How secure are passwords that will be used by future health care workers?

H.A. 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

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

B. Dawn Medlin
Computer Information Systems Department
Appalachian State University
Boone, NC, 28608
medlinbd@appstate.edu

Abstract

Employees within the health care industry play an important role in the protection of patients and their own private and personal information. In most cases passwords provide the first line of defense which means that the use of insecure passwords can be costly. This paper reports on the results of an empirical study that was carried out among students at two universities, one in the USA and the other in South Africa, to assess their password choices. Results indicate that most students either do not know how to select a secure password or that they simply choose to ignore basic password security principles. The effects of their password choices if weak could have a detrimental effect on patients, the employees themselves, and their organizations.

Keywords: Password Management, Security Awareness, Health Care Organizations

1. Introduction

Computer security generally refers to three important aspects found in any computer-related system namely, confidentiality, integrity and availability (Pfleeger and Pfleeger, 2007). The use of passwords, or any other authentication process, is closely linked to all three of these aspects. Confidentiality ensures that resources are accessed only by authorized parties; Integrity means that modifications can only be done by authorized parties; and, Availability means that resources are only accessible to authorized parties at appropriate times (Pfleeger and Pfleeger, 2007).

The importance of using secure passwords and maintaining good password management principles can not be underestimated and most Information and Communication Technology (ICT) standards make reference to specific control objectives to ensure that people and organizations adhere to good password practices (SANS, 2005). Despite the fact that almost all modern systems and IT assets are being protected with passwords – at least as a first line of defense – it appears as if the use and the selection of secure passwords are not a straightforward process. Much has been written in the literature on problems associated with passwords and its use. Examples include problems such as the re-use of passwords (Ives *et al*, 2007), memorability of passwords (Vu *et al*, 2007) and practicing good password principles in general (Furnell, 2007; Furnell and Zekri, 2006; Cazier and Medlin, 2006b; and Summers and Bosworth, 2004).

Considering the importance of passwords and the problems related to the use of passwords, this paper reports on the results of an empirical study carried out among university students in South Africa and the USA to assess the degree of the security of their passwords choices. Certainly, students can be regarded as the future IT health care workers of tomorrow, therefore it makes sense to evaluate young people's knowledge and behavior pertaining to password practices. Descriptions of similar studies can be found in Garrison (2006) – an analysis of student passwords; Cazier and Medlin (2006a) – a study of healthcare workers' password practices; and, Stanton *et al* (2005) – a survey of end-user password-related behaviors.

In the next section a brief background on passwords and associated problems is given. This is followed by a discussion of an empirical experiment, and its results, that was carried out. Concluding remarks are then given in the last section.

2. Passwords

According to Burnett and Kleiman (2006) passwords are used to authenticate users. It is something a user knows (secret knowledge) and presents to an authentication system to get access to certain resources. In addition to prove a user's identity (authenticate) it is also used to keep sensitive information secure (privacy) and prevent someone from later rejecting the validity of transactions authenticated by a password (non-repudiation). The problem is that passwords have weaknesses e.g. more than one person can possess knowledge of the secret (password), one can loose the password or it can be stolen. Researchers have concurred that passwords are therefore completely dependent on the common sense and behavior of password holders and the only defense is to build strong passwords, protect it carefully and change it regularly.

2.1 Weak passwords

The definition of weak passwords includes any words that may appear in a dictionary, e.g., words that only utilize letters and no other type of special character. As an example, nouns or proper names are poor choices for passwords, including nicknames or the name of a spouse or pet. Unfortunately, most users create passwords containing a family name, pet name, birthday, or anniversary (Cazier and Medlin, 2006b). These passwords are weak because they can be easily cracked through the use of cracking software.

In order to also gain information without having to break into a system or use social engineering tactics, individuals who are interested in obtaining information about another

person might do so by looking in the phone directory or by picking up an individual's mail. Today, hackers and social engineers can obtain information by “googling” someone. Google's search and information retrieval capabilities have made it the first stop for many hackers in their quest to obtain personal information, often from a comfortable and anonymous distance. Google is just one of the services that indexes web pages on the Internet, not only acquiring information but integrating it into databases, such as individuals’ phone numbers, addressees, and directions to their homes. Using all of these types of information gathering techniques allows hackers to build a profile of an employee and thus may be able to guess their password.

