Mesopotamian journal of Cybersecurity
Vol.2021, **pp**. 5–8
DOI: https://doi.org/10.58496/MJCS/2021/002; ISSN: 2958-6542
https://mesopotamian.press/journals/index.php/CyberSecurity

Research Article

Harmony Search for Security Enhancement

Rana Talib Rasheed [1,*], Yitong Niu [2], Shamis N. Abd1[1]

[1] *Al-Salam University college, Iraq*

[2] *Belarusian-Russian University, Mira Avenue 43, Mogilev, 212000, Republic of Belarus*

ARTICLE INFO

Article History

Received 17 Sep 2020
Accepted 7 Jan 2021
Published 10 Jan 2021

Keywords

Honeywords

metaheuristic

harmony search

ABSTRACT

The honeyword system can be considered as a mechanism for detecting passwords aiming to develop hashed password security via creating a password cracking easier to being detected. A lot of false passwords come with true passwords for forming false and true passwords for all users. When a hacker logs in and uses a honeyword, a silent alarm trigger illustrates that the honeyword system could be compromised. A lot of mechanisms of honeyword generating have been submitted and all of them have a defect in the generation, a support shortage for every honeyword characteristic, and a slew of honeyword complications. HSA (harmony search algorithm), a metaheuristic intelligence algorithm getting inspiration from music, can be utilized here for offering a way to generate honeyword. The suggested mechanism of honeyword generating is enhancing the generating, enhancing every honeyword characteristic, and addressing the shortcomings of each prior approach. This paper is showing many previous mechanisms of honeyword generating, clarifying the proposed one, discussing every experimental finding, and comparing the novel mechanism of honeyword generating with the ones before it.

1. INTRODUCTION

Due it its memorability and easiness, a password-based authenticating can be considered as the most common authenticating method. A lot of attacking methods, for example password cracking, were utilized for examining this approach. Password cracking can be considered as a non-ethical as well as non-common method to retrieve a password from data transmitted or maintained via computer systems. Honeywords can be considered as a simple mechanism for increasing honeywords connected with user accounts, hence developing hashed password security as well as simplifying password cracking for detection [1].

An opponent that gets access to the database of hashed passwords and gets the hashing reversed is not going to specify the actual password. If a honeyword is utilized in the signing in process, a silent alert is going to be activated. Honeychecker is a supplementary server which distinguishes between the actual and honeywords and connected with the signing in server by a secure connection [2]. A metaheuristic can be considered as a higher-level process utilized in mathematical optimization and computer science for identifying, developing, or choosing a heuristic which might offer a fine solution to optimization problems. Optimization problems are issues in mathematics, computer science, and economics in which the target is identifying the best answer [3]. Every metaheuristic algorithm is swarm, nature-inspired, physics-based, evaluation-based, or unique solutions. HAS can been considered as a special music-inspired algorithm which mimics the improvising process of a musician aiming to solve an optimization problem via getting the best solution [4]. The technique of honeywords functions via generating a honeyword (false password) from a sugarword (true password), then having it entered as a sweetword into the file of usernames and passwords, then hashed [5, 6]. If opponents get a simple password from a hashed one, he/she has to figure out the true password among a few sweetwords in the correct way; if not, a calm alert to the admin of the system might work, giving the signal that a password cracking is possible [7, 8]. Every action done by administrators is dictated by the policies of the organization and might cause the account to be banned, deferred, or notified [9,10]

*Corresponding author. Email: rana.talib@alsalam.edu.iq

2. HARMONY SEARCH INTELLIGENCE ALGORITHM

It can be considered as a metaheuristic optimization algorithm built upon natural events in which musicians search for the most superior notes for creating good harmony, comparing with looking for the most suitable solutions for problems [11].

The Harmony Search Intelligence Algorithm can be considered as implementable, owns a population diversity, converges quickly to the most suitable solution, and allocates a fine one in good time. It could allocate a stability between exploitation and exploration [12]. Random search, HMCR (harmony memory considering rate), and PAR (pitch adjusting rate) can be considered as the three operators which make up the HSA performance process [13].

The improvising of a musician for a pitch requires one of those three rules to be followed [14]: (1) the playing of a pitch from memory, (2) the playing of a neighboring pitch from memory, and (3) the producing of a random pitch from the sound range [15]. This is mimicked in all HAS variable selections: (1) the selecting of a value from HS memory, (2) the selecting of a close value from HS memory, and (3) the selecting of a random value from the potential value range. Algorithm 1 illustrates the general steps of the algorithm, that might be altered built upon the encoded problem [16].

```
Step 1: set up the optimization issue and algorithm parameters
Step 2: Create a harmony memory
Step 3: Create a new harmony
Step 4: Update the step 3
Step 5: Continue using Step3 and Step4 until the termination condition is met
```

ALGORITHM 1: The general steps of the harmony search algorithm

3. THE PROPOSED SYSTEM

The suggested honeyword system proposes utilizing the special metaheuristic music-inspired HSA as a new way to implement the honeyword generating process. HSA underwent a lot of alterations to appropriate the honeyword generation problem space and treat every one of its solutions as a honeyword. the study here selects HSA due to its easiness, simple implementing, diversity, fast converges, providing as good as possible to a good solution, and providing a stability between exploitation and exploration. The suggested honeyword system has been taken for the legacy-UI, that is more convenient to every user since it is only needed for a username and password for getting access. The last one includes letters, numbers, and characters. Thirty-six sweetwords can be utilized in the suggested system, that means k - 36; the adversary possesses a 1/36(≈3%) chance of a successful selection of the sugarword and possesses a (1–3% - 97%) probability of the selection of a honeyword. The recommend for the suggested system is that the hacker is not going to be able to choose the sugarword even if he/she knows one of its tokens due to the fact that the tokens in the sweetwords are repeated for five times. So, the hacker possesses a 1/6(≈17%) probability of the selection of the sugarword. The suggested honeyword system seeks to improve the generation process, develop every honeyword characteristic, and address every problem of previous approaches. The suggested HSA treats the password tokens differently. For every token type, there is a variant generator (letter, number, character generator). those generators function in parallel. For the letter tokens, the HSA constructs its evaluation criteria and pitch adjustment mechanism.

