PASSWORD MANAGEMENT: EMPIRICAL RESULTS FROM A RSA AND USA STUDY

HA Kruger[*], T Steyn[*], L Drevin[*], BD Medlin[#]

[*]School of Computer, Statistical and Mathematical Sciences
North-West University (Potchefstroom Campus)

[#]Computer Information Systems Department
Appalachian State University

[*]Hennie.Kruger@nwu.ac.za, Tjaart.Steyn@nwu.ac.za,
Lynette.Drevin@nwu.ac.za
Private Bag X6001, Potchefstroom, 2520, South Africa
+27 18 299 2531

[#]Medlinbd@appstate.edu
Boone, NC, USA, 28607
828 262 2411

ABSTRACT

“The state of information security as a whole is a disaster, a train wreck”. This view is given by Forte and Power (2007) describing the state of information security towards the end of the first decade of the 21st century. Amongst solutions offered, the view that security programs have to be holistic is proposed indicating that technical controls are of little value without the workforce understanding the risks of their irresponsible behavior. Another solution proposed by them is the role of awareness and education. All levels of users should be targeted letting them understand their role and responsibility in information security. Password related behavior is often highlighted as a key component of information security awareness. However, studies have shown that password hygiene is generally poor amongst users (Stanton, Stam, Mastrangelo, & Jolton, 2005).

In an effort to identify, categorize and prioritize those factors that may have a significant impact on password behavior, a study was conducted amongst students in South Africa and the United States of America to investigate certain aspects of password management practices. The objective of this paper is to report on the empirical results obtained, using techniques such as cause-and-effect diagrams and Pareto analyses.

KEY WORDS

Password management, ICT Security Awareness, Cause-and-Effect diagrams, Pareto analyses.

PASSWORD MANAGEMENT: EMPIRICAL RESULTS FROM A RSA AND USA STUDY

1 INTRODUCTION

Information security has become an important issue in modern organizations. However, not everybody is convinced that information security and the associated measures implemented are producing the expected results. Forte and Power (2007) states that "the state of information security as a whole is a disaster, a train wreck". They argued that technical controls are of little value without the workforce understanding the risks of their irresponsible behavior and advocate that the role of education and awareness programs should receive more attention.

A project to evaluate security awareness levels of staff was initiated in 2005 and consists firstly of an identification phase where key areas, on which measurements can be taken, were identified. Secondly, knowledge, attitude and behavior of staff may be surveyed to determine their awareness levels pertaining to the identified areas. The assessment of appropriate system generated data also forms part of this phase. Finally, the data may then be used to construct a model that may assist in improving the overall information security culture. These phases are described in detail in Kruger, Drevin and Steyn (2006). During the identification phase, the effectiveness of password management has emerged as an issue that should be evaluated. This is in line with the fact that password related behavior is often highlighted as a key component in security programs. However, studies have shown that password behavior is generally poor amongst users (Stanton, Stam, Mastrangelo & Jolton, 2005). The verification of awareness levels that relate to the effective use of passwords would assist in covering some of the main objectives of any security program e.g. the integrity and confidentiality of data.

This paper reports on the use of cause-and-effect diagrams to identify significant causes of poor password management behavior and to assist in the prioritization of the identified causes, Pareto analyses were used. The study was conducted amongst students in South Africa and the United States of America and some comparative results and statistics will be presented.

The remainder of the paper is organized as follows. In the next section the methodology used is briefly presented. Section 3 discusses the results obtained with some concluding remarks in the last section.

2 METHODOLOGY

In this study, the effectiveness of password management was described in terms of two categories – *secure* passwords and *confidentiality* of passwords. Both these categories are defined by different criteria e.g. secure passwords may be defined by password length (Pfleeger and Pfleeger, 2007), how regular passwords are changed (Furnell, 2007), etc., while confidentiality may be defined by criteria such as making passwords available to others – by writing it down or telling someone (Pfleeger and Pfleeger, 2007), the use of different passwords for different systems (Furnell, 2007), etc.

