© 2017 IJSRST | Volume 3 | Issue 1 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

4D Password Authentication Scheme

Gurwinder Singh

Punjab College of Commerce and Agriculture, Vill-Sarkapra, P. O. Chunni Kalan, Fatehgarh sahib, Punjab, India

ABSTRACT

There are so many authentication schemes used presently, but they all have some drawbacks. It is very easy for anyone to filch or hack our passwords. So lately, the 3D password paradigm has been introduced. The 3D passwords which are more customizable and very interesting way of authentication. A 3D password is a multifactor authentication scheme that combines Recognisation + Recall +Tokens +Biometrics in one authentication system. This research paper presents a study of the 3D password and an approach to strengthen it by way of adding a Fourth dimension (also called 4D), that deals with gesture recognition and time recording, and that would help strengthen the authentication scheme altogether. Hence we attempt to propose a 4D password as a parent class of 3D password.

Keywords: Authentication, Textual Password, Graphical Password, Bio-metrics, 3D Password, 4D password.

I. INTRODUCTION

The dramatic increase of computer usage has given rise to many security concerns. One major security concern is authentication, which is the process of validating who you are to whom you claimed to be. In general, human authentication techniques can be classified as shown in figure:

Textual Passwords

Recall-based techniques require the user to repeat or reproduce a secret that the user created before. Recognition based techniques require the user to identify and recognize the secret, or part of it, that the user selected before. One of the most common recall-based authentication schemes used in the computer world is textual passwords. One major drawback of the textual password is its two conflicting requirements: the selection of passwords that are easy to remember and, at the same time, are hard to guess.

Graphical Passwords

Various graphical password schemes have been proposed. Graphical passwords are based on the idea that users can recall and recognize pictures better than words. However, some of the graphical password schemes require a long time to be performed. Moreover, most of the graphical passwords can be easily observed or recorded while the legitimate user is performing the graphical password; thus, it is vulnerable to shoulder surfing attacks. Currently, most graphical passwords are still in their research phase and require more enhancements and usability studies to deploy them in the market.

Biometrics

Many biometric schemes have been proposed; fingerprints, palm prints, hand geometry, face recognition, voice recognition, iris recognition, and retina recognition are all different biometric schemes. Each biometric recognition scheme has its advantages and disadvantages based on several factors such as consistency, uniqueness, and acceptability. One of the main drawbacks of applying biometrics is its intrusiveness upon a user's personal characteristic. Moreover, retina biometrical recognition schemes require the user to willingly subject their eyes to a low-intensity infrared light. In addition, most biometric systems require a special scanning device to authenticate

users, which is not applicable for remote and Internet users.

