IMPACT OF GLOBAL SOCIAL CHANGES ON THE SECURITY OF PASSWORD AUTHENTICATION

Miloslav Hub[1,a,*] and Kateřina Příhodová[2,b]

[1]Faculty of Economics and Administration, University of Pardubice, Studentska 84, 532 10 Pardubice, Czech Republic

[2] Faculty of Economics and Administration, University of Pardubice, Studentska 84, 532 10 Pardubice, Czech Republic

[a]miloslav.hub@upce.cz, [b]st30351@student.upce.cz

*Corresponding author

Abstract. An authentication is the process of verifying the identity with the required degree of assurance. An example might be logging into e-mail inbox when a user firstly enters his username (identification) and his password (authentication). Although, different ways of authentication (biometrics, smart cards…) exist currently, an authentication through passwords is often used because of easy implementation and low financial requirements. But this way of authentication is not generally considered to be too secure because users often choose easy to guess short passwords, divulge theirs passwords to others, remark theirs passwords, and often use the same password for different services. Many existing passwords are not resilient to various forms of attack, such as a dictionary attack or brute force attack that also has relatively high economic impacts. However, due to globalization, there are significant social changes that affect the passwords that end users choose and therefore their security. At this time, users are choosing other passwords than they used to, such as choosing English terms for their passwords, using other mnemonic tools, and so on. The goal of this paper is to evaluate the password authentication security from the globalization point of view with respect to the ability of end users. Through the proposed dictionary attack and brute force simulation model, the attacks on the passwords that were acquired over the last fifteen years will be carried out and the impact of globalization on their security will be analysed.

Keywords: global social changes; security; authetication; passwords; dictionary attack; brute force attack

JEL Classification: L86

1. Introduction

At times when the Internet was a purely academic network, it was unthinkable that anyone would try to gain access to data that was not intended for him or to fraudulently impersonating anyone else. At that time, users knew each other and therefore trusted each other. The turning point came when the commercial sphere was gaining access to the Internet. The number of users increased sharply, including those who did not have the purest intentions. The Internet has become anonymous and is currently accessible to almost anyone. Nowadays, internet is used by both commercial sphere and non-commercial sphere, an example is municipal institutions, that also which also emphasize security (Fuka et al., 2016). With the increase of the number of users, the number of data and thus their aggregate value also increases. Anonymity allows users to perform actions that are contrary to "morality" without the possibility of finding the originator. The problem of anonymity is therefore addressed through identification and authentication. While identification is the assertion of an entity (user, process, etc.) about its identity, authentication is the process by which it can be validated or disproved by appropriate means of identity.

Although there exists a different types of authentication (Barkadehi et al., 2018), there exist three basic authentication methods that are distinguished:

- knowledge authentication (passwords, PINs,…);
- authentication through an authentication thing (smart cards, tokens,…);
- biometric authentication (iris scanning, finger print,…).

Although many mature authentication mechanisms exist (for example smart cards, biometrics), currently passwords are still used for these purposes (AlAzzazi & Sheikh, 2007), (Shieh et al., 2007), (Lee et al., 2008), (Juang & Greenstein, 2018), (Luo et al., 2019). The reasons of passwords using are low expenses and easiness of implementation.

Due to the fact that impostors are always looking for new ways on how to get access to protected accounts, many factors that influence password authentication security exist. A lot of authors frequently discuss about the factors that influence password security, for example: length, randomness, and the period the password is used. However, it is certain that the password security has a strong influence on the user's behavior, both when choosing a password and managing it (Hub, 2015), (Kusyanti & Sari, 2017). Conversely, overly secure passwords can put excessive demands on users (Hub et al., 2010), (Woods & Siponen, 2018). That's why you have great new authentication as intuitive graphical passwords (Mahey et al., 2018).

Some authors are trying to make a distinction between a “weak” and a “strong” password, commonly by using an expert’s opinion (Burnett & Kleiman, 2006), (Furnell, 2007), (Farrell, 2008), (Erguler, 2016), (Li et al., 2017), (AlSabah et al., 2018). Other authors are trying to break passwords, and the results of their experiments are present as a proof of the passwords weakness (Klein, 1990), (Garrison, 2008), (Tatli, 2008). The alternative way is to create a mathematical model of a password attack that results in value of a password security (Tukey, 1962), (Shay & Bertino, 2009), (Rass & König, 2018).

2. Research question

Globalization affects many things (Mudambi, 1998). Already in 2003 a hypothesis about the impact of globalisation to passwords selection was formulated (Hub, 2003, A). This hypothesis was then discussed somewhat fuzzily and not very concretely. The aim of the paper is to analyse the long-term trend of choice of passwords by end users and to discuss the effects of global social trends on this trend. At the same time, further development of changes in the behaviour of end users in the choice of password and impact on the security of information systems will be predicted.

