Securing the Data using Advance Authentication Technique

Ajaykumar Donta
Department of MCA
Lokmanya Tilak College of Engineering, KoparKhairne, University of Mumbai, India

Prof. Sudhakar Jadhav
Department of MCA
Lokmanya Tilak College of Engineering, KoparKhairne, University of Mumbai, India

Prathamesh Bhawtankar
Department of MCA
Lokmanya Tilak College of Engineering, KoparKhairne, University of Mumbai, India

Abstract

Providing Authentication to any computer means to provide more security to that computer. There are many authentication techniques, such as textual password, graphical password, etc. but each of this individually having some limitations & drawbacks and also these can be hacked or cracked by the various applications. To overcome the drawbacks of existing authentication technique, a new improved authentication technique is proposed called as 3D password. It is multi-password & multi-factor authentication system. It combines a various authentication techniques such as textual password, graphical password etc. In this paper we have introduced our contribution towards 3D Password to make it more secure & more user-friendly to users of all categories. This paper also explains: what is 3D password? Working of 3D password scheme. All these concepts are briefly introduced & explained in this paper section wise.

Keywords- 3D password, Virtual Environment, textual password, Authentication, Graphical Password

I. INTRODUCTION

Now a day's authentication is an important aspect about the security, so we cannot ignore the security related to the important data. We can secure our data in various ways like Knowledge based, Token based, Biometric based. Knowledge based[8] password can be further divided as Recall based and Recognition based. In Recall based technique, someone repeats secrets that are already created. Most common form of this type is Textual password. Textual password[6] usually consists of text, alphanumeric characters, and special characters etc. which are of short length. Such passwords can be easily hacked by hackers. Normally users use textual passwords, but they don't consider the security. They are select words of significance from dictionaries or like name and birthday combination, making then liable to dictionary or brute force attacks.[1]

Another concept for authentication is graphical password[7]. The concept behind graphical passwords is that users would find it easy to remember and identify pictures as compared to words. But, this faces a lot of problems. Some graphical passwords require a long time to be executed, and more importantly, they can easily be noted. Now-a-days as the technology has changed many fast processors and tools are available on internet it has become very easy to crack the authentication schemes. So in this paper, we have introduced 3D password a new authentication scheme. 3D password is multi password authentication scheme. The 3D password represents a 3D virtual environment containing various virtual objects. In virtual environment user navigates through this environment and interacts with the objects.

II. EXISTING SYSTEM

Current authentication systems have many problems. Textual passwords are commonly used. Users choose meaningful words from dictionaries, which make hackers easy to break. Many available graphical passwords have a password space that is less than or equal to the textual password space. Smart cards or tokens can be stolen. In biometric password there may be problem like eye scanning or finger print problem etc. The 3Dpassword is a multi-factor authentication scheme. The design of the 3D virtual environment and the type of objects selected determine the 3D password key space. User have free to select whether the 3D password will be recall based, recognition based, or token based, or combination of two schemes or more.

III. PROPOSED SYSTEM: 3D PASSWORD

3D password is combination of textual password, graphical password and biometrics. So that 3D password is multifactor & multi password authentication technique. The 3D password represents a 3D virtual environment containing various virtual objects like museum, game zone etc. The user navigates through this environment and interacts with the objects. The 3D password is simply

All rights reserved by *www.grdjournals.com*

the combination and the sequence of user interactions that occur in the 3D virtual environment. This can be done by designing a 3D virtual environment that contains objects that request information to be recalled, information to be recognized, tokens to be presented, and biometric data to be verified.

A. Objective of Proposed System

- To provide more secure authentication technique than existing one.
- To design & develop more user friendly & easier authentication scheme and giving user to freedom of selecting more than one password scheme as single system.
- To overcome the drawbacks & limitations of previously existing systems (textual password, graphical password. Etc.).
- New scheme should be combination of textual password, graphical password etc.

IV. 3D VIRTUAL ENVIRONMENT

For authentication using 3D password we need 3D virtual environment where user navigate and moves in 3D virtual environment to create a password which is based on navigation and moves in the virtual environment.

