International Journal of Pure and Applied Mathematics
Volume 117 No. 21 2017, 961-965
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

Dynamic Cued Click Point Algorithm to Provide Cryptographic Password Authentication

P. Ashok* R.R. Prianka[2] R. Lavanya[3] R.G. Gokila[4]
Assistant Professor
*Department of Computer Science and Engineering[1, 2]
Department of Information Technology[3, 4]
Sri Sai Ram Institute of Technology, Chennai, India[1]
E.G.S Pillay Engineering College, Nagapattinam, India[3,4]
RMK College of Engineering and Technology[2]
*ashokit009@gmail.com

Abstract: Nowadays, password based authentication is one the most common way of authentication for most of the user logins. However, the advancement in technology also posing many threats for the password authentication systems. Everybody will be keen to know others password. But there exists a very few who is very keen to devise a new authentication. In this paper, we have proposed a more advanced password authentication method yet a simple one which gives a tough competition for the attacker to break the password. For this, we are providing a special key-display interface to assist the modified cued click point's technique which helps in the more sophisticated dynamic authentication method. This interface helps to break the single password into a combination of 4 passwords and also adds three more password strings to the current password which is entered. It also uses a special one way encryption algorithm called Nesting 93 which is developed explicitly for this system. It helps to prevent almost any kind of attacks.

Keywords: Authentication, password, security, encryption, authentication protocol, and password based authentication, Cued click points

1. Introduction

Security has been the most annoying problem in the recent years. Especially providing access to an authenticated user is definitely not as easy as it looks. All the users may want to have a more secured authentication system but no one seems to be compromised with the usability of the system. While making the authentication scheme more complex can be considered as one way but it is very important to have the complexity in the attacker side and not in the user side itself. To address this problem, we provide the combination of the password field and the key interface along with the modified cued click points which helps to produce a more sophisticated authentication scheme.

Cued Click Points (CCP) was generally designed to minimize pattern and to minimize the usefulness of hotspots for attackers. Instead of 3 click points on one image, Cued Click Points uses single click on three dissimilar images[1, 2, 3]. In modified CCP, instead of using click points on images we use Click Points on the key interface which was provided and this helps to break the password into a combination of 4 passwords. Also a one way encryption technique has been explicitly developed for this system. All these days we have been using one way hashing algorithm. It is a logical algorithm that helps in mapping information of whimsical range to a byte string of a specified size (an hashing function) which has been designed to also be a one way function, that is a function which is not feasible to transpose. The only way to recreate the input data from an ideal cryptographic hash function's output is to attempt a brute-force search of possible inputs to see if they produce a match, or use a "rainbow table" of matched hashes. This makes it a disadvantage for the system. Cued Click Points (CCP) a cued-recollect graphical password technique where users click on any one point in an image for the sequence of images. The upcoming image which is shown to the user is based on the previous click point. The results were positive. Performance was very excellent in terms of speed accuracy and number of mistakes. Users preferred cued click points to Pass Points saying that choosing and remembering only one point in one image is easier, and that seeing each image triggered their memory of where the respective point was located. Cued click points appears to allow greater security than Pass Points; the workload for attackers of CCP can be arbitrarily increased by augmenting the number of images in the system. Recognition may it be through images or others is the easiest way for human memory where pure or complete recollect is most difficult as the data must be accessed from memory with no triggers [12]. Cued recollect through images falling somewhere between these two since they offers cue which should showcase context and trigger the stored memory. The disadvantage of the cued click point system is, it is very tedious to click the images every time when you login to the system and it's too time consuming. There comes the system to overcome the disadvantage. The image that has been used for cued click points has been modified as keypad system in the proposed system interface. The system has been developed so as to provide flexibility to the users in all possible way and to increase the work of the hackers. The entire encryption technique resides inside the key interface of the system. Another way of encrypting your password that has been used widely but more insecurely is encryption using key values. For encryption algorithms, a key specifies the transformation of plaintext into cipher text, and vice versa for decryption algorithms. Keys also sp entication
co