New social networking sites, such as www.myspace.com further compound this problem. As more and more people put more details of their life on a searchable web, hacker’s are able to learn much more about their targets, increasing the chances of a breach.

Considering the importance of computer security and the important role that passwords are playing in the process, it is clear that passwords require a certain degree of complexity in order to protect health care assets effectively.

2.2 Secure passwords

A strong password is simply a password that no one else can predict (or guess) within a reasonable amount of time (Burnett and Kleiman, 2006). To comply with this, users should, in the first place, ensure that their password-related behavior is acceptable. Basic guidelines for password behavior include aspects such as do not write your password down, do not tell it to someone, do not write it on a piece of paper and then throw it in the garbage, and do not use the same password all the time (Smith, 2001). Once users understand and comply with these password behavior principles, they should then ensure

that they choose strong passwords that also satisfy complexity and uniqueness requirements. According to Summers and Bosworth (2004) some examples of how to achieve this include a minimum password length of six to ten characters. It must contain at least three of the following: alpha, uppercase alpha, digits and special characters, the alpha, number and special characters must be mixed up (do not just add digits to the end of the password) and, do not use 'dictionary' words.

2.3 Problems when choosing secure passwords

A password should be difficult to guess which means it should not be something that can easily be associated with the user. At the same time the password must be something the user can easily remember (Whitman and Mattord, 2005). To comply with the former, a password should be constructed as a word or words that consists of a large enough number of characters (e.g. ten characters) which were chosen randomly. Burnett and Kleiman (2006) give an informative discussion on randomness and how it is linked to concepts such as even distribution of characters chosen, unpredictability and uniqueness. They conclude that humans generally have a poor understanding of randomness and that they are therefore not really capable of complying with the randomness requirement when having to choose a password. There are of course other ways of generating a string of random characters e.g. to make use of programs that are specifically designed to be used as password generators and that can provide users with ready-made passwords (Cazier and Medlin, 2006b). However, due to the random nature of characters, the passwords may be difficult to remember - this is a contradiction of the requirement that users should be able to easily remember their passwords. The memorability of passwords is an important issue and Vu *et al* (2007) conducted a study to evaluate the tradeoff between password security and memorability of passwords. They made certain

recommendations to enhance both the security and memorability of passwords e.g. a minimum length restriction, inclusion of special characters and digits, avoiding the use of simple patterns etc.

Passwords are important and from the discussion so far it seems as if there are certain problems associated with passwords and how they are used that may compromise the safeguarding of health care resources and assets. At the same time it is also apparent that there are certain basic rules and behavior guidelines which, when followed, may increase and maintain an acceptable level of password security. In the next section an empirical experiment that was performed amongst students, to assess the degree of secure passwords used by them, is described.

3. Cracking Passwords

But adhering to security experts' suggestions about the creation of good passwords usually involves a tradeoff. If a password is easy to create and remember, it is probably also easy for others to guess or a hacker to crack.

Weak passwords can be easily cracked or broken, and with enough time and effort, so can good passwords. Password cracking is the process of figuring out or the breaking of passwords in order to gain unauthorized access to a system or account. In today's e-commerce environment where more users are participating in online shopping, banking, and other electronic endeavors, it is much easier for hackers to gain entrance into networked systems than one would think.

There is a distinct difference between "cracking" and "hacking." Essentially, "codes are cracked" and "machines are hacked." If a password is cracked, it could allow the hacker to assume the legitimate user's identity, thereby allowing access to all data that the legitimate user is authorized to view.

