Graphical Password Authentication System

Akshay Karode, Sanket Mistry and Saurabh Chavan
Computer Department, Mumbai University, Mumbai

Computer Department, Mumbai University, Mumbai

Computer Department, Mumbai University, Mumbai

Abstract

Computer security depends largely on passwords to authenticate human users from attackers. The most common computer authentication method is to use alphanumerical usernames and passwords. However, this method has been shown to have significant drawbacks. For example, users tend to pick passwords that can be easily guessed. On the other hand, if a password is hard to guess, then it is often hard to remember. To address this problem, some researchers have developed authentication methods that use pictures as passwords. In this paper, we conduct a comprehensive survey of the existing graphical password techniques and provide a possible theory of our own.

IJERT

1. 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: authentication, security operations, and developing secure systems.

Here we focus on the authentication problem. User authentication is a fundamental component in most computer security contexts. Studies showed that since user can only remember a limited number of passwords, they tend to write them down or will use the same passwords for different accounts. To address the problems with traditional username-password authentication, alternative authentication methods, such as biometrics, have been used. In this paper, however, we will focus on another alternative: using image as passwords.

2. Graphical Password

Graphical passwords refer to using pictures (also drawings) as passwords. In theory, graphical passwords are easier to remember, since humans remember pictures better than words [1]. Also, they should be more resistant to brute- force attacks, since the search space is practically infinite.

In general, graphical passwords techniques are classified into two main categories: recognition-based and recall-based graphical techniques [2].

2.1 Recognition Based System

In recognition-based techniques, a user is authenticated by challenging him/her to identify one or more images he or she chooses during the registration stage. Recognition-based systems, also known as cognometric systems [4] or searchmetric systems [3], generally require that users memorize a portfolio of images during password creation, and then to log in, must recognize their images from among decoys. Humans have exceptional ability to recognize images previously seen, even those viewed very briefly [8], [9]. From a security perspective, such systems are not suitable replacements for text password schemes, as they have password spaces comparable in cardinality to only 4 or 5 digit PINs (assuming a set of images whose cardinality remains reasonable, with respect to usability). Recognition based systems have been proposed using various types of images, most notably: faces, random art, everyday objects, and icons. Renaud [3] discusses specific security and usability considerations, and offers usability design guidelines focusing on recognition-based systems.

In some graphical password schemes, the system must retain knowledge of some details of the shared secret, 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.

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 to as drawmetric systems [4] because users recall and reproduce a secret drawing. 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 [5] because retrieval is done without memory prompts or cues. Users sometimes devise ways of using the interface as a cue even though it is not intended as such, transforming the task 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 [6], [7]. Although there is currently no evidence of this happening with graphical passwords, it remains a plausible coping strategy if users can devise a way of relating a recall based graphical password to a corresponding account name.

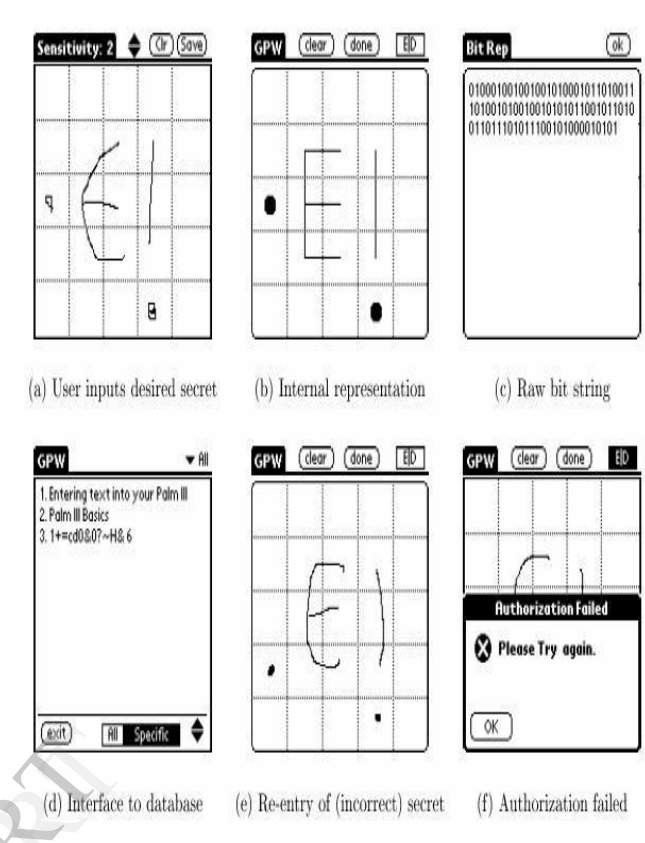

Fig. 1 Recall based system.

These systems are generally susceptible to shoulder surfing to the extent that in many cases, 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.

3. Proposed System

In graphical authentication there are various techniques to secure your password. Here we are proposing a new algorithm of authentication using images. We used a grid based approach to authenticate by using image as a reference.
At the time of registration, user will upload his/her image or set of images along with all details; then user selected image will appear on the page with transparent grid layer on it. So user will select certain grids to set his/her password as shown in the figure below.

