International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume2, Issue 6 (June '2016)

EXPLORING SECURITY USING ONE TIME DYNAMIC PERSUASIVE CUED CLICK POINT

Charles Vijay,
Department of Computer Science and Engineering,
Sasurie Academy of Engineering,
Coimbatore,India.

R.Saranya,
Assistant Professor,
Department of Computer Science and Engineering,
Sasurie Academy of Engineering,
Coimbatore, India.

Abstract: Now-a-days security is a necessary component for every infrastructure due to increase in hacking activities. Many approaches have been used to improve the efficiency of security systems. To make the process even better, the One Time Dynamic Persuasive Cued Click-Point (OTD-PCCP) graphical password scheme is proposed. This paper proposes the selection of password in a powerful secure space, where greater security is assured. In order to improve the security, the password selection utilizes the click-based graphical passwords that allow the users to choose their passwords randomly. The security and the usability of the proposed system are assessed thoroughly. A sequence of images is selected and those images are split in grid format. Split regions are then numbered in any random order. When the user attempts to login, the system generates a One-Time Password (OTP). Received OTP are numbers that represent the indexed region of the image. Clicking on the same indexed region with respect to the received OTP make the user authentic.

Keywords: One Time Dynamic- Persuasive Cued Click-Point , One Time Password, Graphical passwords, authentication, persuasive technology,security.

I. INTRODUCTION

Authentication is the method of determining someone or something is who or what it is declared to be. Now a days most common form of authentication is login passwords. Knowledge of the password is the guarantee that the user is original. The user must use the previously declared password to get authentic. The weakness of these kinds of traditional authentication systems is that passwords can often be stolen, or forgotten or accidentally revealed. Computer/network security rest on two simple goals. First and the foremost is denying unauthorized access to resources and secondly, ensuring that authorized persons can access the resources whenever they need. These objectives can be accomplished with much number of components. First and the most important way is to allocate access permissions to resources that help define which users can or cannot gain access to those resources and under what conditions. Authentication is an inevitable part of a modern security model. This process helps confirming the identity of a user that is trying to access a resources or log on. There are many different types of authentication mechanisms, but all serve the same purpose. Software authentications are done mainly using passwords, patterns and biometrics. Authentication can be accomplished in many ways. The importance of selecting an environment appropriate authentication method is perhaps the most crucial decision in designing secure systems Mostly, access to a computer system is based on the alphanumeric passwords. The problem arises in terms of two fundamental requirements:

- The Password should be unforgettable and the user always prefers user friendly authentication procedures.
- Passwords should be very secure i.e., hard to guess, changed frequently and should be varied for different accounts of the same user. Their password should not be stored or written down as plain text.

To overcome the issues related with text password dependent secure authentication framework, numerous investigators have proposed different concepts of authentication mechanisms and developed the graphical password system. Graphical password systems are very efficient alternative to conventional authentication system, especially the text password system. The main objective of the proposed work is to improve the security, make it user friendly and reduce the guessing probability of the password. Thus, in the proposed work to enhance the security level of existing graphical authentication system, three level authentication such as graphical password, text password and automated one time password (OTP) is implemented. The OTP is received via phone or email which is given at the time registration by the user.

II. RELATED WORK

In [3] author proposed a method named Cued Click Points (CCP) to resolve the authentication. The basic idea of the CCP depends on the human identification pattern. For example recollecting and remembering the graphical patterns instead of memorizing a sequence of characters. User always find it very difficult to remember long random, meaningless alphanumeric string as passwords. These difficulties are reduced by using CCP. The information system is easier and more open to access via the internet, at the same time need for security also increased. Today's world of network, computing can be a frightening and dangerous place with attackers, hackers, crackers, scammers, and spammers at work. A home computer user installing high-speed internet service and a wireless network cannot even begin without a strong firewall and up-to-date virus protection. The community of security researchers and practitioners has come in response to threats, one hand increasing research innovation and on the other hand rapid vigilance in practice. However, it is now becoming widely

IJCRCST © 2016 | All Rights Reserved

recognized that security is also basically a human-computer interaction (HCI) problem. Thus, the author in [4] presents an enhanced usability goal for authentication framework to support the user in selecting the best and efficient password. As a result, graphical password system is used with the One Time Password (OTP) method.

