Behaviour & Information Technology
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/tbit20

Impact of restrictive composition policy on user password choices

John Campbell [a], Wanli Ma [a] & Dale Kleeman [a]
[a] Faculty of Information Sciences and Engineering, University of Canberra, Canberra, ACT, 2601, Australia
Published online: 09 Aug 2010.

To cite this article: John Campbell, Wanli Ma & Dale Kleeman (2011) Impact of restrictive composition policy on user password choices, Behaviour & Information Technology, 30:3, 379-388, DOI: 10.1080/0144929X.2010.492876

To link to this article: http://dx.doi.org/10.1080/0144929X.2010.492876

Behaviour & Information Technology
Vol. 30, No. 3, May–June 2011, 379–388

Taylor & Francis
Taylor & Francis Group

Impact of restrictive composition policy on user password choices

John Campbell*, Wanli Ma and Dale Kleeman

Faculty of Information Sciences and Engineering, University of Canberra, Canberra ACT 2601, Australia

(*Received 31 January 2009; final version received 6 May 2010*)

This study investigates the efficacy of using a restrictive password composition policy. 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 restrictive password composition policies actually change user behaviours in significant ways. The results of this study show that a password composition policy reduces the similarity of passwords to dictionary words. However, in this case the regime did not reduce the use of meaningful information in passwords such as names and birth dates, nor did it reduce password recycling.

Keywords: password authentication; password composition policy; computer security

1. Introduction

Although more secure user authentication systems are available (e.g. see Boukhonine *et al*. 2005), password-based authentication remains the most common way to control access to computer-based resources. Passwords remain in widespread use because they are conceptually simple for both system designers and end users, and provide cost effective protection for many systems if used correctly.

Prior studies have identified user behaviour as one of the main risks to the effectiveness of password security measures (Rhodes 2004, Trček *et al*. 2007, Tam *et al*. 2010). For example, users may compromise password security through forgetfulness, by writing or storing passwords in a place where others have access, by openly sharing passwords with others or by selecting passwords composed of easily guessed words. These weaknesses are known to seriously undermine the efficacy of password access systems (Carstens *et al*. 2004, Conklin *et al*. 2004b). The literature emphasises memory constraints as an important factor explaining why users frequently choose weak passwords (Zviran and Haga 1999, Vu *et al*. 2007), and a range of methods have been proposed to assist users to create passwords that are both memorable and difficult to crack (Furnell *et al*. 2000, Irakleous *et al*. 2002, Proctor *et al*. 2002, Furnell *et al*. 2004, Warkentin *et al*. 2004, Renaud and Ramsay 2007).

In practice, the overall security of password authenticated systems is complex and reflects the interplay between user and system level vulnerabilities. Conklin *et al*. (2004a) identified three types of security vulnerabilities in password authenticated systems: (1) brute force attack targeting the logon interface using common dictionary-based words to guess a password, or an offline attack directed against the password hash file; (2) password discovery using scripts, Trojan viruses, key loggers, or system level exploits and (3) social engineering where the user is manipulated to provide password and account information using a variety of means including phishing and spoofed web sites.

The threat of dictionary-based attacks can be substantially reduced by using system controls such as limiting the number of logon attempts or requiring that additional imaged data be keyed. However, significant vulnerabilities remain in relation to offline hash file attacks, password discovery and social engineering. Despite the existence of these more serious vulnerabilities, many organisations remain heavily reliant on password composition policies to force users to select passwords that are more complex and, by inference, less vulnerable to online dictionary-based attack at the system interface level. Apart from failing to address all critical vulnerabilities, there also remains some doubt about the effectiveness of password composition policies to change typical user behaviours associated with password selection. This article investigates whether a restrictive password composition policy actually leads to changed user behaviours.

*Corresponding author. Email: john.campbell@canberra.edu.au

ISSN 0144-929X print/ISSN 1362-3001 online

DOI: 10.1080/0144929X.2010.492876
http://www.informaworld.com

A conceptual model is developed in the following section which is then used to support an experiment of how password composition rules influence user-defined choices.

