User-Centric Adaptive Password Policies to Combat Password Fatigue

Article *in* The International Arab Journal of Information Technology · January 2022

DOI: 10.34028/iajit/19/1/7

2 authors, including:

Yaqoob Al-Slais
University of Bahrain
7 PUBLICATIONS **36** CITATIONS

User-Centric Adaptive Password Policies to Combat Password Fatigue

Yaqoob Al-Slais and Wael El-Medany
College of Information Technology, University of Bahrain, Kingdom of Bahrain

Abstract: *Today, online users will have an average of 25 password-protected accounts online, yet use, on average, 6.5 passwords. The excessive cognitive burden of remembering large amounts of passwords causes Password Fatigue. Therefore users tend to reuse passwords or recycle password patterns whenever prompted to change their passwords regularly. Researchers have created Adaptive Password Policies to prevent users from creating new passwords similar to previously created ones. However, this approach creates user frustration as it neglects users' cognitive burden. This paper proposes a novel User-Centric Adaptive Password Policy (UCAPP) Framework for password creation and management that assigns users system-generated passwords based on a cognitive-behavioural agent-based model. The framework comprises a Password Policy Assignment Test (PassPAST), a Cognitive Burden Scale (CBS), a User Profiling Algorithm, and a Password Generator (PassGEN). The framework creates tailor-made password policies that maintain password memorability for users of different cognitive thresholds without sacrificing password strength and entropy. The framework successfully created 30-40% stronger passwords for Critical users and random (non-mnemonic) passwords for Typical users based on each individual's cognitive password thresholds in a preliminary test*.

Keywords: *Cognitive burden, cybersecurity, human factors, adaptive password policy, password fatigue*.

Received January 1, 2020; accepted February 15, 2021
https://doi.org/10.34028/iajit/19/1/7

1. Introduction

The field of cybersecurity has grown in research interest exponentially over the last five years, with new techniques in cryptography, hashing, and other security solutions reaching the market at breakneck speed. In reality, without paying attention to the human factor, all advances in cybersecurity become weaker. According to Widdowson [28], in over 95% of cybersecurity incidents, the human element is a contributing factor. Another analysis from American telecommunication giant Verizon showed that 90% of successful data breaches resulted from exploiting users who used default or weak passwords [11].

Textual passwords, despite their weaknesses, are the dominant access control for the vast majority of online services accessed through mobile and desktop devices alike. A strong password is complex and difficult to guess but memorable at the same time. Splashdata[1], a password management company, publishes the world's 100 worst passwords every year to raise awareness of the dangers of using weak passwords. When users choose their passwords without guidance, they are usually weak and easy to guess [32, 33]. Therefore, organizations and services opt for enforcing password policies to encourage users to create strong passwords.

Password policies vary significantly between different organizations and online services, and more recently, governments have published several password policy standards, but there is no vigorous enforcement of these standards. The most widely referred of these standards is the American Department of Commerce's National Institute of Standards and Technology (NIST) Cybersecurity Framework developed in Kiefer and Manulis [14] in addition to the United Kingdom's National Cyber Security Centre (NCSC) password guidelines [3]. Table (1) compares several national and country-bloc recommendations and standards in regards to password policies. The main factors of robust password policies revolve around password length, its complexity, and expiration. Despite the variances between the standards, there is a consensus around longer passwords or passphrases and less focus on complexity and a strong drive towards eliminating password expiration.

Password policies enforced by most organizations and online services are rigid. They use a one size fits all approach, disregarding that users today handle multiple passwords, which cause heavy cognitive burdens, or what is widely known as password fatigue.

[1]http://teamsid.com/1-50-worst-passwords-2019

Table 1. Comparison of government password policy standards.

Standards	Password Length	Password Complexity	Password Expiration
National Institute of Standards and Technology (NIST) - USA	Random-six characters minimum User-created-eight characters minimum	Blacklist of common passwords Dictionary words	Strongly discourages enforcement of password expiry
National Cybersecurity Centre (NCSC) - UK	No password length capping but encourages users not to be excessive.	Does not recommend complexity measures with special symbols (!@#$%^&*)	Strongly discourages enforcement of password expiry
European Union Agency for Cybersecurity (ENISA)	Recommends random passwords of 14 characters and above	Discourages admin enforcement of mixed cases as they can be predictable	No standard for password expiry
Australian Cyber Security Centre (ACSC)	Recommends passphrases of a minimum of 14 characters	Passphrases comprise a minimum of four random words	Passwords/ Passphrases expire every twelve months
Canadian Government Password Guidance	Minimum of 12 characters	Disable or reduce complexity policies	Eliminate password expiration

