Information and Knowledge Management
ISSN 2224-5758 (Paper) ISSN 2224-896X (Online)
Vol.4, No.6, 2014
www.iiste.org

Voiced 3D Password Authentication

Mr. Mohammed Hussein Ali
Lecturer, Department of Computer Science,Cihan University \Sulaimaniah \Iraq
E-mail : m_tam_2005t@yahoo.com

Abstract
In today's world, security is important aspect in day to day life .So, everyone used various ways for security purpose. People use passwords for their security .Generally, everyone uses textual password. Textual password is combination of alphabets and numbers. People keep textual password as name of their favorite things, actors or actress, dish and meaningful word from dictionary. But the person who is very close to that person can easily guess the password. Graphical password is advanced version of password. Graphical passwords have received considerable attention lately as Potential alternatives to text-based passwords. Graphical password is composed of images, parts of images, or sketches. These passwords are very easy to use and remember. To overcome the Drawbacks of previously existing authentication technique. We present A new improved authentication technique , This authentication Scheme is called as " voiced 3D password". The voiced 3D password is multi-password & multi-factor authentication system as it uses a different authentication techniques such As textual password , sound password, graphical password , biometrical password . Most important part of 3d password scheme is inclusion of 3D virtual environment. We proposed that user first can write him/her user name and textual password and then the program provide a studio for choosing the specific sound , then passed to 3D virtual environment . Shoulder-suffering attack is still can affect the schema of 3D password , so we add the Voiced 3D password to reduce that affect .
Keywords:3D password , textual password , graphical password , biometric password , voiced password, Quick hull algorithms, convex hull algorithm .

1. Introduction :

Normally the authentication scheme the user undergoes is particularly very strict. Throughout the years authentication has been a very interesting approach. With all the means of technology developing, it can be very easy for 'others' to fabricate or to steal identity or to hack someone password , Ideally there are two different types of Authentication schemes are available according to nature of scheme & techniques used, those types are:

1.1 Recall based:

In this authentication tech. user need to recall or remember his/her password which is created before .
Knowledge based authentication is a part of this technique, E.g. Textual password, graphical password etc. this technique is commonly used all over the world where security needed.

1.2 Recognition based:

In this user need to identify, recognize password created before. Recognition based authentication can be used in graphical password. Generally this technique is not use much more as Recall based is used.
Still both recall based & recognition based authentication techniques having some drawbacks & limitations when they are used separately or used single authentication scheme at a time. And we have seriously attack called Shoulder-suffering attack is still can affect the schema of 3D password .
To overcome these drawbacks & limitations of previously existing authentication schemes. We have introduced a new authentication scheme which is based on previously existing schemes. This authentication scheme is based on combination of passwords called as "voiced 3D Password" as shown in fig 2.

2.Authentication:

The process of identifying an individual usually based on a user name and password. In security systems, authentication is distinct from *authorization* , which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he \ she claims to be, but says nothing about the access rights of the individual.

3.Drawbacks In Existing Authentication system :

3.1 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 are search 25% of the passwords out of 15,000 users can guessed correctly by using brute force dictionary.

3.2 Graphical Password:

By using graphical passwords the users can recall and remember pictures more than words. But most graphical

passwords are susceptive for shoulder surfing attacks, where an attacker can record the user's graphical password by camera.

3.3 Biometric recognition:

Each biometric recognition scheme has its advantages and disadvantages . One of the main advantages of biometric is the person is the key ,so the user doesn't need to remember any thing .each part is unique like eye , face , fingerprint ,etc .disadvantages of biometric is those parts may be changed if you are ill ,like ; face injured , eyes puffy , voice problems , finger disfiguration .

4.Suggested System :

The projected system is a multi factor authentication scheme which combines the advantages of other authentication systems . Our system provide three stages :

4.1.1 Users can first apply their regular password and user name then just he\she have to remember the special his\her three letters .

