IT USERS' AWARENESS ABOUT THE NEED OF STRONG PASSWORDS CREATION

KONECKI, M.; OREHOVACKI, T. & STAPIC, Z.

Abstract: *Business world today, along with belonging processes, is becoming more and more dynamic and complex. Information as a vital resource has to be adequately protected. Security generally has become an issue of great importance. One of the security mechanisms and actual security issues is the problem of strong passwords creation. This problem is directly connected with the users' awareness about strong passwords creation. In our research we have analyzed the strength of passwords created by experienced IT users. Known password strength determination algorithms have been used in our analysis. Two hypotheses were created and tested using analysis of gathered data, correlation and regression. Conclusions and possible resolutions are presented and discussed.*

Key words: *password, strenght, security, awareness*

Authors´ data: Konecki, M[ario]; **Orehovacki**, T[ihomir]; **Stapic**, Z[latko], Faculty of Organization and Informatics, Pavlinska 2, 42000, Varazdin, HR, mario.konecki@foi.hr, tihomir.orehovacki@foi.hr, zlatko.stapic@foi.hr

This Publication has to be referred as: Konecki, M[ario];Orehovacki, T[ihomir];Stapic, Z[latko] (2008). It Users' Awareness about the Need of Strong Passwords Creation, Chapter 33 in DAAAM International Scientific Book 2008, pp. 387-394, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-901509-69-0, ISSN 1726-9687, Vienna, Austria
DOI: 10.2507/daaam.scibook.2008.33

1. Introduction

With increasing number of applications, particularly web applications, in all areas of business and education, their importance becomes more significant for the proper functioning of number of systems. Systems that we encounter in our everyday lives and business are connected between each other and web applications are substituting more of standard desktop solutions every day. With more web applications in use, the question about their security becomes more and more important.

It has become obvious that there are many flaws in web security that can be identified (Scott & Sharp, 2003) which can result in malicious activities in business, education and other areas. Web security becomes one of the most important topics. The need to protect web applications and online accounts became of great priority as the whole systems start to be supported by these kinds of resources.

There are many flaws in Internet applications that can be identified (Konecki, Hutinski & Orehovački, 2007). Among these flaws in this paper we look at the problem of access controls. When talking about this problem the main concern is the need for creation of strong passwords. By strong passwords we consider those that are hard to crack down. It was of our interest to find out how strong passwords that experienced IT users create really are so In this paper we analyze this problem using a number of algorithms that can be found today for password strength determination. We also discuss these results and possible solutions.

2. Password Strength

Password strength is a measurement of the effectiveness of a password as an authentication credential. The strength of a password is a function of length, complexity, and randomness (US-CERT, 2008). Or in simple words the stronger password is the harder it is to crack it down. Algorithms for password strength determination and results of passwords strength analysis will be mentioned in later section of this paper.

The most common way of measuring password strength is “bit strength”, the same method that is used to measure the strength of encryption (NIST, 2006)(Allan, 2004). Bit strength represents total number of permutations in a password. A password with eight-bit strength has 256 possible permutations. When we look at the structure of a passwords than we can see that they are made up of ASCII characters, which include all lower case and uppercase letters, in addition to all numbers and symbols (punctuation included). Although every character on a computer keyboard technically occupies eight bits of space, characters used in passwords never use eight bits of space - they are limited to only 6.5 bits at a maximum (Allan, 2004).

There is one important dilemma that occurs when talking about password creation. If a password is weak then it is easy to remember, but if it is very strong then it is hard to remember and it is usually written down which consequently represents another potential threat (Yee & Sitaker, 2006).

Passwords are the most commonly used type of authentication on the Web but they also have many potential weaknesses and problems (Yee & Sitaker, 2006). There is always already mentioned dilemma between strong and weak passwords. Weak passwords are those that consist of ordinary words or combinations of them with numbers or other words. They are easy to remember but they are very vulnerable to so called dictionary attacks where attacker uses brute force to try guessing the password. Strong passwords are more resistant to this kind of attacks but are hard to remember. Also it is a good practice to change password frequently and to have different passwords for every service and account. This password should not be written down because it presents additional threat but it also puts a heavy burden on user who has to memorize them all and the possibility of forgetting some password or remembering it wrong is not insignificant.

