Research Article

Information Security Management: Password Security Issues

Elda Kuka

Faculty of Economy,
University of Tirana

Prof. Assoc. Dr. Rovena Bahiti

Faculty of Economy,
University of Tirana

Doi: 10.2478/ajis-2018-0045

Abstract

As users of technology in our everyday actions we need to authenticate in different applications, in fast and secure mode. Although passwords are called the least secure mode of authentication, it's the simplicity of entering a textual password for just a few seconds, especially when a fast transaction is needed, the main advantage that textual password based authentication method has against other authentication methods. We have prepared a questionnaire that will help us to identify the practices, characteristics, and problems of creation and usage of passwords in online applications, services and social networks. The target population is a group of users who have knowledge on information technology in public administration.

Keywords: *information security management, password security, textual password, questionnaire*

1. Introduction

Authentication is any protocol or process that permits one entity to establish the identity of another entity (Jadhao & Dole, 2013; Jyoti & Kumar, 2014). Passwords play a large part of the user's authentication experience. Nowadays, each and everyone use many websites and online applications requiring us to create accounts and think up passwords in a hurry. They are the near universal means for gaining access to accounts of all kinds. Email, banks, portals, dating and social networking sites all require passwords (Florencio & Herley, 2007). There are multiple studies on password usage, including people's selection of passwords (Gehringer, 2000), strength and memorability of user chosen passwords (Yan et al, 2004; Kuo et al, 2004) (Florencio et al, 2007), and the number of passwords and accounts users have (Gaw & Felten, 2006; Florencio & Herley, 2007). There are also alternative authentication methods like hardware authentication, but they require an issuing authority and can be implemented in environments that justify the costs of installation and maintenance. Shay et al. say text based passwords are the most preferred method because they do not require extra hardware, the user can type easily and the system developers can implement as well (Shay et al, 2010). Passwords are the most comfortable authentication method because you need just a few seconds to put a password in an online application or service, but are the least secure authentication method. In 2013, Deloitte declared that more than 90% of passwords are possible to be prone of cracking[1]. Global Security Report from TrustWave 2017, states that one of the top factors on data compromise for 2016 are weak passwords (4.7%)[2]

[1] *Deloitte, 2013; https://www2.deloitte.com/ca/en/pages/technology-media-and telecommunications/articles/tmt-predictions-2013.html*

[2] *Global Security Report, TrustWave 2017*

Shay et al., through a survey of 470 students, showed that the students were annoyed when university adopted a new password policy requiring more complex passwords, but at the same time, the students felt more secure (Shay et al, 2010). Singh et al. conducted a qualitative study about how people shared banking passwords with spouses or significant others (Singh et al, 2007). Gaw and Felten interviewed 49 undergraduate students and found that the students had 7.8 accounts on average, with three or fewer passwords (Gaw & Felten, 2006). If we make a general classification of passwords that are generated by a human being, each of these would follow in one of these three categories: word password, non word password, or mixed of both. Non word passwords contain a character set which do not have any meaning such as location, names, etc. so these words cannot be found in the dictionary. Word passwords contain the dictionary words or some modification of them. Mixed passwords are a combination of the first two, so one part has a certain meaning, and the other one has no meaning. The basic policy for creating a password is, “minimum length of 8 characters, maximum length of 14 characters and all visible keyboard keys (except space) are allowed” (Helkala & Snekkenes, 2009). The aim of this paper is to identify practices, characteristics, and problems in creating and usability of passwords by Albanian users; by users we mean individuals who use computer systems, or online application and services including social networks, and they have knowledge on information technology. This paper is organized as follows. On section number two we have described the methodology of this paper. On section three, we make a general presentation of questionnaires results and interpret them performing a comparative analysis. On section four we describe the conclusions and recommendations. As a limitation of this paper, we have taken into our consideration only the visible characters of a QWERTY typical keyboard. This implies there are 26 lowercase and 26 uppercase letters, 10 numbers and 32 special characters.

2. Methodology

For our survey, we have used a questionnaire, about Albanian users’ practices and characteristics in creation and usage of passwords. This questionnaire is used to interview the employees who work in public administration in IT departments, so they have knowledge on information technology issues; they have experience in authenticating in computer systems, online systems and web applications. The questionnaire was developed online through Zoho Survey service. It was written in Albanian language and was developed through the period 01.04.2017-01.05.2017. The questionnaire contained seven questions, out of which 6 were closed questions and 1 was open question. A total of 197 completed questionnaires were obtained, from the target group of 250 users.

3. Analysis of the Results of Questionnaires

As mentioned previously, the questionnaires were used to gather information from users who have a background in information technology issues. Below, we will show the results of each question.

