SCIENTIFIC JOURNAL OF POLISH NAVAL ACADEMY
2019 (LX) 2 (217)

sciendo

DOI: 10.2478/sjpna-2019-0010

USING GAMIFICATION AND FEAR APPEAL INSTEAD OF PASSWORD STRENGTH METERS TO INCREASE PASSWORD ENTROPY

Przemysław Rodwald

Polish Naval Academy, Faculty of Navigation and Naval Weapons, Śmidowicza 69 Str., 81-127 Gdynia, Poland; e-mail: p.rodwald@amw.gdynia.pl; ORCID ID 0000-0003-4261-8688

ABSTRACT

It is very common for users to create weak passwords. Currently, the majority of websites deploy password strength meters to provide timely feedback. These meters are in wide use and their effects on the security of passwords have been relatively well studied. In this paper another type of feedback is studied: a gamified approach supported by fear appeal. In this approach, users are encouraged to make passwords stronger through the use of visual and textual stories. This approach is supported by data-driven suggestions about how to improve password security as well as by fear appeal. To prove the effectiveness of this gamified password creation process, an experiment was performed in which users changed their passwords in two ways: without any feedback, and with gamified feedback with fear appeal. To support the initial findings a questionnaire was completed by participants at the end of research.

Key words:
gamification, passwords, computer security, education.

Research article

INTRODUCTION

The traditional use of usernames combined with passwords is still the most widespread method of authentication [2]. The popularity of this technique is based on at least four factors: it is easy to implement, it requires little or no effort for users to become accustomed to it, it is cheap or even free, and passwords are 'portable'. Thus, password-based authentication will undoubtedly remain the predominant security mechanism for the foreseeable future, although some companies are trying to develop new solutions [33]. Over the last few years various alternative authentication mechanisms have been proposed. Examples include picture gesture authentication [29], graphical passwords [30], biometric authentication, mobile authentication [44], multi-factor authentication [12]. Other new web authentication techniques are also currently under development [48]. However, passwords are still most common and day by day widely reproduce among new web sites.

Unfortunately, for years users have had the tendency to choose weak passwords [1]. Passwords that are easy to remember but easy to guess (by attackers) as well. Users additionally re-use passwords across multiple sites; this means that if passwords are leaked from one site, attackers can effortlessly gain access to another sites for users who reuse their passwords. One challenge is how to successfully encourage users to choose strong passwords. Strong passwords have particular attributes: appropriate length, composition rules, is not on the list of most popular passwords, is not a dictionary word, cannot be found in publicly available data breaches [39]. In the 'perfect digital World' users should have truly random, long, unique passwords. But in the 'real World' users choose predictable passwords [27] which are easy to remember. That is why a password creation process is often a kind of trade-off between security and usability.

Additionally, regular data breaches have been observed in recent years. Such leaks of credentials are not limited to only 'small' websites: Yahoo [49], Dropbox [40], Adobe [36], MySpace [41], LinkedIn [43], Uber [35] are the best examples of some 'big' ones. Apart from losing private access to compromised sites, a much broader risk is caused by the habit of reusing passwords across many websites [5, 22, 34]. Some online services try to mitigate the risk of password reusage by enhancing the authorization process. Beyond 'something you know' (users' passwords), implement 'something you have' (users' device profiles) or 'somewhere you are' (users' physical locations) mechanisms [34]. However, passwords are still the first line of defence.

This article presents a new approach to password creation. In this approach users are encouraged by a gamified cartoon and a text story; data-driven suggestions of how to make a password stronger are presented and the time it would take a hacker to crack the password is displayed to frighten users. The structure of this paper is as follows. After the introduction, an overview of related work and background information on entropy, password meters and gamification are presented. Next, the proposed system is described. In the main part of this paper the experiment is described, and the results are presented. The results are supported by a survey. Finally, conclusions and areas of further research are indicated.

RELATED WORK

Entropy

One of the most influential documents about password strength estimation and many other password policies is the NIST Electronic Authentication Guideline SP-800-63-2. The second revision of this paper, dated August 2013 [46] (now superseded by the third revision [39], dated June 2017), covers the notion of measuring password entropy. The idea behind NIST's proposal is based on the Shannon's theory [19]. Information theory, according to Shannon, is based on a measure of the amount of information that is random due to random variables. In terms of the probability distribution function, most often this randomness or information entropy is expressed using the following equation:

$$H(X) = -\sum_{X} P(X = x) \log_2 P(X = x), \quad (1)$$

where $P(X = x)$ — the probability that the variable X has the value x.