The order in which actions and interactions are performed with respect to the objects in the virtual environment creates the users 3D password. The 3D password key space is based on the basis of the design of the 3D virtual environment and the nature of the objects selected. The advantage of the 3D password is that it can combine many existing systems of authentication, providing an extremely high degree of security to the user.[2]

Figures below shows some snapshots of 3D Virtual Environment of different real time scenarios created in virtual environments. These virtual environments are interactive virtual environment as user can interact with these environments & creates his/her own 3D password easily.

All rights reserved by *www.grdjournals.com*

Fig. 1&2&3: snapshots of 3D Virtual Environments

V. SYSTEM OVERVIEW

The 3D password is a multifactor authentication scheme. The 3D password represents a 3D virtual environment containing various virtual objects. The user navigates through this environment and interacts with the objects. The 3D password is simply the combination and the sequence of user interactions that occur in the 3D virtual environment. The 3D password can combine textual password, graphical password and biometrics into one authentication scheme. This can be done by designing a 3D virtual environment that contains objects that request information to be recalled, information to be recognized, tokens to be presented, and biometric data to be verified.

For example, the user can enter the virtual environment and type something on a computer, then enter a room that has a fingerprint recognition device and provide his/her fingerprint.

Another example is that user can go to the virtual garage, open the car door, and turn on the radio to a specific channel. The combination and the sequence of the previous actions toward the specific objects create the user's 3D password. Virtual objects can be any object that is in real life. Any obvious actions and interactions toward the real life objects can be done in the virtual 3D environment toward the virtual objects. Moreover, any user input (such as speaking in a specific location) in the virtual 3D environment can be considered as a part of the 3D password:

VI. WORKING OF 3D PASSWORD SCHEME

Following is an example that shows how to create the 3d password using chess virtual environment. Consider that the user want to fill the registration form and store the password using 3D password authentication concept.

While before using the 3D password he/she must need to set the 3D password. Whenever the user clicks on the set 3D Password button he/she navigates into the chess virtual environment as shown in the following figure 4.

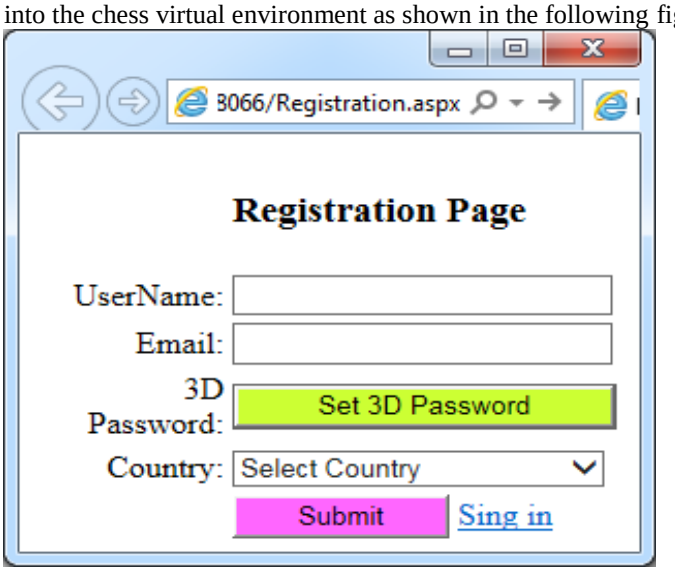

Fig. 4: Registration form

All rights reserved by *www.grdjournals.com*

Now the user is in the chess virtual environment. User is now able to set the 3D password while navigating into the virtual environment.

Following figure 5 shows an environment for a chess game, having a total of 32 pieces, out of which 16 are red and 16 are white. In this environment there are also have seven buttons all together namely, New button, Swap button, Record button, Stop button, Play button, Confirm button, Close button and one Checkbox option. Each button works as specified below:

A. New Button

By clicking this button initializes all the pieces (white and red). While to clicking this button, the environment is completely empty stage.

Fig. 5: Chess Environment

B. Swap Button

Swap button is used in order to change the position of the red and white pieces. It exchanges the positions of the white and red pieces respectively.

C. Record Button

Before creating the 3D password, the user must click this button, as a result of which the sequence of actions and interactions are stored as the 3D password as a string.

D. Stop Button

This button is used to end the sequence of actions and interactions. Clicking this button stops recording the user's movements and the recorded actions and interactions are saved as a 3D password in the form of a string.