3. Methodology

The following steps were set to achieve the goal of this paper:

1. To conduct exploration data analysis on passwords gathered in the past
2. To conduct rigorous quantitative evaluation of security of passwords gathered in the past.
3. To gather appropriate amount of passwords in 2018.
4. To conduct exploration data analysis on passwords gathered in 2018.
5. To conduct rigorous quantitative evaluation of security of passwords gathered in 2018.
6. To compare security of passwords gathered in 2018 and in the past.
7. To discuss results and to formulate conclusions.

As the past data the dataset collected in 2005 (Hub, 2005) respectively dataset collected in 2008 (Hub & Čapek, 2011) will be used. The new dataset will be collected from the beginning in 2018 by the same manner as past datasets that will making it possible to compare each other.

Exploration data analysis (EDA) represents procedures for analysing data, techniques for interpreting the results of such procedures, ways of planning the gathering of data to make its analysis easier, more precise or more accurate, and all the machinery and results of (mathematical) statistics which apply to analysing data (Tukey, 1962). During exploration data analysis especially length of passwords, type of passwords and correlation between characters in passwords and general Czech texts will be analysed. This gives us an idea of the long-term trends of password choice.

As a measure of security of a given password the expected value of the number of attempts an attacker has to carry out to break the password *S(p_i)* will be used (Hub & Čapek, 2009) (see Eq. 1).

$$S(p_i) = \frac{N_i + 1}{2} + \sum_{j=1}^{i-1} N_j \qquad (1)$$

where:

$S(p_i)$ ... Security of a password *p* that is a word from *i*-th reduced dictionary.

i.......... The order of the reduced dictionary that contains a password *p*.

N_i .... The size of the *i*-th reduced dictionary.

It must to be noted, that the creation of reduced dictionary is created on the base of its success rate *SDA(d)* (see Eq 2) and is detailed descripted in (Hub & Čapek, 2009).

$$SDA(d) = \frac{NBP_d}{N_d \cdot NP} \qquad (2)$$

where:

SDA(d) Success rate of the dictionary attack on dictionary *d*.

NBP_d.. The number of passwords that would be broken by dictionary *d*.

N_d....... The size of dictionary *d*.

NP...... Total number of tested passwords used in the attack simulation.

4. Results

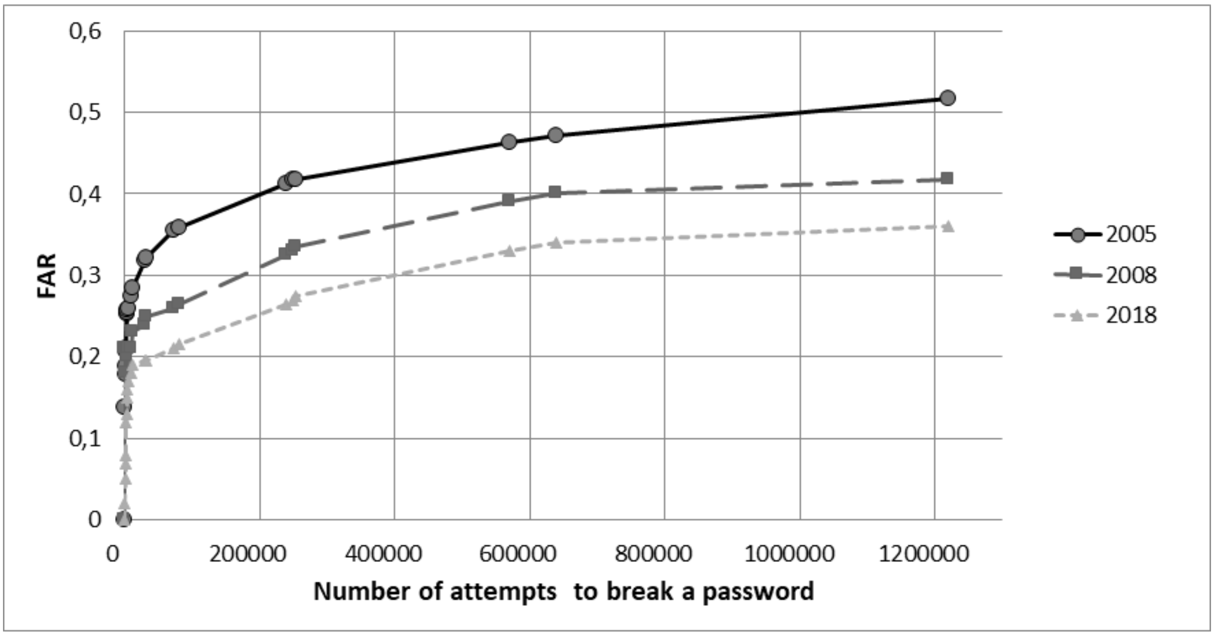
In the past, the first set of 2,958 passwords was collected during 2005 (Hub, 2005) (in fact, the first collection was conducted in 2003 (Hub, 2003, B), but because of small amount of data, this study can not be used for a comparison). All users who choose passwords were native Czech speakers. The requirements for password choosing was:

