International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 6 632 – 635

Advance Authentication Technique: 3D Password

Pooja M. Shelke
PGDCST, HVMP, Amravati

F. M. Shelke
PRPCEM, Amravati

Mr. B. G. Pund
PGDCST, HVPM, Amravati

Abstract-Providing more security to any system requires providing any authentication strategy to that system. There are many authentication strategies, such as textual password, graphical password, etc.
But these techniques have some limitation and drawback like they can easily hacked or cracked by using various tools. One of the tools is brute-force algorithm. So, to overcome the drawbacks of existing authentication technique, a new improved authentication strategy is proposed. This strategy is multi-password and multi-factor authentication system as it combines a various authentication techniques such as textual password, graphical password etc. Most important part of 3d password scheme is inclusion of 3d virtual environment. This authentication Strategy is more advanced than any other schemes as we can combine existing schemes. Also this Strategy is tough to break & easy to use. This paper introduced contribution towards 3D Password to make it more secure & more user-friendly to users of all categories.

Keywords: *3D password, Virtual Environment, Authentication, textual password, graphical password*

*****

I. INTRODUCTION

Authentication can be categorized as[2][4] Knowledge based (what you know), Token based (what you have), Biometric based (what you are). Knowledge based password can be further divided as [9] Recall based and Recognition based. In Recall based technique, one repeats some secret that is already created. Most common form of this type is Textual password. Textual password [7] usually consists of text, alphanumeric characters, etc. which are of short length. Such passwords can be easily hacked by means of Keystroke recording, brute force attack, Phishing, etc.
Users commonly use textual passwords, but do not take their security into account. They are select words of significance from dictionaries, making then liable to dictionary or brute force attacks. [1]
Another concept for authentication is graphical password [8]. The principle behind graphical passwords is that users would find it easy to remember and identify pictures as compared to words. But, this faces a number of complications. 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 multifactor & multi password authentication scheme. The 3D password presents a 3D virtual environment containing various virtual objects. The user navigates through this environment and interacts with the objects.

II. EXISTING SYSTEM

Current authentication systems suffer from many weaknesses. Textual passwords are commonly used. Users choose meaningful words from dictionaries, which make textual passwords easy to break and vulnerable to dictionary or brute force attacks. 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. Many biometric authentications have been proposed. However, users tend to resist using biometrics because of their intrusiveness and the effect on their privacy. Moreover, biometrics cannot be revoked. 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 freedom to select whether the 3D password will be solely recall, recognition, or token based, or combination of two schemes or more.

III. PROPOSED SYSTEM: 3D PASSWORD

3D password is combination of both recall-based (i.e. textual password) & recognition based (i.e. graphical password, biometrics). So that 3D password is multifactor & multi password authentication scheme. The 3D password is a multifactor authentication scheme. The 3D password presents 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 recognition, recall, token, and biometrics based systems 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.

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 recall-, recognition -based authentication schemes.

IV. 3D VIRTUAL ENVIRONMENT

For authentication with 3D password a new virtual environment is introduced called as 3D virtual environment

where user navigate, moves in 3D virtual environment to create a password which is based on both the schemes.
The order in which actions and interactions are performed with respect to the objects constitutes the users 3D password. The 3D password key space is built 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.

Fig. snapshots of 3D Virtual Environments

V. SYSTEM OVERVIEW

The 3D password is a multifactor authentication scheme. The 3D password presents 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 recognition, recall, token, and biometrics based systems 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 that exists in (x1, y1, z1) position, then enter a room that has a fingerprint recognition device that exists in a position (x2 , y2 , z2) and provide his/her fingerprint. Then, the 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 construct the user's 3D password. Virtual objects can be any object that we encounter 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. We can have the following objects:

1. A computer with which the user can type.
2. A paper or a white board that a user can write on.
3. An ATM machine that requires a smart card and PIN.
4. A light that can be switched on/off.
5. A television or radio where channels can be selected.
6. A car that can be driven.
8. A chair that can be moved from one place to another.
9. Any graphical password scheme

I. WORKING OF 3D PASSWORD SCHEME:

Following is an example that shows how to create the 3d password using chess virtual environment. In this, the password is created based on the position of the chess pieces on the chess board and also whether the white pieces are towards the user or the black ones i.e. the position of the chessboard. Figure A shows the 3D design of chess, which consists of 16 white objects and 16 black objects having a total of 32 objects. There are 3 buttons provided viz. Help, Reset and Submit. The pieces are moves forward and backward using the mouse.
The **Help button** on click will pop up the instructions to be followed while creating the password.
The **Reset button** will place the pieces back to the original position.
The **submit button** will create the password and this password will be stored in the database. Each square of the chessboard is given a position (example: [1, a], [2, b]) so that the user can remember the password with ease.

