Imperial Journal of Interdisciplinary Research (IJIR)
Vol-2, Issue-5, 2016
ISSN: 2454-1362, http://www.onlinejournal.in

4D Password Mechanism

Miss Bhavana Borkar , Miss Shiba Sheikh, Prof. P. D. Kaware
BE Final year CSE, HVPM COET Amravati, Maharashtra
BE Final year CSE, HVPM COET Amravati, Maharashtra
Prof, HVPM COET Amravati, Maharashtra.

Abstract— *We have had many authentication schemes presently, but they all have some drawbacks. So lately, the 3D password paradigm was introduced. The 3-D password is a multifactor authentication scheme. It can combine all existing authentication schemes into a single 3-D virtual environment.*
However the 3-D password is still 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. Moreover, gathering attackers from different backgrounds to break the system is one of the future works that will lead to system improvement and prove the complexity of breaking a 3-D password. This paper presents a study of the 3D password and an approach to strengthen it by way of adding a Fourth dimension, that deals with gesture recognition and time recording, and that would help strengthen the authentication paradigm altogether. Hence we attempt to propose a 4-D password as a one-up method to the 3-D password.

Index Terms—*security, authentication (key words)*

I. INTRODUCTION

AUTHENTICATION is a process of validating who you are to whom you claimed to be, or in other words a process of identifying an individual, usually based on a username and password. Currently what we have in the field, are the following set of techniques:

Human Authentication Techniques are as follows:
1. Knowledge Base (What you know)
2. Token Based (What you have)
3. Biometrics (What you are)
4. Recognition Based (What you recognize)

Computer Authentication Techniques are as follows:
1. Textual Passwords
2. Graphical Passwords
3. Biometric schemes (fingerprints, voice recognition etc.)

We are provided with many password types such as textual passwords, biometric scanning, tokens or cards (such as an ATM card) etc. But there are many weaknesses in the current authentication systems. The most common computer authentication method is to use alphanumerical usernames and passwords. One of the main problems is the difficulty of remembering passwords. Studies have shown that users tend to pick short passwords or passwords that are easy to remember. Unfortunately, these passwords can also be easily guessed or broken.
According to a recent Computer world news article, the security team at a large company ran a network password cracker and within 30 seconds, they identified about 80% of the passwords
Following is the brief summary of *Human Authentication Techniques:-*
Knowledge Based Authentication Techniques are the most widely used authentication techniques and include both text-based and picture-based passwords.
These technique is commonly referred to as KBA, is a method of authentication which seeks to prove the identity of someone accessing a service, such as a financial institution or Website . As the name suggests, KBA requires the knowledge of private information of the individual to prove that the person providing the identity information is the owner of the identity.

Token Based Authentication Techniques, such as key cards, bank cards and smart cards are widely used. Many token based authentication systems also use knowledge based techniques to enhance security. For example, ATM cards are generally used together with a PIN number.
Token-based authentication is a security technique that authenticates the users who attempt to log in to a server, a network, or some other secure system, using a security token provided by the server. An authentication is successful if a user can prove to a server that he or she is a valid user by passing a security token. The service validates the security token and processes the user request. After the token is validated by the service, it is used to establish security context for the client, so the service can make authorization decisions or audit activity for successive user request.
Biometrics Based Authentication Technique, such as fingerprints, iris scan, or facial recognition, are not yet widely adopted. The major drawback of this approach is that such systems can be expensive, and the identification process can be slow and often

unreliable. However, this type of technique provides the highest level of security.

The Picture-Based OR Graphical Password Techniques can be further divided into two categories: recognition-based and recall-based graphical techniques.

Using *recognition-based techniques*, a user is presented with a set of images and the user passes the authentication by recognizing and identifying the images he or she selected during the registration stage.

Using *recall-based techniques*, a user is asked to reproduce something that he or she created or selected earlier during the registration stage.Main flaw was that password space was small since, the number of images were limited to 30.

Graphical Passwords can also be used. One of the main arguments for graphical passwords is that pictures are easier to remember than text strings. As the technology has changed many fast processors and tools are available on internet, it has become very easy to hack the graphical password. The 3D passwords scheme has been introduced as a one up solution to these issues.

