**Analysis Of Grid Based Password Authentication Techniques**

M. Hemamalini

Assistant Professor, Department of Computer Science, A.V.C. College (Autonomous),

Mannampandal, Mayiladuthurai, [maliniavcce@gmail.com](mailto:maliniavcce@gmail.com)

R. Subathra

R. Subathra, Research scholar, Department of Computer Science, A.V.C. College (Autonomous),

Mannampandal, Mayiladuthurai, [subaramalingam1605@gmail.com](mailto:subaramalingam1605@gmail.com)

**ABSTRACT**— **The textual passwords have been used as an authentication method for a long time. It is well-known that users tend to select passwords that are easy to remember. It is easy for an attacker to obtain the password by probing for candidate passwords. This authentication method is easily cracked using some vulnerable techniques. Graphical password authentication is another method for the textual password-based method. Humans are better at recognizing graphical based information than text based information. The graphical password method is easy to use and securable than existing password techniques. Grid based password are also ones that have caught up with others in popularity. This paper analysis the security of such system.**

Keywords—password protection; graphical password techniques; click point; authentication techniques.

# **Introduction**

Text based password authentication is commonly used for all users. This is more vulnerable method for some password guessing techniques. Like some traditional password attacks are dictionary attack, brute force, eves dropping and shoulder surfing problem. User can choose random alphanumeric and lengthy password character for data protection. The major issue is hard to remember the lengthy password. The user picks short length password and easy to memorable [1]. Unfortunately, nowadays human-computer interaction is compulsory fated for all developing field. Focusing three main important securities is authentication, developing secure systems and security operations [2].

# **literature survey**

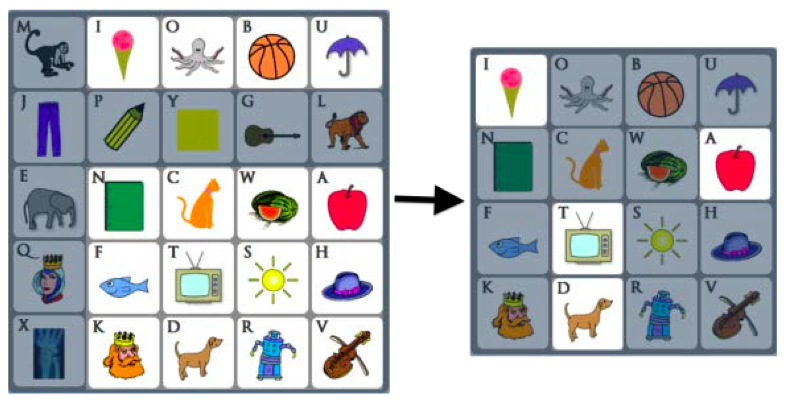
Mainly graphical authentication using pictorial based password. It is easy to remember and provide minimum password guessing attacks. Majorly graphical password is categorized two types namely Recognition based Recall based techniques. In recognition based techniques shows set of images, user can have must to choose the picture based password in registration stage. When users enter the login process, exactly choose the same set of image password. Recognition based techniques using images are facial pictures, random art images, objects and icons etc. [2]. In recall based techniques, using pictorial password and reproduce some of them to creating registration phase. User need to set as password for secret drawing. User easily pick the password, in each of time hard to remember the exact password and against to password guessing attacks.

1. RECOGNITION BASED TECHNIQUES

In recognition based techniques user can set password in the grid based image.

1. *IMAGE PASS SCHEME*

Image pass scheme. In this technique show the 5\*5 grid pattern in registration phase. User chooses any picture to set as password. In login time, the image pattern is show as various formats. User picks the registered image and validate to next process [3].

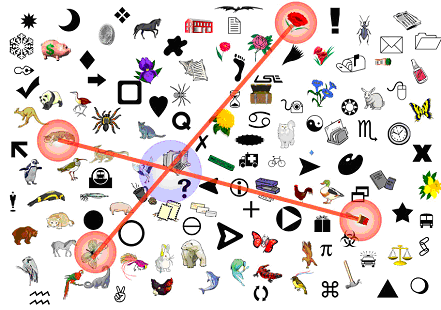


*Fig. 1. Image pass scheme*

#### MOVABLE FRAME SCHEME

This scheme uses three pass-objects within the frame.