E. Play Button

This button is used by user to check the actions and interactions that have been performed after pressing the stop button. Once this button is clicked, the user can see a playback of the actions and interactions which have been stored as a 3D password.

F. Confirm Button

This button confirms the 3D password. Once this button is clicked, the user cannot change the 3D password.

G. Close Button

While clicking this button, the environment is closed and control returns to the registration form.

VII. APPLICATIONS OF 3D PASSWORD

Because a 3-D password can have a password space that is very large compared to other authentication schemes, the 3-D password's main application domains are protecting critical systems and resources. Possible applications include the following:

– Critical servers: Many large organizations have critical servers that are usually protected by a textual password. A 3-D password authentication proposes a sound re-placement for a textual password. Moreover, entrances to such locations are usually protected by access cards and sometimes PIN numbers. Therefore, a 3-D password can be used to protect the entrance to such locations and protect the usage of such servers.

All rights reserved by *www.grdjournals.com*

- Nuclear and military facilities: Such facilities should be protected by the most powerful authentication systems. Space, and since it can contain token-, biometrics-, recognition-, and knowledge-based authentications in a single authentication system, it is a sound choice for high-level security locations.
- Airplanes and jetfighters: Because of the possible threat of misusing airplanes and jetfighters for political agendas, usage of such airplanes should be protected by a powerful authentication system. The 3-D password is recommended for these systems.

In addition, 3-D passwords can be used in less critical systems because the 3-D virtual environment can be designed to fit any system's needs. A small 3-D virtual environment can be used in many systems, including the following: [3][4][5]

1) ATMs;
2) Personal digital assistants;
3) Desktop computers and laptop logins;
4) Web authentication

VIII. CONCLUSION

There are many authentication techniques available such as Textual Passwords, Graphical Passwords, Biometric Identification, etc. but each of these, individually having some drawbacks. In this paper we overcome these limitations using the 3D Password scheme.3D password is an advance authentication technique through this we can secure our important data without worry about the hikers. The main purpose of this paper is to shown that how to set the 3D password and to secure our data. This paper presented 3D Virtual Environment of Chess which showed that the number of possible 3D Passwords making it difficult for a hacker to break it. Thus this paper tells about our study on 3D password and how to construct 3d password.

ACKNOWLEDGMENT

We would like to thank our lecturers, Prof. Sudhakar Jadhav for their support in preparing this paper.

REFERENCES

[1] D. V. Klein, ―Foiling the cracker: A survey of, and to passwords security,‖ in Proc. USENIX Security, pp.–14
[2] Fawaz A. Alsulaiman and Abdulmotaleb El Saddik, "Three-Dimensional Password for More Secure Authentication", IEEE TRANSACTIONS ON INSTRUMENTATION AND MEASUREMENT, VOL. 57, NO. 9, SEPTEMBER 2008
[3] Vishal Kolhe, Vipul Gunjal, Sayali Kalasakar, Pranjal Rathod,"Secure Authentication with 3D Password ",International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 2, March 2013
[4] Fawaz A. Alsulaiman and Abdulmotaleb El Saddik, "A Novel 3D Graphical Password Schema‖, IEEE International Conference on Virtual Environments, Human-Computer Interfaces, and Measurement Systems, July 2006.
[5] Ms. Vidya Mhaske-Dhamdhere, Prof. G. A. Patil," Three Dimensional Object Used for Data Security",2010 International Conference on Computational Intelligence and Communication Networks © 2010, IEEE.
[6] Banita Chadha, Dr. Puneet Goswami, "3d Password –A Secure Tool", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 1, January 2014
[7] Shraddha M. Gurav, Leena S. Gawade, Prathamey K. Rane, Nilesh R. Khochare, "Graphical Password Authentication" 2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies © 2014 IEEE
[8] Ms. Vidya Mhaske-Dhamdhere, Bhakti Pawar, Pallavi Ghodke, Pratibha Yadav, "3-D Graphical Password Used For Authentication", Vidya Mhaske et al ,Int.J.Computer Technology & Applications,Vol 3 (2), 510-519

All rights reserved by *www.grdjournals.com*