Determinants of Password Security: Some Educational Aspects

Lynette Drevin, Hennie Kruger, Tjaart Steyn

Determinants of password security: some educational aspects

Lynette Drevin[1], **Hennie Kruger**[2], **Tjaart Steyn**[3]

Computer Science & Information Systems
North-West University, Private Bag X6001, Potchefstroom, 2520
South Africa
[1] ldrevin@acm.org, [2] Hennie.Kruger@nwu.ac.za, [3] Tjaart.Steyn@nwu.ac.za

Abstract: Development and integration of technology give organisations the opportunity to be globally competitive. However, the potential misuse of Information Technology (IT) is a reality that has to be dealt with by management, individuals and information security professionals. Numerous threats have emerged over time in the networked world, but so have the ways of alleviating these risks. However, security problems are still imminent – as highlighted by the plethora of media articles and research efforts. The insider risk is stated as being around 80% of security threats [1] in a company. With this statistic in mind, management has to plan how to allocate resources to counteract the risks. Very often, simple measures such as good password behaviour are overlooked or not rated high enough to include in all security awareness programmes. This paper will focus on a study that assesses password management of future IT professionals. It will be demonstrated how management and educators can use these results to focus their efforts in order to improve users' password practices and thereby enhancing overall IT security.

Keywords: Password management, ICT security awareness, Pareto analysis, cause-and-effect diagrams, password strength and confidentiality

1 Introduction

With the increased usage of information systems and e-business, it has become important to protect information against a wide variety of threats, such as social engineering attacks leading to phishing and identity theft, viruses, spyware, and denial-of-service attacks. There are users in the networked world who are adequately protected, but many individuals are novice users who are ignorant or simply unaware of these vulnerabilities. They spend hours online on social network groups, online banking applications and other systems. Businesses have also changed work practices. Many e-applications are currently in use, such as e-

commerce, e-government and e-health. With the use of these and other applications, the previously mentioned risks also pose challenges to the management of organisations that need to allocate budgets to every aspect of business – including the protection of information resources. Information security includes not only technology solutions but also people [2]. One of the most basic and important aspects of protecting access to applications and information is authentication. Users, employees, and management are all subjected to authentication processes to restrict access to authorised persons only. There are different ways to authenticate users, such as the use of a physical token (e.g. something you have), secret knowledge (e.g. something you know), or biometrics (e.g. something you are) [3]. Commonly used is the mechanism of passwords. Studies have shown that the behaviour of users in this regard is not always of a high standard; therefore, the quality of password security is impeded [4], [5]. Users should be made aware of what good password behaviour entails, how to manage their passwords and what the related risks are.

One could argue that the last word has been said about password management, as much has been published on password usage and behaviour. However, it remains highly topical, as can be seen in recent research publications. Examples include graphical passwords [5], social practice of passwords [6] and improvement of passwords through persuasion [7].

Bearing in mind the increase in the number of information users and online applications and the resulting risks, a study was undertaken to provide some insight into the determinants that may impact the standard of password management and behaviour of users. In this study, a measuring instrument was developed and certain techniques applied in order to identify and prioritise important factors when assessing future IT users' perspectives on password usage.

The important password management determinants that emerge from this study will allow management and educators to expend their efforts in order to improve password practices. The remainder of the paper is organised as follows: In section 2, the background to the exercise is given. Section 3 discusses the methodology used. Section 4 details the results of the study, and section 5 presents some concluding remarks.

2 Background

This study stems from a framework developed during 2006 to evaluate ICT security awareness levels [8]. One of the key areas identified in this framework was the acquiring of appropriate data that could be useful to evaluate knowledge and behaviour of users. Password-related information was part of the required data. It was decided to focus this study on evaluating password management and behaviour of students who are the future IT users and IT business leaders.

The literature gives numerous examples of good password practices [4], [3], [9]. Studies to improve authentication through the use of passwords are also in abundance and guidelines are given to address password insecurities [10], [5], [6].

Users from all backgrounds and educational levels use IT and online applications; therefore, the advice given in literature on how to increase password efficiency can be applied by all. As mentioned, this study focuses on students in a university environment and on the assessment of their password practices. Universities are managed and operated these days in much the same way as other businesses, although their main activities are education and research. They also rely heavily on ICT resources and should therefore be secured so as to adhere to the confidentiality, integrity and availability principles. Student users are given access to systems and applications mainly via user accounts and passwords. They are restricted to their own systems and networked areas and should not have access to university systems containing marks, examination papers, financial data, etc. Failing to keep passwords confidential and making use of passwords that can easily be guessed could result in considerable financial losses and/or examination irregularities. Apart from the usual dishonest behaviour that should be avoided, it seems appropriate to assess the password behaviour and attitudes of young people. They are the IT users and ICT professionals of tomorrow and should be educated about threats and consequences of inadequate password practices.

