IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. V (Mar-Apr. 2014), PP 01-06
www.iosrjournals.org

4-D Authentication Mechanism

Ronak Talati, Shubham Shah
Computer Science, Vishwakarma Institute of Information Technology, India

Abstract: *Computer technology is reaching new milestones with every passing day but authentication schemes are still weak in their approach. It has now become a child's play for others to filch, hack or fabricate our passwords. Many authentication schemes have been proposed but each has some drawbacks. Hence, the 3D password paradigm has been introduced. The 3D password is a multi-layer, multifactor authentication mechanism. It consists of a 3D virtual environment on which a user has to perform certain actions. The sequence of actions determines the user's 3D password. It combines all existing authentication schemes like textual, graphical and biometrics into a single 3D virtual environment. The 3D virtual environment is easily customizable by the user as per his requirements. 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 4D password as a super class of 3D password.*

Keywords: *Authentication, Graphical password, Textual password, Virtual Environment, 3D Environment, Biometrics, 4D passwords.*

I. Introduction

Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. In private and public computer networks (including the Internet), authentication is commonly done through the use of logon passwords. Knowledge of the password is assumed to guarantee that the user is authentic. Each user registers initially (or is registered by someone else), using an assigned or self-declared password. On each subsequent use, the user must know and use the previously declared password. The weakness in this system for transactions that are significant (such as the exchange of money) is that passwords can often be stolen, accidentally revealed, or forgotten.

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 drawbacks. Previously there were many authentication techniques that were introduced such as graphical password, text password, biometric authentication.

Currently what we have in the field, are the following set of techniques:

Human Authentication Techniques are as follows:

1. Knowledge Based (What you know and recall)
2. Token Based (What you have i.e. tokens, objects)
3. Biometrics (What you are i.e. your physical body)
4. Recognition Based (What you recognize based on clues)

Computer Authentication Techniques can be classified as follows:

1. Textual Passwords (using alphabets, numbers and special characters)
2. Graphical Passwords (2D scheme via mouse interaction)
3. Biometric schemes (fingerprints, voice recognition etc.)

Textual passwords enjoy widespread used because they are easy to remember and are cheap to implement. They suffer from what is known as the password problem. The easy to use and memorize but at the same time they should be r password should be random and hard to guess.

It is proven via various studies that users are very careless when it comes to choosing and handling alphanumeric passwords. A survey was conducted by Daniel V. Klein where he cracked a sample set of 13797 passwords. Armed only with a mini-dictionary consisting of 62727 words, he was able to crack 25% of the passwords.

To solve this problem, graphical problems are proposed. They are easier to remember since they comprise of pictures rather than words. They were first proposed by Greg Blonder and involved showing user a picture on screen and making him click on various points on the picture to construct his password. This method is useful as it is easier to remember it suffers from one major drawback i.e. it just takes careful observation of the users actions to crack the passwords. This is known as the shoulder surfing problem.

Other techniques involve the use of a physical device, called as a token, which is provided to an authorized user of a system for recognization of the user. Token is an electric form of authentication. It contains data such as an encrypted key, biometric signature, etc. Examples of tokens are ATM card, smart cards, etc. Major drawbacks involve loss of the token, or users not wanting to physically carry the token, etc.

Biometric systems are based on identification based on specific human traits. They consists of the human physiology (fingerprint, face, DNA, etc.) and behavior (typing rhythm,gait,voice.) It is one of the most powerful forms of authentication but also one of the most dangerous. If a biometric device is used then the device is in danger of being stolen / destroyed. The same applies to a human. Also it also depends on the acceptability of a person to subject his body to IR exposure.

With the increments in technology and their availability in the internet, it is very easy to crack passwords based on the classic authentication schemes. Hence a new scheme is proposed as a one-up solution to these problems. This is the 3D password scheme. It is a multi-level, multi-factor authentication scheme. It combines all of the above mentioned schemes into one single customizable virtual environment. The interaction of the user within this virtual environment and the order of interaction forms the user's password.

II. The 3d Password Scheme

The 3D Password mechanism is a relatively new authentication system that combines RECOGNITION + RECALL + TOKENS + BIOMETRIC as one via a 3D virtual environment. Hence it is multifactor authentication scheme. The 3D virtual environment contains several objects or items with which the user can interact. The type of interaction varies from one item to another. The password is formulated by storing the actions and their sequence in an encrypted database. The user can select which schemes will be a part of his authentication scheme. The user can interact only with those items that request information that the user is comfortable to give and ignore the others. E.g. if an iris scan is required but the user does not wish to expose his eyes to IR then he may simply skip that step. Giving this freedom of choice to the users allows for highly customizable interface and virtually any number of passwords. Consequently it becomes difficult for the attacker to guess the password.

