Anarchy to Data Security- 3D Password: A Review

Rahul Lohiya[1], R. K. Gupta[2]
[1]*Research Scholar, Department of CSE & ITM.I.T.S., Gwalior, Madhya Pradesh, India*
[2]*Professor and Head, Department of CSE & ITM.I.T.S., Gwalior, Madhya Pradesh, India*
lohiya001@gmail.com
iitm_rkg@rediffmail.com

***Abstract*- Password, one of the effective and easy solutions recommended today for securing the highly confidential data. Though there are many efficiently implementations performed for password strength. The strength may range from simple password combination of alphanumeric and special characters to finger prints and face recognition techniques. But these methods have not been proven as the adequate resolution to the problem. In this regard, 3-D password has come out as one of the best solution for the password strength. The 3-D password is a multifactor authentication scheme, though customized according to user choice is a combination of textual passwords, graphical passwords and various types of biometrics into a 3-D virtual environment.**

***Keywords* - Biometrics, Graphical passwords, Textual passwords, Token-based scheme, 3-D virtual environment.**

Introduction

The widespread usage of computer has leaded the concern of security against data. Though numerous innovations have been made in computer security, various schemes are available specializing towards securing the arcane data. The authentication to this data needs to be provided for limiting the access by user. Authentication can be defined as a process by which a system verifies the identity of a user who wishes to access it. Since Access control is normally based on the identity of the user who requests access to a resource, it is essential for effective security. In general, human authentication techniques can be classified as knowledge based (what you know), token based (what you have), and biometrics (what you are) [1]. The knowledge based authentication can be further categorized as: Recall based, which require the user to repeat or reproduce a secret that user created; Recognition based, which require the user to identify and recognize the secret, or its part, that the user selected. The authentication can be done in the form of a password.

A password is a secret aggregation of alphanumeric and special characters that is used for authentication, to validate identity or grant access to a resource. The password can be textual, graphical, biometrics, token based and also naive 3-D password.

Textual passwords are kept very simple say a word from the dictionary or the pet names, friends etc hence are weak and susceptible to numerous types of attacks. It's the user ability for security to maintain the user ID and password secret.

Klein [2] acquired a database of nearly 15,000 user accounts that had alphanumerical passwords, and stated that 25% of the passwords were guessed using a small, yet well formed dictionary of (3×10^6) words.

Graphical passwords are hinged on the conception that users can recall and recognize pictures better than words. In theory, graphical passwords are easier to remember since human remembers pictures better than words [5]. 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 [1].

Biometric authentication scheme adverts to a wide range of technologies which automate the identification or verification of an individual. Based on human characteristics or body organs biometric authentications are: Physiological: face, fingerprint, iris; and Behavioral: hand-written signature, voice.

Token based authentication scheme is a security technique that authenticates the users to attempt to login to a server, a network, or some other secure system, using a security token provided by the server. The token are of two types: Hardware Token involves additional costs, such as the cost of the token and any replacement fees. The user needs to carry the token along with them. Also he/she needs multiple tokens for multiple websites and devices; Software Token requires some amount of user training, along with the reinstallation and configuration in case of operating system corruption or problem.

The 3-D password offers a virtual environment with various virtual objects. The user pace through the environment and interacts with these objects. The 3-D password is simply the combination and arrangement

of user interactions that occur in the 3-D environment. The user who adopts to keep biometric data private might not need to interact with the objects that require biometric information. Hence, it is the user's exquisite and decision to construct the desired and preferred 3-D password.

The further discussion in the paper includes 3-D password scheme along with its outline, selection and inputs, 3-D virtual environment design percept, and application; security analysis; and conclusion and future work.

II 3-D Password Scheme

The fact that vulnerabilities exist in preexisting password schemes, researchers are thinking of a password and authentication scheme, which is more efficient in terms of security. The scheme can be a multi factor authentication scheme which can use combination of textual password, graphical password, token based password and biometric password for authentication purpose. It can be used address the shortcoming of the existing schemes.

A. 3D Password Outline

A three dimensional password is a new authentication technique which can be used to render the high security to the data from the unauthorized user by combining recall based, recognition based, token, graphical and textual password into one authentication system. The 3D password is simply the unification and the subsequence of user interactions that occur in the 3-d virtual environment. The idea is too simple; the user interacts through virtual objects in the virtual environment which is present in the 3D space. The interaction can be done by designing the 3-D virtual environment which contains some virtual objects. It can be understood with the help of an example.

