3D Password: A novel approach for more secure authentication

Ms. Swati Bilapatte
M. E. (Computer), MGM College of Engineering and Technology
Email: swatibilapatte.03@gmail.com

Prof. Sumit Bhattacharjee
Department of Computer, MGM College of Engineering and Technology
Email: sumitnew@hotmail.com

Abstract— The melodramatic increase of computer usage has given rise to many security concerns. One major security concern is Authentication; process of validating who you are to who you claimed to be. Authentication provides more security to the system. Many existing authentication schemes such as textual password, graphical password etc. are available, each one having its own drawbacks and limitations. This paper introduced a new authentication technique, called 3D Password that overcomes the drawback of previously existing authentication schemes. The 3D Password is multi-factor and multi-password authentication techniques that consist of 3D virtual environment containing real time object scenarios. 3D virtual environment is the user interface that looks like same as real time environment but is not actual real time environment. Compared to other authentication techniques 3D Password is more advanced and secure, as it is easy to use and difficult to break. This paper also focuses on explaining what is 3D Password?, how to create 3D password, working of 3D Password and some design principles for designing 3D virtual environment.

Keywords- Authentication, Graphical password, Multi-factor, Textual password, 3D Password, 3D Virtual environment.

I. INTRODUCTION

Generally, the authentication scheme that user experiences are mostly very kind or very firm. Authentication has been a very remarkable approach, throughout the years. The tremendous rise and use of internet and related technologies has made easy for the 'intruders' to formulate or to steal identity or to hack someone's password. Authentication is the utmost significant security service that can be provided to the system by different authentication schemes. Authentication protects any system from unauthorized access, so that only authorized persons can have right to use or handle that system & data related to that system securely. Many effective and secure authentication schemes are available, having some drawback. Earlier, many authentication procedures were presented such as graphical password, text password, Biometric authentication, token-based etc.

Commonly, four types of authentication techniques are available such as:

1. Knowledge based: means what you know. The best example of this authentication scheme is textual password.

2. Recognition Based: means what you recognize. Example includes graphical password, iris recognition, face recognition, etc.

3. Biometrics: means what you are. Includes Thumb impression, voice recognition, etc.

4. Token based: means what you have. This includes Credit cards, ATM cards, etc. as an example.

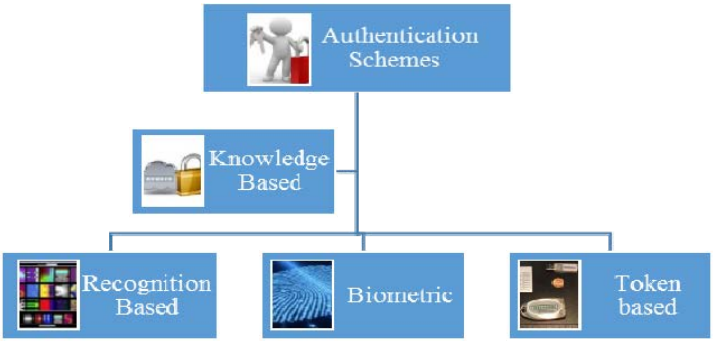

Fig 1.Authentication Schemes

According to nature of scheme and method used preferably, two types of authentication schemes are available:

A. Recall based

In this authentication scheme, user is required to recall or remember his/her password which had been created before. The user need to reproduce or repeat a secret that the user had created previously in recall based techniques. Knowledge based authentication is a part of this technique. Textual password is the most commonly used recall based authentication scheme used in the computer world where security is needed. Textual password has one major disadvantage due to its two contradictory requirements at the same time; password selection must be easy to remember and tough to guess.

B. Recognition based

In this scheme, user is required to identify and recognize his/ her password that had been created before. Recognition based authentication can be used in graphical password. The user need to identify and recognize the secret, or part of the secret, that the user had already selected previously in recognition based techniques. With graphical passwords, user can recall and recognize images, part of images, or sketches well than words. Moreover, graphical passwords are vulnerable to shoulder surfing attacks as graphical passwords can easily be observed and recorded while the authenticated user is carrying out graphical password. At present, most graphical passwords are still in their research stage and need more enrichment and usability trainings to deploy them in the arcade.

