International Journal of Computer Engineering and Applications, Volume IX, Issue XI, Nov. 15
www.ijcea.com ISSN 2321-3469

3D PASSWORD MODERN APPROACH TO SECURITY

Anagha Kelkar[1], Komal Mukadam [1]

[1] *Department of Information Technology, B.E. Information Technology, V.E.S Institute of Technology, India*

ABSTRACT:

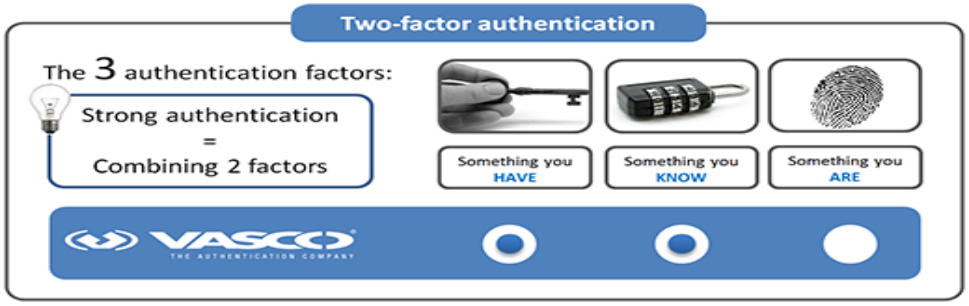
Authentication is provided to protect a system from potential threats and to ensure that only authorized people can have right to use or handle that system & data related to that system securely. Authentication is one of the most important security service provided to system by the different authentication schemes or algorithms. There are many authentication algorithms are available such as Graphical password, Text password, Biometric authentication etc. These passwords are not completely secure and effective and have some drawbacks. To overcome the limitations and drawbacks of the existing authentication schemes 3D password is introduced. The 3D Password is multi-feature, multi-factor authentication scheme that combines the benefits of currently used authentication schemes into single 3D virtual environment. This paper intents to focus on the concept of the new authentication scheme, its working and the applications of 3D password.

Keywords: Authentication, Multi-factor, Multi-feature, Virtual objects, Graphical passwords, textual passwords, 3D password.

[1] 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 are available some are effective & secure but having some drawback. Previously there are many authentication techniques were introduced such as graphical password, text password, Biometric authentication, etc. generally there are four types of authentication techniques are available such as:

- Knowledge based: means what you know. Textual password is the best example of this authentication scheme.
- Token based: means what you have. This includes Credit cards, ATM cards, etc. as an example.
- Biometrics: means what you are. Includes Thumb impression, etc.
- Recognition Based: means what you recognize. Includes graphical password, iris recognition, face recognition, etc.



Drawback in existing Authentication System:

Textual Password:

Textual Passwords should be easy to remember at the same time hard to guess. But if a textual Secured authentication: 3D password 243 password is hard to guess then it is very difficult to remember also. Full password space for 8 characters consisting of both numbers and characters is 2 *1014.From a research 25% of the passwords out of 15,000 users can guessed correctly by using brute force dictionary.

Graphical Password:

Graphical passwords came as users can recall and recognize pictures more than words. But most graphical passwords are susceptible for shoulder surfing attacks, where an attacker can observe or record the valid user graphical password by camera. The main weakness while applying biometric is its intrusiveness upon a user's personnel characteristics. They require special scanning device to verify the user which is not acceptable for remote and internet users. Smart cards can be lost or stolen and the user has to carry the token whenever access required.

[2] PROPOSED SYSTEM

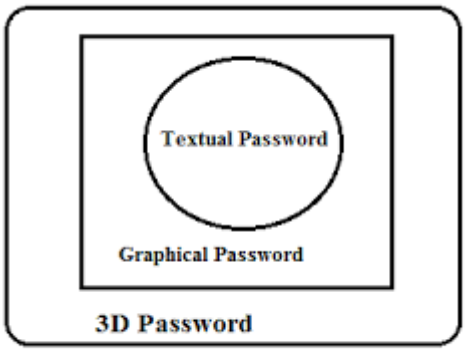


Fig. 3D password as Multi-factor & Multi-password Authentication scheme.

The proposed authentication system is a multi-factor and multi-password secure authentication scheme as it combines the benefits of previous existing authentication schemes into single platform authentication scheme together. The proposed system presents, the user with 3D virtual environment that contains several virtual objects or items with which the user can interact. Within this 3D virtual environment user can navigates and interact with various virtual objects. The users 3D Password is constructed by combining the sequence of actions and interaction towards the moving virtual objects

inside the 3D virtual environment. The proposed system can combine the previously existing schemes for example, textual passwords, graphical passwords, biometrics and even token based etc. in a single 3D virtual environment. The users need and preferences would reflect the choice of user in selecting which authentication scheme will be part of the user's 3D Password. A user who are good at recalling and remembering a password might prefer to select textual and graphical password as a part of their 3D Password. Moreover, users who find hard to recall and remember might prefer to select biometrics or smart cards as part of their 3D Password. Thus, it would be user's freedom to choose and decide how the ideal and desired 3D Password will be constructed.

