T.Pavan Kumar, Nagesh Vadaparthi, A.Manvi, A.Alekhya/ International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 3, Issue 2, March -April 2013, pp.1749-1751

Secure Sessionbased Authentication Schemes

T.Pavan Kumar[1], Nagesh Vadaparthi[2], A.Manvi[3], A.Alekhya[4]
[1,2,3,4]Department of Information Technology, MVGR College of Engineering, Vizianagaram.

ABSTRACT:

Authentication is a process of verifying the identity of someone (a user, device, or an entity) who wants to access data, resources, or applications. Validating the identity shall establish a trust relationship for further interactions. Authentication even enables the accountability by making it possible to integrate both access and actions to specific identities. There are a huge number of techniques to provide security in terms of authentication. But still there is wide scope for much enhanced authentication schemes. Hence in this paper, we proposed a novel technique which is based of one-time Draw-a-secret method.

I. INTRODUCTION

In the current world of advanced technology, internet has become a part ofhuman life. But, the most promising issue is to protect the password. There are various techniques available in the literature for assuring the security of password. But, still there is a wide scope for improving the security aspects in protecting the passwords. Though there are various techniques viz., encryption of passwords, hiding of passwords etc., graphical image based authentication has its own importance in assuring the security.The above techniques are prone to cracking, dictionary attacks etc. [1]. Thus there is a need for an alternative technique to protect the passwords. This has paved a path for utilization of graphical passwords [2,3,4,5]. However, most existing graphical password authentication techniques are sensitive to shoulder surfing [1]. Therefore, there is a need for a novel approach that can resist the problems existing with the current graphical authentication schemes.

In this paper we propose a novel approach for graphical authentication schemes based on colors and images.In this technique we suggest new DAS scheme which overcomes the issues in DAS and RDAS. The paper is organized as the section-2 describes in detail about ODAS(One-Time Draw –a-Secret) scheme and various levels of authentication and section-3 conclude the paper.

Related Techniques

In this technique we have suggested a novel technique that can be applied for PCs, PDAs etc. In this approach security has been provided through session passwords. The process includes 4 levels of authentication where in the first level registration process is carried out, second level incudes pair-based authentication, third level is hybrid-based authentication and finally the fourth level is our newly proposed one-time draw-a-secret (ODAS) scheme.

REGISTRATION PROCESS:

In this process user needs to enter his mobile number. The users mobile number is initially verified as shown in fig(1)and a textual session-password is generated which is sent to the users mobile.