Biometric authentication is a prolonged feature of graphical passwords. Many biometric schemes have been proposed that includes fingerprints, palms prints, hand geometry, face recognition, voice recognition, iris recognition, retina recognition, heartbeat pulses, and etc. Acceptability, consistency and uniqueness are the aspect that describes the pros and cons of each biometric scheme. One of the major shortcoming of applying biometric is its inappropriateness and its effect on user's personal distinctive. Some users may even refuse to undergo low intensity infrared exposure to their retinas.

Many authentication systems, particularly in banking, require not only what the user knows but also what the user possesses (token-based systems) [2]. On the other hand, by using simple methods many reports have revealed that token are susceptible to fraud, loss, or theft.

The organization of paper is as follows: section 2 describes the literature survey. Section 3 discuss the goal and objective of the proposed system. Section 4 introduces and elaborates the 3D Password and also discusses some guidelines for designing 3D virtual environment. Section 5 discusses the security analysis along with the possible attacks and their counter measures and applications. Section 6 concludes the paper and suggests future directions.

II. RELATED WORK

Normally, users are likely to practice textual passwords as they are easy to use and remember. A textual password has password space of eight characters and is a combination of numbers and character string. Therefore, users tend to choose meaningful words from dictionary making it susceptible to dictionary or brute force attack. In 1990, Klein has collected the password of approximately 15,000 account users that had textual password and showed, 25% of the password were predicted easily using well-formed dictionary of 3*10^6 words. By conducting such experiment Klein could crack 10-15 passwords per day. Compared to today's technology Klein performed experiments, where the processing capabilities, memory, networking and other resources were very inadequate. The advanced version of securing password is graphical passwords. Blonder, was the first to familiarize graphical password schema. According to Blonder, graphical passwords is a predetermined image, where the user can select or touch regions of the image causing the sequence of interaction and the location of touches to constructs the graphical password for user. After Blonder, many graphical passwords paradigms have been proposed.

At present there are two broad categories of graphical passwords:

1) Recall based

2) Recognition based.

Pass faces is a recognition based graphical password, merely works by requiring the user to select a subgroup of *k* faces from a group of *n* faces. The system shows *m* faces and one of the faces belongs to the subgroup *k*, for authenticating. In order to complete the authentication process, user does selection many times. Story scheme is another paradigm, that form Story line by selecting the picture which is a collection of real like objects (person, food, flowers, bikes, etc.).

Blonder's proposed idea of graphical password is considered under recall based as, user needs to remember the selected touch locations. Furthermore, Pass Point is a recognition-based graphical password schema, by presenting a background picture the user is permitted to select any point on the picture as the user's password which is user's Pass Point. Jermyn *et al.,* presented a recall-based graphical password paradigm called Draw a Secret (DAS) which basically is a grid that allow users to create drawing. Users drawing comprise of strokes,

which constitutes as users password. Password space is affected by grids size and complexity. Conversely, due to human blunders grid complexity confines certain limitations. In case of large grid size, it's very difficult to recall where the drawing started, ended and where the middle points were exactly.

Comprehensively, another way of authenticating system is done using Biometric that includes Fingerprints, palm prints, face recognition, voice recognition, iris and retina recognition and heartbeat pulses are all different ways of practicing biometric authentication. Individual characteristics are exposed to variation from time to time due to numerous causes for instance face makeup, change of hairstyle, aging, scarring and illness(change of voice-due to throat infection). In addition, few people may tend to refuse biometrics for some reasons like exposure to low intensity IR light or retina scanning. Moreover, people may think that it's not safe to keep the copy of their fingerprint as it may affect their privacy. The main problem with Biometric authentication is that it cannot be revoked, in case the user data is counterfeit.

Token-based authentication systems are based on palpable objects. To protect tokens from theft and loss and to provide authentication several token-based authentication systems requires personal identification number (PIN).