Transferring this equation (1) to password entropy [20], if a password of size a characters is chosen at random from an alphabet of n characters (for example: 62 for all English lower and upper-case letters with digits; 94 for standard ISO characters on a typical keyboard) then the entropy of the password is ns. Two examples: a) for a password composed of 10 letters only (lower and upper) the entropy is calculated as 52^{10}, which could be estimated to 2^{57}, i.e. the password has 57 bits of entropy; b) for a password composed of 8 characters from a 94-character alphabet, the entropy is equal to 9^{48}, which could be estimated to 2^{52}, i.e. the password has 52 bits of entropy. For randomly chosen passwords the equation (1) could be transformed

to the formula $\log_2(n^s)$. However, users rarely use truly random passwords, therefore scoring passwords based on this formula is useless in the real world. NIST developed a formula to roughly estimate password entropy not for random passwords but for passwords selected by users [46]. The entropy for the full keyboard alphabet is calculated according to the rules given in the original NIST paper: the entropy of the first character is taken to be 4 bits; the entropy of the next 7 characters are 2 bits per character; for the 9th through the 20th character the entropy is taken to be 1.5 bits per character; for characters 21 and above the entropy is taken to be 1 bit per character; a bonus of 6 bits of entropy is assigned for a composition rule that requires both upper case and non-alphabetic characters and a bonus of up to 6 bits of entropy is added for an extensive dictionary check. Such an estimation of password strength used to be adopted by many password meters.

Weir at al [26] showed that NIST's entropy measure does not provide a valid metric for measuring the security provided by password creation policies. The existence and effectiveness of password-cracking tools, such like Hashcat [37] or John the Ripper [45], leads to scenarios in which the probability of success in breaking a password is far from what NIST's entropy predicts [6]. Some passwords that appeared strong on meters based on NIST's entropy are broken relatively quickly by password--cracking software. It seems that modern and reliable password strength meters must take breaking difficulty into consideration. The number of guesses required to crack a password is often a more accurate metric of password strength than entropy [14].

Even though NIST's approach is not perfect and a few other entropy measure strategies have been developed, for example Bonneau's predictor [3], a technique that simulates adversarial guessing using artificial neural networks [15], or Castelluccia's adaptive password-strength meter [31], in this paper NIST entropy is used as a simple and fast way to compare the strength of passwords.

Password meters

One of the most popular mechanisms that has been adopted by many web-services and which helps and encourages users to choose stronger passwords is a proactive password checker. The most popular way to implement such a mechanism is with a bar. Such a bar grows and/or changes colour (most often from red to green) to categorize password as weak, medium or strong. The only aim of such a bar, often called a password strength meter, is to motivate users to create stronger passwords.

Among studies of password meters some findings are worth underlining, the most important of which is that password meters make passwords stronger. Ur at al. [24] tested 14 password meters during 2.931 password creation sessions and found that meters with a variety of visual appearances caused users to create longer passwords. Edelman at al. [9] observed that the presence of password meters yielded significantly stronger passwords. Instead of forcing users to choose stronger passwords by the use of strict policies, a better approach is to provide feedback of the quality of the typed password. Users who see meters, no matter what type, colour, segmentation, size, etc. tend to create stronger passwords. But password meters could mislead users among different sites by their inconsistences [4]. A password can be classified as strong by one password meter and as weak by another. Additionally, password meters do not always follow the guidelines and policies presented on the webpages. Such inconsistencies include differences in meters/policies between account creation page and password reset page, lack of precision in recommendations/hints provided to users, or incompatibility between guidelines and effective password evaluation [10]. Research [24] indicates that only stringent meters based on scoring algorithms make passwords more resistant to password-cracking algorithms. In this study a password strength meter will be replaced by gamified story.

Feedback

One of the most important aspects of the password creation process is feedback on why a password is weak and what should be done to improve its strength. Password meters are helpful in this area but are not sufficient. Researchers have found that a data-driven meter with detailed feedback leads users to create more secure and, just as importantly, passwords that are equally memorable [23]. Furthermore, NIST's current publication requires that users who select a blacklisted password should be advised to select another one: 'If the chosen secret is found in the list, the CSP or verifier SHALL advise the subscriber that they need to select a different secret' [39]. This advisory part, which is provided by text feedback in a password create/change form, has a positive effect on password strength [24]. Users react positively to the text feedback, the content of which should be tailored to the user's behaviour [32]: discourage users from using blacklisted passwords, discourage users from just adding digits or symbols to the end of the password, etc. On the other hand, this textual advice should not overwhelm users with too much

information. If a large amount of text with many suggestions, warnings or hints is displayed, users might even not read it. The balance between the amount of information and its utility should be preserved.