Password fatigue leads users to circumvent how they handle passwords [16] by creating easy-to-guess passwords that cover the minimum requirements of the password policy, reusing passwords across several accounts, or writing them down and placing them in plain sight. Naturally, these types of workarounds can lead to colossal security vulnerabilities. Users from all age, education, and computer literacy backgrounds are prone to facing password fatigue at different levels. They have multiple password recall thresholds, i.e., their capability to remember multiple passwords with different password policies.

Password policy should reflect users' capabilities and mental thresholds when creating new passwords to register to new services or to access the accounts they are currently using. Therefore, there is a need to introduce flexible and adaptive password policies to fit individual users' needs.

This paper proposes a User-Centric Adaptive Password Policy (UCAPP) framework to introduce adaptive password policies that consider individual users' backgrounds and cognitive burden based on a cognitive-behavioural agent-based model. The framework creates a system-generated random password based on the result of a small group of online tests to measure the user's password forget rate, recall threshold, and password write threshold.

The remainder of this paper consists of five sections. Section Two will explore related works in adaptive password policies and their effects on users, followed by a background into the cognitive agent-based model used in assigning the password policy to the user in section three. Whereas section four will discuss the proposed framework and its components in further detail and then present several examples of the framework in use. Finally, in section five, we present the paper's conclusions and future work.

2. Background

The work in [15, 16] uses a cognitive-behavioural agent-based model to determine a user's capability to remember a password. On the other hand, the likelihood of that user to forget a password and reset it. The model also considers the user's probability of writing down the password, which is widely considered a security risk. The model consists of nine parameters within three categories: password recall, password reset, and password security risk.

This section serves as a background for the proposed framework. The framework will utilize three of these parameters in its tests: password forget rate, password recall threshold, and password write threshold.

2.1. Password Forget Rate

The initial password forget rate is the likelihood the user will forget the password once a service account and password are created. Weaker passwords and reused ones over a variety of services will have a smaller initial password forget rate.

2.2. Recall Threshold

As the parameter's name suggests, it is the threshold that the user can recall their password. As shown in Fig.\ref{recall} If the password strength value $S-{a, b}$ exceeds the users' recall threshold, they will attempt to use the password B. If the user is unsuccessful in recalling the password, they will resort to another action, for example, to reset the password or create a new account.

2.3. Password Write Threshold

The password write threshold occurs when the cognitive burden is exceeded when creating a new password, or in most cases when resetting a password. The user opts to write down the password instead of memorizing it.

3. Related Works

The human element in any cybersecurity or computer security situation is the weakest link [8]. Despite this fact, many cybersecurity risk frameworks fail to recognize that humans directly or indirectly are an inherent risk to any system [19]. Also, many services online do not recognize the need for memorability when asking users to create new passwords. Woods [29] argues that adopting insecure password practices has cost organizations millions of dollars due to security breaches and helpdesk costs. Ideally, human

vulnerabilities such as memory limitation and the cognitive burden should be identified and managed before leading to a security breach [7].

Social factors such as age, gender, education, and computer literacy can affect human risk factors, with users having low literacy and low computer literacy being especially vulnerable [13]. Middle-aged users have shown to be less capable of remembering passwords than younger people between the ages of 25-35 years old. In contrast, elderly users are not significantly weaker in remembering passwords than middle-aged users [21]. Gratian *et al*. [9] found that women generally generate weaker passwords than men, and young adults from 18-25 also tend to generate weaker passwords to access their accounts.

Yan *et al*. [30] state that human memory for sequences is temporally limited, with a short term capacity of around seven characters, between the range of five as a minimum and nine as a maximum. Compounded with the fact that the average user has over 25 password-protected accounts and uses an average of 6.5 passwords shared between them [33], users naturally will experience a password overload and massive cognitive burden. Consequently, users will use coping mechanisms, such as reusing, recycling, or writing down passwords [14]. Stobert and Biddle [25] found that security experts admitted that they create weak passwords and reuse them on low-value accounts. Low-value accounts are those used to register to news portals, game applications [27], and throwaway accounts that do not utilize personal information [15]. High-value accounts store or utilize sensitive information such as credit card numbers and work-related emails and information [4].

