International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor (2018): 7.426

Session Authentication Using Color Schemes and Images

Manjula Devi B[1], Rinny Mamachan[2]

[1, 2] Sri Shakthi Institute of Engineering and Technology, Coimbatore, Tamil Nadu, India

Abstract: ***Authentication is the first step in information security. It requires the user to set a password and remember it at the log in time. Textual passwords are the most traditional schemes that are used for providing security, but textual passwords are vulnerable to dictionary attacks, shoulder surfing, and spy ware. Graphical password schemes overcome the shortcomings of textual passwords, but they are vulnerable to shoulder surfing attacks. To address this problem, text can be used in combination with the colors and images to generate session passwords, thereby making a stronger authentication scheme. In this project the authentication scheme uses colors and text for generating session passwords.***

Keywords: Authentication, Session Passwords, Random Art Images

1. Introduction

Textual passwords are most common method of authentication purpose. The vulnerabilities of this method like eaves dropping, dictionary attack, social engineering and shoulder surfing are well known. The paper proposes a new password authentication technique which use session password. Session passwords are one- time passwords used only once. Once the session is terminated, the password is no longer useful. For every log in process, user must input a different password. Session passwords provide better security against dictionary attacks and brute force attacks as password changes for every session. The proposed authentication schemes use text and color schemes for generating session passwords.

2. Literature Survey

Today, computers are connected with other computers, and a world-wide net- work has been established. Authentication schemes range from simple to complex. And its has been discerned that none of the recent authentication schemes can resists all sorts of attacks. With this outcome this paper proposes authentication schemes which can resists all sorts of attacks.

Dhamija and Perrig et al proposed Dej'a Vu: A user study using Images for Authentication
In this journal they proposed, a system for user authentication. Dej'a Vu is based on the observation that people have an excellent memory for images. Using Dej'a Vu, the user creates an image portfolio, by selecting a subset of p images out of a set of sample images. For authenticating the user, the system presents a challenge set, consisting of n images. This challenge set contains m images out of the portfolios. The remaining n-m images are called the decoy images. The user must correctly identify the images which are part of her portfolios.The results have showed that 90% of all users succeeded in the authentication using this technique, while only 70% succeeded using text based passwords. A weakness is that the server needs to store the seeds of the portfolio images of each users in plain text. Coming in handy, it can be tedious and time consuming.

Ms Grinal Tuscano, Aakriti Tulasyan, Akshata Shetty, MalvinaRumao, Aishwarya Shetty: Graphical password authentication using Pass faces
They proposed a graphical password authentication technique which focuses on providing more powerful secure authentication mechanism. System goes through several phases before creating a password and while logging into the system such as image selection, image distortion, text association and manually password generation.

There is a growing interest in using pictures as passwords instead of text passwords. The main reason for using Graphical passwords is that they can be easily recalled. This paper proposes a two step graphical password authentication system which is based on Pass faces. In order to make the system user friendly and at the same time difficult to crack, images are combined along with text.

Sonia Chiasson, van Oorschot and Robert Biddle: Graphical Password Authentication Using Cued Click Points
They developed a technique called Cued Click Points. In this users click one point on each of c = 5 images rather than five points on one image. In ccp each click results in showing a next image, in effect leading users down a "path" as they click on their sequence of points. A wrong click leads down an incorrect path, with an precise indication of authentication failure only after the final click. For implementation, CCP initially functions like Pass Points. During pass-word creation, method is used to determine a clickpoint's tolerance square and corresponding grid. Each click-point in a subsequent login attempt, this grid is retrieved and used to determine whether the click-point falls within resistance of the original point. With CCP, we further need to regulate which next image to display.

Auser's initial image is selected by the system based on some user characteristic. The sequence is rejuvenate on-the-fly from the function each time a user enters the password. If a user enters an incorrect click-point, then the arrangement of images from that point on wards will be incorrect and thus the login attempt will fail. For an attacker who does not know the correct arrangement of images, this cue will not be helpful.

Ccp is susceptible to shoulder-surfing attack. If the username, the image sequence, and the click-points are observed through shoulder surfing then an attacker has all of the information needed to break into the account, as is the case with Pass Points and most other password systems.

The Cued Click-Point method is very useful and provides great security. By taking advantage of user's ability to recognize images and the memory trigger associated with seeing a new image. Cued Click Point is more protected than the previous graphical authentication methods. CCP increases the workload for attackers by forcing them to first acquire image sets for each user, and then analyse for hotspot on each of these images. Cued Click-Points method has advantages over other password schemes in terms of usability, security and memorable authentication mechanism.

