IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 5, Ver. I (Sept - Oct. 2016), PP 58-63
www.iosrjournals.org

A More Secure Position Based Graphical Password Authentication

Mohd. Aqil Khan[1], YDS Arya[2], Gaurav Agarwal[3]
[1]*Ph.D.Scholar Venkteshwara University Gajraula, India*
[2]*Professor Invertis University Bareilly, India*
[3]*Assistant Professor Invertis University Bareilly, India*

Abstract: *We are proposing a new pass-point graphical password authentication by using a simple virtual environment. Our virtual environment is influenced by a social networking site' s game. In this system, user interacts with the virtual environment and user can generate sequence of interactions according to his /her choice which will gather by a background process. This process decides whether the user is authenticated user or a not, depending on which the system allows or denies accessing the resources. There are many existing authentication schemes are based on a simple pas-point mechanism, most of them are unsuccessful due to the shoulder surfing attacks. The proposed scheme seems sometime similar to the pass-point techniques but it is very much different with respect to the authentication process.*

Keywords: *Graphical password; Pass-Point; Authentication; Position based Graphical password.*

I. Introduction

Now days as we have seen that there is a rapid increase of computer system and internet. These systems and internets handle a large amount of data, demanding the need of secure authentication system. There are different authentication techniques available for securing these data. Every user which using the computer system has some sought of information to be securely stored which is not to be stolen, edited or viewed by somebody else[1].

Earlier, we used to use a textual secret e.g. password for securing our data later, people thought of that the password could be estimated. Hence, they came up with the idea of smart cards, PIN passwords etc. Even though these cards could be stolen [2]. After these problems the textual password converted into the graphical passwords. Which were based on the techniques known as the recall and recognition base (combinable said knowledge based graphical passwords) [3].

Humans do posses a lack of memory hence to produce a textual password after a long time of non-utilization of an account could lead to misery. But in recognition mechanism (used in the graphical password scenario) the system shows the users a set of graphical passwords out of which the user previously elected one provides a login. Thus, in this scenario we overcome the fact of memory loss. Graphical passwords also provide some kind of recall as well as recognition, which was also proving failure in authentication.

System developed, which prove to be a more secure method of access but at the same time there was problem in identifying the attributes of the legitimate user. E.g. suppose we have taken the example of To overcome these problems biometric fingerprint recognition if the user' s finger had a cut with a material then he or she will again register finger after healing because biometric system will not recognize it [4].

Though the biometrics was already available with the user physical aspects it did also possess disadvantages based on several factors such as consistency, uniqueness, and acceptability.

In this paper we propose a mechanism of graphical passwords (recall and recognition) combinable with a virtual environment. However, this technique have been tried to bring such authentication [5].

The proposed system depicts a virtual environment in pass-point graphical password scheme with some items placed randomly in it. The idea is taken by the game involve in a social networking site. The user' s password consists of a sequence of interactions with the items in the environment [6]. The actions performed by the users describe his/her physical and mental behaviors to the authentication system, then the system decide whether the user is genuine or not.

As the proposed system depends on the individual mental level of a user, hence, the system is safe, secure and easy to use.

This paper consists related inventions and innovations and also, describes the proposed scheme in which we will discuss the guidelines of building the virtual environment and its applications.

II. Related Inventions and Innovations

In the security of passwords a new revolution is brought by Blonder by developing the graphical password schemes [7]. The graphical passwords consist of both recall and recognition methodologies e.g. Pass-

faces, Pass-point, DAS etc. Theses techniques could produce a longer password size it suffered from the shoulder surfing attack.

Our work is based on the pass-point technique. The pass point system was the extended version of Blonder' s method and proposed by Wiedenbeck et al in year 2005 [8]. According to the method proposed by them, system eliminates the predefined boundaries and will allow arbitrary images to be used. As a result, a user can click on any place on an image to create a password. A tolerance around each chosen pixel is calculated. In order to be authenticated, user must click with in the tolerance of their chosen pixels and also in the correct sequence as shown in the figure 1.

As in this technique any picture can be used and picture may contain many memorable points, so the possible password space is very large. Wiedenbeck, et al. conducted a user study Google (2007 This technique was firstly based on memorization of human [9].), in which one group of participants were asked to use alphanumerical password, while the other group was asked to use the graphical password. The result showed that graphical password took fewer attempts for the user than alphanumerical passwords. However, graphical password users had more difficulties learning the password, and took more time to input their passwords than the alphanumerical users [10].

The proposed system involves the efficient utilization of the mechanism used in pass-point method with small size and optimal solution by using a virtual image.

III. The Proposed System

The proposed system is developed to overcome some disadvantages of previous system. These disadvantages are as follows:

- The system should be smaller in size so that the utilization of user can increase
- The proposed system should be easy to use
- The proposed system gives the higher size of password as compared to the previous system
- Password provided by the system should be easy to recall
- User should have the freedom of selecting their password [11].

Keeping these points in mind we developed a system as follows.