To assist in understanding and identifying problems associated with ineffective password management, two cause-and-effect diagrams were constructed for the two categories. A cause-and-effect diagram is a tool that can be used to represent the relationship between some effect that could be measured and the set of possible causes that produce the effect (Berenson and Levine, 1996). The diagrams are constructed by showing the effect or problem on the right hand side of the diagram and the major causes listed on the left hand side. The causes may also be subdivided into a few major categories depending on the problem under investigation. Following a comprehensive process that included literature surveys, brain storming sessions and pilot studies, a list of 23 causes were identified relevant to secure passwords and the confidentiality of passwords. These causes were grouped into main categories with the help of validation techniques such as content validation, reliability tests and construct validation. The final result was a 5-factor instrument (questionnaire) consisting of 23 items derived from the 23 causes for the two categories studied and was defined as follows:

Secure Passwords	**Confidentiality of Passwords**
Attitude/viewpoint – measured by 3 different items	Attitude/viewpoint – measured by 3 different items
Knowledge and Resources – measured by 4 different items	Knowledge and Resources – measured by 3 different items
Expectation and Feedback – measured by 2 different items	Expectation and Feedback – measured by 2 different items
Skills – measured by 1 item	Knowledge related behavior – measured by 1 item
Own perception of behavior – measured by 2 different items	Own perception of behavior – measured by 2 different items

The complete process covering the construction of the cause-and-effect diagrams, the development of the measuring instrument and reliability test results can be found in Kruger, Drevin and Steyn (2008).

3 APPLICATION AND RESULTS

Using the measuring instrument described in section 2, an empirical experiment was conducted at two universities, one in South Africa and the other in the USA, to see how students apply password management principles. A significant user base of students exists at universities and there are a large number of confidential and privacy security issues associated with student users that can directly be linked to passwords and the management of passwords. As with other users, students should be prohibited from accessing systems where test and examination marks can be changed; test and examination papers can be accessed before student assessments take place; or, where fraudulent actions such as altering of financial data can be done. By not keeping a password confidential or making use of passwords that can easily be guessed, considerable financial losses can be incurred by students e.g. when somebody else uses the password to download large files from the Internet. Irregularities during examinations and tests that are done on computers are also likely when students can access other students' work. Apart from the usual dishonest behavior that should be avoided, it seems to be appropriate to assess the password management knowledge and attitude of young people. They are the business and ICT leaders of the future and should be made aware of the risks and consequences of poor password management.

A simple web application was used to make the questionnaire available to students at the two universities. Although a total of 507 responses were received it was decided to use only those with the field of study in natural sciences and economic and management sciences. In addition, only students in their 3rd year of study or higher were considered. The reason for this selection was to try and ensure that a homogeneous group of students are used to compare the results between the two universities. The final comparison was therefore performed on 193 responses of which 93 were from the South African university and 100 from the university in the USA.

The final results were presented as Pareto charts. A Pareto chart or diagram is a graphical representation in the form of a bar graph that is used to arrange information in such a way that priorities and relative importance of data can be established. It is often used by managers to direct efforts to the biggest improvement opportunity by highlighting the vital few causes in contrast to the trivial many (Pareto diagram, 2007). The charts are constructed by arranging the bars in decreasing order from left to right along the x-axis. Cumulative percentages are then used to assist in analyzing the chart.

Figure 1 contains the Pareto charts for the two universities for the main factors relevant to secure passwords, while figure 2 presents the charts for the confidentiality of passwords. It can be seen from figure 1 that the order of the main factors relevant to secure passwords, is the same for both universities with the factor *Expectation and Feedback* the most significant. This factor was measured by two items – *secure passwords are not compulsory* and *secure passwords are not important*. Looking at figure 2, it is clear that *Expectation and Feedback* – measured by *confidentiality of passwords is not compulsory* and *confidentiality of passwords is not important* is once again the biggest concern when dealing with confidentiality of passwords. Based on this it must be accepted that the current message (feedback) that students, at both universities, receive from management, lecturers, their environment, their peers, etc. is that the use of secure passwords as well as the confidentiality of passwords are not really important and also not compulsory – it is not really expected from them to use secure passwords or to keep their passwords confidential and compliance of this will not be verified.

