Using Combined One-Time Password for Prevention of Phishing Attacks

Somayeh Nasiri
Department of Computer Engineering
Zanjan Branch
Islamic Azad University
Zanjan, Iran
snasiri30@yahoo.com

Mohammad Tahqhighi Sharabian
Department of Computer Engineering
Zanjan Branch
Islamic Azad University
Zanjan, Iran
mtahghighi@yahoo.com

Mojtaba Aajami
Department of Computer Engineering
Zanjan Branch
Islamic Azad University
Zanjan, Iran
mojtaba.aajami@gmail.com

Abstract—**As technologies and communications develop, more sabotaging attacks occur including phishing attacks which jeopardize users' security and critical information like their passwords and credentials. Several solutions have been proposed for existing dangers. One of which is the use of one-time passwords. This issue has remained as a main challenge and requires more extensive research. In this research, we have focused on one-time password combinations and we also have proposed solutions based on behavioral patterns which lead to significant optimizations while tending the simplicity for users. Efficiency of the proposed method has been measured through defining scenarios, modeling and simulations based on a prevention rate index. In addition, complexity coefficient of the proposed method showing the probability of unpredictability of passwords for attackers has been calculated. Ultimately, a descriptive comparison has shown that the proposed method is superior to some of the existing methods.**

Keywords-phishing; one-time password; cyber attacks

I. INTRODUCTION

Electronic banking continuously requires new methods aimed at improvement of security, with respect to the extensiveness of bank, commercial and personal transactions and that most of them are conducted on the internet. One proposed method for this purpose is the use of one-time passwords (OTPs). OTPs are considered as suitable alternatives for secondary passwords and are proposed for securing the access of users to various electronic systems. In OTPs, encryption technics are used for production of one-time random passwords. Using one-time passwords for functions including authentication, not only improves the security of transactions, but also can be used for prevention of attacks aimed at stealing users' information. These types of attacks are known as phishing attacks. These have various forms and constantly impose a threat on users' security in virtual spaces. Phishing attacks are considered as a serious threat for classified information. Usually, an attacker sends out fake messages to fool people in order to steal their personal information. Unaware users who follow the instructions of these messages are directed to fake pages and then are asked to enter their credentials. Any sabotaging attack using a fake webpage for persuasion of users towards entering their security details is described as a phishing attack. According to observations in [1], more than 70 percent of phishing activities are aimed at stealing usernames and passwords of users' accounts. By making use of these information and user accounts, an attacker can even have access to more valuable information. OTPs can protect authentication mechanisms against different types of attacks. Authors in [1] proposed a method based on production of a unique random password at each login time. This method employs timestamps and number sequences for calculations. A test version of a two-factor authentication has been developed for cellphones based on this method and it has been practically used for one year. Authors in [2] proposed a method for prevention of phishing attacks. This method uses keywords to validate the originality of webpages. By this means direction of users' towards fake pages is prevented. Authors in [3] proposed a handy authentication system which eliminates the need for entering password during the process of authentication. Authors in [4] investigated different phishing methods along with methods of prevention. They proposed a method that makes use of a combination of OTPs and voice recognition for the prevention of phishing attacks. Authors in [5] proposed a design that makes use of development and integration of two famous protocols, PJP and AMP with OTPs. The PJP protocol uses passwords' security key. On the other hand, AMP protocol is an optimized account management system which considers user's previous activities in order to decide whether to lock the account or not. In addition, the proposed method uses the MD5 standard hash technic before transfer and saving in order to protect passwords. Ultimately, the security has been analyzed through making use of several simulated public attacks aiming for passwords. Authors in [6] proposed a method for prevention of phishing threats in websites. This method benefits from a visual encryption by making use of images and OTP. In this method, the main image is divided into two blocks and also a one-time password is generated as well. In [7], author elaborated on cons of typed passwords and proposed a method that makes use of picture combinations for passwords. This method can be a suitable alternative for typed passwords.