The concept behind the model is that exploitation of a system's vulnerabilities involves abnormal usage of system and this abnormality can be detected by looking for the abnormal patterns in the audit records. The model proposed is capable of detecting break-ins, penetrations, and other forms of computer anomaly[5]. In this paper we are using four algorithms are used.

II. The 3D Password Scheme

Current authentication systems suffer from many weaknesses. Textual passwords are commonly used. Users tend to choose meaningful words from dictionaries, which make textual passwords easy to break and vulnerable to dictionary or brute force attacks. Many available graphical passwords have a password space that is less than or equal to the textual password space. Smart cards or tokens can be stolen. Many biometric authentications have been proposed. However, users tend to resist using biometrics because of their intrusiveness and the effect on their privacy. Moreover, biometrics cannot be revoked. The 3Dpassword is a multi factor authentication scheme. The design of the 3D virtual environment and the type of objects selected determine the 3D password key space. Moreover, user have freedom to select whether the 3D password will be solely recall, recognition, or token based, or combination of two schemes or more and given the large number of objects and items in the environment, the number of possible 3D passwords will increase. Thus, it becomes much more difficult for the attacker to guess the user's 3-D password. This freedom of selection is necessary because users are different and they have different requirements. Therefore, to ensure high user acceptability, the user's freedom of selection is important.

The 3D Password scheme is a relatively new authentication scheme that combines RECOGNITION +RECALL + TOKENS + BIOMETRIC in one authentication system [6]. The 3-D password is a multifactor authentication scheme that combines the benefits of various existing authentication schemes.

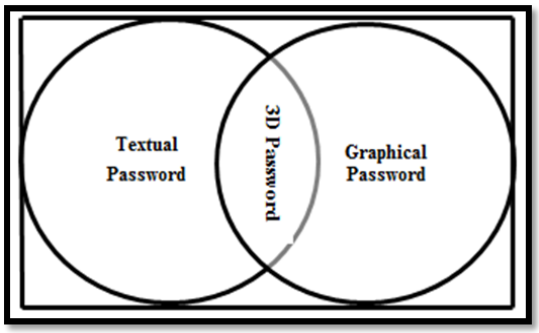

Figure.1 3D Password (Multifactor and Multi-Password Authentication Scheme)

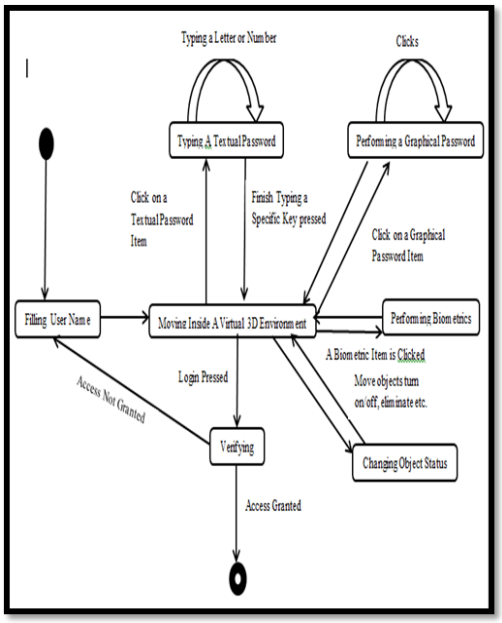

Figure.2 State Diagram of Creating 3D Password

This 3-D virtual environment contains several objects or items with which the user can interact. The type of interaction varies from one item to another. The 3-D password is constructed by observing the actions and interactions of the user and by observing the sequences of such actions. It is the user's choice to select which type of authentication techniques will be part of their 3-D password [6].

This is achieved by providing only that information that the user is agree to provide and ignoring the other

request information that the user is not comfortable to provide.
For example, if an item requests a thumb impression and the user is not comfortable in providing such information, then the user simply avoids interacting with that item.

A.Working:

Consider a three dimensional virtual environment space that is of the size S×S×S. Each point in the three dimensional environment space represented by the coordinates (x, y, z) € [1..S] × [1..S] × [1..S]. The objects are distributed in the three-dimensional virtual environment. Every object has its own (x, y, z) coordinates [6].