Some guidelines for creation of strong passwords are given below (Microsoft, 2006)(Schneier, 2007)(Google, 2008).:

- Include numbers, symbols, upper and lowercase letters in passwords
- Password length should be around 12 to 14 characters
- Avoid passwords based on repetition, dictionary words, letter or number sequences, usernames, or biographical information like names or dates.

The main enemy of proper authentication is the user itself. Users tend to use a few weak passwords or if they use strong ones, they write them down. Gaw and Felten showed in their study that the major of users used only 3 different passwords and they reused them at least twice (Gaw & Felten, 2006). Users create new accounts but not new passwords.

In spite of a lot of talk about password creation and password strength problem users tend to generate weak passwords. There are however a few methods that administrators can use to enforce better passwords (Spafford, 1992):

- Educate and encourage users to make better choices of passwords.
- Generate strong passwords for users and do not allow them to choose passwords of their own creation. This is often done using some random password generator.
- Check passwords after-the-fact and force users to change those that can be easily broken with a dictionary attack.
- Screen users' password choices and prevent weak ones from being installed.

In order to enhance passwords a term mnemonic passwords has emerged. Users are instructed to create mnemonic passwords following next principles (Kuo, Romanosky & Cranon, 2006):

1. Think of a memorable sentence or phrase containing at least seven or eight words.
2. Select a letter, number, or special character to represent each word in your password. A common method is to use the first letter of every word.
3. Ideally, the password should contain a mixture of lower case and upper case letters, numbers, punctuation, and special characters (such as ^ or %).
4. Remember the phrase.

Example of mnemonic password would be the following. If there is a phrase "Don't fear, you will live for ever" the mnemonic password would be Dfywl4e.

It is commonly believed that mnemonic passwords are better that the ordinary ones for 3 reasons (Kuo, Romanosky & Cranon, 2006):

1. Mnemonic passwords do not appear in any passwords cracking dictionary files.
2. Mnemonic passwords encourage users to use different classes of characters such as punctuation, comma, etc.
3. The list of possible phrases and passwords is practically infinite.

However there is still a lack of empirical knowledge about the strength of these passwords in comparison with ordinary ones.

The main advantage of mnemonic passwords is that they are still not well supported in majority of cracking software and methods but this will certainly change over time if the usage of this kind of passwords becomes common practice.

Besides mnemonic passwords there are also other attempts to improve authentication resistance but most of them showed to be unpractical for widespread use or showed some other flaw. Some alternatives to mnemonic passwords are given below (Kuo, Romanosky & Cranon, 2006):

- Cognitive password authentication selects a set of personal questions upon each logon (Zviran & Haga, 1990). These questions are easy to remember but it is a little too complicated for widespread use. These personal information could be guessed or find out by social engineering.
- Pass-sentences and pass-phrases are textual passwords composed of long, grammatically correct phrases (Spector & Ginzberg, 1994). These personalized phrases are easy to remember but too long for repeated use.
- Randomly generated, human pronounceable passwords are produced by concatenating pronounceable syllables into new "words." Most of these generators (Debian Package, 2008)(Van Vleck, 1997) are based on Morrie Gasser's work (Federal Information Processing Standards Publication, 1993)(Gasser, 1975). Generated passwords are resistant to dictionary attacks but there are some vulnerabilities in the Gasser algorithm itself (Ganesan & Davies, 1994).

3. Study Methodology and Results

In order to find out the habits of experienced IT users in creation of passwords a group of 183 undergraduate students from third and fourth year of study has been selected. In the selected group of undergraduates were student of computer science. 80% of students were males and 20% females. Students have been instructed to form a password without mentioning specific purpose. These passwords have been tested with 3 selected password strength determination algorithms:

1. Google password meter (Google, 2008)
2. Microsoft password checker (Microsoft, 2008)
3. The Password Meter (The Password Meter, 2008)

The results of all 3 algorithms were analyzed and an average result has been created in order to see how much passwords of each strength level there are. All algorithms have given pretty much the same results on all tested passwords with some minor discrepancies. Two of three chosen algorithms gave almost identical results and remaining algorithm gave a slightly more optimistic results that the previous ones. Analysis of these results showed that over 70% of students generate weak passwords and just over 7% of them generated strong passwords for protection of their data. If we analyze results of this research according to gender we can conclude that female students showed higher lever of awareness and need to create strong passwords. Namely, 71.72% of male and 65.78% of female students have generated weak passwords while 6.21% of male and 13.16% of female students generated strong passwords. Results analysis by the year of study showed that the students of third year are more couscous that the students of fourth year. Just a bit over 71% of third year students have generated weak passwords and almost 9% of them have generated strong passwords. On the other hand, almost 70% of fourth year students have generated weak passwords and just a bit over 6% of them have generated strong passwords. Overall presentation of gathered and analyzed data by the gender and year of study is shown in figure 1 and figure 2.

