IJCSN International Journal of Computer Science and Network, Volume 3, Issue 6, December 2014
ISSN (Online) : 2277-5420 **www.IJCSN.org**
Impact Factor: 0.274



# A Review on Shoulder Surfing Attack in Authentication Technique

**[1] Pranjali Waghmare, [2] Rushi Longadge, [3] Deepak Kapgate**

[1,2,3] Dept of CSE, GHRAET, R.T.M. Nagpur University
Nagpur, Maharashtra, India

**Abstract -** Security is a important factor in computer system now a days. Users of computer system give a primary preference to security. Authentication is a process used to provide security to the user. Authentication is a process of identifying the person's identity or conforming the identity of a particular person. There are various authentication method, but most commonly used method is textual password. Combination of alphabet and number create a secure password. But it has some drawbacks i.e. it can be easily guess by third person also called attacker. If it make complex then it could be hard to memorize. Also it is susceptible to various attacks such as brute force attack, dictionary attack, social engineering attack, eves dropping, etc. to overcome the drawback of textual password graphical password system introduced. Graphical system is easy to memorize but it undergo shoulder surfing attack which is quite big problem. in which any entity or person can observe users password directly or by using any device. This paper survey the various shoulder surfing attacks in graphical password approach.

***Keywords -*** *Authentication, Graphical Password, Shoulder surfing attack.*

## 1. Introduction

Authentication is topic of the information security which deals with the protection of the user's privacy. Authentication is a process which gives permission to allowed the user in particular system. Authentication techniques are categorized as Token based authentication, Biometric based authentication, knowledge based authentication. In Token based authentication tokens are use as password. This includes Smart card, credit cards. Some Token based techniques also combined with the Knowledge based authentication to enhance the security such as, while using the ATM we need card as well as PIN No. for authentication. Tokens are simple and cheap and can be easily reproduced. But tokens has their own drawbacks that, it is a physical object which is all time not convenient to the user to carry everywhere, also it need a hardware for authentication. It can be easily stolen so the tokens are use with the Pin numbers [1]. Biometric system refers to the human characteristics and traits. Biometric system includes physiological and behavioral characteristics of human beings. Biometric techniques are classified as Contact Biometric technologies and Contactless Biometric technologies. Iris scan, fingerprint scan, facial recognition are some examples of Biometric authentication. This technique will provide highest security but, it is not yet adopted. This system is very much expensive, and requires special hardware is the major drawback of this system [2].

Knowledge base technique involves alphanumeric password and Graphical password. Alphanumeric passwords are introduced in the 1960s. it is very simple and easy way of authentication. But it is susceptible to various attacks such as bruit force attack, dictionary attack, etc. to overcome this problem, later graphical password authentication were introduced. Graphical password uses image as a password, which is easy to remember by the user. But it is susceptible to shoulder surfing attack. Now by considering those problems of previous system, to overcome the drawback. Authentications is used as wide application in many areas like military application, industrial purpose, government offices, etc.

In this paper, section 2 includes Related Work , in section 3 it includes security aspect In the authentication , section 4 includes drawbacks, section 5 includes Discussion regarding all techniques and section 6 includes Conclusion.

## 2. Related Work

User authentication is most fundamental component in computer security context. There are various techniques use for authenticating the user. Such as recognition based

authentication, recall based authentication, pure recall based authentication. Most common method for authentication is alphanumeric password authentication. In which combination of alphabet and numbers used as password. It is simple and easy to use but susceptible to various attacks such as dictionary attack, bruit force attack, etc. to overcome these drawback Graphical password were introduced. Graphical passwords are is easy to remember by user and also resistant to dictionary attack, bruit force attack, etc. some authentication technique are discuss below.

Draw a secret [3] is a method of authentication in which the password is enter using mouse. This technique uses 2D grid platform. In which user have to draw the character or object in particular sequence at the time of registration. During the login time user has to redraw the same character or object on the 2D grid at the same order. In Draw a Secret technique it is not important to draw a perfect shape or should be start from particular place, but the order of redrawing the character or object is important for successful login. This technique has a drawback that it undergo shoulder surfing attack.

