Research Article

Image Based Graphical Authentication System using Clickpoints

Ajay Sharma¹, Prof. M. Hema²
Department of Computer Science and Engineering
SRM Institute of Science and Technology, Chennai, India

Abstract:
An image-based password works by providing the user with a password which is created by selecting the images and then selecting the click points in the images. These two combined forms a password. Now at the time of logging in again, the user is given has to select the click points from these images. The images are provided in order. The user has to select the click points in these images, which he previously selected. Hence, these passwords are called graphical passwords. The most common practice in user security is the usage of the alphanumerical usernames and passwords. This method has its cons. For example, it makes the guessing of the password and breaking into the account easily. If we consider a password which is difficult to guess, the user forgets it. So, to remove this problem, usage of the images and the click points as the password is proposed. And further, encryption is done on the file using the Advanced Encryption Standard. The graphical password is easier to remember and even enhance security.

1. INTRODUCTION
One of the most important factors in information security is data security and authentication. Using the internet, we can publish anything across the world. Every institution tries to have better security, both for its internal data and the clients. User authentication is the primary component of any organization because, after the authentication, the user can access the system. Traditional security techniques are less secure than the upcoming techniques. Since it is a human tendency to remember images easily than the text. So, an image based security system will enhance both the security and memo ability.

2. PREVIOUSLY USED TECHNIQUES

2.1. TEXT OR ALPHANUMERIC PASSWORD
In this password authentication, the user has to create a password using alphabets and number or a combination of both. This is the most commonly used techniques. But it has its disadvantages too. There are chances of the password being stolen by the hackers. We can see that in many interfaces, the password has to be a minimum of eight in length and it should be a combination of alphabets and digits. Still, this password authentication does not provide much security. Cons- These passwords are difficult to recall as the password has to be a combination of the numbers and alphabets and should include the special characters. To reduce the risk of forgetting the password, many users store the password in a text file in their system. The password can be easily stolen if the file is accessible. If not, there are many attackers who use spyware which can easily be plugged into the system and steal the password.

2.2 BIOMETRIC AUTHENTICATION
Biometric Authentication is a type of user authentication which uses the body elements for the evaluation of the user's identity. These are one of the most secure authentication systems preventing any unauthorized access. There are no flaws in the system for hackers to detect and then steal the password. Biometric authentication is mainly used when there are critical security requirements. It is a long term security system for any organization. The various ways to implement the biometric authentication are iris scanner, fingerprint scanner, audio analyzers etc. Cons-The biometric authentication is costly as a huge amount of hardware is required in comparison to other authentication techniques. The method is not suitable for who do not have the ability to put fingers, hands or eyes properly on the system e.g. arthritic persons.

2.3 SMART CARD AUTHENTICATION
In this authentication technique, there is a chip on the user's card and all the information is stored on the chip. It provides strong security. It can be combined with other authentication systems and provide additional security and protection. The card is swiped by the user to prove his authenticity.

Cons- The cards are small and can be lost easily.
It can increase the initial cost i.e. at the time when it is deployed.

3. LITERATURE SURVEY ON GRAPHICAL PASSWORDS
Nikam [12] proposed a graphical password scheme which also consists of text. At the time of the registration phase, different colors are shown to the user. The user has to select any one color to set the password. In the login phase, there is a circle having eight sectors with each having a different color. This is shown to the user. User can choose the sector which consists of the letter for the password and then can drag it into the sector having the colored are selected during the registration. Lashkari [3] proposed a new way of authentication in which the authentication is done by the selection of the images in different sizes of grids. The image is to be chosen from a 4*4 grid and the size of the grid during registration and login is different. Albayati [13] proposed a scheme which uses decoy image portions. A picture is to be uploaded by the user from the mobile gallery and the complexity level of the image is to be chosen. At the time of login, the system shows the portion of images which belong to the original image and depending on the complexity level selected at the time of registration. Tivka, M.L. [14]introduced an authentication technique consisting of cryptography, hashing, and the graphical passwords. At the registration phase, the user provides the login information and the password which he chooses is

International Journal of Engineering Science and Computing, April 2019

http://ijesc.org/
encrypted and stored in the database. At the second stage, he has to choose an image from the gallery as a password. At the time of login, the user enters the credentials which we provided during the registration phase. After two failed attempts, the user will be blocked and has to re-register. G.E. Blonder[4] introduced a password authentication technique. Using this technique, user can select some click points to choose the password from the images which were defined. At the time of login the user has to select points which were select a the registration time and then he is identified. Rane et al.[7] proposed a draw based technique in which at the time of login the images are shown to the user. The user has to select the images to make a password. After this, the user clicks on image from them to draw secret. During login, the user draws secret which was chosen in the registration phase.

4. INTRODUCED AUTHENTICATION TECHNIQUE

The technique is based on images. The user has to select a number of images he will choose in the registration phase. After selecting the number of images, the user has to select the images from the random display. Then, the user has to choose the click points in various images. The click points on the images will act as a password and will be required next time the user has to log in.

4.1 FEATURES OF INTRODUCED TECHNIQUE

(i) Valid username
The user has to enter a valid username. The user will be redirected to the image selection window after he enters a valid username.

(ii) Images
The user has to select a minimum of 3 and maximum of 5 images during the registration phase. Then, he will be redirected to the next page. In the next page different images are shown and the user has to choose the given number of images.

(iii) Click point
The user has to add click points in the various images that he chose. The click points, along with the images act as password and are required during the login phase.

(iv) Vault
The file is containing the information of the user is encrypted using the Advanced Encryption Standard.

4.1.1 REGISTRATION PHASE

During the registration phase, the user has to register by providing personal information such as email, name. The username should be unique. Then, the user has to select the number of images he has to choose and select as a password. Upon selecting the number of images, the user has to select the images and add the click points in the various images and now the login process is completed. Figure 2 shows the registration phase of the system.

5. IMPLEMENTATION AND ANALYSIS

The images based authentication is more secure than the textual passwords and much cheaper than the biometric authentication. The application was developed using python and the MySQL database was used to test the system.

6. RESULTS

The comparison was done on the following factors such as Security, Installation cost, Data redundancy, acceptance and memo ability.

- The proposed authentication system is more secure than textual password.
- It is easy to use.
- Images can be easily memorized.
- Images are not shown to unauthorized users.

7. CONCLUSION

This paper described image based graphical authentication techniques using cued click points. The introduced technique is based on the additional improvements in the previous technique by the researchers. In this technique, the user has to add click points at the registration. At the time of login, he has to click on the points he chose previously. The images and the click points are not visible to the unauthorized user.

8. REFERENCES


