IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Volume 6, PP 58-60

Recognition And Recall Based Graphical Password Authentication

Mr. Santosh M.Dodamani[1], Ms. Aarti B.Valsang[2],
[1](Computer Department, Atharva college of Engineering Mumbai, India)
[2](Computer Department, A.G. Patil Institute of Technology Solapur, India)

Abstract : *Security is that the degree of protection to persons or person against danger, damage, loss, and crime. The need for security often means that standard human-computer-interaction approaches cannot directly apply. Nowadays, as day today activities are more open to the internet, the importance of security for applications is tremendously increased. Using static passwords alone makes it easy for the hackers to hack the users account. An important usability goal for authentication system is to support users in selecting better password. User often creates memorable passwords that are easy for attackers to guess, but strong system assigned passwords are difficult for users to remember. So researchers of modern days have gone for alternative methods. Here a graphical password is discussed.*

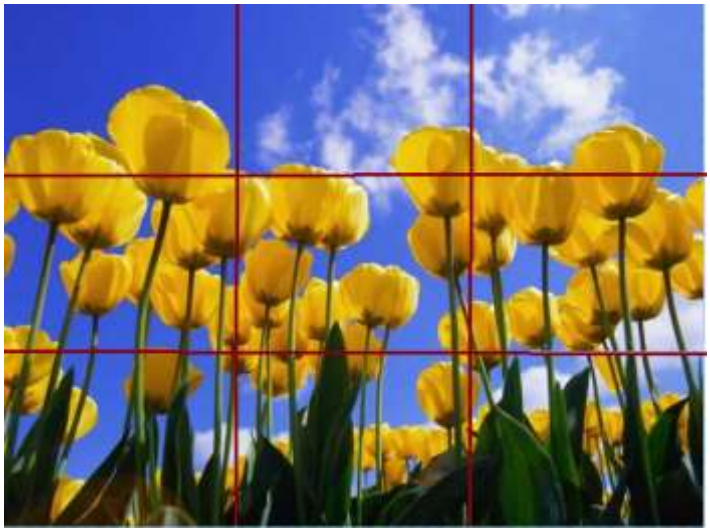
Keywords : *Cybercrime, Graphical, Face Recognition, Biometric.*

I. Introduction

Nowadays people do not go to a bank to make a transaction, do not go to an Electric board to pay bill, and do not go to railway station to make a train reservation and what not. All these times consuming and these tasks are making easy at your foot step because of Internet. For doing all these tasks now days people are using smart phone app and for this everyone hits respective portals/sites. There are many such areas where we need where we need security against Cybercrime such all activity involve human interaction with computers [1]. So the authentication is the most important and fundamental activity in all computer security systems.

Security researchers have made their efforts to protect systems against the different attacks and also individual user digital data. Because of increasing threats and crimes over the internet or networked systems, there is great need for preventions of such activities. We use alphanumerical usernames and passwords for authentication purpose but studies show that user can only remember a limited number of passwords. Generally user will note down password somewhere or will repeatedly use the same passwords for different accounts. Sometimes users will use a password that is simple and easy to remember to avoid the complexity.

Some other techniques like Biometrics Face recognition, Retina scanning are used to increase the security but it requires lot of investments. The alternative techniques to increase security to next level, some authentication methods have developed that use pictures as passwords or a second level of authentication. In this article we will work on another alternative using image as passwords. The below image is used for spam prevention as a second level of authentication.



Users need to remember the password but is difficult to remember complex, random passwords. Human being has long term memory limitation, so user can forget a password that is not used regularly. Having

multiple passwords may leads the user either jumble the elements of the different passwords or confuse the password for which system it corresponds to. Users normally face the password memory problems which decreases the password complexity and number of passwords. This habit reduces password security. Normally secure password should be 8 characters length, random, with upper-case characters, lowercase characters, special characters and digits. Users ignore such password recommendations, and use instead short, simple passwords that are relatively easy to remember and easy to discover using dictionary attacks. It is often observed that users choose short password and it contain only alphabetic consisting of personal names of family or friends, pets, etc. Users generally write down their passwords as note or sometime share the passwords with others, or use the same password for multiple systems.

II. Proposed Methodology

Graphical password is an authentication system which allows the users to select from images, in a specific order, presented in a graphical user interface (GUI). Graphical passwords can be easily remembered, as users remember images better than words. Graphical passwords techniques are categorized into two main techniques: recall-based and recognition-based graphical techniques [2].

