningful data, memorability, and similarity to dictionary words.

Passwords Composed with Meaningful Information

There are a range of utilities available that enforce password composition rules. For example, Microsoft provides the capability for a system administrator to set a restrictive password policy that enforces password aging, minimal length, or a mix of upper and lowercase letters, numbers or symbols etc. (Microsoft 2006). It is generally assumed that rule enforcement does actually lead to more secure passwords. Surprisingly however, there is no research evidence that this is the case. However, evidence from earlier research does suggest that well documented security policies do not by themselves lead to more secure systems (Foltz et al. 2005). Consequently, restrictions on password composition may not prevent users from compromising system security by choosing vulnerable passwords containing meaningful data. For example, consider the following password criteria based on good password practice (Pfleeger and Pfleeger 2003):

- Password should not contain all or part of the users account name
- Password should be at least 8 characters long
- Password is not 'password' or a deviation thereof; or left blank
- Password contains characters from three of the following four categories:
  - English uppercase characters (A…Z)
  - English lowercase characters (a…z)
  - Base 10 digits (0…9)
  - Non-alphanumeric (!@#$%^&* etc.)

While the various elements of this policy appear to adequately address traditional password weaknesses, it is relatively easy to compose examples containing large amounts of meaningful information, but that still satisfy all the requirements of the policy. For example: Broncos#1, NinaLee05, =Lunatic=, Diamond*, etc. While each of these examples satisfies the password composition rules listed above, these particular combinations could still be easily guessed or hacked. Nevertheless, as the intention of composition rules is to reduce the meaningful information contained in passwords, we will test the following proposition:

P1: The enforcement of password composition rules will reduce the meaningful information contained in user-defined passwords.

Password Memorability

Due to the predominance of password authentication systems, many users are required to remember passwords for a range of different systems and applications. Remembering a unique password for each system can be difficult for users. It is therefore no surprise that many users select dictionary words, personal names or other meaningful information as the basis for their passwords because they are easier to remember. For similar reasons users frequently select the same password for multiple accounts (Ives et al. 2004). As such, should an intruder obtain the password of one protected account, it is quite likely that he will be able to reuse that password, or a

close variation thereof, to gain access to other devices or computer applications belonging to the same individual. In this context, password composition rules are expected to result in passwords that are less similar to earlier password choices but, as a result, will be more difficult to remember. Consequently, we test the two propositions:

P2: The enforcement of password composition rules will reduce password reuse.

P3: The enforcement of password composition rules will produce passwords that are difficult to remember.

Password Similarity to Common Dictionary Words

Passwords containing common dictionary words can be cracked within minutes and sometimes even seconds. We found that a modest desktop computer (Intel Pentium 4, 2.4 GHz, without Hyper-Threading turned on) running the Fedora Core 5 operating system can complete a crypt[1] function in about 10 microseconds creating the capacity to test up to 10^5 passwords in one second. Checking all of the 479,625 words contained in the Fedora Core 5 English spell-checking dictionary takes approximately 5 seconds. Consequently, the paramount objective of enforcing password composition policy is to ensure that users create passwords that are less susceptible to dictionary-based attack. Consequently, we test the following proposition:

P4: The enforcement of password composition rules will produce passwords that are less similar to dictionary words.

RESEARCH DESIGN

The research employs an experimental research design where participants are randomly allocated to one of two main study groups. As described in Figure 1, the two groups cover unrestricted password composition (Group A – the experimental control group) and restricted password composition (Group B - the experimental treatment group). Each of these study groups was then exposed to different password composition criteria and asked to compose and change a password for a hypothetical work-based computer account using an online password interface designed for this purpose. The research context and password composition tasks were designed to simulate the experience of a password composition exercise for a new employee. Details of the experimental protocol for each group are provided in Table 1.