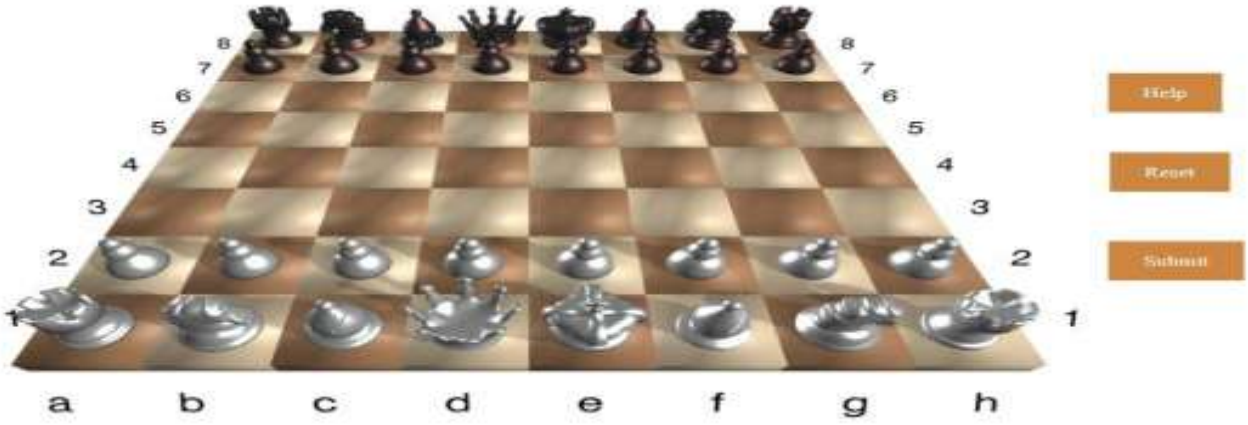

Fig. A: chess 3d virtual environment

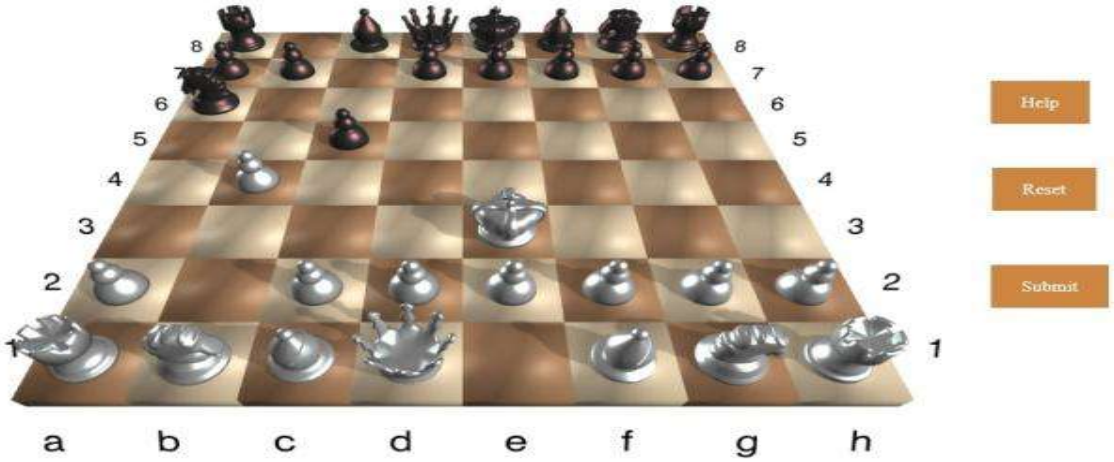

Fig. B: 3d Password creation

When the user enters into this environment, the user is free to place the pieces at any position on the chess board. One can even delete the pieces by simply dragging and dropping it out of the chessboard. The user has to memorize only the pieces moved and their position onto the chessboard. Figure B shows an example of creating the 3D Password in the virtual environment.

The function fen() gives the overall status of the chessboard. It stores the position of the pieces in the form a string. Whenever a chess piece is moved, its new position is recorded and changes are made to the string accordingly. For example, when the pieces are at their original position (refer fig. A), the string is rnbqkbnr/pppppppp/8/8/8/8/PPPPPPPP/RNBQKBNR where the letters indicate the type of chess piece may be „p" for pawn, „q" for queen and so on. Capital letters indicate the white pieces and small letters indicate the black pieces. The number 8 indicates that, the row is empty. When the chess pieces are moved (refer fig. B), the string will be modified as, r1bqkbnr/pp1ppppp/n7/2p5/1P6/4K3/PPPPPPPP/RNBQ1BNR . To make this environment user friendly, the chess board has been assigned positions which the user can memorize easily as compared to memorizing the string. This string is then stored into the database.

VI. 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 replacement 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.

- 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: [4][5][6]

1) ATMs;

2) Personal digital assistants;

3) Desktop computers and laptop logins;

4) Web authentication

VII. 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 a multifactor authentication scheme which combines existing authentication techniques into 3D Virtual Environment. This environment contains various virtual objects. The user navigates through this environment and interacts with the objects. The combination and sequence of the user interactions in the environment forms the 3D Password. This paper presented 3D Virtual Environment of Chess which showed that the number of possible 3D Passwords almost tends to infinity making it difficult for a hacker to break it. Thus this paper tells about our study about 3D password and how to construct 3d password.

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] A.B.Gadicha , V.B.Gadicha , ―Virtual Realization using 3D Password‖, in International Journal of Electronics and Computer Science Engineering, ISSN 2277-1956/V1N2-216-222

[4] Vishal Kolhe, Vipul Gunjal, SayaliKalasakar, PranjalRathod,"Secure Authentication with 3D Password ",International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 2, March 2013

[5] 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.

[6] Ms. VidyaMhaske-Dhamdhere, Prof. G. A. Patil," Three Dimensional Object Used for Data Security",2010 International Conference on Computational Intelligence and Communication Networks © 2010, IEEE.

[7] Banita Chadha, Dr. PuneetGoswami, "3d Password –A Secure Tool", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 1, January 2014

[8] 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

[9] Ms. VidyaMhaske-Dhamdhere, Bhakti Pawar, PallaviGhodke, Pratibha Yadav, "3-D Graphical Password Used For Authentication", Vidya Mhaske et al ,Int.J.Computer Technology & Applications,Vol 3 (2), 510-519