Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 4, April 2015, pg.324 – 329

RESEARCH ARTICLE

Graphical Password Authentication System

Sayli Chavan[1], Shardul Gaikwad[2], Prathama Parab[3], Govind Wakure[4]
Department of Information Technology, MCT's Rajiv Gandhi Institute of Technology, University of Mumbai, Mumbai, Maharashtra, India
[1] chavansayli93@gmail.com; [2] gaikwad.shardul76@gmail.com;
[3] prathamaparab14@gmail.com; [4] govind.wakure@gmail.com

Abstract— Computer security depends largely on passwords to authenticate the human users from attackers. The most common computer authentication method is to use alphanumerical usernames and passwords. However, there are significant drawbacks in this method. For example, Passwords selected by users are easily guessed by the attacker. On the other hand, passwords which are difficult to guess are difficult to remember. To overcome this problem of low security, Authentication methods are developed by researchers that use images as password. In this research paper, we conduct a comprehensive survey of the existing graphical password techniques and provide a possible theory of our own.

Keywords— Graphical Password, Authentication, cued, recall based, click points

I. INTRODUCTION

Human factors are often considered the weakest link in a computer security system. If we point out that there are three major areas where human-computer interaction is important: security operations, developing secure systems, authentication. We focus on the authentication problem here. User authentication is a fundamental component in most computer security contexts. Studies about passwords shows that user can only remember a limited number of passwords, they tend to note them down somewhere or will use the same/similar passwords for different accounts. Biometrics is one of the various authentication methods used to tackle the problems associated with traditional username-passwords. In this paper, however, we will deal with another alternative: using image as passwords.

