A Survey in Shoulder Surfing Attack in 3D Password

Vaishali Jain[1], Akhil Dubey[1], Banita Chadha[2]
[1]M.Tech. Scholars, Dept. of Computer Science & Engg.
[2]Associate Professor, Dept. of Computer Science & Engg.
IEC-College of Engineering & Technology
Greater Noida, U.P., INDIA

***Abstract*— Security is the key factor which is achieved by means of authentication in this computer era. Authentication is the act of establishing or conforming something, as authentic, the claims made by or about the things are true. There are many authentication schemes such as textual password or graphical password. But each of these has some limitations and drawbacks. To overcome the drawbacks of previously existing authentication schemes, a new 3D password scheme is used. It is a multi -factor and multi- password authentication scheme that combine recognition, recall, tokens and biometric in one authentication system. The system of authentication presents a 3D virtual environment to the user where in the user navigates and interacts with the objects. 3D password is constructed by observing the actions and interactions by the users and by observing the sequence of such actions. It is flexible and provides unlimited passwords possibility but it is vulnerable to shoulder surfing attack which is using direct observation techniques such as looking over someone's shoulder to get passwords, pin no. and other sensitive personal information. A malicious observer may be able to acquire the user's password credentials when he enters information using hand held input devices. In this paper we have explained about 3D password scheme and its working. We also describe shoulder surfing attack in this scheme and then we presenting the convex hull click scheme as countermeasure of shoulder surfing attack in 3D password scheme.**

Keywords*— *Authentication, Textual password, Graphical password, 3D password, Shoulder surfing Attack, Convex Hull Click

I. Introduction

Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. In order to protect any system, authentication must be provided, so that only authorized users can have right to use or alter the data related to that system securely. There are four types of authentication techniques which are commonly used and shown in the fig below:

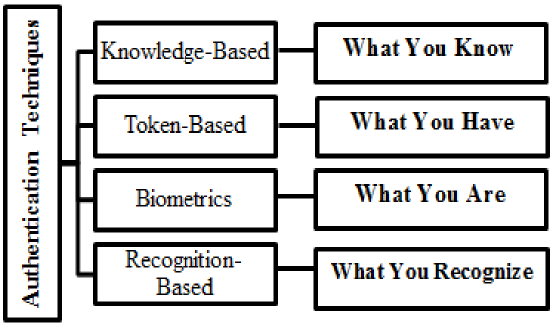

Figure.1. Authentication Techniques

Recall-Based: Recall-Based techniques require the user to repeat or reproduce a secret that the user created before [6]. Knowledge-based authentication is a part of this technique, e.g. Textual Password, Graphical Password etc. this technique is commonly used all over the world where security needed [1].

Recognition-Based: In this authentication technique, the user requires to identify and recognize the secret, or part of it, that it has selected before .Recognition based authentication can be used in graphical password.

When both recall and recognition based techniques are used separately or used as single authentication scheme, then both techniques have some vulnerabilities. To overcome the vulnerability of existing system, we introduce a new authentication scheme called 3D password, which is based on combination of recall and recognition based authentication techniques as well as biometric and many other schemes. All these schemes are implemented in virtual environment while creating 3D password, where this environment contains various virtual objects through which user interacts with. The interaction with 3D environment changes as per user changes. 3D password is constructed by observing the sequence of such actions [1] [6] [7].

II. 3D PASSWORD

3D Password is a multifactor and multi-password scheme as it uses the combination of both recall-based (textual password) and recognition-based (graphical password, biometric etc.). The concept of 3D password promotes development, diplomacy and defense in security strategies [5]. 3D password scheme combines the benefit of different authentication scheme in single virtual environment. By this user will have the choice to select whether this password will be only recall, biometrics, token or recognition based, or a combination of two or more schemes [5]? The ease which 3D password provides is the user can make infinite number of 3D password by combining any two or more different schemes. Giving the user the freedom of selection as to what type of authentication schemes will be included in their 3D password and given the large number of objects and items in the virtual environment, the number of possible 3D passwords will increase. Then it becomes much more difficult for the attacker to gain the user's 3D password.

