A password generator tool to increase users' awareness on bad password construction strategies

Pieris Tsokkis, Eliana Stavrou
Computing Department, Applied Cyber Security Research Lab
University of Central Lancashire Cyprus
Larnaca, Cyprus
ptsokkis@uclan.ac.uk, estavrou@uclan.ac.uk

***Abstract*— Cybersecurity education and training activities are essential to empower end users to take informed decisions and address cyber threats. An ongoing problem that still troubles the cybersecurity community is the selection of weak passwords. Users keep using weak passwords, cultivating the risk of compromisation. Users often choose passwords that appear to be strong. This creates a false sense of security as users have the belief that their passwords cannot be guessed. Unfortunately, given that attackers are aware of the users' habits, they often recover users' passwords. Therefore, it is imperative to educate people about the bad password construction strategies and empower them to select stronger passwords. Educational activities should be enhanced by integrating practical aspects that will assist the users to realize the problem. This work identifies and combines a range of bad password construction strategies and designs a relevant tool to practically demonstrate the strategies to the users.**

Keywords – bad password construction strategies, end user situational awareness, cybersecurity education, password cracking, user profiling, personally related passwords

I. INTRODUCTION

The global digital society that is formulated by the interconnection of ICT systems, supporting the Internet of Things (IoT) paradigm [1], has created new opportunities but also increased cyber threats. Critical services in areas such as healthcare, transport and energy, operate through cyberspace and reach a wide spread audience. Therefore, cyberspace has become a key enabler and a critical asset for the growth of modern digital societies, thus it is imperative to ensure its protection.

Unfortunately, as indicated by latest reports [2], cyber threats keep rising, although a broad range of operational and technical countermeasures are utilized. The human factor plays a significant role in cybersecurity, especially with regards to successfully addressing cyber threats and minimizing their impact on critical assets. Often, the human factor is considered the weakest link in cybersecurity as it hinders the effectiveness of the security solutions due to the insecure decisions and relevant actions that are taken [3]. Therefore, it is crucial to empower end-users and enhance their knowledge, so they can take responsible decisions when it comes to various security aspects.

978-1-5386-3779-1/18/$31.00 ©2018 IEEE

A key security aspect that users need to be educated about is user authentication, specifically the selection of strong passwords [4]. Although a variety of measures (e.g. awareness activities, password-strength checkers, password-composition policies, etc.) are taken to prevent users from selecting weak passwords, statistics [2] reveal that the problem remains. Selection of weak passwords can happen due to various reasons [3] such as ignorance on the subject; choosing convenience over following good security practices; due to a false sense of security [5], etc. The latter, concerns a factor that is challenging to address. A false sense of security can occur when end users are adhering to password policies but in an insecure way. Often, in their attempt to create a memorable password, they employ a variety of password construction strategies, with the belief that hackers will not be able to predict their password. This misconception can impact the perception of the end users with regards to the protection level that is actually achieved. Even if their password adheres to the respective password policy, it can still lead to a weak password. Therefore, it is vital to enhance the situational awareness of end users to eliminate, or at least, minimize the potential of a false sense of security. Given that weak passwords are one of the main vulnerabilities that attackers exploit to gain unauthorised access, it is imperative to keep educating people on the subject and enhancing their knowledge, so they can select stronger passwords. This can be achieved by designing educational tools [6] that can practically demonstrate to the end users the password construction strategies that are known to the cybersecurity community, including both defenders and attackers. Such tools can assist end users to realize what kind of potential passwords can be generated by specific construction strategies and assist them taking more informed decisions with regards to the strategy they utilize. Existing tools are not designed with the objective of demonstrating the aforementioned aspects.

The objective of this research work is to: a) investigate and identify bad password construction strategies that should be taken into consideration when designing educational / awareness activities and tools, and b) design a tool that can complement training and awareness efforts and demonstrate to the end users the specified bad practices and the relevant passwords that can be generated, thus the need to be aware of their existence so they can be avoided. Section II discusses related work. Section III specifies known password construction practices. Section IV presents the design of a

demonstration tool and discusses how the tool can be utilized to complement a training curriculum. Section V constitutes conclusion.

II. Related Work

The problem of weak passwords is not new to the research community. The last few decades, the research community is actively investigating the issue, analyzing users' habits and making valuable observations with regards to the utilized password selection strategies. Morris and Thompson [7] performed one of the very early studies, demonstrating that a significant number of users were choosing as passwords, words found in dictionaries. In later studies [8] [9], it was observed that passwords that contained personal information of a user (such as name, surname, or telephone number) could be easily recovered. Furthermore, a study delivered by Brown et al. [10] observed that the most widely used personal information in passwords are those related to the user (e.g. date of birth), followed by information related to the user's family, lovers and friends. The authors also found that the most frequently used information was names and dates. A similar conclusion was made in [11]. The author has identified that users commonly include information related to their life, such as numbers (e.g. dates), words (e.g. pets), names (e.g. of friends, family) or locations (e.g. cities). Recently, Li, Wang, and Sun [12], analyzed an exposed collection of passwords and confirmed that users still include personal information in their passwords.

