Authentication Model using the Bundled CAPTCHA OTP Instead of Traditional Password

Thivanon Kansuwan
Research Center of Information Technology for the Future
(ITF) Department of InformationTechnology, Faculty of
Informatics Mahasarakham University, Thailand
60011284504@msu.ac.th

Thawatchai Chomsiri
Research Center of Information Technology for the Future
(ITF) Department of InformationTechnology, Faculty of
Informatics Mahasarakham University , Thailand
thawatchai99@gmail.com

Abstract— **In this research, we present identity verification using the "Bundled CAPTCHA OTP" instead of using the traditional password. This includes a combination of CAPTCHA and One Time Password (OTP) to reduce processing steps. Moreover, a user does not have to remember any password. The Bundled CAPTCHA OTP which is the unique random parameter for any login will be used instead of a traditional password. We use an e-mail as the way to receive client-side the Bundled CAPTCHA OTP because it is easier to apply without any problems compare to using mobile phones. Since mobile phones may be crashing, lost, change frequently, and easier violent access than e-mail. In this paper, we present a processing model of the proposed system and discuss advantages and disadvantages of the model.**

Keywords—CAPTCHA OTP, Traditional Password, Authentication

I. Introduction

Among the password authentication, the secure password setting [1] is based on the length of passwords and characters used to set the password. If a user selects words which is easy to guess or use frequently, the security level of authentication is reduced.

Many researchers have invented a safe and low cost authentication method to reduce the process or method of identity verification. There is a use of the password that the user has, and combine with the OTP (One Time Password) which randomized by the server, to prevent hacker data capture. This is because an encrypted passwords using HTTPS are not as secure as they should be [2]. The researchers Lamport [3] and Shimizu [4] have proposed password hashing for authentication whereas N.M. Haller [5] have proposed password hashing using a hashing function. However, these research depend on the 'traditional password' to help the authentication more secure. The users still have to remember the complex password.

In this paper we proposed the authentication model using the "Bundled CAPTCHA OTP" instead of the traditional password. This model can prevents password capture, and reduce user's tasks. We use e-mail as a way to send the Bundled CAPTCHA OTP picture to the user. Therefore, the hacker is difficult to capture the "Bundled CAPTCHA OTP" and do a replay attack because it will be changed in every sessions[2].

In this paper, we will discuss the basic theories and related research in Section 2. The proposed model will be presented in Section 3. Discussion and evaluation will be drawn in Section 4. We lastly conclude the paper in Section 5.

II. Background and Related Works

The Covr Security [6] is a non-password authentication method that is used for trading or electronic transactions. This platform is based on a smartphone and uses a 6-digit access code. The Covr Security sends the password to the smartphone via IP instead of SMS. It does not control user in web applications and network devices because it focuses on applications in the field of mobile application.

Mohamed Hamdy Eldefrawa, Muhammad Khurram Khan, and Khaled Alghathber presented One-Time Password System with Infinite Nested Hash Chains [7], It is a way to bring One Time Password (OTP) to a hash for endless encryption. N.M Haller present the S/Key One-time password system [5] which uses a hashing function checking the password for the value of the hash.

An authentication is a way to check who is accessing the system. The user will be required to prove that he/she is a real user; for example, his/her identity is in the university registration system. You will need to login using your username and password to prove yourself as a real user. And the authentication mechanism can also be done in several ways, such as using the following to prove identity.

- "What you have", such as a credit card or ATM card.
- "What you know", such as Password or PIN
- "What you are" (by using biometric), such as fingerprints. Retinal scan or face scans.

978-1-5386-8072-8/19/$31.00 ©2019 IEEE

However, these methods can be a combination use, to enhance the security of the system. Take "what you have" combine with "what you know" to be more effective, like swiping credit cards. The user must have a credit card and password to use the card securely.

CAPTCHA [8] [9] (Completely Automated Public Turing Computer and Humans Apart) is a technique used to test the user as a human, not automatic program (bot) by converting letters to images or distorted characters. Sometimes the letters (or numbers) are twisted. If hackers are attacking a CAPTCHA, they must write a special program that can read the distorted letters or numbers displayed on the screen, and then translate it correctly. If web programmers create messier distorted letter, it is more difficult to attack. Consequently, the security of the system will be increased.

OTP (One Time Password) [10] [11] is a one-time password to login in order to verify and confirm ownership of personal information in the system. To access the system again, the user must use a new set of OTP code. The OTP will be changed every time. Therefore, using OTP will help to protect and secure the system.