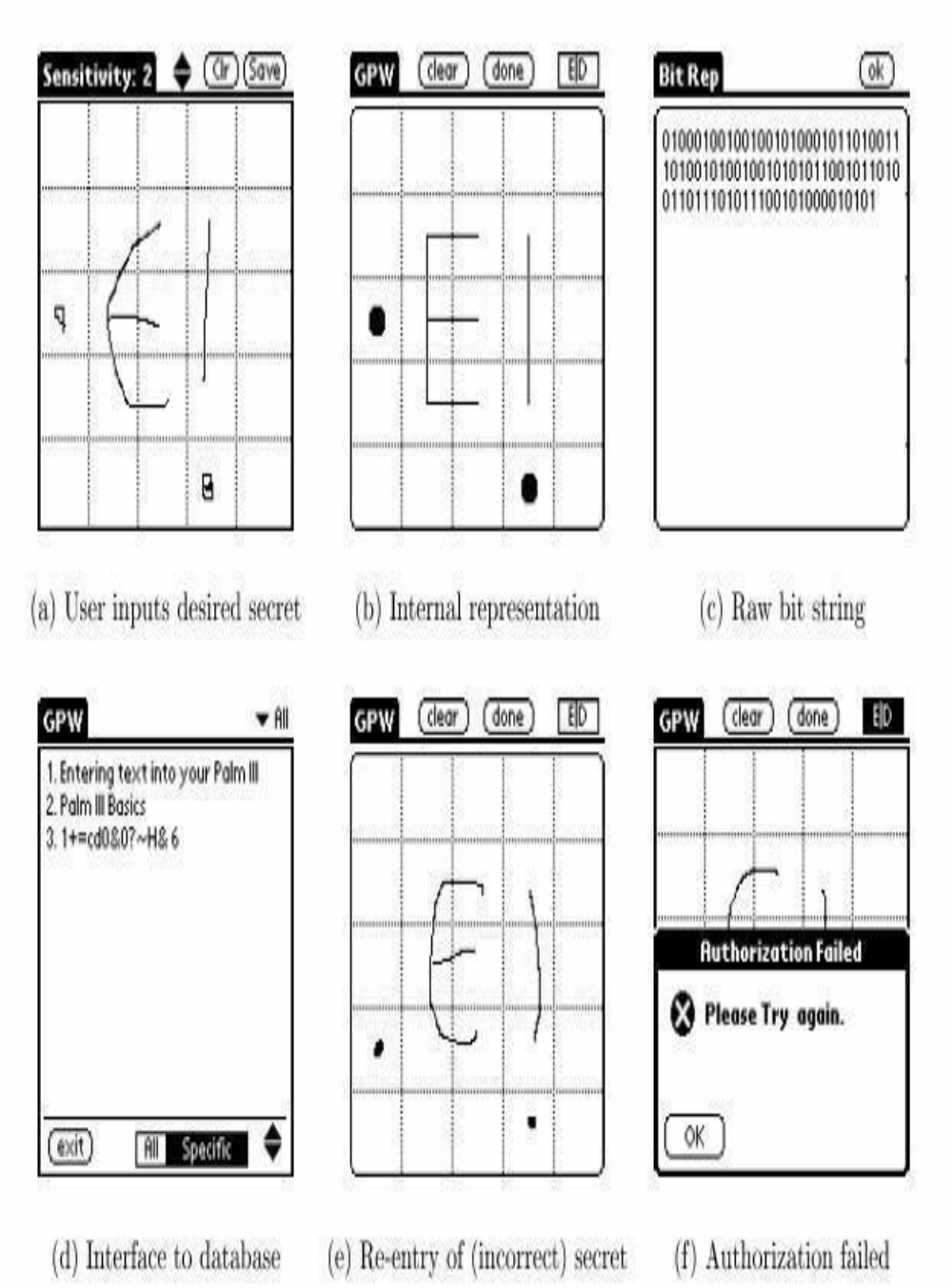

Fig.1 : Recall Based

II. LITERATURE SURVEY

In the literature, several techniques have been proposed to reduce the limitations of the traditional alphanumerical password. One of the proposed solution is to use an easy to remember long phrases (passphrase) rather than a single word [6]. Another proposed solution is to use graphical passwords, in which graphics (images) are used instead of alphanumerical passwords. This can be achieved by asking the user to select regions from an image rather than typing characters as in alphanumeric password approaches.

III. PROPOSED SYSTEM

Graphical passwords refer to using images (also drawings) as passwords. In theory, graphical passwords can be easily remembered, as users remember images better than words [2]. Also, they should be more resistant to brute-force attacks, because there is practically an infinite search space. Graphical passwords techniques are categorized into two main techniques: recall-based and recognition-based graphical techniques [1].

A. 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 cognometric systems [3] or searchmetric systems [4], generally require that users memorize a number of images during password creation, and then to log in, must identify their images from among decoys. Humans have unique ability to identify images previously seen, even those viewed very briefly [7] [9]. From a security point of view, these systems are not acceptable replacements for text password schemes, as they have password spaces which are compared in cardinality to only 4 or 5 digit PINs (considering a set of images whose cardinality remains reasonable, with respect to usability and security). Recognition based systems have been proposed using usability and security considerations, and offers usability. Renaud [4] discusses specific design guidelines which focuses on recognition-based systems.

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. This information must be stored such that its original form is available to the system (possibly under reversible encryption), and thus may be available to anyone gaining access to the stored information.
E.g. Phishing attack and shoulder surfing attack.

B. 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 to as drawmetric systems [3] 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 (which may arguably act as a mild memory cue). Recall is a difficult memory task [6] because retrieval is done without memory prompts or cues. Users sometimes devise ways from which the interface could be used as a cue even though it is not intended as such, the task is transformed into one of cued recall, although one where the same cue is available to all users and to attackers. Text passwords can also be categorized as using recall memory. With text passwords, there is evidence that users often include the name of the system as part of their passwords [5], [8]. Although there is currently no evidence of this happening with graphical passwords, it remains a seemingly valid coping strategy if users can devise a way of relating a recall based graphical password to a corresponding account name.

To a great extent these systems are generally susceptible to shoulder surfing attack, the entire drawing is visible on the screen as it is being entered, and thus an attacker need accurately observe or record only one login for the entire password to be revealed.
You can secure your password using various techniques in graphical authentication. Here we are proposing a new algorithm of authentication using images. To authenticate, we use a grid based approach by using image as a reference. User will upload the image/set of images along with all his/her details during the time of the registration. Then the image selected by the user will appear on the page with transparent grid layer on it. Then certain grids are selected by the user to set his/her password as shown in the figure below.

