Study and Importance of 3D Password

Chanda Patel[1] Rakesh Patel[2] Sushma Gupta[3]
[1,3]B.E. Student [2]Lecturer
[1,2,3]Department of Information Technology
[1,2,3]Kirodimal Institute of Technology, Raigarh(C.G.),India

Abstract— Existing systems of authentication are plagued by many weaknesses. Commonly, textual passwords are used to secure data or user accounts. However these can be cracked by the application of various brute-force algorithms as the maximum password length is fixed and there are a finite number of possibilities which exist. The 3D password authentication scheme is based on a combination of multiple sets of factors. A 3D virtual environment is presented to the user where he navigates and interacts with a multitude of objects which are present. The order in which actions and interactions are performed with respect to the objects constitutes the user's 3D password.

Key words: 3D Password, data mining, Web data

I. INTRODUCTION

Generally there are four types of authentication techniques are available such as:

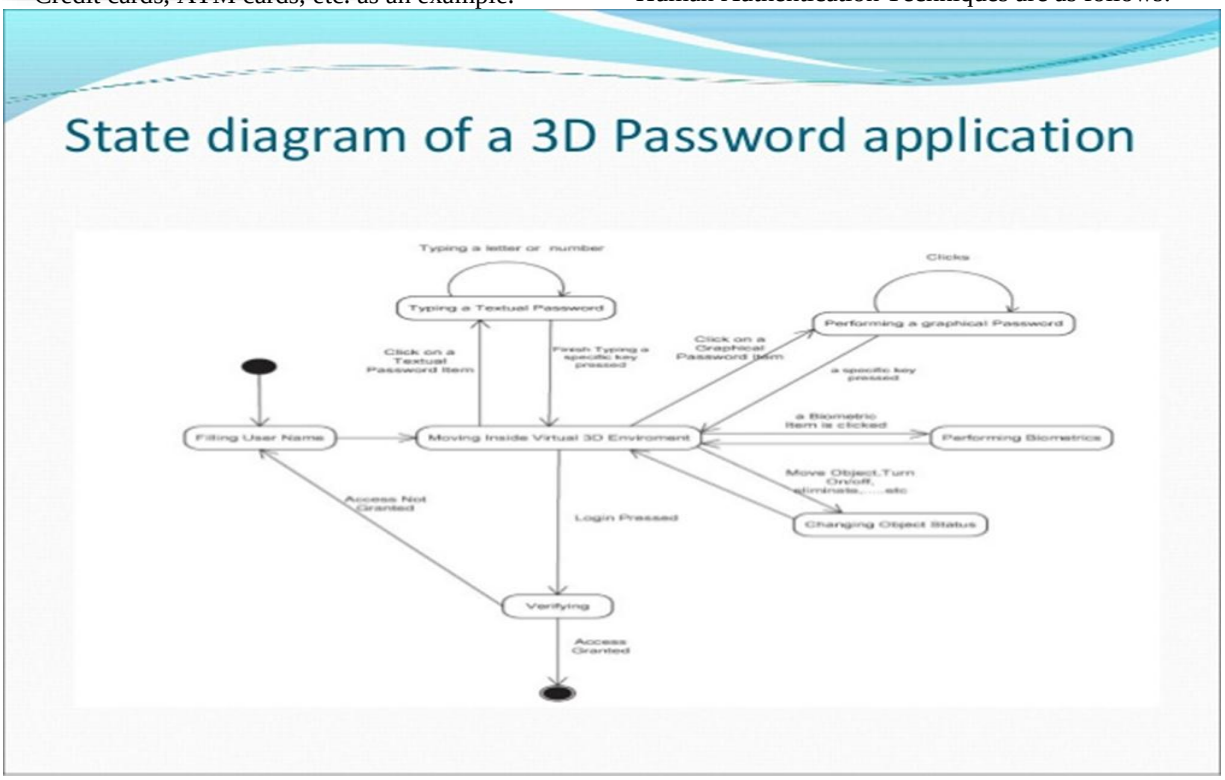
- Knowledge based: means what you know. Textual password is the best example of this authentication scheme.
- Token based: means what you have. This includes Credit cards, ATM cards, etc. as an example.
- Biometrics: means what you are. Includes Thumb impression, etc.
- Recognition Based: means what you recognize. Includes graphical password, iris recognition, face recognition, etc.

