Secured Authentication with 3-D Password

Dr. Chandragupta Warnekar
Department of Computer Science and Engineering
Jhulelal Institute of Technology
Nagpur, India.

Nikita . V. Mulchandani
Department of Computer Science and Engineering
Jhulelal Institute of Technology
Nagpur, India.

***Abstract*— The dramatic increase in usage of computer systems (both in standalone & network mode) has given rise to many security concerns. One such major system-security concern is Authentication; which ensures that only the authorized person is approaching the system resources. It is a process of identifying an individual, usually based on a username and a password. Providing Authentication also leads to more secured interaction with that system. The available authentication techniques include: textual or graphical passwords, bio-matrics, etc. However, the existing schemes suffer from certain weaknesses like when a person uses textual passwords, generally the choice is meaningful words from dictionary or nick names, date of birth, etc. which can be cracked easily whereas graphical passwords are vulnerable to shoulder surfing attacks. To overcome the drawbacks of existing techniques, a new improved authentication technique called "3D passwords" is proposed. It is multi-password & multi-factor authentication scheme as it combines multiple authentication techniques. Most important part of 3D password scheme is inclusion of 3D virtual environment consisting of real time object scenarios. It is not an actual real time environment, but a user interface which looks like a real environment. This scheme is hard to break & easy to use.**

This paper explains: What is 3D password? How the scheme actually works? Few more concepts related to 3D password, applications and advantages of scheme etc.

Index Terms: System Security, Authentication, 3-D Virtual Environment, 3-D Password.

1. INTRODUCTION

The general field of Computer Security is concerned with the protection of vital information during storage, retrieval, processing and communication via computer systems and networks.

Users commonly use textual passwords, ignoring the security recommendations. Thus, they are inclined to select words of significance from dictionaries, making the system less secured. The fundamental principle behind graphical passwords is that users would find it easier to remember and identify pictures as compared to words.

However, this paradigm faces a number of complications. Some graphical passwords require a long time to be executed, and more importantly, they can easily be noted or observed by others, while the user is in the process of authentication. Smaller available textual password space also makes it easy to crack

Therefore, this paper suggest the idea of **3D passwords** which are more secured, customizable and very interesting way of authentication.

2. WHAT IS 3D PASSWORD?

The 3D password is a paradigm which is based on a combination of multiple sets of factors. This authentication scheme is based on combination of different authentication schemes into a single scheme, to generate secured passwords. This system presents a 3D virtual environment containing various virtual objects, where in the user navigates and interacts with the multitude of objects that are present. The order in which actions and interactions are performed with respect to the objects constitutes the user's 3D password. The flexible 3D password key space is built on the basis of the design of the 3D virtual environment and sequence and interactions with the objects selected. The 3D Password scheme is a new authentication scheme that combines RECOGNISATION + RECALLS + TOKENS + BIOMETRIC in one authentication system. The diagram below depicts the scope of 3D password which encompasses all the conventional password schemes.

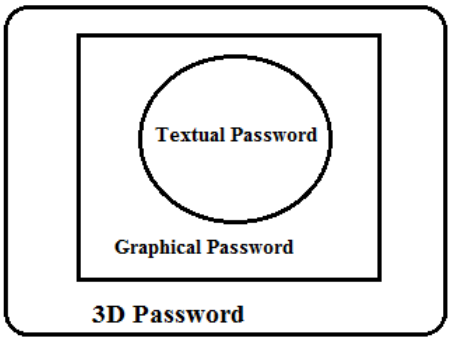

Fig. 3D password as Multi-factor & Multi-password Authentication scheme.

2.2 *Objectives:*

- To provide more secure authentication technique than the existing ones.
- To design & develop more user friendly & easier authentication scheme and giving user a freedom of selecting more than one password scheme as single system. It should be hard to break & easy to use.
- To overcome the drawbacks & limitations of previously existing systems (textual password, graphical password. Etc.)

3. 3D PASSWORD AS STRONG AUTHENTICATION

The 3-D password is constructed by following the sequence of actions and interactions of the user in the virtual world. The user has a choice to select the order of actions and interactions for authentication purpose. Thus the final Authentication scheme chosen by user only would be the part of their 3D password. This is achieved through interacting only with the objects that acquire information that the user is comfortable in providing and ignoring the objects that request information that user does not prefer to provide. With this scheme the user has freedom of choice as to what type of authentication scheme will be part of their 3-D password and given the large number of objects and items in an environment, the number of possible 3-D passwords will increase. Thus, it becomes much difficult for the attacker to guess the user's 3-D password.

The 3D password can combine recognition, token, recall and biometrics based systems into single authentication scheme. This can be done by designing a 3D virtual environment that contains objects that request information to be recalled, information to be recognized, tokens to be presented, and biometric data to be verified.

Virtual objects can be any object that we encounter in real life. Any obvious actions and interactions towards the real life objects can be done in the virtual 3D environment. Moreover, any user input (such as speaking in a specific location) in the virtual 3D environment can be considered as a part of the 3D password.