Signature-Writing-Parameters

Handwritten signatures have long been used as a proof of writing of, or at least agreement with, the details of a document. The reasons of using signature as authorship proof are as follows:

1) The signature is authentic. The signature convinces the document's recipient that the signer carefully signed the document.
2) The signature is unforgeable. The signature is a proof that the signer and no one else carefully signed the document.
3) The signature is not reusable. The signature is a part of document; an un- scrupulous person cannot move the signature to a different document.
4) The signature is unalterable. After the document is signed, it cannot be altered.
5) The signature unrepudiatable. The signature and the document are physical objects. The signer cannot claim that he/she did not sign it, later.

Presently, handwritten signatures are verified by human with his/her eyes. Obviously, the verification result depends on his/her subjectivity. A system using computers for verification does not have such a shortcoming. But for the effective use of computers, we need to find suitable signature-writing-parameters.

In the identification system, the successful verification rate is not greater than 93%. But 7% is left for the further improvement. It is guessed that this result has something to do with the proficiency of the use of mouse. In usual, mouse is not used for writing signatures, so tests do not get used to writing signatures using mouse. Although tests in the experiments are familiar with using computers, they are not familiar with writing a signature using mouse. This is probably why the successful verification rate does not achieve a higher rate than 93%.

But at the time of registration the user draws a signature that is extracted by the system. At the time of registration, the signature is normalized and the parameters are extracted and its checked and the user is authenticated if the parameters are matched. But drawing with the mouse is not easy and actual parameters are not matched with the signature which is done at the time of registration. This scheme are prone to forgery of the signature.

Graphical Passwords

Approach to computer systems is most often based on the use of alphanumeric passwords. However, users have difficulty in remembering a password that is long and odd-appearing. Instead they create short, simple, and insecure passwords. Graphical passwords have been constructed to try to make passwords more memorable and easier for people to use and, therefore, more secure. Most of the graphical password schemes were introduced in order to overcome the disadvantages in text based passwords. But, unfortunately, not many of them turned out to be successful. Graphical passwords may offer better protection than text-based passwords because many people, in an attempt to memorize text based passwords, use plain words (rather than the recommended jumble of characters). A dictionary search can often bonk on a password and allow a hacker to gain entry into a system in seconds. But if a series of selectable images is used on successive screen pages, and if there are many images on each page, a hacker must try every possible combination at random. In this paper, we conduct a survey on the existing graphical password technique. We will discuss the strength and weakness of the graphical password schemes and also focus on the future scope in this field. In this survey, we want to answer to answer some questions such as:

1) Is graphical password more secure than text password?
2) What are the general issues in terms with design and implementation the graphical passwords?
3) What are the current weakness of each graphical password techniques?

4. Proposed System

In the proposed system, the system checks whether the user is already registered or not. If the user is already registered, then it advances to the login page. The user calculates the session password from the login interface. This session password is concatenated with the text password given during registration. But if the user is not registered, the system displays the registration interface. Here, the user enters the personal details, text password and also provides ratings to the random art images. This will be followed by the login phase where the user enters the password. The system also calculates the password in every session. This will be compared with the user entered password. If both are same, the user will be authenticated.

Primary-level Authentication

Here the user can choose either pair-based or textual-based authentication.

Pair-based authentication

There is grid which consists of both numbers and alphabets arranged randomly. The secret pass is remembered as pair where first letter describes the row and second, the column. The interchange letter of the selected row and column generates the character which is a part of the session password.

Hybrid textual authentication

The set of colors displayed are ranked based on the ranking given during registration. It is also remembered as a pair where the first number denotes the row and second, the

column. The intersection number of the row and column in the interface grid will be the password for the session.

Secondary-level Authentication
Here a 3X3 grid with dots is shown and the user has to draw the pattern which he has given during registration. If both the patterns matches, then the user will be given access to the files and folders. This type of authentication technique provides a higher level security for one's documents. It is difficult for the intruder to hack the system as it contains multiple levels of authentication. It is also less vulnerable to common hacking methods such as shoulder surfing, dictionary attacks, eaves dropping, etc.

Login Phase
In this Module, the user has to enter the password based on the interface displayed on the screen. The user chooses four images of random images as their password and the users have to select their pass image from images.

1) Find each digit of session password using the random arts and the number grid.
2) Concatenate the session password with the text password submitted during registration. 3. Submit the entire password.

Verification Phase
The system verifies the password entered by comparing with content of the password achieved during registration. The authentication techniques should be verified extensively for usability and effectiveness.

1) Check whether the entered password is correct.
2) If yes, authenticate the user to enter into the desired application.
3) Else
   a) If the number of attempts is below 4, reload the page.
   b) Else, exit the application.

5. Input

The input is the combination of session and textual password. The session password is obtained by comparing the pair based random arts, using a matrix.