There are five main techniques hackers can use to identify a password:

1. **Steal it.** That means looking over your shoulder when you type it, or finding the piece of paper where you wrote it down.
2. **Guess it.** Psychologists say that we create passwords that are familiar to us, usually consisting of the names of spouses or favorite sports team, so it is relatively easy for others to guess it.
3. **Brute force attack.** This is where every possible combination of letters, numbers and symbols is used in an attempt to guess the password. While an extremely labor intensive task, with modern fast processors and software tools this method should not be underestimated.
4. **Dictionary attack.** The dictionary attack uses combinations of words. In the first attempt, words available in a general dictionary are chosen. Software tools are readily available that can try every word in a dictionary or word list or both until your password is found. Dictionaries with hundreds of thousands of words, as well as specialist, technical and foreign language dictionaries are available, as are lists of thousands of words that are often used as passwords such as "qwerty", "abcdef" etc.
5. **Hybrid attack.** This method of attack uses a hybrid check which mixes the aforementioned two attack techniques by using dictionary type words as a base and then using brute force to check for permutations of that word. Essentially, it combines the best of both methods and is considered to be highly effective against passwords where little or no imagination was used.

Passwords can be cracked through a variety of methods, with the simplest method being the use of a dictionary or word list. Electronic dictionaries exist currently for a variety of languages that include English, Spanish, French, and many other foreign languages. Dictionaries also exist that contain words from TV shows, movies, music, sports, and numerous hobbies. In reality, unfortunately, what emerges from the human mind is seldom truly random. So the more efficient computer programs systematically use extended dictionaries that can identify different combinations of words.

Whereas dictionaries or wordlists rely on speed, the second method of password cracking relies purely on power. The brute force attack method, as previously mentioned attempts to crack the password by simply comparing every possible combination and permutation of characters available until it finds a match for the password. As the name implies, brute forcing is very powerful, and given enough time can crack any conceivable password. Once a password is cracked, it could allow the hacker to assume the legitimate user's identity, thereby allowing access to all data that the legitimate user is authorized to view. Even worse, the hacker may be able to escalate those privileges into taking control of the entire network.

In an effort to mimic human behavior, many of the most powerful password-cracking dictionaries add twists beyond simply suggesting a word. They experiment with first and last names, sports teams, fictional characters, numbers, punctuation symbols, and foreign-language terms. They reverse the spellings, string words together, substitute zeros and ones for the lowercase O and L and try popular keyboard sequences like "qwerty".

The reason that most software cracking programs are so very effective is that they usually attack an institution's passwords en masse. No one may know which specific person at a company is a Michael Jordan fan, but among 1,000 people in the United States, the probability that at least one is a Michael Jordan fan and has a related password is fairly high. The same is true with other famous sports stars or teams (Andrews, 2004).

In contrast to weak passwords, governmental agencies such as the Department of Defense in 1985 and organizations such as CERT (Computer Emergency Response Team) have provided guidance in the creation of good passwords. These found that passwords are made more secure by adding both length and strength.

4. Assessing Passwords – an empirical experiment

Data collection

The evaluation of passwords used amongst students formed part of another research project to study the effectiveness of password management that was performed earlier

(Kruger, Drevin and Steyn, 2008). During this study a measuring instrument was developed to evaluate certain dimensions of password management. The instrument (questionnaire) was made available to students via a simple web application and after completing the questionnaire, respondents were asked to save their responses using a password. The passwords were then recorded and used for analyses in the current study. It is accepted that in some cases users may not use the same level of secure passwords to save a document than what they would have used, for example, as a personal network password. However, the assumption was made that the document passwords would be a fair reflection of how respondents think about passwords and how passwords are chosen by them, e.g. if someone uses a family name as a password, it is likely that the same type of password will be used in other instances as well. In addition, ethical and privacy considerations prohibited the use of actual network passwords of students.

The broader study of evaluating password management effectiveness was conducted at two different universities – one in South Africa and the other one in the United States of America. A total of 936 passwords were collected from students attending the two universities and were used for the evaluation. The objective with the data gathering was to ensure that a reasonable sized international sample was used – the purpose was not to do a comparative study of password use between the two universities and all responses were therefore treated as one sample.

The sample consisted of 56% male and 44% female respondents. Additionally, the majority of respondents were from the Economics field of study (33%), followed by the major field of Natural Science with 21% or 197 respondents. These two areas of study were closely followed by Engineering majors with 20%. The three lowest major

respondents were Theology with 1%, Law with 3%, and Art with 7%. It should also be noted that 8% (77) of the respondents majored in the area of Health.

