An Empirical Assessment of Factors Impeding Effective Password Management

Hennie Kruger  
School of Computer, Statistical and Mathematical Sciences  
North-West University (Potchefstroom Campus), Private Bag X6001, Potchefstroom, 2520  
South Africa  
Hennie.Kruger@nwu.ac.za

Tjaart Steyn  
School of Computer, Statistical and Mathematical Sciences  
North-West University (Potchefstroom Campus), Private Bag X6001, Potchefstroom, 2520  
South Africa  
Tjaart.Steyn@nwu.ac.za

*B. Dawn Medlin  
Computer Information Systems Department  
Appalachian State University  
Boone, NC, 28607  
medlinbd@appstate.edu

Lynette Drevin  
School of Computer, Statistical and Mathematical Sciences  
North-West University (Potchefstroom Campus), Private Bag X6001, Potchefstroom, 2520  
South Africa  
Lynette.Drevin@nwu.ac.za

*corresponding author

Keywords: Password Management, ICT Security Awareness, Security
Abstract

Since passwords are one of the main mechanisms used to protect data and information, it is important to ensure that passwords are managed correctly and that those factors which will have a significant impact on password management are identified and prioritized. Therefore, in order for an information and communication technology (ICT) overall security program to be successful it must include a security awareness program or component. The aim of this paper is to perform an exploratory study with the objective of introducing certain fundamental causes that may impact password management. Empirical results, followed by a survey as well as the application of several management science techniques are presented.
INTRODUCTION

Information and data have become one of the most important aspects in the day to day operations of any organization. With the arrival and growth of the Internet and the World Wide Web, the protection of data is no longer limited to just operational data inherent to an organization. Transactions such as online banking and commerce have resulted in large amounts of sensitive business and personal information that must be managed. As with any other asset, the asset of data and information must be protected, and organizations go to great lengths to accomplish this task. Technical controls such as firewalls and monitoring software are implemented and complemented by procedural controls such as security policies, but unfortunately more protection is sometimes needed.

One of the most basic and important aspects of protecting data and information is authentication. Users and staff are all subjected to authentication processes to restrict access to authorized persons only. Although there are different ways of authentication, most authentication systems are based on the use of a physical token (something you have), secret knowledge (something you know), or biometrics (something you are) (Burnett and Kleiman, 2006). The most common authentication mechanism is the use of a password (something you know), which offers a relatively secure system. However, human practice, such as bad password management, may degrade the quality of password security (Pfleeger and Pfleeger, 2007). Organizations and individuals should therefore be aware of those factors that may compromise password management and the resulting risks.

With this in mind, an exploratory study was undertaken to provide some insight into those factors that will impact the effectiveness of password management. It was assumed that certain problematic issues pertaining to password management exist. The purpose of the study was to apply certain techniques and develop a measuring instrument that will assist in identifying and prioritizing the most significant issues. Cause-and-effect diagrams and Pareto analyses were some of the tools employed to assess student perspectives on password management issues. The study was conducted from a positivistic philosophical stance, where the underlying scientific method assumes that the world is ordered and objective investigation thereof is possible (Oates, 2006).
BACKGROUND

There are many examples in the literature that emphasize the importance of good password practices, describe problems related to passwords and then offer guidelines on how to address the shortcomings. A few examples include a study by Vu, Proctor, Bhargav-Spantzel, Tai, Cook and Schultz, who performed experiments on how to improve password security and enhance password memorability (Vu et al., 2007); Ives, Walsh and Schneider gave recommendations on how to improve authentication systems (Ives et al., 2007); and Furnell, in a study on website password practices, suggests that more should be done to advise and support users in order to protect them and to ensure efficient password use (Furnell, 2007). Most text books on ICT security also address password management; examples include Pfleeger and Pfleeger (2007), Burnett and Kleiman (2006) and Gollmann (1999).

The guidelines in the literature are generally applicable to all businesses, but in this study the focus is on students in a university environment to see how they would apply password management principles. Modern universities, with their core business focused on teaching and research, are managed and operated along the same lines as any other business. They also rely heavily on ICT resources and their databases need to be as accurate and confidential as any other organization. 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; 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 personal losses can be incurred by students if someone else uses their password. Irregularities during examinations and tests that are taken on computers are also likely when students can access other students’ work.