2.1. Recognition Based System

In recognition-based techniques, Authentication is done by challenging the user to identify image or images that the user had selected during the registration stage. Another name for recognition-based systems is search metric systems. It is generally require that users memorize a number of images during password creation, and then to log in, must identify their images among them. Humans have unique ability to identify images previously seen, even those which has been viewed very briefly. Recognition based systems have been proposed using usability and security considerations, and offers usability. In some graphical password schemes, Knowledge of some details of the shared secret must be retained by the system, i.e., user specific profile data e.g. in recognition schemes, the system must know which images belong to a user's portfolio in order to display them.

Sobrado and Birget Scheme is recognition based system that displays a number of pass-objects (pre-selected by user) among many other objects, user click inside the convex hull bounded by pass-objects. In Pass face scheme human faces are used as password. And in Dhamija and Perrig Scheme Pick several pictures out of many choices, identify them later in authentication.

2.2. Recall Based System

In recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage. Recall-based graphical password systems are occasionally referred as draw metric systems since a secret drawing is recalled and reproduced by the user. In these systems, users typically draw their password either on a blank canvas or on a grid. You can secure your password using various techniques in graphical authentication.

To authenticate, we use a grid based approach by using image as a reference. Draw-A-Secret (DAS) Scheme User draws a simple picture on a 2D grid. The coordinates of the grids occupied by the picture are stored in the order of drawing. Redrawing has to touch the same grids in the same sequence in authentication. Then certain grids are selected by the user to set his/her password as shown in the figure below a major drawback of graphical password authentication is shoulder surfing.

Another one is Pass Point Scheme which allows users to click on any place on an image to create a password. A tolerance around each chosen pixel is calculated. In order to be authenticated, user must click within the tolerances in the correct sequence. Signature scheme is another graphical user authentication conducted by having the user drawing their signature using a mouse.

III. Implementation

Graphical Password can be implemented in authenticating several systems and websites. The implementation has few focuses:

- Password: Contain image as reference & encryption algorithm.
- Login: Contains username, images, Graphical password and related methods.
- SSR shield: Contains shield for Shoulder surfing.
- Grids: Contains unique grid values and grid clicking related methods.

IV. Conclusion

The system security is very high as it uses graphical three level password authentications. Graphical password schemes provide a way of making more human-friendly passwords. Dictionary attacks and brute force

search are infeasible. Require much more storage space than text based passwords. Password registration and log-in process take too long. Shoulder Surfing: As the name implies, shoulder surfing is watching over people's shoulders as they process information. Because of their graphic nature, nearly all graphical password schemes are quite vulnerable to shoulder surfing.

Acknowledgements

It gives me a great pleasure and satisfaction in presenting the paper on "Recognition and Recall based Graphical password Authentication" Before I get into the depth of the things, I show my sincere gratitude towards respected Prof. Santosh Dodamani who have directly or indirectly helped me in the completion of this paper successfully

References

[1] M.Manjunath, Mr. K. Ishthaq Ahamed and Ms. Suchithra, Security Implementation of 3-Level Security System Using Image Based Authentication, *International Journal of Emerging trends and technology,2(2),*2013,401-404.

[2] Aakansha Gokhale, Vijaya Waghmare,The Recognition and Recall Approach based Graphical Password Technique, *International Journal of Computer Applications,22-27*

[3] Vamsi Krishna Vemuri, S D Vara Prasad, *A Secure Authentication System by Using Three Level security, International Journal of Engineering Science and Computing,*2014,344-348

[4] Swarna Lakshmi M, Roobini S, Shalie Monicka A, Saraswathi V, Ms. N. Radha, *International Journal of Advance Research in Science and Engineering*, 6(3),2017,79-87

[5] Nagesh.D Kamble, J.Dharani, Implementation of Security System Using 3-Level Authentication, *International Journal Of Engineering Development And Research*,2(2),2014,1528-1532

[6] Lalu Varghese, Nadiya Mathew, Sumy Saju, Vishnu K Prasad, Three level Password Authentication System, *International Journal of Recent Development in Engineering and Technology*,2(4),2014,127-131

[7] Mughele Ese Sophia, Three – Level Password Authentication, *European Journal of Computer Science and Information Technology*,3(5),2014,1-7