Adams and Sasse's [1] paper titled "Users are not the Enemy" stated that enforcing password policies in the workplace led to high dissatisfaction, low motivation, and insecure practices. The policies did not meet the users' work practices. Over time, passwords have become an administrative tool that creates a false sense of security [5]. Kothari et al. introduced a novel approach for measuring the possibility of forgetting passwords and the efficiency of security and password policies within the workspace by utilizing a cognitive behavioural agent-based model [17].

Many government password policies and recommendations encourage more prolonged passwords rather than using complexity measures. A strategy to create longer passwords is by using mnemonic passwords derived from phrases or random words. The Bitcoin community has also introduced a mnemonic method to recall private keys through seed phrases based on the Bitcoin Improvement Proposal 39 (BIP39) [26]. Seed phrases are twelve-word phrase derived from a list of 2048 human-readable and meaningful words from several different languages. Mansour and Mahmoud [18] introduced a different approach that introduces keystroke latency times in passwords, where users need to enter their passwords in a certain rhythm to access their data.

Another approach is simplifying system-generated passwords and tailoring them to the users' preference. For example, Huh *et al*. [12] created the Surpass system, which allows users to modify system-generated passwords by editing and replacing a small number of characters. The study found that users who changed 3-4 characters had an increased password memorability of 21%.

Adaptive password policies are a relatively new cybersecurity concept that ensures users do not repeat similar password patterns when resetting passwords. Segreti *et al*. [22] define adaptive password policies as policies that dynamically change password requirements over time as users create new passwords. The researchers found that adaptive policies provided significant security benefit with minimal usability trade-off. Castelluccia *et al*. [6] used Markov models trained on a password database to create adaptive password strength meters to ensure users create strong passwords and not rely on previous passwords or password strategies.

Guo *et al*. [10] developed a Dynamic Personalized Password Policy (DPPP) by prompting nudges and gives password policy recommendations based on the users' personality. The study relied on the relationship between personality traits such as openness and agreeableness with users' perceptions of their cognitive abilities. The resulting passwords were stronger than the Basic8 and 3class8 password structures.

The work in [24, 31] created a dynamic password policy generator algorithm to increase the difficulty for attackers to crack passwords stored onto a database. The algorithm generates policies dynamically depending on the frequency of the characters that the user enters as a password.

The current applications of adaptive password policies focus on creating strong passwords and limiting users' ability to create new passwords derived from previous ones or using their password strategies and patterns. We believe that such approaches in creating adaptive password policies can lead to user frustration and increase users' cognitive burden in memorizing and recalling passwords. Adaptive Password policies should have a more user-centric approach by providing memorable passwords based on the user's cognitive ability without sacrificing password strength and memorability.

4. Proposed Framework

The proposed UCAPP framework comprises the Password Policy Assignment tests (PassPAST), the Cognitive Burden Scale (CBS), and the Password Generator (PassGEN). As shown in Figure 1, the framework initiates by the user entering some personal data such as age, educational level, and computer

literacy level. Then the user is subject to several brief tests through the novel PassPAST tests to measure their Password Forget Rate, password recall threshold, and password write threshold based on the work of Kothari *et al*. [17].

After completing the tests, the result is accumulated and stored in the Test Results Database and then compared on the CBS rating scale. The user receives the newly system-generated password based on their profile. The following sections will describe each component in further details.

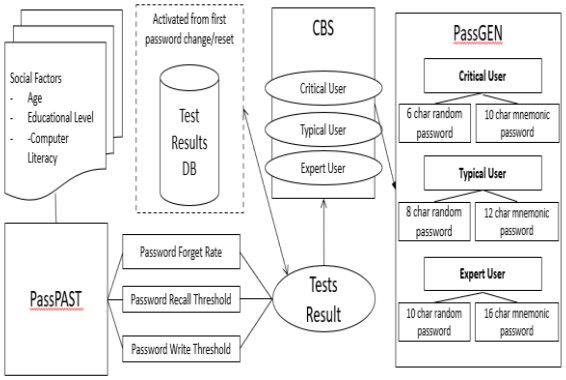

Figure 1. Proposed adaptive password policy framework.

4.1. PassPAST

When users first create their account to access a service, they will enter their social factor data (age, educational level, and computer literacy). Each item has a corresponding score as part of the final test results. Table 2 shows the weighing scale from (1-3) based on the user's answers. As for the age factor, users between the ages of 26-35 will have the highest scores of (3), whereas the age groups 18-25, 36-50, and 50-75 share the same score of (2) as all three groups do not have significant differences in password recall capabilities based on the literature [2, 19, 20].