Fig-1: Mobile number validation screen

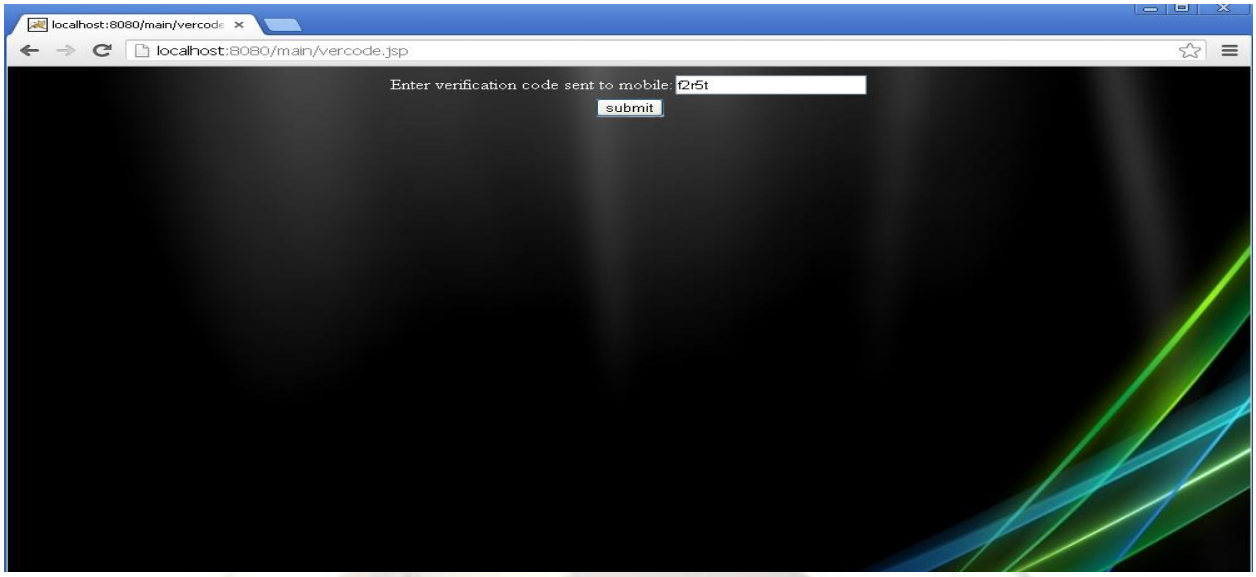

Fig-2: Authentication by OTP

Now the user needs to enter this OTP at the authentication screen as shown in fig(2). If the user is not registered he will be navigated to the registration page before getting login.If the client is a new user, then he must go through a few steps to get access to the application. First his mobile number is verified as said above and then after getting verified registration form is displayed as shown in fig(3).

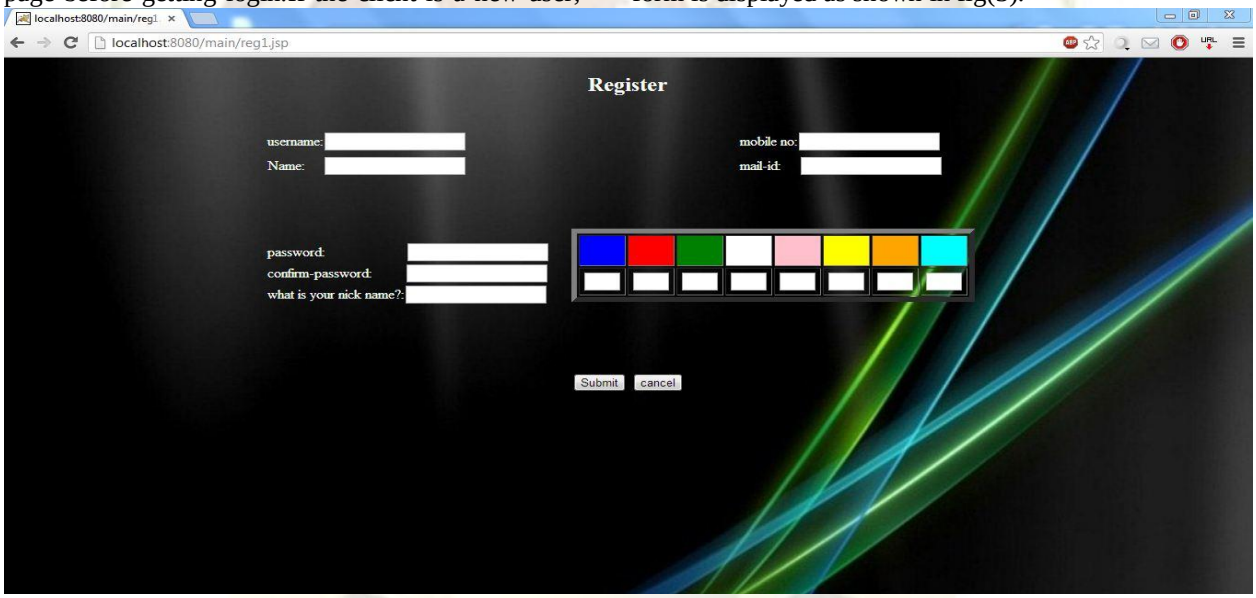

Fig-3: Registration Form

Then after entering his details in registration form a few DAS patterns are displayed where he needs to select his DAS scheme and finally has permissions to enter into the application as shown in fig(4). The DAS scheme is stored in database for future verification.