Apart from the usual dishonest behavior that should be avoided, it seems appropriate to assess and address 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.

For the purpose of this study, effective password management was viewed 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, as they were derived from existing literature that provides guidelines on the use of passwords. Both categories are defined by different criteria and can be represented schematically as follows in Figure 1. It should be noted that there is a certain degree of interaction between the two categories and that they are not completely independent determinants of effective password management.

![Effective Password Management Diagram]

**Figure 1: Effective password management categories**

To assist in understanding why ineffective password management occurs, cause-and-effect diagrams were constructed. 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 technique was originally developed by Kaoru Ishikawa in the 1960’s and is also called an Ishikawa diagram (Ishikawa
and Lu, 1985). Other names used to refer to the tool include Fishbone diagram (because of the way various causes are arranged on the diagram) and a Root Cause Analysis diagram (because of the ability to identify possible root causes for a specific effect or problem).

Cause-and-effect diagrams were 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 are often subdivided into a few major categories depending on the problem under investigation. Berenson and Levine (1996) referred to examples of categories such as manpower, methods, materials and machinery that can be used. Within each major category, specific causes are listed as branches or sub-branches. Cause-and-effect diagrams offer a number of advantages and are often used when there is a need to understand certain processes, determine root causes to specific problems, or identifying areas for data collection etc. (Chang and Lin, 2006 ; Suwignjo et al, 2000).

The nature of the problem in this study can be summarized by any one of the following statements: “What is causing ineffective password management by students?” or alternatively, “What factors affect ineffective password management choices by students?” Further, the purpose is to identify a few key sources that contribute most significantly to the problem of ineffective password management. These are typical cause-and-effect problem statements, so the use of a cause-and-effect diagram seems to be an appropriate option to analyze the password management problem. The next section describes the construction of such a diagram for this research project as well as the development of a measuring instrument that could be used to evaluate the causes identified.

RESEARCH METHODOLOGY

It was accepted for this study that the effective management of passwords is dependent on two main factors - - strong passwords and confidentiality of passwords. Each of these two factors was investigated using a cause-and-effect diagram in order to provide a greater level of detail.

Cause-and-effect diagram

The problem in both cases was simply formulated as “Strong passwords are not used” and “Passwords are not kept confidential.” The next step was to identify the main possible
causes for these problems (the effect to be investigated) in order to complete the branches of the diagram.

The establishment of causes was based on the organizational assumptions that human performance is a function of ability and motivation; ability is a function of aptitude and education (knowledge/skills); and motivation is a function of desire and commitment (Dark, 2006). This assumption provided a framework of categories that could be used in the cause-and-effect diagrams. The actual causes were then identified through brainstorming sessions by the research team and validated, firstly, against appropriate literature such as Pfleeger and Pfleeger (2007), Burnett and Kleiman (2006) and Furnell (2007), and secondly, during the pilot study. Following several iterations of refinement, 11 causes were identified for the strong password problem and 10 for the confidential password problem.

Figure 2 shows the final cause-and-effect diagram for the strong password problem with the final grouping of causes in specific categories. These groupings were obtained through factor analysis performed during the pilot studies.

![Figure 2: Cause-and-effect diagram for Strong passwords](image-url)
**Instrument Development and Validation**

The development of a cause-and-effect diagram is typically followed by a data gathering process to determine those causes that have a more significant impact on the problem and how they may be addressed. The causes identified on the two diagrams were therefore converted into a questionnaire, with the objective to test and empirically validate the effectiveness of password management.