SMS based authentication methods send a one-time password to the cellphone of users. Afterwards, users may enter the received code in order to verify their login. Although that this method is well capable of preventing unauthorized use of passwords, still an attacker may guess a set of passwords which lead to either a successful attack or blockage of user's account. Authors in [8] proposed a system that enables the service device to validate the correctness of the one-time password. In this method, the password will only be sent to the system if its correctness is validated. This method not only reduces the risk of successful attacks, but also warns the system so that required defensive mechanisms are applied in time. As smart phones have become more and more prevalent, different OTP generators have also been developed as smartphone applications. However there is no guaranty for classification of generated passwords. Authors in [9] proposed a solution which not only has a suitable flexibility, but also makes use of hardware based security as well. By this means, smartphones are transformed into a suitable apparatus for generation of one-time passwords. In fact the former is done without taking any effects from the device's security glitches or imposing any impacts on the operating system. Although OTPs are widely used for prevention of phishing and replay attacks, supplying the security of OTPs is also a main challenge. In [10], authors proposed a model for optimization of security of OTPs. This method uses elliptic curve and iris biometrics encryptions. Among the advantages of this method, it can be referred to shorted key lengths compared to RSA and dynamic production of private keys when necessary.

In this research, authors have investigated different phishing methods along with methods of using OTPs. The aforementioned methods are combined in order to obtain a general solution and ultimately, a method for preventing phishing attacks and promoting users' information confidentiality, will be proposed.

II. PROPOSED METHOD

A. General Description

Benefitting from the idea of OTPs, this paper presents a new method that combines text and image encryption methods with innovative solutions based on behavioral parameters. This method increases the complexity of the generated OTP and makes it hard for attackers to reveal them through their, usually automatically, tools. In other words, a set of behaviors would be specified for the user and the user should enter the received OTP with respect to the determined behavioral pattern. On the user's side, the aforementioned pattern is transformed into a code and later, it is compared with the determined behavioral pattern by the service provider side. After validation, the rest of the combined OTP will be evaluated. The proposed method is a combined solution that includes image passwords, typed text messages and behavioral patterns. In the proposed method, a profile is created during registering phase. At this point, in addition to entering required information including name, surname, personal information, a unique username and the password; the user must also select a category of images which would be used for the generation of the visual password. Typed password would also be generated based on the user's account information. Nonetheless, the user must also determine a special behavioral pattern for entering the password. Specific typed, visual and behavioral pattern passwords are generated during each phase of the process of authentication based on the unique username of each individual user. The visual password would be shown to the user on the login page. The typed password will be sent to the user along with an instruction determining the behavioral pattern. Afterwards, a time window would appear on the service provider side which is aimed for controlling the time length of validity of the generated OTP. The user observes the visual password on the login page and receives the SMS code including the typed password and the determined behavioral pattern. He/she should enter his/her password along with typed, visual and behavioral pattern passwords received. On the user's side, the entire activities of the user including his/her behavioral patterns would be saved and encrypted. These behavioral patterns would be used for the generation of the OTP sent towards the service provider. The validation sector on the service provider side will first investigate the time window and then, will extract the behavioral pattern and decrypt it. In case of a match, the system will proceed towards investigating the visual and typed passwords. If the values match with predetermined values, the entered username and password would be authenticated. The aforementioned procedure means that user authentication mechanism is executed in a multilevel process. Different aspects of the proposed method would be explained with more details in the following.

B. Registration and Creation of User Profile

In this phase, the user must enter the following information which would shape his/her user account. This user account or profile will be used during the generation phases of visual, typed and behavioral pattern (BP) passwords.