- the password had to contain one character at minimum;
- maximum length of the password was not restricted;
- users had no time limit when choosing a password;
- a password could contain arbitrary characters typed using a Czech keyboard.

The second set of 1,895 really used passwords was collected in 2008 (Hub & Čapek, 2011). For a better, more convenient comparison of both studies, the requirements were exactly the same.

Because of the aim of this paper is to study long-time trends in a password choosing, new data were collected between January – May 2018. The requirements to a password choosing were exactly same. During this period totally 1,048 passwords were chosen.

Figure 1: Security of passwords collected in different periods



The passwords collected in different periods were inserted to dictionary attack and brute-force attack model and given values were compared (see figure 1). This result for example says that any password in 2018 were possible to break with probability approximately 0.3 after 400,000 attempts.

5. Conclusion

The passwords used in 2018 are more secure against dictionary and brute-force attack than passwords used in 2005 and 2008 respectively. When looking at the passwords in more detail, there is a trend in the use of foreign words such as passwords or parts of them. Users increasingly choose foreign terms, foreign-language names for their passwords, increasing the set of candidate passwords a potential attacker has to test. In this respect, global social change has a positive impact on password authentication in this case. Of course, it is important to keep in mind that these global social changes will also be adapted by attackers who are likely to adjust the list of dictionaries used during dictionary attacks.

Acknowledgment

This article was supported by projects No. SGS_2018_021 of the University of Pardubice.

References

[1] AlAzzazi, A. and Sheikh, A. E. (2007). Security Software Engineering: Do it the right way, *Proceedings of the 6th WSEAS Int. Conf. on Software Engineering, Parallel and Distributed Systems*, Corfu Island, Greece, pp. 19-23.

[2] AlSabah, M., Oligeri, G., Riley, R. (2018). Your culture is in your password: An analysis of a demographically-diverse password dataset. *Computers & security*, volume: 77, pages: 427-441. ISSN: 0167-4048.

[3] Barkadehi, M. H., Nilashi, M. Ibrahim, O., Fardi, A. Z. and Samad, S. (2018). Authentication systems: A literature review and classification. *Telematics and Informatics*, Volume 35, Issue 5, Pages 1491-1511. DOI: 10.1016/j.tele.2018.03.018.

[4] Burnett, M. and Kleiman, D. (2006). *Perfect Passwords*. Rockland, MA: Syngress Publishing. p. 181. ISBN 1-59749-041-5.

[5] Erguler, I. (2016) Achieving Flatness: Selecting the *Honeywords from Existing User Passwords. IEEE* transactions on dependable and secure computing, vol. 13, issue 2, p. 284-295. ISSN 1545-5971.

[6] Farrell, S. (2008). Password policy purgatory. *IEEE internet computing*, volume: 12, issue: 5, pages: 84-87. ISSN: 1089-7801.

[7] Fuka, J., Kubíková, Z., Brodský, Z. (2016). Role of Municipal Police in Providing of Security in Selected Municipality in Czech Republic. In *Proceedings of the 28th International Business Information Management Association Conference*. Norristown: International Business Information Management Association-IBIMA, p. 1636 - 1643. ISBN 978-0-9860419-8-3.

[8] Furnell, S. (2007). An assessment of website password practices. *Computers & security*, volume: 26, issue: 7-8, pages: 445-451. ISSN: 0167-404

[9] Garrison, Ch. P. (2008) An Evaluation of Passwords, *On line CPA Journal*, May, Accesable http://www.nysscpa.org/cpajournal/2008/

[10] Hub, M. (2003a). Bezpečnost znalostní autentizace. *Sborník příspěvků 3. mezinárodní konference doktorandů Partipácia doktorandov na vedecko-výskumnej činnosti,* p. 53-57. Bratislava. ISBN 80-225-1700-3.

[11] Hub, M. (2003b). Vliv globalizace na aplikaci znalostní autentizace. *Sborník příspěvků z 13. mezinárodní konference Podnikání globalizace etika*, p. 40-42. Pardubice. ISBN 80-903188-3-5.