An initial draft questionnaire was developed containing the 21 items (questions) identified with the cause-and-effect diagrams. These items had to be answered on a 3-point scale (Yes, No and Do Not Know). As the final measuring exercise was planned to be conducted with students, additional questions such as year of study, study course, gender etc. were added. To facilitate the distribution of the questionnaire, a small web application was developed to make the questionnaire available and to capture responses. An initial small pilot test was then conducted where 50 students were randomly asked to complete the questionnaire – the aim was to determine if questions, and the wording of questions, made sense and also to verify that the web application operated correctly. Limited statistical tests and the frequencies of responses indicated that certain adjustments were necessary. The wording of certain questions was changed, some of the questions were changed from negative to positive statements and the “Do Not Know” option was changed to “Unsure”. The result was a 23-item (12 *strong password* items and 11 *confidential password* items) questionnaire with an additional five other general questions. The 12 items, pertaining to strong passwords, are seen on the cause-and-effect-diagram (Figure 2). A similar cause-and-effect diagram, containing the 11 items for confidentiality of passwords, was constructed but not shown here. A second pilot study was then conducted to test the changes made. Seventy one students were asked to complete the questionnaire, and again some minor adjustments were made.

In order to validate the instrument, before the actual measuring experiment could take place, a third and final pilot study was conducted. E-mail messages were sent to four different class groups, ranging from first to third year students, requesting they visit the website where the questionnaire was located and to complete it. Responses were received from 329 students and used for validation purposes. The validation was performed along guidelines suggested by Straub and included content validation, reliability tests and construct validation (Straub, 1989).
**Content validation**

Content validation is a process whereby test items are studied and weighted for their representativeness (Kerlinger, 1986). In this study content validity was established through relevant literature sources, two initial pilot studies and the use of basic statistical tests. Reliability refers to the accuracy or precision of a measuring instrument; i.e., if the same set of objects is measured again and again with the same instrument, will similar results be obtained? One way to assess consistency is to calculate a Cronbach alpha coefficient (Kerlinger, 1986). The overall coefficient for the 12 items pertaining to *strong* passwords was 0.77 and for the 11 items pertaining to *confidential* passwords, the coefficient was 0.76. Although the Cronbach alpha coefficients were slightly lower for each construct (factor) identified during factor analysis, the results were accepted as reasonable.

**Construct validity**

Construct validity primarily answers questions such as what factors or constructs account for variance in test performance (Kerlinger, 1986). To identify possible constructs underlying the measuring instrument, exploratory factor analysis was employed. The factor analysis, where factors were extracted by means of the principle component method, followed by varimax rotation, yielded 5 and 4 factors for strong passwords and confidential passwords respectively. The results are shown in tables 1(a) and 1(b).
Table 1(a): Factor loadings – Strong Passwords

<table>
<thead>
<tr>
<th>Item</th>
<th>Factor 1</th>
<th>Factor 2</th>
<th>Factor 3</th>
<th>Factor 4</th>
<th>Factor 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Item 3</td>
<td>0.538</td>
<td>-0.075</td>
<td>0.375</td>
<td>0.152</td>
<td>0.255</td>
</tr>
<tr>
<td>Item 5</td>
<td>0.788</td>
<td>-0.032</td>
<td>0.102</td>
<td>0.068</td>
<td>0.272</td>
</tr>
<tr>
<td>Item 6</td>
<td>0.749</td>
<td>0.185</td>
<td>0.003</td>
<td>-0.001</td>
<td>0.189</td>
</tr>
<tr>
<td>Item 4</td>
<td>-0.176</td>
<td>0.578</td>
<td>0.142</td>
<td>0.381</td>
<td>0.318</td>
</tr>
<tr>
<td>Item 8</td>
<td>0.161</td>
<td>0.785</td>
<td>0.065</td>
<td>0.050</td>
<td>0.016</td>
</tr>
<tr>
<td>Item 10</td>
<td>-0.139</td>
<td>0.590</td>
<td>0.257</td>
<td>0.226</td>
<td>0.079</td>
</tr>
<tr>
<td>Item 11</td>
<td>0.461</td>
<td>0.564</td>
<td>0.193</td>
<td>-0.012</td>
<td>0.091</td>
</tr>
<tr>
<td>Item 7</td>
<td>-0.078</td>
<td>0.103</td>
<td>0.838</td>
<td>0.057</td>
<td>0.158</td>
</tr>
<tr>
<td>Item 9</td>
<td>0.316</td>
<td>0.156</td>
<td>0.776</td>
<td>-0.008</td>
<td>-0.021</td>
</tr>
<tr>
<td>Item 1</td>
<td>0.064</td>
<td>0.096</td>
<td>0.023</td>
<td>0.949</td>
<td>0.002</td>
</tr>
<tr>
<td>Item 2</td>
<td>0.325</td>
<td>0.095</td>
<td>-0.067</td>
<td>-0.061</td>
<td>0.745</td>
</tr>
<tr>
<td>Item 12</td>
<td>0.209</td>
<td>0.081</td>
<td>0.265</td>
<td>0.081</td>
<td>0.761</td>
</tr>
</tbody>
</table>