- Name
- Surname
- Father's name
- ID number
- National Code
- Birth place
- Birth date
- Residence place
- Occupation
- Academic degree
- Username
- Password
- A category of images
- Behavioral pattern for entering the information

C. Generation of Visual Password

The proposed method includes ten categories of different images for the visual password generation. Each of these categories includes 100 images. The user must select one of these categories while signing up. At this phase, the selected category will be used for the generation of visual passwords. Based on the visual password generation method, a 5·2 matrix of existing images would be created with one image in each slot of the matrix. The user observes the matrix and selects the image related to his/her selected category. By doing so a number would be generated according to the position of selected image. This number would also be a part of the generated OTP. By making use of this mechanism, the possibility of guessing the OTP by human attackers will be reduced up to ten times. Since category image detection is very difficult for a program, then even automatic applications do not have a better chance compared to human attackers.

D. Generation of Typed Password

The process of typed password generation is also based on the existing information on the user's profile. For this purpose, a text field existing on the user's profile will be sent to the user along with a four digit random number. By observing the specific field, the user makes sure that the sent OTP is original. Afterwards, he/she will select the title of the field number sent to him/her and then enter the four digit random number. Afterwards, a two digit number is generated based on the position of the selected field on the matrix. This number is used in generation of the OTP in conjunction with a random number. The reason for using a two digit number is that here it is possible to have repeated fields. For example national codes and ID numbers of users may be similar in some cases. Therefore the user must be able to select two matrix slots and a number will be generated based on the priority of his/her choices. For example, if based on image 2, the user first selects his/her Id number and then his/her national code; the generated number will be 45. In case the user has done the reverse, then the generated number would be 54. For cases with no repetitions, digit 0 is selected as the last digit of the code. For example if a user's name was Hassan and the same field was sent to him, by selecting the name option, number of 10 would be used as a part of OTP.

E. Generation of Behavioral Pattern Password

A highly important point taken note of in the previous section is that user's behavioral pattern can be used as a highly suitable criterion for the generation of one-time passwords. In previous example it was observed that priority of conduction of activities by a user can result in generation of various different codes. Inspired from this, we are introducing the idea of the use of behavioral patterns. In other words, the text message sent to the user includes an order for his/her activities. For example the user would be told to first enter the random number, then the typed password and finally the visual password. By this simple scenario and without needing to add a mechanism that is observable by the attacker, we have been able to reduce the possibility of guessing the combined password up to 6 times. In fact if the number of behaviors used in this type of encryption were equal to N, then the possibility of guessing the OTP will be reduced for N times. Combination of this method with previously mentioned methods results in a significant deal of reduction in possibility of guessing the OTP. This in turn shows the superior efficiency of the proposed method.

F. Sending an SMS to the User

Since mobile phones are commonly used throughout the world, using the mechanism of sending a text message is considered as a suitable solution for sending the user the visual code and the instructions related to behavioral pattern. This issue significantly improves the security of proposed method.

G. Activation of Time Window

Since the time length of validity of OTPs must be limited, therefore for each time of sending a user an OTP, a time window is activated on the service provider side. In case the process of authentication does not complete during this time window, the sent OTP will lose its validity and expire. In this case, the user must resend a request for receiving the OTP. The point worth mentioning in this phase is that the time length specified for the timer should be logical based on existing and used mechanisms. Based on the following scenario, we have specified a time length of 3 minutes for the time window.

H. Validation

The process of validation starts when the user receives the OTP. After decryption, the validity must be determined in shortest time possible in order to reduce the server side's computation overhead. In this research, we propose the following order:

1. Time window
2. Behavioral pattern
3. Visual password
4. Typed password

In case the process of authentication fails in any of the above mentioned phases, the whole process will terminate and the user will receive a message of authentication failure.

I. Saving and Encrypting Users' Activities

Since the proposed method makes use of users' behavioral patterns, therefore it requires solutions for saving the activities of the user in order to be able to determine their and conduct the behavioral encryption. For this purpose, it is recommended to make use of two separate services on the client side. The first service saves the activities of the user and the second service encrypts them. By doing so, the principles of service oriented architecture are considered for as well.