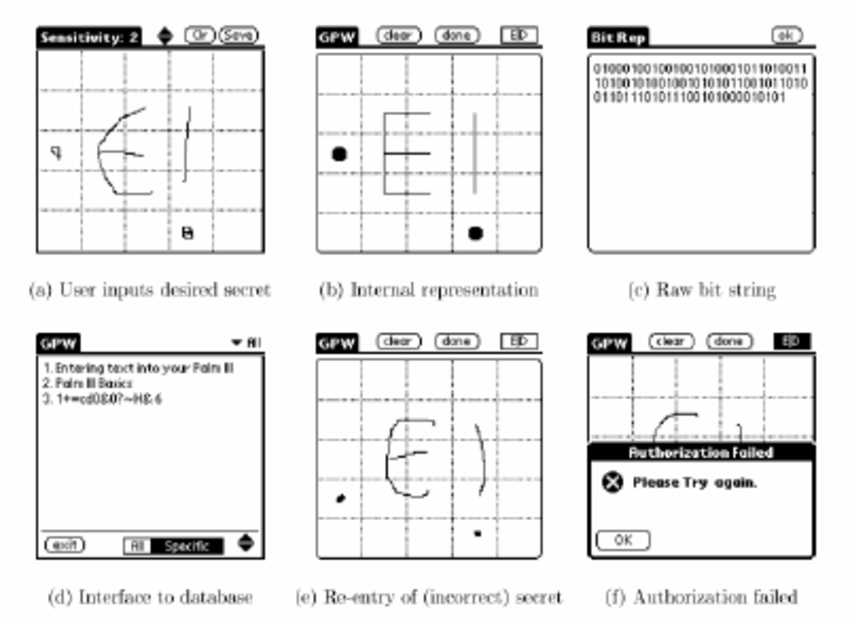
The user can shift the pass-objects by rotating the frame. This process can be continued till the entire pass-objects are placed correctly. This scheme repeats the process few times by randomly rotating or clicking it to reduce the chances of login [4].



*Fig. 2. Movable frame scheme*

1. RECALL BASED TECHNIQUES
2. *Draw A Secret Technique*

Traditional textual password method is a recall based techniques. It’s recreate the stored secret drawing or signature. Draw a Secret (DAS) technique is followed by recall based password authentication techniques in graphical password. In registration phase user draw the secret password, it’s stored the database. When user enters the login phase, the user draws the same location in grid panel. It’s difficult to memorized and highly expansive for implanted this DAS techniques [5].

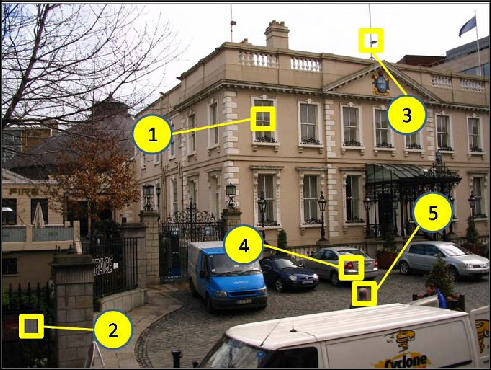


*Fig. 3. Draw a Secret techniques*

# **click based picture password**

Recent days available various graphical based password authentication techniques is used to prevent the sensitive information. In registration stage, user pick to image grid to set the password. Then focusing to find previously selected image location for one or more images in the grid panel [6]. In this techniques image is cue to recall. Example pass point and cued click point.

In pass point techniques, pick the five click points to the specified image and different pixel location for same image for registration stage. When user tries to login, the authorized user picks same order to targeted image and identified the tolerance of image [7].



## Fig. 4. Pass point technique

In cued click points, tend to one click points on five different images. User choose the first image location and displaying next image for depending previously selected image location based [8].