2. Understanding user password choices

Conceptual models of how users make password choices have largely focused on representations that have assumed some rational decision-making process in how passwords are selected. For example, Zviran and Haga (1999) explored password selection as a rational decision-making trade-off between the sensitivity and importance of the data being protected, and password attributes such as memorability. Their contention was that users selected strong or weak passwords depending upon the importance and sensitivity of the data being protected. Another study by Aytes and Connolly (2004) also employed a rational choice perspective arguing that users adopt a contingency approach to password selection based on their awareness of safe practice, perceptions of the probability of negative consequences of choosing a weak password and the potential severity of these negative consequences.

While proven to be useful, the rational choice perspective adopted in these earlier studies assumed that users were objective decision-makers able to weigh up all known risks and benefits associated with choosing a weak or strong password. Unfortunately, there is strong evidence that imperfect knowledge and other cognitive limitations constrain the password selection process (Vu *et al*. 2007). Instead, we contend that password selection is an arational process that is influenced by environmental uncertainty, and constrained by both human limitations and organisational attempts (or lack of) to intervene in the selection process. As indicated by the direction of the arrows in Figure 1, these forces combine to influence password strength as manifest in attributes such as password reuse, similarity to dictionary words and use of meaningful information. Rightly or wrongly, these attributes are frequently cited as vulnerabilities that password composition policies are often relied upon to address.

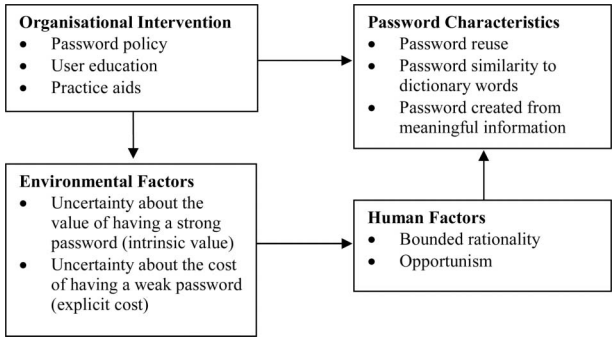


Figure 1. Understanding user password choices in an organisational context.

In Figure 1, human factors reflect the cognitive limitations of humans and their tendency to make opportunistic or self-serving decisions that satisfice rather than optimise outcomes (Simon 1976, Williamson 1985, Rubinstein 1998). This also includes situations where decision-making does not precisely follow a rational analytic process, but contains elements of intuition, bias and emotion (Tversky and Kahneman 1974, Frederick 2002). It is anticipated that cognitive processes associated with selecting a password will embody varying degrees of rational intent, emotion, intuition and personal preference (Kahneman and Frederick 2002). Consequently, there are two important human factors to consider in the password selection process:

(1) *Bounded rationality* – Users have limited information processing capabilities (Miller 1956, Cowan *et al*. 2004) and do not have the resources or cognitive abilities to gather and evaluate all information about existing and future vulnerabilities associated with different password choices and security outcomes. Users also tend to act on intuition and emotion and make choices based on personal preferences or by simply choosing the first alternative that comes to mind (Frederick 2002, Kahneman and Frederick 2002).
(2) *Opportunism* – Users will have a tendency to choose passwords that are convenient and help overcome cognitive limitations such as memory constraints (e.g. passwords that are easy to remember, recycled, self-expressive, etc.). Users can also intentionally abuse organisational computing resources and data (Straub 1990).

The human factors of bounded rationality and opportunism are further exacerbated by two environmental uncertainties:

(1) *Uncertain intrinsic value* – Uncertainty about the potential value from choosing a strong password.
(2) *Uncertain explicit cost* – Uncertainty about the potential cost from selecting a weak password.

While many organisations endeavour to educate users and managers about the costs and benefits of choosing secure passwords (Straub and Welke 1998),

the most common organisational intervention is to implement password composition rules aimed at forcing users to select strong passwords (Campbell *et al*. 2007, Vu *et al*. 2007). Password composition rules provide an explicit framework that constrains user choices during the password selection and replacement process. Despite widespread adoption in organisations, very little is known about how password composition rules change user behaviours except that it is difficult for users to create passwords that are both secure and easy to remember (Yan *et al*. 2004).

Our primary research objective is to assess the efficacy of restrictive password composition rules in forcing users to choose passwords that are more secure and, in so doing, also develop an understanding of the practices users embody in the password creation process that facilitate password recall – particularly password recycling, and the use of dictionary words and other meaningful information.