A. Goal:

The main goal of the proposed system is to design a multi-feature, multi-password secure authentication scheme that combines the various authentication schemes into a single 3D virtual environment which results in a larger password space. The design of 3D virtual environment, the selection of object inside the environment, and the object type reflect the resulted password space. User have freedom to select whether the 3D password will be merely recall, recognition, or token based, or combination of two schemes or more.

B. Objective:

New scheme should provide more secure authentication compared to existing one.

New scheme should build easy to understand and user friendly authentication technique, giving user the freedom of choice to select whether the 3D password would be solely, recall, recognition, biometrics or the mixture of any two schemes or more.

New scheme should provide secrets that are easy to recall and at the same time tough to guess for the intruders.

New scheme should provide such secrets that cannot be easily shared with others and difficult to note down on papers.

New scheme should provide secrets that are mixture of merely recall, recognition, biometrics, and token based authentication schemes or combination of two or more schemes together.

New scheme should provide secrets that are flexible, and authenticated user must be allowed to change or remove them.

[3] 3D PASSWORD

Users nowadays are provided with major password stereotypes such as textual passwords, biometric scanning, tokens or cards (such as an ATM) etc. Mostly textual passwords follow an encryption

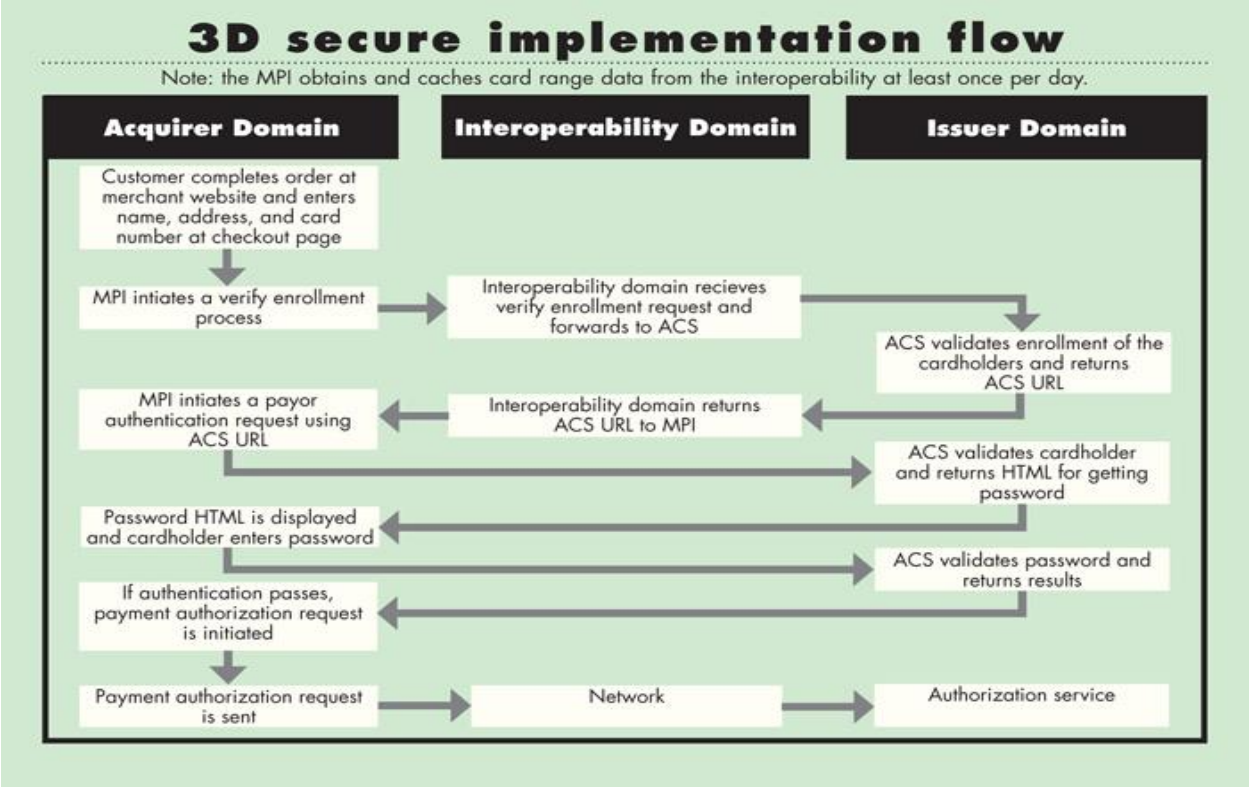
algorithm as mentioned above. Biometric scanning is your "natural" signature and Cards or Tokens prove your validity. But some people hate the fact to carry around their cards, some refuse to undergo strong IR exposure to their retinas(Biometric scanning).Mostly textual passwords, nowadays, are kept very simple say a word from the dictionary or their pet names etc. Years back Klein performed such tests and he could crack 10-15 passwords per day. Now with the technology change, fast processors and many tools on the Internet this has become a Child's Play.
Therefore we present our idea, the 3D passwords which are more customizable and very interesting way of authentication. Now the passwords are based on the fact of Human memory. Generally simple passwords are set so as to quickly recall them. The human memory, in our scheme has to undergo the facts of Recognition, Recalling, Biometrics or Token based authentication. Once implemented and you log in to a secure site, the 3D password GUI opens up. This is an additional textual password which the user can simply put. Once he goes through the first authentication, a 3D virtual room will open on the screen. In our case, let's say a virtual garage