Table 2. Social factor scale (Age).

Age Group	Social Factor Scale (1-3)
18-25	2
26-35	3
36-50	2
51-70	2
>70	1

As for the educational level *E* and computer literacy *C* factors, the scores increase in correlation with their levels. The education level *E* scale starts from Basic Education (up to Grade 9) with a weight of 1 point, followed by Secondary Education (Grade 9-12) with 2 points. Both Undergraduate and Graduate levels' weight is 3 points. In Table 3, Computer literacy consists of five levels with a corresponding scale (1-4). Starting from Fundamentals which denotes the bare minimum of typing, using a mouse and navigating files. Basic level comprises the skills to use email and baseline tools of office applications, whereas intermediate has higher proficiency in utilizing office applications, including spreadsheets and databases. Advanced level encompasses programming capabilities.

Table 3. Computer literacy factor scale

Computer Literacy	Scale
Fundamentals	1
Basic	2
Intermediate	3
Advanced	4

The PassPAST tests are a series of five brief tests to measure the initial password-forget rate, the password recall threshold, and the password-write threshold. The user answers each test question within 60 seconds. As shown in Table 4, the user completes the first task by entering a new password. The user can freely enter any password without constraints. Then it is analyzed for password length, uppercase and lowercase letters, digits, symbols and run through a dictionary check. Based on the result of the analysis, the PassPAST calculates the entropy of the user-created password using Shannon's [23] entropy as shown in Equation (1), where P_l is password length and n is the number of characters in a character set :

$$En = P_l * log_2(n) \quad (1)$$

Shannon's [23] Entropy After 30 seconds from creating the password, PassPAST requires the user to re-enter their password, and this step is repeated in the remaining four steps.

The following three tasks require the user to recall a system-generated password to measure their short term password recall rate. The first task displays a six-character password, then an eight-character password, and the third a ten-character password. In the final step, the PassPAST requires the user to re-enter one of the previously shown passwords. Whether it was correct or not, the entered password will be measured for entropy and indicate how many characters is the threshold to recalling passwords.

Once the user completes all tests successfully, the results are stored in a database and transmitted to the CBS.

Table 4. PassPAST test tasks and parameters.

Step	Task	Parameter
1	Pre-Task: User enters social factors data	Age, Education Level, Computer Literacy level
2	Task 1: Enter a new password	Initial password strength Initial Password Forget Rate
3	Task 2: re-enter the six-character system-generated password	Password Recall Threshold
4	Task 3: re-enter the eight-character system-generated password	Password Recall Threshold
5	Task 4: re-enter the ten-character system-generated password	Password Recall Threshold
6	Task 5: Enter a previous password	Password Write Threshold

4.2. Cognitive Burden Scale and User Profiling Algorithm

The next step in the proposed framework measures the cognitive burden and profiles the user as either a critical, typical, or expert user. As shown in Algorithm (1), the cognitive burden is the result of multiplying the initial password entropy entered by the user with the sum of the Forget Rate (FT), Recall Threshold (RT) and Write Threshold (WT) collected from the previous tests. The Profiling step relies on three ranges (0-60), (60-120), (Above 120), for Critical, Typical, and Expert Users, respectively.

Algorithm 1: User Profiling

Step 1 Calculate Social Factor
Input Age, Computer Literacy, Education level
Social Factor=A+C+E
Step 2 Calculate Cognitive Burden
*Cognitive Burden = Initial Password Entropy *(FR+RT+WT)*
Step 3 Profile User
*User Profile=Social Factor*Cognitive Burden*
If User Profile >0 && <60
Then "Critical User"
If User Profile >60 && <120
Then "Typical User"
If User Profile >120
Then "Expert User"

Table 5 shows an example of several users completing the tests and profiled through the CBS. A Critical User (CU) is a user that experiences a high forget rate, low password recall threshold, and low write threshold. CUs will receive highly memorable passwords with moderate entropy.

Typical Users (TU) are the average users who experience a moderate forget rate, high recall threshold, and a moderate write threshold. TUs will receive a more complex password. The third profile, Expert Users (EU), have low password forget rates and a high recall threshold and write threshold, meaning that their cognitive ability can handle high complexity passwords with ease.

Table 5. Example of User Profile through CBS.

