An Assessment of the Human Factors Affecting the Password Performance of South African Online Consumers

R. Butler and M.J. Butler

Stellenbosch University, South Africa
e-mail: rbutler@sun.ac.za; martin.butler@usb.ac.za

Abstract

User identification and authentication is regarded as the basis of computer security. In spite of many new technologies to assist with authentication, passwords remain central to access control systems in most computer systems. The password practices that online consumers apply have a direct effect on the level of security and are often the target of an array of attacks. Research suggests that passwords breaches are frequently the result of poor user security behaviour. Internationally, poor password behaviour among users is common. The objective of this study was to investigate the password performance of South African online consumers and to understand the factors contributing to poor password performance. A web-based survey was designed to determine online consumers' perceptions of their password-related knowledge, measure their ability to apply safe practices and asses their motivational levels to employ secure practices. Poor password practices among South African online consumers were evident from this study. Using a construct for password performance, this analysis indicated a deficiency in the knowledge, capability and motivation of users. Ignorance, Incompetence and Indifference were apparent as causes for online consumers' poor password behaviour. It is suggested that measures aimed at improving password performance be tailored based on the underlying causes for poor password performance as indicated by this study.

Keywords

Passwords, Password Performance, Security, Human Behaviour

1. Introduction

Almost every person interacts with a computer or computer system on a daily basis. For decades, user identification and authentication has been regarded as the foundation of computer security (Zviran and Haga, 1999:162; Conklin, Dietrich and Walz, 2004:1). According to Adams and Sasse (1999:41) confidentiality is an important aspect of computer security which relies on systems (such as passwords) to identify and authenticate computer users.

Stallings (1995:213) describes the use of a password system as 'the front line of defence against intruders'. The main purpose of a password system is to prevent unauthorized persons from violating a computer system's integrity and validity by gaining unauthorised access. As the use of technology increases, having to identify oneself uniquely by way of a password before being allowed to perform certain actions has become acceptable, understandable and even expected in order to ensure

a secure environment (Weber, Guster, Safonov and Schmidt, 2008:45; Chiasson and Biddle, 2007:1).

Although other user authentication systems such as biometrics (using physical characteristics), Single-Sign-on and One-time-Pin (using device ownership), are evolving, the use of passwords remain a cost effective and efficient method to control access and authenticate computer users (Conklin *et al*. 2004:1; Campbell, Kleeman and Ma, 2007:2; Gehringer, 2002:369; Tam, Glassman and Vandenwauver, 2010:233). In fact, the advent of new technologies like cloud based computing effectively removes the first barrier to access, physical presence, as more computing applications move to the Internet, increasing the importance of secure authentication.

2. Attacks to discover passwords

Computer systems are vulnerable to a wide array of security violations (Florencio and Herley, 2007:657). Zviran and Haga (1999:164) remarks that almost every penetration of a computer system at some stage relies on the attacker's ability to compromise a password. Attacks on passwords can occur at the following levels (Campbell *et al*. 2007:3; Furnell, 2005a:10; Notoatmodjo and Thomborson, 2009:71; Butler, 2007:520; Florencio and Herley, 2007:657):

- At the system-end, where attackers launch technical or brute force attacks to crack or guess the passwords of authorized users.
- Attacks on the communication channel with which passwords are transmitted, by increasingly sophisticated technologies deployed on different layers of the network infrastructure.
- Attacks aimed directly at the user to discover his or her password. Phishing and Social Engineering are increasingly popular methods of deceiving computer users into disclosing their passwords.

Yet, despite these problems relating to password security remaining 'conspicuously unsolved', passwords as a means to identify users and their access rights, whether in isolation or combination, remains the most common method of authentication (Furnell, 2005a:9 and 11; Furnell, Dowland, Illingworth and Reynolds, 2000:529). Passwords that are hacked, cracked or disclosed can be used to gain unauthorised access to systems, and may result in financial losses and fraud.