Let the user first enters in the virtual environment and open the door of a room which is at the position of (x1, y1, z1). After opening the room, user arrives into the room and look toward the computer which is at the (x2, y2, z2) position and enter the password, and then enters into the virtual garage having the iris scanner that exist at (x3, y3, z3) position and provide his/her iris scanning. Now, the user can go to the car and open the car door, to switch the radio at the specific channel. The combination and sequence of these steps with virtual objects are used to make 3-D password.

Virtual objects can be of any type which is present in the real world or in our real life. It can also be the objects that usually deal in the daily life. Moreover the task performed by the user like walking at particular place, speaking on a particular location can be considered as an input and can be used as a part of 3-d password. We can use some objects for the authentication purpose which are as follows:

1. A computer on which the user can type.
2. A white board that a user can drawn on
3. A light that can be switched on/off.
4. Any biometric device.
5. Any real life objects
6. A car that can be driven.
7. A staple that can be punched.
8. Any graphical password scheme.
9. An ATM machine that require a smart card and PIN.
10. Any upcoming authentication scheme.

Here the same object can play different role in the password. The action of one object which exist at the location of (x1, y1, z1) coordinates is different from the same object located at different location say (x2, y2, z2) where $x1 \neq x2$, $y1 \neq y2$ and $z1 \neq z2$. Therefore, to perform the legitimate 3-D password, the user must follow the same scenario performed by the legitimate user [1].

I. B. *3D Password Selection and Inputs*

The 3-D password can be made by selecting the environment and providing inputs to it. Consider a 3-D virtual environment having the size G×G×G. Every point can be expressed by the coordinates (x, y, z) ϵ [1…G] × [1...G] × [1...G]. All objects are distributed around the 3-D virtual environment with its own and unique (x, y, z) coordinates. Now just take into consideration that user cat navigate into the 3-D virtual environment and comes into the touch with the objects using any input device like computer, scanner, camera to take pictures, iris scanner, mouse, keyboard, microphone etc. The sequence of actions and interactions using the previous input devices are considered as the user's 3-D password. For example, let us assume a user who interacts through the 3-D virtual environment that consists of a department and a computer room. Let us assume that the user is in the virtual department and the user turns around to the door located in (15, 24, 06) and opens it. Then, the user closes the door. The user then finds a computer to the left of the computer lab, which exists in the position (6, 51, 18), and the user types "GWALIOR." Then, the user walks to the computer lab and picks up a pen located at (42, 33, 60) and draws only one dot in a paper located in (1, 18, 30), which is the dot (*x*, *y*) coordinate relative to the paper space is (330, 130). The user then presses the login button. The initial representation of user actions in the 3-D virtual environment can be recorded as follows

(15, 24, 06) Action = Open the office door;
(15, 24, 06) Action = Close the office door;
(6, 51, 18) Action = Typing, “G”;
(4, 34, 18) Action = Typing, “W”;
(4, 34, 18) Action = Typing, “A”;
(4, 34, 18) Action = Typing, “L”;
(4, 34, 18) Action = Typing, “I”;
(4, 34, 18) Action = Typing, “O”;
(4, 34, 18) Action = Typing, “R”;
(42, 33, 60) Action = Pick up the pen;
(1, 18, 80) Action = Drawing, point = (330, 130).

It is only an example. We can take any example to understand it which define that for the 3-D password authentication, user has to follow the same sequence and type of actions and interactions towards the objects. Fig shows the virtual environment which is basically for the experimental purpose.

Figure (1): Snapshot of proof of concept three-dimensional virtual environment. A virtual art gallery consisting of 36 pictures and 6 computers, where users can navigate and interact with virtual objects by either typing or drawing. [7]

C. 3-D Virtual Environment Design Percepts

3D password Authentication scheme’s effectiveness, usability and acceptability are influenced by the design of 3D virtual environment. Therefore designing a well studied 3D virtual environment is indispensable that reflects legislation’s compulsion and security requisites. The design of 3D virtual environments should follow these guidelines –

1. Real-Life similarity**:** The anticipated 3D virtual environment should be realistic what user used to seeing in real life. Objects in virtual environment are closely similar in shape of real objects, size may be scaled. Also the action and interaction towards these objects are imitated as in real scenario.
2. Object uniqueness and distinction: All the virtual objects or items inside 3-D virtual environment should be distinct. Objects may perceptibly synonym but they should distinct by their attributes such as position. Hence interaction with 1 object is not similar to other. If the objects are similar like 20 computers in one place then they should be designed such that user might not get confused.
3. Three dimensional virtual environment sizes and its object design: An office or a city or even the world can be illustrated by a 3-D virtual environment. Therefore the size of 3-D virtual environment is dependent on the desired system.