III. PROPOSED MODEL

In this Section, we will recall the traditional password authentication including CAPTCHA and OTP in Subsection A, and we will then explain the proposed model in the Subsection B.

A. *Authentication using a Traditional Password*

Considering an authentication by using the traditional password, the process of authentication will have a sequence of steps as follows.

Phase-I [Client]

1. User inputs the Username into the login form.
2. User inputs the Password into the login form.
3. User inputs the CAPTCHA into the login form.
4. User presses the login button.

Phase-II [Server]

5. Server checks the client's Username, client's Password, and client's CAPTCHA. If these fields are incorrect the server will send an error message to the user, and the user has to refill the correct values of these fields. If these fields are correct the server will continue to the next step.

6. Server generates a random OTP, and send the OTP to user's e-mail or user's SMS.

Phase-III [Client]

7. User opens the e-mail / SMS, and finds the OTP.
6. User and fills the OTP into the login page.

Phase-IV [Server]

7. Server checks the client's OTP. If the OTP is incorrect the server will send an error message to the user, and the user has to refill the correct values of the OTP. If the OTP is correct the server will send the main page to the user. In some systems, if user fill an incorrect OTP, the user may be forced to begin from the first step in Phase-I.

In the process of an authentication using traditional password, the user (client) needs to complete the username, password and CAPTCHA, follow by press a login button. This takes four steps for the user. In step 5, the server checks the username, password, and the CAPTCHA sent by the user. If these fields are incorrect the server will send an error message to the user, and the user has to refill the correct values to these fields. If these fields are correct the server will continue to step-6 by generating a random OTP, and send the OTP to user's e-mail or user's SMS. Consequently, the user has to take more two steps which are (1) opening user's e-mail / SMS in order to find the OTP, and (2) filling the OTP into the login page. Finally, the server will send the login page to the user if the OTP sent by the user is correct. Therefore, we can assume that in the process of an authentication using traditional password, the client needs to take 6 steps.

B. *Authentication using the "Bundled CAPTCHA OTP"*

We have designed the novel authentication model by bundling or merging the CAPTCHA and the OTP together into the one called "Bundled CAPTCHA OTP". We use the bundled CAPTCHA OTP instead of traditional password and other factors. The bundled CAPTCHA OTP will be generated by server and sent to the user's e-mail. The user has to register his/her e-mail address to the system before logging in. Thus, the e-mail will act as a possession factor for the user. Only owner of the e-mail can access the OTP. This means that the proposed method uses the possession factor to make the secure authentication. Moreover, the CAPTCHA help to prevent brute force attacks. Combining (bundling) the CAPTCHA and the OTP together can reduce number of factors needed by the system. Consequently, number of steps in the authentication process will be reduced as well. Our proposed model is different from Detchasit Pansa's model [12] because our proposed model does not depend on user's password.

Figure 1 shows the process of the proposed model. The process starts with the process number 1, client sending the username to the server so that the server knows and verifies who wants to login.