III. PROPOSED SYSTEM

The proposed authentication system is a multi-factor and multi-password secure authentication scheme as it combines the benefits of previous existing authentication schemes into single platform authentication scheme together. The proposed system presents, the user with 3D virtual environment that contains several virtual objects or items with which the user can interact. Within this 3D virtual environment user can navigates and interact with various virtual objects. The users 3D Password is constructed by combining the sequence of actions and interaction towards the moving virtual objects inside the 3D virtual environment. The proposed system can combine the previously existing schemes for example, textual passwords, graphical passwords, biometrics and even token based etc. in a single 3D virtual environment. The users need and preferences would reflect the choice of user in selecting which authentication scheme will be part of the user's 3D Password. A user who are good at recalling and remembering a password might prefer to select textual and graphical password as a part of their 3D Password. Moreover, users who find hard to recall and remember might prefer to select biometrics or smart cards as part of their 3D Password. Thus, it would be user's freedom to choose and decide how the ideal and desired 3D Password will be constructed.

A. Goal

The main goal of the proposed system is to design a multi-feature, multi-password secure authentication scheme that combines the various authentication schemes into a single 3D virtual environment which results in a larger password space. The design of 3D virtual environment, the selection of object inside the environment, and the object type reflect the resulted password space. User have freedom to select whether the 3D password will be merely recall, recognition, or token based, or combination of two schemes or more.

B. Objective

- New scheme should provide more secure authentication compared to existing one.
- New scheme should build easy to understand and user friendly authentication technique, giving user the freedom of choice to select whether the 3D password would be solely, recall, recognition, biometrics or the mixture of any two schemes or more.
- New scheme should provide secrets that are easy to recall and at the same time tough to guess for the intruders.
- New scheme should provide such secrets that cannot be easily shared with others and difficult to note down on papers.
- New scheme should provide secrets that are mixture of merely recall, recognition, biometrics, and token based authentication schemes or combination of two or more schemes together.
- New scheme should provide secrets that are flexible, and authenticated user must be allowed to change or remove them.

IV 3D PASSWORD

The 3D password is a paradigm which is based on amalgamation of compound sets of characteristics. Comparatively, 3D Password is a new enhanced authentication scheme that combines RECOGNITION+RECALL +TOKENS+BIOMETRIC into single authentication system.

A. 3D Password Creation

As 3D Password is multi-feature so multiple password schemes such as textual password, graphical password, biometrics, and even token based passwords together can be used as a part of users 3D Password. Different users have different requirements so users must be given the freedom of selection and decision to choose which authentication schemes will be part of users 3D Password. The figure depicts state diagram for creating a 3D Password application.

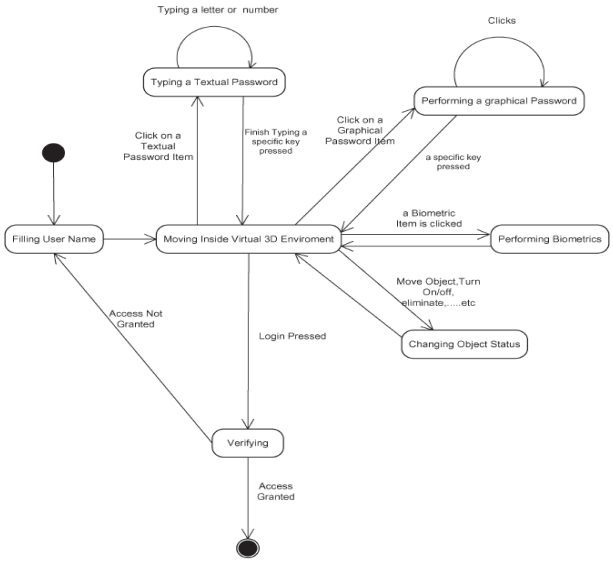

Fig 2. State diagram of creating 3D Password Application [1] [2] [4]

B. Working of 3D Password

The first step user need to do in 3D Password is to authenticate himself/herself using simple textual password and is done through by providing user's username and password. Refer Fig 3.

Fig 3. User entering Textual Password in 3D virtual environment [5]

On successful authentication, user is presented with 3D virtual environment GUI screen that consist of virtual computer and keyboard where the user need to enter password that is stored in a simple encrypted text file in the form of (x1, y1, z1) co-ordinates. After successful completion of this authentication step, user automatically enter into an art gallery (or virtual environment), where the user has to select multiple virtual objects/items present inside that gallery. The sequence in which user has clicked on moving objects, for those particular objects the sequence of points (i.e. their x, y, z co-ordinates) are stored in text file in the encrypted form. In this manner, 3D Password is constructed and set for that specific user. Afterwards, when users want to access his/her account then the user has to select all the objects in same sequence which he/she has selected at the time of creating their 3D Password. Sequence is compared with the stored coordinates and if match is found then, authentication is successful and user is given the access.

