ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

Hybrid Authentication Technique

Yash Khandelwal[1], Jay Shah[2], Shaunak Shah[3,], Neha Katre[4]

Student, Information Technology, DJSCOE, Mumbai, India [1,2,3]

Assistant Professor, Information Technology, DJSCOE, Mumbai, India [4]

Abstract: The most common type of computer authentication is using alphanumeric characters. This method has significant drawbacks as users tend to pick passwords that are easy to guess. To overcome this problem, some researchers have developed authentication methods that use images as passwords which is known as graphical password. Using graphical password, users click on images rather than entering keywords or alphanumeric characters which proves to be more beneficial in order to overcome the shoulder surfing attack. The authentication done using graphical password is called as graphical password authentication. This authentication strategy has been designed to make the password more memorable and provides a high level of security. In this study, we have proposed a new strategy where the user has to initially choose a certain number of images as his/her password and with each image the user has to enter the corresponding string for that image. During the log-in, the user will be displayed a grid consisting of random images including the first image of the password. The user has to enter the location of the first image along with the string corresponding to that image and continue till the complete password is authenticated.

Keywords: Graphical authentication, textual, password, security.

I. INTRODUCTION

A password authentication protocol (PAP) is a protocol that uses a password [1]. These passwords provide security against unwanted access to the resources. When the user wants to access any network for security purposes the web application authenticates the user [2]. One of the major functions of any security system is that it should not provide the private data to an unauthorized user. Computer systems and the information they store and process are valuable resources which need to be protected. The simplest form of a password is textual password which is nothing but a string of characters. If the authentication is successful it provides access to the resources. It is knowledge based authentication method because it requires knowledge of the password, which was entered during the registration phase. Text based authentication is the most commonly used authentication technique. The biggest advantage of this technique is that the passwords are user friendly [3]. However, there are issues associated with textual password, user usually selects a password which he/she can easily remember, which in turn makes the password weak. Furthermore, textual password is vulnerable to guessing, dictionary attack, shoulder-surfing, brute-force attack, hidden camera and spyware attacks [4]. To overcome these limitations of text-based password, a technique such as graphical password is used. A graphical password authentication is a system that works by having the user select from images, in a specific order presented in a graphical user interface(GUI).It is believed that the visual memory in humans is the best type of memory therefore the graphical password authentication technique is an effective password authentication technique[5]. In general, graphical passwords techniques are classified into two main categories: recognition-based and recall-based graphical techniques [6]. In recognition-based graphical technique a user is asked to identify one or more images he chose during the registration phase and on successful identification the user is given access to the data. In recall-based graphical technique the user is asked to replicate the password (for example-a signature) that he made during the registration phase and if he does so then he is given access to the relevant data or application. However there are some disadvantages of the graphical password scheme which are as follows:- login process takes a longer time [7], the shoulder surfing attack(which means looking over someone's shoulder to get passwords) ,etc. Therefore to overcome the disadvantages of textual and graphical password authentication scheme, we propose a hybrid authentication technique. In section II we provide a brief overview of the existing systems for password authentication-their advantages and disadvantages. Section III contains our proposed system and the algorithm and the conclusion is given in section IV.

II. EXISTING SYSTEMS IN PASSWORD AUTHENTICATION SCHEME

There are various authentication schemes that uses text as well as graphics however they lack the security factor. The various existing authentication schemes are as follows:

A. Recall Based System

In Recall based password authentication the users need to reproduce their passwords that they had made during their registration phase [8].

Example: Pass point algorithm:
Pass point is an improvised version of Blonder's algorithm. In Blonder's algorithm [9] the user has to click on predefined regions of an image in a particular sequential order, which is provided to the user while setting up an account as shown in Figure 1. After successful clicks the user is given authorization. In Blonder's algorithm invisible boundaries are created to guide the system to verify the authenticity of tap points by

DOI 10.17148/IJARCCE.2015.4977

user. The main weakness of Blonder's algorithm is that, since it has limited number of predetermined click regions the password needs to be of greater length to make it more secure from attackers. Therefore, pass point was created to overcome the drawbacks of Blonder's algorithm. In Pass point algorithm [10] there is no need to create invisible boundaries like the Blonder's algorithm. As shown in figure 2 the user can select any points in the image, also the image to be used can be any real life and complex. It does not need to use cartoon-like images like that in the case of Blonder's algorithm. The main drawback of Pass point algorithm is that it takes a lot of time for the users to learn the password. The time taken can be even greater than that of the text based alphanumeric passwords. Also the time taken to login into the system is greater than text based password system [10].