An interesting type of feedback is fear appeals — messages that are intended to increase the perception of a threat and one's ability to cope with it [25]. Such a fear appeals have two main components: a) statements suggesting an imminent threat, and b) statements recommending a certain course of action, including encouragement of one's ability or efficacy to follow the recommended course of action [13]. Vance at al. found that while interactive password strength meters and static fear appealed treatment are not effective, the interactive fear appeal treatment resulted in significantly stronger passwords.

In our system text feedback composed of two elements is proposed. The first text element is responsible for providing gentle suggestions on how to improve password strength. The second suggests a threat — the time it would take a brute-force attack to break a password.

Gamification

Gamification, defined as a usage of game-design elements in non-gaming contexts [7, 8], has been a hot topic over the last few years. Increasing user engagement and enhancing positive patterns are desirable in many areas including marketing, education, recruitment, etc. The effects are greatly dependent on the context in which the gamification is being implemented, as well as on users [11]. Some of the most popular gamification mechanisms are points, leader boards, badges, levels, and stories/themes.

The use of gamification or something similar during password creation process is not new. For example, Sotirakopoulos [21] and Egelman at al. [9] investigate if peer pressure motivators stimulate users more effectively than other types of existing motivators (like password meters) in creating stronger passwords. They use a type of leader board on which a password is compared to other passwords in the system. Seitz and Hussmann propose a game in which players score points by rating the strength of passwords accurately under time pressure [18].

Points or levels are quite similar to simple password meters. The more points a password is awarded, the greener the meter is. The most promising and challenging gamified element is based on a story or some theme, therefore a five-level story with a graphical theme selected by the user is used in the proposed system.

GAMIFIED PASSWORD CHANGE SYSTEM

System design

For the purpose of this study a system responsible for changing passwords was designed and implemented. A simple form of this system, with the typical inputs of a password change form, is presented in fig. 1. In this system the only restriction for the password is minimum length (8 characters). Users do not receive any other information or suggestions about the password.

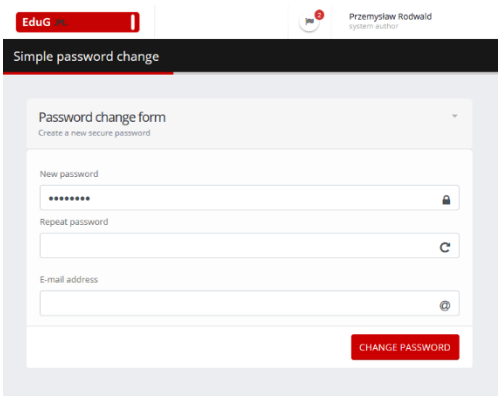

Fig. 1. Simple password change form (tablet view)

An advanced form of this system, referred to as the gamified form, is presented in fig. 2. The system consists of three elements: a graphic theme, a password change form (the same as in fig. 1) and a secure password guide.

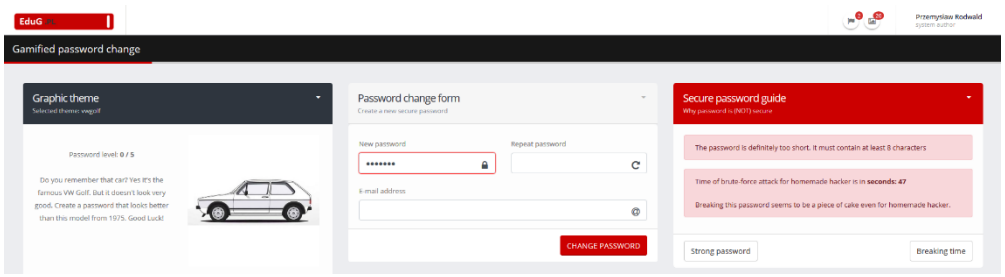

Fig. 2. Gamified password change form (desktop view)

The most significant element, the gamified part (the so-called graphic theme) consists of three elements: the indicator of password strength (from 0 to 5), a text

comment encouraging a stronger password, and the corresponding graphic element. A few sample graphic stories are presented in fig. 3.

