3D Password

Mr. Vaibhav Kharade
MET Institute of Computer Science, Mumbai, 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 various authentication services or security 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 many drawbacks. To overcome the disadvantages and drawbacks of the existing authentication schemes 3D password is introduced. The 3D Password is multi-feature, multi-factor authentication service that has the combination of most commonly used security services into single 3D virtual environment. This Research paper intents to conceptualize the new authentication service, its working and the applications of 3D password.

Key words: 3D Password, Authentication

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 various authentication algorithms available some of them are secure but have some drawbacks. At previous time there were many authentication techniques introduced such as graphical password, text password, Biometric authentication, etc. generally there are four types of authentication techniques available such as:

- Knowledge based: means what you know.Textual password is the best example of this authentication service.
- 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.

A. *Textual Password:*

Textual Passwords should be easy to remember at the same time hard to guess. But if a textual 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.

B. *Graphical Password:*

Graphical passwords came as users can recall and recognize pictures more than words. But most graphical passwords are likely to be harmed by 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.

II. Proposed-3D Password Based System

The projected system is a multi-factor authentication scheme which combines the advantages of other authentication schemes. Users can choose whether the 3D password will be only recall, biometrics, recognition, or token based, or a combination of two schemes or more. This choice of selection is necessary because users are different and they have different requirements. So, for assurity of high user acceptability, the user's freedom of selection is essential. The following necessities are satisfied in proposed scheme:

1) The new scheme provide secrets that are easy to remember and very difficult for intruders to guess.
2) The new service provides secrets that are not easy to write down on paper. Moreover, the service secrets should be difficult to share with others.
3) The new service provides secrets that can be easily revoked or changed. This scheme consists of:

Keys and secrets very easy to be remembered by the users but too difficult to be attacked by intruders.

These keys and secrets are not easy to presented or formulated in written. Such keys and secrets are not easily sharable or leak able. These keys and secrets can be easily transformed according to user or revoked as and when required.

III. 3D Virtual Environment

The effectiveness of the design of 3D virtual environment will increase with the number of the 3D objects contained in the 3D environment.

As there are more number of objects the more is the probability of the number of 3D passwords. And then more number of 3D passwords implies more difficulty for the attackers to crack the system by any of the techniques available. The 3D virtual environment space created on 2 D systems is in correspondence with the real world space.

Therefore interaction with this 3D environment is just like how one interacts with the real world objects in routine on day to day basis. Another important thing which should be kept in mind while designing this environment is that the objects contained in this environment should be unique from every other object present in the virtual space. Every 3D object needs to have its own position, attributes, size, and shape and type such that the interaction with first object will always be differently recognized from the interaction of the user with the second object.

Interactions and 3D objects need to be distinguishable enough so as to not let the user into any kind of ambiguity. As the prime motive of this new authentication scheme is easy to remember and difficult to be attacked or guessed. Analogy can be if you a car showroom have 20 same models of a car, each should be sold out to the user with a unique differentiable number on the number plate otherwise how difficult it would be to trace your own car out of similar models of the same car.

IV. System implementation

The 3D password is a multi-factor authentication service. The 3D password award formally a 3D virtual environment which contains various virtual objects.

The user navigates through this virtual environment and interacts with various objects. The 3D password is basically the permutation, 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 service.

This can be achieved by means of designing a 3D virtual environment that holds objects that request information to be recalled, recognition of information, presentation of tokens, and verification of biometric data. For example, the user can enter the virtual environment and type something on a computer that exists in v1(x1 , y1 , z1) position, then enter a room that has a fingerprint recognition device that exists in a position v2(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 frequency. The permutation, combination and the sequence of the user's actions toward the specific objects construct the user's 3D password. Virtual objects can be any object that we encounter in real life. Any apparent actions and interactions contributing to real life objects can be gained in the virtual 3D environment contributing 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 entities:

1) A computer with which the user can input.
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 ATM machine that requires a smart card and PIN.
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 chair that can be moved from one place to another.
11) Any graphical password design
12) A book that can be moved from one place to another.