3. The efficacy of password composition rules

The objective of password composition rules is to reduce the probability of a system intrusion by proactively preventing users from creating passwords that are easy to guess or that have similarities to common dictionary words (Piscitello and Kent 2003). In terms of our research focus, we therefore seek to evaluate the impact of password composition rules on three well-known and measurable weaknesses in user-defined passwords: similarity to dictionary words, the use of other meaningful information and password reuse.

3.1. Password similarity with dictionary words

Passwords that contain common dictionary words can sometimes be cracked within minutes and even seconds. We have estimated that a modest desktop computer (Intel Pentium 4, 2.4 GHz) running the Fedora Core 5 operating system can complete a password encryption function in about 10 microseconds creating the capacity to test up to 10^5 passwords in 1 s (based on crypt(3) which is widely used for Un*x password encryption). As there are 479,625 words in the Fedora Core 5 English spell-checking dictionary, a comparison against this word list will take approximately 5 s. Consequently, the paramount objective of enforcing password composition rules is to ensure that users create passwords that offer protection against dictionary-based attack. Therefore, we test the following proposition:

> P1: The enforcement of password composition rules will produce passwords that are less similar to dictionary words.

3.2. Passwords containing meaningful information

There are many operating system 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. (Microsoft 2009). In most cases, it is generally assumed that the enforcement of password composition rules will lead to the creation of passwords that are more secure. Surprisingly there is little research evidence to support this assumption. However, there is evidence that even well structured and documented security policies do not necessarily lead to more secure systems (Foltz *et al*. 2005). The corollary is that restrictions on password composition may not prevent users from compromising system security as they may still choose a password that contains meaningful data or is easily guessed from common word derivations. Nevertheless, as the intention of composition rules is to reduce the use of meaningful information contained in a password, we can test the following proposition:

> P2: The enforcement of password composition rules will reduce the incidence of meaningful information contained in user-defined passwords.

3.3. Password recycling

Due to the prevalence of password authentication systems, many users are required to remember passwords for a range of different systems and applications. Remembering many unique passwords for different systems and applications is difficult in practice and it is therefore no surprise that many users select dictionary words, personal names or other meaningful information as the basis for their passwords simply because these kinds of information have context and are therefore easier to remember. For similar reasons users are reported to 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 impose constraints that lead to the creation of passwords that are less similar to earlier password choices. We test the following proposition:

> P3: The enforcement of password composition rules will reduce password reuse.

4. Research method

This study employed an experimental research design where participants were randomly allocated to one of two main study groups. Each of the study groups was exposed to different password composition regimes: (1) unrestricted password composition (Group A – experimental control group), and (2) restricted password composition (Group B – experimental treatment group).

The research context and password composition task was designed so as to simulate the experience of a password composition exercise for a new employee. Participants were asked to compose a password for a hypothetical work-based computer account using a simple online password interface designed for this purpose. Both groups were provided with a common set of general instructions explaining the context of the experiment and a separate information sheet explaining the rights of participants and other important information about research ethics. Beyond the general instructions, each group was also provided with a set of instructions describing how to access the online password capturing interface, create a password and complete an exit survey.

A common logon and participant consent interface was used for both groups (see Figure 2). However, the password capture application provided customised screens for the two password composition groups. The online password capture interface used for the unrestricted password group is illustrated in Figure 3a, and in Figure 3b for the restricted password group. The application shared a common introductory screen which authenticated the user and their group membership then branched to a second screen for the password composition task. While the unrestricted group had no limitations on password creation, the following rules were enforced for the restricted group:

- Password does not contain all or part of the user's logon code
- Password is at least eight characters long
- Password is not 'password' or a deviation thereof; or left blank
- Password must contain 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.)

The password composition rules enforced on the restricted group were based on what is generally considered to be good password practice (Pfleeger and Pfleeger 2003). The combination of a minimum password length with special characters is frequently cited as a sound basis for the creation of secure user-defined passwords. In reality, it is common for some users to access several different applications requiring passwords (each perhaps with slightly different password composition requirements). However, the experiment examined user behaviour in the context of a single hypothetical password protected computer account for accessing email and other organisational resources. This approach was adopted so as to highlight the potential impact of user practice on organisational systems, and to reduce the potential for confounding effects associated with other types of applications.