II.I 3D PASSWORD INTERFACE

Let us consider a 3D virtual environment space of size $G \times G \times G$. The 3D environment space is represented by the coordinates$(x, y, z) \in [1. . . G] \times [1. . . G] \times [1. . . G]$. The objects are distributed in the 3D virtual environment with unique (x, y, z) coordinates. We assume that the user can navigate into the 3D virtual environment and interact with the objects using any input device such as a mouse, keyboard, fingerprint scanner, iris scanner, stylus, card reader, and microphone. We consider the sequence of those actions and interactions using the previous input devices as the user's 3D password.

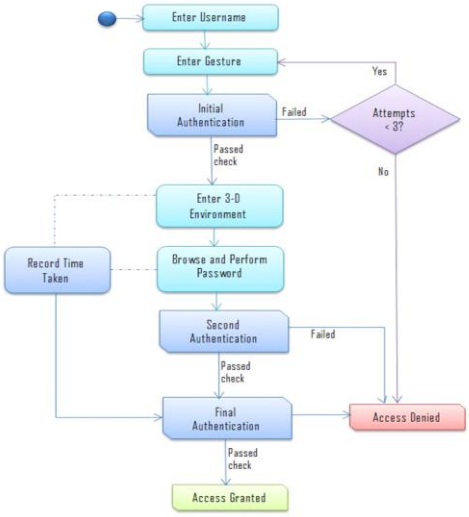
For example, consider a user who navigates through the 3D virtual environment that consists of an office and a meeting room. Let us assume that the user is in the virtual office and the user turns around to the door located in (21, 65, 84) and opens it. Then, the user closes the door. The user then finds a computer to the left, which exists in the position (50, 20, 10), and the user types "HELLO." Then, the user walks to the meeting room and picks up a pen located at (10, 24, 80) and draws only one dot in a paper located in (0, 0, 30), which is the dot (x, y) coordinate relative to the paper space is (350, 180).The user then presses the login button. The initial representation of user actions in the 3D virtual environment can be recorded as follows:

(21, 65, 84) Action = Open the office door;
(21, 65, 84) Action = Close the office door;
(50, 20, 10) Action = Typing, "H";
(50, 20, 10) Action = Typing, "E";
(50, 20, 10) Action = Typing, "L";
(50, 20, 10) Action = Typing, "L";
(50, 20, 10) Action = Typing, "O";
(10, 24, 80) Action = Pick up the pen;
(0, 0, 30) Action = Drawing, point = (350, 180).

After the user has performed these actions, he will exit out of the 3D environment. After backend verification, access will be granted.

Creating a 3D virtual environment is a complex process and can be broken down into the following steps :-

Modeling: We create the physical environment and objects using brushes, primitives and solid entites.
Layout: We organize all the objects on a base map.
Texturing: All the objects are given detailing and color by mapping them onto 2D bitmaps.
Rendering: The final scene is rendered from different places at different camera angles and lightning angles.



The 3D virtual environment construction manners the strength of the 3D password. The first step is to build a 3D object environment that reflects the administration needs and the security requirements. While designing such an environment, we must keep consider the following points :-

I. Real Life Simulation: The environment should be as close to the real life as possible. Objects and interactions amongst them should reflect real life situations.
II. Object uniqueness and peculiarity: Every virtual object is distinct. Every object has its own attributes such as position, colour, shape, size, location. Therefore the interaction of the user towards various objects is unique and the distinguishing factor increases the user's recognition of objects.
Hence, it provides more enhancement to the system usability.
III. Environment Size: A 3D virtual environment can be as large as a city or even as small as a single room or office. The time factor is directly proportional to the size of the 3d environment.
IV. System Importance: The 3D password should be selected such that it reflects the properties of the system. The same logic must be applied while setting the number of objects and their position.

III. Introducing The Fourth Dimension

The 4D Password scheme is an attempt to make the existing 3D scheme even more robust and powerful. We propose to add another key to the current scheme, and this will lend more stability and make any hacking attempts difficult. 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. It requires the physical presence of the user. Hence, the final password of the user would be Hand Gesture + 3D Password.

Now let's have a closer look as to how this gesture would be generated and saved. 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 3D 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 = 3D 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 3D password itself.

III.I 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 4D password scheme.