4.1.2 The system provide a special sound studio which is provide different types of sounds and tones .

4.1.3 The most important stage , For authentication with 3D password a new virtual environment is introduced called as 3D virtual environment where user navigate , moving in 3D virtual environment to create a password

Fig. 1 shows some snapshots of 3D Virtual Environment of different real time scenarios created in virtual environment like art gallery, office, and study room, etc. These virtual environments are interactive virtual environment. Because user can interact with these environment & creates his/her own 3D password easily.

(A) (B)

Fig 1 (A) snapshot of office , (B) snapshot of room

4.2 How the sound studio works ?

The system can provide any type of the Sound Effect Maker which is a tool used for applying different sound effects for sound files. The tool supports sound effects like chorus, compression, distortion, echo, flange etc. These features can be adjusted as per user preference.

4.3 How the 3D password works ?

After login the textual password the user moved to the sound studio to select the sound or tone , Then user automatically enter 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 doors , close doors, etc. The sequence in which user has clicked (i.e. interacting 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. Next time when user want to access his account then he has to select all the object which he has selected at the time of creating password with proper sequence .This sequence is then compared with coordinates which are stored in file. If authentication successful thereafter access is given to authorized user. voiced 3D password working algorithm is shown in fig.3. Which will give the flowchart for voiced 3D password creation & authentication process.

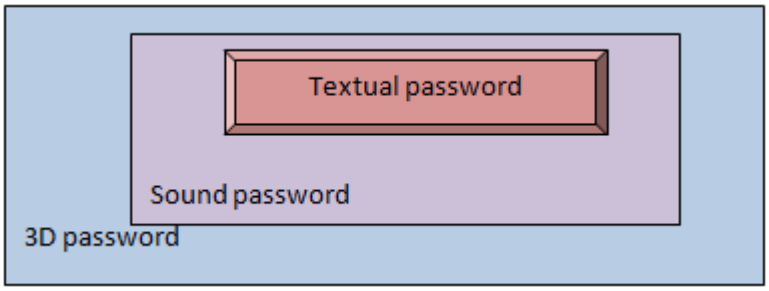


Fig 2 . voiced 3D password as multi factor and multi passwords

4.4 OBJECTIVE OF SUGGESTED SYSTEM :

- To provide more secure authentication technique than existing one.
- To design & develop more user friendly & easier authentication scheme and giving user to freedom of selecting more than one password scheme as single system.
- To overcome the drawbacks & limitations of previously existing systems (textual password, graphical password.etc).
- New scheme should be combination of sound , recall-, recognition -, biometrics-, and token based authentication schemes.