The research experiment involved 151 undergraduate student participants studying within a university business faculty. This cohort was sampled so as to provide indicative information on the password composition practice that university educated recruits might bring into a new employment position within an organisation. Students were approached in tutorial classes with each class being randomly allocated to a

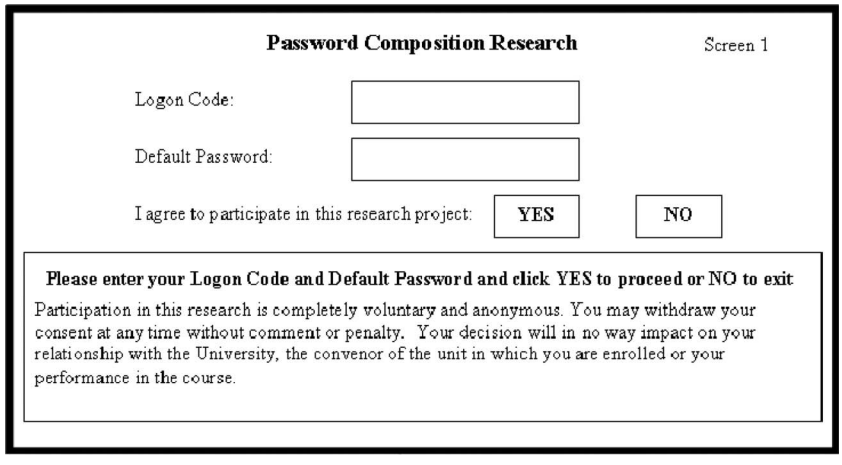
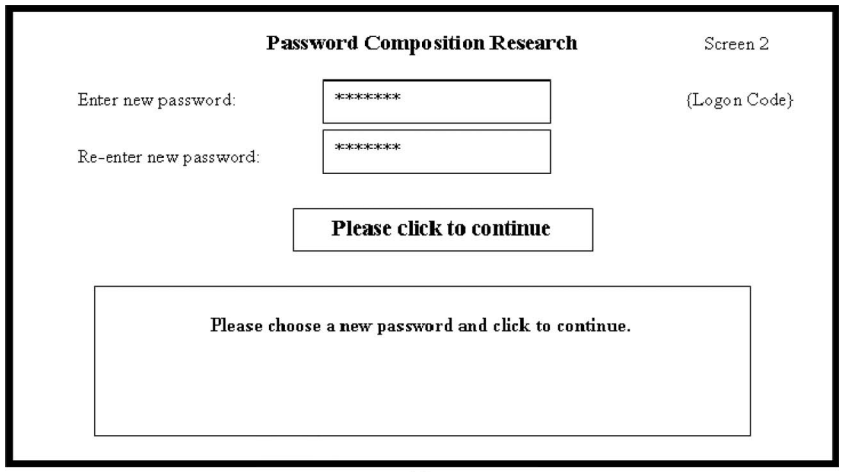
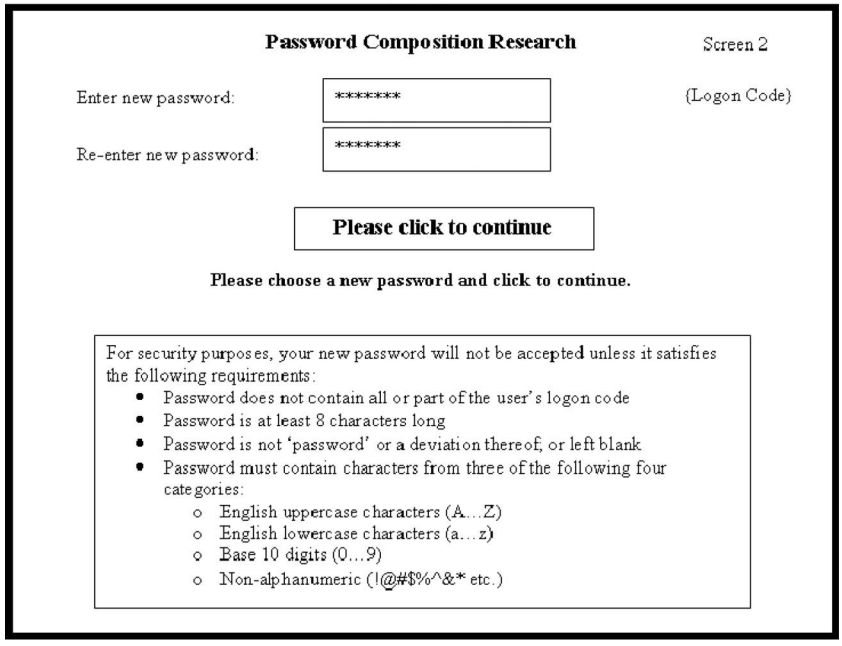


Figure 2. Initial logon and research consent screen common to both experimental groups.