While technology can provide a level of protection against some of these attacks, the human remains a potential weak link. According to Tam *et al*. (2010:233) even the most sophisticated security systems becomes useless if computer users do not choose and manage their passwords properly. Not selecting and managing passwords with care may make that password more susceptible to potential abuse and misuse (Furnell, 2005a:10).

Since attacks can be aimed at cracking 'weak' passwords as well as gaining access to all ('strong' and 'weak') passwords, it is imperative that proper password practices encompass both (1) the creation and (2) the management of passwords, to control

access to information that could be compromised, altered or even destroyed. Although the practices concerned when creating and managing of passwords are interdependent, they are for the purposes of this study viewed as distinct, yet sharing certain actions.

3. Physiological determinants of performance

User behaviour concerning passwords has a direct effect on the level of security of a computer system (Gehringer 2002:369). While certain password users may be proficient in their password practices, proper security measures and guidelines are often 'unknown, neglected, or avoided' by other computer users (Notoatmodjo and Thomborson, 2009:71). Researchers (Pfleeger and Caputo, 2012; Anderson and Agarwal, 2010) suggest a greater understanding of the behaviour of users to prevent them from being the 'weakest link' concerning password security.

Users differ in their password performance as their behaviour is influenced by a number of aspects (McCloy, Campbell and Cudeck, 1994:493). According to Heider (1958), as cited by Anderson and Butzin (1974:598), an individual's performance in a particular task is a function of the individual's ability and motivation relating to that task:

$$\text{Performance} = \text{Ability} \times \text{Motivation}$$

Ability refers to the knowledge, skills and competencies that enable a human to perform a particular task. It is associated with what people know and think, what they can do and how they behave because of how they feel. Aspects that can influence a user's ability include their personality, prior education, previous experience, etc. (McCloy *et al*. 1994:494). Motivation refers to the underlying drive behind a user's particular behaviour in performing that task. The user's desire to extend effort, the intensity of the effort, as well as the user's commitment in extending effort, all impact motivation (McCloy *et al*. 1994:494).

Heider's function for performance was refined by McCloy *et al*. (1994) who found that performance (PC) is a function of the knowledge of facts, rules, principles and procedures (declarative knowledge - DK) relating to a task, the user's capability when his/her knowledge has been successfully combined with knowing how and being able to perform that task (procedural knowledge and skills – PKS) and motivation (M).

$$PC = f(DK, PKS, M)$$

4. Password performance model

Based on the function for an individual's performance in a task, the determinants of a user's password performance can be defined as the following (refer to Figure 1):

- **Knowledge**: the user's knowledge and education relating to password practices;

- **Capability**: the user's competence to successfully combine password-related knowledge with knowing how and being able to apply proper password practices.
- **Motivation**: the underlying desire behind the user's password behaviour.

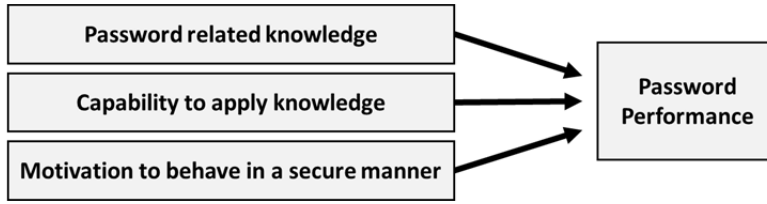

Figure 1: Password performance model

This construct for the determinants of password performance represents an opportunity to deconstruct poor password performance in a way different than most research to date. If the reasons why users do not apply proper password practices are known, then appropriate methods aimed at addressing the underlying causes for poor password behaviour can be designed and implemented to improve password security.

5. Research problem and objective

Accepting that poor password performance is common among computer users, it is not known whether all three determinants of password performance (as indicated in Figure 1) are problematic within the South African context. It is also unknown if measures aimed at improving password security are sufficient to address the particular underlying cause(s) of poor password performance that may be present among users. In order to improve password security it is necessary that any problematic areas first be identified. Any such areas can then form the essence of further research, as well as mitigation measures, to improve password security, at the very least, within the South African context.