4. THE PROPOSED HAS ALGORITHM STEPS

The system utilizes the suggested HSA for generating honeywords as a token generating process; the sugarword can be considered as tokenized in three separate tokens: letter, number, and characters, then they are treated in variant generators (letter, number, character generator), and the resulting honeywords can be collected with the sugarword for providing the sweetwords. The tokens of the password are going to be handled as pitches. As it was spoken of previously, the suggested HSA owns three token generators operating in a paralleled way. The alphabet generator can be considered as the most significant and complex of all relying on mechanism of HAS in solving problems, while the digit and special character generator is easier relying on the easier mechanism of random generation. The most significant part of the honeyword due to being the hackers' preferred selection to figure out real passwords. It can be considered as the most complex generator which relies on the mechanism of HAS in solving problems; the tokens of passwords are going to be dealt with as pitches. The sugarword's alphabet token is going to be utilized as the generator's input. It can be considered as the seed utilized in producing honeywords alphabet tokens.

If the sugarword is (killer6+). the generated sweetwords via the suggested HAS are going to be as follows:

TABLE I. - HSA EMPLOYING

killer6+	kicker6+	dealer6+
killer2[	kicker2[	dealer2[
killer1-	kicker1-	dealer1-
killer8_	kicker8_	dealer8_
killer7{	kicker7{	dealer7{
killer7+	kicker7+	dealer7+

5. RESULTS AND DISCUSSIONS

The experimental outcomes, a comparing between the HAS and the previous honeyword generation method, and a discussion is going to be covered here.

The HSA can be experimented on different password tokens, containing the letter token, that is the most important token since the guess of the true password is the hacker’s first aim. Table 2 illustrates the experimental outcomes utilizing every parameter listed in the section.

The generation procedure for the letter token is going to be built upon the HSA approach in the solving the problem; eighty tokens are going to be made, but just the most superior five are going to be shown in the outcome table. A fundamental random generator is going to be utilized for the number and character tokens, with character alterations raking place randomly but with the same seed token length. The generated tokes are going to be 6. For the complete example, see Example 2. The proposed HSA generates honeywords which the adversary has no ability to guess. Storage: As the suggested HSA saves every username and sweetword, a lot of previous generating mechanism store more information as well as data.

Funding

Non.

Conflicts Of Interest

The authors declare no conflicts of interest.

Acknowledgment

Authors would like to thank Alsalam university college for their support .

REFERENCES

[1] L. Fang, H. Zhu, B. Lv, Z. Liu, W. Meng, Y. Yu, ... & Z. Cao, "HandiText: Handwriting recognition based on dynamic characteristics with incremental LSTM," ACM Transactions on Data Science, vol. 1, no. 4, pp. 1-18, 2020.

[2] A. Bahuguna, R. K. Bisht, & J. Pande, "Roadmap amid chaos: cyber security management for organisations," in 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), pp. 1-6, IEEE, July 2018.

[3] N. Chakraborty, M. Mukherjee, J. Li, M. Shojafar, & Y. Pan, "Cryptanalysis of a honeyword system in the IoT platform," IEEE Internet of Things Journal, vol. 9, no. 4, pp. 2614-2626, 2021.

[4] T. Win & K. S. M. Moe, "Protecting private data using improved honey encryption and honeywords generation algorithm," Doctoral dissertation, MERAL Portal, 2018.

[5] N. Chakraborty, S. Singh, & S. Mondal, "On designing a questionnaire based honeyword generation approach for achieving flatness," in 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), pp. 444-455, IEEE, August 2018.

[6] Y. Guo, Z. Zhang, & Y. Guo, "Superword: A honeyword system for achieving higher security goals," Computers & Security, vol. 103, p. 101689, 2021.

[7] A. Ala’a, A. A. Alsewari, H. S. Alamri, & K. Z. Zamli, "Comprehensive review of the development of the harmony search algorithm and its applications," IEEE Access, vol. 7, pp. 14233-14245, 2019.

[8] J. Gong, Z. Zhang, J. Liu, C. Guan, & S. Liu, "Hybrid algorithm of harmony search for dynamic parallel row ordering problem," Journal of Manufacturing Systems, vol. 58, pp. 159-175, 2021.

[9] S. Erwin & W. Saputri, "Hybrid multilevel thresholding and improved harmony search algorithm for segmentation," International Journal of Electrical and Computer Engineering (IJECE), vol. 8, no. 6, pp. 4593-4602, 2018.

[10] T. Bhattacharyya, B. Chatterjee, P. K. Singh, J. H. Yoon, Z. W. Geem, & R. Sarkar, "Mayfly in harmony: A new hybrid meta-heuristic feature selection algorithm," IEEE Access, vol. 8, pp. 195929-195945, 2020.

[11] S. Palaniappan, V. Parthipan, & R. Johnson, "Secure user authentication using honeywords," in International conference on Computer Networks, Big data and IoT, pp. 896-903, Springer, Cham, December 2018.