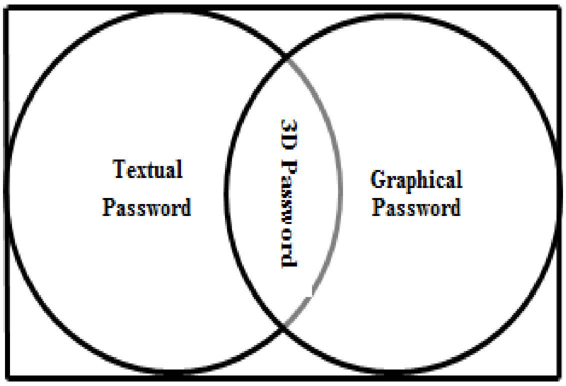

Figure.2 3D Password (Multifactor and Multi-Password Authentication Scheme)

A. Requirements of 3D Password Scheme

1) The new scheme should not be either recall based or recognition based only. Instead, the scheme should be a combination of recall, recognition, biometrics and token-based authentication schemes.
2) Users ought to have the freedom to select whether the 3D password will be solely recall, biometrics, recognition or token based or a combination of two schemes or more.
3) The new scheme should provide secrets that are easy to remember and very difficult for intruders to guess.
4) The new scheme should provide secrets that are easy to remember and very difficult for intruders to guess.
5) The new scheme should provide secrets that are not easy to write down on paper.
6) The new scheme secrets should be difficult to share with others.
7) The new scheme should provide secrets that can be easily revoked or changed.

B. Architectural Study

As 3D password is a multifactor and multi-password scheme which combines many password schemes like Textual password, Graphical password, biometric etc. Choosing of different schemes is solely depend on the system requirements. Figure 3 shows state diagram of 3D password creation.

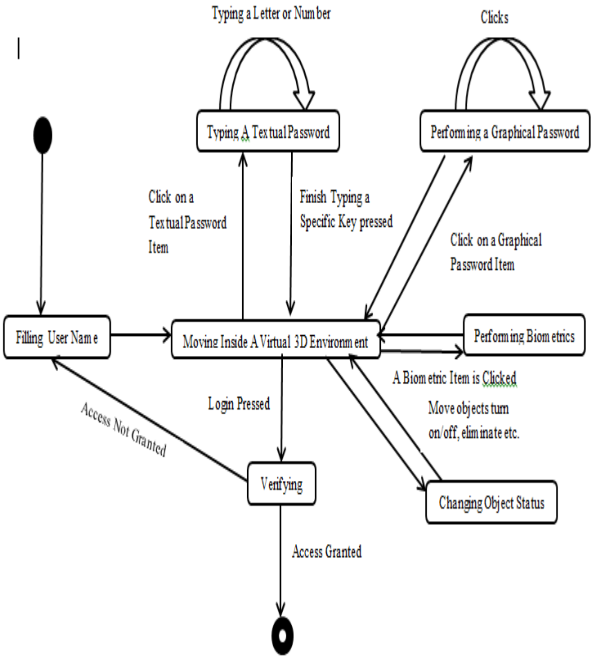
Typing a Letter or Number
Clicks
Typing A Textual Password
Performing a Graphical Password
Click on a Textual Password Item
Finish Typing a Specific Key pressed
Click on a Graphical Password Item
Filling User Name
Moving Inside A Virtual 3D Environment
Performing Biometrics
A Biometric Item is Clicked
Move objects turn on/off, eliminate etc.
Login Pressed
Access Not Granted
Verifying
Changing Object Status
Access Granted

Figure. 3 State Diagram of Creating 3D Password[1] [5] [6] [8] [9]

C. 3D Password System Design

3D password is a multifactor scheme. Multifactor means it uses the combination of all existing authentication schemes in one scheme, different schemes as textual password, graphical password or biometrics. Here we use only combination of textual and graphical password schemes. We don't use biometric scheme because the hardware cost is more and it is vulnerable to many attacks and moreover, inclusion of biometric may leads to increasing the cost of scheme as more hardware parts are needed.

For accessing the system the user must follow the following steps:

- Registration

While constructing the 3D password first the user registers himself by filling all fields they are, full name field contains the name of user who wish to register, address field contains the full address of user, State field contains State of user, city field contains the city of user, telephone number field store the personal telephone number of user, mobile number, email id provided into the email field, user name contains in user field and password is selected in password field. [4] After filling all the details, user will click on the next button where the user will enter in a virtual environment consists of number of pass-icons. In this virtual environment, the user will choose its graphical password using convex hull click algorithm.

- Authentication

For authentication, first user login to the system using his/her user name and textual password. If he succeed in login then he is presented with the virtual environment which consists of number of pass icons, if the user creates the same graphical password which he has stored using convex hull click algorithm then he will succeed in login, and user will declared as authentic, else user will not be able to login into the system.

D. System Flow

Figure.4 shows the flow of the 3D password system working. This working shows that how the access will be granted to the user in 3D password system. If the user is not legitimate then it can't access the system.