The objective of this study was to:

1. Determine the password practices applied by South African online consumers.
2. Analyse poor password practices according to the determinants of password performance – i.e. Knowledge, Capability and Motivation.
3. Comment on known mitigation practices' ability to address the underlying causes for poor password performance and guide future research.

6. Methodology

The research instrument was a survey that contained 43 questions, both structured and open-ended. It was designed and refined via two iterations of pilot testing. In order to put users who might fear that they may be required to share potentially sensitive information at ease, care was taken to ensure respondents that their

passwords would not be asked, and that the purpose of the study was to merely gather information on the practices that users apply.

The survey contained questions to determine the following three aspects:

- Knowledge: A self-assessment of respondents' perceived knowledge relating to password creation and management.
- Capability: The password creation and management practices that respondents apply. The survey also contained a section where users were provided with a number of passwords and had to distinguish between more and less secure passwords. The strength of the passwords provided was tested against various password strength meters.
- Motivation: Based on the responses it was determined whether convenience or security was the more predominant concern to users when they create and manage passwords.

The survey was distributed via email to a database of online South African users from the authors' tertiary institution as well as via snowball method by the researchers. Users' perceptions about their password practices' knowledge and application as well as motivation were analysed. Based on the perceptions and practices applied a score was calculated for each respondents' Knowledge, Capability and Motivation. Although a 100% (absolute) score in each area would represent perfect password performance a cut-off point of 70% was deemed sufficient, and used for analysis.

7. Data analyses

The responses was analysed to determine the levels of Knowledge, Capability and Motivation, independently for each respondent. Figure 2 provides a frequency distribution of the analyses.

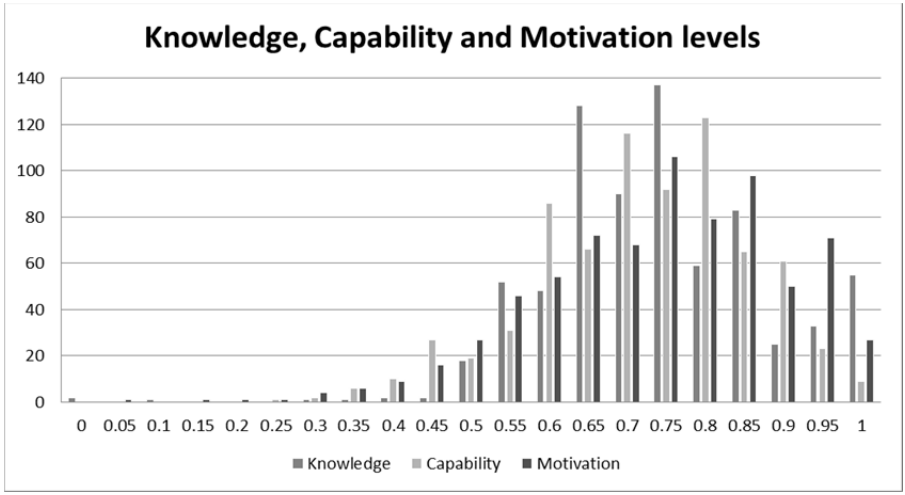

Figure 2: Knowledge, Capability and Motivation levels of respondents

When analysing the Knowledge, Capability and Motivation of the 737 respondents, 55 respondents (7,5%) perceived that they possess absolute knowledge of password practices. However, a mere 9 respondents (1,2%) demonstrated flawless capability to apply proper password practices and only 27 (3,7%) displayed a perfect 'security first' aptitude when selecting and managing passwords.

The poor password performance indicated in this study is no different from previous studies. However, it is suggested that there are three factors that contribute to these practices. The factors, based on the determinants of performance (in Figure 1) and the data analysis (Figure 2) are:

- Lack of password-related knowledge, i.e. **Ignorance**;
- Lack of capability to apply proper password practices, i.e. **Incompetence**; and
- Lack of motivation to apply secure practices, i.e. **Indifference**.

