ISSN 2348 – 7968

Secure Access Level Using OTP, Pair Based Matrix and Captcha

Mr. Suraj Adhav, Miss. Sonali Khamkar, Miss. Pranoti Barge and Miss. Shital Kharde
Department of Computer, Savitribai Phule Pune University, Pune,
Maharashtra, India

Abstract

Data Security is the study of methods of protecting data from unauthorized disclosure and modification .Text password is popular but become a older form of user authentication on websites due to its simplicity. These passwords are prone to be stolen and compromised under different threats and vulnerabilities like Dictionary attack, Shoulder surfing, eves dropping, etc. Then Captcha technology come into existence but again it fails as an individual .Further graphical passwords are coming to the existence but the graphical passwords have their own disadvantages like they require more time to Authenticate and the usability issues .That means individually all schemes has their own drawbacks and less secure but together they provide more security. So our paper provides OTP , Pair Based Matrix and Captcha technologies together in such a way that provides higher level of security .This technique is relatively new approach towards information security.

Keywords: *Password Reuse Attack, Password Stealing Attack, User Authentication, Pair Based Matrix, Captcha.*

1. Introduction

The method which we used earlier is a Textual password in which the password which are lengthy is considered as secured password but the lengthy passwords is difficult to remember thus the user pick short password but short password are easily crack or hack. The new technique is proposed which is graphical password scheme. This graphical password schemes overcome the shoulder surfing problem in Textual password but these schemes have also some limitations and drawbacks like more time for Authentication and it's quite expensive. So we proposed new password authentication technique is Session password .In which two new schemes are used Hybrid Textual Scheme and Pair-based Authentication scheme. Its gives the options for user to select the password as a color or alphanumerical grid. When user logins into the system new password is created for each session and that session is remains until user gets log out. For each new session new password is generated by system and that password is only valid for that particular session. When session is terminated the password is no longer in use.

Now a day's millions of peoples are using internet daily and day by day this number is increasing. Today for authentication user name and password is used the generally .so the security must be provided so that we can prevent hackers from accessing the account data. So authentication must needed in order to protect user accounts. Authentication is provided by using next techniques i.e. pair based authentication scheme. The user has to first register its fixed password only once at the time of registration. In a pair based scheme Textual passwords are provided.

2. OTP

In this paper, we propose a user authentication protocol called one time password (OTP) which leverages a user’s cell phone and short message service (SMS) that prevent password stealing and password reuse attacks. In our opinion, it is difficult to thwart password reuse attacks from such scheme where the users have to remember something. It has been observed that the main cause of stealing password attacks is when users uses the passwords to untrusted public computers. Therefore, the main concept of OTP is free users from having to remember or typing any passwords into conventional computers for authentication. Unlike generic user authentication, OTP involves a new component, the cellphone, which is used to generate one-time passwords and as a new communication channel, SMS, which is used to transmit authentication messages to it. OTP presents the following advantages.

2.1 Anti-malware

Malware like keylogger that gather sensitive information from users computer, especially their passwords are amazingly common. In OTP, users are able to log into web services with the password that is randomly generated. That’s the reason malware cannot obtain a user’s password from untrusted computers.

2.2 Phishing Protection

Adversaries often launch phishing attacks for stealing users' passwords by deceiving users when they connect to forged websites. As mentioned above, OTP allows users to successfully log into websites without revealing passwords to the computers. Users who adopt OTP are guaranteed to face phishing attacks.

2.3 Secure Registration and Recovery

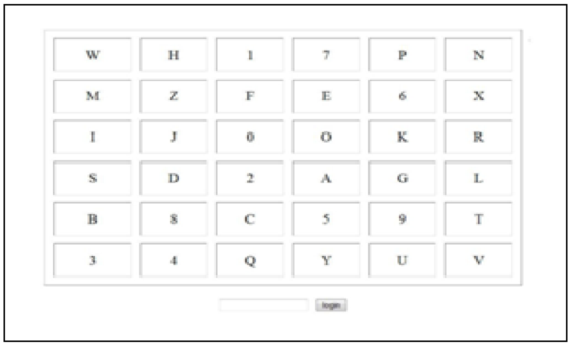
In OTP, SMS is an out-of-band communication interface. OTP cooperates with the telecommunication service provider (TSP) in order to obtain the correct phone numbers of users respectively. SMS aids OTP in establishing a secure channel for message exchange in the registration as well as recovery phases. Recovery phase is designed to deal with cases where a user loses his cell phone or forget his password. With the aid of new SIM cards, OTP still works on new cell phones.

2.4 Password Reuse Prevention and Weak Password Avoidance

OTP achieves one-time password approach in which the cell phone automatically derives different passwords for each login. We can say that the password is different during each login and because of this approach, users do not need to remember any password for login. They only keep a long term password for accessing their data, and leave the rest of the work to OTP.

3. Pair Based Matrix

The second level is Pair Based Matrix in which we proposed new password authentication technique is Session password .In which new scheme are used Pair-based Authentication scheme. Its gives the options for user to select the password as alphanumerical grid. Whenever user logins into the system every time new session is created and that session remains as it is until user gets log out. For each new session the new password is generated by system and that password is valid only for that particular session. When session is terminated the password is no longer for use.