Another interesting observation was made in [13]. The authors identified that 43% of people are using the same password or slightly modified across different accounts. They also developed an algorithm to predict the transformation rules that the users applied on their passwords, and managed to recover 30% of the slightly modified passwords. This demonstrates the risk of compromising different user's accounts, when one of the transformed passwords has been compromised. Often, users miscalculate the risks involved, therefore, they take actions that lead to vulnerabilities, e.g. weak passwords.

Another approach was taken in [14], where the authors asked participants to compose passwords, taking into consideration specific composition rules. The objective was to observe if the constructed passwords met the appropriate construction rules and if they were strong enough. The authors managed to discover 20% of the passwords, using a keyboard pattern that was utilized by the users. Chou et al. [15] also demonstrated that passwords adhering to commonly used keyboard patterns of adjacent and parallel keys, called AP patterns, can be recovered. On a later study [16], the authors discovered that users used semantic patterns in their passwords which could have a major impact on security. Semantics are sequences of words that have a meaning. For example, they have found that many passwords contained concepts relating to love, animals, food and money, and they have presented approaches for recovering such passwords.

Observations and reported cyber security incidents, indicate that end users are keep using bad password selection strategies. Creating a password with the above construction techniques, increases the risk of compromisation, since these techniques are known to both defenders and attackers. To address the problem, a variety of solutions have been proposed to assist people selecting stronger passwords.

One such solution is the design of password meters, e.g. [17] [18], that calculate how strong a password might be by calculating the number of predictions an attacker requires, on average, to recover the password. The strength of the password depends on its architecture; the longer and more complex the password is, the more difficult it is to be cracked. Although the usage of password meters is promising to address the problem of weak passwords, further work needs to be done to enhance their functionality. Castelluccia et al. [19] stated that password meters are providing insufficient feedback to the users, and that meters did not influence the users to select secure passwords [20]. Carnavalet's et al. [21] also indicated that password meters have several weaknesses such as lack of consistency, providing wrong feedback and sometimes misleading strength outcomes. In such cases, password strength meters are not effective, and they don't assist users to learn from their mistakes. As a result, users will continue to choose weak passwords.

Another solution to empower the selection of strong passwords is through password composition policies that are enforced by computer systems during password construction. A password composition policy can be defined as a list of rules, with the purpose of forcing or advising users to construct secure passwords. Some examples of password policies include: a) Uppercase and lowercase letters, b) One or more numbers, c) Special characters (e.g. !, @, #), d) Password must have length 8 or more, and e) Prohibit the usage of company name or an abbreviation. Password composition policies are a necessity to drive users choosing strong passwords. Nevertheless, it appears that common password policies continue to be exposed to on-line attacks [22] and that people fail to remember passwords created with strict password policies [23] [24]. Moreover, as observed in [25], users often employ circumvention strategies to create a password that adheres to the password policy but is still easy to remember. Unfortunately, such circumvention strategies lead to highly predictable passwords. This indicates the need to balance security and usability to make password policies more effective.

The fact that user selection strategies are known, led to the design of a variety of user profiling tools, e.g. [26] [27] [28], that can generate potential passwords that could be utilized by a specific user. However, these tools are focusing on optimizing the password cracking process, rather that educating users about the known bad password selection strategies. More specific tools are needed [6] to empower end users and minimize the risk of compromisation due to the selection of weak passwords.

III. Common Password Construction Strategies

The objective of this research work is to identify bad password construction strategies that should be taken into consideration when designing educational / awareness activities and tools. By promoting the integration of these strategies into educational activities, the aim is to enhance

users' awareness and assist them in realizing how a potential strategy can lead to weak passwords. Therefore, it can promote better decisions and the construction of stronger passwords.

The following categories of password construction strategies have been identified, based on the investigations performed in the literature, from exposed password lists, different password cracking tools and online reports about most utilized passwords:

a) User-related information. This category includes information about a person, his/her family and interests.

b) Keyboard combinations. Users often use keyboard patterns from a specific device, e.g. smartphone, laptop, etc.

c) Placement strategy. This category includes strategies that append one or more numbers / letters / symbols at the front, end or within a word.

d) Word processing. Password construction strategies may specify word processing rules such as reversing, rotating or doubling a word, etc.

e) Substitution. Another typical strategy is to substitute one or more letters in a word with symbols and/or numbers.

f) Capitalization. This category includes capitalizing one or more letters at any given place in a word.

g) Append dates. Users often append dates to a word such as a partial date, a season, a year, etc.

h) Combination. More advanced strategies can be generated by combining strategies from the aforementioned categories.