J. Receiving Typed and Visual Passwords

Another service used on the client side will receive the visual and typed passwords and prepares them for production of the OTP.

K. Generating and Sending the OTP

In this phase, a unique number will be produced as a part of OTP based on behavioral patterns, typed passwords and visual passwords. The OTP will be sent to the service provider for validation. Since the used password includes no information regarding user's profile, therefore it will have a high security against phishing attacks.

III. Simulation Results

In order to evaluate the proposed method, it was simulated in MATLAB and its performance has been studied under different scenarios. Additionally, rates of prevention of different attacks have been investigated. Afterwards, complexity coefficient of the proposed method has been analytically measured. Finally, a descriptive comparison has been made between the proposed method and previous ones.

A. *Simulation*

The required data for evaluation have been collected through the modeling of different types of attacks. Two possible outcomes are considered for each attack. Either the proposed method is able to resist the attack or not. In order to make this simulation as simple as possible, we assumed that the phishing attack was partially successful and the attacker has been able to hypothesize a primary combination for the OTP. These hypotheses are used for evaluation as special data. Each of the scenarios mentioned in Table I requires consideration for different sets of conditions in order to be realized. We have simulated this by assuming that the attacker has obtained access to parts of information existing on the user's profile. We have ultimately designed a suitable set of data for investigation of results of attacks of interest. We have created a hypothetical user profile for our simulations (Table II).

TABLE I. SCENARIOS USED FOR SIMULATION OF PHISHING ATTACKS

title	details
Scenario 1	The attacker directs the user towards a fake website and tries to steal his/her password. In this case the user must notice the fakeness of the webpage and act reluctantly
Scenario 2	The attacker fakes the user's identity and obtains access to the website and tries to guess the password. In this case the website must identify the attacker based on behavioral patterns
Scenario 3	The attacker saves the previous OTPs sent to the user and tries to complete its knowledge about the user's profile. In this case the complexity coefficient of the OTP must be able to challenge the activities of the attacker

TABLE II. PROFILE OF THE HYPOTHETIC USER

Title	Value
Name	'Ali'
Surname	'Reazaie'
Father's name	'Mohammad'
Id number	'8'
National code	'3040488254'
Birth date	'11/1370/11'
Birth place	'Karaj'
Residence	'Tehran'
Occupation	'Student'
Academic degree	'M.A'.
Username	'Ali123'
Password	'789Ali425R'
Image category	'Flower'
Behavioral pattern	'Pic-Text-Num'

B. *Test Results*

Figure 1 shows the prevention rate of the proposed method based on performed experiments in aforementioned scenarios. The rate of prevention of phishing has been yielded as 100% for the proposed method. This shows the superior efficiency and functionality of the proposed method in terms of prevention of phishing attacks.

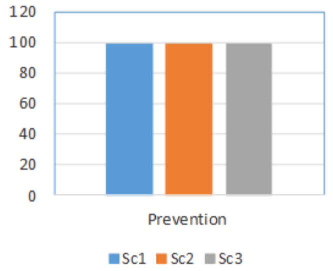


Fig. 1. Comparison of prevention rates of the proposed method

C. *Analysis of Complexity Coefficient*

Complexity coefficient of a password shows the power of that password in prevention of being guessed by attackers. In cases in which an attacker has obtained partial of full access to user's information, still an OTP must show a suitable preventive nature in this regard. While keeping the simplicity of our method, we have elaborated on its complexity at different levels.