2. Related Works

Password authentication scheme using session based passwords in which it uses two session techniques for generating session bases passwords one is using the set of pairs of hidden passwords and the other is using the color rating while setting the password but both uses the grid structure to generate the password [4,5,6]. Knowledge based authentication scheme which uses a combination of both text and graphical passwords and persuasive cued click points assist in choosing the graphical passwords [1, 7, and 8]. A study on various authentication schemes and provides a graphical authentication technique using recognition and recall based techniques [9]. A web based password authentication scheme which resolves the problems in the traditional password authentication or digital signature using Single-Block Hash Function [10]. Deals with secure authentication and transaction protocol by combining digital certificates and dynamic password by realizing the mutual authentication that exists between the client and the server [11].In Pass Points, the passwords have certain click points on a particular image that is used as click-points for passwords by repeating the sequence of clicks in the proper order, but security is major drawback since hacker could able to guess the password. Cued Click Points (CCP) is a scheme where users pick one click point per image until selected images. The screen displays one image at a time; that image is replaced by the next image as soon as a user selects a click point. The system determines the next image to display based on the user's click point on the current image. Suppose, user enters an incorrect click-point, the image will also be incorrect. Unknown or hacker is who was saw an unrecognized image will know that they made an error with their previous click-point. Conversely, this implicit feedback is not helpful to an attacker who does not know the expected sequence of image [13].Persuasive cued click points (PCCP) during password creation; normally the image is dimmed except for a small view port area that is randomly positioned on the image. Users must select a image password (click point) within the current image. If they are unable or unwilling to select a point in the current image, they may use the Shuffle button to randomly reposition the image. The view port guides users to select more random passwords that are less likely to include hotspots (are shown in figure3). A user who is determined to reach a certain click point may still Shuffle until the view port moves to the specific location, but this will take lot of time and more tedious process [13].

3. PASSWORD CUED CLICK POINTS RECOGNITION (CCRP)

In this, the proposed system consists of a password field along with the special key display interface. This interface consists of ten set of keys numbered from 0 to 9. Each key is assigned to a set of twelve digit alpha numeric character and the constraint that has been specified to every single user of the system is that, the user has to select at least three to five clicks in the key interface each time when the user wants to login to the system. The clicks in the interface are made along with the password. User can just type the password in the password field and that password can be an alpha numeric one. But the other constrain is the password should eventually begin with an alphabet. The flexibility given to the user in this system is the user can have the click points anywhere in the password. May it be at the last or at the middle or in between the password? The entire encryption of the system resides inside the keys. The keys that are typed also belongs to the password, i.e., the keys selected belongs to your password but the keys that have been selected will not be visible in password field. If suppose your password is "crypt124" where the numerical have been clicked through the mouse in the key interface, the numerical values that have been clicked will not be visible in the password field even as a hidden text. Here comes the other advantage of preventing our system from being attacked from brute force attack. This system breaks the user's conventional single password into a set of four passwords and also adds a set of three strings while entering using the interface. So typically it sends seven set of strings to the encryption process in spite of the single password which is given by the user. This seven set of strings is taken as the input for the one way encryption algorithm called One-time Data Division (ODD). when the user enters the password, for example if the user enters the password as "cryptopassx3y2z1" then in this password the numeric characters 3,2 and 1 are the numbers which should be used in the interface. The sequence will be explained as follows

1) User enters the password "cryptopassx" in the password field.
2) User clicks the key '3" in the key-interface while the content in the password field is still "cryptopassx".
3) Now the current input to the system is "cryptopassx" and the six digit alpha numeric string which is assigned to key "3"
3) Now the user again enters "y" in password field along with "cryptopassx". Now the password in password field is "cryptopassxy".
4) Now the user clicks "2" in the interface while the content in the password field is still "cryptopassxy". Now the current input
to the string is of four strings two from password field and two from the interface.
5) Again the points 3 and 4 are repeated.
6) Finally when user enters the submit button the current password field content "cryptopassxyz" will also be taken as the input. Therefore totally seven strings will be passed to the encryption algorithm. Four from the password field and three from the interface.
7) This seven set of strings will be used in the encryption algorithm called "One-time Data Division (ODD)" which is developed explicitly for this system.

After the encryption process, we will get an encrypted string which consists of all the 93 printable characters available except the blank space. This encrypted password is made of up of exactly 256 characters which will be stored in the database. So whenever the authentication occurs, the encrypted password from the user is compared with the encrypted password stored in the database. This is a one way encryption algorithm so it cannot be decrypted to its original form. If the us me.

