3D Graphical Authentication System

V.S. Tamboli[1], Kakade Shraddha [2], Asawa Sarvesh[3,] Cholke Anushka[4]

[1] Department of computer technology, PREC(Poly) Loni, India
[2]Department of computer technology, PREC(Poly) Loni, India
[3]Department of computer technology, PREC(Poly) Loni, India
[4]Department of computer technology, PREC(Poly) Loni, India

ABSTRACT

Current authentication systems suffer from many weaknesses. Textual passwords are commonly used; however, users do not follow their requirements. 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.
In this paper, we present and evaluate our contribution, i.e., the 3-D password. The 3-D password is a multifactor authentication scheme. To be authenticated, we present a 3-D virtual environment where the user navigates and interacts with various objects. The sequence of actions and interactions toward the objects inside the 3-D environment constructs the user's 3-D password.

Keyword: - *Authentication, Smartcard, Biometric, Textual Password,3D password.*

1. 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:

1. Textual passwords
2. Graphical passwords
3. Biometrics
4. 3D Passwords.

Users nowadays are provided with major password stereotypes such as textual passwords, biometric scanning, tokens or cards (such as an ATM) etc. Biometric scanning is your "natural" signature and Cards or Tokens prove your validity. But some people hate the fact to carry around their cards, some refuse to undergo strong IR exposure to their retinas (Biometric scanning). Mostly textual passwords, nowadays, are kept very simply say a word from the dictionary or their pet names, nickname etc. Years back Klein [1] performed such tests and he could crack 10-15 passwords per day. Now with the technology change, fast processors and many tools on the Internet this has become a Child's Play.

Therefore, we present our idea, the 3D passwords which are more customizable and very interesting way of authentication. Now the passwords are based on the fact of Human memory. Generally simple passwords are set so as to quickly recall them. The human memory, in our scheme has to undergo the facts of Recognition, Recalling, Biometrics or Token based authentication. Once implemented and you log in to a secure site, the 3D password GUI opens up. This is an additional textual password which the user can simply put. Once he goes through the first authentication, a 3D virtual room will open on the screen.

2. LITERATURE REVIEW AND OBJECTIVE

2.1 Literature Review

[1] Dhatri Raval, in her paper explains about the various already available password authentication schemes such as knowledge based, token based, recognition based, biometrics based.

[2] Parul, Neetu Verma, in their paper discuss about the drawbacks of the already available authentication schemes. They explained that people use textual passwords which are easy to remember and they can be cracked easily using Brute force attacks.

[3] Nayana S, Dr. Niranjanamurthy, Dr. Dharmendra Chahar, in their paper explains about the advantages and disadvantages of the 3D password. They explained that the 3D password is better than the other existing authentication systems but on the other hand it is expensive.

[4] Tejal M. Kognule, Monica G. Gole, Priyanka T. Dabade, Sagar B. Gawade, in their paper explains about the objects inside the 3D virtual environment. They found that the objects must be clearly visible and identical to each other.

[5] Mrs Ashwini B P, Ms Bhumika J, Ms Chinmayee T S, Mr. G M Akshay Bhat, Mr Naveen Kumar N, in their paper explain about the goals of the 3D password scheme. They explained that the 3D password must be the combination of both recall-based and recognition-based authentication techniques and these are not easy as to write on paper as they are coordinates.

[6] Ganesh Jairam Rajguru, in his paper he focuses on how the 3D password can be generated. And how they can be represented on a 2D screen.

[7] Parag Vade, Vaidehi Rahangdale, Saurabh Veer, in their paper focuses on the mathematical concepts related to 3D password scheme. They discuss on the time complexity, space complexity and the class problem related to the 3D password.

[8] Sahana R. Gadagkar, Aditya Pawaskar, Mrs Ranjeeta B. Pandhare, in their paper discuss about the design of the 3D environment. They also discussed about the length of the 3D password based on the design of the System.

[9] Anagha Kelkar, Komal Mukadam, in their paper discussed about the devices required to develop the 3 D password authentication systems. They mostly focussed on the input devices through which the user interacts the 3 D environment.

[10] P.K. Dhanya, M. Keerthiga, S Dinakar, in their paper discussed on the various attacks that are being done on the already available authentication schemes. They explained about Brute force attack, timing attacks, well studied attacks etc.

2.1 Objective

Objective is to provide a more secured and strong authentication system for various important systems without traditional authentication schemas such as Textual passwords, Graphical passwords, Biometrics,3D Passwords and to provide authentication with the 3D environment by click points which will be not guessed by any unauthorized user.

3. Materials and Methods

This is the system architecture of the 3D authentication system.
There are many authentication systems are available now a days like textual and graphical password, smart cards, biometrics scan etc. But all of this have some drawbacks such as textual passwords can be guessed easily, smart cards can be stolen, for biometrics scan users tend to resist using biometrics because of their intrusiveness and the effect on their privacy. but this system has the combination of textual password and points from provided image and 3D environment. User have to enter the password and have to click on the appropriate point to get access to the secured system. User have to select single point first and then have to select multiple points(4) for registration.