1) Behavior

At this level, using behavioral patterns plays a significant role. We have defined behavioral patterns as a series of activities by users. Based on these activities, we have considered different orders for entering different parts of the OTP. At this level, the coefficient of complexity increases according to number of different parts of an OTP and based on the factorial relationship of number of parts of OTP. In other words, if there are N numbers of parts of OTP, then the complexity coefficient will be relative to the factorial of this value.

$$\text{Complexity\_Factor} \propto n! \tag{1}$$

2) Comprehension

At this level we have made use of human comprehension of images. A human user can easily distinguish different image categories. However this would be a very hard task for an automated program. Therefore by making use of this method, a new level of complexity is introduced. This issue also holds for identification of categories related to text information. Therefore if K numbers of image categories are used, and each category includes M numbers of pictures, then the complexity coefficient of OTP will increase relative to the following relation:

$$\text{Complexity\_Factor} \propto m^{k} \tag{2}$$

The upper content also holds for text categories as well. In case there are T numbers of text categories, the complexity coefficient of the proposed OTP increases relatively to the following relation.

$$\text{Complexity\_Factor} \propto c \times t2 \qquad (3)$$

In (3), c is a constant value and is relative to attacker's identification of text categories.

3) Diversity

In this level, the number of digits produced for the OTP is highly important. If the number of used digits is equal to d digits, then the complexity coefficient will increase relative to the following relationship.

$$\text{Complexity\_Factor} \propto 10^{d} \qquad (4)$$

4) Overall

Therefore, the overall complexity of the proposed method can be estimated easily:

$$\text{Complexity\_Factor} = n! \times m^{k} \times c \times t^{2} \times 10^{d} \qquad (5)$$

Putting used values in the variables we have:

$$\text{Complexity\_Factor} = 3! \times 100^{10} \times c \times 10^{2} \times 10^{4} \Rightarrow$$

$$\text{Complexity\_Factor} = 6c10^{26} \qquad (6)$$

Even assuming that the attacker has complete knowledge regarding text categories of the used language, still the obtained value is large and significant. This is definitely a suitable security for the used password. With respect to simplicity and user-friendly state of the passwords created, this issue is considered highly important.

D. *Descriptive Comparison*

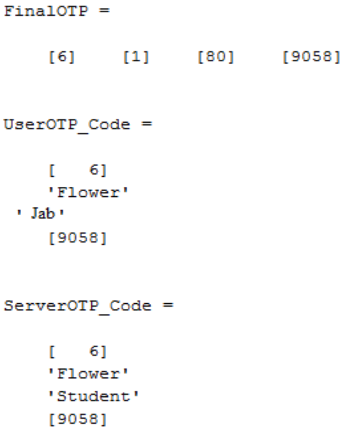
Table III represents a descriptive comparison between the proposed method and other combined or simple methods. It has been assumed that simple methods merely use numbers for generation of OTPs and that combined methods do not use BPs.

TABLE III. DESCRIPTIVE COMPARISON OF PROPOSED METHOD

criterion	Simple method	Combined method	Proposed method
Complexity	Less	Average	More
Prevention rate	Less	Average	More
Simplicity	More	Less	Less
attractiveness	less	more	more

E. *Final Evaluation*

According to the results, the proposed method is evidently highly efficient against phishing attacks and imposes several improvements on complexity coefficient of the generated OTP along with preventing different types of phishing attacks. The proposed method has high overall efficiency and has introduced several optimizations. Based on simulation results, on analytic investigation of complexity coefficients and on descriptive comparisons it can be expected that the present research will become a starting point for future researches regarding growth and development of OTPs aimed at prevention of phishing attacks. Main breakthrough of this project is paying attention to users' behavioral patterns. Separation of coding of the OTP in calculations on the server and client sides is another advantage of the proposed method. In fact even if attacks such as eavesdropping are present, the security of the protocol may still be maintained. Figure 2 shows this issue based on a series of sample generated codes in proposed method.



```
FinalOTP =

    [6]    [1]    [80]    [9058]


UserOTP_Code =

    [   6]
    'Flower'
  ' Jab'
    [9058]


ServerOTP_Code =

    [   6]
    'Flower'
    'Student'
    [9058]
```