3.1 *System architecture:*

In this work we are implementing the authentication framework by using 3D graphical objects as a password. This is very easy to remember instead of remembering a character, numbered and alphanumeric password. Also prevent the key logger software to catch the keystrokes and its monitoring. Fig.2 shows the login process of the system.

Following are the general steps for authentication:
1. User will connect to the server for system login.
2. After successful client-server connection registration form will be filled up.
3. User will now enter into virtual 3-D environment.
4. Now the user will perform its authentication steps according to set design.(like textual, graphical, numerical, bio-metrics etc.)
5. User enters his textual password. If the textual password is accepted and successfully logged in, it will enter into graphical password window else it will go back to Login form.
6. On the other hand, if the graphical password is successfully logged in, various services will be performed such as biometrics and tokens.(turning on light, opening cupboard etc.)
7. Services include Upload ( ), Save ( ), Delete ( ), Open ( ) and etc.
8. Finally, the user will log out from the 3-D environment

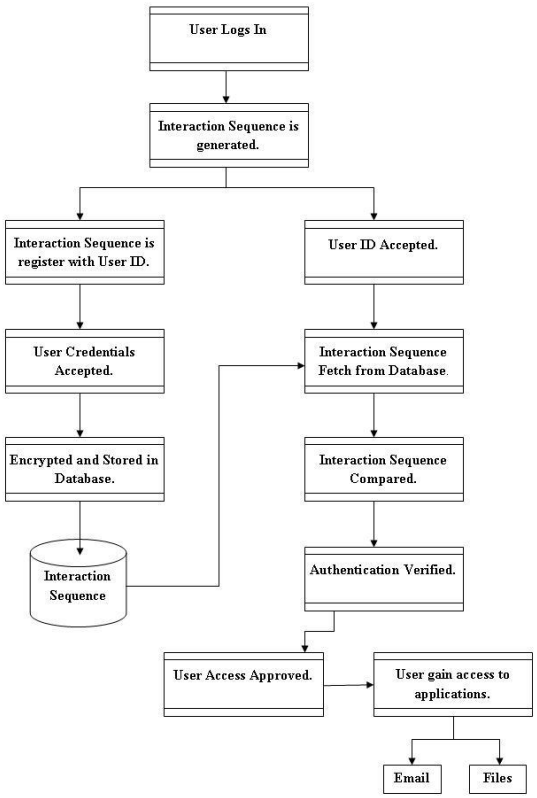

Fig:2 System Architecture

Some design guidelines related to 3d environment are such as

- To design an environment that reflects the admistrator's needs and fulfills the requirement.
- Virtual environment should be selected in a way that it is similar to real life objects and environment.
- Every object should be unique & distinct from other.
- Virtual environment size should be considerable.
- To provides the scheme that allows secrets to be easily changed or revoked.

3.2. 3D Password Selection and Inputs:

Consider a three dimensional virtual environment space that is of the size G×G×G. Each point in the three dimensional environment space represented by the coordinates (x, y, z) [1..G] × [1..G] ×[1..G]. The objects are distributed in the three-dimensional virtual environment. Every object has its own coordinates (x,y,z). Assume that the

user can navigate and walk through the three-dimensional virtual environment and can see the objects and interact with the objects. The input device for interaction with objects can be a mouse, a keyboard, stylus, a card reader, a microphone …etc. User's actions, interactions and inputs towards the objects and towards the three-dimensional virtual environment are mapped into a sequence of three-dimensional coordinates and actions, interactions and inputs.

For example, consider a user navigates through the three-dimensional virtual environment and types "AB" into a computer that exists in the position of (13, 2, 30). The user then walks over and turns ON the light located in (20, 6, 12), and then goes to a chess-board located in (55, 3, 30) and draws just one dot in the (x, y, z) coordinate of the board at the specific point of (530,250). The user then presses the login button. The representation of user actions, interactions and inputs towards the objects and the three-dimensional virtual environments can be represented as the following:

(13, 2, 30) Action = Typing, "A",
(13, 2, 30) Action = Typing, "B",
(20, 6, 12) Action = Turning the Light, ON,
(55, 3, 30) Action = drawing, point = (530,250)

Two 3D passwords are equal to each other when the sequence of actions towards every specific object is equal and the actions themselves are equal towards the objects. As described earlier, three-dimensional virtual environments can be designed to include any virtual objects.

The first step in building a 3D password system is designing the three-dimensional virtual environment. The selection of what objects to use, locations, and types of responses are very critical tasks. The design affects the strength, usability and performance of the 3D password.

4 SECURITY ANALYSIS

The information content of a password space defined as "the entropy of the probability distribution over that space given by the relative frequencies of the passwords that users actually choose". However, trying to have a scheme that has very large possible passwords is one of the important parts in resisting the attack on such a scheme.

