ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 1, Issue 5, November 2012

New Era of authentication: 3-D Password

Shubham Bhardwaj, Varun Gandhi, Varsha Yadav, Lalit Poddar

***Abstract* — Current authentication systems suffer from many weaknesses. Textual passwords are commonly used. Users tend to choose common words from dictionaries and day to day life, which make textual passwords easy to crack and exposed to dictionary or basic force attacks. Smart cards or tokens can be stolen. Many biometric authentications have been proposed but some people hate the fact to carry around their cards, some refuse to undergo strong IR exposure to their retinas. The 3-D password is a multifactor authentication scheme. Mainly the 3-D passwords are the combination of physical and biometric authentication. The sequence of actions and interfaces toward the objects inside the 3-D environment constructs the user's 3-D password. The 3-D password can combine most existing authentication schemes such as textual passwords, graphical passwords, and various types of biometrics into a 3-D virtual environment. The design of the 3-D virtual environment and the type of objects selected conclude the 3-D password key space.**

***Keywords* — 3-D password, authentication, biometric, virtual environment**

I. INTRODUCTION

Normally the authentication scheme the user experiences are particularly very easy or very difficult. Throughout the years authentication has been a very exciting approach. Having a lot of technologies around, it can be very easy for 'others' to steal identity or to hack user's password. Therefore many procedures have come up for the calculation of a secret key to secure user's password. The algorithms or procedures are based on approach to pick a random number in the range of 10^6 and then the risks of the same number coming is rare.

User mostly uses textual passwords, graphical passwords or the biometrics to secure their things or works nowadays. The above tactic is mainly used in textual algorithm. But most of the people uses their day to day used name or number such as their pet name or their phone numbers or their date of birth as their passwords which are easily detectable by a hacker.

Smart cards are also used for authentication but they also fails and these tokens or smart card can be stolen. Many biometric authentications have been introduced but most of the users are not willing to biometrics due to their inappropriateness and the effect on their privacy. So these biometrics cannot be implemented everywhere.[3]

Therefore the idea of 3-D password is come up. This is easily customizable and very interesting way of authentication than before. **The concept of 3-D passwords promotes development, diplomacy, and defence as security strategies**. It is a multi feature authentication scheme which combines the benefits of different authentication schemes in a 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. User can make infinite number of 3-D passwords by combining any two or more different schemes. Therefore this scheme will be more acceptable to user as it will provide more security than any other authentication schemes.

Giving the user the freedom of selection as to what type of authentication schemes will be included in their 3-D password and given the large number of objects and items in the environment(virtual), the number of possible 3-D passwords will increase. Thus, it becomes much more difficult for the attacker or say hackers to guess the user's 3-D password.

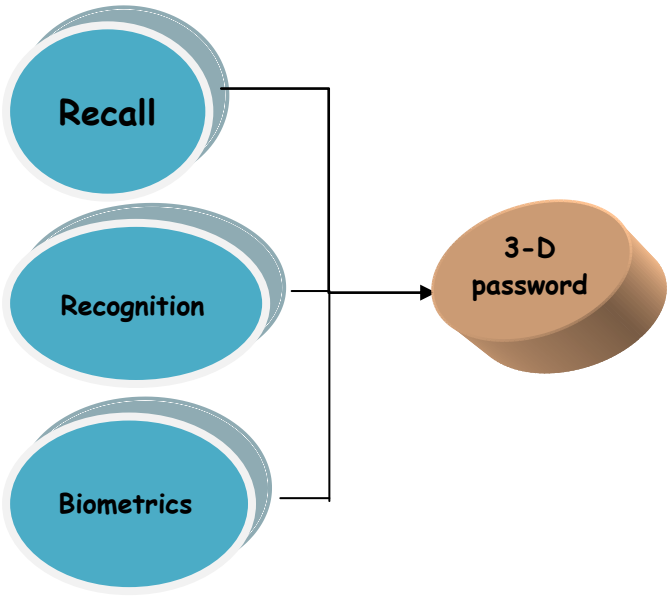

Fig. 1 .Basic idea of 3-D password

II. BRIEF DESCRIPTION OF 3-D ENVIRONMENT

Fig.2. Snapshot of 3-d virtual environment [1]