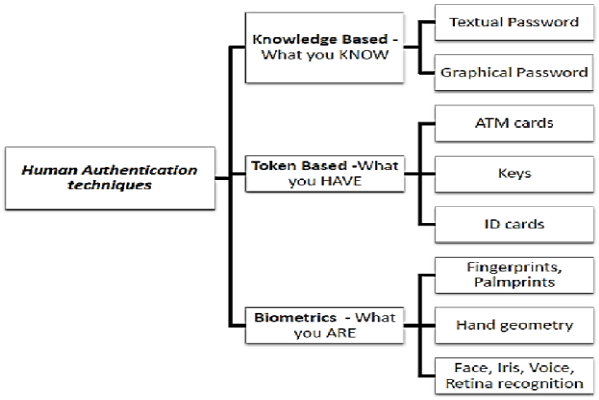

Figure 1. Human Authentication Techniques – Classification

II. METHODS AND MATERIAL

A. Literature Review

Many user studies and survey have confirmed that people can recall graphical password more reliably than text based password over a long period of time. This seems to be the main advantages of graphical passwords. Graphical password system can be classified as either recognition-based, cued recall-based or pure recall-based [1]. Dhamija and Perrig [2] proposed a graphical authentication scheme based on Hash Visualization techniques [3].Several authentication protocols have been proposed to integrate bio-metric authentication with user name and password authentication and/or graphical authentication. However, given the limited candidate faces on the screen, the security of Pass faces is vulnerable to trial attacks. Convex Hull Click [4] is developed to overcome the problem of passwords that are vulnerable to shoulder surfing in a public environment. It motivates the users to log in quickly and accurately. The suggested number of icons to ensure a large password space makes the screen crowded for users to find out the right click region. It was also be found that, the Convex Hull occasionally forms too narrow a space for users to click on. Another shoulder surfing resistant graphical password scheme is obtained by adding a light graphic layer to traditional textual-based password scheme [5].The scheme has proved to be effective against shoulder surfing attacks, and yet as it is alphanumeric-based, it contains the inevitable drawbacks of alphanumeric passwords .Token based techniques, such as key cards, bankcards and smart cards are widely used. Many token-based authentication systems also use knowledge based techniques to enhance security.

B. 3D Password Authentication Scheme

The 3-D password can combine recognition-, recall-, token-, and biometrics-based systems into one authentication scheme. This can be done by designing a 3-D virtual environment that contains objects that request information to be recalled, information to be recognized, tokens to be presented, and biometrical 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 3-D password.

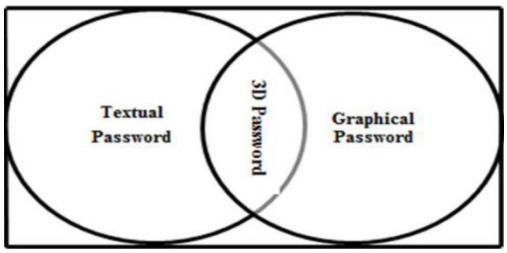

Figure 2. 3D Password (Multifactor and Multi-Password Authentication Scheme)

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 3-D environment toward the virtual objects. Moreover, any user input (such as speaking in a specific location) in the virtual 3-D environment can be considered as a part of the 3-D 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 biometrical 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.

C. 3D Password Applications

Because a 3-D password can have a password space that is very large compared to other authentication schemes, the 3-D password‟s main application domains are protecting critical systems and resources. Possible critical applications include the following.

1. Critical servers: Many large organizations have critical servers that are usually protected by a textual password. A 3-D password authentication proposes a sound replacement for a textual password. Moreover, entrances to such locations are usually protected by access cards and sometimes PIN numbers. Therefore, a 3-D password can be used to protect the entrance to such locations and protect the usage of such servers.
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 in a single authentication system, it is a sound choice for high level security locations.
3. Airplanes and jetfighters: Because of the possible threat of misusing airplanes and jetfighters for religion-political agendas, usage of such airplanes should be protected by a powerful authentication system. The 3-D password is recommended for these systems.

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

1. ATMs;
2. Personal digital assistants;
3. Desktop computers and laptop logins;
4. Web authentication.

D. Advantages of 3D Password

- ✓ Flexibility: 3D Passwords allows Multifactor authentication biometric, textual passwords can be embedded in 3D password technology.
- ✓ Strength: This scenario provides almost unlimited passwords possibility.
- ✓ Ease to Memorize: can be remembered in the form of short story.
- ✓ Respect of Privacy: Organizers can select authentication schemes that respect users‟ privacy.
- ✓ It provides user options to choose the type of authentication of his own choice.
- ✓ It leads to unsuccessful brute force attack.
- ✓ It provides high level security to the system which contains more important data.
- ✓ 3D graphical password has no limit.
- ✓ Difficult to share.
- ✓ Freedom to select.
- ✓ Difficult to crack.

E. Disadvantages of 3D Password

- ✓ Difficult for blind people to use this technology.
- ✓ Requires sophisticated computer technology.
- ✓ Expensive
- ✓ A lot of program coding is required.
- ✓ 3D password required very large memory space.

III. RESULTS AND DISCUSSION

A. 4 D-Authentications Scheme

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. 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.