A large 3-D virtual environment will increase the time required by the user to perform the task. Also, a large 3-D virtual environment can contain ample of virtual objects. Therefore, the probable 3-D password space broadens. On the other side, asmall3-Dvirtual environment usually contains only a lesser number of objects, and hence, performing a 3-D password will take less time.

The type of object and its number assist in designing 3-D password and depict the importance of the protected system. The object type such as textual password or fingerprint reflects the response of the object. Selecting the right object response types and the number of objects affects the probable password space of a 3-D password [1].

D. 3-D Password Application

In advert to the 3-D password implementation, its large space compared to other application schemes has provided predominant application in protecting crucial systems and resources. These may include the following:

1. Critical Servers: Large organizations having huge critical data may adopt 3-D password as a compelling option in place of textual passwords in scenario. The entrance to these sites is generally protected by access cards or sometimes PIN numbers. Therefore, a 3-D password may be used as an option to protect the entrance to such locations and protect the usage of such servers.
2. Nuclear and Military Facilities: The equipment used in military area should be protected by some powerful authentication scheme because unauthorized access to these equipments may prove hazardous. Thus 3-D password provides a very substantial solution by offering a large

probable password space hence is a vital option for high level security locations.

3. Airplanes and Jetfighters: To protect the airplanes and jetfighters from exploitation, forcible authentication scheme such as this, 3-D password well suited preference due to its multifactor authentication feature.
4. Banking: Almost all the Indian banks started 3D password service for security of buyer who wants to buy online or pay online.[8]

II. Security Analysis

The stability of the password determines the adversity for the attacker to smash down the system. The study and the analysis for its measurement are based on the information content of the password space. It may be defined as "the entropy of the probability distribution over that space given by the relative frequencies of the passwords that users actually choose" [4]. As the textual passwords are easy to crack by the assailant, it is encouraged to have following two factors:

1. A scheme having large password space in 3-D password as it will require more efforts to be put by the attacker/assailant to break the authentication system.
2. To searchfor a scheme that has no prior or existing knowledge of themost probable user password selection and which may also resistthe attack on such an authentication scheme.

A. 3-D Password space size

The time required to attack an authentication mechanism depends on the size of the password space. Thus to determine password space of 3-D password it is desired to count a convinced number of actions, interactions, and inputs towards all objectsin the 3-D virtual environment. It is assumed that the length of the 3-D password is L_{max}, and the portability of the 3-D password of size greater than is L_{max} is zero. For measuring the 3-D password space, $\Pi(L_{max},G)$ is calculated on a 3-D virtual environment that has the space(G×G×G) for a 3-D password of length (number of actions, interactions, and inputs) of L_{max} or less.

$$\Pi(L_{max},G) = \sum_{n=1}^{n=L_{max}} \left(m + g(AC)\right)^n \quad (1)$$

Here, AC represents the possible actionstowardthe3-Dvirtualenvironment, whereas Π represents the total number of possible 3-D passwords of length L_{max} or less [1].

$$m = \sum_{i=1}^{i=O^{max}} h(O_i, T_i, x_i, y_i, z_i) \quad (2)$$

Here, O^{max} is the number ofobjects in the 3-D virtual environment, where $x_i = x_i$, $y_i = y_j$, and $z_i = z_j$, only if i = j.

The design of the 3-D environment will arbitrate the value of O^{max}. The variable m represents all possible actions and interactions toward all existing objects O_i. g(AC) in equation (1), counts the total number of actions and inputs toward the 3-D virtual environment,whereas m in equation (2), counts the actions and interactions toward the objects.

$$h(O_i, T_i, x_i, y_i, z_i) = f(O_i, T_i, x_i, y_i, z_i) \quad (3)$$

Is a function defined as the number of possible actions and interactions toward the object O_i, based on the object type T_i. Object types can be textual password objects, DAS objects, or any authentication scheme [7].