(a)



(b)

Figure 3. (a) Password composition screen for Group A (experimental control group). (b) Password composition screen for Group B (password policy constrained group).

treatment or control group. This resulted in 73 individuals participating in the control group environment (Group A), and 78 individuals participating in the treatment group environment (Group B). After completing the password composition task, participants were also asked to complete a short online exit survey which is described in the Appendix.

5. Results

This section reports the results of tests of the password attributes (1) similarity to dictionary words; (2) meaningful information and (3) password recycling. The results show that password composition rules reduce the likelihood of a successful brute force dictionary-based attack. However, a strict regime did not reduce the use of meaningful data in passwords such as names and birth dates, nor did it reduce password recycling.

5.1. Password similarity to dictionary words

Guessing a password is somewhat different from guessing an ordinary word. It is not a Markov process, where one is able to more accurately guess the next character based on our knowledge of previous characters. Without prior knowledge of the

composition of a password (length and character set used), trying combinations of all possible characters in all possible lengths is very costly. However, a hacker can implement strategies that increase the likelihood of success such as trying common combinations before attempting brute force enumeration of all possible password possibilities. Prior research has shown that many users choose passwords derived from common dictionary words (Bryant and Campbell 2006). Testing for subtle changes to dictionary words, the names of well-known people and places, commonly used phrases, movie titles, etc. fits well with this guessing strategy. In this case a likely process for cracking a password might consist of the following:

(1) Directly test all words in the attack dictionary;
(2) Test 1 and 2 character variations of all words in the attack dictionary;
(3) Enumerate all possible password candidates consisting of a smaller character set (i.e. use only lower case characters or all lower case characters plus digit characters).

One way of measuring password vulnerability to dictionary style attack is to assess the similarity between a password string and common dictionary words using Levenshtein's edit distance (Levenshtein 1965). The edit value is the difference between two strings (in this case a password key and its closest dictionary word) calculated by adding the number of single character insertions and deletions required to make the string values equivalent. To measure how different a password is from all words contained in the base dictionary, we must first check the Levenshtein's edit distance of the password against each word in our dictionary. The calculated measure is the minimum distance between the password and the closest word in the dictionary list.

In our study, the standard Fedora Core 5 English dictionary (Fedora 2009) was used to generate a Levenshtein's edit distance score for each user defined password generated by the participants in the experiment. Although more comprehensive dictionaries would most likely be used for password cracking, this dictionary is adequate for the purpose of demonstrating the differences between the treatment and control groups. Table 1 shows the distribution of distance measures for each group. The differences between the experimental control and treatment groups are quite marked. The Levenshtein's edit distances for passwords created by the unrestricted group range from a potentially insecure value of zero through to seven. In contrast, the restricted password composition group created passwords with edit distances ranging from 2 through to a very high value of 10. Statistical testing indicated that the Levenshtein's edit distances are significantly higher ($t = 4.449$, $p = 0.0001$) where the password composition rules were enforced ($M = 4.78$, $SD = 1.79$) in comparison to the unconstrained group ($M = 3.44$, $SD = 1.91$). Therefore, Proposition 1 is supported as the enforcement of password composition rules produced passwords that were less similar to a standard dictionary of words.

As mentioned earlier, it takes around only 5 s to completely test every word in the Fedora dictionary meaning that any password with Levenshtein's edit distance of zero will be cracked within 5 s. If a password has a Levenshtein's edit distance of one, without prior knowledge about the password, a perpetrator has to test every single combination of one edit distance to every word contained in our attack dictionary of 479,625 words. If the character set is restricted to lower case 'a' to 'z' and digit '0' to '9', there are 343×10^6 combinations and it will take approximately 1 h to test these combinations using an Intel Pentium 4, 2.4 GHz computer. For a Levenshtein's edit distance of two, there are 283×10^9 combinations which would require approximately 65 days of testing. Therefore, it is reasonable to presume that a password which has a Levenshtein's edit distance of three and above should be safe from dictionary-based attack.