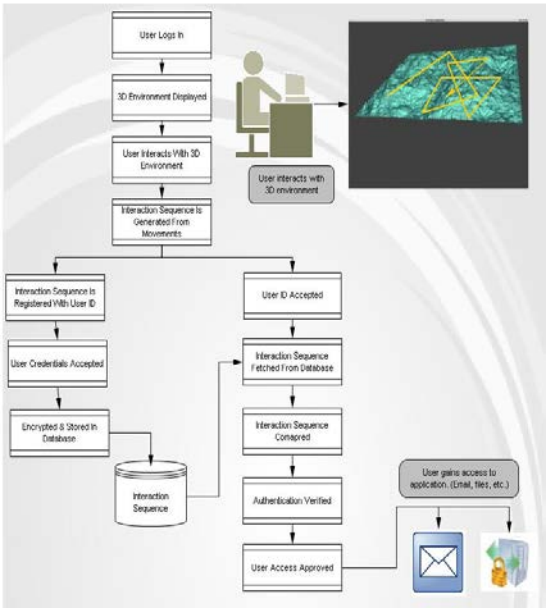

Figure.3 Working of 3D password scheme

For example, consider a user who navigates through the 3D virtual environment that consists of a ground and a classroom. The input device for interactions with objects can be a mouse, a keyboard, stylus, a card reader, a microphone etc. Let us assume that the user is in the virtual ground and the user turns around to the door located in (10, 16, 80) and opens it. Then, the user closes the door. The user types "WAFFLE" into a computer that exists in the position of (18, 5, 20). 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 [6]. The initial representation of user actions in the 3D virtual environment can be recorded as follows:

(10, 16, 80) Action = Open the office door;
(10, 16, 80) Action = Close the office door;
(18, 5, 20) Action = Typing, “W”;
(18, 5, 20) Action = Typing, “A”;
(18, 5, 20) Action = Typing, “F”;
(18, 5, 20) Action = Typing, “F”;
(18, 5, 20) Action = Typing, “L”;
(18, 5, 20) Action = Typing, “E”;
(15, 6, 20) Action = Turning the Light Off;
(55, 3, 30) Action = drawing, point = (420,170);

After the user has performed all these actions, he will exit out of the 3-D environment and after backend verification, access will be granted to user who is authorized.

III. Introducing The Fourth Dimension

As the 3D authentication scheme suffers from many weaknesses such as shoulder surfing attack, timing attack etc., there is the possibility of hacking the 3D password. The 4-D Password scheme is an attempt to make the existing scheme even more robust and powerful [2]. We propose to add another key to the current scheme, and this will lend more stability and make the attacks on user privacy even more difficult to succeed in.
This key, what we propose to refer to as the ‘FOURTH DIMENSION’ would be an encrypted string that encapsulates a gesture that the user is supposed to make with his hands, in front of a webcam, apart from his password. This will help ensure that the user is physically present for login. Hence, the final password of the user would be:

Hand Gesture + 3-D Password.

We have a mapping function F(x), such that if we put V as the input string, then it creates F(V), which is our final encrypted key. The user does not need to bother with any of these.
All he needs to do is remember the gesture, which would be captured as a binary string S. This would be saved as a precursor to his 3-D password. The String V would then be encrypted and appended to the already existing password.
Hence, the end result would be a password that looks like this:

P = 3-D password + F(V).

The addition of F(V) at the end would actually increase the complexity of the password. The attacker will now have to guess the string V as well as try to decipher function F(x), in addition to the complex techniques required to decipher a user’s 3-D password itself.

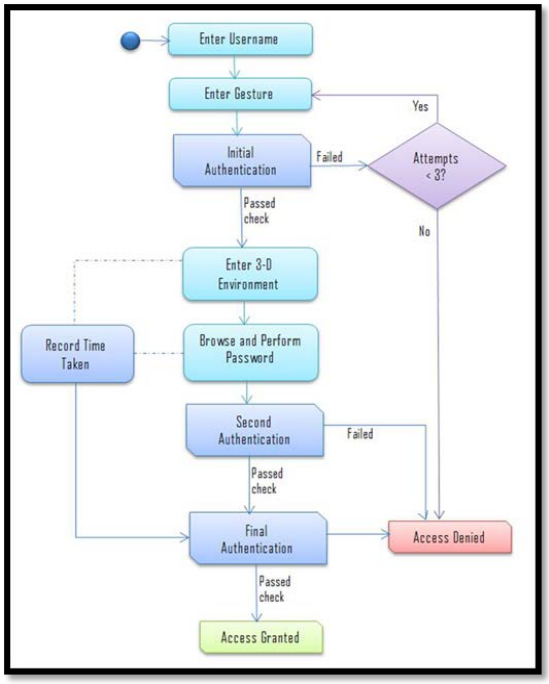

Figure.4 The 4-D Password Scheme.