User	Initial password	Entropy (bits)	Forget rate	Recall rate	Recall threshold	Profile
1	password	37.6 (0)	0.2	0.3	0.4	Critical
2	55ajj26r	41.3	0.4	0.6	0.6	Typical
3	Blue mountain range river	78.6	0.6	0.7	0.7	Expert
4	$!Lv3r8akk	65.5	0.8	0.8	0.9	Expert

The proposed framework's adaptiveness does not rely solely on profiling the users for the first time creating a password but on utilizing the Naïve Bayes classifier based on the user's historical data whenever they decide to change or reset their password. The adaptive approach leads to an experience where initially the user was, for example, a TU. However, upon resetting or changing their password and the cognitive burden they are experiencing at that time, they can shift their policy towards a CU. Users can experience both "levelling up" or "levelling down" regarding password policy assignment.

4.3. Password Generator PassGEN

The final step in the proposed framework is generating the password based on the user profile. As shown in Figure 1, each profile has two password formats, the first being a random password with lower and uppercase letters, digits (0-9), and special symbols (!@#$%^&*) resulting in entropy of approximately 6.55 bits per character. A random password from a minimum of six characters (39.2 bits) is an adequate strength to protect from online attacks. The second format is a mnemonic password from a dictionary of 8,000 English language words[2]. The reasoning behind having two formats is to increase the difficulty and cost of brute force attacks from security adversaries as users receive their password format randomly.

5. Results

This section displays preliminary test results using the proposed framework and its effectiveness in creating memorable, manageable, and secure passwords with high entropy. As shown in Table 6, Users (1-4) received SGPs based on their profile, as for the first CU, their password entropy improved from zero to 52.4 bits. Despite the password being weak due to its short length and use of dictionary words (USA and Queen), it is both memorable and more secure than the previous password.

The two TU profiles have different initial password techniques. The first had a random password and a mnemonic password for the latter. Both SGPs shared the exact value of entropy of 68.2. Mnemonic passwords are more memorable and have a lighter cognitive load than random passwords. The final EU received an SGP of similar format and entropy as their initial password due to their performance in the PassPAST tests and displayed great comfort using random passwords.

The proposed framework successfully generated 30-40% stronger passwords for CU and random (non-mnemonic) TUs. It also generated strong passwords with high entropy for TUs and EUs. However, the Critical users' SGPs were still weak and require strengthening, possibly adding more characters and relying on mnemonic passwords rather than having random and mnemonic password formats.

[2] https://github.com/ciamkr/English-words-list/blob/master/CommonDictionaryWords

Table 6. Adaptive password policies results.

User	Initial password	Entropy (bits)	Profile	SGP	Entropy (bits)
1	password	37.6 (0)	CU	UsaQueen	52.4
2	55ajj26r	41.3	TU	9KRqR*J644	68.2
3	Blue mountain range river	78.6	TU	CoffeeLaptopWoof	68.2
4	$!Lv3r8akk	65.5	EU	5B\GmB%R7&	65.5

6. Threats to Validity

The main threat is that the PassPAST is currently vulnerable to be "gamed" by users to produce CU profiles and receive more accessible passwords. Shannon's entropy used in this framework does not consider information gained from Social Engineering techniques and its effect on a password's entropy. Nor does it calculate the entropy after conducting a dictionary check despite research finding that such checks resulted in non-statistically significant decreases in observed entropy [11].

7. Conclusions

Password policies are rigid and neglect human memory limitations and cause frustration and cognitive burdens on users. This paper's proposed framework provides a solution that allows organizations and online services to apply adaptive password policies that fit the user's capability by utilizing a cognitive agent-based model through the PassPAST.

The framework for all levels of users was successful in generating strong passwords with high entropy to withstand online attacks and offline brute force attacks, with mnemonic passwords potentially a more favourable choice for users. Also, adaptive password policies can help reduce costs from helpdesk assistance in resetting passwords when applied in organizations instead of current single policies.

8. Future Work

As the proposed framework's concept is in its infancy, the following steps are to create an implementation of the proposed framework and formulate a case study on a sample of users that measures the long term memorability of the SGP as a proof of concept. Future work can incorporate different machine learning techniques to assign password policies where users cannot "game" the system to receive the most specific passwords. Another research area can utilize the password managers' framework to add a personalized approach to generating memorable passwords, besides handling the storage and simplification of private keys for Blockchain applications.