As the proposed system is the combination of different authentication schemes. So it presents a simple virtual environment containing various items. In the proposed system a user can go through the virtual environment and changes the state of different items present in the image. On the other hand in the pass-point method a user can click the different points in the image but can not change the state of any object. For example in a virtual environment a user can switch the light on for login, move a chair from one end to another end to login etc. the combination and sequence of these actions can create the password of user. The main difference from pass-point and the proposed technique is that there is not only the clicking of object but here the object can move. Here are some more examples for virtual environment.

- Opening and closing of window or door.
- Using a virtual keyboard for text.
- Biometric authentication in virtual environment
- Virtually writing on a paper
- Movement of any item.

If we are changing the state of any object in registration process then in the login phase user have to follow same sequence as he done in registration phase.

Password Procedure

In the proposed work there is freedom for user to select his password in virtual environment. But these actions should have some meaning, for example if a user simply clicks the roof and floor then it has no meaning because this action can be recorded by any intruder by random clicking on image. The virtual environment consists of many kinds of actions and the range of state change. For example, user' s password consists of actions of closing and opening of window, making a sequence of objects for making the password more complex. But this type of sequence must require the recall power of user. The above procedure is easy to perform and changeable but it may be difficult for some users to recall.

Designing the Virtual Environment

In the proposed work there is freedom for user to select his password in virtual environment. But these actions should have some meaning, for example if a user simply clicks the roof and floor then it has no meaning because this action can be recorded by any intruder by random clicking on image. The virtual environment consists of many kinds of actions and the range of state change. For example, user' s password consists of actions of closing and opening of window, making a sequence of objects for making the password more complex. But this type of sequence must require the recall power of user. The above procedure is easy to perform and changeable but it may be difficult for some users to recall.

Designing the Virtual Environment

As discussed above that user can develop the virtual environment of his / her own choice or he can use the environment already exists. But there are some factors which should be considered.

- There should not be a large number of objects in the environment because they can confuse the user. Limited number of object helps the user to understand the environment.
- The developer should construct the environment such a way that the users uniquely identify the object. Their must not be two different object to solve the same purpose.
- The environment should deploy the authenticated system and should not be in inappropriate manner like distracting objects etc.

Here are some examples of virtual environment. (Figure 2 : a, b, c).

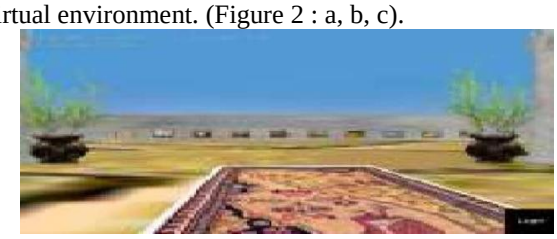

Figure: 2a

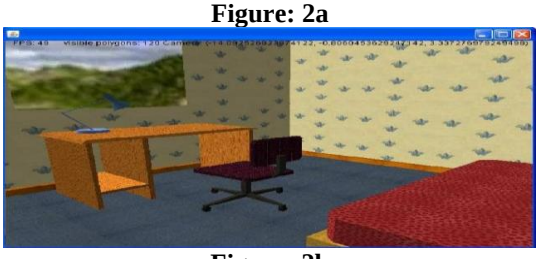

Figure: 2b

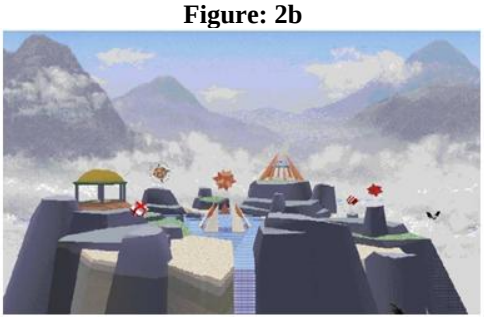

Figure: 2c

Examples of virtual environment

IV. Analysis and Results

As mentioned above that for our analysis we have taken the virtual environment of a game published by a social network site. Figure 3a shows the registration process in which user decorates his / her military according to mind state. Figure shows the arrangement of tanks, soldiers and artillery in the registration process. Figure 3b shows the login process in which user recall the process of registration and move the object to the desired state. If user correctly recall the changes of states and move the objects correctly in the same state as in registration process then he/she will be the legitimate user. Figure 3c shows the system after successful login.

Figure 3a: Registration phase

Figure 3b: Movement of objects

Figure 3c: Successful login after Recall.

V. Results

The successful authentication result generated by using false acceptance rate (FAR) and false rejection rate (FRR). For our analysis we have taken the group of 20 peoples who are using the same game on social network site. There are different numbers of objects to move and found following results.