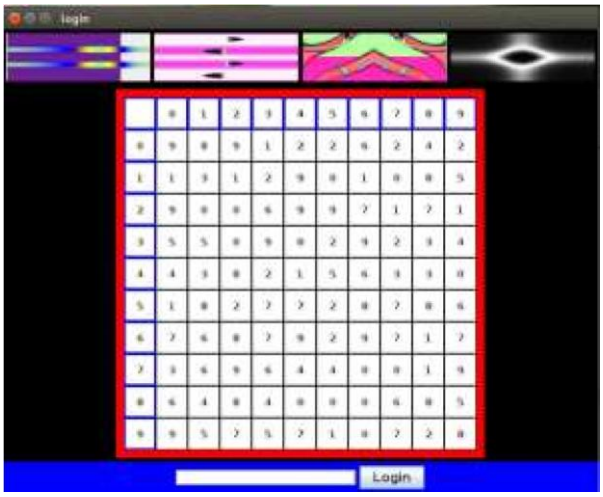

Figure 1: Entering the Session Password

6. Output

The output will be the successful login to the particular file or folder. Hence the files can be readily accessed.

Figure 2: Successful Login

7. Analysis

The use of one time passwords or session passwords makes this system efficient than other authentication means. The performance of the system can be evaluated by considering the following parameters**:**

Security
The use of session passwords makes it very difficult for the hackers to predict the passwords. Hence it eliminates most of the attacks to a very large extent.

Cost
Here, passwords are generated and validated using computer programs. This system does not require any hardware as it completely focuses on the software part. Thus the implementation cost is low when compared to the existing systems such as biometric**s.**

Usability
Since users have a better memory for images rather than texts, this system allows the user to achieve a secure and effective authentication.

Availability
Since the system does not enforces any hardware requirements, it can be implemented in any platform or environment such as personal computers, social networking sites, application lockers etc.

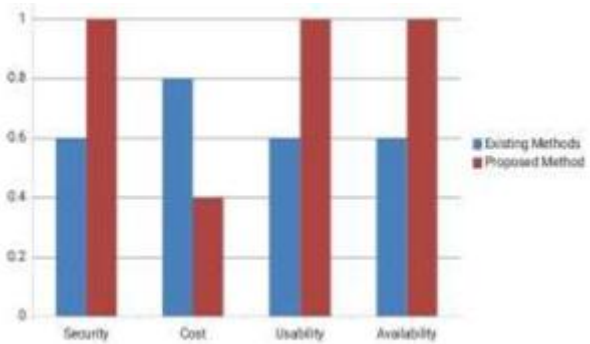

Figure 3: Comparison of existing and proposed methods

8. Conclusion and Future Scope

We proposed an authentication mechanism that uses one time passwords or session passwords. It also makes it difficult for the intruders to crack since the passwords are obtained by matching color schemes. Even if a password is hacked, it cannot be used for the next login as it is valid only once. Thus this method offers better security by preventing unauthorized access. Though color passwords are in its initial stages, they can be extended for providing secure access to social networking. This technique can be developed as windows application such as folder locker or as an application locker for smart phones. It can also be used as an external gateway authentication to connect the application to a database or to any external devices.

References

[1] *Shefali Amlani, Shweta Jaiswal, SuchitraPatil, "Session Authentication Using color Scheme*", International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 6(2), 2015, 1420-1423.
[2] Rachna Dhamija, Adrian Perrig,"*Deja Vu: A User Study Using Images for Authentication*", SIMS/CS, University of California Berkeley.
[3] Ms GrinalTuscano, AakritiTulasyan, Akshata Shetty, MalvinaRumao, Aishwarya Shetty, *"Graphical password authentication using Pass faces"*, Int. Journal of Engineering Research and Applications, ISSN:2248-9622, Vol.5, Issue3, (Part-5)March 2015, pp.60-64.
[4] Manjunath G, Satheesh K, Saranyadevi C, Nithya M, *"Text-Based Shoulder Surfing Resistant Graphical Password Scheme"*, International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 5 (2), 2014, 2277-2280.
[5] Balaji, Lakshmi. A, V. Revanth, M.Saragini, V. Venkateswara Reddy, *"Authentication Techniques for Engendering Session Passwords with Colors and Text*", Advances in Information Technology and Management Vol. 1, No. 2, 2012.
[6] S. Balaji, Lakshmi.A, V.Revanth, M.Saragini, V. Venkateswara Reddy, "*Authentication Techniques for Engendering Session Passwords with Colors and Text*", Advances in Information Technology and Management Vol. 1, No. 2, 2012.
[7] D.W. Davies, W.L. Price, *"Security for Computer Network"*, John Wiley & Son, Ltd, 1984.
[7] M. Kasukawa, Y. Mori, K. Komatsu, H. Akaike, H. Kakuda, "*An Evaluation and Improvement of User Authentication System Based on Keystroke Timing Data*", Transactions of Information Processing Society of Japan, Vol.33, No.5, pp.728-735, 1992. (in Japanese).