The **3D password** is a multi-factor 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 fingerprint reader that requires the user's fingerprint;

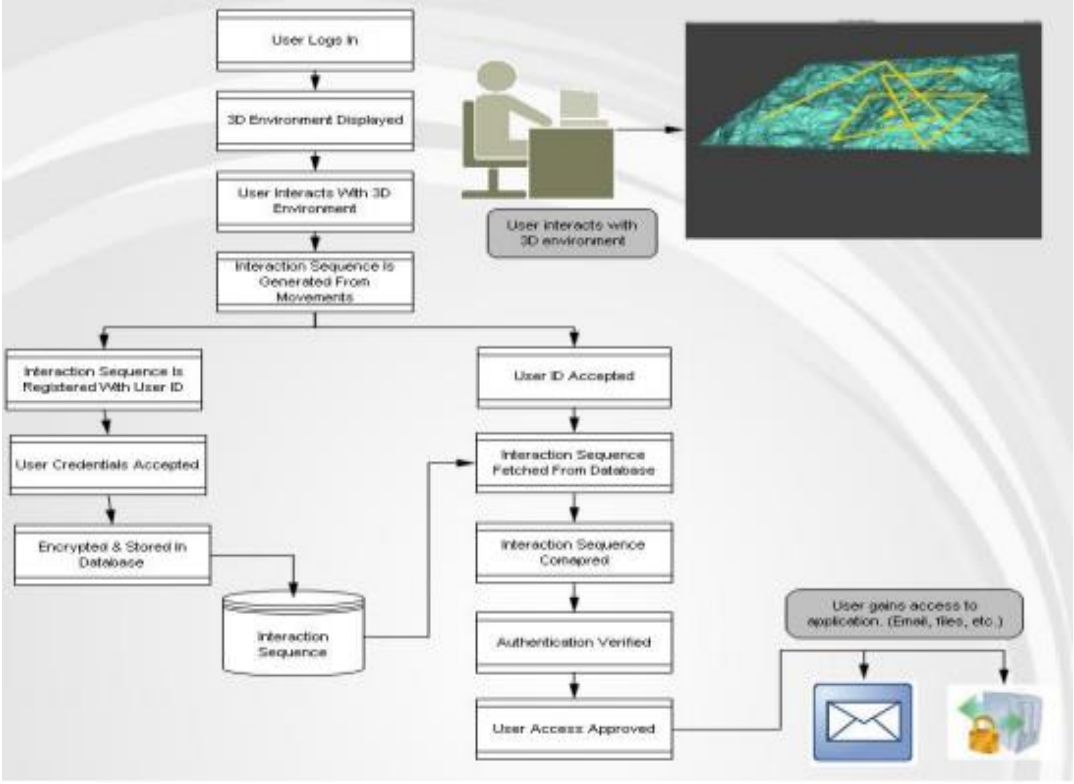
3) A biometric recognition device;
4) A paper or a white board that a user can write, sign, or draw on;
5) An automated teller machine (ATM) that requests a token;
6) A light that can be switched on/off;
7) A television or radio where channels can be selected;
8) A staple that can be punched;
9) A car that can be driven;
10) A book that can be moved from one place to another;
11) Any graphical password scheme;
12) Any real life object;
13) Any upcoming authentication scheme

[4] WORKING/IMPLEMENTATION



In 3D password the user First Authenticates with simple textual password this means that the user provides a username and a password. This authentication is validated and if it 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(x1, y1, z1). After this authentication is successfully completed, Then user then 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. Now this password is used of authentication when the user logs in next time. The user has to perform the actions in the same sequence as that it the file for the authentication to be successful. If authentication successful the access is given to authorized user. The working of the 3D password is as shown in the figure.