IJERT

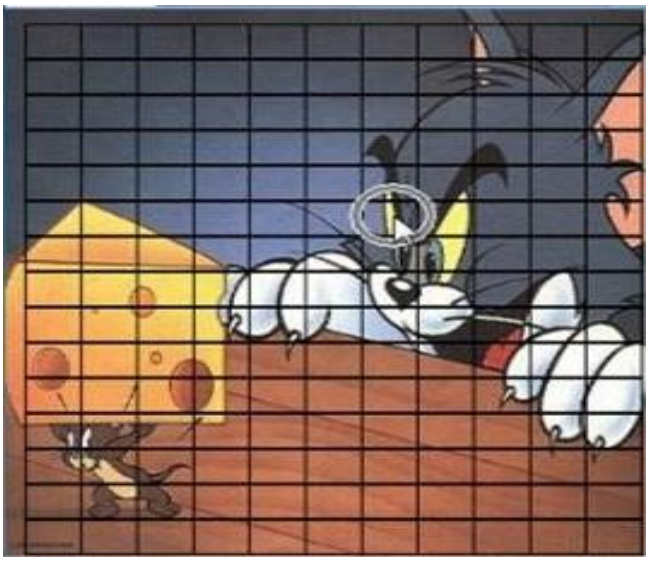

Fig. 2 Grid approach.

Shoulder surfing is a major drawback of graphical password authentication. To overcome this we have developed SSR (Shoulder Surfing Resistant) shield. The shield containing multiple fake mouse pointers are programed in such a way that it moves randomly in an image area and the original pointer will look exactly as fake mouse pointers. This shield provides a top layer for grid clicking as well as confusing other person.

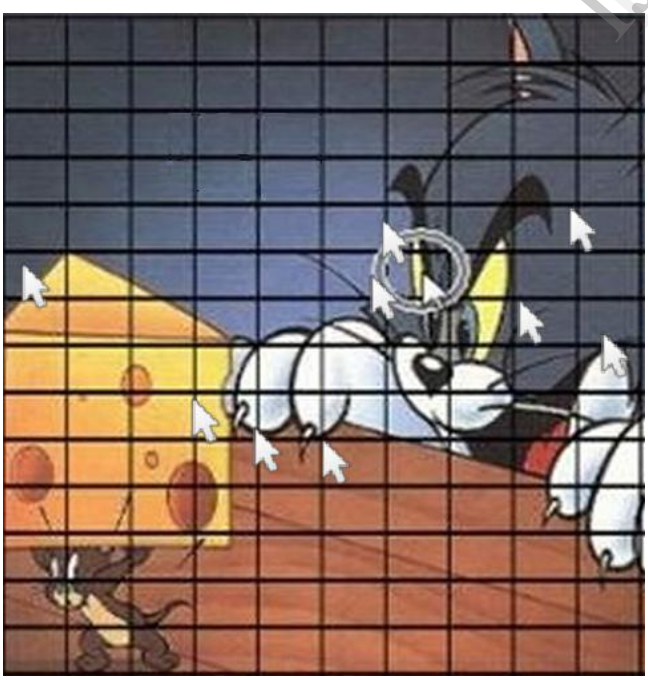

Fig. 3 Shoulder surfing resistant shield.

4. 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:

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

IJERT

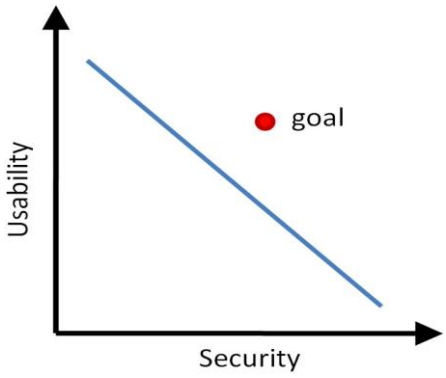

Fig. 4 Usability vs Security.

The working of our system is shown with the help of a flow graph in figure 5.

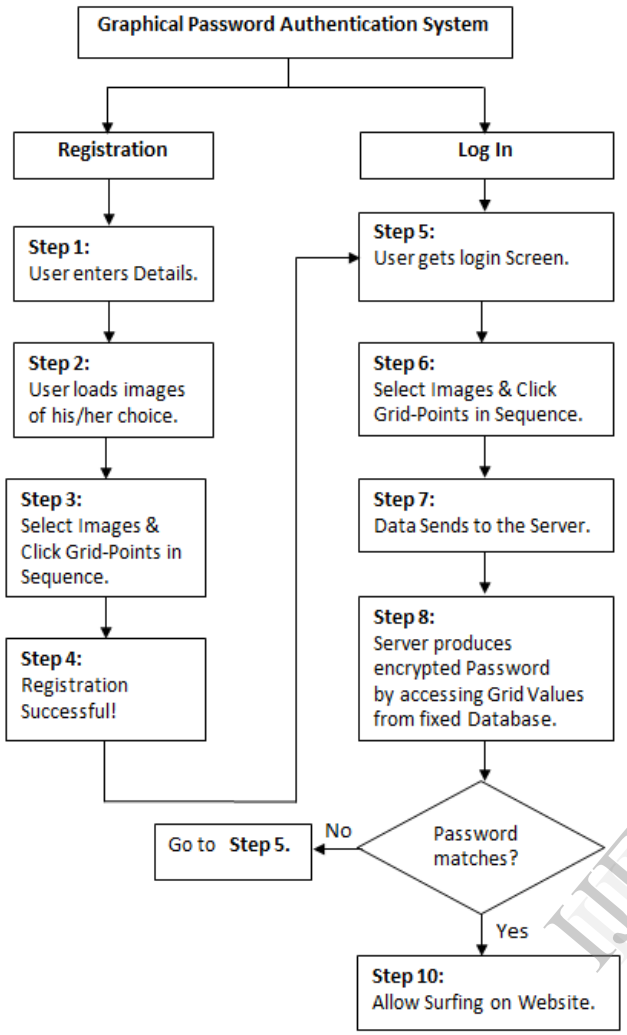

Fig. 5 Flow graph.

5. Conclusions

In this extended 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 adapted in future as a major authentication system.

6. References

[1] 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.

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

[3] 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.

[4] A.De Angeli, 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[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.

IJERT