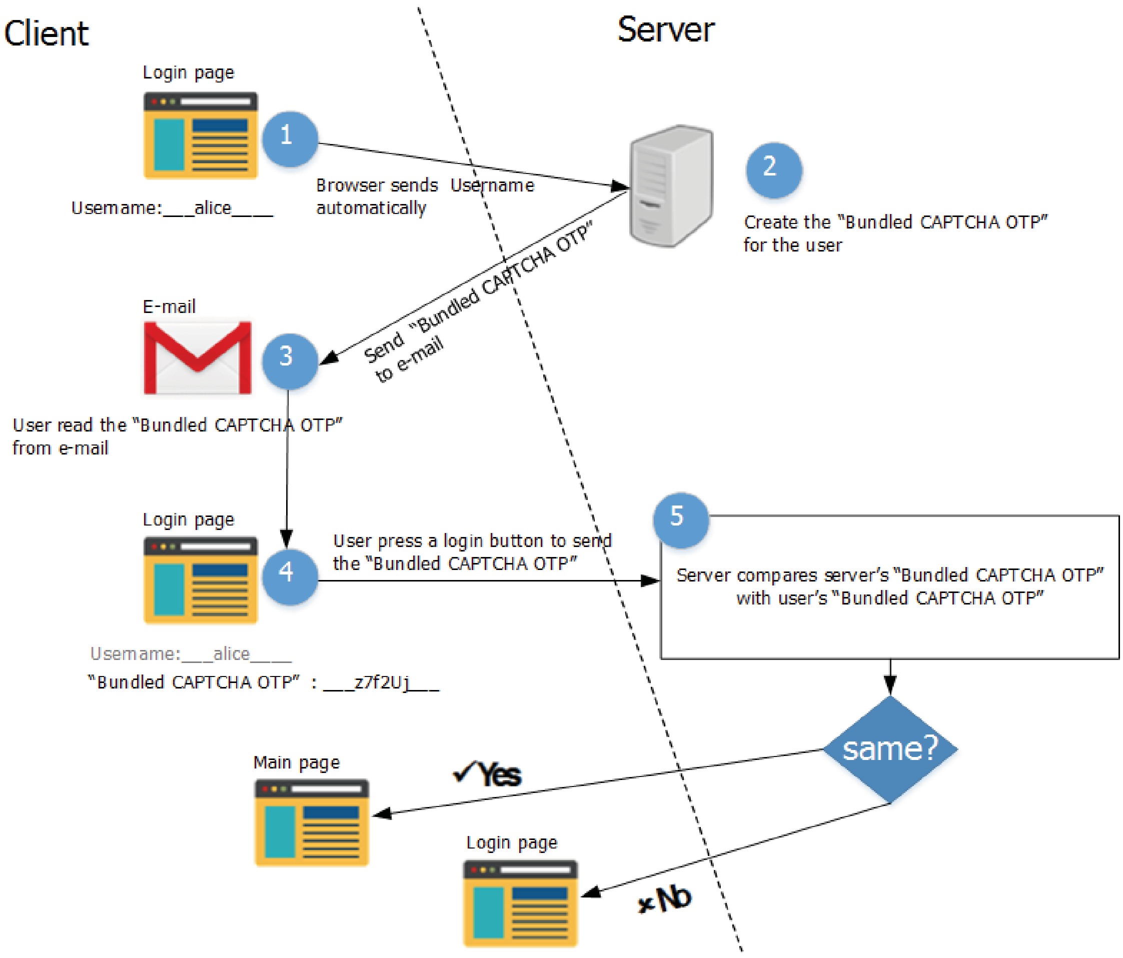
Client
Server
Login page
1
Username:___alice____
Browser sends Username automatically
2
Create the "Bundled CAPTCHA OTP" for the user
Send "Bundled CAPTCHA OTP" to e-mail
E-mail
3
User read the "Bundled CAPTCHA OTP" from e-mail
Login page
4
User press a login button to send the "Bundled CAPTCHA OTP"
Username:___alice____
"Bundled CAPTCHA OTP" : ___z7f2Uj___
5
Server compares server's "Bundled CAPTCHA OTP" with user's "Bundled CAPTCHA OTP"
same?
Main page
✓Yes
Login page
×No

Fig. 1. Model of authentication using the 'Bundled CAPTCHA OTP' insread of the traditional password

In process number 2, once the Server has received the username and verified that any user wants to authentication and username are available in server's database, a picture of the Bundled CAPTCHA OTP is sent to the e-mail of the user who wants to authenticate.

In process number 3, the client must open the mailbox to read the Bundled CAPTCHA OTP value sent from the server. The user will enter the value in the login page according to process number 4.

In process number 5, the server compares the Bundled CAPCHA OTP sent by the client with the Bundled CAPTCHA OTP on the server side. If they are matched, the system will allow the client to pass the authentication. If the comparison result is not matched, the client will not be allowed pass the authentication.

IV. Discussion and Evaluation

According to the propose model, steps needed by user have been reduced from 6 to 4 steps. The four steps are follows:

- Entering the Username
- Check e-mail for reading the Bundled CAPCHA OTP
- Entering the Bundled CAPCHA OTP into the login form
- Pressing the 'Login' button on the login form

In this model, the e-mail is the use of "What you have" and a number or a word in the Bundled CAPTCHA OTP is "What you know". This similar to using an ATM card (or a key card) with a PIN. With the proposed model, users do not need to remember complex passwords. They also do not need to protect their password from hacker.

Therefore, the proposed Bundled CAPTCHA OTP is more advanced and easy to use in comparison to the traditional password authentication.