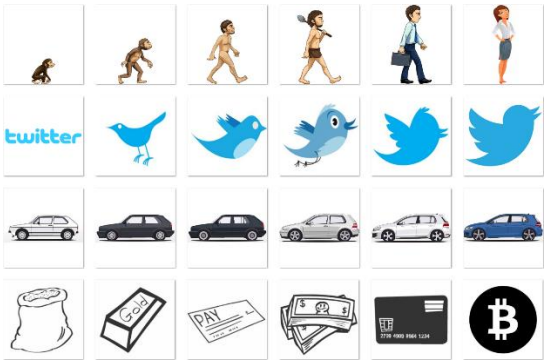

Fig. 3. Sample graphic stories from the gamified password system

When working on the secure password guide part, after studies of many password checkers some factors were selected and taken into account in our system: more obvious ones include checking password length and character complexity; more sophisticated ones include repetitions of chars (aaasss111, mkomkomko), easy keyboard sequence (qwerty, 1qazxsw2), or leet transformations (letter S can be replaced by 5 or $). And finishing with diversity of datasets: popular dictionaries used by hackers (popular words, names, surnames), large database of password leaks (API provided by pwnedpasswords.com [42]). To avoid overwhelming users with too much information about password security, at most three warnings/suggestions are presented. For example, when a password is too short, not complex enough, consists of repetitions, exists in a database of popular words, exists in leaks, only the three most important pieces of feedback information are provided.

A separate box provides information about the time required to break a password by a brute-force technique. For time estimation the SHA-256 cryptographic hash function is used. Although hashes from the MD/SHA cryptographic hash function family are no longer recommended for password storage [17], they are still one of the most common forms of storing passwords on websites [47]. Time is estimated under the assumption that a homemade attacker with a single GPU (graphics processing unit) like the *Nvidia GTX 1080 Ti* is able to check 5 billion ($5x10^9$) passwords per second; a professional hacker/cryptominer with a dedicated hardware solution (for example *AntMiner S9* [38]) is able to check up to 14 trillion ($14x10^{12}$) passwords per second.

Participants

Participants were recruited from the students of two universities: WSB University in Poznań (group 1) and the Polish Naval Academy in Gdynia (group 2). Group 1 contains 116 civilian students aged 20–22 from studies in the faculty of defence at WSB University. Group 2 consists of 50 students (40 civilian, 10 military) aged 20–21 who had already taken part in the course 'Security of IT systems'. It is worth mentioning that students from group 2 took password change sessions after a dedicated lecture about password security. During the lecture the following topics were discussed: evolution of password storage (from plaintext, through MD/SHA family hash functions, mechanisms that increase the security of hashes like salting and incrementing a number of hash calculations, to adaptative functions like PBKDF2, bcrypt, ARGON2, scrypt); password breaking techniques (brute-force, dictionary, hybrid attacks); software for password breaking (Hashcat, John the Ripper); password leaks; suggestions on how to create a strong password (mnemonics, passphrases). Students from group 2 can be considered as having a good understanding of the topic.

Study design

We performed a user study to test the effectiveness of our gamified proposal with comparison to a simple password change form. The study was divided into three separate parts: session 1 (simple form), session 2 (gamified form), and questionnaire. During session 1, participants were asked to change a password in the simple form (available at edug.pl/password.php?form=norm&lang=en) presented in fig. 1. For participants from group 1 this was not changing a 'real' password. During the test a lecturer explained that they should treat this system as an educational web system that requires login (not banking, not e-mail). As an e-mail they are not obliged to provide real data. The students from group 2 use the edug.pl system as part of their daily routine during classes, therefore for them this password changing was real. As an e-mail address they had to provide real data existing in the system database. After session 1 participants were asked again to change a password but this time in the gamified form (available at edug.pl/password.php?form=game&lang=en) presented in fig. 2. They were introduced by the lecturer that they could select a graphic theme and that during the typing of the password two blocks of information would be presented: suggestions about password security and the time it would take to break the password.

Students were informed that during both sessions, passwords (as plaintexts) would not be stored, but some characteristics would be collected (password entropy, password length, password complexity, breaking time).

Questionnaire

Participants evaluated their experience in a questionnaire immediately after the gamified password changing session. The questionnaire consists of five questions. Question 1: 'The password created by you in the gamified system in comparison to the password created by you in the simple system was: a) stronger, b) the same, c) weaker?'. Question 2: 'How and which graphic theme did you choose (select it)?', which had two possible answers: a) 'I remained at the randomly chosen motive', b) 'I chose the theme myself'. All themes are presented in fig. 4.