References

[1] Adams A. and Sasse M., "Users Are Not The Enemy," *Communications of the ACM*, vol. 42, no. 12, pp. 40-46, 1999.

[2] Alin Z., Boncea R., and Rotuna Carmen B., "user Behavior Characteristics for Mobile and Web Applications," *in Proceedings of The 12th International Conference on Virtual Learning*, Sibiu, 2006.

[3] Becker I., Parkin S., and Sasse M., "The Rewards and Costs of Stronger Passwords in a University: Linking Password Lifetime to Strength," *in Proceedings of 27th USENIX Security Symposium*, Usenix, pp. 239-253, 2018.

[4] Campbell J., Kleeman D., and Ma W., "Password Composition Policy: Does Enforcement Lead to Better Password Choices?," *in Proceedings of the 17th Australasian Conference on Information Systems*, South Australia, pp. 1-8, 2006.

[5] Campbell J., Ma W., and Kleeman D., "Impact of Restrictive Composition Policy on user Password Choices," *Behaviour and Information Technology*, vol. 30, no. 3, pp. 379-388, 2011.

[6] Castelluccia C., Dürmuth M., and Perito D., "Adaptive Password-Strength Meters from Markov Models," *in Proceedings of 19th Annual Network and Distributed System Security Symposium*, San Diego, 2012.

[7] Cooke N. and McNeese M., "Preface to Special Issue on the Cognitive Science of Cyber Defence Analysis," *EAI Endorsed Transactions on Security and Safety*, vol. 13, no. 1-6, pp. 1-3, 2013.

[8] Evans M., Maglaras L., He Y., and Janicke H., "Human Behaviour as an Aspect of Cybersecurity Assurance," *Security and Communication Networks*, vol. 9, no. 17, pp. 4667-4679, 2016.

[9] Gratian M., Bandi S., Cukier M., Dykstra J., and Ginther A., "Correlating Human Traits and Cyber Security Behavior Intentions," *Computers and Security*, vol. 73, pp. 345-358, 2018.

[10] Guo Y., Zhang Z., Guo Y., and Guo X., "Nudging Personalized Password Policies By Understanding Users' Personality," *Computers and Security*, vol. 94, pp. 101801, 2020.

[11] Halevi T., Memon N., Lewis J., Kumaraguru P., Arora S., Dagar N., Aloul F., and Chen J., "Cultural and Psychological Factors in Cyber-Security," *Journal of Mobile Multimedia*, vol. 13 no. 1-2, pp. 43-56, 2017.

[12] Huh J., Oh S., Kim H., Beznosov K., Mohan A., and Rajagopalan S., "Surpass: System-initiated User-replaceable Passwords," *in Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, New York, pp. 170-181, 2015.

[13] Inglesant P. and Sasse M., "The True Cost of Unusable Password Policies," *in Proceedings of the 28th International Conference on Human Factors in Computing System*, Atlanta, pp. 383-392, 2010.

[14] Kiefer F. and Manulis M., "Zero-Knowledge Password Policy Checks and Verifier-Based Pake," *in Proceedings of 19th European Symposium on Research in Computer Security*, Wroclaw, pp. 295-312, 2014.

[15] Komanduri S., Shay R., Gage Kelley P., Mazurek M., Bauer L., Christin N., Cranor L., and Egelman S., "of Passwords and People: Measuring the Effect of Password-Composition Policies," *in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, New York, pp. 2595-2604, 2011.

[16] Korbar B., Blythe J., Koppel R., Kothari V., and Smith S., "Validating an Agent-Based Model of Human Password Behavior," *in Proceedings of Workshops at the 30th AAAI Conference on Artificial Intelligence*, Arizona, pp. 167-174, 2016.

[17] Kothari V., Blythe J., Smith S., and Koppel R., "Measuring the Security Impacts of Password Policies Using Cognitive Behavioral Agent-Based Modeling," *in Proceedings of the Symposium and Bootcamp on the Science of Security*, New York, pp. 1-9, 2015.

[18] Mansour K. and Mahmoud K., "A New Approach for Textual Password Hardening using Keystroke Latency Times," *The International Arab Journal of Information Technology*, vol. 18, no. 3, pp. 336-346, 2021.

[19] Oltramari A., Henshel D., Cains M., and Hoffman B., "Towards A Human Factors Ontology for Cyber Security," *in Proceedings of CEUR Workshop*, pp. 26-33, 2015.