V. Working

In 3D password the user First gets verified with simple text 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 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 any action in that environment like switching button on/off or perform task 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 choosing correct 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. Consider a three dimensional virtual atmosphere space that is of the size G×G×G. Each point in the three dimensional atmosphere space represented by the coordinates.(x,y,z)∈[1..G] × [1..G] ×[1..G].The entities are distributed in the 3D virtual environment. Every entity has its own (x,y,z) co-ordinates. Assume the user can navigate and walk through the three-dimensional virtual atmosphere and can see the entities and interact with the entities. The input device for interactions with entities can be a mouse, a keyboard, stylus, a card reader, a microphone…etc. For example, consider a user who navigates through the 3D virtual atmosphere that consists of a temple area. Let us assume that the user is in the virtual area and the user turns around to the bell located in (9,16, 80) and rings it. Then, the user touch deity feet. The user types "VAIBHAV" into a computer that exists in the position of (10, 5, 25). The user then walks over and turns off the light located in (15, 6, 20), and then goes to a white board located in (55, 3, 30) and draws just one dot in the (x,y) coordinate of the white board at the specific point of (420,170). The user then presses the login button. The user actions in the 3D virtual environment can be recorded as follows:

(9, 16, 80) Action = Ring the bell;
(9, 16, 80) Action = touch deity feet;
(10, 5, 25) Action = Typing, "V";
(10, 5, 25) Action = Typing, "A";
(10, 5, 25) Action = Typing, "I";
(10, 5, 25) Action = Typing, "B";
(10, 5, 25) Action = Typing, "H";
(10, 5, 25) Action = Typing, "A";
(10, 5, 25) Action = Typing, "V";
(15, 6, 20) Action = Turning the Light Off;
(55, 3, 30) Action = drawing,point = (420,170);

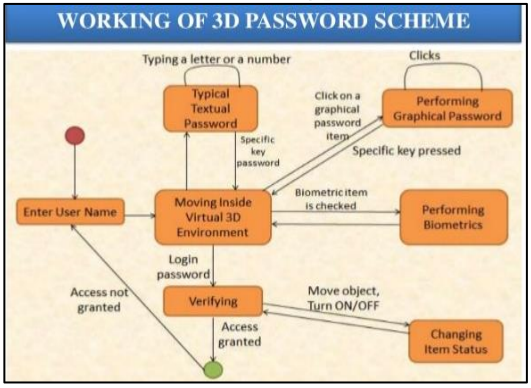

Fig. 1.1: Working of 3D password

VI. 3D PASSWORD DIFFERENTIATORS

1) Flexibility: The projected system is a multi-factor authentication scheme which combines the advantages of other authentication schemes.
2) Strength: It provides almost unlimited password possibility.
3) Easy to Remember: it can be remembered easily as a short story.
4) Privacy: organizers have option. Organizers can choose authentication designs that respect users privacy.

VII. 3D PASSWORD APPLICATION AREAS

1) Critical Servers: Many large organizations are provided security in text format.3D password provides sound replacement for these textual passwords.
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: A large number of Indian banks use 3D password service for the security of buyer who is willing to buy or pay online

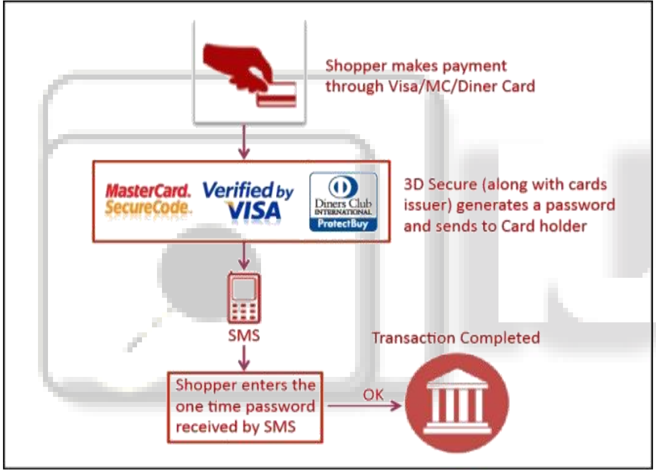
Shopper makes payment through Visa/MC/Diner Card
MasterCard. SecureCode.
Verified by VISA
Diners Club International ProtectBuy
3D Secure (along with cards issuer) generates a password and sends to Card holder
SMS
Transaction Completed
Shopper enters the one time password received by SMS
OK

Fig. 1.2: Working of 3D password in online payment

4) Nuclear and military Facilities: 3D password has a very large password space and since it combines RECOGNITION RECALL+TOKENS+BIOMETRIC in one authentication system, it can be used for providing security to nuclear and military facilities.
   Desktop and Laptop Logins, Web Authentication.