IV. PASSWORD GENERATOR TOOL BASED ON USER PROFILING

This section presents a tool that has been designed taking into consideration the password construction strategies specified in section III. The tool demonstrates what kind of passwords can be constructed by utilizing one or more strategies and assists the end-users to identify the password construction strategies that can generate weak passwords. The objective is to integrate the tool into educational / awareness activities and assist efforts that target to empower the users to select stronger passwords.

The tool design is inspired by the conceptual architecture in [6] and focuses on the processing of personal information to generate candidate passwords. As explained in section II, one of the frequently utilized password construction strategies is using personal information. In order to increase the effectiveness of their passwords, end users process their password further, by applying other strategies. For example, a user selects his spouse name e.g. Jessica. He decides to add part of his birthday date, apply substitution and also add a symbol, resulting to Je$sic@1203!. The user created a password that at a first glance may be considered as complex enough, thus the user has the belief that it is not easily guessable. These situations create a false sense of security. Unfortunately, the approach taken created a predictable password that can easily lead to a security breach and exposure of sensitive data. The proposed tool targets to highlight these situations and educate the users accordingly.

The following sections present the operation and main features of the proposed tool. The tool provides a sequence of screens to the user, to provide appropriate input and to select among the listed password construction strategies. At the end, the generated list of passwords is presented to the user.

A. Operation

The operation of the tool focuses on four key features:

1) Profiling the user

User profiling includes identifying information with regards to the individual, his/her family and interests. As indicated in Fig. 1, there are predefined fields and the user is expected to enter the relevant information. Moreover, the tool supports extendibility by allowing the user to enter a new field, not included in the tool. A new field can be entered by selecting the button "Add key".

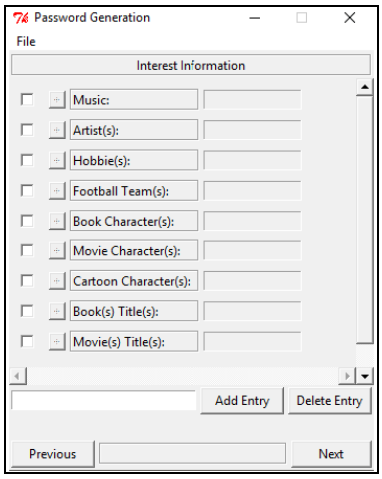

Fig. 1. User profiling password construction strategy

2) Presenting known password construction strategies that can lead to weak passwords

The tool presents a screen to the user that lists a set of categories. The categories list specific password construction strategies. Overall, the tool implements 318 password construction strategies. By selecting a category from the left side of the screen (Fig. 2), the listed strategies are presented to the user. The user can select strategies from the following list:

- All. This category contains all the password construction strategies implemented by the tool.

- Top 10 / Top 20. This category contains the 10 or 20 most widely used password construction strategies. For example, a recent study [12] revealed that most of users include dates at the end of their passwords. So potential passwords can be generated by considering the user's name + year of birth.

- Numbers. This category includes password construction strategies which are related with numbers. For example, inserting numbers at the end, at the front or inside a string. An example of a listed strategy includes appending 3 numbers at the end of a string. Potential passwords could be

generated by the children name + any three combinations of numbers, e.g. alice123, alice111, alice000, etc.

- Symbols. This category includes password construction strategies which are related with symbols. For example, inserting special characters at the end, at the front or inside a string. One of the listed strategies include adding one symbol at any position in a string, e.g. !alice, a!lice, al!ice, ali!ce, *alice, etc.

- Letters. This category includes password construction strategies which are related with letters, both uppercase and lowercase. For example, append one uppercase letter at the end of a string, e.g. aliceR.

- Dates. A variety of studies revealed that users are adding dates in their passwords. Partial or full dates can be inserted at any given position in a string e.g. alice2018.

- Key combinations. This category contains password construction strategies based on the patterns presented in [14].

- Hashcat rules. Hashcat [29] is a well know password cracking tool. The password construction strategies of Hashcat are included to demonstrate how powerful existing password cracking tools are, especially if the hacker is aware of user information.

- Advanced. This category combines strategies from previous listed categories. For example, it creates potential passwords by inserting one symbol at the start of a string and three numbers at the end, e.g. !alice876, !alice123, etc.