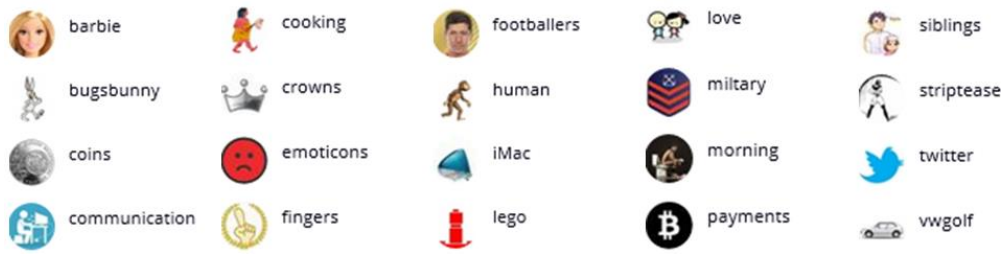

Fig. 4. Themes in the gamified system

Question 3: 'What element had the greatest impact on you when building your password?', which had three answers: a) 'the desire to see the next pictures (comments) in the selected theme', b) 'comments about the strength of the password', c) 'the time it would take to break the password'. Question 4: 'Is the gamified approach more effective in building a strong password in comparison to the classic password meters on many websites?', which had three simple options: a) 'yes', b) 'no', c) 'I don't know'. Question 5: 'How do you remember passwords?', which had the possible answers: a) 'in my browser', b) 'in dedicated software like 1Password, Dashlane, KeePass, LastPass', c) 'in my mind', d) 'another way'.

RESULTS

During the password changing/creating sessions some characteristics were collected. Even though the total number of unique stored sessions was 367, only

266 are important from the perspective of this article (133 session pairs). Only those, for which two unique password change sessions are stored: one for a simple password change form and one for a gamified password change form (for the same e-mail address). Tab. 1 shows the minimum, average and maximum values for length, number of character classes, and entropy.

Most recent research on the use of gamification in educational contexts have shown that it has served its purpose well, for it has increased student engagement and motivation [12, 40]. To prove the validity of author's attempt to implement gamification in academic teaching, after course completion, an anonymous questionnaire was filled in by students taking part in the gamification-oriented classes.

Tab. 1. Password composition characteristics for the simple and gamified forms

		length	character classes	entropy
simple form	min	8	1	18
	avg	11.02	2.49	25.05
	max	24	4	46
gamified form	min	8	1	18
	avg	12.89	2.83	28.88
	max	33	4	55

The most significant results are as follows: the average password length is almost two characters longer in the gamified system; the average entropy is 15% more in the gamified system. We compared the changes in password strength for each participant and the results are presented in tab. 2.

Tab. 2. Password composition characteristics between the gamified and the simple form

	min	avg	max
password length in gamified form / password length in simple form	0.73	1.20	3.67
character classes in gamified form / character classes in simple form	0.50	1.23	4.00
password entropy in gamified form / password entropy in simple form	0.79	1.17	2.16

Password length is in gamified form: equal to a simple form for 52, greater for 65 participants. Only 16 users decided to define a shorter password in the gamified system. 93 participants had the same number of character classes in both systems, while for 36 users the number of character classes was larger in the gamified system than in the simple system. Password entropy is in gamified form: greater for 73, equal for 44 participants (they mostly setup the same password in both systems), and smaller for 16 users. Breaking time is in gamified system: greater for 74, equal

for 43 and smaller for 16 pair of passwords. Our findings worth to point out: average password complexity is around 17% higher in a gamified system.

The most significant results of the questionnaire are presented in tab. 3. The majority of participants in both groups claim that the password created in the gamified system was stronger than in the simple system and that the gamified approach is more effective than classic password meters. Students were involved in the password creation process: almost 75% chose the graphic theme themselves. The most interesting are results about the greatest impact for passwords. We noticed here a significant difference between both groups. Participants unrelated with IT topics (group 1) mostly (72%) selected the time it would take to break the password, whereas participants who understand the topics of storing and breaking passwords preferred the gamified approach (44%) then 'scared' (40%). In both groups, suggestions about password security are important for only about 17% of participants.

Tab. 3. Most significant results of the questionnaire

Number of participants who:	group 1	group 2
completed the questionnaire	116 [100%]	50 [100%]
claimed that the password created in the gamified system was stronger than in the simple system (question 1, answer a)	65 [56%]	37 [74%]
stayed with the randomly chosen graphic theme (question 2, answer a)	29 [25%]	14 [28%]
chose the graphic theme themselves (question 2, answer b)	87 [75%]	36 [72%]
claimed that the greatest factor when building a password was:		
desire to see the next pictures (comments) (question 3, answer a)	13 [11%]	22 [44%]
suggestions about password security (question 3, answer b)	20 [17%]	8 [16%]
the time it would take to break the password (question 3, answer c)	83 [72%]	20 [40%]
claimed that the gamified approach is more effective than classic password meters (question 4, answer a)	73 [63%]	45 [90%]
claimed that they 'remember' passwords:		
in the browser (question 5, answer a)	19 [17%]	8 [16%]
in dedicated software (question 5, answer b)	0 [0%]	6 [12%]
in their memory (question 5, answer c)	87 [76%]	35 [70%]
another way (question 5, answer d)	10 [9%]	1 [2%]

Password memorability was checked indirectly only for group 2 participants. After the survey the password remind link was deactivated. Students had to login to the edug.pl system as part of their daily routine at university, therefore students who forgot their password had to ask a supervisor for help to regain access to the system. There was only one such incident. Considering the majority of students remember their passwords in their own memory (76% and 70% of participants selected 'in my own memory' for question 5), one can assume that the gamified approach was not significantly correlated with password memorability.