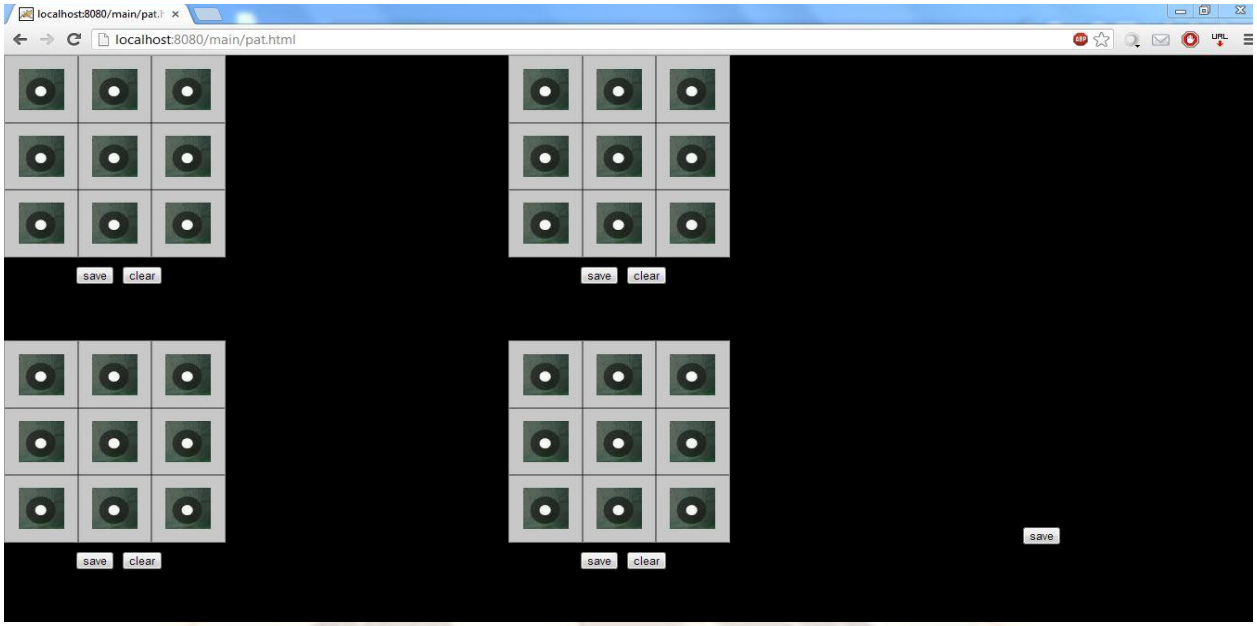

Fig-4: ODAS Scheme

PAIR-BASED AUTHENTICATION:

The pair based password is also known as secret password. The minimum length of the pair-based password is 8 characters. The user is made to enter the pair-based password with the help of a user-interface by dividing the password into pairs which was entered in registration page as shown in the above fig(4) named as password.

The user interface is divided into 6*6 grid which display a combination of letters and numbers. This grid changes randomly for every login. The secret pass which he enters in pairs is considered as a pair of letters in which the first letter is used to select the row and second letter selects the column. This intersection letter is treated as password to cross this level of Authentication.

HYBRID-BASED AUTHENTICATION:

The user at the time of registration is made to rate the colors as shown in fig(4) in the range of numbers 1 to 8.The interface contains 8 colors for which the user gives the rating. Depending on the ratings given by the user to the colors, and also a grid of 8*8 size which changes for every login, the session password is obtained.

II. ODAS

In the **One-Time Draw-a-Secret**level a grid of 3*3 consisting of set of same patterns are displayed. Here the session password is drawn based on the pattern selected during registration phase. This pattern changes for every login. For the first login we draw the first pattern. But as the login count increases the pattern gets rotated and is stored in the database. Now the user has to enter the rotated pattern after somelogins. This rotation is done based on some angle.

III. CONCLUSION

Authentication is an act of confirming the truth of an attribute of a datum or entity. This might involve confirming the identity of a person or software program, tracing the origins of an artifact, or ensuring that a product is what its packaging and labeling claims to be. Authentication often involves verifying the validity of at least one form of identification. Therefore it plays a vital role in accessing the data or entity. Hence, in this paper we have proposed a novel approach for secured authentication technique based on DAS which provides high security.

REFERENCES

[1] S.Balaji et al, "Authentication Techniques for Engendering Session Passwords with Colors and Text", Advances in Computer Science and its Applications, 1(3):189-195, 2012.

[2] H.Zhao and X.Li, "S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme", 21st International Conference AINAW 07, Vol.2, pp:467-472, Canada 2007.

[3] X.Suo, Y.Zhu and G.S.Owen, "Graphical Passwords: A Survey", Proceesing of ACSAC, 2005.

[4] A.H.Lashkari et al., "A New algorithm on Graphical User Authentication (GUA) based on multi-line grids", Scientific Research and Essays, 5(24):3865-3875, 2010.

[5] A.Sreelatha et al., "Authentication Schemes for Session Passwords using Color and Images", International Journal of Network Security & its Applications (IJNSA), 3(3):111-119, 2011.