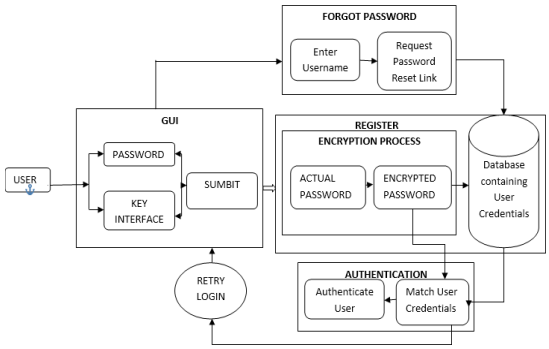

Figure 1.Cued click points recognition

It is named as "One-time Data Division (ODD)" since it uses the Divide as well as Nest concept which can be inferred from the name itself. 93 is derived from the fact that our final encrypted password consists of 93 printable characters in the ASCII value range from 33 to 125 which includes all the numbers, characters & special characters. The Divide and Nest concept is that each password string gets divided into a single character and the alpha numeric string is inserted or nested between those characters and then combined and the process goes on for the rest of the string then it goes through a set of several transformations which remains the core of the algorithm. This algorithm produces a string of 256 characters which is a combination of all the 93printable characters except the blank space. Since this is a one way encryption algorithm, even the system administrator doesn't have any rights to access the user profiles and the user profile is highly secured. This encryption algorithm can be easily customized for individual organization and instead of six digit alphanumeric characters we can use alpha numeric string of different lengths which increases linearly with 2. As the length increases, the complexity increases and the pattern formation becomes further strong.

Algorithm:

Initialize:

Strings p ->{ p_1, p_2, p_3, p_4}
#password Key values c ->{c_1, c_2,
c_3} # key value
{I_1, I_2, I_3}= null #intermediate string

Joined in a special way to produce an intermediate string

$p_1 \bowtie c_1$ —> I_1; $P_2 \bowtie c_2$ —> I_2; $P_3 \bowtie c_3$ —>I_3;
$I_3 \bowtie p_4$ —>I_4; I_4 —>ASCII;

lossy data compression

ASCII—>s s = =Φ
while (if more character in char stream) c=(next character in
the char stream) if=(string S+C in the dictionary)
s=s+c
else//(if S is empty,zero is its codeword) Output the code word corresponding to S
Output C
Add the string S+C to the dictionary s= =Φ
if(s ==Φ)
Output the code word → S end

Output

Final encrypted password which consists of exactly 256 characters

4. Performance Evaluation

Table 1. Sucesss rate comparison

	Persuasive Cued Click Point		**Password Cued Click Point**	
	Success rate (%)	**Security success rate (%)**	**Success rate (%)**	**Security success rate (%)**
Attempt 1	4/5 (80)	20	3/5 (60)	40
Attempt 2	3/5 (60)	40	2/5 (40)	60
Attempt 3	5/5 (100)	0	4/5 (80)	20
		20 (mean rate)		40 (mean rate)

It indicates the success rate at the time of few attempts when a password entered. Success rates were considered as the number of trials finished without making errors or restarts. In this observation, initially three attempts are considered and each attempt has a password which includes clicking on few click values in-between password. In comparison, Password Cued Click Point reported higher success rate then Persuasive Cued ClickPoint

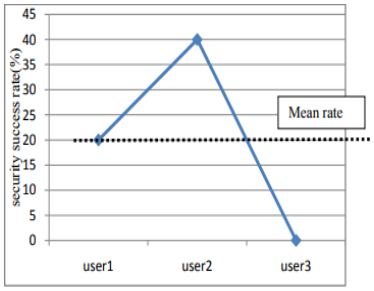

Figure 2. Persuasive Cued Click Point

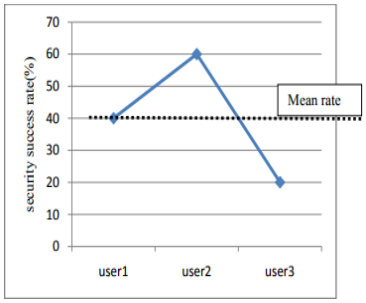

Figure 3, Password Cued Click Point

Results

This password authentication scheme has been successfully developed and tested under various user credentials. Since the authentication is due to the textual password scheme combined with the modified cued click points it produces 100% success rate in authenticating each user. Generally textual data are relatively easier to compare than the graphical one while authenticating because of the accuracy in textual data.