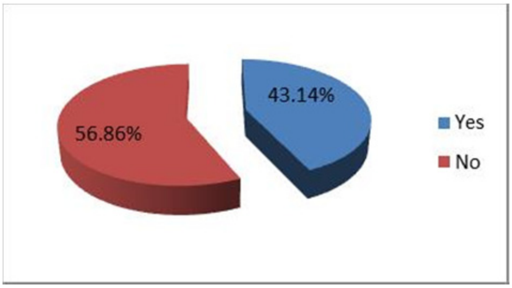

Figure 1: The usage of the same password in different accounts

Based on the figure above, regarding the usage of the same password on several accounts, or different applications, round 57% of the users use different passwords in various applications, but still 43% of them use the same password in different accounts. Considering users' background we see that still for a large number of users is easier to use the same password in multiple accounts.

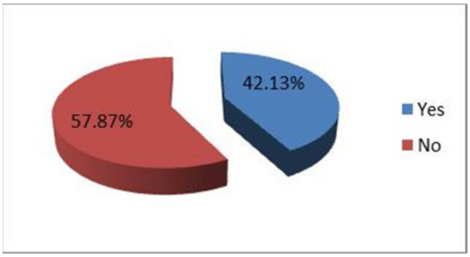

Figure 2: Problems in memorizing or remembering the passwords

The second question dealt with the issue of memorizing or remembering passwords. Only 57.87% of the users do not have problems with remembering the passwords when they type them, while 42.13 % have problems remembering passwords. As we can see from figure nr.1 and, from figure no.2, there is almost the same number of users who use different passwords in different accounts that doesn't have problems in memorizing the passwords.

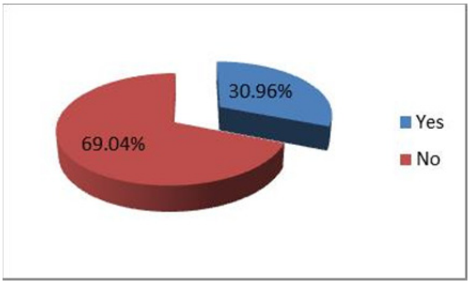

Figure 3: Password sharing at least with another person

Figure no. 3 shows that 69.04% of the users do not share their password with other persons (we haven't asked who this person could be).

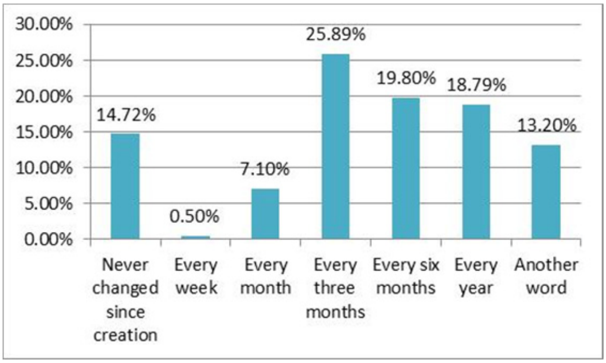

Figure 4: Frequency of password changing

Regarding the frequency of passwords changing passwords, the percentage of the users that change the passwords within, and after three months is higher than the percentage of users who never change their passwords. So, regarding the security policy recommendation that passwords should be changed frequently, it seems that they perform well.

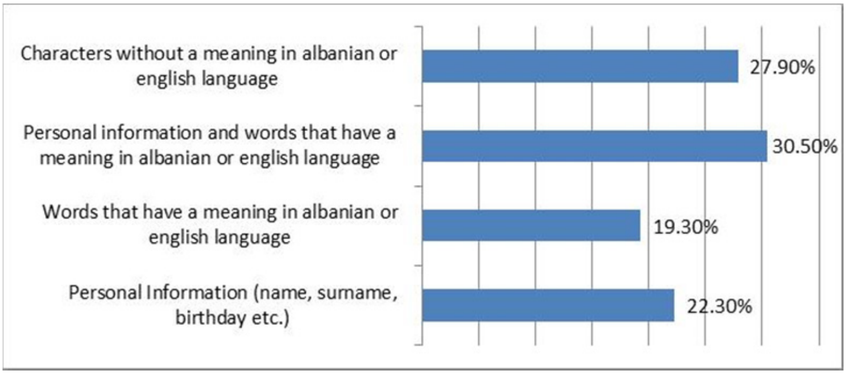

Figure 5: The meaning of the characters in the password

Figure no. 5, shows the results regarding the meaning of characters in the password. The percentage of users who use personal information, and /or words that have a meaning in Albanian or English language is round 72%. This percentage is very high, making them vulnerable as they can suffer a dictionary attack. Only 27.9% uses nor personal information nor characters with a meaning in Albanian or English language.