Other descriptive statistics should be noted. The largest numbers of respondents were in their first year of study (36%, 337), followed by 25% (234) in their third year of study. The smallest numbers of respondents were in their last year of study with only one percent difference (19%, 178) between the second and fourth year students.

3.2 Results and Discussion

Only two properties, password length and mix of characters used, were initially evaluated. The reasons for choosing these two properties were mainly because they seem to be the most important ones (mentioned in most the review of literature), they are basic properties that can easily be understood and applied by all users and, finally, it was fairly easy to verify if the sample of passwords comply with them. A program was developed to classify and count the passwords according to the properties and the results are summarized in Table 1.

Table 1 shows that students are not complying with one of the basic rules which states that a mixture of characters from different character sets should be used. Less than half of those evaluated (45%) have used more than one character set to construct a password.

Table 1 – Summary of mix of characters used in passwords

Number	Percentage	Characters used in passwords
91	9.72	Only numbers
398	42.52	Only lower case alphabetic characters
17	1.82	Only upper case alphabetic characters
3	0.32	Only symbols (special characters)
427	45.62	Combination of at least two character sets
936	**100**	

In Figure 2 we see that 46% of respondents used passwords with a length equal to or less than 6 characters – even though it means that 54% used passwords of length 7 or more, the statistics are simply not favorably. The length requirement is an even more basic requirement which students either choose to ignore or they are not aware of it. The average length of all passwords appears to be appropriate at between 8 and 9 characters.

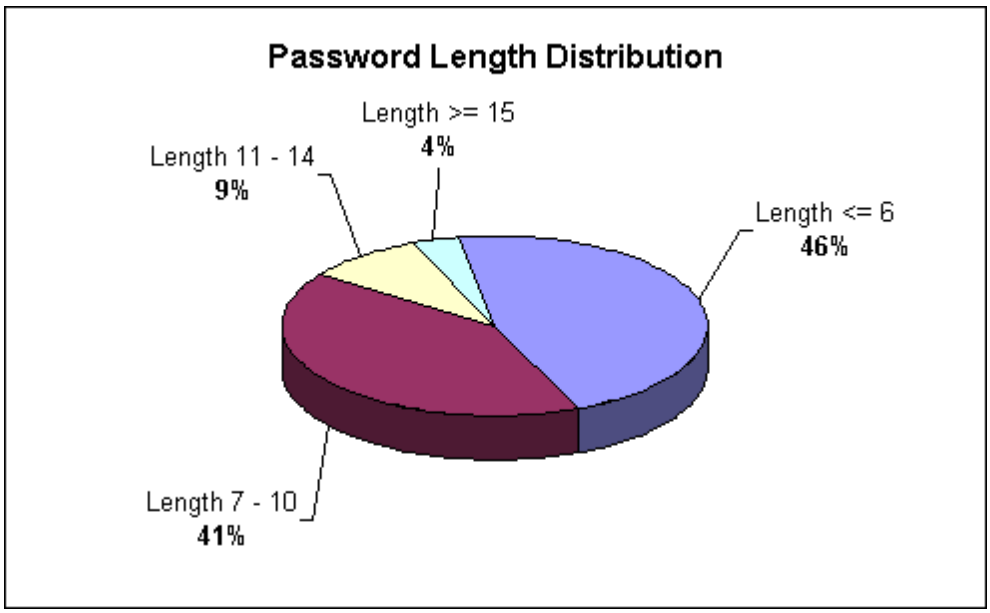

Figure 2 – Password length distribution

Another interesting observation regarding the length of passwords used was derived from the questionnaire used to verify password practices (Kruger, Drevin and Steyn, 2008). One of the questions explicitly asked respondents whether they belief that the passwords they are using are secure passwords. Almost half of the respondents (49%) stated that they use secure passwords. When checking their passwords and applying only the one rule concerning password length, it was found however, that 46% of those who said that they are using secure passwords have passwords with 6, or less, characters. This finding is 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.