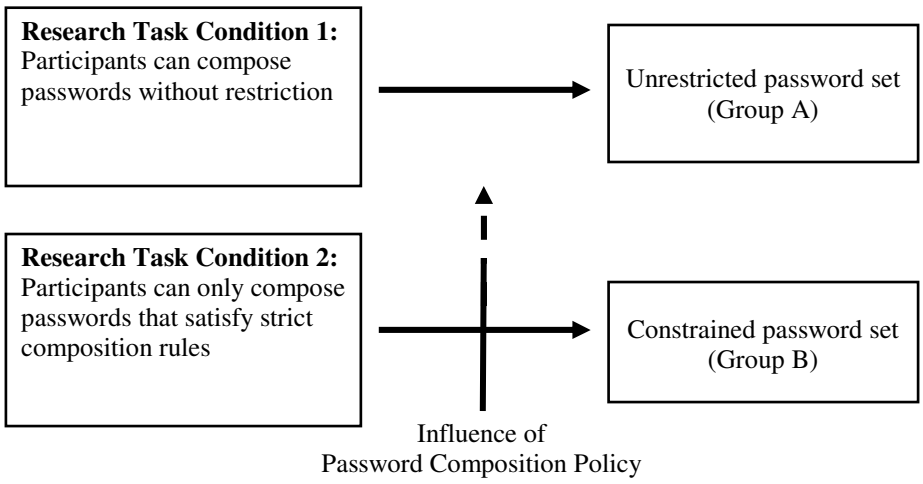

Figure 1: Impact of password composition policy on user-defined passwords

Data

The research experiment was conducted in June 2006 and involved 62 undergraduate student participants studying within an Australian university business faculty. This cohort was sampled so as to provide indicative

[1] crypt(3) is widely used for Un*x password encryption. Although different password encryption algorithms are available, the performance of crypt(3) provides a reasonable benchmark for password cracking speed.

information on the password composition behaviour that university educated recruits might bring into new employment positions within organisations operating in the knowledge economy. Students were approached in tutorial classes with each class being randomly allocated to a treatment or control group. This resulted in 27 individuals participating in the control group environment (Group A), and 35 individuals participating in the treatment group environment (Group B). As well as the password composition tasks described above in Table 1, participants were also asked to complete a short survey which is listed in the Appendix.

General Instructions Provided To Both Groups	Instructions for the No Enforcement Rules Group	Instructions for the Enforcement Rules Group
We are giving you this instruction sheet as part of the password security experiment that is described in the attached *Research Participant Information Sheet*. If you agree to participate in this study, you are required to put yourself in the place of a new graduate employee. As part of your induction you have been given details about a password protected computer account for accessing email and other online organizational resources. You would usually be required to log on to this account every day as part of your normal work duties. You will also be required to remote access this account using an Internet connection when you are working away from the office. This might occur once or twice a week. Your task here is to compose a new password for your work-based computer account and then to answer a brief online survey. Completing this task should take between 5 and 10 minutes. Please ensure that you observe all of the instructions contained in the following three steps.	**Step 1** Please go to the following web address: **{online survey web address}** If you do not wish to participate in this study, please use the mouse to click on the "NO" button and then return this instruction sheet. If you do agree to participate, then please enter your Logon Code and Default Password and click the "YES" button. **Step 2** Choose and enter your new password in the required fields. When you have successfully created your new password, please click the continue button. **Step 3** Please complete all survey questions and then click the continue button to conclude the research task.	**Step 1** Please go to the following web address: **{online survey web address}** If you do not wish to participate in this study, please use the mouse to click on the "NO" button and then return this instruction sheet. If you do agree to participate, then please enter your Logon Code and Default Password and click the "YES" button. **Step 2** Choose and enter your new password in the required fields. For security purposes, your new password will not be accepted unless it satisfies the following requirements: • Password does not contain all or part of the users account name • Password is at least 8 characters long • Password is not 'password' or a deviation thereof, or left blank • Password must contain characters from three of the following four categories: o English uppercase characters (A…Z) o English lowercase characters (a…z) o Base 10 digits (0…9) o Non-alphanumeric (!@#$%^&* etc.) When you have successfully created your new password, please click the continue button. **Step 3** Please complete all survey questions and then click the continue button to conclude the research task.

Table 1: Experimental instructions and password composition tasks for the control and treatment groups

RESULTS

Passwords Containing Meaningful Information

Participants were asked whether the password chosen contained meaningful data such as a name, birth year etc. or was composed using some other approach such as a pass-phrase, pronounceable phrase or random keyboard characters. The enforcement of password composition policy has reduced the meaningful information contained in passwords (from 29.4 percent down to 11.4 percent of passwords), but not the use of combinations of meaningful information such as a name in combination with a birth date (from 16.7 percent in the control group increasing to 42.9 percent for the enforced policy group).

Inferential statistical testing was used to asses Proposition 1. Because of sample size restrictions, the responses were recoded into a dichotomous variable with meaningful and combination of meaningful data responses coded with a value of one. All other response choices were recoded with a zero. A subsequent chi-square test established that there was no statistical difference between each group in relation to the use of meaningful data within passwords, χ^2 (1, N=59) = .407, p<.262. Therefore, we conclude that Proposition 1 is not supported and that the enforcement of password composition rules does not reduce the amount of meaningful information contained in user-defined passwords.