TABLE I. A COMPARISON BETWEEN THE PROPOSED MODEL AND TRADITIONAL PASSWORD AUTHENTICATION

	Model			
	Traditional Password	Traditional Password + CAPTCHA	Traditional Password + CAPCHA + OTP	The proposed model
Security	Low	Low	High	High
Ease of use	Easy	Easy	Hard	Easy

Table I provides a comparison of three traditional password security and usage scenarios: (1) Traditional Password (2) Traditional Password + CAPTCHA (3) Traditional Password + CAPTCHA + OTP with (4) The proposed model (Bundled CAPTCHA OTP). According to the table, we found that the proposed model is more secure, and easier to use in comparison to the other traditional authentication models.

We evaluated the efficiency of the proposed method by measuring the time duration ('t') of the authentication. We record the time point which users entering the username as 't1', and then record the time point which the authentication is completed as 't2'. The time consumption ('t') for the authentication is t=t2-t1. We test with approximately 10 websites (5 websites use only password, and 4 websites use password and CAPTCHA or OTP). We also test approximately 30-40 times for each website and calculate average values of time consumption ('t'). We found that the proposed method does not take longer than websites which use the traditional scheme (password and CAPTCHA or OTP) as shown in Table II.

TABLE II. A COMPARISON OF TIME CONSUMPTION ('T') BETWEEN WEBSITES USING TRADITIONAL PASSWORD AUTHENTICATIONS AND THE PROPOSED METHOD

The tested websites	Category		Average values of time consumption (seconds)
	Normal Password	Password + CHAPTCHA or OTP	
www.facebook.com	✓	×	18.18
www.icloud.com	✓	×	20.26
www.sanook.com	✓	×	16.74
www.amazon.com	✓	×	14.84
www.mediafire.com	✓	×	16.74
www.2chatcha.com	×	✓	31.32
www.payeer.com	×	✓	28.56
www.faucethub.io	×	✓	26.49
www.freedoge.co.in	×	✓	27.63
The proposed method	×	×	27.01

Moreover, the Bundled CAPTCHA OTP (proposed in this paper) is easy to use because the users does not need to remember the complex passwords as have been used in the traditional authentication schemes.

V. CONCLUSION AND FUTURE WORKS

In this research, we have designed authentication model by combining a CAPTCHA and a One Time Password (OTP) altogether for easier operation with higher security. The system and users take fewer steps. Moreover, the users do not have to remember complicated passwords. We have designed a simple, step-by-step authentication model call the "Bundled CAPTCHA OTP". The proposed model use less resources, operate quickly. In future work, we plan to apply the Bundled CAPTCHA OTP to operate with biometric authentication, e.g., eye retina or human DNA to improve a level of security in the future world.

REFERENCE

[1] Wiedenbeck, S., et al., PassPoints: Design and longitudinal evaluation of a graphical password system. International journal of human-computer studies, 2005. 63(1-2): p. 102-127.

[2] Haller, N., et al., A one-time password system. 1998.

[3] Lamport, L., Password authentication with insecure communication. Communications of the ACM, 1981. 24(11): p. 770-772.

[4] Shimizu, A., A dynamic password authentication method using a one-way function. Systems and computers in Japan, 1991. 22(7): p. 32-40.

[5] Haller, N., The S/KEY one-time password system. 1995.

[6] Covr Security. 2018; Available from: https://www.covrsecurity.com/.

[7] Eldefrawy, M.H., M.K. Khan, and K. Alghathbar, One-time password system with infinite nested Hash chains, in Security Technology, Disaster Recovery and Business Continuity. 2010, Springer. p. 161-170.

[8] Von Ahn, L., et al. CAPTCHA: Using hard AI problems for security. in International Conference on the Theory and Applications of Cryptographic Techniques. 2003. Springer.

[9] Mori, G. and J. Malik. Recognizing objects in adversarial clutter: Breaking a visual CAPTCHA. in Computer Vision and Pattern Recognition, 2003. Proceedings. 2003 IEEE Computer Society Conference on. 2003. IEEE.

[10] Rayes, M.O., One-time password. Encyclopedia of Cryptography and Security, 2011: p. 885-887.

[11] Adams, C., One-Time Password, in Encyclopedia of Cryptography and Security. 2005, Springer. p. 446-446.

[12] Detchasit Pansa, and Thawatchai Chomsiri. "Integrating the Dynamic Password Authentication with Possession Factor and CAPTCHA". Proc. 2018 Joint 10th International Conference on Soft Computing and Intelligent Systems and 19th International Symposium on Advanced Intelligent Systems, 5-8 December 2018, Toyama, Japan, p. 530-535, 2018.