The function in equation (3) is determined from the object type, countsthe possible actions and interactions that the object can accept. As discussed earlier, an object type is oneof the important factors that affects the overall password space.Therefore, higher outcomes of function f imply larger 3-D password space size.

From all the three equations, it is observed that the numberof objects and the type of actions and interactions determinesthe probable password space. Therefore, the design of the 3-D virtual environment is a very sophisticated part of the 3-D passwordsystem.

B. 3-D Password Distribution Knowledge

Users probably use the passwords which have some meaning and some type of relation with him/her, which is the key for the dictionary attack. Dictionary attack makes the success rate too high for breaking the textual password. Any Authentication scheme is affected by the knowledge distribution of the user's secrets [1]

The 3-d password uses the combination of multiple passwords for providing the security, and the knowledge about the selection of different password is not available till now for the attacker so it is very difficult to break. The tasks become very difficult due to the presence of different authentication scheme into same 3-d environment. However in order to get such knowledge, attacker must have the prior knowledge of all the passwords which are being used in the 3-d environment for the authentication purpose. For example attacker should have the knowledge of most of the textual passwords, various kind of graphical passwords, which user use probably.

III. Conclusion and Future Work

Since the 3-D password is a novel approach towards the confidentiality of data. It has come to light in the direction of revolution in data security. The 3D password is just introduced means it is in its childhood [8]. This revolution by 3-D password may flourish out the sinful minds of the assailants. Though the textual passwords, biometrics, token based passwords and graphical passwords have been sufficiently accepted as convincing schemes, these schemes are imprecise yet as they still come across few shortcomings. 3-D password on behalf of all these schemes provides better consequence by managing multifactor strategy that combines these various authentication schemes into a single 3-D virtual environment. Also it is the user's preference that what authentication schemes will be the part of the 3-D password. If user do not prefer any biometric authentication then interaction with the biometric objects in the 3-D virtual environment is not desirable. Hence user is free to construct their own desirable 3-D password by skipping the hassle authentication mechanisms.

Although it has been an efficient scheme studied, it instead been analyzed some imperfections. As it is the combination of various authentication schemes, it may experience following shortcomings:

- Password Recovery in 3-D password may prove rigid, whereas it is simple to recover passwords in other schemes.
- It becomes too much complex to develop such a system.
- It may become time consuming as it might employ more time in authentication.
- It solely relies on the GUI dominantly. In case Graphical User Interface crashes, the entire security system suffers.

Thinking out the above mentioned shortcomings, the perspectives in this approach is gathering attackers from different backgrounds to crack the system that will lead to system improvement and also might prove the complexity of breaking a 3-D password. Above this, it will evidence how the attackers will gain the knowledge of the approximate 3-D passwords to drive their attacks. One possible threat still against 3-D password is Shoulder Surfing Attack which needs to be handled.

3-D password is despite in its early phase, achieving the above obsessions will conclude in a most effective, efficient, user friendly and highly secure authentication scheme.

REFERENCES

[1] "Three Dimensional password for more secured authentication" Fawaz A. Alsulaiman and Abdulmotaleb El Saddik, Senior Member, IEEE; IEEE Transactions On Instrumentation and Measurement, vol. 57, no. 9, September 2008

[2] Daniel V.Klein. Foiling the Cracker: A Survey of, and Improvement to Passwords Security. Proceedings of the USENIX Security Workshop,1990

[3] G. E. Blonder, "Graphical password," U.S. Patent 5559961, Sep. 24, 1996.

[4] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The design and analysis of graphical passwords," in *Proc. 8th USENIX Security Symp.*, Washington DC, Aug. 1999, pp. 1–14.

[5] J. Thorpe, P.C. van Oorschot. Graphical Dictionaries and the Memorable Space of Graphical Passwords. USENIX Security 2004, San Diego, August 9-13, 2004.

[6] Antonella De Angeli, Lynne Conentry, Graham Johnson and Karen Renaud, Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems. International journal of Human-Computer Studies, 63:128-152, july 2005

[7] F. A. Alsulaiman and A. El Saddik, "A novel 3D graphical password schema," in Proc. IEEE Int. Conf. Virtual Environ., Human-Comput. Interfaces, Meas. Syst., Jul. 2006

[8] Duhan Pooja, Gupta Shilpi , Sangwan Sujata, & Gulati Vinita, Secured authentication : 3-D password, I.J.E.M.S., VOL.3(2) 2012: 242 – 245

