Journal of Advances in Science and Technology
Vol. 12, Issue No. 25, (Special Issue) December-2016, ISSN 2230-9659

3D Password for Secure Authentication

Prof. Ashwini Gavali[1]*, Suhasini H.[2], Shilpa R. N.[3]

[1]Asst. Prof., CSE Dept., KLECET, Chikodi

[2]Students, KLE College of Engineering and Technology, Chikodi, Distt.-Belagavi State-Karnataka, India

[3]Students, KLE College of Engineering and Technology, Chikodi, Distt.-Belagavi State-Karnataka, India

Abstract – Providing Authentication to any system leads to provide more security to that system. There are many authentication technique available, Such as textual password, Graphical password, etc. but each of this individually have some limitations & drawbacks. To overcome the drawbacks of previously existing authentication technique, a new improved authentication technique is used. This authentication scheme is called as 3D password. The 3D password is multi-password & multi-factor authentication system as it uses a various authentication techniques such as textual password, graphical password etc. Most important part of 3D password scheme is inclusion of 3D virtual environment. 3D virtual environment is an environment which is consisting of real time object scenarios. It is not actual real time environment, it is just user interface provided to scheme which looks like same as real environment. 3D password is more secured authentication scheme than any other authentication techniques. Because this authentication scheme is more advanced than any other schemes. Also this scheme is hard to break & easy to use. In this paper, we have introduced our contribution towards 3D Password to become more secure & more user friendly to users of all categories. This paper also explains about what is 3D password?, working of 3D password scheme, some mathematical concept related to 3D password, applications of scheme etc. all these concepts are briefly introduced & explained in this paper as per section wise.

----------♦----------

I. INTRODUCTION

Authentication is one of the most important security service provided to system by the different authentication schemes or algorithms. To protect any system, authentication must be provided, so that only authorized persons can have right to use or handle that system & data related to that system securely. There are many authentication algorithms available some are effective & secured but having some drawbacks. Previously there were many authentication techniques introduced such as graphical password, text password, biometric authentication, etc. generally there are four types of authentication techniques are available such as:

1. **Knowledge based:** means what you know. Textual password is the best example of this authentication scheme.

2. **Token based:** means what you have. This includes Credit cards, ATM cards, etc as an example.

3. **Biometrics:** means what you are. Includes Thumb impression, etc.

4. **Recognition Based:** means what you recognize. Includes graphical password, iris recognition, face recognition, etc.

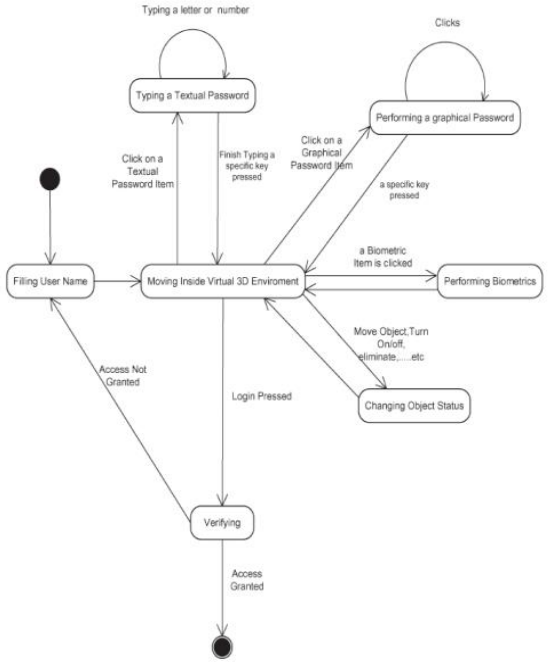
II. OBJECTIVE OF PROPOSED SYSTEM

- To provide more secured 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 -, biometrics-, and token based authentication scheme.

III. WORKING OF 3D PASSWORD SCHEME

In 3D password user have to first authenticate with simple textual password (i.e. user need to provide user name & password). Once authentication is

successful, then user moves in 3D virtual environment. Thereafter, a computer with keyboard will be seen on screen. On that screen user have to enter password (textual) which is stored in a simple text file in the form of encrypted co-ordinates. After successfully completion of this authentication, then user automatically enters into an art gallery, where he/she has to select multiple point in that gallery or he can do some action in that environment like switching button on/off or perform action associated with any object like opening door, etc.