Rachna Dhamija and Adrian perrige [4] proposed Déjà vu authentication technique, in this system user creates a portfolio of certain number of images during the registration phase. From which user has to select some images as their password. During the login phase the images are appear on the screen from which user has to identify those selected images from the portfolio of images and select it as password. But this system is susceptible to shoulder surfing attack.

Passfaces [6],[13] is a technique where system shows nine human faces in the form of grid and user has to select the appropriate image which has been selected previously during the registration phase. User has to select only one face from eight decoy images and this procedure is repeated for four times during the login phase. So user has to select four images from the four different nine grid of images.

Passpoint [7] is a technique in which only one image is selected during the registration. From that image, particular part of image or cued of image are selected as the password. User can select multiple cued randomly from the image but user should memorize the sequence of cued entered at the time of registration. During the login time preselected image will appear on the screen. User has to enter the preselected cued of images in the same order as they selected during registration. As human mind can memorize images better than text so this method is easy to remember. But this method suffers shoulder surfing attack.

CCP [8] refers to Cued Click Point is authentication technique coming from passpoint. In which during the registration certain number of images are selected in the particular order. From each image only one cued click point will be selected. During the login time first image will appear on the screen, user has to identify the correct cued and should select as password. If the selected cued is correct then it will open the next image. Same procedure is applied for all the images. But if any one image cued is wrong then it will not display the next image. This method is easy to remember by the user and unbreakable. But this method undergoes shoulder surfing attack.

Convex hull [9] is a technique in which some pass objects are selected as the password at the time of registration. User should memorize that pass object as their password. At the time of login some decoy image objects as well as the pass objects are appear on the screen. From which users have to identify the pass objects which itself forms a invisible convex hull. User has to click inside the convex hull for successful login. but drawback of this method is, it is hard to identify the pass objects from all the image objects appear on the screen. This technique uses many decoy objects for creating more confusion to attacker. But it will make display more crowded. if objects will be reduces then possibility of guessing the password will be increases.

Two level graphical authentication [10] is a technique where two different methods are combines each other forms one authentication scheme. In first level authentication user has to enter textual password. And after successful authentication of first level, second level authentication window appears. In second level authentication Graphical passwords are use. two level authentication provide better security but This technique is time consuming.

Sonia chiasson et. al.[11], [14] at the time of registration user has to select an image and place a viewport on the particular part of image. For getting the next grid of images user has to shuffle the viewport from one place to another in an image. The same process is applied till user gets certain grid of images as their password. During the login phase the same image will be appear and user has to select the previously selected viewport as password for authentication. D. Surya devi et. al.[12],[15] propose session authentication technique for secure authentication. In that they uses two different techniques such that for text password they uses pair based authentication in

which, one string is taken as permanent password. The pair of two consecutive strings form horizontal and vertical intersection which is the first letter of new password. In this way we get new password during each session. Second technique is based on pair of color codes used as password called as hybrid textual authentication. In which some colors are taken in series of order and we have to assign a code to each color. Those codes should be memorize by the user. In both the method password will be changes in each different session. That means each time different password will be created. So that we can consider this approach will use to resist the shoulder surfing attack.

## 3. Security Aspect in Authentication Technique

### 3.1 Social Engineering

It refers to the psychological manipulation of people into performing actions or divulging confidential information.

### 3.2 Dictionary Attack

This attack is a guessing type of attack. in which attacker has a list of string which cantain likely words or letter combinations. By using this combinations attacker try to guess the password.

### 3.3 Brute Force Attack

It consists of systematically checking all possible keys or passwords until the correct one is found. In the worst case, this would involve traversing the entire search space.

### 3.4 Guessing

Attacker can guess the password by trying the personal information of the user.

### 3.5 Shoulder Surfing Attack

In Shoulder surfing attack, attacker can observe password directly or trap password using any device. It is most commonly occurring attack.

