USER SIDE AUTHENTICATION USING SESSION PASSWORDS AND COLORS BOX

Prashant Vasant Divase[1], Surajkumar Rajeshwar Thakare[2], Mandar Arun Pingale[3],Vivek Jagnnath Patsawane [4], Mr. C. B. Pednekar [5]

[1,2,3,4]*Computer Department, Pune University, (India)*

[5]*Asst. Prof, Computer Department, Pune University,(India)*

ABSTRACT

In today's world, security is required to transmit confidential information over the network. Security is also demanded in wide range of applications. The most common method used for authentication is textual password. But textual passwords can be easily hack by guessing, spoofing or by the software tools available now a days like Keyboard logger or Mouse logger if we use our normal keyboard or mouse while filling Authentication information. Random and lengthy passwords can make the system secure. But the main problem is, the difficulty of remembering those passwords and that is also can be hack and crack by using Hacking software tools. To overcome this problem the alternative techniques were used that was graphical passwords and biometrics but Most of the graphical schemes are vulnerable to shoulder surfing. So encryption and decryption is the only method on which we can trust for secure authenticity but encryption and decryption using RSA algorithm is not so secure because of using ASCII character. The same cipher text will be produced if the same character is repeated more than one place in the plain text. That's why we are using the new technology for encryption and decryption that is MRGA.

Keywords : Authentication, Encryption and Decryption, RSA algorithm, Spoofing, Textual password.

I INTRODUCTION

Textual Password can easily hack by hacker. Graphical passwords are introduced as alternative techniques to textual passwords. Most of the graphical schemes are difficult to shoulder surfing as compare to textual password. Text can be combined with images or color to generate session passwords for authentication. Session passwords can be used only once and every time a new password is generated. In this application, two techniques are proposed to generate session passwords using text and colors which are resistant to shoulder surfing. Session passwords are passwords that are used only once. Once the session is terminated, the session password is no longer useful. For every login process, users input different passwords. The session passwords provide better security against attacks as password changes for every session. In MRGA we are trying to improve and make more strong password rather than virtual keyboard and plain text password. The proposed authentication schemes use text and colors for generating session passwords. When the session password is entered an innovative algorithm namely Magic Rectangle Generation Algorithm (MRGA) is being proposed in this work. It is helpful to enhance the security due to its complexity in encryption process. The singly even magic rectangle is formed based on the seed number, start number, row sum and column sum. The value of row sum

and column sum is very difficult to be traced. User has to enter his password from the matrix which includes all characters and numbers. And that would be of 6*6 ‘s matrix so it is very difficult for hacker to crack his password, and one more thing is that when user tries for login he has to enter the password from the 6*6’s matrix virtual keyboard and the first two latters of his original password would be pair and the interaction point (key) will consider as his new password for that session only and then next pair and then next…So like this user enters his new session password which would be very difficult for hackers to guess even after shoulder surfing.

II RELATED WORK

2.1 Dhamija and Perrig

Dhamija and Perrig proposed a graphical authentication scheme based on the Hash Visualization technique. In their system, they proposed a graphical authentication scheme where the user has to identify the pre-defined images to prove user’s authenticity. In this system, the user selects a certain number of images from a set of random pictures during registration. Later, during login the user has to identify the pre-selected images for authentication from a set of images. The results showed that 90% of all participants succeeded in the authentication using this technique, while only 70% succeeded using text-based passwords and PINS. The average log-in time, however, is longer than the traditional approach[1].

Advantage

Though the average time taken to log into the system in longer than that of the traditional approach, it has a much lower rate of failure. [2]

Disadvantage

One drawback of this technique is that since the number of thumb nail images is limited to 30, the password space is small. Each thumbnail image is assigned a numerical value, and the sequence of selection will generate a numerical password. The result showed that the image sequence length was generally shorter than the textural password length. To address this problem, two pictures can be combined to compose a new alphabet element, thus expanding the image alphabet size. A weakness of this system is that the server needs to store the seeds of the required images of each user in plain text. Also, the process of selecting a set of pictures from the picture database can be boring and time consuming for the user.[2]

2.2 Passface

Passfaces are graphical passwords that use faces as a unique verification technology for secure logon. Offering two factor authentication to provide a high level of authentication assurance, Passfaces supports a wide range of operating environments in which strong authentication is required. Passfaces Web Access easily integrates with existing security systems in financial, government, healthcare, and corporate networks. Passfaces is completely intuitive to use and combines two way authentication – user-to-site and site-to-user in a single, reliable process.[3]

What is Two Factor Authentication?

Two-factor authentication is a security process in which the user provides two means of identification, one of which is typically a physical token, such as a card, and the other of which is typically something memorized, such as a security code.