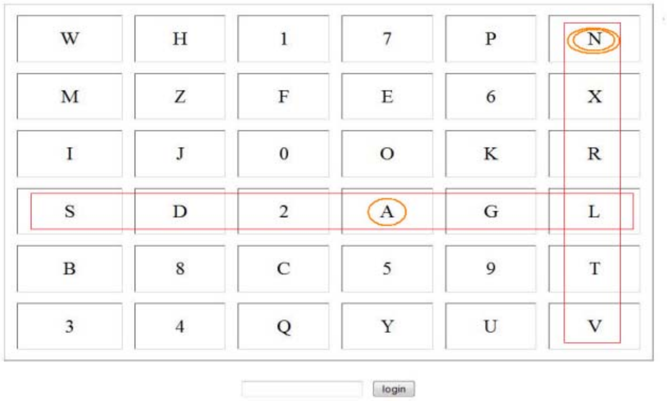


W	H	1	7	P	N
M	Z	F	E	6	X
I	J	0	O	K	R
S	D	2	A	G	L
B	8	C	5	9	T
3	4	Q	Y	U	V

Fig. 1 Login interface.

User has to enter the password at the time of registration. The length of password is minimum 8 characters. At the time of login we create the session password based on users original password entered at the time of registration by using 6x6 matrix grid provided on login page.

In pair based mechanism the user has to consider his/her password in terms of pairs. The pair based technique consist of 6x6 matrix in which alphabets and digits are displayed. In this no alphabets and digits are repeated and these alphabets and digits are displayed in random manner and it will change each time when we refresh the page or the new session is started. In the pair the first character is used to select the row and the second character is used to select the column. Then the user has to identify intersection character as password for that session only. If the password length is n then session password length = n/2. When particular session is end then password which is used for that session is also destroyed.



W	H	1	7	P	N
M	Z	F	E	6	X
I	J	0	O	K	R
S	D	2	A	G	L
B	8	C	5	9	T
3	4	Q	Y	U	V

Fig. 2 Intersection letter for pair AN

4. Captcha

Our next level is Captcha. It was introduced in to provide higher level in a user authentication protocol, which we call *Captcha-based Password Authentication (CbPA) protocol*, to counter online dictionary attacks. The CbPA-protocol in requires solving a Captcha challenge after inputting a valid pair of user ID and password until and unless a valid browser cookie is received. Here the Captcha is used with Pair Based Matrix so that higher security can be achieved. Here the blur and light Captcha screen with captcha digits is displayed .The user has to first insert the password based on Pair Based Matrix in the text box and immediately after that captcha is being filled and this merged passed is the final password.

Captcha was also used with recognition-based graphical passwords to address spyware, wherein a text Captcha is displayed below each image; a user locates her own pass-images from decoy images, and enters the characters at specific locations of the Captcha below each pass-image as her password during authentication. These specific locations were selected for each pass-image during password creation as a part of the password. In the above schemes, Captcha is an independent entity, used together with a text or graphical password. On the contrary, a CaRP is both a Captcha and a graphical password scheme, which are intrinsically combined into a single entity.

5. Conclusion

The previous techniques does not have that much capability to secure password from hackers or third party location .because in this techniques only one password is used for each and every session and password is transfer for authentication of users. Thus these passwords are easily hacked by hackers. We proposed a system called Session password, in this technique it provides a new password for each particular session and need not to transfer password form server each time for authentication purpose. Hence Session password scheme provides more security than the other existed systems.

References

[1] Hung-Min Sun, Yao-Hsin Chen, and Yue-Hsun Lin, oPass: “A User Authentication Protocol Resistant to Password Stealing and Password Reuse Attacks”, Ieee Transactions On Information Forensics And Security, Vol. 7, No. 2, April 2012.

[2] Bin B. Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, and Ning Xu, "Captcha as Graphical Passwords—A New Security Primitive Based on Hard AI Problems", Ieee Transactions On Information Forensics And Security, Vol. 9, No. 6, June 2014

[3] Prof. Bogiri Nagaraju Computer KJCOEMR Pune, Maharashtra,"Authentication Schemes for Session Passwords using Hybrid and Paired based Techniques", *Multidisciplinary Journal of Research in Engineering and Technology Volume 1, Issue 2, Pg.175-182*

[4] R. Dhamija, and A. Perrig. “Déjà Vu: A User Study Using Images for Authentication”. In 9 th USENIX Security Symposium, 2000.

[5] Jermyn, I., Mayer A., Monrose, F., Reiter, M., and Rubin., “The design and analysis of graphical passwords” in

Proceedings of USENIX Security Symposium, August 1999.

[6] R. Biddle, S. Chiasson, and P. C. van Oorschot, “Graphical passwords: Learning from the first twelve years,” ACM Comput. Surveys, vol. 44, no. 4, 2012.

[7] H. Tao and C. Adams, “Pass-Go: A proposal to improve the usability of graphical passwords,” Int. J. Netw. Security, vol. 7, no. 2, pp. 273–292, 2008.