A closer inspection of the data indicates that a little over 34% of the control group (unrestricted password choice) had a Levenshtein's edit distance of 2 or less while only 9% of the restricted password group had Levenshtein's edit distance value of 2 or less. While this

Table 1. Levenshtein's edit distance calculated for all passwords using the standard Fedora Core 5 dictionary.

	Levenshtein's edit distance										
Experimental condition	0	1	2	3	4	5	6	7	8	9	10
Unrestricted choice ($n = 73$)	5 6.8%	9 12.3%	11 15.1%	9 12.3%	18 24.7%	6 8.2%	14 19.2%	1 1.4%	0	0	0
Restricted choice ($n = 78$)	0	0	7 9.0%	12 15.4%	17 21.8%	18 23.1%	14 17.9%	4 5.1%	3 3.8%	1 1.3%	2 2.6%

Table 2. Types of information reported as being a component of user-defined passwords.

Experimental condition	Meaningful detail	Combination of meaningful detail	Pronounceable password	Passphrase	Random	Other
Unrestricted choice ($n = 73$), missing = 4	28	15	3	2	8	13
	38.4%	20.5%	4.1%	2.7%	11.0%	17.8%
Restricted choice ($n = 78$), missing = 1	21	31	3	1	12	9
	26.9%	39.7%	3.8%	1.3%	15.4%	11.5%

result is an improvement over having no policy at all, a substantial proportion of passwords created under the restrictive regime remain vulnerable and further improvement is required.

5.2. *Passwords containing meaningful information*

In the exit survey, participants were asked whether the password they chose contained meaningful information such as a name or birth year, or whether it was composed using some other approach such as a passphrase, pronounceable phrase or random keyboard characters. Table 2 shows the various approaches used by respondents to compose their passwords. While the incidence of meaningful information contained in passwords created by the restricted group was noticeably less than that for the unrestricted group, the proportion of passwords containing a combination of meaningful detail is much larger. Overall this result is the opposite of the relationship predicted by proposition 2. Clearly the imposition of password composition rules has forced many respondents to choose passwords that are based less on only one kind of meaningful data and more on combinations such as names combined with birth years.

Inferential statistical testing was used to assess Proposition 2. The various response values were recoded with meaningful and combination of meaningful data responses aggregated and all other responses also summed. A subsequent chi-square test established that there was no statistical difference between each group in relation to the use of forms of meaningful data within passwords, χ^2 (1, $N = 150$) = 0.014, $p = 0.906$. Therefore, we conclude that Proposition 2 is not supported and that the enforcement of password composition rules does not reduce the amount of meaningful information contained in user-defined passwords.

5.3. *Password recycling*

Participants were asked whether the password chosen was the same, similar or completely different from one used in the past. Table 3 shows the distribution of responses by participants in each group. Although there were variations in the raw responses, a chi-square test established no statistical difference between each group in relation to password reuse, χ^2 (2, $N = 150$) = 0.04, $p = 0.979$. This result does not support Proposition 3 which stated that the enforcement of restrictive password composition rules will reduce password reuse.

Table 3. Incidence of password reuse for each experimental group.

Experimental condition	Password has been used before	Password is similar to one used before	Password not used before
Unrestricted choice ($n = 73$), missing = 1	20	22	30
	27.4%	30.1%	41.1%
Restricted choice ($n = 78$), missing = 2	14	26	36
	17.9%	33.3%	46.2%

6. Discussion

The motivation for this research was to investigate the impact of a restrictive password composition policy on changing user behaviours. In order to adequately investigate this issue, we developed a conceptual model of user behaviour and then used this model to examine how organisational intervention using restrictive password composition rules might discourage users from recycling passwords and using meaningful information. We also examined the difference between user-defined passwords and common dictionary words.

An analysis using Levenshtein's edit distance showed that the enforcement of restrictive password composition rules resulted in a statistically significant increase in the distance between user-defined passwords and common dictionary words. However, this in itself does not mean that vulnerability to dictionary-based attack diminished. The average Levenshtein's edit distance calculated for the restrictive policy group and the control group (4.78 and 3.44, respectively) suggests that both groups are relatively safe from dictionary-based attack. However, there are a significant number of passwords generated in both study

groups that have low distance measures and, as a result, remain susceptible to this type of attack.