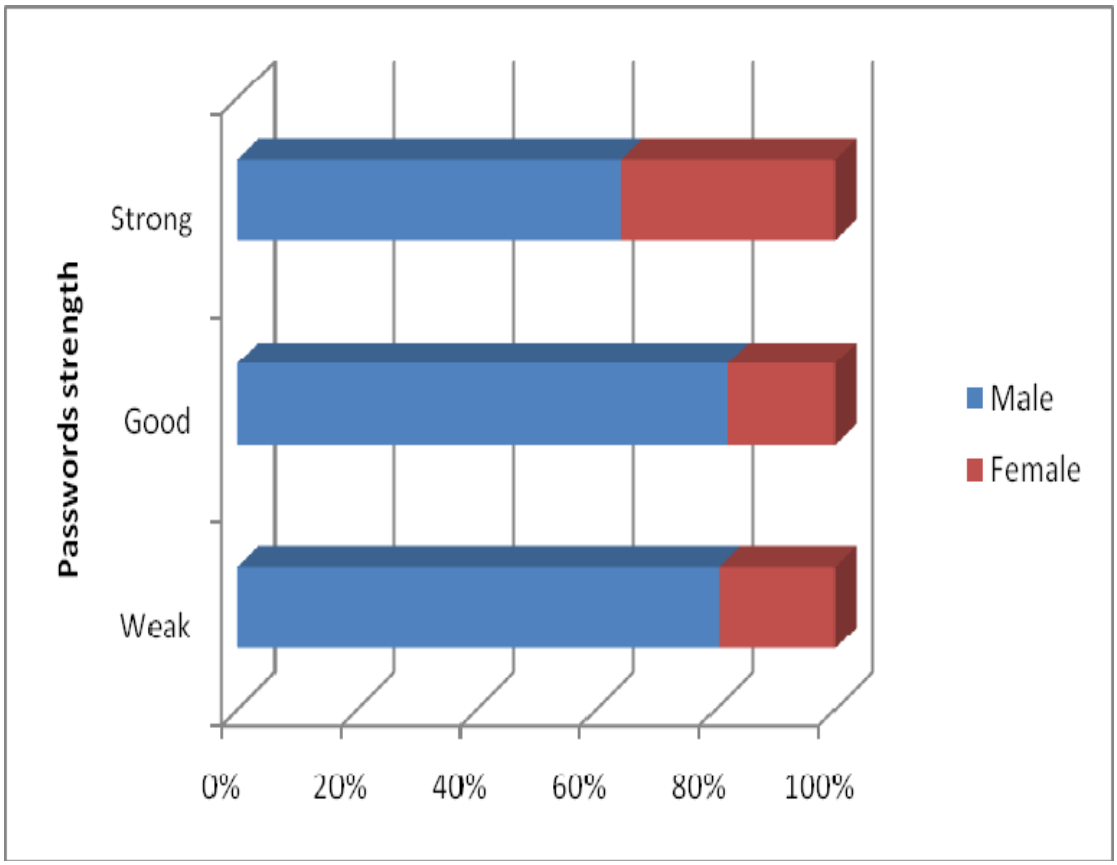

Fig 1. Analysis of data by the gender

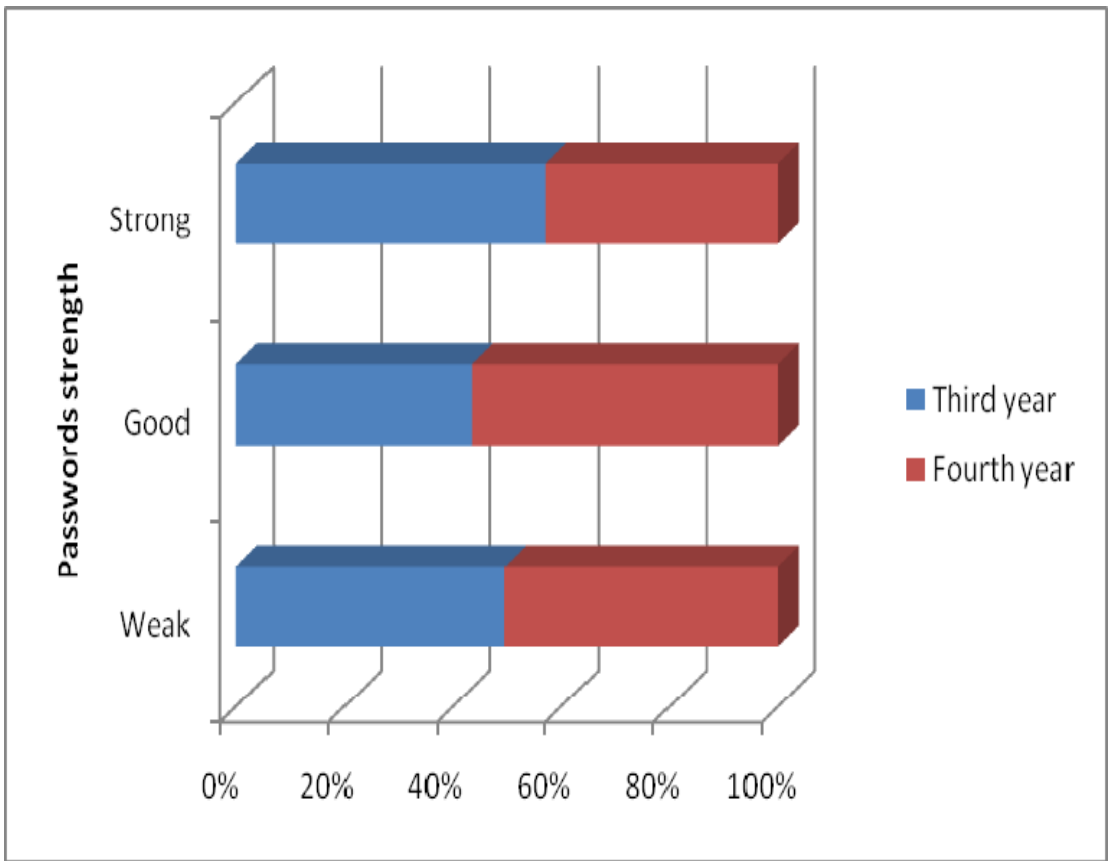

Fig 2. Analysis of data by the year of study

If we analyze gathered data by the most commonly used password attacks we get very disappointing results. Namely, as much as 72.68% of all generated passwords is vulnerable to standard dictionary attacks while 38.25% of passwords would be easily obtained by the usage of social engineering. Finally, mentioned form of mnemonic passwords was used by just 4.37% of students. As in the previous case student of forth year of study showed slightly worse results that the students of third year. From all mentioned it can be concluded that in spite of the fact that the question of security is one of the most actual questions today very few of experienced users care enough about it when dealing with protection of their privacy and security of their own data. Because of that there is a great need to raise awareness about the importance of security and information in users of all profiles to a significantly higher level.

To further test this conclusion we conducted correlation and linear regression tests on gathered data to see if there is any connection between the year of study (x) and quality of created password (y).

Correlation (r) was -0,0114. Negative correlation suggests that higher year students would have weaker passwords but the value of correlations is so small that it practically has no significance. Linear regression y = 2,3671 - 0,0002981 * x shows also very insignificant connection between variables x and y which supports results of calculated correlation. The both tests support conclusion that all experienced IT experts, regardless of the year of the study, showed poor awareness about the need of creating strong passwords for their own protection.

4. Conclusion and Future Work

The problem of creating appropriate passwords is something that is actual and has to be addressed in a proper way. Our research results have shown that even experienced IT users create weak passwords. This brings us to the conclusion that there isn't just a problem with methods and knowledge about strong passwords creation but with awareness about importance of this matter. Experienced IT users certainly know how to create strong passwords and why there are important, but further education and guidance are necessary in the field of the users' perception on this issue.

In our future work we will conduct a more detailed study and will try to classify password strength checking methods and algorithms according to their overall quality. We will research how users react when they are asked to form a password for several different purposes and we will try to see which factors could have influence on better motivation for strong passwords creation.