Discussion and limitations

Our results provide a few interesting contributions. First, we found that the gamified approach increases password strength. Passwords in the gamified system are on average 20% longer and have 17% greater entropy. Second, we identified that depending on users' knowledge about passwords (storing, breaking, leakages), their motives for choosing stronger passwords vary. For 'normal' users the most significant factor is the interactive fear appeal; breaking time is the strongest argument for them. Topic oriented students are more prone to enjoyment and therefore the gamified approach is more suitable for them. Third, both groups were rather bored with and indifferent to widely used suggestions on how to make passwords more secure. Such suggestions should be replaced or strengthened by other indicators, such as interactive fear appeals or gamification.

Our findings need to be considered in light of the following limitations. First, all the participants are students aged 21–23, which could impact our results. Second, although our experiment involved an actual website, for group 1 it was not a real system. For group 2 it was a real system, but it did not store any sensitive information about users. The results would likely be different for 'important' accounts (banks, social media).

Acknowledgments

The author wants to thank Bartosz Biernacik from War Studies University for his help in providing questionnaire among students from WSB University in Poznań.

REFERENCES

[1] Bishop M., Klein D. V., *Improving system security via proactive password checking*, 'Computers & Security', 1995, 14(3), pp. 233–249.

[2] Bonneau J., Herley C., Oorschot P. C. van, Stajano F., *Passwords and the evolution of imperfect authentication*, 'Communications of the ACM', 2015, 58(7), pp. 78–87.

[3] Bonneau J., *The science of guessing: analyzing an anonymized corpus of 70 million passwords*, Security and Privacy (SP), IEEE, Symposium, 2012, pp. 538–552.

[4] Carné de Carnavalet de X., Mohammad M., *From Very Weak to Very Strong: Analyzing Password-Strength Meters 2014*, Conference 'Network and Distributed System Security Symposium', DOI: 10.14722/ndss.2014.23268 10.14722/ndss.2014.23268.

[5] Das A., Bonneau J., Caesar M., Borisov N., Wang X., *The tangled web of password reuse*, Symposium on Network and Distributed System Security, 2014, Vol. 14, pp. 23–26.

[6] Dell'Amico M., Michiardi P., Roudier Y., *Password strength: An empirical analysis*, Proceedings IEEE, INFOCOM, 2010, pp. 1–9.

[7] Deterding S., Dixon D., Khaled R., Nacke L., *From game design elements to gamefulness: defining gamification*, Proceedings of the 15th International Academic MindTrek Conference 'Envisioning future media environments', 2011, pp. 9–15.

[8] Deterding S., Sicart M., Nacke L., O'Hara K., Dixon D., *Gamification. using game-design elements in non-gaming contexts*, CHI'11 — Extended abstracts on human factors in computing systems, 2011, pp. 2425–2428.

[9] Egelman S., Sotirakopoulos A., Muslukhov I., Beznosov K., Herley C., *Does my password go up to eleven? The impact of password meters on password selection*, Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 2013, pp. 2379–2388.

[10] Furnell S., *An assessment of website password practices*, 'Computers & Security', 2007, Vol. 26(7–8), pp. 445–451.

[11] Hamari J., Koivisto J., Sarsa H., *Does gamification work? A literature review of empirical studies on gamification*, IEEE, System Sciences (HICSS), 47th Hawaii International Conference, 2014, pp. 3025–3034.

[12] Huang X., Xiang Y., Bertino E., Zhou J., Xu L., *Robust multifactor authentication for fragile communications*, IEEE, 'Transactions on Dependable and Secure Computing', 2014, Vol. 11, No. 6, pp. 568–581, DOI: 10.1109/TDSC.2013.2297110.

[13] Johnston A. C., Warkentin M., *Fear appeals and information security behaviors: an empirical study*, 'MIS Quarterly', 2010, pp. 549–566.

[14] Kelley P. G., Komanduri S., Mazurek M. L., Shay R., Vidas T., Bauer L., Lopez J., *Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms*, Security and Privacy (SP), IEEE, Symposium, 2012, pp. 523–537.

[15] Melicher W., Ur B., Segreti S. M., Komanduri S., Bauer L., Christin N., Cranor L. F., *Fast, Lean, and Accurate: Modeling Password Guessability Using Neural Networks*, USENIX Security Symposium, 2016, pp. 175–191.