VIII. SECURITY ANALYSIS

A. Brute Force Attack

The attack is very difficult because Time required to login may vary from 20s to 2 min therefore it is very time taken. Cost of Attacks: A 3D Virtual environment is made up of biometric object, the attacker has to forge all biometric information.

B. Well-Studied Attack

The attacker searches the highest probability distribution of 3D passwords. The attacker has to acquire ample of knowledge of 3D password distributions, in order to attack. It is very difficult for the attacker as he has to do detailed analysis of existing authentication designs that are used in building 3D environment. The attacker may also need to study of the user's selection of entities for the 3D password. besides this, a well planned attack is very hard to implement as the attacker has to perform a customized task for every different 3D virtual environment design. This atmosphere has a number of entities and types of entity responses that differ from any other 3D virtual atmosphere. Therefore, a carefully customized study is required to initialize an effective attack.//Careful study of all level with integration between several design implementation of authentication require huge time and study lots of database or repositories of password . Practically impossible for a programmer or hacker.

C. Shoulder Surfing Attack

An attacker makes use of camera to record the user's 3D password or tries to look at the valid user while the 3D password is being performed. This attack is the most accomplishing type of attack against 3D passwords and some other graphical passwords. Besides this, the user's 3D password may contain biometric data or textual passwords that cannot be seen from behind. Hence, a 3D password should always be performed in a secure place where no one watches you or shoulder surfing attack cannot be performed.

Most successful where camera is installed but most failed incase integrated with biometric tools and techniques so only valid user can login.

D. Timing Attack

The Attacker notices the time taken by a valid user to perform correct login using 3D Password which gives an indication of 3-D Passwords length. This attack cannot be pass since it gives the attacker only hints.

IX. FUTURE WORK

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. There is no need of finger prints or card for authentication in 3D passwords 3D password provides choice to the user to construct the 3D password according to their needs and their preferences. Users do not have to carry cards if they do not want to. They have the choice to construct their 3D password according to their needs and their preferences.3D virtual environment reflects password space of a 3D password, which is designed by 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. Cricket players can use a three dimensional virtual atmosphere of a stadium where they can navigate and interact with entities that they are familiar with. Various kinds of attacks are possible on textual password and token based passwords which are presently used for authentication The projected system is a multi-factor, multi-feature authentication scheme which combines the advantages of presently used authentication schemes into single 3D virtual environment. The 3D password is just introduced means it is in its childhood. A study on a large number of people is required.

The 3D password user's experience can be enhanced and improved by

1) Interpreting feedback of user
2) Designing 3D virtual environment of different types
3) Deciding on password spaces
4) Overall experiences of users from such environment. 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] "Secure Authentication with 3D Password" by Vishal Kolhe,Vipul Gunjal,SayaliKalasakar, Pranjal Rathod International Journal of Engineering Science and Innovative Technology.
[2] "SECURED AUTHENTICATION: 3D PASSWORD" by Duhan Pooja, Gupta Shilpi, Sangwan Sujata, & Gulati Vinita International Journal of Engineering and Management Studies.
[3] "Secure Authentication with 3D Password" by S. Ranjitha IFET College of Engineering.
[4] "3-D PASSWORD – A more secured authentication" by Anuradha Srivastava
[5] "3D PASSWORD – Seminar" .
[6] "A Novel 3D graphical password schema" by Fawaz A Alsulaiman and Abdulmotaleb El Saddik Real User Corporation.
[7] http://www.seminarsonly.com/computer%20science/3D password.php.
[8] https://www.uniassignment.com/essay-samples/information-technology/secured-authentication-3d-password information-technology-essay.php
[9] "The Science behind Passfaces.http://www.realusers.comaccessed October 2005".