[20] Pilar D., Jaeger A., Gomes C., and Stein L., "Passwords Usage and Human Memory Limitations: A Survey across Age and Educational Background," *PLoS ONE*, vol. 7, no. 12, pp. e51067, 2012.

[21] Rinn C., Summers K., Rhodes E., Virothaisakun J., and Chisnell D., "Password Creation Strategies Across High- And Low-Literacy Web Users," *in Proceedings of the 78th ASIS&T Annual Meeting: Information Science with Impact: Research in and for the Community*, USA, pp.1-9, 2015.

[22] Segreti S., Melicher W., Komanduri S., Melicher D., Shay R., Ur B., Bauer L., and Christin N., "Diversify to Survive: Making Passwords Stronger with Adaptive Policies," *in Proceedings of 30th Symposium on Usable Privacy and Security*, pp. 1-12, 2017.

[23] Shannon C., "A Mathematical Theory of Communication," *The Bell System Technical Journal*, vol. 27, no. 3, pp. 379-423, 1948.

[24] Singh A. and Raj S., "Securing Password Using Dynamic Password Policy Generator Algorithm," *Journal of King Saud University-Computer and Information Sciences*, 2019.

[25] Stobert E. and Biddle R., "Expert Password Management," *in Proceedings of International Conference on Passwords*, Cambridge, pp. 3-20, 2015.

[26] Van Der Horst L., Choo K., and Le-Khac N., "Process Memory Investigation of the Bitcoin Clients Electrum and Bitcoin Core," *IEEE Access*, vol. 5, pp. 22385-22398, 2017.

[27] Wang D. and Wang P., "The Emperor's New Password Creation Policies: an Evaluation of Leading Web Services And The Effect of Role in Resisting Against Online Guessing," *in Proceedings of European Symposium on Research in Computer Security*, Vienna, pp. 456-477, 2015.

[28] Widdowson A., "CHEAT: An Updated Approach for Incorporating Human Factors in Cyber-Security Assessments," *Engineering and Technology Reference*, pp. 1-7, 2016.

[29] Woods N., "Frequently Using Passwords Increases Their Memorability-A False Assumption or Reality?," *in Proceedings of the 23rd Americas Conference on Information Systems*, pp. 1-5, 2017.

[30] Yan J., Blackwell A., Anderson R., and Grant A., "Password Memorability and Security: Empirical Results," *IEEE Security and Privacy*, vol. 2, no. 5, pp. 25-31, 2004.

[31] Yang S., Ji S., and Beyah R., "DPPG: A Dynamic Password Policy Generation System," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 3, pp. 545-558, 2018.

[32] Zhang J., Luo X., Akkaladevi S., and Ziegelmayer J., "Improving Multiple-Password Recall: An Empirical Study," *European Journal of Information Systems*, vol. 18, no. 2, pp. 165-176, 2009.

[33] Zhang-Kennedy L., Chiasson S., and Van Oorschot P., "Revisiting Password Rules: Facilitating Human Management of Passwords," *in Proceedings of APWG Symposium on Electronic Crime Research*, Toronto, pp. 81-90, 2016.

Yaqoob Al-Slais completed his MSc.in Social Informatics and Systems from Nagoya University, Japan in 2011. His undergraduate degree was a BSc. In Multimedia Technology at Leeds Metropolitan University (now Leeds Beckett) in 2005. Before joining the Information Systems department at the University of Bahrain as a Graduate Research Assistant in 2012, Yaqoob worked as a Computer Training Specialist at the Ministry of Education, raising Bahraini teachers' competencies in using ICT and Multimedia in education. Research interests include Social Informatics, Cybersecurity, privacy-aware and privacy-friendly systems, and intelligent automation. Yaqoob is currently pursuing his PhD in Computing and Information Sciences program at the University of Bahrain.

Wael El-medany holds a PhD degree in Electrical Engineering, Manchester University, UK, 1999; MSc degree in computer communications, Menoufia University, Egypt, 1991; BSc degree in Electronic Engineering, Menoufia University, Egypt 1987. He is the founding and managing editor of the International Journal of Computing and Digital Systems (IJCDS). He is the founder and Chair of MobiApps, DPNoC, and WoTBD workshops series. El-Medany is a senior IEEE member, a member of editorial boards and TPC member of many international journals and conferences, and acts as chairperson in many conferences. His research interests are in ASIC design, FPGA, embedded systems, remote monitoring systems, and reconfigurable computing.