[16] Naiakshina A., Danilova A., Tiefenau C., Herzog M., Dechand S., Smith M., *Why Do Developers Get Password Storage Wrong? A Qualitative Usability Study*, ACM, Proceedings of the SIGSAC Conference on Computer and Communications Security, 2017, pp. 311–328.

[17] Rodwald P., Biernacik B., *Password protection in IT systems*, 'Bulletin of the Military University of Technology', 2018, Vol. 67, pp. 73–92, DOI: 10.5604/01.3001.0011.8036.

[18] Seitz T., Hussmann H., *PASDJO: quantifying password strength perceptions with an online game*, ACM, Proceedings of the 29th Australian Conference on Computer-Human Interaction, 2017, pp. 117–125.

[19] Shannon C. E., *A mathematical theory of communication*, 'Bell System Technical Journal', 1948, Vol. 27, pp. 379–423, 623–656.

[20] Shannon C. E., *Prediction and Entropy of Printed English*, 'Bell System Technical Journal', 1951, Vol. 30, No. 1, pp. 50–64.

[21] Sotirakopoulos A., *Influencing User Password Choice Through Peer Pressure*, master thesis, The University of British Columbia, Vancouver 2011.

[22] Stobert E., Biddle R., *The password life cycle: user behavior in managing passwords*, Proceedings SOUPS, 2014.

[23] Ur B., Alfieri F., Aung M., Bauer L., Christin N., Colnago J., Johnson N., *Design and evaluation of a data-driven password meter*, Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, 2017, pp. 3775–3786.

[24] Ur B., Kelley P. G., Komanduri S., Lee J., Maass M., Mazurek M. L., Christin N., *How does your password measure up? The effect of strength meters on password creation*, USENIX Security Symposium, 2012, pp. 65–80.

[25] Vance A., Eargle D., Ouimet K., Straub D., *Enhancing password security through interactive fear appeals: A web-based field experiment*, IEEE, System Sciences (HICSS), 46th Hawaii International Conference, 2013, pp. 2988–2997.

[26] Weir M., Aggarwal S., Collins M., Stern H., *Testing metrics for password creation policies by attacking large sets of revealed passwords*, Proceedings of the 17th ACM conference on Computer and communications security, 2010, pp. 162–175.

[27] Zezschwitz E. von, Luca A. de, Hussmann H., *Survival of the shortest: A retrospective analysis of influencing factors on password composition*, 'Proceedings of the IFIP Conference on Human--Computer Interaction', 2013, Publ. Springer, Berlin, Heidelberg, 2013, pp. 460–467.

[28] Zhang-Kennedy L., Chiasson S., Biddle R., *Password advice shouldn't be boring: Visualizing password guessing attacks*, IEEE, 'eCrime Researchers Summit', 2013, pp. 1–11.

[29] Zhao Z., Ahn G.-J., Hu H., *Picture gesture authentication: Empirical analysis, automated attacks, and scheme evaluation*, ACM, 'Transactions on Information and System Security (TISSEC)', 2015, Vol. 17, No. 4, pp. 1–37.

[30] Zhu B., Yan J., Bao G., Mao M., Xu N., *Captcha as graphical passwords–a new security primitive based on hard AI problems*, IEEE, 'Transactions on Information Forensics and Security', 2014, Vol. 9, No. 6, pp. 891–904, DOI: 10.1109/TIFS.2014.2312547.

[31] Castelluccia C., Dürmuth M., Perito D., *Adaptive Password-Strength Meters from Markov Models*, Symposium on Network and Distributed System Security, 2012, [online], https://www.ei.ruhr-uni-bochum.de/media/ei/veroeffentlichungen/2016/01/15/2012-ndss-pwd-strength.pdf [access 02.11.2018].

[32] Habib H., Colnago J., Melicher W., Ur B., Segreti S., Bauer L., Cranor L., *Password creation in the presence of blacklists*, Proceedings USEC, 2017, [online], https://www.archive.ece.cmu.edu/~lbauer/papers/2017/usec2017-blacklists.pdf [access 02.11.2018].

[33] Reilly M., *Google Has a Plan to Kill Off Passwords*, [online], https://www.technologyreview.com/s/601575/google-has-a-plan-to-kill-off-passwords [access 02.11.2018].

[34] Thomas K., Li F., Zand A., Barrett J., Ranieri J., Invernizzi L., Markov Y., Comanescu O., Eranti, V., Moscicki A., Margolis D., Paxson V., Bursztein E., *Data Breaches, Phishing, or Malware? Understanding the Risks of Stolen Credentials*, 2017, [online], https://research.google.com/pubs/pub46437.html [access 02.11.2018].