Password Reuse and Memorability

Participants were asked whether the password chosen was the same, similar or completely different from one used in the past. Table 2 shows the distribution of responses by participants in each of our two groups. The impact of enforced password composition policy appears to have decreased the incidence of password reuse (53.8 percent in the control group compared to 17.6 percent in the enforced policy group). A subsequent chi-square test established that there was a statistical difference between each group in relation to password reuse, χ^2 (2, N=60) = 8.725, p<.013. This result supports Proposition 2 which stated that the enforcement of password composition rules will reduce password reuse.

To assess memorability, participants were asked how likely they would be able to remember their new password by the next day and by the next week. A t-test for independent groups was used to assess the differences between the group perceptions for both the one and seven day time periods. There was no significant difference between expectations of the control group (M=4.42, SD=1.065) and the experimental group (M=4.11, SD=1.207) over a one day period, t(59)=1.038, p=.165. However, there was a significant difference in expectations between the control group (M=4.27, SD=1.151) and the experimental group (M=3.60, SD=1.143) over a seven day period, t(59)=2.255, p=.014. Although both groups expect to still be able to remember their password the next day, the enforced composition rules group perceived their passwords to be more difficult to remember over a slightly longer period of one week. Based on these results, we conclude that Proposition 3 is supported and the enforcement of password composition rules do produce passwords that are more difficult to remember over time.

Experimental Condition	Has been used before	Is similar to one used before	Not used before	Totals
No enforcement	14	6	6	26
	53.8%	23.1%	23.1%	100%
Enforced policy	6	13	15	34
	17.6%	38.2%	44.1%	100%

Table 2: Incidence of password reuse for each experimental group

Passwords Similarity with Dictionary Words

A measure of password vulnerability to dictionary style attack can be tested by assessing the similarity between a password string and common dictionary words using Levenshtein's edit distance (Levenshtein 1965). This metric calculates the distance between two strings by counting and then adding the minimal number of single character manipulations required, such as an insertion or deletion, to make the string values equivalent (Stephen 1994). The Fedora Core 5 English dictionary (Fedora 2006) was used to generate a Levenshtein's edit distance score for each password based on its closest dictionary word. Although more comprehensive dictionaries would most likely be used for password cracking purposes, this dictionary is adequate for the purpose of demonstrating the differences between the treatment and control groups. Table 3 shows the distribution of distance measures for each group. The differences between the experimental control and treatment groups are quite marked. The control group appears to have two distributions of distances – the first contained passwords that ranged from zero to two edit distances, and the second cluster containing passwords that ranged from four to six single character edits. In contrast, the enforced policy group created passwords with edit distances ranging from two through to eight. Statistical testing indicated that the Levenshtein's edit distances are significantly higher where the password composition rules were enforced (M=4.63, SD=1.416) in comparison to the unconstrained group (M=3.37, SD=1.964), t(60)= -2.931, p=.005). Therefore, Proposition 4 is also supported as the enforcement of password composition rules produces passwords that are less similar to a standard dictionary of words.

A closer inspection of the data reveals that almost 26 percent of the control group (no enforced composition policy) had a Levenshtein's edit distance of two or fewer. While the lowest edit distance for the enforced policy group was two which accounted for a little less than six percent of passwords created by this group. While this result is a significant improvement over having no password composition rules, further improvement is clearly still required.

Experimental Condition	Levenshtein's edit distance									Totals
	0	1	2	3	4	5	6	7	8	
No enforcement	2	5	3		10	2	5			27
	7.4%	18.5%	11.1%		37.0%	7.4%	18.5%			100%
Enforced policy			2	6	8	10	6	2	1	35
			5.7%	17.1%	22.9%	28.6%	17.1%	5.7%	2.9 %	100%

Table 3: Levenshtein's edit distance calculated based on the standard Fedora Core 5 English dictionary.

DISCUSSION

The motivation for this research was to investigate the impact of password composition rules on password security. In order to answer this question, we first examined how the enforcement of password composition rules might discourage users from reusing passwords and using meaningful information. We also examined password memorability and measured the distance between passwords and common dictionary words. From the data it appears that enforced password composition rules do not discourage the use of meaningful information in passwords. While there is a significant reduction in password reuse, the level of reuse reported by participants remains very high (more 54 percent of participants reported that they chose passwords containing meaningful or a combination of meaningful data). Also, participants perceive that these passwords are less memorable over a relatively short time-frame of one week. Altogether, the findings are cause for concern as they indicate that the enforced composition rules used in this study are ineffectual on these intransigent user behaviours. An analysis of the Levenshtein's edit distances show that both groups are relatively safe from dictionary-based attack. However, there remain significant numbers of passwords generated by both study groups that are highly susceptible to dictionary-based attack.