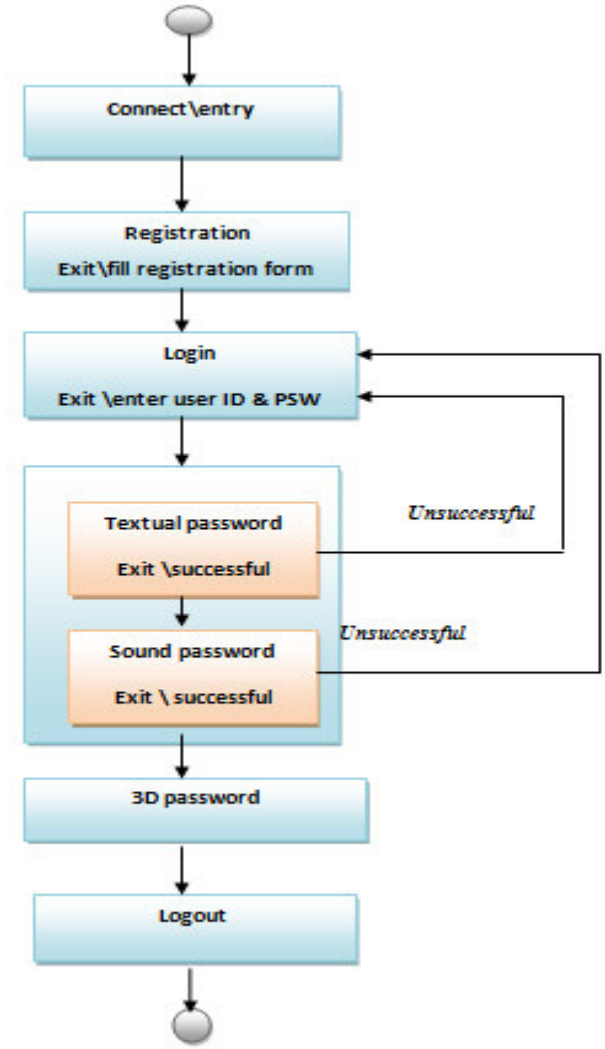
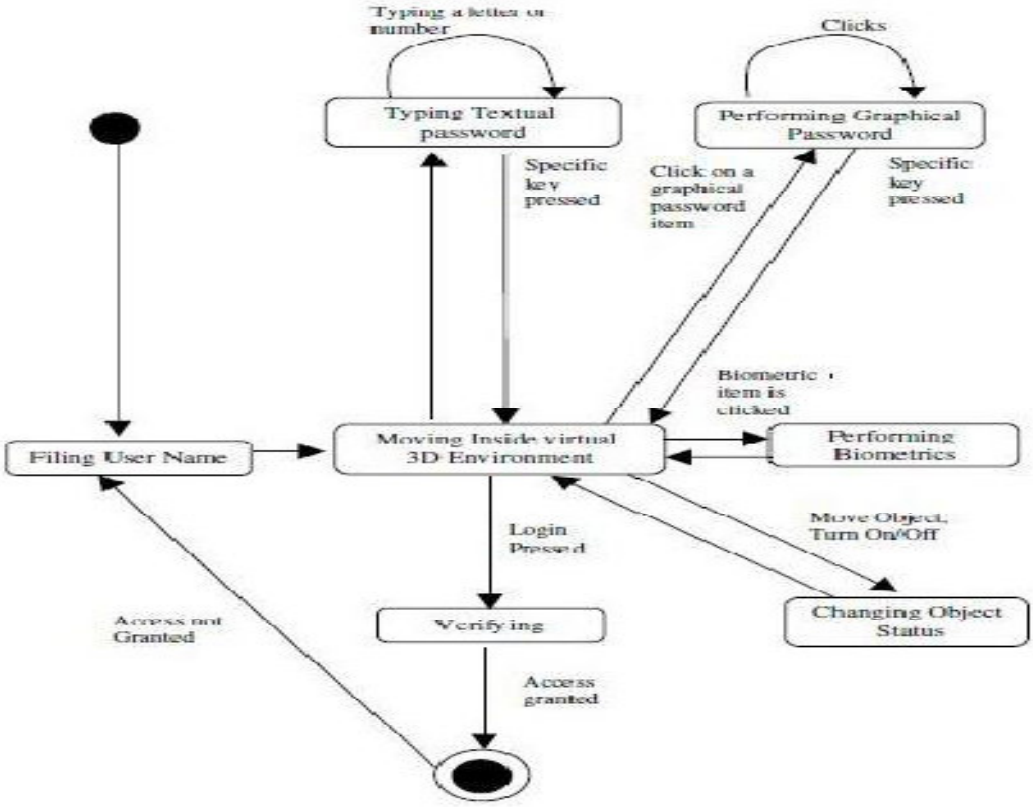


Fig 3 . system overview



State diagram

5.Analysis Of Voiced 3d Password Secure Authentication :

5.1 Attacks & countermeasures:

As mentioned earlier voiced 3D password is most secure authentication. We will see different kinds of attacks & how voiced 3D password scheme is more secure against different attacks.

5.1.1 Timing Attacks

This attack is based on how much time required completing successful sign-in using voiced 3D password scheme. Timing attacks can be very much effective while Authentication scheme is not well designed. But, as our voiced 3D password scheme is designed more securely, these kinds of attacks are not easily possible on voiced 3D Password & also not much effective as well.

5.1.2 Brute force Attacks

In This kind of attacks the attacker has to try n number of possibilities of voiced 3D Password. As these attacks considers following two points.

- Required time to login: as in voiced 3d password time required for successful login varies & is depend on number of actions & interactions, the size of 3d virtual environment.
- Cost required to attack: as voiced 3d password scheme requires 3D virtual environment & cost of creating such a environment is very high.