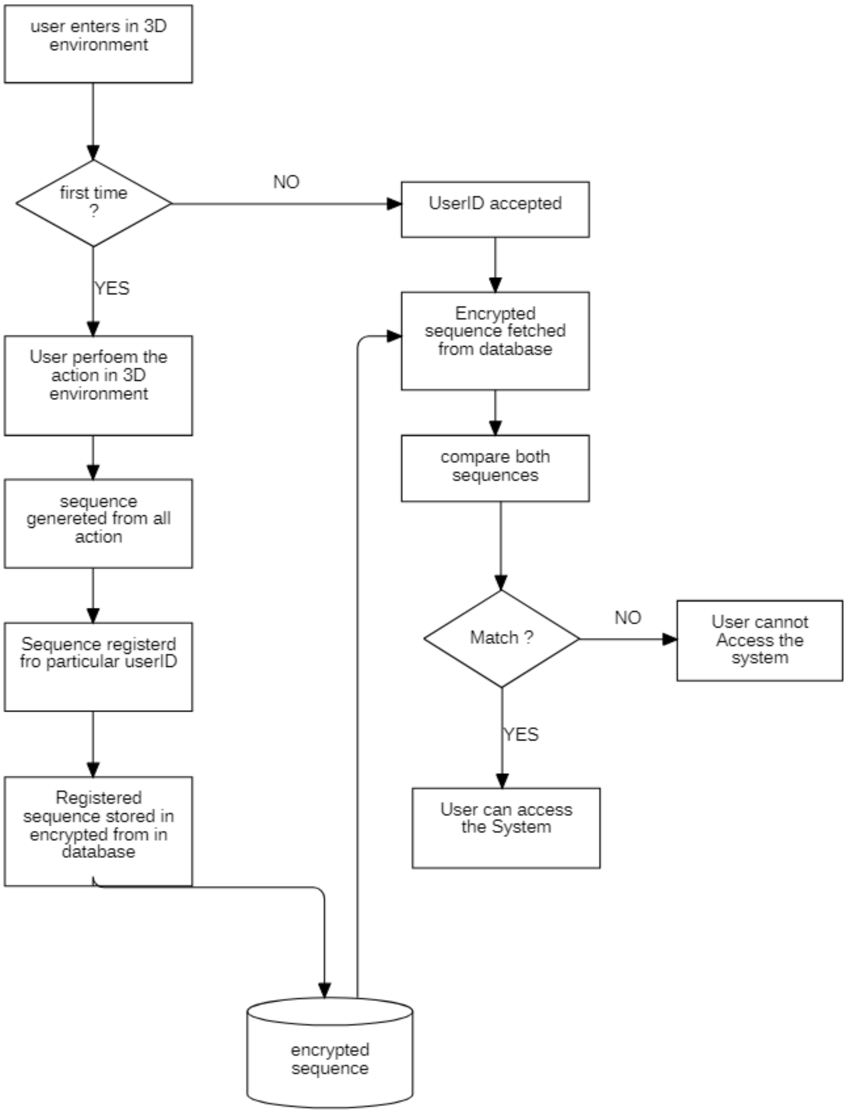
user enters in 3D environment
first time ?
NO
UserID accepted
YES
User perfoem the action in 3D environment
sequence genereted from all action
Sequence registerd fro particular userID
Registered sequence stored in encrypted from in database
encrypted sequence
Encrypted sequence fetched from database
compare both sequences
Match ?
NO
User cannot Access the system
YES
User can access the System

Fig -1: System Architecture

4. CONCLUSIONS

There are many authentication schemes in the current state. Some of them are based on user's physical and behavioral properties, and some other authentication schemes are based on user's knowledge such as textual and graphical passwords. Moreover, there are some other important authentication schemes that are based on what you have, such as smart cards. Among the various authentication schemes, textual password and token-based schemes, or the combination of both, are commonly applied. However, as mentioned before, both authentication schemes are vulnerable to certain attacks. Moreover, there are many authentication schemes that are currently under study and they may require additional time and effort to be applicable for commercial use, but this proposed, 3D authentication project have the potential to secure the applications such as banking applications, with both the textual password with the selection points from 3D environment.

5. ACKNOWLEDGEMENT

With deep sense of gratitude, we would like to thanks all the people who have lighted our path with their kind guidance. We are very grateful to these intellectuals who did their best to help during our project work.

It is our proud privilege to express deep sense of gratitude to, Prof. Rathi of Padmashri Dr. Vitthalrao Vikhe Patil Institute of Technology and Engineering (Polytechnic), Loni, for his comments and kind permission to complete this project. We remain indebted H.O.D Kakade Sir of Computer Technology Department for their timely suggestion and valuable guidance.

The special gratitude goes to all the staff members, technical staff members, of Computer Technology Department for their expensive, excellent and precious guidance in completion of this work. We thanks to all the colleagues for their appreciable help for our working project.

We are also thankful to our parents who have provided their wishful support for completion of our project work successfully.

And lastly, we thanks to all our friends and the people who are directly or indirectly related to our project work.

6. REFERENCES

[1] D. V. Klein, “Foiling the cracker: A survey of, and improvement to passwords security,” in Proc. USENIX Security Workshop, 1990, pp. 5–14.

[2] 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] NBC news, ATM Fraud: Banking on Your Money, Dateline Hidden Cameras Show Criminals Owning ATMs, Dec. 11, 2003.

[4] T. Kitten, Keeping an Eye on the ATM. (2005, Jul. 11). [Online] Available: Marketplace’s Table - Resulting number of possible 3-d passwords of total length Lmax om

[5] BBC news, Cash Machine Fraud up, Say Banks, Nov. 4, 2006.

[6] Table - Resulting number of possible 3-d passwords of total length Lmax Table - Resulting number of possible 3-d passwords of total length Lmax

[7] G. E. Blonder, “Graphical password,” U.S. Patent 5 559 961, Sep. 24, 1996.

[8] R. Dhamija and A. Perrig, “Déjà Vu: A user study using images for authentication,” in Proc. 9th USINEX Security Symp., Denver, CO, Aug. 2000, pp. 45–58.

[9] Real User Corporation, The Science Behind Passfaces. (2005, Oct.).