A comparison between the percentages of respondents that were knowledgeable, capable and security-motivated, as opposed to those that were not, is depicted in Figure 3. The analysis indicates the presence of all three factors contributing to poor password behaviour amongst the respondents. Although the motivation levels are slightly better than those for knowledge and capability, all three factors remain problematic and are thus drivers of poor password performance among South African online consumers.

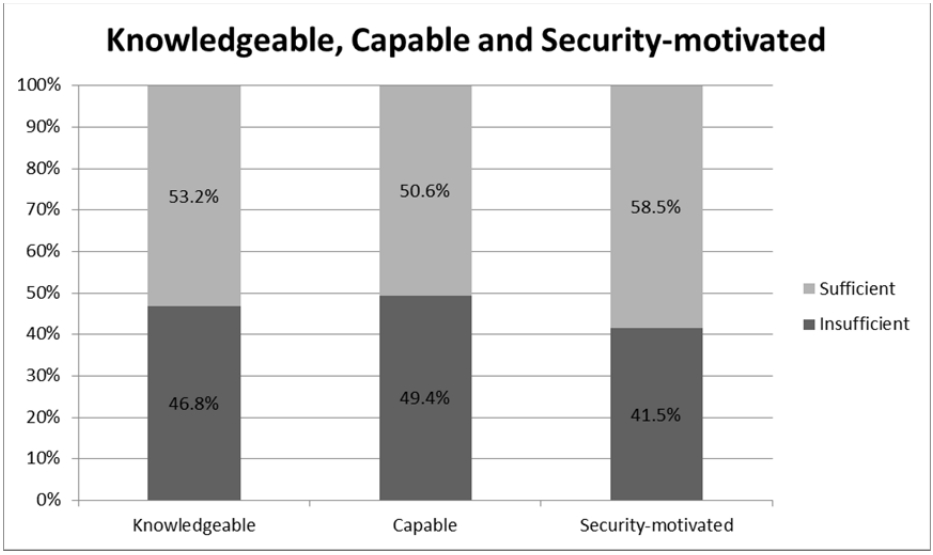

Figure 3: Respondent performance on determinant of behaviour

Although many technological mitigation measures, such as enforcing password complexity and imposing regular password changes, have been proposed to address poor password practices, the authors are interested to see if existing mitigation actions focus on the human aspects that were shown by this study to be the underlying causes for poor password performance. As deficiencies in all three determinants of password performance are evident it is essential that all three areas be addressed to improve password security.

8. Findings and discussion

8.1. Knowledge vs Ignorance

Furnell (2007:445) remarks that one of the reasons why many computer users do not apply safe password practices is because 'they may not know any better' due to a lack of appropriate knowledge, guidance and support. This was confirmed by Adams and Sasse (1999:42), who found inadequate knowledge of what constitutes secure passwords among users and as a result users tend to 'make up their own rules'. Various researchers (Riley, 2006; Conklin *et al*. 2004:5; Adams and Sasse, 1999:43 and 46; Butler, 2007:250) have found that users lack knowledge of proper password practices, security risks, users' vulnerability and possible consequences. Due to their ignorance these users apply poor password practices and/or engage in more risky behaviour.

The survey results regarding respondents' Knowledge indicate that 47% of the respondents were 'ignorant' as they perceived their knowledge of password practices as insufficient. Only 35% of the respondents indicated that they 'knew exactly' what

a strong password is. Insufficient knowledge was also indicated in an open-ended question which asked respondents about any matters not specifically addressed in this survey that would potentially make them change their passwords. 128 respondents (17%) indicated that completing this survey already had them thinking about changing their password, made them realise that they are applying unsafe password practices, or that they need more information and knowledge on security and safe password practices.