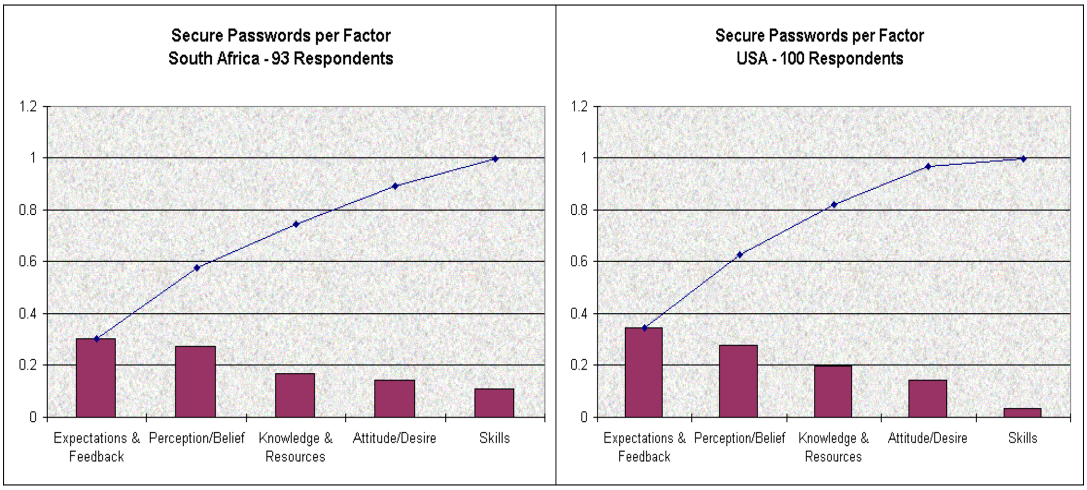

Figure 1 – Pareto charts for secure passwords

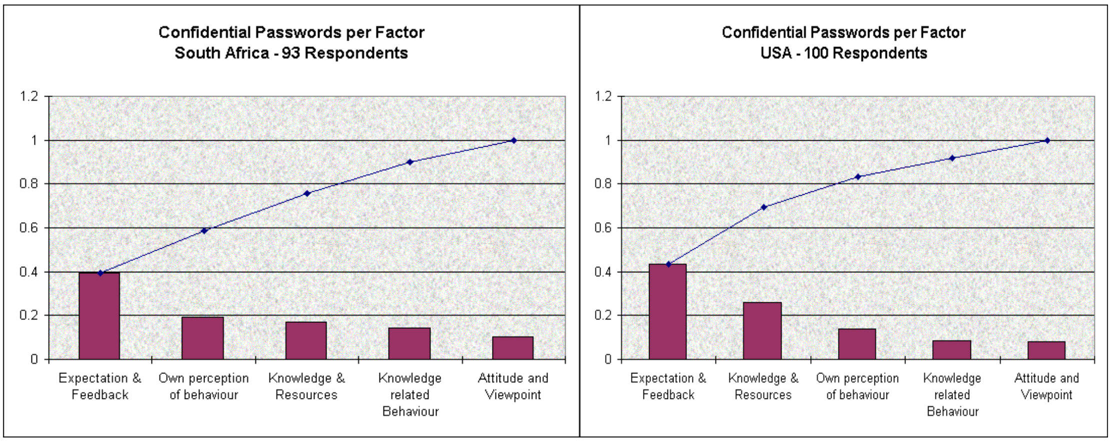

Figure 2 – Pareto charts for confidential passwords

It should also be noted from the Pareto charts that by addressing only the first factor (Expectations and Feedback) about 40% of problems related to confidentiality of passwords at both universities can be solved. In the case of secure passwords, more than 30% of problems at the two universities can be solved. These facts from the Pareto charts create a perfect opportunity for management to address specific password management issues instead of implementing, for example, a comprehensive and expensive awareness program. Each one of the factors, and the items related to them, was analyzed in a similar way but are not presented here.

Two other interesting observations based on the responses suggest that in some cases students believe that they are complying with good password management principles but their behavior may indicate differently. In the first instance, one of the questions explicitly asked respondents whether they belief that the passwords they are using are secure passwords. Almost half of the respondents (46%) in South Africa stated that they use secure passwords. When checking their passwords and applying two basic rules concerning password length and the use of different character sets, it was found however, that 63% of those who said that they are using secure passwords have passwords with 6, or less, characters or make use of only one character set. At the university in the USA, the figure was much lower at 14% who said that they use secure passwords of which 29% had weak passwords when measured against the same two rules. Another concern when looking at these statistics is that 54% of students at the South African university and an alarming 86% of students at the university in the USA stated (admit) that they do not use secure passwords.