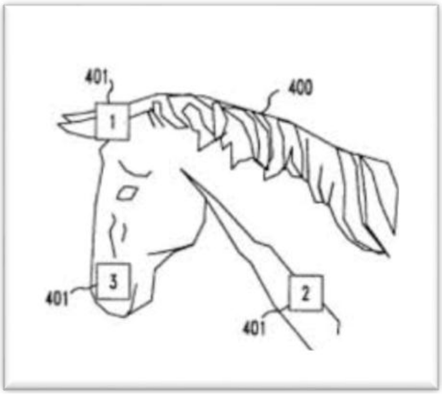


Figure 1: Example of Blonder's Algorithm.

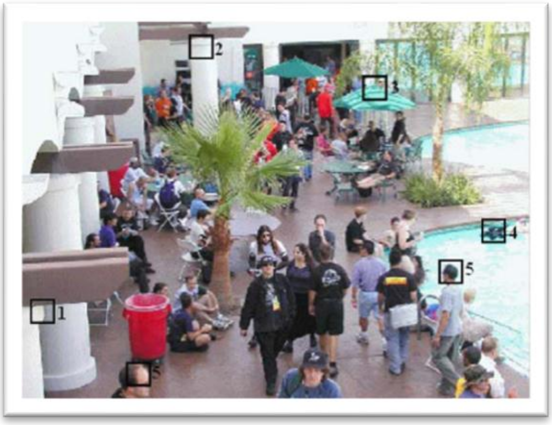


Figure 2: Example of Passpoints Algorithm.

B. Recognition based System

In this category users will choose pictures, icons or symbols from a collection of images. In authentication process the users need to recognize their registration choice among a set of candidates [11].

Example: Sobrado and Birget Scheme:

Sobrado and Birget developed a graphical password technique that deals with the shoulder surfing problem. In the first scheme, the system will display a number of pass-objects (pre-selected by user) among many other objects [12]. To be authenticated, a user needs to recognize pass-objects and click inside the convex hull formed by all the pass-objects as shown in figure 3. In order to make the password hard to guess, Sobrado and Birget suggested using 1000 objects, which makes the display very crowded and the objects almost indistinguishable, but using fewer objects may lead to a smaller password space, since the resulting convex hull can be large. In their second algorithm, a user moves a frame (and the objects within it) until the pass object on the frame lines up with the other two pass objects [13]. The authors also suggest repeating the process a few more times to minimize the likelihood of logging in by randomly clicking or rotating. The main drawback of these algorithms is that the log in process can be slow.

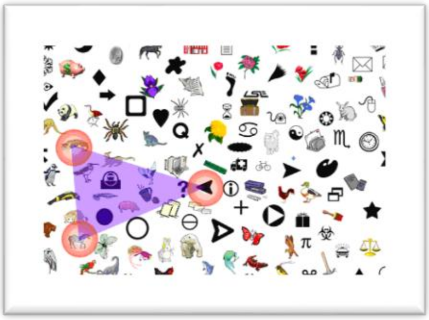
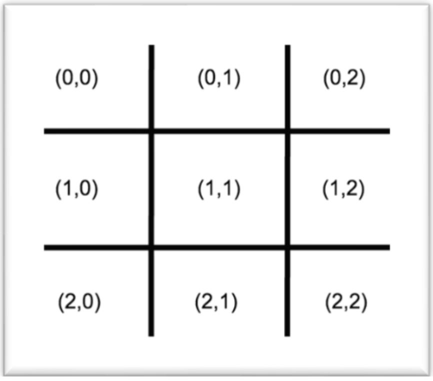


Figure 3 :Example of Recognition Based System.

III. PROPOSED SYSTEM

Our proposed system is based on graphical password authentication system and textual based password authentication, which overcomes the demerits of text based and graphical password authentication techniques. The method is a 2-level authentication system consisting of 3 steps, thereby-reducing the probability of an attacker breaking into the system. Despite the recent surge of graphical password authentication techniques, its drawbacks are well known and the most eminent of it is the 'shoulder surfing' attack. Therefore to avoid this attack, we provide a customized solution in which the user does not have to make the use of mouse clicks rather the user selects his/her image by the use of grid values. The grid values are shown in figure 4.



(0,0)	(0,1)	(0,2)
(1,0)	(1,1)	(1,2)
(2,0)	(2,1)	(2,2)

Figure 4: Values of the grid from where the image will be selected.

Now, if the user had selected the image on the grid value (2,2)

Rather than clicking on the image the user will enter the grid value from his keyboard to avoid shoulder-surfing attack.

The **Algorithm** is as follows:

ALGORITHM:

Registration Phase: The user has to fill in the details for the required (*) fields. The fields are as follows:

1. Username
2. Password 1 for image 1
3. Password 2 for image 2
4. Password 3 for image 3

The example of the registration phase is shown in figure 5.