3) Processing the user-specified information using selected strategies

The user selects specific strategies that represent what he/she had in mind using to generate a password. For example, as Fig. 2 indicates, the user considered a key combination. So, a potential password could be Jessicaaws.

4) Generating potential passwords up to a given length

The last step is to choose a given length and generate potential passwords. At the end, the user can go over the list of generated passwords (Fig. 3) and search if specific password instances he/she was considering, are included in the list.

B. Demonstration and evaluation

To demonstrate the usage of the tool and to evaluate it, an appropriate awareness activity was designed. The purpose of the activity was to assist end users to evaluate if currently selected password construction strategies and relevant passwords are weak. The activity involved 3 main tasks:

a) The activity involved 30 participants (age: 23 – 55) that initially, they were asked to provide a potential password they would consider using. They have been advised not to reveal passwords that they were currently using.

b) Once the password collection was completed, passwords were analyzed. Results are presented in Table 1, indicating how many of the passwords included a specific type of information. Overall, it can be observed that most of the passwords include personal information, confirming once more users' tendency towards this strategy. Only a small percentage (10%) listed random passwords. The identified trends have been discussed with participants, so they were aware of the patterns utilized. For example, results indicate that there was a high tendency (40%) towards considering dates e.g. full date, year, etc.

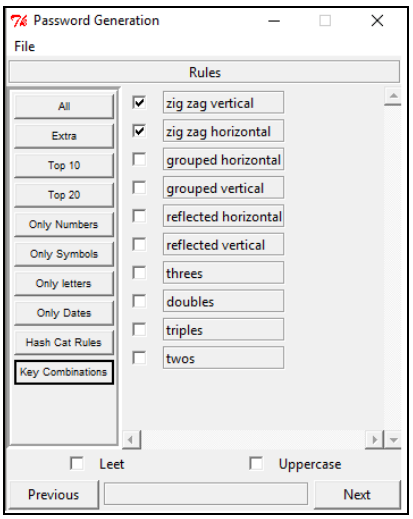

Fig. 2. Key combination password construction strategy

Fig. 3. Generated password list

TABLE I. EVALUATION RESULTS

	Included information	Number of passwords	Percentage
1	Date	12	40%
2	Name	7	23.33%
3	Sequence	4	13.33%
1	Random	3	10%
5	Surname	2	6.66%
6	Fictional characters	2	6.66%
7	Phone number	2	6.66%
8	Football team	1	3.33%

9	Phrase	1	3.33%
10	Places	1	3.33%

c) An evaluation of the tool was performed, considering user information and the password construction strategies that were relevant to the analysis performed in the previous task. The tool was able to identify about 47% of the passwords, demonstrating to the users that the selected strategies led to predictable passwords. This helped users enhance their perception of how strong their passwords are, considering specific construction strategies. At the end of the activity, 80% of the users reported that they will change the passwords they are currently using as they have realized that the construction strategy they considered led to the creation of weak passwords.

V. Conclusions

Passwords remain one of the main authentication techniques that users utilize to gain access to systems and information. Yet, weak passwords still trouble the cybersecurity community as they are among the key vulnerabilities that can be exploited by attackers to compromise a system and access critical information. The human factor plays a significant role in the protection of systems. The decisions taken by end users can positively or negatively impact the protection level that can be achieved. Therefore, it is imperative to continue educational and training efforts and empowering end users to take informed decisions. With regards to the construction of passwords, end users have to realize what password construction strategies might lead to weak passwords, even though at a first glance some of the chosen passwords may seem complex enough. Educational activities need to integrate practical activities and tools to demonstrate the usage of known strategies and potential passwords that can be generated, and which are easily guessable. By providing practical examples to the end users, we can help them realize the issue and promote the construction of stronger passwords. As a future work, authors are planning to enhance the functionality of the tool and create new cybersecurity educational activities.

References

[1] D. Evans, " The Internet of Things How the Next Evolution of the Internet Is Changing Everything," in CISCO White paper, 2011.

[2] "ENISA Threat Landscape 2016," [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016. [Accessed 10 November 2017].

[3] M. Bada and A. Sasse, "Cyber Security Awareness Campaigns: Why do they fail to change behaviour?," Global Cyber Security Capacity Centre, 2015.

[4] A. L. F. Han, D. F. Wong and L. S. Chao, "Password Cracking and Countermeasures in Computer Security: A Survey," in Cryptography and security, https://arxiv.org/abs/1411.7803.

[5] N. T. Ambade and A. Dixit, "Graphical Passwords Authentication: A Survey," IJCSMC, vol. 4, no. 2, pp. 247-254, 2015.