Secondly, another question asked respondents whether they believe that they are keeping their passwords confidential. At the South African university 76% answered that they do keep their password confidential but 15% of the same students also indicated that they would make their passwords available to others when needed. At the university in the USA 77% said that they keep their passwords confidential and only 5% of them would give their passwords to somebody else. These two findings are in line with a similar result described by Albrechtsen (2007). According to Albrechtsen's study users stated that although information security is important, they are not always able to point out practical security actions with which they contribute to information security – basically they are not aware of what they could or should do. This is probably true in this case as well. Students may view passwords as an important issue and they may believe that they are using secure passwords but they are not always aware of the practical requirements such as password length.

Table 1 lists some other interesting issues when analyzing each factor and is based on the frequency of answers received from students.

Table 1 – Additional findings

	Universities	
Item	**South Africa**	**USA**
I use simple passwords so that it can easily be remembered	55% admit that they use simple passwords	50% admit that they use simple passwords
I know where to get help or information regarding *secure* passwords	37% do not know where to get help	61% do not know where to get help
I know where to get help or information regarding the *confidentiality* of passwords	41% do not know where to get help	61% do not know where to get help
I can define (or explain) the concept "confidentiality of passwords"	15% admit that they cannot explain the concept	33% admit that they cannot explain the concept

In general the overall results revealed the following. The most significant issues, according to the Pareto charts, and to which students should be made aware of include aspects such as:

- Proper use of passwords which include the use of secure passwords and keeping passwords confidential *is compulsory*.
- Passwords are an extremely *important* aspect of ICT security and improper use will degrade the quality of security and increase the probability of a number of security risks.
- The use of simple passwords that can easily be remembered is not acceptable.
- Making passwords available to other people is not allowed.

- Where to get help or information on proper password principles.

Addressing these few simple principles would solve on average more than 60% of the problems related to effective password management. The remaining factors and their associated items can be evaluated in the same manner and simultaneously, or in a follow-up exercise, be addressed. On the positive side of the scale it appears as if students have the necessary skills e.g. they know where and how to physically change passwords; they generally have a positive attitude or viewpoint towards effective password management e.g. they think that it is worthwhile to use secure and confidential passwords and they do not claim that they are too busy to concern themselves with secure and confidential passwords. They also agree in general that passwords should be kept confidential.

4 CONCLUSION

This paper presented a study where cause-and-effect diagrams were used to assist in evaluating password management practices amongst students at two universities – one in South Africa and the other in the USA. Pareto analyses were then used to identify and prioritize significant aspects. Results indicated that students at both universities do not regard the use of secure passwords, or keeping their passwords confidential, as an important aspect; they did not experience it as being compulsory; and, most of them would use simple passwords that can easily be remembered.

The use of cause-and-effect diagrams and the Pareto analyses proved to be extremely helpful in understanding and gaining insight into those factors that have a significant impact on the effectiveness of password management. Results obtained also created an opportunity for directed security awareness programs where efforts can be focused on specific important issues instead of conducting the usual comprehensive programs where aspects that may not be significant are also addressed.

5 ACKNOWLEDGEMENT

This paper is based upon work that is financially supported by the National Research Foundation (NRF). The opinions expressed in this paper are those of the authors.

6 REFERENCES

Albrechtsen, E. 2007. A qualitative study of users' view on information security. *Computers & Security*, 26:276-289.

Berenson, M.L. & Levine, D.M. 1996. *Basic Business Statistics. Concepts and Applications.* Sixth edition. Upper Saddle River, NJ: Prentice Hall.

Forte, D. & Power, R. 2007. The state of information security towards the close of the first decade of the 21st century. *Computer Fraud & Security*, October, 2007.

Furnell, S. 2007. An assessment of website password practices. *Computers & Security*, 26:445-451.

Kruger, H.A., Drevin, L. & Steyn, T. 2006. A framework for evaluating ICT security awareness, *In: Proceedings of the 2006 ISSA Conference, Johannesburg, South Africa,* 5-7 July 2006 (on CD).

Kruger, H.A., Drevin, L. & Steyn, T. 2008. Password management assessment. Technical Report. North-West University, South Africa, FABWI-N-RKW:2008-222**.**

Pareto Diagram. 2007. [Web:] http://mot.vuse.vanderbilt.edu/mt322/Pareto.htm [Date of use: July 2007].

Pfleeger, C.P. & Pfleeger, S.L. 2007. *Security in Computing.* Fourth edition. Prentice Hall.

Stanton, J.M., Stam, K.R., Mastrangelo, P. & Jolton, J. 2005. Analysis of end user security behaviors. *Computers & Security*, 24(2):124-133.