8.2. Capability vs Incompetence

While some computer users may apply poor password practices due to ignorance, studies by Furnell, Bryant and Phippen (2007), Riley (2006), Tam *et al*. (2010) and Wessels and Steenkamp (2007:11) found that although users do possess the knowledge to distinguish between secure and insecure practices, their practical application thereof often lacks, indicating an incompetence among these users.

Nine questions in the survey required respondents to assess the strength of various passwords. Only 85 respondents (11%) were able to rank the strength of all of the passwords correctly. When compared with the 35% of respondents who indicated that they 'knew exactly' what a strong password was, it is clear that users may not be capable to apply their knowledge on password practices. In analysing practices it transpired that 49% of the respondents' practiced poor password behaviour, as opposed to 28% and 29% of the respondents who respectively felt that they possessed the necessary knowledge to apply proper password creation and management practices. Weak practices indicated include insecure practices in the composition of passwords, not selecting unique passwords for all accounts and purposes, re-using past passwords or variations thereof, using passwords simultaneously for more than one site, sharing passwords and not regularly changing passwords.

Possible reasons for respondents' incapability to apply proper password practices may be that users overestimate their perceived knowledge regarding password practices due to a phenomenon known as optimistic bias (Weinstein, 1980:806). Optimistic bias may lead password users to overestimate their ability to create 'strong' passwords that are properly managed and protected, and/or underestimate the potential risk associated with compromised passwords.

8.3. Motivation vs Indifference

The first step towards a proper password system is selecting 'strong' passwords (Stallings, 1995:218) that are hard to guess (secure) but still memorable (convenient) (Conklin *et al*. 2004:5). However, Yan, Blackwell, Anderson and Grant (2004:25) found that users rarely choose passwords that are both hard to guess and easy to remember as they are confronted with a 'security-convenience trade-off' (Tam *et al*. 2010:242). In addition users often perceive security measures as 'obstacles' and secondary to the primary task that they are trying to achieve, resulting in users who 'ignore or even subvert the security' (Pfleeger and Caputo, 2012:602). Studies have

indicated that this conflict between convenience and the security of passwords may be present despite users' knowledge of proper password practices (Brown, Bracken, Zoccoli and Douglas, 2004:650; Carstens, McCauley-Bell, Malone and DeMara, 2004:68; Weber *et al*. 2008:46).

Other factors that intensify the strain on users' memories are the increasing number of password-protected systems, enforced password lifetime and composition rules and human memory limitations (Conklin *et al*. 2004:3; Carstens *et al*. 2004:68; Furnell, 2005a:10). Notoatmodjo and Thomborson (2009:71) refer to computer users suffering from 'password overload' and suggest that password overload is a major contributor to unsafe password practices. To deal with this memory issue users began developing their own methods to remember their passwords. When the security motivation is secondary to convenience it leads to weak password practices, which include using short and weak passwords that are easy to remember, sharing passwords, writing down passwords, re-using passwords and not changing passwords regularly (Campbell *et al*. 2007:3; Furnell, 2005a:10; Zviran and Haga, 1999:164-165; Yan *et al*. 2004:25).

The study revealed that 42% of the respondents' Motivation when choosing and managing passwords was convenience rather than security. When creating passwords more users ranked the 'ease of remembering' and passwords that are 'short and easy to enter' more important than the 'strength' of passwords and the 'perceived risk associated with the site' on which the password will be used. When posed with several possible future situations and requiring respondents to indicate which of these will, may or will not lead to a possible change of their passwords, it was also clear that security was not the foremost concern. Indifference, that is a lack of motivation to apply secure practices, is thus an important aspect to address in order to improve users' poor password practices.

9. Addressing poor password performance

An important departure point to address poor password performance is to recognise that proper password security involve both human and technological aspects (Brostoff and Sasse, 2002:41). Yet, technologies incorporated into security systems, although an important part of mitigation, are of little value if users aren't educated or don't understand the measures, risks or consequences associated with poor password practices. To improve password performance one of the most common suggestions made by researchers is the education of computer users through improved security education, training and awareness programs (Riley, 2006; Conklin *et al*. 2004:5; Adams and Sasse, 1999:43 and 46; Butler, 2007:250; Furnell *et al*. 2007:417).