The major problem of knowledge based authentication, especially text based password is the high probability of guess ability. Thus, in [5] author presents Persuasive Cued Click points (PCCP) which includes the security and usability evaluation. Persuasive Technology is not a method to implement; instead it is a technology which inspires the people to behave in a desired manner. An authentication system which implements Persuasive Technology should continuously monitor the system and create inspiration for users to select strong password for authentication. For making this system more effective, the user must not ignore the persuasive elements and resultant password must be memorable. Idea behind Persuasive Cued Click Point (PCCP) is to select random point as password from provided images. PCCP provides a strong way to communicate or select a strong password between provided images. It also gives suggestion for selecting random images. Previous work on Persuasive Cued Click Point (PCCP) ie Cued Click Point (CCP) shows that it is more secure method for authentication, which selects random point on images by using higher priority which in turn avoid guessing attacks. Visual attention research shows that dissimilar people are involved to the same expectable area on the images. This advises that if user selects their own click-based graphical password without direction, hotspots will be a question. In order to overcome the problem of hotspots persuasive factor is implemented. Here user is asked to choose the click point from a system generated view port thereby reducing the problem of hotspots.

In [6] author discussed a novel authentication system based on a graphical password which utilizes images for the illustration of the password and to authenticate the user from unauthorized attacks. This approach is emerging for the authentication resolution. The main aim of this proposed approach is to decrease the guessing attack, brute force attack and dictionary attack. The Persuasive Cued Click-Points graphical password scheme is assessed in [7] in terms of security and usability and using the implementation considerations. The significant aim of usability for the authentication system based on knowledge, is to help the users while choosing the passwords with high degree of security in the effective security space. In order to make the users' selection in click-based graphical passwords, persuasion is used which attempts to choose the passwords which will be more random and difficult to guess.

III. ONE TIME DYNAMIC PERSUASIVE CUED CLICK POINTS

The main objective of the present study is to improve the security system by the integration of graphical such as Persuasive Cued Click-Points (as shown in Figure 1), text and auto generated OTP. The OTP is received via mobile or email to an authentic user or registered user.

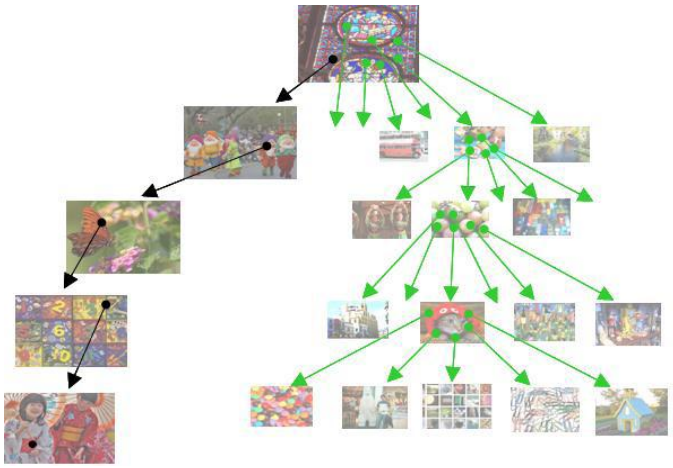

Figure 1 :Click-based graphical password

The text based password contains numbers, alphabets or any character. Most widely used authentication mechanism is text based password authentication. However it is evident that most users are frustrated with their experience with this traditional authentication method in general. Due to the increasing security issues, users are forced to choose very formal authentication methods even in day to day common lives.

Graphical authentication systems works in the same way as any of the knowledge based traditional authentication systems work. It verifies the knowledge of secret that the user shares with the system. The only difference with other authentication system is that this system relies on human visual memory. In OTD-PCCP, first, user has to choose a sequence of images and each image is split into a grid format (say 3x3) and this split region are numbered randomly from one to nine (as shown in Figure 2) During the time of login, username is verified and as soon as the verification, system generates a One Time Password and this OTP is sent to the user's mobile and mail. For entering into the system, user has to click on the same indexed location of the image as in the received message. Considering the difficulty of memorizing the indexed order, this order is been send to user's mail for reference. So the user has nothing to memorize.