Ideally there are two types of Authentication schemes are available according to nature of scheme & techniques used, those types are

1) Recall based: In this authentication tech. user need to recall or remember his/her password [4]
2) Recognition based: In this user need to identify, recognize password created before. [4]
3) Graphical password. Generally this technique is not use much more as Recall based is used.

II. AUTHENTICATION

Authentication is a process of validating who are you to whom you claimed to be or a process of identifying an individual, usually based on a username and password. Human Authentication Techniques are as follows:



Knowledge Base (What you know)

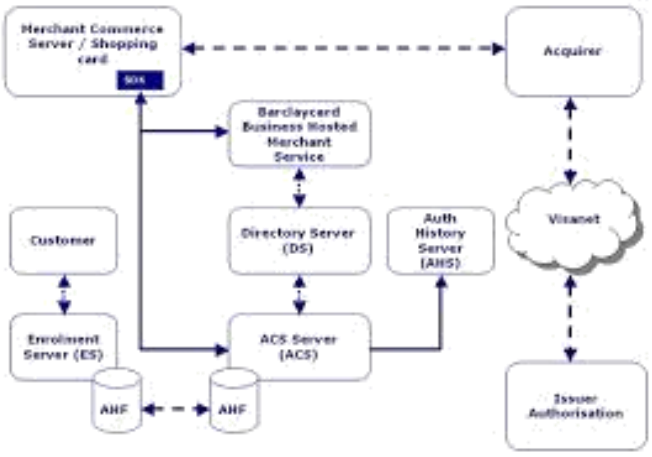
- Token Based(what you have)
- Biometrics(what you are)
- Recognition Based(What you recognise)
- Computer Authentication Techniques are as follows:
- Textual Passwords (Recall Based)-Recall what you have created before.
- Graphical Passwords (Recall Based + Recognition Based)
- Biometric schemes (fingerprints, voice recognition etc)

A. History

Users commonly use textual passwords, but do not take their recommendations into account. They are inclined to select words of significance from dictionaries, making then liable to dictionary or brute force attacks. [3]A number ofgraphical passwords also have a password space that is lesser than or equal to the textual password space. Other forms of authentication also taken into account what is possessed by the user in addition to what is known by them, a common example being token based systems that are used in banking. These arenevertheless susceptible to fraud, loss or theft.

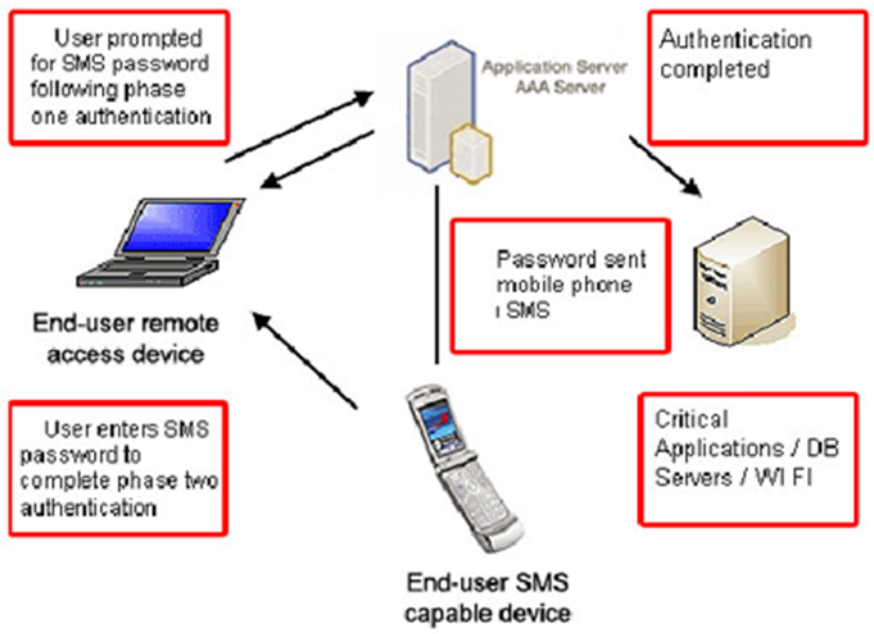
B. 3D Password Scheme

The advantage of the 3D password is that it can combine many existing systems of authentication, providing an extremely high degree of security to the user. [2 The order in which actions and interactions are performed with respect to the objects constitutes the user's 3D password. A 3D virtual environment is presented to the user where he navigates and interacts with a multitude of objects which are present. The order in which actions and interactions are performed with respect to the objects constitutes the use's 3D password. The 3D password key space is built on the basis of the design of the 3D virtual environment and the nature of the objects selected. The advantage of the 3D password is that it can combine many existing systems of authentication, providing an extremely high degree of security to the user.



