© 2014 IJIRT | Volume 1 Issue 5 | ISSN : 2349-6002

A study of 3D Password

Zinal G. Solanki, Payal T. Mahida
Department of IT Systems & Network Security
Shri S'ad Vidya Mandal Institute of Technology, Bharuch, Gujarat, India

***Abstract*— The current security systems have weaknesses which can be vulnerable to threat. Textual passwords are commonly used. Users usually choose meaningful words from dictionaries, which make it easy to crack and revealed vulnerable to hacking or brute force attacks. Many graphical passwords have a password space that is less than or equal to textual password scheme. Smart cards or tokens can be lost or stolen. Many biometric authentications have been proposed but some people refuse because of their intrusiveness and effect on their privacy. This paper represents multifactor authentication scheme 3D Password. It include all the types of security schemes Textual, Graphical and many others but users provided option to choose the level of security and user acceptability. More over we provide a 3D virtual environment to navigate and interact with various objects more effectively and productively, The sequence of actions and interactions made by the user towards the objects inside the 3D environment constructs the user's password.**

***Index Terms*— Authentication, Textual passwords, Biometrics, Graphical passwords, 3D passwords, 3D virtual environment.**

I. BACKGROUND

The Dramatic increase of computer usage has lead to rise many security concerns. One of the most important security concern is authentication, which is process of identifying an individual, usually based on a username and password. In general, human authentication techniques can be classified as

1 Knowledge based (what you know)
2 Token based (what you have)
3 Biometrics (what you are)

Knowledge-based authentication can be further divided into two categories as: 1)Recall based and 2)Recognition based [6]. Recall-based techniques require the user to reproduce a secret that is 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 is textual passwords. One major drawback of the textual password is its two conflicting requirements: the selection of passwords should be easy to remember, at the same time it should be hard to guess. Klein[1] collected alphanumerical passwords of nearly 15,000 accounts and he reached the following observation: 25% of the passwords were guessed by using well-formed dictionary of 3×10^6 words. Full textual password space for eight-character passwords consisting of alphanumeric value is almost 2×10^{14} possible passwords, which is easy to crack 25% of the passwords by using only a small subset of the full password space. Graphical password schemes have been proposed as a possible alternative to text-based schemes, motivated by the fact that humans can remember pictures better than text [2]. The first graphical password schema was introduced by Blonder [2], which was based on idea of having a predetermined image, the user can select or touch regions of the image causing the sequence and the location of the touches to construct the user's graphical password. Graphical passwords can be divided into two categories as follows: 1) recognition based and 2) recall based. Various graphical password schemes have been proposed. Graphical passwords are based on the idea that users can recall and recognize pictures better than words. Some of graphical password schema recall based are: Draw a Secret (DAS), is simply a grid in which the user creates a drawing. The user's drawings, which consist of strokes, are considered to be the user's password. It becomes very hard to recall for very large grid size. PassPoint[5]: system extended Blonder's idea by eliminating the predefined boundaries and allowing arbitrary images to be used. Where user is free to select any point on the picture as password (PassPoint). But its time consuming also vulnerable to guessing attacks. Cued Click Point[5]; rather than five click-points on a image (as PassPoint), CCP uses one click-point on five different images shown in sequence. Some of graphical password schema . recognition based are: Story schema[5]; to form a story line it requires the selection of pictures of objects (people, cars, foods, airplanes, etc.), which is an insecure authentication scheme. Déjà Vu[3]; this process authenticates users by choosing portfolios among temptation portfolios. These portfolios are art randomized portfolios. Each image is derived from 8-B seed that is in plain text format. Therefore, an authentication server does not need to store the whole image; it simply needs to store the 8-B seed. Users spent more time on browsing to create image portfolios than passwords. Passface [5] is a technique developed on the assumption that people can recall human faces easier than other pictures. The basic idea is; user is asked to choose four images of human faces from a face database as their future password. In authentication stage, user can see a grid of nine faces, consisting of one face previously chosen by the user and eight temptation faces. If user recognizes, clicks anywhere on the known face. If user correctly identifies the four faces; authenticated successfully. Most of the graphical passwords can be easily recorded while

the legitimate user is performing; 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. From many authentication systems, particularly in banking, require not only Knowledge based (what the user knows) but also token-based (what the user possesses), which can be vulnerable to fraud, loss or theft. The most secure system is the 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. some human properties are vulnerable to change by time due to several reasons such as aging, scarring, face makeup, hairstyle and sickness. 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 characteristics. Most biometric systems require a special scanning device to authenticate users, that involves additional hardware costs as scanners. which is not applicable for remote and Internet users. Biometrics cannot be revoked, which leads to a confusion in case the user's data has been forged. Unlike other authentication schemes where the user can alter his textual password in case of a stolen password or replace his/her token if it has been stolen or forged, a user's biometrics cannot be revoked. After going through the defects in the above mentioned schemes we will easily agree to the fact that no security system is as safe as applicable as it appears to be. So, this paper come with a better idea, "3D Password".