We viewed effective password management in terms of two categories – *strong or secure* passwords and *confidentiality* of passwords. It is assumed that these two aspects define "good" and "poor" password practices. The two categories were derived from existing literature that provides guidelines on the use of passwords [4], [12].

Strong or secure passwords include principles such as:

- Choose long passwords
- Change passwords often
- Avoid names or dictionary words

Confidentiality of passwords includes principles such as:

- Do not write them down
- Do not use the same password for all applications
- Do not tell anyone your passwords

To comprehend ineffective password management of users, cause-and-effect diagrams were constructed. Also known as an Ishikawa diagram or a fishbone diagram, a cause-and-effect diagram can be used to represent the relationship between some effect that could be measured and the set of possible causes that produce the effect [11]. The effect or problem is shown on the right-hand side of the diagram and the main causes are listed on the left. The causes can be further divided into a few major categories, depending on the problem at hand. Within each major category, specific causes can be listed as branches or sub-branches. These diagrams are useful when it is necessary to understand processes or to

identify core causes of problems. The construction of the cause-and-effect diagrams was guided by the following two questions:

- "What is causing the ineffective password management of students?"
- "What factors affect the ineffective password management of students?"

The next section describes the methodology used, i.e. how the cause-and-effect diagram and the measuring instrument were developed.

3 Methodology used

3.1 Cause-and-effect diagram

It was assumed that the effectiveness of password management is influenced by two main factors, namely *strong* passwords and *confidentiality* of passwords. Two cause-and-effect diagrams were constructed for these two factors, using the following two problem statements: *"Strong passwords are not used"* and *"Passwords are not kept confidential"*.

In order to establish the causes of the problems, the argument of Dark [2] was used, where human performance is described as a function of ability and motivation. This assumption provided a framework of categories that was used in the diagrams. The final cause-and-effect diagrams were developed using research strategies such as brainstorming sessions by the research team, validation against appropriate literature [4], [3], [12] and the use of pilot studies. Figure 1 shows the final cause-and-effect diagram for the confidential password problem [13].

3.2 Development and validation of the instrument

The construction of the cause-and-effect diagrams was followed by a data gathering process to determine the significant causes that impact the problem. This was done by converting causes identified on the two diagrams into a questionnaire. The objective was to test and empirically validate the factors that may influence the effectiveness of password management. A list of 23 causes was identified as relevant to secure passwords and the confidentiality of passwords. These causes were then 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 [13]. The secure/strong aspect was tested by 12 items, and the confidentiality dimension by 11 items.

In order to distribute the questionnaire, a web application was used to reach the students and to capture responses. The next section presents the results.

4 Results

The experiment was conducted at a South African university with three campuses located in three different cities – one of which was selected for the exercise. The campus has a well equipped ICT infrastructure and the students are linked to a central network that gives access to all the necessary applications that they need for their studies. Apart from a compulsory computer literacy module, no official security awareness programme is offered to the students.