These future results should teach us and should give us the basic idea of steps that should be performed in order to improve the awareness of IT users about the importance of strong passwords creation. The authentication and security of different systems that contain personal or confidential data will be consequently improved.

5. References

Allan, A. (2004). Passwords are near the breaking point, Gartner Inc., URL: http://www.indevis.de/dokumente/gartner_passwords_breakpoint.pdf, *Accessed:* 2008-05-25

Debian Package: GPW, URL: http://www.mnis.fr/deb30/utils/gpw.html, *Accessed:* 2008-06-02

Federal Information Processing Standards Publication 181, Standard for Automated Password Generator. National Institute of Standards and Technology (1993), URL: http://www.itl.nist.gov/fipspubs/fip181.htm, *Accessed:* 2008-06-02

Google (2008). Password Help, URL: https://www.google.com/accounts/PasswordHelp, *Accessed:* 2008-05-28

Gaw, S. & Felten, E. W. (2006**).** Password management strategies for online accounts, *ACM International Conference Proceeding Series*, Vol. 149, pp. 44 – 55, ISBN: 1-59593-448-0, Pittsburgh, Pennsylvania.

Gasser, M (1975). A Random Word Generator for Pronounceable Passwords. Technical Report ESD-TR-75-97, Electronic Systems Division, Hanscom Air Force Base, 1975.

Ganesan, R. & Davies, C (1994). A New Attack on Random Pronounceable Password Generators. *Proceedings of the 17th NIST-NCSC National Computer Security Conference*,.

Google, URL: https://www.google.com/accounts/NewAccount, *Accessed:* 2008-06-10

Konecki, M.; Hutinski, Ž. & Orehovački, T**.** (2007). Secure web applications?, *Proceedings of 30th MIPRO Jubilee International Convention on Information System*

Security, pp. 162 - 166, ISBN: 978-953-233-031-1, Opatija, Croatia, May 21-25 2007, MIPRO.

Kuo, C.; Romanosky, C. & Cranon, L. F. (2006). Human selection of mnemonic phrase-based passwords, *ACM International Conference Proceeding Series*, Vol. 149, pp. 67 – 78, ISBN: 1-59593-448-0, Pittsburgh, Pennsylvania.

Microsoft (2006). Strong passwords: How to create and use them, URL: http://www.microsoft.com/protect/yourself/password/create.mspx, *Accessed:* 2008-05-26

Microsoft (2008), Password Checker, URL: http://www.microsoft.com/protect/yourself/password/checker.mspx, *Accessed:* 2008-06-10

NIST (2006). *Information Security*, URL: http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf, *Accessed:* 2008-05-25

Scott, D. & Sharp R (2003). Specifying and enforcing application-level Web security policies, *IEEE Transactions on Knowledge & Data Engineering*, Vol. 15, No. 4, pp. 771-783, ISSN: 1041-4347

Schneier, B. (2007). Choosing secure passwords, URL: http://www.schneier.com/blog/archives/2007/01/choosing_secure.html, *Accessed:* 2008-05-26

Spafford, E. H. (1992). OPUS: preventing weak password choices, *Computers and Security,* Vol. 11, No. 3, pp. 273 – 278, ISSN: 0167-4048.

Spector, Y. & Ginzberg, J (1994). Pass-sentence - a new approach to computer code. *Computers & Security*, Vol 13, pp. 145-160, ISSN: 0167-4048.

The Password Meter, URL: http://www.passwordmeter.com/, *Accessed:* 2008-06-10

US-CERT (2008), *National Cyber Alert System*, URL: http://www.us-cert.gov/cas/tips/ST04-002.html, *Accessed:* 2008-05-25

Van Vleck, T (1997). Java Password Generator, URL: http://www.multicians.org/thvv/gpw.html, *Accessed:* 2008-06-02

Yee, K-P & Sitaker, K (2006). Passpet: convenient password management and phishing protection, *ACM International Conference Proceeding Series*; Vol. 149, pp. 32 – 43, ISBN: 1-59593-448-0, Pittsburgh, Pennsylvania.

Zviran. M. & Haga, W.J. (1990). Cognitive Passwords: The Key to Easy Access Control, *Computers & Security*, pp. 723-736, ISSN: 0167-4048.