2.1 Different object that can be used in 3D environment [1]

a) A computer with which the user can type;

b) A fingerprint reader that requires the user's fingerprint;

c) A biometric recognition device;

d) A paper or a white board that a user can write, sign, or draw on;

e) An automated teller machine (ATM) that requests a token;

f) A light that can be switched on/off;

g) A television or radio where channels can be selected;

h) A staple that can be punched;

i) A car that can be driven;

j) A book that can be moved from one place to another;

k) Any graphical password scheme;

l) Any real life object;

m) Any upcoming authentication scheme.

III. 3-D PASSWORD SELECTION AND INPUTS

Let us consider a 3-D virtual environment space of size G×G×G. The 3-D environment space is represented by the coordinates (x, y, z) [1, . . ., G] ∈ × [1, ..., G] × [1,. . . , G].
The objects are distributed in the 3-D virtual environment with unique (x, y, z) coordinates.
We assume that the user can navigate into 3-D virtual environment and interact with the objects using any input device such as a mouse, keyboard, fingerprint scanner, card reader, and microphone. We consider the sequence of those actions and interactions using the previous input devices as the user's 3-D password [4].
The initial representation of user actions in the 3-D virtual environment can be recorded as follows:
1. (10,20,21) Action = Open the room door;
2. (10,20,21) Action = Close the room door;
3. (5,7,16) Action = Typing, "S";
4. (5,7,16) Action = Typing, "K";
5. (5,7,16) Action = Typing, "A"; (5,7,16) Action = Typing, "V";
6. (5,7,16) Action = Typing, "O"; (5,7,16) Action = Typing, "V";
7. (10,44,71) Action = Pick up the book;
8. (1,38, 71) Action = Drawing, point = (110,290).

Fig. 3. User entering textual password in 3-D environment [5]

IV. IMPLEMENTATION OF 3-D PASSWORD

Following are the steps for authentication (refer fig.4):

1. User will connect to the server for system login.

2. After successful client-server connection registration form will be filled up.

3. User will now enter into virtual 3-D environment.

4. Now the user will perform its authentication steps according to set design.

5. User enters his textual password. If the textual password is successfully logged in, it will enter into graphical password window else it will go back to Login form (refer fig.3).

6. On the other hand, if the graphical password is successfully logged in various services will be performed such as biometrics and tokens.