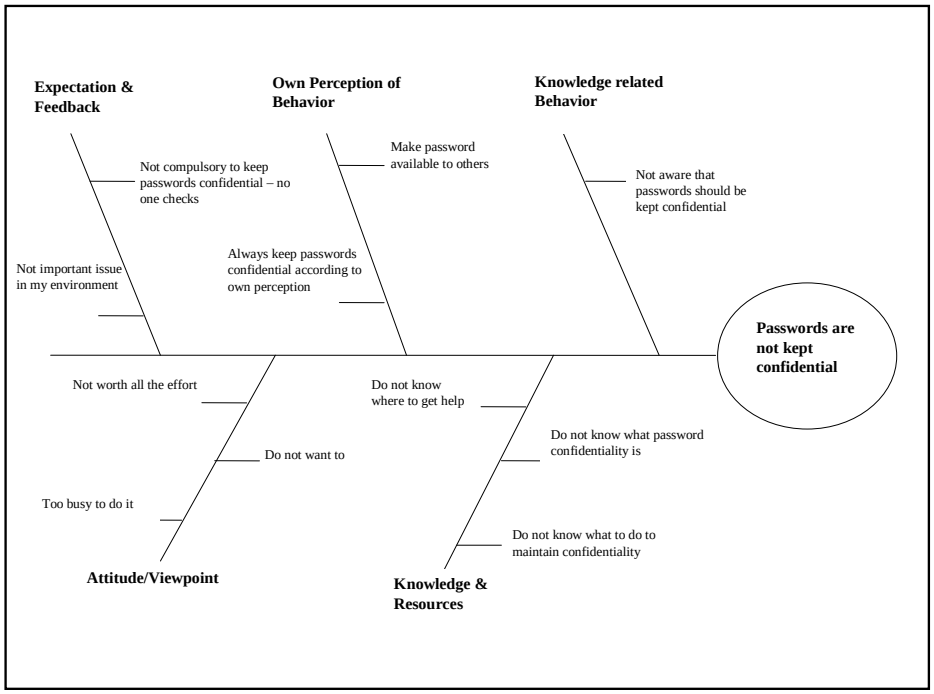

Figure 1 – Cause-and-effect diagram for confidential passwords

Following a number of pilot studies, e-mail messages were sent to 9 different selected class groups with students ranging from first to fourth year and from different study disciplines. They were requested via e-mail and by their lecturers to complete the web-based questionnaire; 395 responses were subsequently received and completed.

The final results were presented as Pareto charts, which are graphical views with bars that are used to present information in such a way that priorities and relative importance of data can be identified. Pareto charts are often used by managers to direct efforts to the biggest improvement opportunity by highlighting the vital few causes in contrast to the trivial many [14]. The charts are constructed

by arranging the bars in decreasing order from left to right along the x-axis, and the cumulative percentages are then used to assist with the analysis of the charts.

Figure 2 contains the Pareto chart for the factors relevant to confidential passwords. More Pareto charts were constructed to present the individual items that contribute to confidential passwords. A similar chart was constructed for the strong password section, which is not presented here.

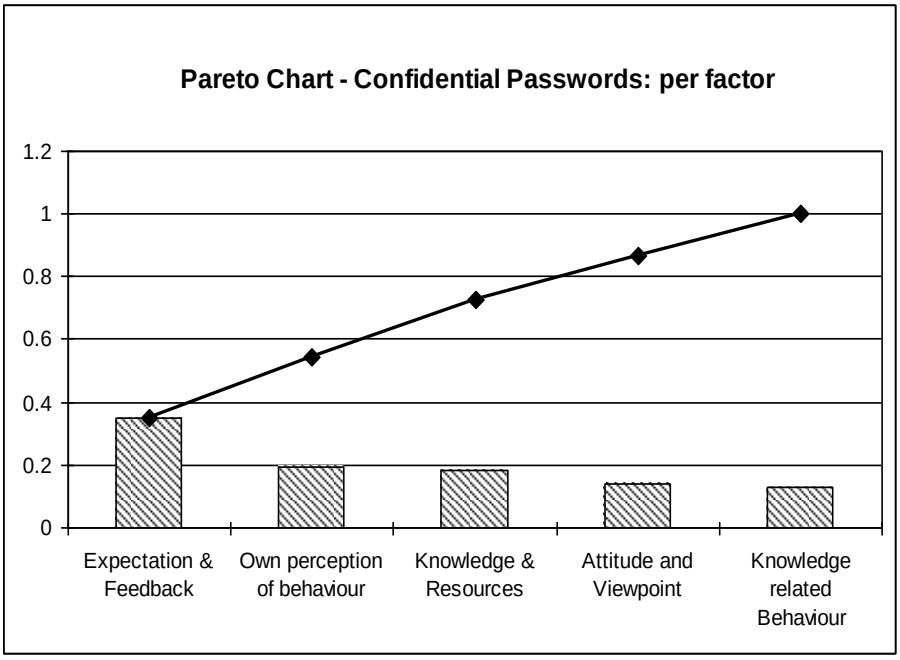

Figure 2 – Pareto chart per factor for confidential passwords

From figure 2, we can see that the *Expectations and Feedback* factor is the most significant determinant that needs to be addressed in order to improve the confidentiality aspect of password management among students. Two items ("*keeping passwords confidential is compulsory in my work environment"* and *"confidentiality of passwords is an important issue in my work environment"*) were used to measure this aspect. Based on the responses, and as shown on the Pareto chart, the perception is that the current message (feedback) that students receive from management, lecturers, their environment, their peers, etc. is that confidentially of passwords is not really important and also not compulsory. It is not really expected of students to keep passwords confidential and the practice thereof is not verified. When interpreting the Pareto chart for individual items (which is not presented here), the mutual importance of each item can also be established to guide educational efforts. In this survey, the most important

individual item, which explains almost 20% of the confidentiality problem, is: "*keeping passwords confidential is compulsory in my work environment – it is regularly checked to see if people keep their password confidential*". The next item, explaining another 18% of the confidentiality problem, is: "*I know where to get help or information regarding the confidentiality of passwords*". These pieces of information determine the important factors, so that management can address specific password behaviour and practices instead of implementing a comprehensive awareness programme. Each of the factors, as well as their related items, can be analysed similarly.