Algorithm for Registration:

- The user has to select three images from a pool of images existing in the system.
- Every time the user selects an image, he/she has to select an alphanumeric string that will be associated with the corresponding image only, having a limit of 0-3 characters.
  Example-If the user wants to select the image in the grid (1, 1) and the corresponding password for image 1 is sh. Then he/she has to write the following in the row of IMAGE 1: 1sh1
- User has to remember the order of the selected images
- The user will be provided with an example that displays how he/she has to enter his/her password at the time of log-in.

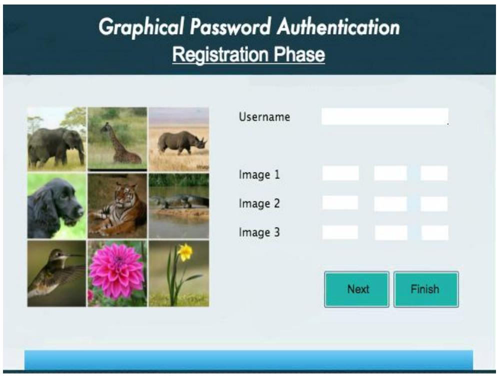


Figure 5: Registration Phase

Algorithm for Log-in Phase:

- Initially in the log-in, user has to enter the username.
- Next, user will be provided with a grid of (3x3) images. One of the images within this grid will be the first image that the user has selected during the registration phase. (Note that the user does not have to select the image with his mouse rather he has to enter the location of the image.)
- In the password field, the user has to enter the following:
  1. The x-coordinate of the image location.
  2. The alphanumeric string entered during the registration phase for the corresponding image.
  3. The y-coordinate of the image location.
     Example: The location of the image-1 is (1, 3) and the string associated with it is suppose AB.

Therefore the password for image-1 will be - 1AB3.

- Next, the user will be provided with a new shuffled grid consisting of the second image and the user has to follow the above steps and do the same for the third grid.
- In the end, system will verify the complete password and the user will be logged in based on the result.

Advantages of Our Proposed System:

The main advantage of our proposed system is that it helps in overcoming the shoulder surfing attack because the user no longer has to click on a set of images displayed on the screen, which helps to prevent any direct observation from the attacker. Secondly, this system has a two level authentication mechanism and hence proving to be highly secured system.

IV. CONCLUSION

As security is of prime importance in this world of technology therefore in this paper, we have proposed a more secure password authentication system. The system combines graphical password scheme along with textual authentication scheme to form a hybrid method for authentication. This authentication scheme ensures protection against attacks such as shoulder sniffing attack, dictionary attack, etc.

REFERENCES

[1] Https://en.wikipedia.org/wiki/password_authentication_protocol.

[2] Shraddham. Gurav, leena s. Gawade, prathamey k. Rane, nilesh r. Khochare , “graphical password authentication-a cloud securing scheme”, 2014 international conference on electronic systems, signal processing and computing technologies

[3] Roshni rajavat, bhavna gala, asmita redekar,”textual and graphical authentication scheme resistant to shoulder surfing”, international journal of computer applications.

[4] Arash habibi lashkari, dr. Omar bin zakaria, samaneh farmand, dr. Rosli saleh, 2009, “shoulder surfing attack in graphical password”, international journal of computer science and information security (ijcsis).

[5] Nelson, d.l., u.s. Reed, and j.r. Walling, “picture superiority effect”, journal of experimental psychology: human learning and memory.

[6] Xiaoyuan suo, ying zhu, and g. Scott owen, 2005, “graphical passwords: a survey “, annual computer security applications conference.

[7] Http://www.seminarsonly.com/labels/graphical-password-authentication-advantages-and-disadvantages.php.

[8] Arash habibi lashkari, farnaz towhidi, dr.rosli saleh, samaneh farmand, “a complete comparision on pure and cued recall-based graphical user authentication algorithms”.

[9] Greg e. Blonder, graphical password u.s. Patent no. 5559961, 1996.

[10] Ejike ekeke kingsley ugochukwu,yusmadi yah jusoh , ” a review on the graphical user authentication algorithm: recognition-based and recall-based”.

[11] Arash habibi lashkari, farnaz towhidi, dr.rosli saleh, samaneh farmand, “a complete comparision on pure and cued recall-based graphical user authentication algorithms”.

[12] Xiaoyuan suo, “a design and analysis of graphical password”

[13] Xiaoyuan suo, ying zhu, g. Scott. Owen, “graphical passwords: a survey”

DOI 10.17148/IJARCCE.2015.4977