CYBERSECURITY USING 3D PASSWORD

GANGULA THIRUPATHI,
Assistance Professor,
Department of Computer Science and Engineering,

DR RAMASAMY VELMANI,
Professor,
Department of Electronics and Communications Engineering,

Siddhartha Institute of Technology and Sciences,
Narapally, Hyderabad, Telangana – 500 088.

ABSTRACT

Providing security to any system is part of the authentication process. Authentication can be done using text, biometrics, or other techniques. This type of textual password usually employs an encryption mechanism to assure security. Each method has its own set of limitations and drawbacks. To address the flaws, a new authentication technique is now available. A multi-factor and multi-factor authentication strategy, the 3D Password approach is a multi-factor and multi-factor authentication technique. The most important part of 3D Password is the virtual environment that houses the user interface and appears to be a real-time environment but is not. A 3D password is more secure than other authentication systems since it is difficult to crack and simple to use. The 3D password has the advantage of combining existing system authentication with superior user security. This research focuses on how to create 3D passwords as well as design suggestions for 3D passwords. The 3D password is used to get around the limitations and flaws of existing authentication methods. The 3D Password is a multi-featured, multi-factor authentication system that combines the benefits of existing authentication techniques into a single virtual 3D environment. This presentation will focus on the new authentication technique's concept, how it works, and how it could be applied.

I. INTRODUCTION

Authentication is one of the most important security services provided by various authentication systems or algorithms. To secure any system, authentication must be set up so that only authorised personnel may use or control the system and the data it contains. There are a number of different authentication methods available, some of which are efficient and secure yet have disadvantages. Many authentication mechanisms, such as graphical passwords, text passwords, biometric authentication, and so on, have been introduced in the past.

There are four different authentication methods

- Knowledge Base: What you already know is referred to as "knowledge based." A textual password is the best example of this authentication system. A textual password is the best example of a knowledge base technique. Token Basis Authentication: Token base authentication can be used with any ATM or swipe card. A recognition base technique is any graphical password or face identification approach.
- Biometrics Base: A thumb or finger impression is an example of a biometrics base authentication technique.
- Recall Base: System security is a major worry these days. The Scheme Textual is an example of a recall-based Scheme. To secure the system, the user inputs a password. A Strong Textual Password can help safeguard a system to some extent. It is, however, difficult to remember.
- Recognition Base: The user must identify and recognise his or her own password, which he or she created, in the Recognition Base system. With graphical passwords, a shoulder surfing attack is a concern. A biometrics-based authentication technique is also included in the recognition strategy. Authentication methods include fingerprints, palm prints, face recognition, voice recognition, retina recantation, and other biometrics. Biometrics employs the technology of recording or replaying biometric data. An attack can also be launched, as well as a hill climbing attack. With token-based authentication, there is a risk of fraud, loss, and theft.

II. RELATED SURVEY

By adding authentication to any system, that system gains more security. There are numerous authentication approaches available, such as substance word, graphical word, and so on. However, each of these has its own set of limits and drawbacks. A new better authentication approach is used to solve the disadvantages of previously existing authentication techniques. This authentication theme is known as 3D password.(Smita Verma 2014)

Adding authentication to any system increases the security of that system. There are a variety of authentication systems available, such as textual passwords, graphical passwords, and so on, but each has its own set of limits and drawbacks. A new improved authentication technique is employed to solve the shortcomings of previously existing authentication techniques. This authentication scheme is known as 3D password. (P.K.Dhanya, 2014)

III. METHODOLOGY

Textual, biometric, and other authentication methods are available. To ensure security, this form of textual password usually uses an encryption method. Each of these methods has its own set of limits and disadvantages. These passwords aren't 100% secure or effective, and they contain certain flaws. Because it incorporates the benefits of earlier existing authentication methods into a single platform authentication scheme, the proposed authentication system is a multi-factor and multi-password secure authentication technique. The suggested system provides a 3D virtual world with multiple virtual objects or items with which the user can interact. The user can browse and interact with many virtual objects in this 3D virtual environment. The user's 3D Password is created by putting together a series of actions and interactions with moving virtual objects in a 3D virtual environment. In a single 3D virtual environment, the suggested system can incorporate previously established schemes such as textual passwords, graphical passwords, biometrics, and even token-based schemes. The user's needs and preferences would be reflected in the authentication system that will be included in the user's 3D Password. A user who is adept at remembering and recalling passwords may want to include textual and graphical passwords in their 3D Password. Furthermore, individuals who have trouble remembering and recalling passwords may want to incorporate biometrics or smart cards as part of their 3D Password. As a result, the user would have the option to choose and decide how the ideal and desired 3D Password should be implemented.