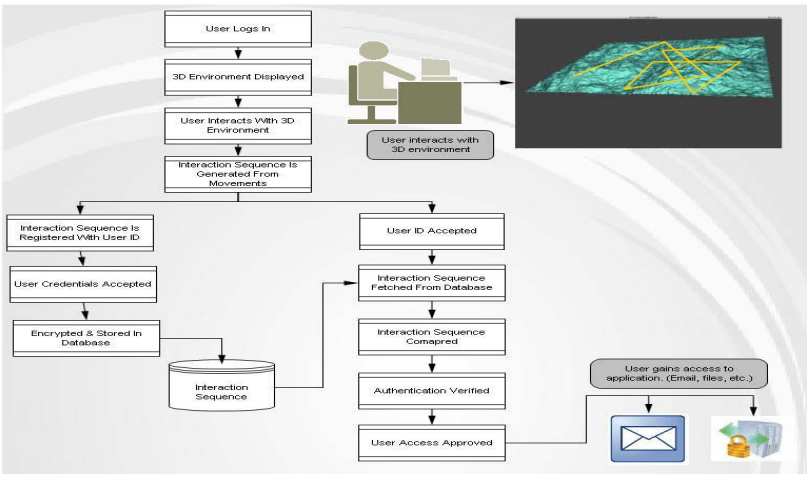

Fig 4. Working of 3D Password Scheme [4]

C. 3D Virtual Environment Design Guidelines

Design of 3D virtual environment imitating the need and security requirements of the user is the first step in creating 3D Password that affects usability, acceptability and effectiveness of the3D Password system.

Following are the guidelines that need to be considered while designing 3D virtual environment.

1) Real-life similarity

The prospective 3D virtual environment should reflect what people are used to seeing in real life [1]. Virtual objects should be relatively similar in size to real objects and their responses should be realistic. Possible actions and interactions toward virtual objects should reflect real-life situations.

2) Object uniqueness and distinction

Every virtual object/item present inside the 3D virtual environment should be different from each other and their uniqueness must come from the fact that every virtual object has its own attribute for instance position. Thus, the prospective interaction with object 1 is not equal to the interaction with object 2. Therefore, 3D virtual environment design should consider the distinguishing factors of virtual objects that increase the user's recognition of objects thereby, improving system usability.

3) Three dimensional virtual environment size

Size of 3D virtual environment do matters and should be studied carefully. A 3D virtual environment can depict a city or even the world. On the other hand, it can depict a space as focused as a single room or office [1]. A large 3D virtual environment contains large number of virtual objects and hence, requires more time to create 3D password compared to small 3D virtual environment that contains few virtual objects.

4) Number of objects(items) and their types

Most important part to be consider while designing 3D virtual environment is to determine the type of object that reflect what kind of responses the object will have and number of objects to be placed in the virtual environment. Selection of the right type of object and number of object affects the probable 3D Password space.

5) System importance

The 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 [2].

V 3D PASSWORD AS MORE SECURE AUTHENTICATION SCHEME

A. Attacks and counter measures

In this section, we try to cover and study different types of possible attacks that are practice against 3D Password and see how secure 3D Password is against such attacks. In addition, we try to propose counter measure for such attacks.

1) Brute force attack.

In type of attack, attacker tries n number of possible combination of 3D Password. To perform this attack two things need to be considered.

- Required time to login: in case of 3D password successful login time varies due to dependence on number of interactions and the size of 3D virtual environment does matter.
- Cost required to attack: main requirement of 3D Password is 3D virtual environment and cost of creating such an environment is very high.

2) Well-studied attack

To launch this kind of attack, attackers need to acquire the knowledge of the most probable distribution of 3D Password. To acquire such kind of knowledge attacker needs to study all the previous authentications schemes that are used in the 3D virtual environment which is very tough. For that the attacker even may need to gather the information regarding forging of all existing biometrical and token based data too. In addition, it requires a study of the user's selection of objects, or a combination of objects, that the user will use as a 3D password [1]. Furthermore, this kind of attack is hard to achieve as the attacker must need to perform a customized attack for every different 3D virtual environment design.