A.Signup Process:

Consider a web-based repository of research work for scientists, wherein each scientist has his own account which stores his files and folders. This repository employs the 4-D password scheme.
As a new user, I will sign up as follows:
1. Choose a username.
2. I will be redirected to the password generation page.
3. I will enter the 3-D environment.
4. Inside the environment, I will perform certain actions, as have been discussed before.
5. I will exit out of the environment and submit my actions.
6. I will then be asked to perform a gesture in front of the webcam. This gesture, once successfully captured, will be saved. I will be notified of the time that I had taken to perform this gesture this time.
7. I will need to remember it for subsequent attempts at login Sign up process is complete.

B.Loging In:

Now when I log in, I will have to enter my username, and then perform my gesture. Once this is submitted and verified, I will enter the 3-D environment and perform my password.
I will exit and submit it. Once that is verified ,will be granted access to my account.

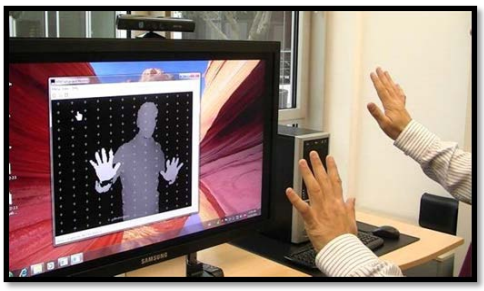

Figure.5Gesture Recognition in use

C.Significance

The addition of an extra gesture will create an unlimited host of password combinations. Also it will ensure that there is a person attempting to login, and not some automated program, or bot.
Another check that can be applied here, is the measure of the total time taken for the 3-D Authentication by the user. This time can be considered a part of the user's authentication, and the user must perform subsequent attempts within the same time limit, give or take a few more seconds. So each password can then have a time window associated with it.
On later attempts, a timer can be made to run in parallel to the 3-D browsing session. Based on the total time taken, certain conclusions can be drawn out:
1. If time taken tends to zero, it might be an attempt made by an automated hacking process.
2. If time taken is very large, it may well be possible that another user is attempting to replicate the user's actions, step by step.
This additional check will provide more soundness to the 4-D password scheme.

IV. SECURITY ANALYSIS

To realize and understand how far an authentication scheme is secure, we have to consider all possible attack methods. We have to study whether the authentication scheme proposed is immune against such attacks or not.

A. Keylogger:

In many cases, the attacker installs an invisible software called a keylogger, which is designed to capture all keys typed through the user's keyboard and output them as a stream in a text file. This way the attacker finds out the user's password by browsing through the file. But here, since the nature of password is not textual, this attempt will be a total failure.

B. Well Studied Attack:

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 .The 3D 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. Even then, the probability of a successful attack is extremely scarce.

With a 4-D password, there is the extra process of determining the gesture as well. The chances that an attacker can guess the gesture, out of thousands of possible human movements, is going to be as hard as it sounds. Plus, both the gesture and the 3-D password need to guessed correctly. So chances of a successful attack in this case are bleak, to mention the least.

C. 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 ensure that the 3D password should be performed in a secure place where a shoulder surfing attack cannot be performed. Also, with the 4-D password, the nuances of the gesture, even if visible to the attacker, may not be emulated successfully, and also the physique will have to match with the user, since the system would compare it with the earlier recording.

D.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. Also this would lend the attacker no help in finding out the extra gesture; which is exclusive of the 4D password only.

E. Brute Force Attack:

The attacker has to try all possible 3D passwords. This kind of attack is very difficult for the following reasons.

1. Time required to login may vary from 20s to 2 min therefore it is very time consuming.

2. Cost of Attack: 3D virtual environment contains biometrics recognition objects and token based objects.The attacker has to forge all possible biometric information and forge all the required tokens.

V.WHAT MAKES IT CLICK

A.4-D Password Differentiators:

1.**Flexibility:**4D Passwords allows Multifactor Authentication. Biometric, graphical and textual passwords can be embedded in 4D password technology.