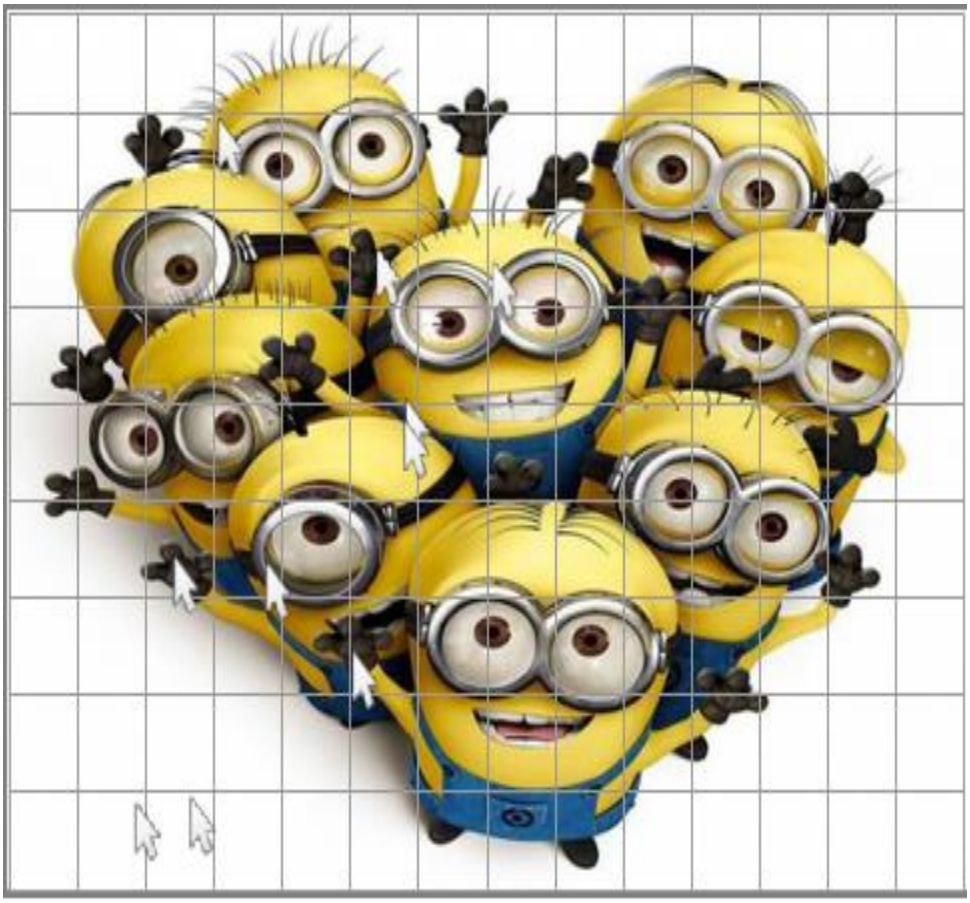

Fig.2: Grid Approach

A major drawback of graphical password authentication is shoulder surfing. A Shoulder Surfing Resistant shield (SSR) is developed to overcome attacks like shoulder surfing. Multiple Fake Mouse pointers are programmed in the SSR shield such that it moves randomly in an image area and the original pointer will look same as the fake mouse pointer. The SSR shield will provide a top layer for grid clicking as well as confusing the attacker.

C. Implementation and Discussion

The proposed system was implemented using PHP, CSS, JavaScript and Macromedia flash 2008(Action Script 2). This Graphical Password can be implemented in authenticating several systems and websites. The implementation has few focuses:

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

As shown in the figure below researchers are trying to stabilize the goal in text based system. However, the text based approach is not able to achieve the goal because as the password strength increases usability decreases. Our main aim is to achieve this goal. In which the usability as well as the security of the system is maintained in such a way that we don't need to compromise on either of these constraints.