7. Services include Upload (), Save (), Delete (), Open () and etc..

8. Finally, the user will log out from the 3-D environment.

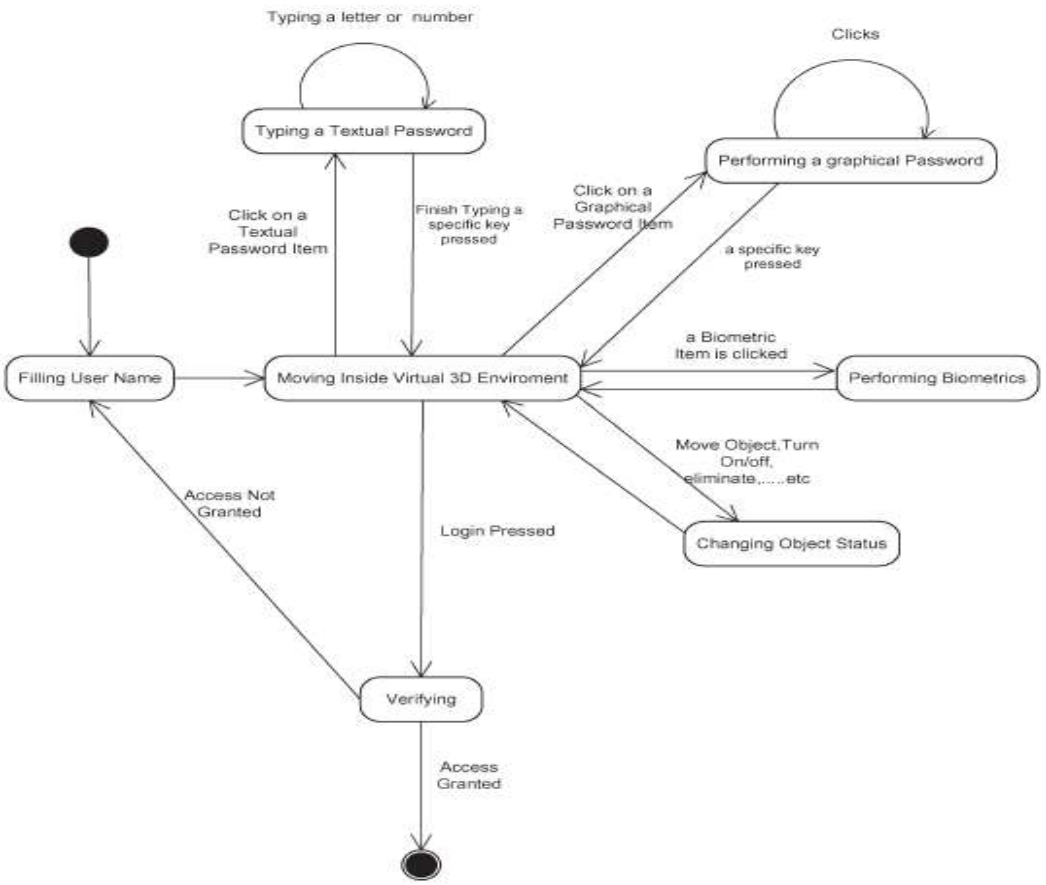

Fig.4 State diagram showing the implementation of 3-D password [4]

V. SECURITY ANALYSIS

5.1. 3D Password space size

To find out the password space, we have to count all possible 3D passwords that have a certain number of actions, interactions, and inputs towards all objects that exist in the 3D virtual environments[2].

5.2. 3D password distribution knowledge

Users tend to use meaningful words for textual passwords. Therefore finding these different words from dictionary is a relatively simple task which yields a high success rate for breaking textual passwords. Pass faces users tend to choose faces that reflect their own taste on facial attractiveness, race, and gender.

Every user has different requirements and preferences when selecting the appropriate 3D Password. This fact will increase the effort required to find a pattern of user's highly selected 3D password. In addition, since the 3D password combines several authentication schemes into a single authentication environment, the attacker has to study every single authentication scheme and has to discover what the most probable selected secrets are. Since every 3D password system can be designed according to the protected system requirements, the attacker has to separately study every 3D password system. Therefore, more effort is required to build the knowledge of most probable 3D passwords [7].

VI. PROBABILITY OF SYSTEM HACK [6]

Let the Textual Password Hack Probability = 1/x
Let the Graphical Password I Hack Probability = 1/y1
Let the Graphical Password I Hack Probability = 1/y2
Let the Graphical Password I Hack Probability = 1/y3
Let the Graphical Password I Hack Probability = 1/y4
Let the Face Recognition Hack Probability = 1/z
Combination Probability = 1/(xy1y2y3y4z)

Combinatorics for the Choice of six
= 6C6*6C5*6C4*6C3*6C2*6C1
= 1*6*15*20*15*6
= 162000

SYSTEM BREAK PROBABILITY:

=
(1/xy1y2y3y4z)*(1/162000)

VII. 3-D PASSWORD APPLICATIONS

The 3-D password can have a password space that is very large compared to other authentication schemes. So, the 3-D password's main application domains are protecting critical systems and resources.

7.1. **Critical servers** – Many large organizations have critical servers that are usually protected by a textual password. A3-D password authentication proposes a sound replacement for a textual password[4].

7.2. Nuclear and military facilities – Such facilities should be protected by the most powerful authentication systems. The 3-D password has a very large probable password space, and since it can contain token, biometrics, recognition, and knowledge-based authentications I a single authentication system, it is a sound choice for high level security locations[4].

7.3. Airplanes and jet fighters – Because of the possible threat of miscuing airplanes and jet fighters for religo-political agendas, usage of such protected by a powerful authentication system[4].