[5] APPLICATIONS

The 3D password can have a password space that is very large compared to other authentication schemes. The main application domains of 3D password are protecting critical systems and resources.
1. **Critical Servers**: Many large organizations have critical servers that are usually protected by a textual password. A 3D password authentication proposes a sound replacement for a textual password.
2. **Airplanes and jet fighters**: In airplanes and jet fighters there is a possible threat of misusing airplanes and jet fighters for religion, political agendas, usage of such airplanes should be protected by a powerful authentication system.
3. **Banking:** 3D passwords as used for passwords of the credit cards for online tractions.

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

1. ATM
2. Personal Digital Assistance
3. Desktop Computers & laptop logins
4. Web Authentication

[6] SECURITY ANALYSIS

It is necessary to consider all possible attack methods to realize and understand how far an authentication scheme is secure. It is important to understand if authentication scheme proposed is immune against such attacks or not. Moreover, if the proposed authentication scheme is not immune, we then have to find the countermeasures that prevent such attacks. The countermeasures to such attacks are detailed in this section.

Brute Force Attack

The attack is very difficult because of the following reasons

1. Time required to login may vary from 20 seconds to 2 minutes therefore it is very time consuming.
2. Cost of Attack: A 3D Virtual environment may contain biometric object, the attacker has to forge all biometric information.

Well-Studied Attack

The attacker tries to find the highest probable distribution of 3D passwords. In order to launch such an attack, the attacker has to acquire knowledge of the most probable 3D password distributions. This is very difficult because the attacker has to study all the existing authentication schemes that are used in the 3D environment. It requires a study of the user's Selection of objects for the 3D password. Moreover, a well-studied attack is very hard to accomplish since the attacker has to perform a customized attack for every different 3D

Virtual environment design. This environment has a number of objects and types of object responses that differ from any other 3D virtual environment. Therefore, a carefully customized study is required to initialize an effective attack.

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. This attack is the most successful type of attack against 3D passwords and some other graphical passwords. However, the user's 3D password may contain biometric data or textual passwords that cannot be seen from behind. Therefore, we assume that the 3D password should be performed in a secure place where a shoulder surfing attack cannot be performed.

Timing Attack

The Attacker observes how long it takes the legitimate user to perform correct log in using 3D Password which gives an indication of 3-D Passwords length. This attack cannot be successful since it gives the attacker mere hints.

[7] FUTURE SCOPE:

Currently, Textual passwords and token-based passwords are the most commonly used authentication schemes. These password schemes have a relatively narrower scope and are more open to attacks. While 3D password provides the users with freedom to select whether the 3D password will be solely recall, biometrics, recognition, or token based, or a combination of two schemes or more.3D passwords does not require figure prints nor cards for the purpose of authentication. 3D password provides choice to the user to construct the 3D password according to their needs and their preferences. A 3D password's probable password space can be reflected by the design of the three-dimensional virtual environment, which is designed by the system administrator. The 3D virtual environment can contain any objects that the administrator feels that the users are familiar with. For example, a football stadium can be emulated as the 3D environment.

[8] CONCLUSION

The textual passwords and token-based passwords currently used for authentication vulnerable to various kinds of attacks. The 3D Password is multi-feature, multi-factor authentication scheme that combines the benefits of currently used authentication schemes into single 3D virtual environment. The 3-D password is a new technique of authentication that is still in its initial 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. The 3D password reflects the user's preferences and requirement for the purpose of authentication and this makes the usage of 3D password user friendly.

REFERENCES

[1] Vishal Kolhe, Vipul Gunjal, Sayali Kalasakar, Pranjal Rathod "Secure Authentication with 3D Password" International Journal of Engineering Science and Innovative Technology (IJESIT)
[2] Duhan Pooja, Gupta Shilpi, Sangwan Sujata, & Gulati Vinita "SECURED AUTHENTICATION: 3D PASSWORD" International Journal of Engineering and Management Studies.
[3] S. Ranjitha "Secure Authentication with 3D Password" IFET College of Engineering
[4] Anuradha Srivastava "3-D PASSWORD – A more secured authentication" Slideshare.net
[5] "3D PASSWORD – Seminar" http://www.seminarsonly.com/computer%20science/3D-password.php