A Survey on Different Authentication Schemes for Session Passwords

Jay Patel, Ashil Patel

Department of Information Technology, L. D. Engineering College, Ahmedabad, Gujarat, India

ABSTRACT

To provide the security mainly authentication and authorisation is given to the system. For that purpose mostly textual passwords are being used. Now day's graphical passwords are also available. The password schemes those are being used by now Days are mostly textual password and the graphical password (pattern matching), textual passwords are vulnerable to eves dropping, dictionary attacks, social engineering and shoulder surfing. Graphical passwords are introduced as alternative techniques to textual passwords. But Most of the graphical schemes are vulnerable to shoulder surfing. This paper shows the study of the available authentication schemes for session password.

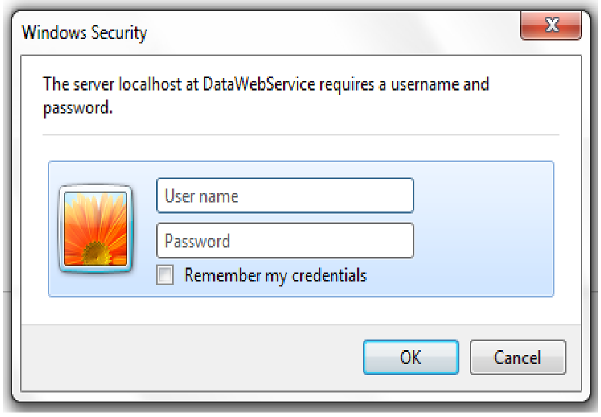
Keywords : Session, Authentication, Image Processing

I. INTRODUCTION

Security is mainly given by two mechanisms which are Authentication and authorisation. Now first we have to understand what is authentication and authorisation.

Authentication verifies "who you are?". It is a process in which the credentials provided are compared to those on file in a database of authenticated users.

For example the simple authentication is done every time when you log in to your mail account from the different computer or other device.


Windows Security

The server localhost at DataWebService requires a username and password.

Figure 1 : Windows Authentication

Authorisation gives information about what you are authorised to do. Authorisation is the function of specifying access rights to resources related to information security and computer security in general and to access control in particular.

Figure 2 : Authorisation

Another question arises "What is session?" In computer science or in particular networking, the session is a semi-permanent interactive information interchange. That is nothing but the interaction of informative communication within the limited time period.

What is session password? Now the password that is being used for the authentication for that session which means that the password is being used for the limited period of time is session password. For every session there will be a new session password.

II. METHODS AND MATERIAL

LITERATURE SURVEY

A. “Déjà Vu: A User Study Using Images for Authentication”[1]

Dhamija and perrig presented a graphical authentication scheme in which use have to identify the correct image from the set of image given to him and the time of authentication. Here they proposed a graphical authentication scheme where the user has to identify the pre-defined images to prove user’s identity.

In this scheme as shown in figure 3. A set of images shown to user and for authentication User must pick the image that is stored in database at the registration time as authenticated image.

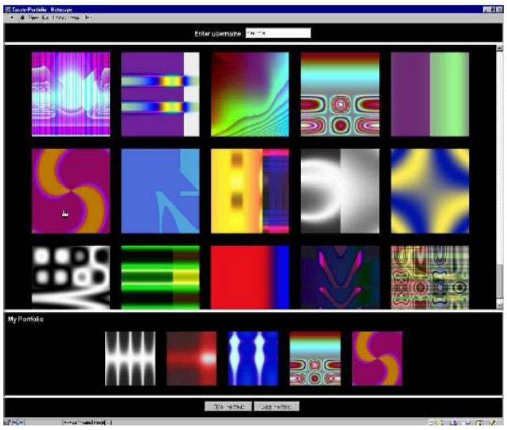


Figure 3: User Study Using Images For Authentication

B. Graphical password authentication using Pass faces [2]

In this graphical authentication scheme In this system the user sees a grid of nine faces and he has to choose one faces which he has previously chosen.

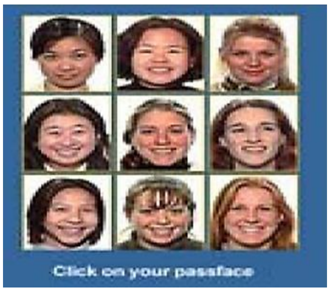


Figure 4: Authentication using pass faces

The password is formed of 4 faces
Pros: Highly secured password scheme
Cons: System is prone to several attempts

C. DAS (Draw- A- Secret) Graphical Password Authentication Scheme [3]

In this system a technique is used called Draw-a-secret. User has to draw the secret picture on a 2D-grid at the registration time for authentication and that secret picture is to be re-drawing by user for the session authentication.
Pros: Highly accurate picture needed for authentication
Cons: Vulnerable to shoulder surfing.