In addition, 3-D passwords can be used in less critical systems because the 3-D virtual environment can be designed to fit to any system needs. A small virtual environment can be used in the following systems like

- ATM[3]
- Personal Digital Assistance
- Desktop Computers & laptop logins
- Web Authentication

VIII. ADVANTAGES OF 3-D PASSWORD [3]

8.1. The new scheme provide secrets that are easy to remember and very difficult for intruders to guess.

8.2 The new scheme provides secrets that are not easy to write down on paper. Moreover, the scheme secrets should be difficult to share with others.

8.3 The new scheme provides secrets that can be easily revoked or changed.

IX. DISADVANTAGES OF 3-D PASSWORD

9.1. As compare to traditional password approach this approach will definitely take more time to do user authentication [4].

9.2. More storage space required because it needs to save images which is large binary objects [4].

9.3. More costly due to required devices like web cam, finger print device etc.

9.4. More complex than previous authentication schemes.

X. CONCLUSION

In 3D password system as number of series of action and interaction in the virtual 3D environment increases then the length of the codeword or the authentication key's length also increases. The amount of memory that is required to store a 3D password is large when compared to a textual password but provides far better security than textual password. Any user can make use of it no special training is required. Now a day's password security is in high demand. This 3D technique will definitely serve the purpose. The choice of what authentication schemes will be part of the user's 3-d password reflects the user's preferences and requirements. A user who prefers to remember and recall a password might choose textual and graphical passwords apart of their 3-D password. On the other hand, user's who have more difficulty with memory or recall might prefer to choose smart cards as their 3-D password. Moreover, user who prefers to keep any kind of biometrical data private might not interact with objects that require biometric information. Therefore, it is the user's choice and decision to construct the desired and preferred 3-D password.

REFERENCES

[1]. Fawaz Alsulaiman and Abdulmotaleb El Saddik , "Three Dimensional Password for more Secure Authentication" **,**IEEE Transactions on Instrumentations and Measurement.

[**2**]**.** Tejal Kognule and Yugandhara Thumbre and Snehal Kognule, "3D password", International Journal of Computer Applications(IJCA),2012.

[**3**]**.** NBC news, ATM Fraud: Banking on Your Money, Dateline Hidden Cameras Show Criminals Owning ATMs, Dec. 11, 2003.

[**4**]**.**Manila M V,"Three-Dimensional Password for More Secure A uthentication",netlab.cs.iitm.ernet.in/cs648/2009/tpf/cs08m028.pdf ,2009.

[5].http://www.123rf.com/photo_10326797_3d-man-secure-login-with-administrator-id-and-password.html.

[**6].** Prof. Gauri Rao ,"SECUREZZA"**,** IT Journal of Research, Volume 1, May 2010

[7]. 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.

Shubham Bhardwaj is currently pursuing degree in Bachelor of Technology in the field of Computer Science & Engineering, Gurgaon, India (2010-2014). He did his schooling from Sumermal Jain Public School, New Delhi, India. Being a research enthusiast, his basic interests include Security, Cloud Computing, Operating System and Networking & Wireless Data Transmission Techniques.

Varsha Yadav is currently pursuing degree in Bachelor of Technology in the field of Computer Science & Engineering, Gurgaon, India (2010-2014). Being a research enthusiast, his basic interests include Security, E-books and Networking & Wireless Data Transmission Techniques.She also has published a research paper on ebooks.

Varun Gandhi is currently pursuing degree in Bachelor of Technology in the field of Computer Science & Engineering, Gurgaon, India (2010-2014). He did his schooling from D.A.V Public School, New Delhi, India. Being a research enthusiast, his basic interests include Security, Cloud Computing, Hacking and Networking & Wireless Data Transmission Techniques.

Lalit Poddar is currently pursuing degree in Bachelor of Technology in the field of Computer Science & Engineering, Gurgaon, India (2010-2014). He did his schooling from Sumermal Jain Public School, New Delhi, India. Being a research enthusiast, his basic interests include Security, Cloud Computing, Photo editing tools and Networking & Wireless Data Transmission Techniques.