II. 3D PASSWORD

The 3D password is a multifactor authentication scheme. It can combine all existing authentication schemes into a single 3D virtual environment. This 3D virtual environment contains several objects with which the user can interact. The type of interaction varies from one object to another. The 3D password is constructed by observing the actions and combination and sequences of the user interactions.

A. 3D PASSWORDS SCHEMA

The 3D password scheme should be combination of recall-, recognition-, biometrics- or token-based authentication schemes. Scheme should provide secrets that should be easy to remember and very difficult to guess for intruders, not easy to write down on paper and difficult to share with others. Scheme should provide secrets that can be easily revoked or changed. Users should have freedom to choose scheme for combination, which can provide high user acceptability.

B. 3D PASSWORD OVERVIEW

3D password is simply the combination and the sequence of user interactions that occur in the 3D virtual environment. The 3D password can combine recall, recognition, biometrics and token-based systems into one authentication scheme. Designing a 3D virtual environment make it possible, these scheme contains objects that request information to be recalled, information to be recognized, tokens to be presented, and biometrical data to be verified.

Virtual objects can be any object that we encounter in real life. Any actions-interactions to the real-life objects can be done with virtual objects in the virtual 3D environment . We can have the following objects:

- A computer with which the user can type;
- A fingerprint reader that requires the user's fingerprint;
- A biometrical recognition device;
- A white board that a user can write, sign or draw on;
- An automated teller machine (ATM) that requests a token;
- A light that can be switched on/off;
- A television or radio where channels can be selected;
- Any graphical password scheme;
- Any real-life object;
- Any upcoming authentication scheme.

C. WORKING OF 3D PASSWORD

Following are the steps for authentication (fig.1):

- User will connect to the server for system login.
- By successful login, client-server connection registration form will be filled up.
- User will now enter into virtual 3D environment.
- Now authentication steps will be performed according to preset design.
- User enters his textual password. If successfully logged in, it will enter into graphical password window else it will go back to Login form.
- Successfully logged in graphical password, will allow various services to be performed such as biometrics and tokens.
- Services include Open (), Save (), Delete () and Upload () etc..
- Finally, logout from the 3D environment.

D. 3D PASSWORD SELECTION AND INPUTS

Let us consider 3D virtual environment space of size G × G × G. The 3D environment space is represented by the coordinates (x, y, z) ∈ [1, . . ., G] × [1, . . , G] × [1,. . ., G]. The objects are distributed in the 3D virtual environment with unique (x, y, z) coordinates. User can navigate into 3D virtual environment and interact with various objects. The initial representation of user actions in the 3D virtual environment can be recorded as[1] follows:

(10, 24, 91) Action = Open the office door;
(10, 24, 91) Action = Close the office door;

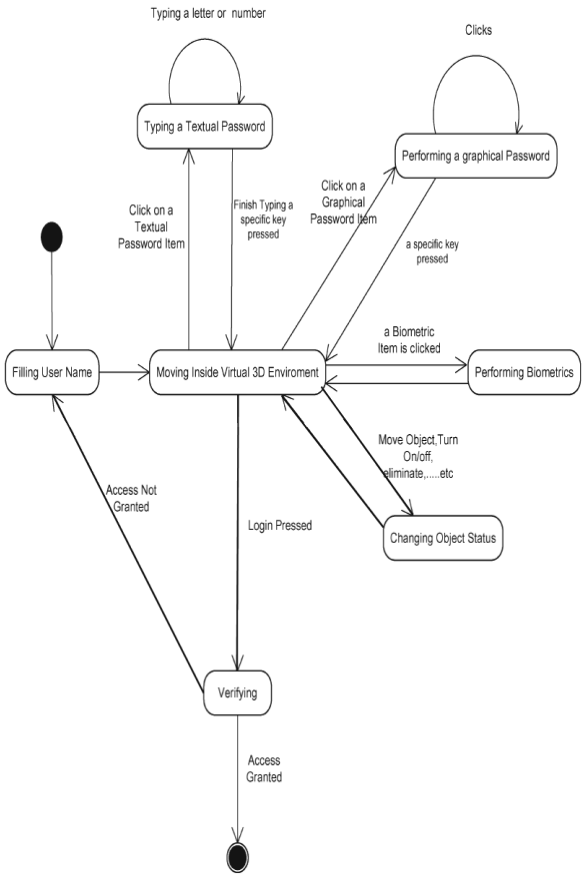

Fig 1 – State Diagram of 3D virtual environment[5]