The results of this study indicated a willingness among respondents to improve their password practices if they had more knowledge on password-related matters. In fact, 65,9% of the respondents indicated that they will definitely, and 29,3% may, change their passwords if they realized that their current password was not very secure. In addition an overwhelming 72% of the respondents indicated that they would like to receive a copy of the guidelines for safer online password practices that are to be

compiled and distributed based on this research in an effort to improve their password-related knowledge.

This willingness of users to acquire knowledge suggests an opportunity for those who define the learning outcomes to design a process that addresses all the underlying causes of poor password performance. As literature indicates that training programs do not necessarily address all the issues that should be dealt with (Anderson and Agarwal, 2010:614 and 616-617), education and training programs can thus be improved to take cognisance of the determinants of password performance. Besides sharing knowledge on secure password practices, password vulnerability, threats and consequences of violations, these programs should focus on users' ability to apply these practices as well as address the motivational issues.

According to Pfleeger and Caputo (2012: 597) a key element to improve security is 'acknowledging the importance of human behaviour when designing, building and using cyber security technology'. When the usability by users is neglected by designers of technology it leads to increased pressure on the users to enforce security (Brostoff and Sasse, 2002:41). Researchers (Furnell, 2005b:274; Furnell, Jusoh and Katsabas, 2006:27; Furnell *et al*. 2007:416) recommend improving the usability of security features as users often don't apply these features because they have problems to find, understand and use these security features. Inglesant and Sasse (2010) advise greater emphasis on human computer interface (HCI) principles to increase the usefulness and effectiveness of password security.

10. Conclusion

Passwords, often in combination with others methods, will remain the most common authentication method used by computer systems for the foreseeable future. The human factor associated with password systems is an important consideration to ensure security. This research suggests that the password performance of users is dependent on the user's Knowledge, Capability and Motivation concerning passwords. It is suggested that initiatives to improve password security should address all aspects of poor password performance. Poor password practices among South African online consumers can be improved through greater attention to the human computer interface and relevant education, training and awareness programs.

11. References

Adams, A. and Sasse, M.A. (1999), "Users are not the Enemy", *Communications of the ACM*, Vol. 42, No. 12, pp40-46, December.

Anderson, C.L. and Agarwal, R. (2010), "Practising Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions", *MIS Quarterly*, Vol. 34, No. 3, pp613-643, September.

Anderson, N.H. and Butzin, C.A. (1974), "Performance = Motivation X Ability: An integrated-theoretical analysis", *Journal of Personality and Social Psychology*, Vol. 30, No. 5, pp598-604.

Brostoff, S. and Sasse, M.A. (2002), "Safe and Sound: a Safety-critical approach to security", Proceedings of the New Security Paradigm Workshop 2001, http://hornbeam.cs.ucl.ac.uk/hcs/people/documents/Angela%20Publications/unsorted/p41-brostoff.pdf, (Accessed 10 April 2014).

Brown, A.S., Bracken, E., Zoccoli, S. and Douglas, K. (2004), "Generating and Remembering Passwords", *Applied Cognitive Psychology*, Vol. 18, pp641-651, June.

Butler, R. (2007), "A framework of anti-phishing measures aimed at protecting the online consumer's identity", *The Electronic Library*, Vol. 25, No. 5, pp517-533.

Campbell, J., Kleeman, D. and Ma, W. (2007), "The good and not so good of enforcing passwords composition rules", *Information Systems Security*, Vol. 16, No. 1, pp2-8.

Carstens, D.S., McCauley-Bell, P.R., Malone, L.C. and DeMara, R.F. (2004), "Evaluation of the human impact of password authentication practices on information security", *Informing Science Journal*, Vol. 7, pp67-85.

Chiasson, S. and Biddle, R. (2007), "Issues in User Authentication", CHI Workshop: Security User Studies: methodology and best practices, April.