Biometrics- Biometric systems can operate in two modes, the first being verification mode and the second being identification mode. In verification mode, the system compares a captured biometric with a template which has been stored in a biometric database such that the user can be successfully authenticated. . The final step is testing. This may involve the use of a smart card, username or identification number such as a PIN indicating which template must be used for comparison. In successive uses, biometric information is detected and matched with the information that has been stored at the time of enrollment. Security during the stages of storage as well as retrieval is of essence in order to make sure that the biometric system is robust. Biometric systems can be coupled with the 3D password to further increase the degree of security, making it extremely secure and suitable for applications in which information security is of essence. Several techniques like face recognition, fingerprint recognition, hand geometry, iris recognition, and palm print, vascular pattern recognition can be used. Pins and passwords may be forgotten and token based identification methods such as passports and driver licenses may be forged, stolen, or lost. Thus the biometric system of identification enjoys a new interest. It can even be applied in the most basic level such as for a user on a home system as it is based on recall on recognition and is easy to use. Biometrics or biometric authentication is used to identify human beings on the basis of their characteristics or traits. It is commonly used as a form of identification and access control. Biometrics identifiers are the different characteristics which can be measured that can be used to identify individuals. There are two categories of biometric identifiers; these include physiological and behavioral characteristics. Biometric functionality encapsulates a variety of different aspects. Selecting the use of a particular biometric for a specified application must take several factors into

1) Universality: Every person using the system should possess the trait.
2) Uniqueness: The trait must be unique to each individual who uses the system such that they can be distinguished from one and another.
3) Permanent: The trait should be permanent and invariant over time.
4) Measurability (Collectability): This refers to the ease with which the trait can be acquired or measured.
5) Performance: This refers to the accuracy, speed and robustness of the technology that is being used.
6) Acceptability: This encompasses how ready individuals are to have their trait captured and
7) Circumvention: This measures how easy it is for a trait to be emulated by making use of an artifact or a substitute. It is unlikely that a single biometric system will meet the needs of all applications



III. MATERIALS AND METHODS

Here the designs of two 3D environments are specified, the first one being a chess game and the second being a rotating cube. In the chess game, the password is based on placing the chess pieces in predefined positions on the chess board and in the case of the rotating cube, the password is constructed base on rotating the cube right, left, up and down in addition to the option of inserting one of the input images on different sides of the cube.

A. Environment 1 – Chess:

When a new user enters the environment, the user must initially enter all his details in the registration form. The user must then click on the environment1 button to select the chess environment. Figure 2[1] below shows an environment for a chess game, having a total of 32 objects, out of which 16 are red and 16 are white. It also encloses seven buttons all together namely, New button, Record button, Stop button, Play button, Confirm button, Close button and Swap button, and one Checkbox option. Each button works as specified

1) New button:
Clicking this button initializes all the objects (white and red). Prior to clicking this button, the environment is completely empty.

2) Swap button:
This button is used in order to change the position of the red and white objects. In simple words, it exchanges the positions of the white and red objects

3) Record button:
Before creating the 3D password, the user must click this button, as a result of which the sequence of actions and interactions are stored as the 3D password as a string. In the event that the record button has not been clicked initially, nothing is recorded and an error occurs when the user slicks the stop button.

4) Stop button:
This button is used to end the sequence of actions and interactions. Clicking this button stops recording the user‟s movements and the recorded actions and interactions are saved as a 3D password in the form of a string.

5) Play button:
This button can be used by to user to check the actions and interactions that have been performed after pressing the stop button. Once this button is clicked, the user can see a playback of the actions and interactions which have been stored as a 3D password.

6) Confirm button:
This button confirms the 3D password. Once this button is clicked, the user cannot change the 3D password. The user can however, change his/her password prior to clicking this button by selecting the new button.

7) Close button:
Once clicked, the environment is closed and control returns to the registration form.

B. Environment

Cube: The second environment presented in this paper is that of a cube. When this environment is selected, the cube is placed at an initial position of (400, 240, 0) co-ordinates with respect to the x, y and z axis. In addition to this point in the environment, another point known as the camera point is fixed. The camera position is set at the co-ordinates (400, 240,-500) on the x, y and z axis respectively. It is a reference point, or the point from which the user can see the sequence of actions and interactions that are being performed on the cube.
The four main actions are described below [1]:

1) Move Cube:
This is a main move cube action having the following six sub actions, Left, Right, Up, Down, In, Out. A click on each of these buttons translates the cube by 45 co-ordinates with respect to which button are clicked.