The three operating modes of 4th dimension

Design mode - the design mode environment is the realm of the application developer access to this mode may be locked with the 4d password system
User mode - in user mode the developer tests the application; in this mode only an administrator is entitled make changes on a finished application custom menus mode- the custom mode is the working area of the user of the finished solution only the functions provided by the developer are available

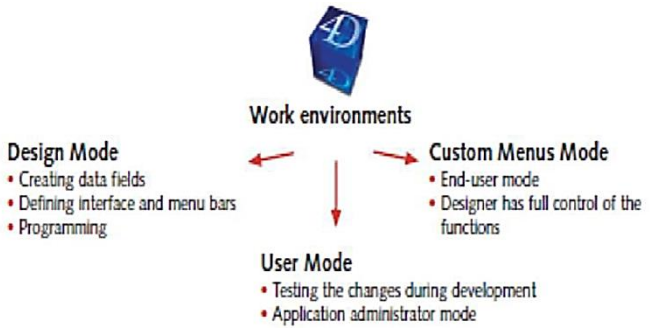

Figure 3

Signup process- consider a web based repository of research work for scientists, 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 following

1. Choose a user name
2. I will be redirected to password generation page
3. I will enter the 3d environment
4. I will exit out of the environment and submit my actions

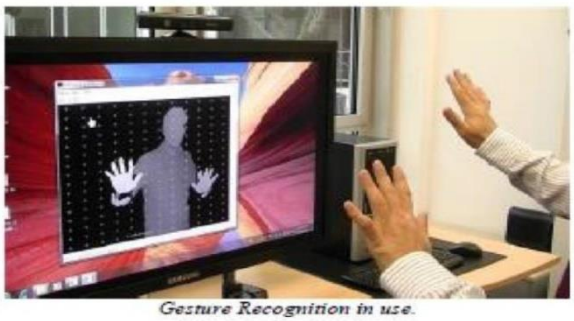
Gesture Recognition in use.

Figure 4

LOGGING IN- now when i log in, i will have to enter my user name, 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.

B. Application of 4D Password

1. Critical Servers: Many organizations are using critical servers which are protected by a textual password. 4D password authentication scheme proposes sound re-placement 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.

C. Advantages of 4D Password

1. Flexibility: 4D Passwords allows Multifactor Authentication. Bio-metric, 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.

D. Disadvantages of 4D Password

1. Security is entirely based on confidentiality and the strength of the password
2. Does not provide strong identity check (only based password)

IV. CONCLUSION AND FUTURE WORK

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 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.

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 sophisticated and robust password generation and authentication technique. A strong authentication technique would ensure strict authentication and authorization. The security levels of cloud environment can be further improved by multi-level of authentication. Also to build strong algorithm for gesture recognition is the future work of our research paper.

V. REFERENCES

[1]. I. Biederman, A. Glass, and E. Stacy. Searching for objects in real world scenes. Journal of Experimental Psychology, pages 22-27, 1973.

[2]. R. Dhamija and A. Perrig," Deja vu: A User Study Using Images for Authentication," in Proceedings of 9th USENIX Security Symposium, 2000.

[3]. A. Perrig and D. Song, "Hash Visualization: A New Technique to Improve Real-World Security, " in Proceedings of the 1999 International Workshop on Cryptographic Techniques and E-Commerce, 1999.

[4]. International Journal of Scientific & Engineering Research, Volume 3, Issue 10, October-2012.

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

[6]. Duhun Pooja, Gupta Shilpi, Sangwan Sujata, & Gulati Vinita, -SECURED AUTHENTICATION: 3D PASSWORD, I.J.E.M.S., VOL.3 (2), 242-245, 2012.

[7]. Grover Aman, Narang Winnie,-4D Password: Strengthening the Authentication Scene, International Journal of Scientific & Engineering Research, Volume 3, Issue 10, October 2012.

[8]. Ronak Talati, Shubham Shah, 4D Authentication Mechanism, IOSR Journal of Computer Engineering, Volume 16, Mar-Apr. 2014.

[9]. Nilima Nikam, Karishna Mane, 4D AUTHENTICATION SYSTEM USING MOUSE GESTURE, Journal of The International Association of Advanced Technology and Science, Vol. 16, March 2015.