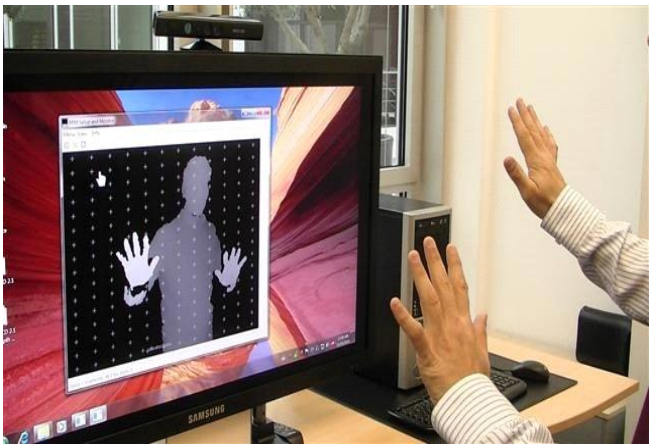
As a new user, I will sign up as follows:
1. Choose a username.
2. I will be redirected to the password generation page.
3. I will enter the 3D environment.
4. Inside the environment, I will perform certain actions, as have been discussed before.

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.

III.II 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 3D environment and perform my password. I will exit and submit it. Once that is verified, I will be granted access to my account.



Gesture Recognition in use.

III.III 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 3D 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 3D 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 4D password scheme.

IV. Security Analysis

We are going to analyze how hard it would be for an attacker to break into this system. A possible measurement is based on the information content of a password space, which is defined in as "the entropy of the probability distribution over that space given by the relative frequencies of the passwords that users actually choose." While textual passwords can have a large space, only a small subset is required to break into the authentication system. Hence it is imperative to have both a large password space and a scheme which has no previous knowledge of user password selection for stronger resistance to attacks.

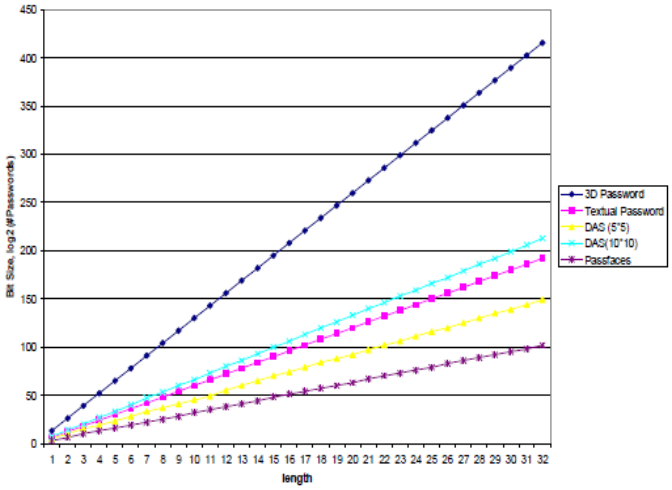
1V.I. Well-Studied Attack

In order to launch such an attack, the attacker has to acquire knowledge of the most probable 3D password distributions. The hacker will need to study various designs of 3D environments and the probable choice of password depending on the user. It will be harder since the hacker will have to customize it for different users and environments. The 3D environment will contain a large number of objects and wide variety of selected authentication schemes so even after a good study. The chances of success are very small.

4D password throws in the extra work for the hacker. He will have to guess the gesture made by the user. Since there are many possible gestures and the recognisation is also based on physique and the time in which the gesture is completed, it becomes virtually impossible to crack.

IV.II Shoulder Surfing Attack

3D passwords are vulnerable to shoulder surfing. All the actions performed on the virtual environment can be carefully observed by means of camera. But some interfaces may contain text or biometric data which can be observed but no sense can be made of it. Also the authentication is more likely to be done in a secure environment. In 4D passwords the nuances of gestures may be recorded but the actual physical performance is quite another story. Not only is difficult to accurately perform the same action but if the matching is based on physique of the user, it will be impossible to do hack into the system.



A comparison between the full password space of 3D Password, Textual Password, PassFaces of size (3×3 possible faces each turn), DAS of grid size (5× 5), and DAS of grid size (10 × 10). The length represents the number of characters for the textual passwords, the number of actions, interactions and inputs towards the objects for the sss3D password, the number of selections for Passfaces, and the number of points that represent the strokes for DAS. The length is up to 32 (characters/actions, interactions, and inputs/selections). The 3D password virtual environment is as specified in Section (IV.A). We can see how the 3D password's possible passwords are much larger than most existing authentication schemes.

IV.III Timed Attack

The time taken by the user to complete the 3D authentication can be measured. This could give attacker hints about the password's length, nothing more. Also it would not solve the problem of guessing the hand gesture.