2) Rotate Cube:
This main action has the following sub actions, rotate cube x-direction, y-direction, z- direction and –x-direction, -y-direction, -z-direction. A single click on one of these buttons will rotate the cube in a 45° direction with respective to which button is clicked.

C. Advantages

- 3D Password scheme is combination of re-call based, recognized based, Biometrics etc. into single authentication technique [1].
- Due to use of multiple schemes into one scheme password space is increased to great extent.
- More secure authentication scheme over currently available schemes.

D. Disadvantages

- Time and memory requirement is large.
- Shoulder-suffering attack is still can affect the schema.
- More expensive as cost required is more than other schemes.

E. Applications:

As 3D password authentication scheme is more useful & more secure than any other authentication schemas, 3D password can be used in wide area where more security is needed to system. Some of areas are as follows:

1) Networking:

Networking involves many areas of computer networks like client-server architecture, critical servers, etc. To provide more security to server of this architecture 3D password can be used. It very efficient & more secure way to keep data or important information secure from unauthorized people. For email applications 3D password is most secure & easier scheme to used.

2) Nuclear & military areas

Nuclear & military area of a country are most important area where more security is needed we can use 3D password scheme in this area for more providing more secure authentication. 3D password scheme can protect data or secrete information about these areas very securely.

3) Airplane & jetfighters

There is possibility of misuse of airplanes and jetfighters for religion-political agendas. 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 [1] [4] [6].

4) Banking:

Almost all the Indian banks started 3Dpassword service for security of buyer who wants to buyonline or pay online.

5) Other areas

we can use 3d password authentication scheme to areas such as ATM, Cyber cafes, Industries (for data security), Laptop‘s or PC‘s, critical servers, web services, etc & many more [1]-[4],[6][7].

IV. Conclusion and Future Work

Currently available schemes include textual password and graphical password .But both 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. The 3-D password is a multifactor & multi password authentication scheme that combines these various authentication schemes.[3] In 3D password system as number of series of action and interaction in the hypothetical 3D environment increases then the length of the codeword also increases. The amount of memory that is required to store a 3D password is large when compared to a textual password.[1]In the existing system, Textual passwords and token-based passwords are the most common used authentication schemes A 3Dpassword’s probable password space can be reflected by the design of the three-dimensional virtual environment, which is designed by the system administrator. The three-dimensional virtual environment can contain any objects at the administrator feels that the users are familiar with. For example, Cricket players can use a three dimensional virtual environment of a stadium. [2]

Reference

[1] 3d Password: Minimal Utilization Ofspace And Vast Security Coupled Withbiometrics For Secure Authentication Ms. Nidhi Maria Paul, Student, Nagarjuna College of Engineering and Technology; Ms. Monisha Shanmugham, Student, Nagarjuna College of Engineering and Technology

[2] Secured Authentication:
3D PASSWORD Department of Computer Science and Engineering, Dronacharya College Of Engineering, Gurgaon* Duhan Pooja, Gupta Shilpi , Sangwan Sujata, & Gulati Vinita.

[3] Secure Authentication with 3D Password

Department of Computer Engineering, Amrutvahini Collage of Engineering, Sangamner Vishal Kolhe, Vipul Gunjal, Sayali Kalasakar, Pranjal Rathod
[4] Secure Authentication with 3D Password
Vishal Kolhe, Vipul Gunjal, Sayali Kalasakar, Pranjal Rathod
[5] Alsulaiman, F.A.; El Saddik, A., "Three- for Secure," IEEE Transactions on Instrumentation and measurement, vol.57, no.9, pp 1929-1938.Sept. 2008.
[6] Vidya Mhaske et al, Int.J.Computer Technology & Applications, Vol 3 (2), ISSN: 2229-6093, 510-519.
[7] Prof. Sonkar S.K.; Dr. Ghungrad S.B., "Minimum Space and Huge Security in 3D Password Scheme", International Journal of Computer Applications (0975-8887), Volume 29-No.4, September 2011
[8] Alsulaiman, F.A.; El Saddik, A., "Three- for Secure," IEEE Transactions on Instrumentation and measurement, vol.57, no.9, pp 1929-1938.Sept. 2008
[9] D. V. Klein, ―Foiling the cracker: A survey of, and to passwords security,‖ in Proc. USENIX Security, pp.–14