While it appears that restrictive password composition rules improved password strength by encouraging the creation of passwords that are less like dictionary words, the results also showed that a restrictive password composition environment did not discourage the use of meaningful information in passwords. Nor did it reduce the incidence of password reuse with more than 51% of participants in the restrictive policy group reporting that they had chosen passwords containing meaningful or a combination of meaningful information. This finding in itself is not necessarily a security concern as these types of passwords will tend to be more easily remembered and users will be less inclined to write them down for later reference. However, it does show that the enforcement of a restrictive password composition policy was largely ineffective in changing these basic user behaviours.

These findings have important implications for understanding user password choices as expressed in our theoretical model in Figure 1. Organisational interventions that principally rely on the enforcement of password composition rules will not prevent vulnerable password choices. From our findings it appears that the password selection process is more affected by human factors such as bounded rationality and opportunism. However, the model suggests that there are alternative opportunities for organisations to intervene to help users create stronger passwords. These include user education and the development of practice aids that assist users to overcome the common pitfalls associated with bounded rationality. In particular, practice aids may help users identify the benefits of using a secure password; provide memory aids and decision prompts and offer real-time feedback on the relative strength of different password choices. Further research is required to investigate how these mechanisms might work in practice particularly in situations where users have multiple password accounts. As this study has relied on self-reported data under experimental conditions, future research is also required to corroborate these findings under field conditions.

7. Conclusion

Although authentication technologies are constantly evolving, passwords remain the predominate means of user authentication. The findings from this study provide important insight into ongoing issues relating to the management of password systems. While the results highlight some of the benefits of enforcing password composition rules, the overall findings are far from emphatic. The efficacy of a password authentication system is premised on the combined strength of the password generation process and in the management practices adopted by users. While most users understand the importance of choosing a strong password, research has repeatedly demonstrated that complex passwords are difficult to remember and can lead to unsound password management practices. Unfortunately many organisations rely solely on restrictive password composition policies to restrict user behaviours. Our findings suggest that this faith is somewhat misplaced. While restrictive composition rules improved password strength against brute force attack using dictionary words, the policy we tested did little to reduce the use of meaningful information and password recycling.

There is a risk that password composition policies have become historically compelling administrative control measures that create a false sense of security. Our research findings largely discredit the use of these policies by showing that they do not greatly change human behaviour. The evidence from this study indicates that other measures are required to ensure password security and that organisations should not rely on the enforcement of password composition policies.

Our finding creates new opportunities for research into what does and does not work in regard to password security and changing basic human behaviours. Our conceptual model suggests that organisations might effect change by providing education and other technical support to ensure that users are fully informed about the risks and benefits of adopting secure password management practices. At the same time, organisations must remain vigilant against other vulnerabilities including offline attack, password discovery and social engineering. Further research is required to better understand how different password policy environments and other practice aids might improve password security by encouraging more secure user behaviours. The conceptual model developed in this research provides a strong theoretical basis for investigating these issues further.

The participants in this study were undergraduate students whose motivations, actions and password choices may differ markedly from older and more experienced individuals using password protected applications in the workplace. Consequently, the generalisability of our findings must be tested in real world settings using a more representative group of users.

References

Aytes, K. and Connolly, T., 2004. Computer security and risky computer practices: a rational choice perspective. *Journal of Organizational and End-User Computing*, 16 (3), 22–40.

Boukhonine, S., Krotov, V., and Rupert, B., 2005. Future security approaches and biometrics. *Communications of the Association for Information Systems*, 16 (48), 937–966.

Bryant, K. and Campbell, J., 2006. User behaviours associated with password security and management. *Australasian Journal of Information Systems*, 14 (1), 81–100.

Campbell, J., Kleeman, D., and Ma, W., 2007. The good and not so good of enforcing password composition rules. *Information Systems Security*, 16 (1), 2–8.

Carstens, D.S., *et al*., 2004. Evaluation of the human impact of password authentication practices on information security. *Informing Science Journal*, 7 (1), 67–85.

Conklin, A., Dietrich, G., and Walz, D., 2004a. Password-based authentication: a system perspective. *In*: *Proceedings of the 37th Hawaii International Conference on System Sciences*, Hawaii, USA.

Conklin, A., *et al*., 2004b. *Principles of computer security: security + and beyond*. New York, NY: McGraw-Hill.

Cowan, N., Chen, Z., and Rouder, J.N., 2004. Constant capacity in an immediate serial-recall task: a logical sequel to Miller (1956). *Psychological Science*, 15 (9), 634–640.