Fig. 2. A sample of generated codes in proposed method

IV. Conclusions and Discussion

In this research we proposed a combined method for prevention of phishing attacks based on visual, text and behavioral patterns which is also relative to the number of selected factors for behavioral patterns and therefore can reduce significantly the rate of phishing attacks success. In addition, the proposed solution is based on selection of images and texts and input of numerical texts with special patterns that may seem attractive to users. In this article, we have proposed the idea of using users' behavioral patterns. By behavioral patterns it is referred to a series of activities performed by a user which can be considered as a special and specific profile for the user and based on it, different passwords could be generated. This idea can open a new door in the domain of encryption. Experiments, analysis and comparisons have shown a suitable efficiency for our proposed method and therefore this method can be selected as a suitable solution for different internet based activities including internet banking and e-commerce.

The research domains related to security against phishing attacks require a more extensive and comprehensive data set for the evaluation of new methods. Therefore, our first recommendation is the conduction of more researches for production of a suitable data set with data belonging to different cyber-attack types. This recommendation can also play a significant role in standardization of future researches. Since attackers' behavioral pattern plays a significant role in this domain, it is required to conduct specific activities in terms of creating a behavioral profile for attackers. As a future research suggestion, attention could be paid to even more complicated behavioral patterns. If it was possible to hide the behavioral pattern within the OTP, increased security could be yielded in the OTP combination.

Even though the proposed method has shown a good performance in experimental conditions, it is still required to be tested in real applications. So, as one last suggestion, attention should be paid to the point that academic studies must have a suitable relation with the related industry. The feedbacks and ideas of real users should be available and used for descriptive evaluations by the academic community. Doing so can have a crucial role in promotion of academic studies and optimization of the relation between the former and related industries.

REFERENCES

[1] C. Huang, S. Ma, K. Chen, "Using one-time passwords to prevent password phishing attacks", Journal of Network and Computer Applications, Vol. 34, No. 4, pp. 1292-1301, 2011

[2] M. Mishra, A. J. Gaurav, A. Jain, "Preventive Anti-Phishing Technique using Code word", International Journal of Computer Science and Information Technologies, Vol. 3, No. 3, pp. 4248-4250, 2012

[3] Y. Huang, Z. Huang, H. Zhao, X. Lai, "A new one-time password method", IERI Procedia,Vol. 4, pp. 32-37, 2013

[4] K. Marimuthu, D. Ganesh Gopal, H. Mehta, A. R. P. Boominathan, "A Novel Way of Integrating Voice Recognition and One Time Passwords to Prevent Password Phishing Attacks", International Journal of Distributed and Parallel Systems, Vol. 5, No. 4, pp. 11-20, 2014

[5] A. Onashoga, A. Sodiya, A. Afolorunso, "One-Time Server-Specific Password Authentication Scheme", Journal of Computing and Information Technology, Vol. 20, No. 2, pp. 85-93, 2012

[6] P. P. N. G. Phani Kumar, R. John Mathew, "An Advanced Anti Phishing Approach Based On Two-Tier Validation", International Journal of Research in Computer and Communication Technology, Vol. 3, No. 9, pp. 1015-1017, 2014

[7] B. K. Kushwaha, "An approach for user authentication One Time Password (Numeric and Graphical) Scheme", Journal of Global Research in Computer Science, Vol. 3, No. 11, pp. 54-57, 2012

[8] J. Hwang, Y. Hsu, G. Liao, "An SMS-Based One-Time-Password Scheme with Client-Side Validation", Journal of Digital Information Management, Vol. 13, No. 2, pp. 69-75, 2015

[9] H. Sun, K. Sun, Y. Wang, J. Jing, "Trust OTP: Transforming Smartphones into Secure One-Time Password Tokens", 22nd ACM SIGSAC Conference on Computer and Communications Security, pp. 976-988, 2015

[10] D. Mahto, D. K. Yadav, "Security Improvement of One-Time Password Using Crypto-Biometric Model", 3rd International Conference on Advanced Computing, Networking and Informatics, Vol. 2, pp. 347-353, India, 2015