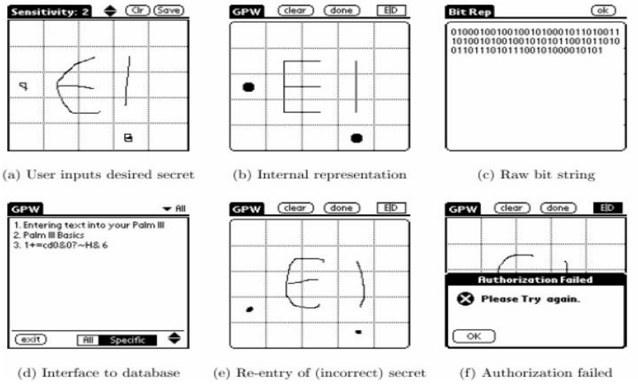


Figure 5: DAS (draw-a-secret) authentication scheme

D. A User Identification System Using Signature Written with Mouse [4]

In this system the authentication is done by using user’s signature by using mouse

The signature must match with the one that is provided at the time of registration
Pros: Forgery of signatures.
Cons: It is difficult to draw the signature in the same perimeters at the time of registration**.**

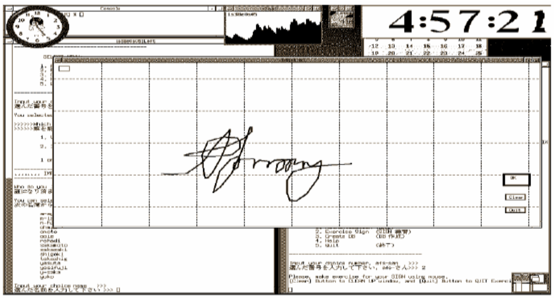


Figure 6 : Signature Based Authorisation

E. Convex hull method [5]

Includes graphical password entry scheme using convex hull method towards Shoulder Surfing attacks.

Large and small passwords can be created
Pros: Make the password hard to guess and large number of objects can be used.
Cons: small passwords can be guessable.

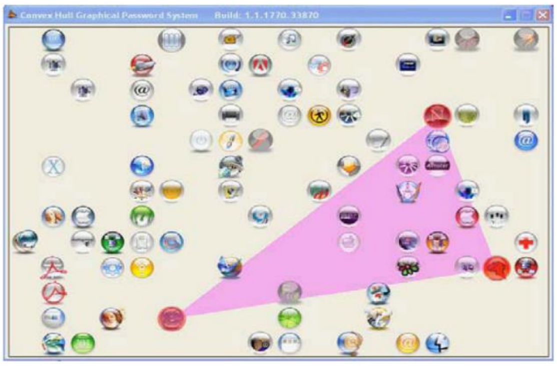


Figure 7 : Objects Based Authorisation

F. Combination of DAS and Story schemes [6]

This graphical scheme combines DAS and Story schemes to provide authenticity to the user.

In this scheme the set of image is being displayed to user and from those images the story is to be generated to form the sequence of the images. And a secret draw or shape is to be drawn on that story based Images. And this sequence of the selected images and the secret drawing on the image grid are to be used for the authentication process

Pros : Shoulder surfing resistant scheme
Cons : It is Prone to other attacks like brute attacks, Guessing etc.

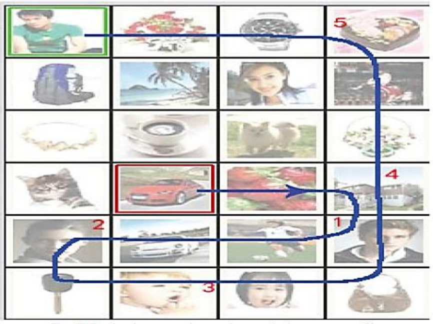


Figure 8 : Pattern Based Authorisation

III. CONCLUSION

In this paper we have studied different authentication schemes for session passwords using different graphical methods. These authentication schemes have their own advantages and disadvantages and mostly these are vulnerable to shoulder surfing attack. So, in future work will be that to improve one of these authentication scheme for session password and to make it more secure from shoulder surfing attack or to introduce a new authentication scheme that will be secure from shoulder surfing attack and vulnerability.

IV. REFERENCES

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

[2] Ms Grinal Tuscano, Aakriti Tulasyan, Akshata Shetty, Malvina Rumao, Aishwarya Shetty. ” Graphical password authentication using Pass faces”, In Ms Grinal Tuscano et al. Int. Journal of Engineering Research and Applications, 2015.

[3] Y.D.S.Arya and Gaurav Agarwal,” Impact of Background Images on the DAS (Draw- A- Secret) Graphical Password Authentication Scheme”, In IJCA Special Issue on “Network Security and Cryptography” NSC, 2011.

[4] 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.

[5] S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, N. Memon, “Design and longitudinal evaluation of a graphical password system”. International J. of Human-Computer Studies 63 (2005) 102-127.

[6] HaichangGao, ZhongjieRen, Xiuling Chang, Xiyang Liu UweAickelin, “A New Graphical Password Scheme Resistant to Shoulder-Surfing