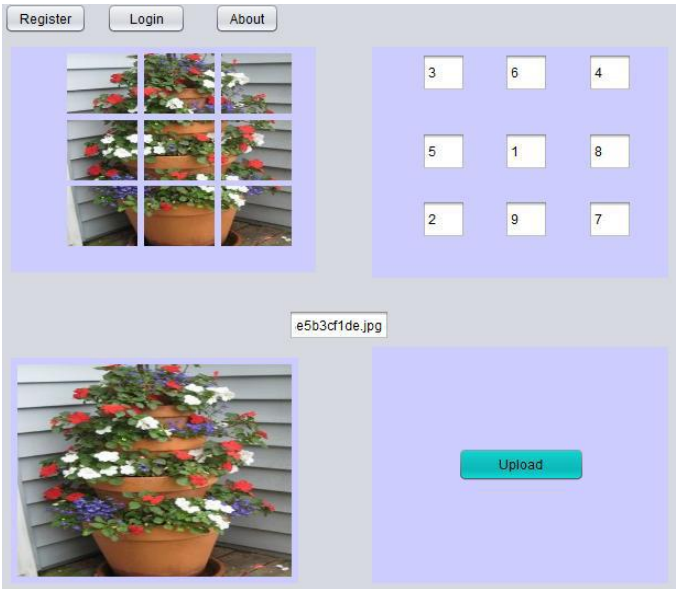

Figure 2: Uploading, splitting and numbering of image

Received OTP are numbers and represents the indexed region of the image. Clicking on the same indexed region with respect to the received OTP make the user authentic. In this proposed work, the OTD-PCCP password is made up of one click point on each image. OTP is numeric password, which is only valid for one login. The length of OTP is based on how many images the user chose during the registration. The proposed system deals with five images and a five digit OTP. The authentic user will be conversant of this OTP through mobile or email-id. The overall system architecture is as shown in Figure 3.

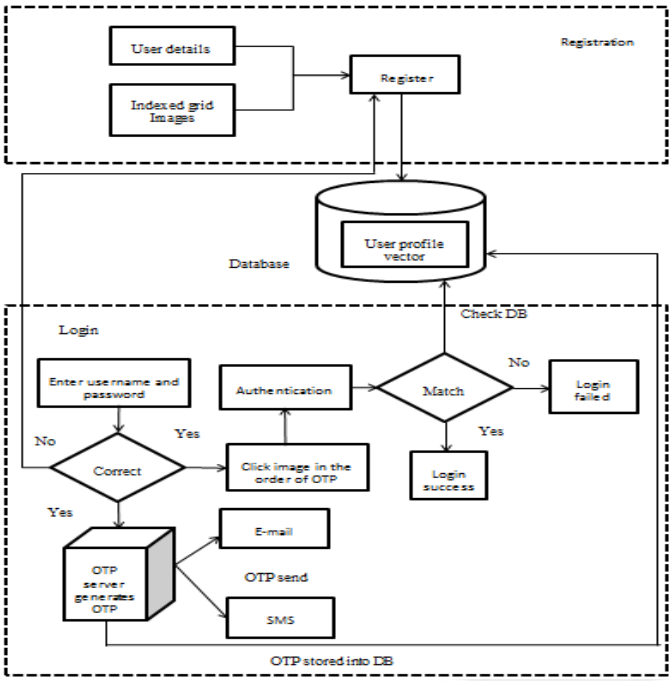

Figure 4: System Architecture

Finally, the user will enter into the system by using all three correct passwords. The three types of password authentication system are combined together so as to improve the security of the proposed system.

Existing graphical based authentication mechanisms have its own security issues like hotspots, shoulder surfing etc. The proposed OTD-PCCP over comes this problems of existing methods by generating OTP every time when the user comes for login. Advantages of the proposed OTD-PCCP are resilient to impersonation, resilient to observation, resilient to guessing. OTD-PCCP improves the security of image authentication and the users are secure.

IV. RESULTS AND DISCUSSIONS

By evaluating the usability of One Time Dynamic Persuasive Cued Click Points(OTD-PCCP) through several performance measures and to place the results in context, proposed system is compared with other authentication schemes currently used like password, biometrics etc. Statistical analysis was used to determine whether differences in the data reflected actual differences between conditions or have occurred by chance.

Following are the performance measures used for memorability and usability analysis and evaluation.