Think of Passfaces as kind of a reverse biometrics. Rather than trying to recreate the complexity of the human brain, Passfaces takes advantage of it. The basic configuration of Passfaces is typically from 3 to 7 Passfaces that make up a single code. This number is variable depending on the application and like a password is determined by the system administrator. The number of Passfaces assigned takes into account a combination of security, usability and practicality considerations.[2]

Advantages

1. Passfaces are very unique in the whole world.
2. Safer than finger print based authentication. Finger prints can be duplicated.
3. Much safer than normal face recognition based authentication. Your normal photo cannot pass off as you in passface system.
4. Even identical twins cannot hack each others passfaces, unless they know it.
5. People can see your passface but still not be able to use it, unless they take a high-res picture of it.[4]

Disadvantages

1. You will look like a fool in public places.
2. The paparazzi might steal your passface using a telephoto lens.
3. Needs a camera. But then most devices come with cameras these days.
4. Sudden changes in faces requires the use of the override password.[4]

2.3 Jermyn, et al.

They proposed a new technique called “Draw- a-Secret” (DAS) where the user is required to re-draw the pre-defined picture on a 2D grid. The basic idea of Draw A Secret technique is that a user is asked to draw a simple picture on a 2D grid. The coordinates of the grid, occupied by the picture are stored in the order of the drawing. During authentication, the user is asked to redraw the picture. If the drawing touches the same grids in the same sequence, then the user is authenticated. But sometimes user fails to recall his/her password during the registration process. In the proposed work we are applying A Background image with das scheme to increase the remembrance of passwords. The basic idea behind the scheme is that the human nature that he or she can recognize pictures easily then the 2dgrids.[3]

Advantages

This paper presents the analysis of Draw-a–Secret technique for graphical passwords and Draw-a-Secret with background image. Both technique are useful to generate a graphical passwords above results shows that in terms of password character sticks the DAS With background Image approaches are useful as it is less time taking also easy to remember. Also, this technique is easy to recall due to introducing of background images. Results show that the security level of such technique is better.[2]

Disadvantages

This technique is easy for user to remember his password because the password is in the graphical form , and that’s

why it is less time consuming also but that can be hack by shoulder surfing.[5]

2.4 Syukri

Syukri developed a technique where authentication is done by drawing user signature using a mouse. This technique included two stages, registration and verification. At the time of registration stage the user draws his signature with a mouse, after that the system extracts the signature area. In the verification stage it takes the user signature as input and does the normalization and then extracts the parameters of the signature. User draw signature using mouse. It is a complicated process. Drawing with mouse in the same perimeters which registered is difficult task.[6]

Advantages

Copy of the anyone's signature is not so simple task. To copy it perfectly needs more practice still if any query identified while login with fake signature will terminate the system, we are saying that copying the original signature is difficult because login with the same perimeters which registered is very difficult task.[6]

Disadvantage

Drawing with mouse in the same perimeters which registered, Drawing with mouse is not familiar to many people, so it is very difficult and complicated process to draw the signature in the same perimeters. For the original user too, it is not only difficult for the other user to enter into any others account but also very difficult for the original user to get enter into his own account because he need to enter the perfect sign with perfect perimeters he used while registration.[6]

III MOTIVATION AND GOAL

All above Systems were defined just for security but all they had some disadvantages and they can be easily cracked by different techniques. According to Syukri,the accuracy of the original user is also very important, otherwise system may show original user as a fake user, because drawing the signature by using mouse is very difficult and the possibility of showing Difference in signature is there[4]

So after studying all previous related works, it motivates us to work on system for security of user's login information, and we will provide two levels to the users for his Authentication, first would be entering the original password in encrypted form by using MR(Magic Rectangle) Matrix and second would be the Matrix of the color grid. This two methods would be session based, so that It would be more secure,because the password of user changes session wise, and new password generates after every login.

IV PROPOSED WORK

4.1 Idea behind Algorithm

In order to overcome the limitations of previous approaches, we are trying to develop an algorithm. We will shortly describe the idea of MR(Magic Rectangle) algorithm below. During registration user submits his password. Maximum length of the password is 8 and it can be called as secret pass. The secret pass should contain even number of characters. Session passwords are generated based on this secret pass. During the login phase, when the user enters his

username an interface consisting of a grid is displayed. The grid is of size 6 x 6 and it consists of alphabets and numbers. These are randomly placed on the grid and the interface changes every time. User has to enter the password depending upon the secret pass. User has to consider his secret pass in terms of pairs. The session password consists of alphabets and digits. The first letter in the pair is used to select the row and the second letter is used to select the column. The intersection letter is part of the session password. This is repeated for all pairs of secret pass.

Color Box Authentication- The User should rate colors from 1 to 8 and he can remember it as "BIGCROPS". Same rating can be given to different colors. During the login phase, when the user enters his username an interface is displayed based on the colors selected by the user. The login interface consists of grid of size 8×6. This grid contains digits 1-8 placed randomly in grid cells. The interface also contains strips of colors. The color grid consists of 2 pairs of colors. Depending on the ratings given to colors, we get the session password.

V CONCLUSION

In our proposed work we are improving confidential security as compare to other security algorithm. It will be helpful for all sites,where user authentication eg .net banking, transfer funds or any application etc is required. Here we are trying to provide more security to user using MRGA algorithm

REFERENCES

[1] R. Dhamija, and A. Perrig. "Déjà Vu: A User Study Using Images for Authentication". In 9th USENIX Security Symposium, 2000.

[2] www.google.com

[3] Real User Corporation: Passfaces. www.passfaces.com

[4] Wikipedia

[5] Jermyn, I., Mayer A., Monrose, F., Reiter, M., and Rubin., "The design and analysis of graphical passwords" in Proceedings of USENIX Security Symposium, August 1999.

[6] A. F. Syukri, E. Okamoto, and M. Mambo, "A User Identification System Using Signature Written with Mouse," in Third Australasian Conference on Information Security and Privacy (ACISP): Springer- Verlag Lecture Notes in Computer Science (1438), 1998, pp. 403-441.

.