5.1.3 Well-studied attacks

In this attack attacker has to study whole password scheme. After studied about scheme the attacker tries combination of different attacks on scheme. As voiced 3d password scheme is multi-factor & multi-password authentication scheme, attacker fail to studied whole scheme. this attacks also not much effective against voiced 3D password scheme.

5.1.4 Key logger

In this attack attacker install as software called key logger on system where authentication scheme is used . This software stores text entered through keyboard & those text are stored in text file. In this way this attacks is more effective & useful for only textual password, but as voiced 3D password is multi password authentication scheme. So that this kind of attacks are not much effective in this case.

5.1.5 Shoulder Surfing attacks

Attacker uses camera for capturing & recording of 3D password. This attack is more effective than any other attacks on 3D password. So that 3D password must be performed in a secure place where this attack can‘t be

performed. Shoulder surfing attacks is still effective & easily possible against 3D password so we bind the voice password to the 3D password.

6.Implementation Fields :

6.1 Critical server: Many large organizations have critical Servers that are usually protected by a textual password . A Voiced 3-D password authentication proposes a sound replacement for a textual password.

6.2 Nuclear and military facilities: Such facilities should be protected by the most powerful authentication systems. The voiced 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.

6.3 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 voiced 3-D password is recommended for these systems.

6.4 Banking : some countries start working with 3D password. Almost all the Indian banks started 3D password service for security of users who wants to buy online or pay online. And who want to add security to their accounting bangs .

In addition, voiced 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

7.Conclusion And Results :

- The voiced 3D password scheme provide :
- *Flexibility:* voiced 3D Passwords allows Multifactor authentication biometric, textual passwords can be embedded in 3D password technology.
- *Strength:* This scenario provides almost unlimited passwords possibility. Shoulder-suffering attack is still can affect the schema of 3D password , so we add the Voiced 3D password to reduce that affect .
- *Easy to Remember:* can be remembered in the form of short story.
- *Privacy:* Organizers can select authentication schemes that respect users privacy.
- Draw back of voiced 3D password :
- Time and memory requirement is large.
- More expensive as cost required is more than other schemes.

References :

SECURED AUTHENTICATION: 3D PASSWORD* Duhan Pooja, Gupta Shilpi , Sangwan Sujata, & Gulati Vinita Department of Computer Science and Engineering, Dronacharya College Of Engineering, Gurgaon ISSN 2229-600X

Alsulaiman, F.A.; El Saddik, A., "Three- for Secure," IEEE Transactions on Instrumentation and measurement, vol.57, no.9, pp 1929-1938.Sept. 2008.

Secure Authentication with 3D Password Vishal Kolhe, Vipul Gunjal, Sayali Kalasakar, Pranjal Rathod Department of Computer Engineering, Amrutvahini Collage of Engineering, Sangamner ISSN: 2319-5967 ISO 9001:2008 Certified International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 2, March 2013

Vidya Mhaske et al, Int.J.Computer Technology & Applications, Vol 3 (2), ISSN: 2229-6093, 510-519.

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

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.

The IISTE is a pioneer in the Open-Access hosting service and academic event management. The aim of the firm is Accelerating Global Knowledge Sharing.

More information about the firm can be found on the homepage:
http://www.iiste.org

CALL FOR JOURNAL PAPERS

There are more than 30 peer-reviewed academic journals hosted under the hosting platform.

Prospective authors of journals can find the submission instruction on the following page: http://www.iiste.org/journals/ All the journals articles are available online to the readers all over the world without financial, legal, or technical barriers other than those inseparable from gaining access to the internet itself. Paper version of the journals is also available upon request of readers and authors.

MORE RESOURCES

Book publication information: http://www.iiste.org/book/

IISTE Knowledge Sharing Partners

EBSCO, Index Copernicus, Ulrich's Periodicals Directory, JournalTOCS, PKP Open Archives Harvester, Bielefeld Academic Search Engine, Elektronische Zeitschriftenbibliothek EZB, Open J-Gate, OCLC WorldCat, Universe Digtial Library , NewJour, Google Scholar