- Time for password creation.
- Time taken for login.
- Time taken for recalling password and
- Login and recall success rates.

A. Time for Password Creation

In this modern computer world, security is not an easy thing to acquire. It comes with lot of works, measures, efforts etc. Users always tend to avoid long registration processes that come before the login process. Security measures won't be user friendly every time, but this little effort of spending time in registering with proper user details can help protecting valuable data from outsiders. Considering the human nature of neglecting long registration processes, here in OTD-PCCP only few important fields are been asked to be fill by the user. Here pictures chosen by the user act as the password. So user must be careful with their choice in order to avoid the hotspots. Survey of 50 people says that 90% find it user friendly and takes less than a minute for successful registration. Time for password creation for OTD-PCCP is same in the case of PCCP and CCP. Compared to other authentication mechanisms like PCCP and CCP, indexing is the only extra field present in the registration process. But survey says that it takes no extra time during password creation.

B. Time for Login

Time taken for login in OTD-PCCP is compared with other authentication mechanisms. OTD-PCCP verifies two parameters during login

1. Username verification
2. Click-point verification

It provides a two factor authentication. As soon as the username is verified, user gets a one-time password to their registered mobile number and email. Successful or unsuccessful login is based on this received OTP and correct sequence of 5 click points. User has nothing to memorize like long meaningless alphanumeric strings as password. During registration, when image is uploaded it is split into nine grid and it is indexed in random order. When user comes for login they have to keep in mind this indexed order for clicking on the correct region as in the OTP. Considering this difficulty of memorizing the indexed order, this order is been send to user's mail for reference. Only the registered user with proper mobile number and mail-id will be authentic. This increases the security of this authentication mechanism. Issues like hotspots, shoulder surfing, guessing attacks are impossible in this authentication method. It takes less than one minute to get authenticated if the information provided is valid.

C. Time Taken for Recalling Password

User has to keep in mind the indexed order for clicking on the correct region as in the OTP, during the time of login. Considering this difficulty of memorizing the indexed order, this order is sent to user's mail. So user has nothing to memorize or keep in mind. They can refer the mail for the order in which they have indexed, during registration. This makes the recalling of password less difficult and this gives the solution for often forgot passwords.

D. Login and Recall Success Rates

Success rates are reported on the first attempt and within three attempts. Success on the first attempt occurs when the password is entered correctly on the first try, with no mistakes or restarts. Restarts are analogous to pressing delete while

entering text passwords. Inspection of the text passwords revealed that most participants re-used passwords across accounts, whereas OTD-PCCP passwords were different by design. This suggests that OTD-PCCP passwords offer additional security since reuse across systems is not possible, yet this did not affect success rates.

TABLE I. **INPUT PARAMETERS FOR CALCULATING COVERAGE RATIOS**

Images	Height	Width	Click Area	View Port Height	View Port Width	OTD-PCCP Coverage Ratio	PCCP Coverage Ratio
Image 1	179. 0	283 .0	10* 10	100	100	0.0003 9585	0.0019 8962
Image 2	165. 0	300 .0	10* 10	100	100	0.0003 9377	0.0019 8411
Image 3	213. 0	275 .0	10* 10	100	100	0.0002 8331	0.0017 1231
Image 4	165. 0	300 .0	10* 10	100	100	0.0003 9353	0.0019 8421
Image 5	383. 0	625 .0	10* 10	100	100	0.0000 1742	0.0004 1621

Table 1 shows the input parameters for calculating the coverage ratio. The table contains image height and width and image hole click area. The table 1 shows the coverage ratio of One Time Dynamic PCCP (OTD-PCCP) and PCCP, the OTD-PCCP get the promising results to compare with the PCCP. The results are shown in Figure 5.