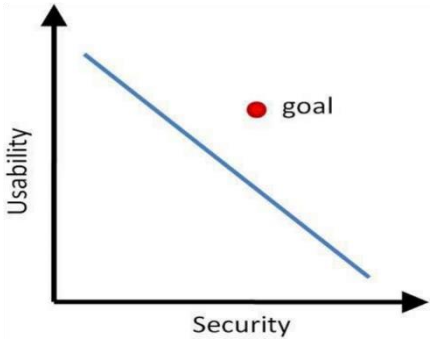

Fig.3: Usability VS Security

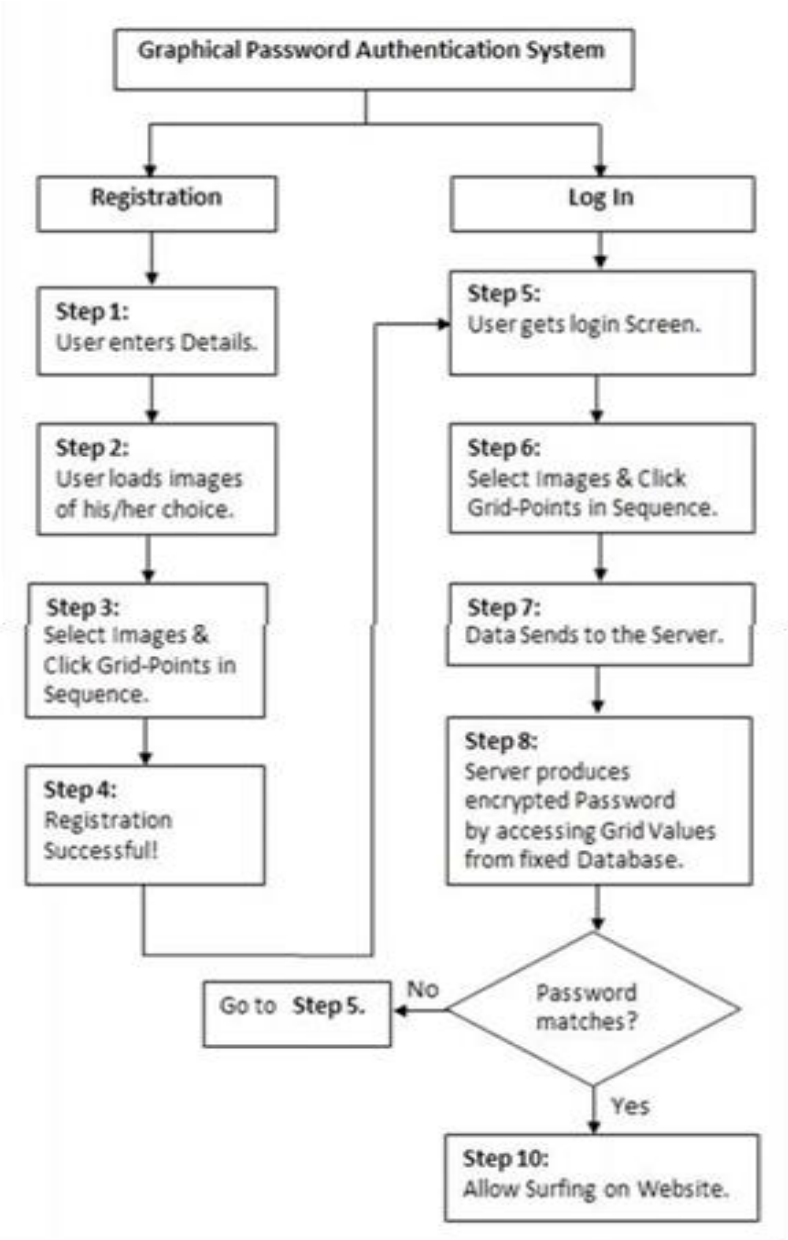

Fig.4: Flow graph.

IV. CONCLUSION

In this abstract we are trying to make our authentication system more user friendly and also we have tried to implement mature & fast Shoulder Surfing Resistant Mechanism. We have considered both methods: text based and graphical based systems and tried to reduce the efforts required by end-user to remember passwords. A look at the advancement in technology over the past few years tells us that the next era will have system security at its core. Thus Graphical Password may be accepted in future as a major authentication system.

ACKNOWLEDGEMENT

It gives the authors great pleasure in expressing our gratitude to all those people who have supported us and had their contributions in making this dissertation possible. First and foremost, we express our profound sense of reverence to our guide **Prof. Govind Wakure**, for his constant guidance, support, motivation and untiring help. We are also thankful to Head of the Information Technology Department and Principal of MCT's Rajiv Gandhi Institute of Technology for their support and valuable suggestions. We are also thankful to all staff members of Information Technology Department, without whom the completion of this report would have been impossible.

REFERENCES

[1] XiaoyuanSuo, Ying Zhu, and G. Scott Owen. Graphical passwords: A survey. In Proceedings of Annual Computer Security Applications Conference, pages 463– 472, 2005.

[2] Antonella De Angeli, Lynne Coventry, Graham John- son, and Karen Renaud. Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems. International Journal of Human-Computer Studies, 63:128–152, July 2005.

[3] A.DeAngeli, L. Coventry, G. Johnson, and K. Renaud, "Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems," International Journal of Human-Computer Studies, vol. 63, no. 1-2, pp. 128–152, 2005.

[4] K. Renaud, "Guidelines for designing graphical authentication mechanism interfaces," International Journal of Information and Computer Security, vol. 3, no. 1, pp. 60– 85, June 2009.

[5] K.-P. L. Vu, R. Proctor, A. Bhargav-Spantzel, B.-L. Tai, J.Cook, and E. Schultz, "Improving password security and memorability to protect personal and organizational information," International Journal of Human-Computer Studies, vol. 65, pp. 744–757, 2007.

[6] F. Craik and J. McDowd, "Age differences in recall and recognition," Journal of Experimental Psychology: Learning, Memory, and Cognition,vol. 13, no. 3, pp. 474– 479, July 1987.

[7] L. Standing, J. Conezio, and R. Haber, "Perception and memory for pictures: Single-trial learning of 2500 visual stimuli," Psychonomic Science, vol. 19, no. 2, p. 7374, 1970.

[8] S. Chiasson, A. Forget, E. Stobert, P. C. van Oorschot, and R. Biddle, "Multiple password interference in text and click-based graphical passwords. " In ACM Computer and Communications Security (CCS), November 2009.

[9] D. Nelson, V. Reed, and J. Walling, "Pictorial Superiority Effect," Journal of Experimental Psychology: Human Learning and Memory, vol. 2, no. 5, pp. 523–528, 1976.