Table 1(b): Factor loadings – Confidential Passwords

<table>
<thead>
<tr>
<th>Item</th>
<th>Factor 1</th>
<th>Factor 2</th>
<th>Factor 3</th>
<th>Factor 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Item 13</td>
<td>0.600</td>
<td>0.118</td>
<td>-0.168</td>
<td>0.411</td>
</tr>
<tr>
<td>Item 17</td>
<td>0.627</td>
<td>-0.125</td>
<td>0.327</td>
<td>-0.209</td>
</tr>
<tr>
<td>Item 20</td>
<td>0.745</td>
<td>0.062</td>
<td>0.153</td>
<td>0.077</td>
</tr>
<tr>
<td>Item 22</td>
<td>0.789</td>
<td>0.039</td>
<td>0.120</td>
<td>0.134</td>
</tr>
<tr>
<td>Item 23</td>
<td>0.635</td>
<td>0.120</td>
<td>0.150</td>
<td>0.404</td>
</tr>
<tr>
<td>Item 18</td>
<td>-0.041</td>
<td>0.869</td>
<td>0.092</td>
<td>-0.130</td>
</tr>
<tr>
<td>Item 21</td>
<td>0.398</td>
<td>0.608</td>
<td>-0.087</td>
<td>0.343</td>
</tr>
<tr>
<td>Item 15</td>
<td>0.040</td>
<td>0.416</td>
<td>0.599</td>
<td>0.134</td>
</tr>
<tr>
<td>Item 16</td>
<td>0.186</td>
<td>-0.080</td>
<td>0.756</td>
<td>0.176</td>
</tr>
<tr>
<td>Item 19</td>
<td>0.162</td>
<td>0.244</td>
<td>0.560</td>
<td>0.139</td>
</tr>
<tr>
<td>Item 14</td>
<td>0.115</td>
<td>-0.062</td>
<td>0.201</td>
<td>0.851</td>
</tr>
</tbody>
</table>
Following a careful study of factor loadings, item groupings and the meaning of specific questions (items), it was decided to sub divide Factor 1, in table 1(b), into two different sub-factors. Items 13 and 23 were treated as one factor, while items 17, 20 and 22 were viewed as another factor. The result was a 5-factor instrument for each of the 2 aspects studied and was defined as follows in Table 2.

Table 2: Factor Definitions

<table>
<thead>
<tr>
<th>Strong Passwords</th>
<th>Confidential Passwords</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attitude/Viewpoint (items 3,5,6)</td>
<td>Attitude/Viewpoint (items 17,20,22)</td>
</tr>
<tr>
<td>Knowledge and Resources (items 4,8,10,11)</td>
<td>Knowledge and Resources (items 15,16,19)</td>
</tr>
<tr>
<td>Expectation and Feedback (items 7,9)</td>
<td>Expectation and Feedback (items 18,21)</td>
</tr>
<tr>
<td>Skills (item 1)</td>
<td>Knowledge related behavior (item 14)</td>
</tr>
<tr>
<td>Own perception of behavior (items 2,12)</td>
<td>Own perception of behavior (items 13,23)</td>
</tr>
</tbody>
</table>

All calculations and tests performed during the instrument development and validation phase were done using the statistical software package Statistica (StatSoft, 2006). A complete list of items and their descriptions as well as reliability test results can be found in Kruger, Drevin and Steyn (2008).

**Application and Results**

Following the final pilot study and validation process, an actual measuring experiment was conducted at a South African university to investigate password management among students. The university consists of three different campuses located in three different cities, one of which was selected for the exercise. The selected campus is the largest of the three with eight divisions (academic faculties) and with more than 26,000 students. The ICT infrastructure at the campus is one of the best, and all students are linked to a central network that gives access to the full spectrum of electronic communication as well as Internet access. A reasonable level of student ICT security is
maintained, but no official security awareness program is in place and students do not receive any formal ICT security awareness training.