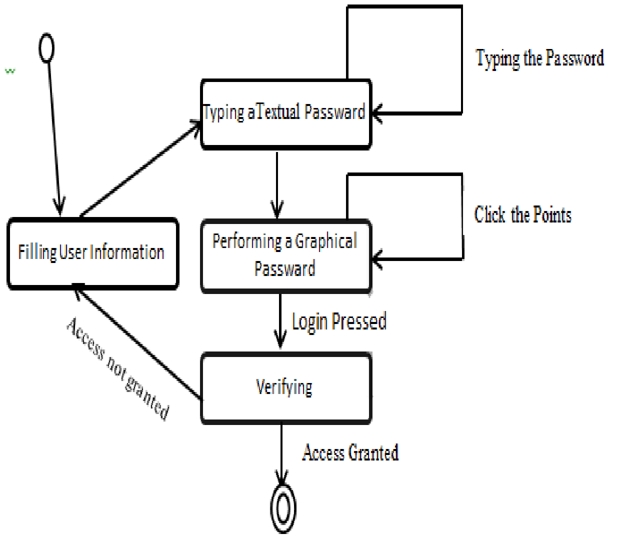

Figure.4 Flow of the System

III. Shoulder Surfing Attack in 3D Password

In shoulder surfing attack, an attacker uses a camera to record the user's 3D password or tries to watch the legitimate user while the 3D password is being performed [1] [6]. Shoulder surfing is using direct observation techniques, such as looking over someone's shoulder, to get information. Shoulder surfing is an effective way to get information in crowded place because it is relatively easy to stand next to someone and watch as they fill out a form, enter a pin number at an ATM machine etc. It can also be done long distance with the aid of binoculars or other vision-enhancing devices. This attack is the most successful type of attack against 3D password and some other graphical password. To make 3D password much more secure and non-vulnerable to shoulder surfing attack, convex hull click point can be used which is a defense mechanism of shoulder surfing attack.

A. Convex Hull Click Point Scheme

Our shoulder surfing resistant scheme, the Convex Hull Click Point scheme (CHC) is a graphical password scheme that guards against shoulder surfing attack. CHC is another multiple round challenge response authentication scheme proposed to lead off shoulder surfing [6]. The system uses a large portfolio consisting of several hundred icons. The icons are displayed using only the image without text. Figure 5 shows a virtual environment which consists of number of icons.

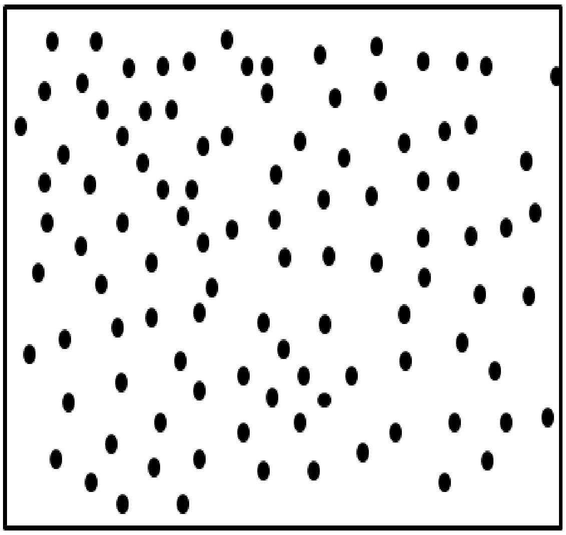

Figure.5 Virtual Environment

To create a password first user creates a convex hull consisting of number of number of points which surrounds many icons in it. Figure 6 shows the convex hull created by the user.

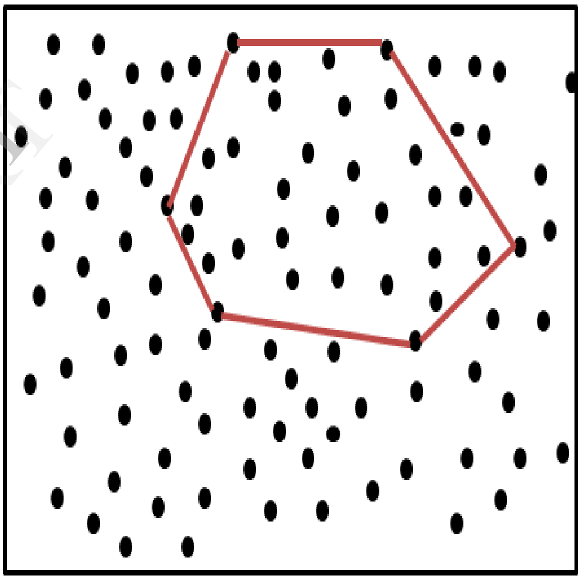

Figure. 6 Convex Hull Created by User

After creating the hull user will click on the pass icons that are inside the hull. The clicks which user pressed inside hull will form the password of user. Figure 7 how user will click inside the hull and form its password. In the figure clicks denotes the icon pressed by user to form its password.