The most significant results that were revealed from this study when interpreting the Pareto charts are as follows:

- Proper use of passwords, including the use of strong 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.
- Users should be made aware of what confidentiality entails and how to get help on this aspect of password management.
- Making passwords available to others is not allowed.

If the above five principles (relating to specific items) could be addressed in security awareness programmes, it would be possible to solve approximately 54% of the problems related to effective password behaviour. The remaining factors and their linked items can be interpreted in the same way. We could also ascertain with this tool that tomorrow's IT users generally have the necessary skills, e.g. they know where and how to change passwords; they generally have a positive attitude or viewpoint towards effective password management, e.g. they think that it is worthwhile to use strong and confidential passwords, and they do not claim to be too busy to concern themselves with strong and confidential passwords.

The above results indicate that educational efforts could be directed more efficiently to focus on problematic aspects of password behaviour.

The following section concludes the paper.

5 Summary and conclusions

As a result of the increased usage of online applications – where passwords are almost always used in the authentication process – and the accompanying threats in the cyber world, all users need to be aware of good password practices.

This paper addressed the password management problem as an essential element in the information security education arena. A study was conducted at a university to identify the important factors that need to be addressed in order to improve password behaviour. Should an organisation be able to identify and

prioritise those significant factors that have an impact on password behaviour, focused awareness programmes can be implemented in such a way that specific issues are addressed. In doing so, financial and other resources can be used more effectively and efficiently. It was shown that tools such as Pareto charts can be valuable. These charts can help identify the important determinants influencing password behaviour among IT users. Educational programmes should include these important factors. [1]

References

1. Walton, R.: Balancing the insider and outsider threat. Computer Fraud & Security, Nov. 8-11 (2006).
2. Dark, M.J.: Security education, Training and Awareness from a Human Performance Technology point of view. (In: Whitman, M.E. & Mattford, H.J., eds. Readings and Cases in the Management of Information Security. Boston : Thomson Course Technology. p. 86-104) (2006).
3. Burnett, M. & Kleiman, D.: Perfect Passwords. Selection, Protection, Authentication. Syngress (2006).
4. Pfleeger, C.P. & Pfleeger, S.L.: Security in Computing. Fourth edition. Upper Saddle River, NJ : Prentice Hall (2007).
5. Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, A. & Memon, N.: PassPoints: Design and longitudinal evaluation of a graphical password system. International Journal of Human-Computer Studies, 63:102-127 (2005).
6. Singh, S., Cabraal, A., Demosthenous, C., Astbrink, G. & Furlong, M.: Password sharing: implications for security design based on social practice, CHI proceedings 27 Apr - 3 May (2007).
7. Forget, A., Chiasson, S., Van Oorschot, P. & Biddle, R.: Improving text passwords through persuasion, Symposium on Usable Privacy and Security, 23-25 Jul (2008).
8. Kruger, H.A., Drevin, L. & Steyn, T.: A framework for evaluating ICT security awareness, In: Proceedings of the 2006 ISSA Conference, Johannesburg, South Africa, 5-7 July 2006 (on CD, 2006).
9. Gollmann, D.: Computer Security. Wiley (1999).
10. Vu, K.L., Proctor, R.W., Bhargav-Spantzel, A., Tai, B.L., Cook, J. & Schultz, E. Improving password security and memorability to protect personal and organizational information. International Journal of Human-Computer Studies, 65:744-757 (2007).
11. Berenson, M.L. & Levine, D.M.: Basic Business Statistics. Concepts and Applications. Sixth edition. Upper Saddle River, NJ : Prentice Hall (1996).
12. Furnell, S.: An assessment of website password practices. Computers & Security, 26:445-451 (2007).
13. Kruger, H.A., Drevin, L. & Steyn, T.: Password management assessment. Technical Report. North-West University, South Africa, FABWI-N-RKW:2008-222 (2008).
14. Pareto Diagram. [Online]. Available WWW: http://mot.vuse.vanderbilt.edu/mt322/Pareto.htm (Accessed 9 July 2007).

[1] This paper is based upon work that was financially supported by the NRF: Grant Number FA200703080000. The opinions expressed in this paper are those of the authors.