2. **Strength:** This scenario provides almost unlimited passwords possibility. Hence, the strength.

3**. Easy to Remember:** Can be remembered in the form of short story.

4. **Privacy:** Organizers can select authentication schemes that respect the user's privacy.

B.Application Areas:

1. **Critical Servers:** Many organizations are using critical servers which are protected by a textual password. 4D
password authentication scheme proposes sound replacement for these textual passwords.

2. **Banking:** Almost all the Indian banks started 3-D password service for security of buyer who wants to buy online or pay online.

3. **Nuclear and military Facilities:** 4D password has a very large password space and since it combines RECOGNITION+RECALL+TOKENS+BIO-METRIC in one authentication system, it can be used for providing security to nuclear and military facilities.

4. **Airplanes and Jet Fighters:** Since airplanes and Jet planes can be misused for religion and political agendas, they should be protected by a powerful authentication scheme.

5. **ATMs, Desktop and Laptop Logins, Web Authentication.**

6. **The Cloud:** Cloud computing is an internet-based model for enabling convenient, on-demand network access to a shared pool of configurable computing resources. It provides various services over internet such as software, hardware, data storage and infra-structure. The 4D password scheme, if successfully implemented here can make the cloud much safer and reliable.

VI. FUTURE SCOPE

Cloud computing provides various internet-based, on demand services like software, hardware, server, infrastructure and data storage. To provide privacy services to the intended customer, it is a better option to use strong password generation and authentication technique. The addition of gesture recognition

technique would ensure that the strict authentication and authorization is possible. This is the future work of our research. Our future work will be carried out in adding multi-dimensional password generation method to multi-level authentication technique.
Also to build strong algorithm for gesture recognition is the future work of our research paper.

VII. CONCLUSION

As the 3D authentication scheme suffers from many weakness such as shoulder surfing attack, timing attack etc., there is the possibility of hacking the 3D password. The 4-D Password scheme makes the existing scheme even more secure and powerful.
The 3D Password is easily hackable by using shoulder surfing attack. Hence a better multi-layer authentication scheme has been proposed in this paper i.e. the 4D Password.
The 4D password scheme combines features of all the existing authentication schemes like text and graphics passwords, biometric scanning techniques, token recognisation schemes and adds two new features i.e. it uses a virtual 3D environment and a gesture recognisation system.
It is fully customizable as per the user wishes i.e. the user has freedom of choice as of what type of authentication scheme will be part of their 3D password
It is also a very powerful against attacks. The first two layers text and graphics can be easily broken via conventional brute force and shoulder surfing techniques. The 3D layer is harder to crack but the addition of gestures makes it stronger since gestures are based on an individual person and his physique which is something the attacker cannot replicate. Also 4D Password scheme ensures that the user is physically present to access the system and hacker is not hacking the system remotely.
We need to create algorithms to implement such schemes and make them available to user.

VIII. REFERENCES

[1] Vishal Kolhe, Vipul Gunjal, Sayali Kalasakar and Pranjal Rathod, "Secure Authentication with 3D Password", in International Journal Of Engineering Science And Innovative Technology(IJESIT).

[2]Grover Aman and Narang Winnie, "4D Authentication: Strengthening The Authentication Scene", in International Journal Of Scientific And Engineering Research (IJSER).

[3]Farnaz Towhidi and Maslin Masrom, "A Survey On Recognition-Based Graphical User Authentication Algorithms", in International Journal Of Computer Science
And Information Security(IJCSIS).

[4] Harsh Kumar Sarohi and Farhat Ullah Khan, "Graphical Password Authentication Schemes: Current
Status and Key Issues", in International Journal Of Computer Science Issues(IJCSI).

[5]Tejal Kongule,Yogundhara Thumbre and Snehal Kongule, "3D Password", in ICACACT.

[6] Duhan Puja, Gupta Shilpi, Sangwan Sujata and Guwati Vinita, "Secured Authentication:3D Password", in International Journal Of Engineering And Management Sciences(IJEMS).

[7] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Basic results," *in Proc. Human-Computer Interaction Int.Las Vegas*, NV, Jul. 25–27, 2005.

[8] Fawaz A. Alsulaiman and Abdulmotaleb El Saddik,"Three-Dimensional Password for More Secure Authentication", in IEEE.