(4, 34, 18) Action = Typing, “H”;
(4, 34, 18) Action = Typing, “E”;
(4, 34, 18) Action = Typing, “L”;
(4, 34, 18) Action = Typing, “L”;
(4, 34, 18) Action = Typing, “O”;
(10, 24, 80) Action = Pick up the pen;
(1, 18, 80) Action = Drawing, point = (330, 130)

III. 3D VIRTUAL ENVIRONMENT

To create 3D password system, need to design a 3D environment that reflects the administration needs and the security requirements. The design of 3D virtual environments should follow these guidelines.

a. *Real-life similarity* : Possible actions and interactions of virtual objects should reflect real-life situations. Object responses should be realistic.
b. *Object uniqueness and distinction* : Attributes of every virtual object are even such as position. Thus, the prospective interaction of obj1 != obj2.
c. *3D virtual environment size* : A large 3D virtual environment will increase the time required by the user to perform a 3D password. Moreover, a large 3D virtual environment can contain a large number of virtual objects and a small 3D virtual environment usually contains only a few objects.
d. *Number of objects (items) and their types*: As part of designing 3D virtual environment is determining the type of object (what kind of responses the object will have) and how many objects should be placed in the environment. The types of objects reflect what kind of responses the object will have.
e. *System importance*: 3D virtual environment should consider what systems will be protected by a 3D password. The number of objects and the types of objects that have been used in the 3D virtual environment should reflect the importance of the protected system.

IV. ATTACKS AND COUNTERMEASURES

a. Brute Force Attack: The attacker has to attempt all possible 3D passwords. This kind of attack is very difficult for the following reasons.
   - Required time to login: Time taken to perform successful login using 3D password varies depending on size, number of actions & interactions using objects in 3D virtual environment.
   - Cost of attack: 3D password scheme can be implemented in 3D virtual environment & its creation costs very high.
b. Well-Studied Attack: attacker has to study all the existing authentication schemes that are used in the 3D environment. User has to further study about user's selection or combination of objects as 3D password, which provide different responses for types of 3D virtual environment. It is hard for

attacker to crack 3D password.

c. Shoulder Surfing Attack: Attacker use camera to capture & recording of, 3D password. One of the most effective attack on 3D password & also to some of graphical passwords. Not possible for biometrics and textual password.

d. Timing Attack: Observing time that legitimate user take to perform a successful login using the 3D password. This observation gives the attacker mere hints. So, it would probably be launched as part of a well-studied or brute force attack. Timing attacks can be very effective if virtual 3D environment is poorly designed.

e. Key Logger : Attacker install software called key logger on system where authentication scheme is used. It stores text entered through keyboard, in the text file. This attack is more effective individual only, not so affective to 3D password.

V. 3D PASSWORD APPLICATIONS

The 3D password can have a password space that is very large compared to other authentication schemes. So, 3D password's main application domains are protecting critical systems and resources.

a. Critical servers – Many large organizations have critical servers that are usually protected by a textual password. A 3D password authentication proposes a sound replacement for a textual password.

b. Nuclear and military facilities – 3D password has very large probable password space and since it can contain token, biometrics and knowledge-based authentications in a single authentication system.

c. Airplanes and jet fighters – There are possible threat of misusing airplanes and jet fighters for religious-political agendas, which are protected by a powerful authentication system.

A small virtual environment can be used in systems such as:

- ATM
- Personal Digital Assistance
- Desktop Computers & laptop logins
- Web Authentication

VI. LITERATURE REVIEW

TABLE I: Comparison of major 3D password techniques

AUTHOR	PUBLICATION & YEAR	METHODOLOGY	LIMITATIONS
Alsulaima et al [4-5]	IEEE 2006, 2008	Users navigate and interact with objects of virtual 3D environment. The combination of all interactions, actions and interactions towards objects and virtual 3D environment, constructs 3D password. Combination of Recall based + Recognition Based + Token Based + Biometric scheme can create 3D password.	Cannot resist strong shoulder-surfing, well known attacks, time and memory requirement is large compare to other typical authentication schemes.
Georgakakis et al[9]	IEEE 2010	NAVI authentication scheme, a novel graphical password scheme where the credentials of the user are a route designed on a predetermined map. The user selects the starting and the ending point and the route is calculated by the provider of the route planning service.	Cannot resist countering shoulder-surfing and key logger/spyware attacks
SK Hafizul Islam [10]	Springer 2014	Three factor password authentication(TF-PWA) scheme based on extended chaotic maps(ECM), based on chaos theory include different cryptosystems with other authentication schemes. ECM-TF-PWA scheme is secure on the difficulties as man-in-middle attack of chaotic map-based	Cannot resist Well studied , Key logger/Spyware attacks