IV.IV. Key logger

A key logger logs all the keys pressed on the keyboard. It runs in the background and is invisible to the user. It will be able to detect the textual component of the password but it will not be able to capture the graphical, biometric, token and gesture components so the software will be a total failure.

IV.V Brute Force Attack

The attacker simply formulates and algorithm to generate and check all possible passwords. This is a last resort method and the most inconvenient due to the following reasons :-

IV.V.I Time Required: The 3D virtual environment consists of combination of text, graphics, biometrics, token and objects plus the interaction sequence amongst these objects. It is time consuming to generate and check all possible combinations.

IV.V.II Cost of attacks: Memory utilization is very high thanks to a large 3D password space. The computer may freeze before reaching the key combination due to the high complexity of the algorithm required.

V. 4d Password Characteristics

V.I Flexibility: 4D Passwords support Multifactor Authentication. Biometric, graphical and textual passwords can be embedded in 4D password technology.

V.II Strength: This scenario provides almost unlimited passwords possibility.

V.III Easy to Remember: Can be remembered in the form of short story.
V.IV Privacy: Organizers can select authentication schemes that respect the user's privacy.

VI. Applications

VI.1 ATMs, Desktop and Laptop Logins, Web Authentication.
VI.II Nuclear and military Facilities: 4D 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.
VI.III 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.
VI.IV Critical server: Many large organizations have critical Servers that are usually protected by a textual password. A 4D password authentication proposes a sound replacement for a textual password
VI.V Banking: Almost all the Indian banks started 3D Password service for security of buyer who wants to buy Online or pay online. "How to Create 3D pass-word for m master card? Our online payment will fail, if will create 3D password, so for generating 3D password, we have to go to our bank's website and then, click 3D secure service and then write our card number, CVV, pin no., and write our password and rewrite it and then click ok or submit." After this we get a 'thank you' message. Like PNB, SBI also started 3D secure services for verified by Visa. Verified by Visa is a new service that will let you use a personal password with your State Bank of India Visa card, giving you added assurance that only you can use your State Bank of India Visa card to make purchases over the Internet.

VII. Conclusion

Technology is getting updated with every passing moment and more and more users are getting aware of this. As more people adopt this technology, it becomes imperative to protect the people's interests by providing more secure authentication schemes.

The authentication techniques which are widely used today have several drawbacks, all of which mean that the passwords provided in these schemes are easily hackable. 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. The user can set any of the options that he is comfortable with. A user unable to recall long textual passwords may use the virtual environment, a user unwilling to subject any part of his body to IR exposure can skip biometrics, a user not wishing to burden himself by carrying cards or tokens can remove the token recognisation system.

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.

Multilayer authentication schemes are just in their early stages. We need to create softwares and algorithms to implement such schemes and present them to user. The feedback coming from the user will come in handy to improve such schemes further.

References

[1] X. Suo, Y. Zhu, and G. S. Owen, "Graphical passwords: A survey," in *Proc. 21st Annu. Comput. Security Appl. Conf.*, Dec. 5–9, 2005, pp. 463–472.
[2] D. V. Klein, "Foiling the cracker: A survey of, and improvement to passwords security," in *Proc. USENIX Security Workshop*, 1990, pp. 5–14. Authorized licensed use limited to: IEEE Xplore. downloaded on March 5, 2009 at 02:38 from IEEE Xplore. Restrictions apply. 1938 IEEE TRANSACTIONS ON INSTRUMENTATION AND MEASUREMENT, VOL. 57, NO. 9, SEPTEMBER 2008
[3] Alsulaiman, F.A.; El Saddik, A., "Three- for Secure," IEEE Transactions on Instrumentation and measurement, vol.57, no.9, pp 1929-1938.Sept. 2008.
[4] Fawaz A. Alsulaiman and Abdulmotaleb El Saddik,"Three-Dimensional Password for More Secure Authentication," IEEE,
[5] *http://ieeexplore.ieee.org*., Last Updated –6 Feb 2008J.
[6] R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in *Proceedings of 9th USENIX Security Symposium*, 2000.
[7] A.B.Gadicha , V.B.Gadicha , ―Virtual Realization using 3D Password‖, in International Journal of Electronics and Computer Science Engineering, ISSN 2277-1956/V1N2-216-222.
[8] Duhan Pooja, Gupta Shilpi , Sangwan Sujata, & Gulati Vinita, ―SECURED AUTHENTICATION: 3D PASSWORD‖, I.J.E.M.S., VOL.3(2),242 – 245, 2012.
[9] Grover Aman, Narang Winnie, ―4-D Password: Strengthening the Authentication Scene‖, International Journal of Scientific & Engineering Research, Volume 3, Issue 10, October-2012.