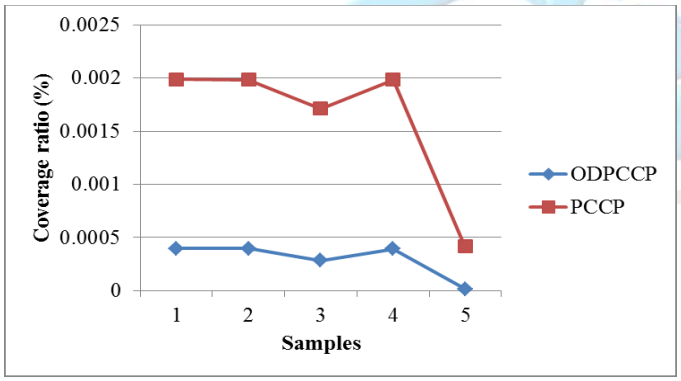

Figure 5: Coverage ratio

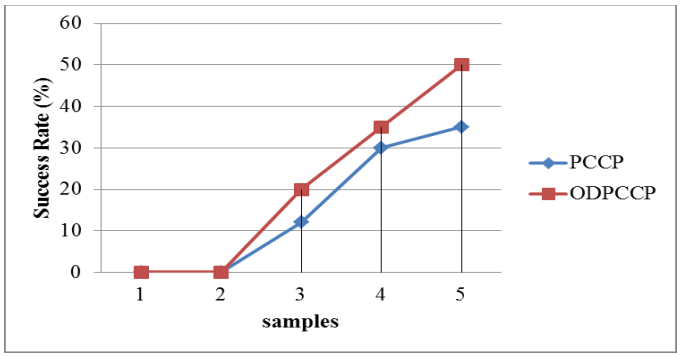

Figure 6: Success Rate

Figure 6 shows the success rate of the OTD-PCCP and PCCP. OTD-PCCP shows the promising results to compare with PCCP. So, the results show that the security level is improved with the reduction in the acceptable value, which avoid user surfing problems.

V.CONCLUSION

The proposed One Time Dynamic Persuasive Cued Click Points scheme shows promise as a usable and memorable authentication mechanism. We believe that OTD-PCCP offers a more secure alternative to PCCP. OTD-PCCP increases the workload for attackers by forcing them to first acquire image sets for each user, and then the mobile number and the mail-id. Furthermore, the system's flexibility to increase the overall number of images in the system allows us to arbitrarily increase this workload. OTD-PCCP is a best alternative to traditional authentication systems. It is resilient to impersonation, resilient to observation, resilient to guessing. This makes the system secure as well as user friendly

VI.REFERENCES

[1] A.Abuthaheer, N.S.JeyaKarthikka, T.M.Thiyagu, "Cued Click Points Graphical Images and Text Password along with Pixel based OTP Authentication", International Journal of Computer Applications, Vol. 87 – No.2, 2014.

[2] M.L.Prasanthi, Devi Srinivas, "Implementation Of Knowledge Based Authentication SystemUsing Persuasive Cued Click Point", International Journal Of Mathematics And Computer Research, Vol.1, issue 1,2013.

[3] B.B.Gite, HariharanSwaminathan, DipaliKalambe, DeeptiPawar, JyotiSarode, "Remote Desktop Access Using Cued Clicked Points and SMS Authentication",International Journal of Advanced Research in Computer and Communication Engineering,Vol. 2, Issue 12, 2013.

[4] RuchiKumari, D.Krishna, V.Sridhar Reddy, "An Image Based Authentication Using Multi-Level Security System", IJESC,2321 -3361, 2013.

[5] Iranna A M,PankajaPatil, "Graphical Password AuthenticationUsing Persuasive Cued Click Point",InternationalJournal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 2, Issue 7, 2013.

[6] Naresh D. Kale, V. A. Chakkarwar, "A Review on Knowledge-Based Authentication MechanismUsing Secure Persuasive Cued Click-Points",International Journal of Emerging Technology and Advanced Engineering, Vol. 4, Issue 12, 2014.

[7] Chiasson,S.,Ottawa, ON, Canada, Stobert, E. , Forget, A. , Biddle, R, "Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism",IEEE Transactions onDependable and Secure Computing, IEEE,1545-5971, 2012.

[8] S. Poornima,G.Babu, "Fast Computation for Digital Image Registration And Performance Evaluation Using Parallel Computation",International Journal of Inventions in Computer Science and Engineering,Vol.2.Issue 2, 2015.

[9] RupaliK.Gurav, K. V. Murali Mohan, Y. David Solomon Raju, "Advanced Wireless Robot Communication using ZigbeeProtocol"International Journal of Inventions in Computer Science and Engineering,Vol. 1, Issue 9, 2014.