5. Conclusion and future works

The significance of selecting an environment appropriate Authentication method is perhaps the most important decision in designing secure systems. This method stands superior to the other password authentication system. It provides more security with less complexity and saves more time. The modified CCP technique along with the interface helps in providing a more sophisticated authentication mechanism with the textual passwords. Since it uses a special one-way encryption algorithm, even the administrator doesn't have any access to the user profiles. If the user forgets his password then he can only reset the password by requesting a password reset link using his username from the administrator which will be sent to the registered e-mail id. And also the algorithm can be customized to produce various different encrypted passwords. This customization of the encryption algorithm makes it very useful for various organizations suiting its requirements. The idea can be extended by removing the mandatory three to five key constraints and giving the user, the freedom to choose any number of keys. This choice of keys makes it much more complex for the attacker to guess or hack the password which in turn provides a stronger and a better authentication system. Also we can provide the user with password reset link in the registered mobile number too

References

[1] Smita Chaturvedi, Rekha Sharma "Securing Text and Image Password Using the Combinations of Persuasive Cued Click Points with Improved Advanced Encryption Standard", International Conference on Advanced Computing Technologies and Applications (ICACTA-2015).

[2] Sonia Chiasson, Elizabeth Stobert, Alain Forget, Robert Biddle,Paul C. van Oorschot "Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism" IEEE Transactions on Dependable and Secure Computing, Volume 9, No. 2, March/April 2012

[3] Binitha V.M. "Persuasive Cued Click Based Graphical Password with Scrambling for Knowledge Based Authentication Technique withImage Scrambling" IOSR Journal of Computer Engineering (IOSR-JCE), e-ISSN: 2278-0661, p- ISSN: 2278-8727, Volume 13, Issue 2 (July - Aug. 2013)

[4] Sanket Prabhu, Vaibhav Shah "Authentication Using Session Based Passwords", International Conference on AdvancedComputing Technologies and Applications (ICACTA-2015).

[5]S.Balaji, Lakshmi.A, V.Revanth, M.Saragini,V.Venkateswara Reddy "Authentication Techniques for Engendering Session Passwords with Colors and Text",Advances in Information Technology and Management, Vol. 1,No.2,2012

[6] M.Sreelatha, M.Shashi, M.Anirudh, M.D.Sultan Ahamer, V.Manoj Kumar "Authentication Schemes for Session Passwords using Color and Images", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3, May 2011

[7] Smita Chaturvedi, Rekha Sharma "Securing Image Password by using Persuasive Cued Click Points with AES Algorithm",
International Journal of Computer Science and Information Technologies(IJCSIT), Vol. 5 (4) , 2014

[8] S. Chiasson, A.Forget, E.Stobert, P.Van Oorschot and R.Biddle "Multiple Password Interfernce in Text and Click-based graphical passwords in ACM Computer and Communications Security (CCS), Nov 2012

[9] S. Jayashri, M.V.Ishwarya, K. RameshKumar, "A Study on Authentication Protocols", International Journal of Emerging Technology & Research, Volume 1, Issue 4,May-June 2014.

[10] Shi-Qi Wang, Jing-Ya Wang, Young-Zhen Li, "The Web Security Password Authentication based the Single – Block Hash Function", International Conference on Electronic Engineering and Computer Science, 2013.

[11] Jing Liu, Qingyu Chen, Jianwei Liu, Jianhua Chen " Design of Secure Authentication and Transaction Protocol based on Digital Certificates and Dynamic Password", International Conference on Computer Science and Service System (CSSS),2011

[12] P. R. Devale Shrikala M. Deshmukh, Anil B. Pawar "Persuasive Cued Click Points with Click Draw Based Graphical Password Scheme", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-2, May 2013

[13] M .Swathi, M. V. Jagannatha Reddy "Authentication Using Persuasive Cued Click Points", International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181, Vol. 2 Issue 7, July – 2013

[14] [illegible] "GRAPHICAL PASSWORD AUTHENTICATION USING PERSUASIVE CUED