## 4. Comparative Work with Drawbacks

Table 1: Comparative work with drawbacks

| Technique | Login Phase | Drawback |
|---|---|---|
| Textual password | Enter character using keyboard | Undergo brute force, dictionary, shoulder surfing attack |
| Draw a Secret | Redraw the sequence same as drawn at registration time | Difficult to redraw the same sequence |
| Déjà vu | Identify the correct images | Time consuming process |
| Passfaces | Identify the four faces in four steps | Time consuming process |
| Passpoint | Select passgrid from given image | Difficult to learn passpoints |
| Ccp | Single click on certain image | Difficulty in identifying clicks |
| Pccp | Select multiple grids from one image | Difficult to learn click points |

## 5. Discussion

We accomplish study of some papers of authentication in this paper. From that we try to understand the difficulties regarding different authentication techniques. Text password authentication is very well known technique but it undergoes various attacks. That why to raise above these attack graphical password authentication techniques are invented. In that many techniques are invented, but these are also undergo some problems such as Some techniques are time consuming, Some techniques are vulnerable to various attacks such as dictionary attack, social engineering, brute force attack, Shoulder surfing attack etc. some techniques required maximum storage space, some are complex technique.

There are various problems in authentication technique in that shoulder surfing attack is severe attack found. Various authentication techniques are invented to overcome the shoulder surfing attack. In that session authentication is a technique which can help to resist the shoulder surfing problem.

## 6. Conclusions

Authentication is a basic component in the aspect of security. Authentication is required to provide the better security to the user. Various survey papers study in above section regarding the various attacks found during the authentication. Textual password authentication is well known authentication technique. it is simple and easy but vulnerable to various attacks. Later graphical password is invented. This is simple and easy to memorize to the user. But undergo various problem such as, it require greater storage space, some are complex and time consuming. A session authentication technique which may help to reduce the shoulder surfing attack.

## References

[1] Ian Jermyn, Alain Mayer, Fabia manrose, Micheal K. Reiter, Aveil D. Rubin, "The Design and analysis of graphical password" Proceedig of the 8th USENIX security symposium Washington, D.C. USA, August 1999.

[2] Narman poh, samy bengio," how do correlation and variance of base experts affect fusion in biometric authentication tasks?", IEEE transaction on signal processing, volume 53, No 11, Nov 2005

[3] Arash Habibi lashkari, Samaneh Farmand, Dr. Rosli Saleh, Dr. Omar Bin Zakaria," A wide range Survey on Recall Based Graphical user authentication algorithm based on ISO and attack patterns",international journals of computer science and information security, vol. 6, no. 3, 2009.

[4] Rachna Dhamija, Adrian Perrig, ," Déjà vu: a user study using images for authentication ", in 9th USENIX security symposium,2000.

[5] Stamati Gkarafli, Anastasios A. Economides, "comparing the proof by knowledge authentication techniques", international journals of computer science and security vol.4, issue 2.

[6] Passfaces Corporation, "The science behind Passfaces", White paper, Available at http://www.passfaces.com/enterprise/resources/whitepapers.htm, July 2009.

[7] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Broadskiy, Nasir Memon, " Passpoints: Design and longitudinal evaluation of a graphical password system", international journal of Human Computer studies 63, 2005.

[8] Sonia chiasson, Alain Forget, Elizabeth Stobert, P. C. Van Oorschot, Robert Biddle, " Multiple password interference in text passwords and click based graphical passwords", ACM CCS 09, Nov 2009.

[9] Leonardo sobrado, Jean Camille birget, Susan Wiedenbeck, Jim Waters," Design and evaluation of a shoulder-surfing resistance graphical password scheme", ACM, may 2006

[10] Kanchan V. Warkar, Nitin J.Janwe," A review on two level Graphical authentication against Key-Logger spyware", national conference on Emerging trends in computer science and information technology 2011.

[11] 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 of Dependable and secure computing, vol. 9,no.2, mar/April 2012.

[12] D. Surya Devi, M. Tamil Selvi, T. Sowmiya, M.J. Pavitra, J. Jeba Emilyn, " Generating session password using text and color to prevent shoulder surfing", international conference on modeling optimization and computing 2012.

[13] H.K. Sarohi, F.U. Khan, "graphical password authentication scheme: current status and key issues", international journal of computer science, volume 10, march 2013.

[14] M. swathi, M.V. Jagannatha Reddy, " Authentication using persuasive cued click points", International journal of engineering research and technology, volume 2 , issue 7, july 2013.

[15] N.S. Joshi," Session passwords using grid and colors for web applications and PDA", IJETAE, volume 3, issue 5, may 2013.