The web application used during the pilot study was used again, and e-mail messages were sent to nine different selected class groups, with students ranging from 1\textsuperscript{st} to 4\textsuperscript{th} year and from different study disciplines. They were requested to complete the questionnaire. A response rate of 44\% or 395 responses were received. The demographic profile of the 395 students is depicted in Figure 3.

![Field of Study](chart1.png)

**Figure 3: Sample Demographic Information**

Figure 4 contains the Pareto chart where we present our final results. 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.

From Figure 4 it is clear that the Expectations and Feedback cause is the most significant issue to be tackled when trying to address the strong password aspect of password management among students. Items 7 and 9 (strong passwords are not compulsory and strong passwords are not important) were used to measure this factor.

![Pareto Chart](image)

**Figure 4 – Pareto Chart per factor for Strong Passwords**

Based on the responses and as shown on the Pareto charts, it must be accepted that the current message (feedback) that students receive from management, lecturers, their environment, their peers, etc. is that the use of strong passwords is not really important and also not compulsory – they are not really expected to use strong passwords
and the use thereof will not be verified. Looking at Figure 5, it can be seen that item 7 is much more important than item 9 and when addressing this cause, more focus should be placed on item 7 (even though both items measure the same cause). 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, can be analyzed in a similar way.

![Strong Passwords per Question](image)

**Figure 5 – Pareto Chart per question for Strong Passwords**

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 strong passwords and keeping passwords confidential is *compulsory*. (Expectations and Feedback)
– 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. (Expectations and Feedback)
– The use of simple passwords that can easily be remembered is not acceptable. (Perception/Belief)
– Making passwords available to other people is not allowed. (Perception/Belief)

From figure 4 it can be seen that addressing these four simple principles, which constitutes the two factors Expectations and Feedback and Perception/Belief would solve more than 50% of the problems related to effective password management. The remaining factors and their associated items can be evaluated in the same manner or in a follow-up exercise. On the positive side of the scale it appears as if students have the necessary skills to know where and how to change passwords; they generally have a positive attitude or viewpoint towards effective password management, think it is worthwhile to use strong and confidential passwords and do not claim that they are too busy to concern themselves with strong and confidential passwords. They also agree in general that passwords should be kept confidential.

Results have shown that a need exists to implement ICT security awareness programs among students to increase effective password management specifically, and ICT security in general. Not all students are aware of certain basic password security principles – information that is often taken for granted as being general knowledge and which may pose serious threats to ICT security at campuses. By understanding the various password management issues that might exist, it becomes possible to recommend approaches that management could adopt to overcome these obstacles.

Conclusions

The increasing importance of data and information necessitates good ICT security practices, and password-based authentication is one of the techniques frequently used for such protection. Proper password management has therefore become an essential element in the information security arena, and comprehensive and expensive security awareness programs are often implemented to educate people concerning the aspects of proper
password management. Should an organization be able to identify and prioritize those factors that significantly impact password management, tailor made awareness programs can be tailored to that organizations core issues. This paper presented a study where cause-and-effect diagrams were used to assist in developing a measuring instrument to evaluate password management among students. Pareto analyses were then used to identify and prioritize significant aspects. Results, where the study was performed, revealed that students do not regard the use of strong passwords, or keeping their passwords confidential, as an important aspect – they did not experience it as being compulsory in their environment and would use simple passwords that can easily be remembered; they would also make their passwords available to other students if necessary.

In general, the study has shown that the use of cause-and-effect diagrams provides a better understanding of those factors that may impact the use of passwords. Applying Pareto analyses revealed additional important insights and allow for identifying and prioritizing improvement opportunities. No similar measurement scales are described in the literature that can be utilized to evaluate the effectiveness of password management. The scale and results presented here will enable management of organizations to more accurately address problems associated with the use of passwords through focused ICT security awareness programs.

The study will be followed-up by an international survey to include students from different universities in different countries in order to broaden the area of experience and to do comparative studies that will generate recommendations that are valid and reliable over a broad spectrum. An initial pilot study, involving students from a campus in the United States has already been completed and will be used as a basis for the intended project.
References