4.1. 3D Password space size:

To find out the password space, we have to count all possible 3D passwords that have a certain number of actions, interactions, and inputs towards all objects that exist in the 3D virtual environments. In this attack, the attacker observes how long it takes the legitimate user to perform a correct sign in using the 3D image logical password. This observation gives the attacker an indication of length of the legitimate user's 3D password.

.

4.2. 3D password distribution knowledge:

Users tend to use meaningful words for textual passwords.

Therefore finding these different words from dictionary is a relatively simple task which yields a high success rate for breaking textual passwords. Pass faces users tend to choose faces that reflect their own taste on facial attractiveness, race, and gender. Every user has different requirements and preferences when selecting the appropriate 3D Password. This fact will increase the effort required to find a pattern of user's highly selected 3D password. In addition, since the 3D password combines several authentication schemes into a single authentication environment, the attacker has to study every single authentication scheme and has to discover what the most probable selected secrets are. Since every 3D password system can be designed according to the protected system requirements, the attacker has to separately study every 3D password system. Therefore, more effort is required to build the knowledge of most probable 3D passwords

5. 3D PASSWORD DIFFERENTIATORS

Flexibility: 3D Passwords allows Multifactor authentication biometric, textual passwords can be embedded in 3D password technology.

Strength: This scenario provides almost unlimited passwords possibility.

Easy to Remember: can be remembered in the form of short story.

Privacy: Organizers can select authentication schemes that respect user's privacy.

Password Space: Due to use of multiple schemes into one scheme password space is increased to great extend.

Security: Combination of re-call based, recognized based, Biometrics .etc into single authentication technique therefore, more secure authentication scheme over currently available schemes.

5.1 3D Password Disadvantages:

- As compared to traditional password approach this approach will definitely take more time to do user authentication.
- More storage space required because it needs to save images which is large binary objects.
- More costly due to required devices like web cam, finger print device etc.
- More complex than previous authentication schemes.

5.2 3D Password Application Areas:

1. **Critical Servers**: Many organizations are using critical servers which are protected by a textual password. 3D password authentication scheme proposes sound replacement for these textual passwords.
2. **Banking:** Almost all the Indian banks started 3D password service for security of buyer who wants to buy online or pay online.
3. **Nuclear and military Facilities:** 3D password has a very large password space and since it combines RECOGNITION + RECALL+ TOKENS+ BIOMETRIC in one authentication system, it can be used for providing security to nuclear and military facilities.
4. **Airplanes and Jetfighters:** Since airplanes and jet planes can be misused for religion and political agendas, they should be protected by a powerful authentication scheme.

5. **Other Areas**: In addition, 3-D passwords can be used in less critical systems because the 3-D virtual environment can be designed to fit any system's needs. ATMs, desktop and laptop logins, web authentication.

6. CONCLUSION AND FUTURE SCOPE

There are many authentication schemes at the current state. Some of them are based on user's physical and behavioural properties and some others are based on user's knowledge such as textual and graphical passwords. Moreover there are some other authentication schemes that are based on what you have such as smart cards. The 3D password is a multi factor authentication scheme that combines the various authentication schemes into a single 3D virtual environment. The virtual environment can contain any existing authentication scheme or even any upcoming authentication schemes, resulting in the very large password space compared to any of the existing schemes. While using 3D password, users have the freedom to select whether the 3D password will be solely recall, biometrics, recognition, or token based, or a combination of two schemes or more. Users do not have to carry cards if they do not want to. They have the choice to construct their 3D password according to their needs and their preferences. A 3D password's probable password space can be reflected by the design of the three-dimensional virtual environment, which is designed by the system administrator. The 3D password is still new & in its early stages. Designing various kinds of 3-D virtual environments, deciding on password spaces, and interpreting user's feedback and experiences from such environments will result in enhancing and improving the experience of the 3-D password. Gathering attackers from different background and attack made by them and how to overcome them is main future work. Inclusion of biometrics leads to increasing cost & hardware in scheme, to reduce this is still field of research.

The 3D password is just introduced means it is in its childhood. A study on a large number of people is required. We are looking at designing different three-dimensional virtual environments that contain objects of all possible authentication schemes

7. REFERENCES

[1] Tejal Kognule and Yugandhara Thumbre and Snehal Kognule, "3D password", International Journal of Computer Applications(IJCA),2012.

[2] Duhan Pooja, Gupta Shilpi , Sangwan Sujata, & Gulati Vinita, ―SECURED AUTHENTICATION: 3D PASSWORD‖, I.J.E.M.S., VOL.3(2),242 – 245, 2012

[3] Vishal Kolhe, Vipul Gunjal, Sayali Kalasakar, Pranjal Rathod,"Secure Authentication with 3D Password ",International Journal of Engineering Science and

Innovative Technology (IJESIT) Volume 2, Issue 2, March 2013

[4] 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

[5] A Novel 3D graphical password schema-Fawaz A Alsulaiman and Abdulmotaleb El Saddik