Conklin, A., Dietrich, G. and Walz, D. (2004), "Password-based Authentication: A System Perspective", Proceedings of the 37th Annual Hawaii International Conference on System Sciences, pp1-10.

Florencio, D. and Herley, C. (2007), "A large-scale study of Web Password Habits", Proceedings of the 16th International Conference on World Wide Web, pp657-666, May.

Furnell, S.M. (2005a), "Authenticating ourselves: will we ever escape the password?", *Network Security*, pp8-13, March.

Furnell, S.M. (2005b), "Why users cannot use security", *Computers and Security*, Vol. 24, pp274-279.

Furnell, S.M. (2007), "An assessment of website password practices", *Computers and Security*, Vol. 26, pp445-451.

Furnell, S.M., Bryant, P. and Phippen, A.D. (2007), "Assessing the security perceptions of personal Internet users", *Computers and Security*, Vol. 26, pp410-417.

Furnell, S.M., Dowland, P.S., Illingworth, H.M. and Reynolds, P.L. (2000), "Authentication and Supervision: A survey of User Attitudes", *Computers and Security*, Vol. 19, pp529-539.

Furnell, S.M., Jusoh, A. and Katsabas, D. (2006), "The challenges of understanding and using security: A survey of end-users", *Computers and Security*, Vol. 25, pp27-35.

Gehringer, E.F. (2002), "Choosing passwords: Security and human factors", *Technology and Society*, pp369-373.

Inglesant, P. and Sasse, M.A. (2010), "The true cost of unusable password policies: password use in the wild", Proceedings of CHI 2010 (ACM Conference on Human Factors in Computing Systems), 10-15 April.

McCloy, R.A., Campbell, J.P. and Cudeck, R. (1994), "A Confirmatory Test of a Model of Performance Determinants", *Journal of Applied Psychology*, Vol. 79, No. 4, pp493-505.

Notoatmodjo, G. and Thomborson, C. (2009), "Passwords and Perceptions", Proceedings of the Australasian Information Security Conference (AISC2009), Wellington, New Zealand, *Conferences in Research and Practice in Information Technology*, Vol. 98, pp71-78.

Pfleeger, S.L. and Caputo, D.D. (2012), "Leveraging Behavioral Science to Mitigate Cyber Security Risk", *Computers & Security*, Vol. 31, No. 4, pp597-611.

Riley, S. (2006), "Password Security: What Users Know and What They Actually Do", *Usability News*, Vol. 8, No. 1, February, http://psychology.wichita.edu/surl/usabilitynews/81/Passwords.asp, (Accessed 19 March 2013).

Stallings, W. (1995), *Network and Internetwork Security Principles and Practice*, Prentice Hall, Englewood Cliffs, New Jersey.

Tam, L., Glassman, M. and Vandenwauver, M. (2010), "The psychology of password management: a tradeoff between security and convenience", *Behaviour and Information Technology*, Vol. 29, No. 3, pp233-244, May-June.

Weber, J.E., Guster, D., Safanov, P. and Schmidt, M.B. (2008), "Weak password security: An empirical study", *Information Security Journal: A Global Perspective*, Vol. 17, No. 1, pp45-54, January.

Weinstein, N.D. (1980), "Unrealistic optimism about future life events", *Journal of Personality and Social Psychology*, Vol. 39, pp806-820.

Wessels, P.L. and Steenkamp, L. (2007), "Assessment of current practices in creating and using passwords as a control mechanism for information access", *South African Journal of Information Management*, Vol. 9, No. 2, June, www.sajim.co.za, (Accessed 15 May 2013).

Yan, J., Blackwell, A., Anderson, R. and Grant, A. (2004), "Password memorability and Security: Empirical results", *Security and Privacy*, IEEE, Vol. 2, No. 5, pp25-31, September-October.

Zviran, M. and Haga, W.J. (1999), "Password security: An empirical study", *Journal of Management Information Systems*, Vol. 15, No. 4, pp161-185.