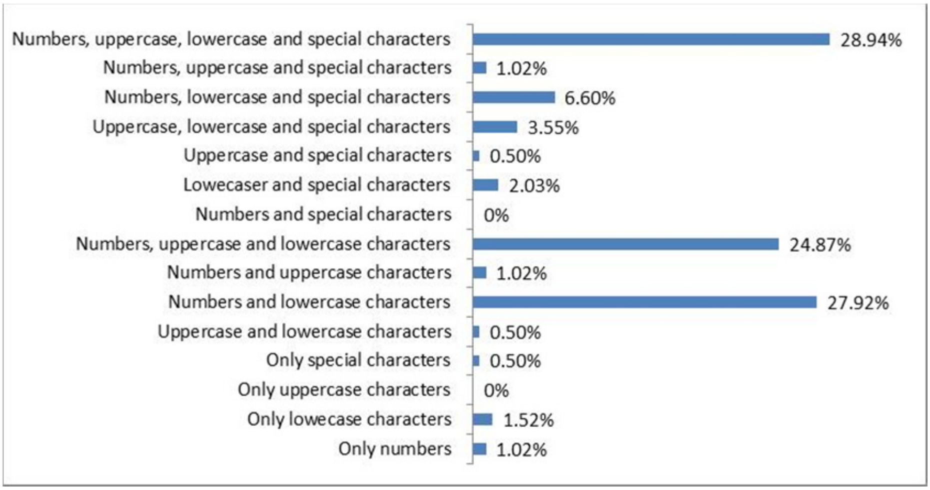

Figure 6: Referring to all your accounts you have, your passwords generally consists of:

Figure no. 6 shows the results when asked about the different kinds of characters that the password is composed of. The results are impressive. The most important figures show that the percentage of the users that use numbers, uppercase, lowercase and, special characters (strong and complex password) is 28.94%, followed by 27.92% that uses numbers and, lowercase characters (fairly strong password) and, 24.87% that use numbers, uppercase and, lowercase characters.

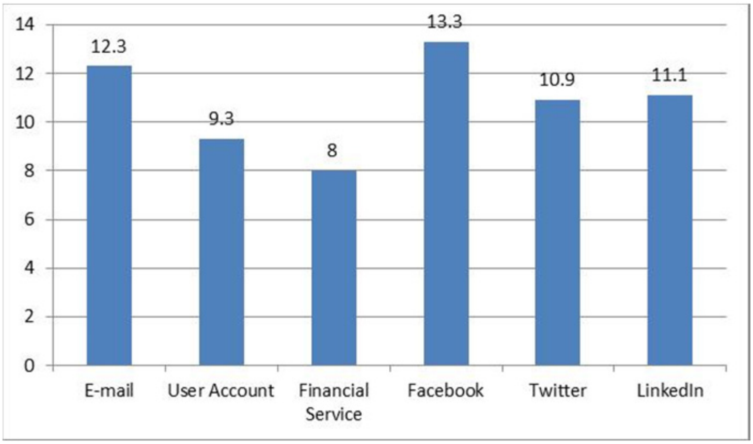

Figure 7: Average length of passwords in characters by different accounts:

Figure no.7 shows the average length of passwords in characters between different accounts we see that the users use long passwords (8 characters or higher long) in each of the accounts.

4. Conclusions and Recommendations

Through this study, we collected and analyzed the responses of users who had knowledge in information technology issues and authenticated themselves in different systems and, social networks. The analyses of the data provided helped us to identify practices, characteristics and problems in creating and usability of textual passwords mode authentication.

References

Florencio D., Herley C., (2007) “A Large-Scale Study of Web Password Habits”, Proceedings of 16th conference “Track: Security, Privacy, Reliability, and Ethics”

Florencio D., Herley C., Coskun B., (2007) “Do strong web passwords accomplish anything?” In Proc. USENIX Hot Topics in Security

Gaw S., Felten E. W., (2006) “Password management strategies for online accounts”. Proceedings of SOUPS

Gehringer E. F. (2002) “Choosing passwords: security and human factors”. In Proc. of ISTAS

Helkala K., Snekkenes E. (2009) “Password generation and search space reduction,”Journal of computers, vol. 4, no. 7.

Jadhao P., Dole L. (2013) “Survey on authentication password techniques,” Internationaljournal of soft computing and engineering (IJSCE) ISSN: 2231-2307, volume-3, issue-2.

Jyoti D., Kumar R. (2014) “Review of Security Analysis and Performance Evaluation of an Enhanced Two-Factor Authenticated Scheme” International Journal of Electrical, Electronics and Computer Engineering 3(1): 218-222(2014)

Kuo C., Romanosky S., Cranor L., (2006) “Human selection of mnemonic phrase-based passwords”. SOUPS

Singh S., Cabraal A., Demosthenous C., Astbrink G., Furlong M., (2007) “Password sharing: implications for security design based on social practice” Proceedings of CHI

Shay R., Kelley P. G., Bauer L., Leon P. G., Christin N., Komanduri S., Mazurek M.L., Cranor L. F. (2010) “Encountring stronger password requirements: user attituedes andbehaviors,” Symposium on usable privacy and security (SOUPS), Redmond, WA USA.

Yan J., Blackwell A., Anderson R., Grant A. (2004) “Password memorability and security: Empirical results”. IEEE Security & Privacy vol. 2 (5) pp. 25-31