Fedora, 2009. *Fedora core 5* [online]. Available from: http://docs.fedoraproject.org/release-notes/fc5/release-notes-ISO/ [Accessed 20 January 2009].

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.

Frederick, S., 2002. Automated choice heuristics. *In*: T. Gilovich, D. Griffin, and D. Kahneman, eds. *Heuristics and biases: the psychology of intuitive judgment*. New York, NY: Cambridge University Press, 548–558.

Furnell, S.M., *et al*., 2000. Authentication and supervision: a survey of user attitudes. *Computers & Security*, 19 (6), 529–539.

Furnell, S.M., Papadopoulos, I., and Dowland, P., 2004. A long-term trial of alternative user authentication technologies. *Information Management & Computer Security*, 12 (2), 178–190.

Irakleous, I., *et al*., 2002. An experimental comparison of secret-based user authentication technologies. *Information Management & Computer Security*, 10 (3), 100–108.

Ives, B., Walsh, K.R., and Schneider, H., 2004. The domino effect of password reuse. *Communications of the ACM*, 47 (4), 75–78.

Kahneman, D. and Frederick, S., 2002. Representativeness revisited: attribute substitution in intuitive judgment. *In*: T. Gilovich, D. Griffin, and D. Kahneman, eds. *Heuristics and biases: the psychology of intuitive judgment*. New York, NY: Cambridge University Press, 49–81.

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

Microsoft, 2009. *Forcing strong password usage throughout your organization* [online]. Available form: http://technet.microsoft.com/en-us/library/cc875814.aspx [Accessed 20 January 2009].

Miller, G.A., 1956. The magical number seven, plus or minus two: some limits on our capacity for processing information. *Psychological Review*, 63, 81–97.

Piscitello, D. and Kent, S., 2003. The sad and increasingly deplorable state of internet security. *Business Communications Review*, February, 49–53.

Pfleeger, C.P. and Pfleeger, S.L., 2003. *Security in computing*. 3rd ed. New York, NY: Prentice Hall.

Proctor, R.W., *et al*., 2002. Improving computer security for authentication of users: influence of proactive password restrictions. *Behaviour Research Methods, Instruments & Computers*, 34 (2), 163–169.

Renaud, L. and Ramsay, J., 2007. Now what was that password again? A more flexible way of identifying and authenticating our seniors. *Behaviour & Information Technology*, 26 (4), July–August, 309–322.

Rhodes, K., 2004. Operations security awareness: the mind has no firewall. *Computer Security Journal*, 16 (2), 27–36.

Rubinstein, A., 1998. *Modeling bounded rationality*. Cambridge, MA: MIT Press.

Simon, H.A., 1976. *Administrative behavior: a study of decision-making processes in administrative organization*. 3rd ed. New York, NY: Free Press.

Straub, D., 1990. Discovering and disciplining computer abuse in organizations: a field study. *MIS Quarterly*, 14 (1), 45–57.

Straub, D. and Welke, R., 1998. Coping with systems risk: security planning models for management decision making. *MIS Quarterly*, 22 (4), 441–469.

Tam, L., Glassman, M., and Vandenwauver, M., 2010. The psychology of password management: a tradeoff between security and convenience. *Behaviour & Information Technology*, 29 (3), 233–244.

Trček, D., *et al*., 2007. Information systems security and human behaviour. *Behaviour & Information Technology*, 26 (2), 113–118.

Tversky, A. and Kahneman, D., 1974. Judgment under uncertainty: heuristics and biases. *Science*, 185, 1124–1131.

Vu, K.L., *et al*., 2007. Improving password security and memorability to protect personal and organizational information. *International Journal of Human-Computer Studies*, 65, 744–757.

Warkentin, M., Davis, K., and Bekkering, E., 2004. Introducing the check-off password systems (COPS): an advancement in user authentication methods and information security. *Journal of Organizational and End User Computing*, 16 (3), 41–58.

Williamson, O., 1985. *The economic institution of capitalism*. New York, NY: Free Press.

Yan, J., *et al*., 2004. Password memorability and security: empirical results. *IEEE Security and Privacy*, September/October, 25–30.

Zviran, M. and Haga, W.J., 1999. Password security: an empirical study. *Journal of Management Information Systems*, 15 (4), 161–185.

Appendix. Example exit 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 similarities 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