The results from this study provide important insight into ongoing issues relating to the creation and management of user-based password management systems. While the results highlight some of the benefits of enforcing password composition rules, the overall findings are far from emphatic. While enforced composition rules improved password strength, they did little to reduce the vulnerabilities caused by the use of meaningful information, password reuse or user forgetfulness. Consequently, organisations should not rely solely on the enforcement of password composition rules to ensure password security. Future research is required to better understand how different password policy environments might improve password security by encouraging positive user behaviours.

REFERENCES

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

Bento, A. and Bento, R. (2004) Empirical Test of a Hacking Model: An Exploratory Study, *Communications of the Association for Information Systems*, 14:32, 678-690.

Boukhonine, S., Krotov, V. and Rupert, B. (2005) Future Security Approaches and Biometrics, *Communications of the Association for Information Systems*, 16:48, 937- 966.

Carstens D.S., McCauley-Bell P., Malone L.C. and DeMara R.F. (2004) Evaluation of the Human Impact of Password Authentication Practices on Information Security, *Informing Science Journal*, 7:1, 67 – 85.

Conklin, A., White, G., Cothren, C., Williams, D. and Davis, R.L. (2004), *Principles of Computer Security: Security+ and Beyond*, McGraw-Hill, New York.

Fedora, (2006) Fedora Core 5, http://fedora.redhat.com/ (accessed February, 2006)

Foltz, C.B., Cronan, T.P. and Jones, T.W. (2005) Have you met your organization's computer usage policy? *Industrial Management & Data Systems*, 105:2, 137 – 146.

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.

Haggerty, J. and Taylor, M. (2005) One born every minute, *ITNOW*, 47, 26-27.

Ives B., Walsh K.R. and Schneider H. (2004) The Domino Effect of Password Reuse, *Communications of the ACM*, 47:4, 75-78.

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

Klein, D. (1990) A Survey of, and Improvements to, Password Security, *Proceedings of the USENIX Second Security Workshop*, Portland, Oregon, August, 5-14.

Klein, D.V. (1999) Defending against the wily surfer — Web based attacks and defenses, *Proceedings of the First Workshop on Intrusion Detection and Network Monitoring*, April 9-12, Santa Clara, California, 81–92.

Levenshtein, V. (1965) Binary codes capable of correcting deletions, insertions, and reversals, *Problems in Information Transmission*, 1, 8-17.

Microsoft, (2006) Step-by-Step Guide to Enforcing Strong Password Policies, http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/directory/activedirectory/stepbystep/strngpw.mspx#EMD (accessed June, 2006)

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

Piscitello, D. and Kent, S. (2003) The Sad And Increasingly Deplorable State Of Internet Security, *Business Communications Review*, Feb., 49-53.

Pfleeger, C.P. and Pfleeger, S.L. (2003) *Security in Computing*. Third ed. Prentice Hall: New York.

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

Stephen G. (1994) String Searching Algorithms, *Lecture Notes Series on Computing*, 3, World Scientific Publishing.

Symantec, (2006a) PPAuditor, http://securityresponse.symantec.com/avcenter/venc/data/ppauditor.html (accessed 20 June 2006)

Symantec, (2006b) RainbowCrack, http://securityresponse.symantec.com/avcenter/venc/data/rainbowcrack.html (accessed 20 June, 2006)

Yan J., Blackwell A., Anderson R. and Grant A. (2004) Password Memorability and Security: Empirical Results. *IEEE Security and Privacy*, September/October, 25-30.

Zhang, M. (2005) Breaking an Improved Password Authenticated Key Exchange Protocol for Imbalanced Wireless Networks, *IEEE Communications Letters*, 9:3, 276-278.

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

APPENDIX

Online Survey Questions

For each of the following question, please tick the box that best applies to you.

What is your age group? ☐ Less than 18 years ☐ 18-25 years ☐ 26-35 years ☐ 36-45 years ☐ 46-55 years ☐ More than 55 years

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

Is the password that you have just created one that you have used in the past?

☐ Yes ☐ Not at all ☐ Password has a similarity to another password that I have used before

How did you choose your password?

☐ Meaningful detail (eg. name, date, street, registration number)
☐ Combination of meaningful details (eg. Bill2000, 4jun88)
☐ Pronounceable password (eg. one4you, 2Bfree)

☐ Using the first letter from each word in a special phrase (eg. "my cat is called Tom" to create the password mcicT)
☐ Random combination of characters (eg. Qcar8&t, CoLL186+)
☐ Other, please specify

_____
_____

If you had to rely on your memory alone, how likely are you to be able to remember this password within 1 day from now?

Very Likely				Very Unlikely
☐	☐	☐	☐	☐

If you had to rely on your memory alone, how likely are you to be able to remember this password within 1 week from now?

Very Likely				Very Unlikely
☐	☐	☐	☐	☐

What steps might you take to help you remember this password?

_____
_____
_____

COPYRIGHT