In order to determine if any specific year of study can be associated with the use of weak passwords, a χ^2-test (Wegner, 1993) was performed using a 6-character limit as the defining criterion for a weak password. The competing hypotheses

H_0: *There is no association between the use of weak passwords and the year of study (i.e. they are independent)*

H_1: *There is an association between the use of weak passwords and the year of study (i.e. they are not independent)*

were considered at a 5% significance level. The null hypothesis (H_0) may then be rejected in favor of the alternative hypothesis (H_1) if the computed χ^2-statistic value exceeds the tabulated χ^2-value (critical value) corresponding to the desired level of significance and degrees of freedom. A χ^2-statistic of 3.775 was computed which is less than the tabulated χ^2-critical value of 7.815 (significance level = 0.05 and degrees of freedom = 3). The null hypothesis (H_0) was therefore accepted and concluded that there is no significant association between the use of weak passwords and the year of study. This result suggests that a common security awareness program strategy (related to passwords) can be adopted for all students – there is no need, as one would have expected, to target specifically new (first year) students as opposed to more senior (fourth year) students when making them aware of password security.

In general, the results discussed, can be summarized as follows. Using only two very basic requirements for secure passwords (length and mix of characters) it was found that students are either not aware of the basic rules or that they choose not to follow them. This was confirmed by checking the password length of those respondents who were of the opinion that they do use secure passwords – a significant number of them had passwords with a length of 6 or less characters. Finally, there is no association between the use of weak passwords and the year of study – senior students are just as guilty as junior students. The results have shown that students, tomorrow's workforce, are not satisfactorily complying with basic password security standards. By ensuring that students are aware of what constitutes a strong password and encouraging them to adhere to required principles and guidelines, it would be possible to increase the level of password security and ultimately security in general.

5. Conclusion

Students are tomorrow's workers and management leaders in the field of health care management. Therefore, it makes sense to make them more aware of security practices in general and good password principles specifically. In this paper an empirical assessment of the use of strong passwords, conducted at two universities, one in South Africa and one in the USA was described. Results revealed that the students are not satisfactorily adhering to basic password security rules such as using a sufficient length of passwords and the use of a mix of characters in passwords. This appears to be a problem with all students regardless of seniority.

Though the health care industry must address security issues due to legal ramifications and regulations so must most industries today. Therefore, this study could be applied to different industries with the final results providing a better understanding of how young

people perceive strong passwords and how they select their passwords. The assessment also provides information on what are the basic security principles that students should be made aware of in order to respond to modern security requirements.

References

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

Burnett, M. & Kleiman, D. 2006. *Perfect Passwords. Selection, Protection, Authentication.* Syngress.

Cazier, J.A. & Medlin, B.D. 2006a. How secure is your Information System? An investigation into actual healthcare worker password practices. *Perspectives in Health Information Management*, 3(8):1-7.

Cazier, J.A. & Medlin, B.D. 2006b. Password Security: An empirical investigation into E-commerce passwords and their crack times. *Information Systems Security: the (ICS)^2 Journal*, 15(6):45-55.

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

Furnell, S. & Zekri, L. 2006. Replacing passwords: in search of the secret remedy. *Network Security*, January 2006:4-8.

Garrison, C.P. 2006. Encouraging good passwords. *Proceedings of the 3rd annual Conference on Information Security Curriculum Development*, 109-112.

Ives, B., Walsh, K.R. & Schneider, H. 2007. The domino effect of password reuse. *Communications of the ACM*, 47(4):75-78.

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

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

SANS 17799:2005. 2005. Information Technology - Security Techniques – Code of practice for information security management (identical implementation of ISO/IEC 17799:2005).

Smith, K. 2001. Security Awareness: Help the users understand. SANS Institute 2001.

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

Summers, W.C. & Bosworth, W. 2004. Password policy – the good, the bad and the ugly. *Proceedings of Winter International Symposium on Information Communication Technologies Conference*.

Vu, K.L., Proctor, R.W., Bhargav-Spantzel, A., Tai, B.L., Cook, J. & Schultz, E. 2007. Improving password security and memorability to protect personal and organizational information. *International Journal of Human-Computer Studies*, 65:744-757.

Wegner, T. 1993. Applied Business Statistics. Methods and Applications. Juta & Co Ltd.

Whitman, M.E. & Mattord, H.J. 2005. Principles of Information Security. 2nd edition. Thomson.