## ccps.png

*Fig. 5. Cued click point technique*

# **GrID BASED AUTHENTICATION SCHEME**

During registration, the grid image will be displayed. The user has to set password as grid location. The registration details are stored in the database by using hashing techniques. During login phase, the user has to set the grid location. If the grid location is correct, then the user can access the system.

Grid based image selection

Registration screen

Display grid image

Set password as grid location

Database

Login screen

Pick grid location

Hashing techniques

Match password

Access website

No

Yes

## 

## **V. COMPARISON BETWEEN CUED CLIK POINT AND PERSUASIVE CUED CLICK POINT**

## Below table represents the success rate and security success rate for Cued Click Point(CCP) and Persuasive Cued Click Point (PCCP). The given dataset analysis persuasive cued click point is provide better performance and efficient success rate then comparing to cued click point techniques.

## TABLE 1. COMPARISION TABLE

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Cued click point (CCP)** | | **Persuasive Cued Click Point (PCCP)** | |
| **Success**  **Rate (%)** | **Security success Rate (%)** | **Success**  **Rate (%)** | **Security success Rate (%)** |
| **User 1** | 4/5(80) | 20 | 3/5(6) | 40 |
| **User 2** | 3/5(60) | 20 | 2/5(40) | 60 |
| **User 3** | 5/5(100) | 0 | 4/5(80) | 20 |

# **VI. GRAPHICAL REPRESENTATION**

## 

**VII. CONCLUSION**

This paper deals with various authentication techniques such as Recognition based techniques and Recall based techniques. Click point based authentication techniques better than the traditional methods. Grid based authentication scheme provides better efficiency against malicious password crackers. It reduces the accessing time and highly secured authentication. Hashing techniques provide additional integrity prevention for stored password.

##### References

Hash Desai, Ninaad Survama, Dipen Desai and Simranjeet Singh Chawla, Sowmyashree, “Grid Based Authentication Password Using Hash Techniques,” International Journal of Engineering Trends & Technology in Computer Science (IJETTCS), volume. 4, issue 5(2), october-2015. Pp.115-118

1. Akshay Karode, Sanket Mistry and Saurbh Chavan, “ Graphical Password Authentication System,” International Journal of Engineering Research & Technology (IJERT), volume. 2, issue 9, september-2013. Pp. 2257-2560
2. N. Aishwaryar, D. Purva Suryavanshi, R. Pratiksha Navarkle, “Survey on Graphical Password Authentication Techniques,” International Research Journal of Engineering and Technology, volume. 5, issue 2, 2018. pp.26-28
3. U.K. Weich, Yu-Chang, Bo-ren Cheng, Chia-Ju Chang.”A Sector-Based Graphical Password Scheme with Resistance to Login-Recording Attacks,” IEICE TRANSACTIONS on Information and Systems, volume. 98, issue 4, 2015. pp.894-901
4. Tsung, Hung Lin, Cheng Chi Lee, Chwei Shyong Tsai and Shin Dong Guo, “A Tabular Steganography Scheme for Graphical Password Authentication,” COMputer Science and Information Systems (ComSIS).volume. 7, issue 4, 2010. Pp.824-841
5. R. Biddle, S. Chiasson and P. Van Oorschot, “Graphical Passwords: Learning from first Twelve Years,” ACM computing surveys, volume. 44, 2012
6. J. Thrope, Van Oorschot, “Human-Seeded Attacks and Exploiting Hot-Spots in Graphical Passwords, ” USENIX Security Symp. 2007
7. S. Chiasson, P. Van Oorschot and R. Biddle, “Graphical Password Authentication Using Cued Click Points, ” Proc. European Symp. Research in Computer Security (ESOICS), sept. 2007. Pp.359-374
8. D. Vijayashri, Imaran R. Shaikh, “Authentication Using Grid-Based Authentication Scheme and Graphical Password, ” International Journal of Science, Engineering and Technology Research (IJSETR), Volume 4, Issue 7, July 2015 2581 ISSN: 2278 – 7798.. Pp.2581-2585.