[35] *2016 Data Security Incident*, Uber Newsroom, [online], www.uber.com/newsroom/2016-data-incident/ [access 02.11.2018].

[36] *Adobe breach impacted at least 38 million users*, Krebs on Security, [online], https://krebsonsecurity.com/2013/10/adobe-breach-impacted-at-least-38-million-users/ [access 02.11.2018].

[37] *Advanced password recovery*, Hashcat, [online] www.hashcat.net/hashcat/ [access 02.11.2018].

[38] *AntMiner S9*, BITMAIN, [online], https://shop.bitmain.com/antminer_s9_asic_bitcoin_miner.htm [access 02.11.2018].

[39] *Digital Identity Guidelines Authentication and Lifecycle Management*, NIST Special Publication 800-63B [online], https://pages.nist.gov/800-63-3/sp800-63b.html, DOI: 10.6028/NIST.SP.800-63-3 [access 02.11.2018].

[40] *Dropbox hack leads to leaking of 68m user passwords on the internet*, The Guardian, [online], https://www.theguardian.com/technology/2016/aug/31/dropbox-hack-passwords-68m-data-breach [access 02.11.2018].

[41] *Hacker tries to sell 427 million stolen myspace passwords for $2,800*, Vice, [online], https://motherboard.vice.com/en_us/article/427-million-myspace-passwords-emails-data-breach [access 02.11.2018].

[42] *Have I been pwned*, API, [online], https://haveibeenpwned.com/API/v2 [access 02.11.2018].

[43] *LinkedIn lost 167 million account credentials in data breach*, Fortune, [online], http://fortune.com/2016/05/18/linkedin-data-breach-email-password/ [access 02.11.2018].

[44] *Mobile Push Authentication*, RSA, [online], https://www.rsa.com/en-us/products/rsa-securid-suite/rsa-securid-access/mobile-push-authentication [access 02.11.2018].

[45] *Password cracker*, John the Ripper, [online], www.openwall.com/john/ [access 02.11.2018].

[46] *Special Publication 800-63-2 Electronic Authentication Guideline*, NIST, [online], https://csrc.nist.gov/publications/detail/sp/800-63/2/archive/2013-08-29, DOI: 10.6028/NIST.SP.800-63-2 [access 02.11.2018].

[47] *Visualizing Data Breaches*, Center Mast, [online], https://centermast.com/2017/03/17/visualizing-data-breaches/ [access 02.11.2018].

[48] *Web Authentication: An API for accessing Public Key Credentials*, WC3, [online], https://www.w3.org/TR/2018/CR-webauthn-20180320 [access 02.11.2018].

[49] *Yahoo hacked, 450,000 passwords posted online*, CNN, [online], www.cnn.com/2012/07/12/tech/web/yahoo-users-hacked [access 02.11.2018].

WYKORZYSTANIE GAMIFIKACJI I KOMUNIKATÓW WYWOŁUJĄCYCH STRACH ZAMIAST MIERNIKÓW SIŁY HASEŁ W CELU ZWIĘKSZENIA ENTROPII HASEŁ

STRESZCZENIE

Użytkownicy systemów informatycznych bardzo często tworzą słabe hasła. W celu dostarczenia informacji zwrotnej o skuteczności tworzonego hasła część stron internetowych wykorzystuje mierniki jego siły. Ich wpływ na bezpieczeństwo został stosunkowo dobrze zbadany. W artykule zaproponowano i zbadano nowe podejście do dostarczania informacji zwrotnej o sile tworzonego hasła. Opiera się ono na gamifikacji wzmocnionej komunikatami wywołującymi poczucie strachu. Użytkownicy są tu motywowani do tworzenia silniejszych haseł poprzez wykorzystanie wizualnych

i tekstowych historyjek. Podejście to jest wspierane przez komunikaty informujące o tym, w jaki sposób można poprawić bezpieczeństwo haseł oraz komunikaty wywołujące strach u użytkowników (na przykład powiadamiające, ile czasu potrzeba hakerowi do złamania hasła). W celu udowodnienia skuteczności zaproponowanej metody przeprowadzono eksperyment, w którym użytkownicy zmieniali swoje hasła na dwa sposoby: bez żadnej informacji zwrotnej oraz przy wykorzystaniu zaproponowanej metody. Uzyskane tezy o skuteczności zaproponowanego podejścia zostały wsparte wynikami przeprowadzonej ankiety.

Słowa kluczowe:
gamifikacja, hasła, bezpieczeństwo IT.

Article history
Received: 04.12.2018
Reviewed: 10.06.2019
Revised: 18.06.2019
Accepted: 20.06.2019