Table 1 Performance of system (with respect to object moved)

OBJECT	3	5	7	9	10
FAR	1.53	0.82	0.51	0.52	0.55
FRR	2.47	3.51	2.31	3.17	5.66

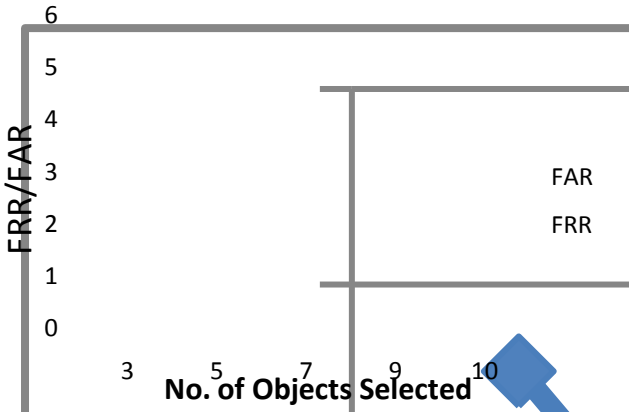

Figure 4: Graph Represent the FRR and FAR values with number of object moved.

Here we can see that the EER (Equal Error Rate) is 3.36 when 5 objects were moved. So we can state that the movement of 5 objects is sufficient to authenticate the legitimate user.

We performed another user study with same group of 20 peoples, with different graphical password techniques and the proposed techniques. The results are as follows.

Table 2 Different techniques accepting and rejection users in first attempt (20 users)

TECHNIQUES	ACCEPTED IN FIRST ATTEMPT	REJACTION
DRAW A SECRET	11	9
PASS FACSE	14	6
PASS POINT	17	3
PROPOSED TECHNIQUE	19	1

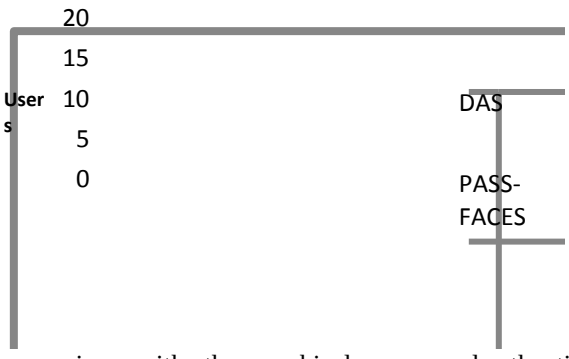

Figure 5: Graphical comparisons with other graphical password authentication techniques.

VI. Conclusion and Future Work

There are many authentication schemes have been developed by utilizing the users physical and mental behavioral attributes. The proposed scheme utilizing both attributes together. The previous schemes are vulnerable to certain attacks also may require additional time and effort to be applicable.

The proposed system solves all the issues related to the past algorithms by utilizing the recalling and recognition ability of human, keeping in mind the disadvantages of these algorithms. Hence this proposed system is user friendly, safe, secure and easy to use that can be applied to all fields. The system proposed by us has a drawback of shoulder surfing attack. A hacker could reveal the password so we suggested that the approach is performed in a secure environment. However, a attacker can see the password in login phase but it is easy in system to change the password and then it may be impossible for any intruder to recall it again and again. This could be a matter of future work.

References

[1] BBC News, Cash Machine Fraud up, Say Banks, Nov. 4, 2006.
[2] ATM fraud- Banking on your money - Dateline NBC - Consumer Alert http://www.msnbc.com
[3] S. Akula and V. Devisetty, "Image Based Registration and Authentication System," in *Proceedings of Midwest Instruction and Computing Symposium*, 2004.
[4] Handbook of Fingerprint Recognition by Davide Maltoni, Dario Maio, Anil K. Jain, Salil Prabhakar
[5] Regunathan Radhakrishnan, Nasir Memon - On The Security Of The Sari Image Authentication System 2002 Polytechnic University, Brooklyn
[6] D. Davis, F. Monrose, and M. K. Reiter, On user choice in graphical password schemes, in Proc. 13th USENIX Security Symp., San Diego, CA, Aug. 2004, pp. 1– 14.
[7] [G. E. Blonder, Graphical password, U.S. Patent 5 559 961, Sep. 24, 1996.
[8] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Basic results," in *Human-Computer Interaction International (HCII 2005)*. Las Vegas, NV, 2005.
[9] Berger, M.A.,(2003), " Password Security is a Must for Any Organisation, is a Must for Any Organisation, Computers in Libraries 23(5), May2003, p41.6-Coventry,L.,De Angeli, A. and Johnson, G.Usability and biometric verification at the ATM, A. and Johnson, G.Usabliltiy and biometric verification at the ATM interface.In Proceedings of the SIGCHI Conference in Human Factors in Computer System (CHI' 03) (Fort Lauderable FL. USA. April 5-10 2003). ACM Press, New York, Ny, 153-160
[10] Wiedenbeck, S., Waters, J., Birget, J.C., Broditskiy, A. and Memon, N. PassPoints: Design and evaluation of a graphical password system. Submitted, (2005).
[11] X. Suo, Y. Zhu, and G. S. Owen, Graphical passwords: A survey, in Proc. 21st Annu. Comput. Security Appl. Conf., Dec. 5– 9, 2005, pp. 463– 472.
[12] http://www.apps.facebook.com/empiresandallies