		Diffe-Hellman (CDH). Extending CDH by adding Hash function.	
Brandon Tran[13]	Winona 2013	The texture get put together, including create a new mesh to make a solid object in Blonder[2], interaction between 2 solid objects obsolete. A mesh is a sculpture of a model that is being created in 3D virtual environment. Selection of objects inside the environment and the object's type reflect the resulted password space then applying Biometric the most secure among all authentication scheme.	Cannot resist strong shoulder-surfing attack.
Huanyu Zhao, Xiaolin Li et al [7]	IEEE 2007	Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme (S3PAS), nearly perfect resistant to shoulder-surfing attack. It can replace text with conventional with invisible triangles. To login, the user must find all his/her original pass-characters in the login image and clicking inside pass-triangles password enters. Login created by 3 original pass-characters by click-rule.	Cannot resist Random Click Attack
Zhao et al [11]	Springer 2012	To resist shoulder-surfing for graphical password system, Convex Hull Click (CHC) scheme, in which user never click directly on their password images. CHC graphical elements uses large number of icons on the screen, the user must recognize pass-icons . The user responds to the challenge by clicking within the convex hull of the pass-icons.	Novice users take objectively long time compared to some traditional schemes.

VII. CONCLUSION

The 3D password is multifactor authentication scheme which combines various authentication schemes into a single 3D virtual environment. The virtual environment can contain any existing authentication scheme or even any upcoming authentication schemes by adding it as a response to actions performed on an object. The design of 3D virtual environment consist of choosing objects inside the environment and the object's type reflect the resulted password space. The user's preferences and requirements reflects by allowing him/her choosing authentication scheme as part of 3D password. Designing various kinds of 3D virtual environments, deciding on password spaces and interpreting user feedback and experiences from such environments will result in enhancing and improving the user experience of the 3D password. Moreover, gathering attackers from different backgrounds to break the system is one of the future works that will lead to system improvement and prove the complexity of breaking a 3D password.

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] G. E. Blonder, "***Graphical password***", U.S. Patent 5 559 961, Sep. 24, 1996.

[3] 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.

[4] Fawaz A. Alsulaiman and Abdulmotaleb El Saddik, "***A Novel 3D Graphical Password Schema***", IEEE International Conference on Virtual Environments, Human-Computer Interfaces and Measurement Systems, July 2006.

[5] Fawaz A. Alsulaiman and Abdulmotaleb El Saddik, "***Three-Dimensional Password for More Secure Authentication***", IEEE Transactions on Instrumentation and Measurement, vol. 57, no. 9, Sep. 2008.

[6] X. Suo, Y. Zhu, and G. S. Owen, "***Graphical passwords: A survey***", in Proc. 21st Annual

Computer Security Application Conference, 463–472, Dec. 5–9, 2005.

[7] Zhao, Huanyu, and Xiaolin Li. "***S3PAS: A scalable shoulder-surfing resistant textual-graphical password authentication scheme.***" Advanced Information Networking and applications Workshops", Vol. 2. IEEE, 2007

[8] Mhaske, Dhamdhere, V., and Patil, G., "***Three Diamentional Object Used for Data Security***." In *Computational Intelligence and Communication Networks (CICN), 2010 International Conference on*, pp. 403-408. IEEE, 2010.

[9] Georgakakis, E., Komninos, N., & Douligeris, C., "***NAVI: Novel authentication with visual information.***", In *Computers and Communications (ISCC), IEEE Symposium on* (pp. 000588-000595), IEEE, July 2012.

[10] SK Hafizul Islam "***Provably secure dynamic identity-based three-factor password authentication scheme using extended chaotic maps***", Springer Science + Business Media Dordrecht, Springer, July 2014.

[11] kabyua, C., Phiri, J., and Zhao, T., "***Metric Based Technique in Multi-factor Authentication System with Artificial Intelligence Technologies***", Future Wireless Network and Information Systems, Springer-Verlag Berlin Heidelberg, Springer, LNEE 143, pp. 89-97, 2012

[12] Tzong-Sun Wu · Ming-Lun Lee · Han-Yu Lin ·Chao-Yuan Wang, "**Shoulder-surfing-proof graphical password authentication scheme"**, Springer-Verlag Berlin Heidelberg**,** Nov. 2, 2013.

[13] Brandon Tran, "***3-D Password Secure Authentication with Biometric Device",*** Conference of the 13th Winona Computer Science Undergraduate Research Symposium, May 2013