The sequence in which user has clicked (i.e. selecting objects) that sequence of points are stored in text file in the encrypted form. In this way the password is set for that particular user. For selection of points we have used 3D Quick Hull algorithm which is based on Convex Hull algorithm from design & analysis of algorithms. Next time when user want to access his account then he has to select all the object which he has selected at the time of creating password .This sequence is then compared with coordinates which are stored in file. If authentication successful, thereafter access is given to authorized user. 3D password working algorithm is shown in which will give the flowchart for 3D password creation & authentication process.

Advantages

1. 3D Password scheme is combination of re-call based, recognized based, Biometrics .etc authentication technique.

2. Due to use of multiple schemes into one scheme password space is increased to great extend.

3. More secure authentication scheme over currently available schemes.

Disadvantages

1. Time and memory requirement is large Shoulder-suffering attack is still can affect the schema.

2. More expensive as cost required is more than other schemes.

Applications

As 3D password authentication scheme is more useful & more secure than any other authentication schemes, 3D password can be used in wide area where more security is needed to system. Some of areas are as follows:

1. **Networking**: Networking involves many areas of computer networks like client-server architecture, critical servers, etc. To provide more security to server of this architecture 3D password can be used. It very efficient & more secure way to keep data or important information secure from unauthorized people. For email applications 3D password is most secure & easier scheme to used.

2. **Nuclear & military area:** Nuclear & military area of a country are most important area where more security is needed we can use 3D password scheme in this area for more providing more secure authentication. 3D password scheme can protect data or secrete information about these areas very securely.

3. **Airplane & jetfighters:** there is possibility of misuse of airplanes and jetfighters for religion-political agendas. 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.

4. **Other areas:** we can use 3d password authentication scheme to areas such as ATM, Cyber cafes, Industries (for data security), Laptop‘s or PC‘s, critical servers, web services, etc & many more.

CONCLUSION

Currently available schemes include textual password and graphical password .But both are vulnerable to certain attacks. Moreover, there are many

authentication schemes that are currently under study and they may require additional time and effort to be applicable for commercial use.

The 3-D password is a multifactor & multi password authentication scheme that combines these various authentication schemes. The virtual environment can contain any existing authentication scheme or even any upcoming authentication schemes. Due to which passwords space increases. It is the user‘s choice and decision to construct the desired and preferred 3-D password. The 3D password is still new & in its early stages.

Designing various kinds of 3-D virtual environments, deciding on password spaces, and interpreting user feedback and experiences from such environments will result in enhancing and improving the user experience of the 3-D password. Gathering attackers from different background and attack made by them and how to overcome them is main future work. Shoulder surfing attacks are still possible so how to overcome that is a field of research & development. Inclusion of biometrics leads to increasing cost & hardware in scheme, to reduce additional time and effort to be applicable for commercial use in scheme, to reduce this is still field of research. So that 3D password can be used in many application areas as discussed earlier & also many more area other than those. Thus this paper tells about our study about 3D password, still it is in early stage.

REFERENCES

Alsulaiman, F.A.; El Saddik, A. (2008). "Three- for Secure," IEEE Transactions on Instrumentation and measurement, vol.57, no.9, pp 1929-1938.

Vidya Mhaske etal, Int.J.Computer Technology & Applications, Vol 3 (2), ISSN: 2229-6093, pp. 510-519.

Tejal Kognule and Yugandhara Thumbre and Snehal Kognule (2012). 3D passwordǁ, International Journal of Computer Applications (IJCA).

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

Fawaz A. Alsulaiman and Abdulmotaleb El Saddik (2006). “A Novel 3D Graphical Password Schemaǁ, IEEE International Conference on Virtual Environments, Human-Computer Interfaces, and Measurement Systems.

Duhan Pooja, Gupta Shilpi, Sangwan Sujata, & Gulati Vinita (2012). SECURED Authentication: 3D Passwordǁ, I.J.E.M.S., VOL.3(2), pp. 242 – 245.

Corresponding Author

Prof. Ashwini Gavali*

Asst. Prof., CSE Dept., KLECET, Chikodi

E-Mail – ashwini_gavali@yahoo.com