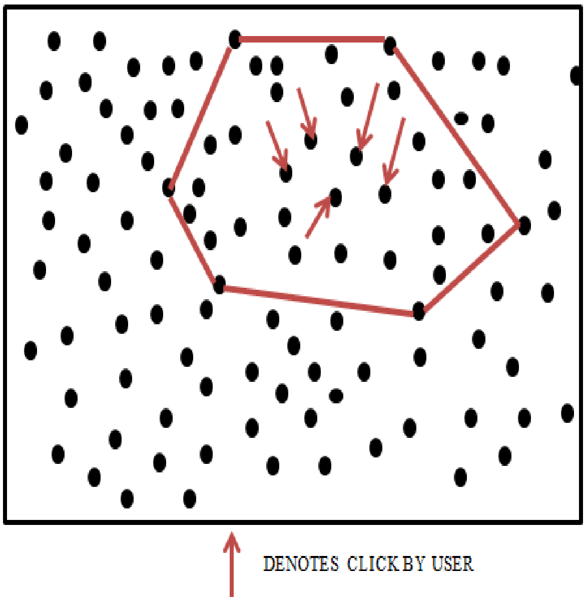

Figure.7 Graphical Password Created by User

The next time the user login to the system it is not necessary the hull which user created will appear in the same location, the location of hull is randomly changes as per login. This makes attacker to locate the location of hull and thereby identify the password.

- Advantages Offered by CHC

a) A Shoulder Surfing resistant scheme.
b) It is more secure, as password space can be made very large by increasing the number of icons or number of pass icons or both.
c) This is infeasible to brute force attack.
d) It avoids accidental login in authentication phase.

IV. Conclusion and Future Work

3D password is a multifactor and multi-password authentication scheme that combines recall based and recognition based scheme. The virtual environment can contain any existing authentication scheme or even any upcoming authentication scheme, due to which password space increases. In this paper we see, to make 3D password authentication scheme more secure and non-vulnerable to shoulder surfing attack Convex Hull Click Point scheme (CHC) can be implemented which offers several advantages other than non-resistant to shoulder surfing attack. CHC algorithm can be implemented while selecting graphical password. In our observation if we implement CHC algorithm in 3D password authentication scheme, then this scheme will provide better results while choosing graphical password. As a future work we should be targeted on increasing the speed of the input of passwords.

References

[1] Vishal Kolhe, Vipul Gunjal, Sayali Kalasakar, Pranjal Rathod, " Secure Authentication with 3D Password", International Journal of Engineering Science and Innovtive Technology(IJESIT), Volume 2, Issue 2, March 2013.

[2] Mr.Jaywant N. Khedkar, Ms.Pragati P. Katalkar, Ms.Shalini V. Pathak, Mrs.Rohini V.Agawane, "Integration of Sound Signature in 3D PasswordAuthentication System",International Journal of Innovative Research in Computer and Communication Engineering,Vol. 1, Issue 2, April 2013.

[3] A Aswathy Nair, Theresa Rani Joseph, Jenny Maria Johny," A Proficient Multilevel Graphical Authentication System", Interanational Journal of Science, Engineering, and Technology Research (IJSETR), Volume 2, No 6, June 2013.

[4] R.N.Muneshwar, S.K.Sonkar, "Virtual Environments Provide Mammoth Security for Critical Server", International Journal of Engineering and Advanced Technology (IJEAT), Volume-2, Issue-3, February 2013.

[5] Shubham Bhardwaj, Varun Gandhi, Varsha Yadav, Lalit Poddar, "New Era of Authentication: 3-D Password", International Journal of Science, Engineering and Technology Research (IJSETR), Volume-1, Issue-5, November 2012.

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

[7] Grover Aman, Narang Winnie,"4-D Password: Strengthening the Authentication Scene", International Journal of Scientific & Engineering Research, Volume 3, Issue 10, October-2012.

[8] Mr. Namdev A. Anwat,Mr. Dattatray S. Shingate,Dr. Varsha H. Patil, "A Secure Authentication Mechanism using 3D Password", International Journal of Advance Research in Science, Engineering and Technology, Vol.01, Issue 01, pp. 29-37.

[9] Fawaz A. Alsulaiman ,Abdulmotaleb El Saddik,"Three Dimensional Password for More Secure Authentication", IEEE Transactions on Instrumentation and Measurement, Vol. 57, No. 9, September 2008.

[10] Harshil Shah, Chirag Lakhani, Sagar Haldankar,"Graphical Password Authentication Based on Polygon Visualization",International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622.