IV. RESULTS AND DISCUSSION

FIGURE 1: AUTHENTICATION SYSTEM

A multi-factor authentication approach is the 3D password. A 3D virtual environment with many virtual items is presented by the 3D password. The user interacts with the objects and navigates across the area. The 3D password is simply the mix and sequence of user activities that take place in the virtual 3D world. In one authentication technique, the 3D password can combine recognition, recall, token, and biometrics-based systems. This can be accomplished by creating a 3D virtual environment with objects that ask for information to be recalled, recognised, tokens to be presented, and biometric data to be confirmed. For instance, the user can enter the virtual environment and type something on a computer at the (x1, y1, z1) position, then enter a room with a fingerprint recognition device in the (x2, y2, z2) position and present his or her fingerprint. The user can then go to the virtual garage, open the car door, and tune in to a certain channel on the radio. The user's 3D password is made up of the combination and sequence of past actions directed towards distinct objects.Any object that we encounter in real life can be used as a virtual object. Any clear activities and interactions with real-world things can be performed on virtual objects in a virtual 3D environment. Furthermore, any user interaction in the virtual 3D environment (such as speaking at a certain spot) might be regarded a part of the 3D password. The following objects are available:

1) A computer that allows the user to type

2) A fingerprint reader that necessitates the usage of the user's fingerprint;

3) A biometric identification system;

4) A piece of paper or a whiteboard on which the user can write, sign, or draw;

5) A token-requesting automated teller machine (ATM);

6) A light that can be turned on and off

7) A television or radio with selectable stations;

8) A staple with the ability to be punched;

9) A vehicle capable of being driven;

10) A book with the ability to be transported from one location to another;

11) Any password scheme that is graphical;

12) Any real-world thing

13) Any authentication system that may be implemented in the future

V. CONCLUSION

Authentication is now done via textual and token-based passwords, which are vulnerable to a range of attacks. The 3D Password is a multi-featured, multi-factor authentication system that combines the benefits of existing authentication techniques into a single virtual 3D environment. The three-dimensional password is a revolutionary authentication system that is currently in its early stages. By building various types of 3-D virtual settings, deciding on password spaces, and assessing user feedback and experiences from such surroundings, the user experience of the 3-D password will be increased and improved. The user's authentication preferences and needs are represented in the 3D password, making 3D password usage simple. The 3D Password technique is more secure and reliable than other authentication mechanisms. By utilising 3d Password, we can make any system more secure, and it will be beneficial for apps used in the commercial world, the government sector, and personal use.

REFERENCES

1. Alsulaiman, F.A.; El Saddik, A., "Three -for Secure" IEEE Transactions on Instrumentation and measurement, vol.57, no.9, pp 1929 - 1938.Sept. 2008.

2. Vishal Kolhe, Vipul Gunjal, Sayali Kalasakar, Pranjal Rathod “Secure Authentication with 3D Password” International Journal of Engineering Science and Innovative Technology (IJESIT)
3. Duhan Pooja, Gupta Shilpi, Sangwan Sujata, & Gulati Vinita “SECURED AUTHENTICATION: 3D PASSWORD” International Journal of Engineering and Management Studies.
4. 3D Password: A Novel Approach for More Secure Authentication. ttp://www.ijcset.com/docs/IJCSET14-05-02-080.pdf
5. S. Ranjitha “Secure Authentication with 3D Password” IFET College of Engineering
6. Anuradha Srivastava “3-D PASSWORD – A more secured authentication” Slideshare.n
7. 3D Password: Minimal Utilization of Space and Vast Security Coupled with Biometrics for Secure Authentication
8. http://www.ijater.com/Files/b8d368dffb71-4b45-95c5-0a7a4b266a1c_IJATER_05_15.pdf