[12] Hub, M. (2005). *Bezpečnost informací – autentizace*. Pardubice: University of Pardubice, 2005. ISBN 80-7194-825-X.

[13] Hub, M. (2015). The Password Authentication from the User's Perspective. *Proceedings of The 26th International Business Information Management Association Conference.* Madrid, Spain: International Business Information Management Association (IBIMA). November 11-12. p. 375-383. ISBN: 978-0-9860419-5-2.

[14] Hub, M. and Čapek, J. (2009). Method of Password Security Evaluation. *The 8th International Symposium on Distributed Computing and Applications to Business, Engineering and Science.* [s.l.] : [s.n.], p. 401-405. ISBN 978-7-121-09595-5.

[15] Hub, M. and Čapek, J. (2011). Security Evaluation of Passwords Used on Internet, *Journal of Algorithms & Computational Technology,* Vol. 5 No. 3. p. 437-450. ISSN 1748-3018.

[16] Hub, M., Čapek, J., Myšková, R. and Roudný, R. (2010). Usability versus security of authentication. *International Conference on Communication and Management in Technological Innovation and Academic Globalization (COMATIA '10).* Tenerife: WSEAS Press, p. 57-61. ISBN 978-960-474-254-7. ISSN 1792-6718.

[17] Juang, K., Greenstein, J. (2018). Integrating Visual Mnemonics and Input Feedback With Passphrases to Improve the Usability and Security of Digital Authentication. *Human factors*, vol. 60, issue 5, p. 658-668. ISSN 0018-7208.

[18] Klein, D. (1990). Foiling the cracker - A Survey of, and Improvements to, Password Security. *Unix Security Workshop II,* USENIX Association.

[19] Kusyanti, A and Sari, Y. (2017). Creating and Protecting Password: A User Intention. (IJACSA) *International Journal of Advanced Computer Science and Applications,* Vol. 8, No. 8, 2017.

[20] Lee, Y. C., Hsieh, Y. C. and You, P. S. (2008). A New Improved Secure Password Authentication Protocol to Resist Guessing Attack in Wireless Networks, *Proceedings of the 7th WSEAS Int. Conf. on Applied Computer & Applied Computational Science (ACACOS '08),* Hangzhou, China, pp. 160-163.

[21] Li, Y., Wang, H. and Sun, K. (2017). Personal Information in Passwords and Its Security Implications. *IEEE transactions on information forensics and security*, vol. 12, issue 10, p. 2320-2333. ISSN 1556-6013.

[22] Luo, W., Hu, Y., Jiang, H and Wang, J. (2019). Authentication by Encrypted Negative Password. *IEEE transactions on information forensics and security,* vol. 14, issue. 1, pages: 114-128. ISSN 1556-6013.

[23] Mahey R., Singh N., Kumar C., Bhagwat N. and Verma P. (2018) Graphical Password Using an Intuitive Approach. *International Conference on Intelligent Computing and Applications*. Advances in Intelligent Systems and Computing, vol. 632. Springer, Singapore. DOI https://doi.org/10.1007/978-981-10-5520-1_15

[24] Mudambi, R. (1998). Technology, globalisation and economic performance. *Journal of management studies*, vol. 35, issue 5, p. 690-692. ISSN 0022-2380.

[25] Rass, A. and König, S. (2018). Password Security as a Game of Entropies. *Entropy*, 20(5), 312; https://doi.org/10.3390/e20050312

[26] Shay, R., Bertino, E. (2009). A comprehensive simulation tool for the analysis of password policies. *International journal of information security*, volume: 8, issue: 4, pages: 275-289. ISSN: 1615-5262.

[27] Shieh, W. G. and Wang, M. T. (2007). An improvement on Lee et al.\'s noncebased authentication scheme. *WSEAS Transactions on Information Science and Applications*. Vol.1, WSEAS Press, pp. 832-836. ISSN 1790-0832.

[28] Tatli, E. I. (2008). Cracking More Password Hashes With Patterns, *IEEE transactions on information forensics and security*, volume: 10, issue: 8, pages: 1656. ISSN: 1556-6013.

[29] Tukey, J. W. (1962). The Future of Data Analysis. *The Annals of Mathematical Statistics*, Volume 33, Number 1, p. 1-67. The Institute of Mathematical Statistics. ISSN 0003-4851.

[30] Woods, N. and Siponen, M. (2018). Too many passwords? How understanding our memory can increase password memorability. *International Journal of Human-Computer Studies*. Volume 111, p. 36-48. https://doi.org/10.1016/j.ijhcs.2017.11.002.