[6] E. Stavrou, "A situation-aware user interface to assess users' ability to construct strong passwords A conceptual architecture," in ", 2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), 2017.

[7] R. Morris and K. Thompson, "Password security: a case history," Communications of the ACM, vol. 22, no. 11, pp. 594-597, 1979.

[8] F. Grampp and R. Morris, "The UNIX system: UNIX operating system security," AT&T Bell Laboratories Technical Journal, vol. 63, no. 8, pp. 1649-1672, 1984.

[9] B. Riddle, M. Miron and J. Semo, "Passwords in use in a university timesharing environment," Computers & Security, vol. 8, no. 7, pp. 569-579, 1989.

[10] A. Brown, E. Bracken, S. Zoccoli and K. Douglas, "Generating and remembering passwords," Applied Cognitive Psychology, vol. 18, no. 6, pp. 641-651, 2004.

[11] S. Riley, "Password security: What users know and what they actually do," 2006. [Online]. Available: http://usabilitynews.org/password-security-what-users-know-and-what-they-actually-do/. [Accessed 10 November 2017].

[12] Y. Li, H. Wang and K. Sun, "A study of personal information in human-chosen passwords and its security implications. In Computer Communications," in IEEE INFOCOM 2016, 2016.

[13] A. Das, J. Bonneau, M. Caesar, N. Borisov and X. Wang, "The Tangled Web of Password Reuse," in NDSS, 2014.

[14] D. Schweitzer, J. Boleng, C. Hughes and L. Murphy, "Visualizing keyboard pattern passwords," in 6th International Workshop on Visualization for Cyber Security, 2009.

[15] H. Chou, H. Lee, C. Hsueh and F. Lai, "Password cracking based on special keyboard patterns," International Journal of Innovative Computing, Information and Control, vol. 8, no. 1, pp. 387-402, 2012.

[16] R. Veras, C. Collins and J. Thorpe, "On the Semantic Patterns of Passwords and their Security Impact," in Proceedings of the Network and Distributed System Security Symposium (NDSS'14), 2014.

[17] A. Sotirakopoulos, I. Muslukov, K. Beznosov, C. Herley and S. Egelman, "Motivating users to choose better passwords through peer pressure," in Symposium On Usable Privacy and Security, 2011.

[18] S. Egelman, A. Sotirakopoulos, I. Muslukhov, K. Beznosov and C. Herley, "Does my password go up to eleven?: the impact of password meters on password selection," in SIGCHI Conference, 2013.

[19] C. Castelluccia, M. Duermuth and D. Perito, "Adaptive Password-Strength Meters from Markov Models," in 19th Annual Network & Distributed System Security Symposium, 2012.

[20] B. Ur, P. Kelley, Komanduri, S., J. Lee, M. Maass, M. Mazurek, T. Passaro, R. Shay, T. Vidas, L. Bauer, N. Christin and L. Cranor, "How does your password measure up? The effect of strength meters on password creation," in 21st USENIX Security symposium, 2012.

[21] X. Carnavalet and M. Mannan, "A large-scale evaluation of high-impact password strength meters," ACM TISSEC, vol. 18, no. 1, 2015.

[22] P. Thorsheim, A. Jøsang, H. Klevjer and B. AlFayyadh, "Improving usability of password management with standardized password policies," in 7th Conf. on Network and Info Systems Security , 2012.

[23] S. Komanduri, R. Shay, P. Kelley, M. Mazurek, L. Bauer, N. Christin, L. Cranor and S. Egelman, "Of passwords and people: measuring the effect of password-composition policies," in Conference on Human Factors in Computing Systems, 2011.

[24] B. Brumen, R. Ivancic and I. Rozamn, "A Comparison of Password Management Policies," in Int. Conf. on Management of Engineering and Technology , 2016.

[25] M. Weir, S. Aggarwal, M. Collins and H. Stern, "Testing metrics for password creation policies by attacking large sets of revealed passwords," in ACM Conf on Computer and Comm security, 2010.

[26] "Common User Passwords Profiler (CUPP)," [Online]. Available: https://github.com/Mebus/cupp. [Accessed 10 November 2017].

[27] "Wyd password profiling tool," [Online]. Available: http://www.remote-exploit.org/articles/misc_research__amp_code/index.html. [Accessed 10 November 2017].

[28] "CeWL - Custom Word List generator," [Online]. Available: https://digi.ninja/projects/cewl.php. [Accessed 10 November 2017].

[29] "Hashcat - Advanced password recovery," [Online]. Available: https://hashcat.net/hashcat/. [Accessed 10 November 2017]