3) Shoulder surfing attack

To perform this attack, attackers make use of camera to capture and record the 3D Password while the legitimate user is carrying with their login process. This attack is more effective than any other attacks on 3D password. To avoid this attack, 3D Password must be performed in a secure place.

4) Timing attack

Here, attackers notices how much time it takes the authenticate user to accomplish an accurate sign-in with the 3D Password. By this observation attacker can get a clue regarding authenticated user's 3D Password length. Yet this attack is not very much effective as it gives mere clues to the attacker. Thus, it would perhaps be performed as a part of either brute force attack or well-studied attack.

B. Advantages & Disadvantages

1) Advantages

- 3D Password is multi-feature and multi-password authentication scheme.
- Large password key space.
- More secure authentication scheme as compared to existing one.

2) Disadvantages

- Large time and memory requirements.
- Shoulder-suffering attack is still effective and can affect this scheme.
- Expensive as compared to previous ones.

C. Applications

As compared to previously existing authentication schemes, 3D Password has large password key space and hence, to protect critical system and resources are 3D Password's main application domain.

1) Critical servers

Commonly, critical servers of many large organizations are protected using textual passwords. A 3D password authentication proposes a sound replacement for a textual password.

2) Nuclear and military facilities

Such facilities should be protected by the most powerful authentication systems. The 3D 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 [1].

3) Airplanes and jet fighters

Because of the possible threat of misusing airplanes and jet fighters for religion-political agendas, usage of such airplanes should be protected by a powerful authentication system [1].

Furthermore, 3D Password can be applied in less critical systems where 3D virtual environment used size are small. Few such applications are as follows

- Web Application Authentication
- ATM
- PDA- Personal Digital Assistance
- Laptop and Desktop Computer logins.

VI CONCLUSION

In the current state many existing authentication schemes are available that are vulnerable to certain kind of attacks. The 3D Password is multi-feature, multi-factor authentication scheme that combines all the benefits of existing authentication schemes into single 3D virtual environment. The 3-D password is still in its early stages. Designing various kinds of 3-D 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 3-D 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 3-D password. Moreover, it will demonstrate how the attackers will acquire the knowledge of the most probable 3-D passwords to launch their attacks. Shoulder surfing attacks are still possible and effective against 3-D passwords. Therefore, a proper solution is a field of research [1].

REFERENCES

[1] "Three-Dimensional password for more secure Authentication", Fawaz A. Alsulaiman and Abdulmotaleb El Saddik, Senior Member, IEEE, IEEE Transactions on Instrumentation and Measurement, vol. 57, no. 9, september 2008.

[2] "Virtual Realization using 3D Password", A.B.Gadicha, V.B.Gadicha, ISSN: 2277-1956, International Journal of Electronics and Computer Science Engineering

[3] "3-D Graphical Password Used For Authentication", Mrs. Vidya Mhaske-Dhamdhere, Bhakti Pawar, Pallavi Ghodke, Pratibha Yadav, Int.J.Computer Technology & Applications,Vol 3 (2), 510-519.

[4] "Secure Authentication with 3D Password",Vishal Kolhe, Vipul Gunjal, Sayali Kalasakar, Pranjal Rathod, International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 2, March 2013.

[5] "New Era of authentication: 3-D Password", Shubham Bhardwaj, Varun Gandhi, Varsha Yadav, Lalit Poddar, ISSN: 2278 – 7798, International Journal of Science, Engineering and Technology Research (IJSETR), Volume 1, Issue 5, November 2012.

[6] " 3D Password : Minimal utilization of space and vast security coupled with biometrices for secure authentication", Ms. Nidhi Maria Paul, Ms. Monisha Shanmugham, International Journal of Advanced Technology & Engineering Research (IJATER), Volume 2, Issue 4, July 2012.

[7] "Minimum Space and Huge Security in 3D Password Scheme", Prof. Sonkar S.K, Dr.Ghungrad.S.B, International Journal of Computer Applications (0975 – 8887), Volume 29– No.4, September 2011