SECURE BY THE USE OF A 3D PASSWORD

Dr. SRIHARI CINTHA,
Professor,
Department of Computer Science and Engineering,

Dr. AYESHA FIRDOUS
Professor,
Department of Electronics and Communications Engineering,

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

ABSTRACT

Authentication of any system entails providing that system with security. 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. A new authenticate mechanism is now available to alleviate the shortcomings. The 3D Password approach is a multi-factor and multi-factor authentication technique. The virtual environment holding the user interface, which appears to be a real-time environment but is not, is the most essential aspect of 3D Password. In comparison to other authentication methods, a 3D password is more secure because it is tough to crack and simple to use. The advantage of the 3D password is that it combines existing system authentication with excellent user security. This study focuses on how to build 3D passwords as well as 3D password design ideas. The 3D password is used to circumvent the limits and shortcomings of existing authentication techniques. The 3D Password is a multi-featured, multi-factor authentication technique that integrates the advantages of existing authentication schemes into a single virtual 3D environment. This presentation will concentrate on the notion of the new authentication technique, how it works, and how it might be used.

I. INTRODUCTION

Authentication is one of the most critical security services that different authentication systems or algorithms provide to a system. To secure any system, authentication must be established so that only authorised individuals have access to use or manage the system and the data associated with it. There are a variety of authentication methods available, some of which are efficient and secure yet have drawbacks. Many authentication systems have been introduced in the past, such as graphical passwords, text passwords, biometric authentication, and so on.

There are four methods of authentication available:

- Knowledge Base: The term "knowledge based" refers to what you already know. The finest example of this authentication mechanism is a textual password. The best illustration of a knowledge base strategy is a textual password. Token Base Authentication: Any ATM card or swipe card is an example of token base authentication. Any graphical password or face identification approach is an example of a recognition basis technique.
- Biometrics Base: One example of a biometrics base authentication mechanism is a thumb or finger impression.
- Recall Base: Nowadays, system security is a serious concern. Textual is an example of a Scheme that is built on recall. The user enters a password to safeguard the system. At a certain degree, a Strong Textual Password can secure a system. It is, nevertheless, tough to memorise.
- Recognition Base: In the Recognition Base system, the user must identify and recognise his or her own password, which he or she created. A shoulder surfing attack is a problem with graphical passwords. The recognition approach also includes a biometrics-based authentication technique. Fingerprints, palm prints, face recognition, voice recognition, retina recantation, and other biometrics authentication methods are used. Recording or replaying biometric data is a technique used in biometrics. It is also possible to launch an attack as well as a hill climbing attack. There is a risk of fraud, loss, and theft with token-based authentication.
- **Purpose**: The proposed system's main goal is to provide a multi-featured, multi-password secure authentication method that merges many authentication techniques into a single 3D virtual environment, resulting in a bigger password space. The resultant password space is reflected in the architecture of the 3D virtual environment, the selection of objects inside the environment, and the object kind. The user can choose whether the 3D password is based on memory, recognition, or tokens, or a mix of two or more schemes.
- **Goal**: In comparison to the existing technique, the new scheme should provide better secure authentication.The new method should create an easy-to-understand and user-friendly authentication mechanism, allowing users to choose whether the 3D password is purely based on recall, recognition, biometrics, or a combination of two or more techniques.

II. RELATED SURVEY

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 technique (Warnekar et al. 2015).

Authentication of any system means providing a security to that system. There are number of authentication techniques like textual, biometrics etc. This type of textual password commonly follows an encryption algorithm to provide security. Each of these techniques has some limitations and drawbacks.To overcome the drawbacks, a new authenticate technique is now available. This new authentication technique, known as 3D Password (Dhatri Raval 2015).

III. METHODOLOGY

ANALYSIS OF THE SYSTEM

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.

The password is D.

Password that is based on numbers

Techniques based on one-time passwords

Existing Authentication System has the following flaw:

Password in Text:

Textual passwords should be simple to remember while also being difficult to guess. However, if a textual Secured authentication: 3D password 243 password is tough to guess, it will be even more difficult to remember. 2 *1014 is the maximum password length for an 8-character password with both numbers and characters. According to a study, brute force dictionary can properly guess 25% of passwords out of 15,000 users.

Graphical Password:

Users can remember and recognise visuals better than words, hence graphical passwords were created. However, most graphical passwords are vulnerable to shoulder surfing attacks, in which an attacker uses a camera to see or record a valid user's graphical password. The biggest disadvantage of using biometrics is that it is obtrusive to a user's personal traits. They necessitate the use of a specialised scanning instrument to verify the user, which is inconvenient for remote or internet users. Smart cards can be lost or stolen, hence the user must always carry the token with them.

Advantages

A 3D password is more secure than a text or graphical password.

1. It allows the user to select the form of authentication he or she prefers.

- Users can choose from a variety of options to create their own sequence.
- A 3D password allows the user to create a sequence that is easier to remember.

2. It prevents brute-force attacks.

- All data and sensitive information, such as passwords, are encrypted, making brute force attacks difficult to decipher.
- Because 3D passwords use a combination of recognition and recall, they are difficult to remember. 3. Provides a high level of protection for the system that includes more sensitive information.
- It provides data security by utilising numerous aspects and techniques to protect data.

3. Protect yourself from malicious malware such as key loggers.

- When software such as a key logger is installed on a computer, it is impossible to protect your data because these programmes save all word typed on the keyboard. A graphical password is also used for authentication in 3D passwords.

IV. RESULT AND DISCUSSION

IMPLEMENTATION

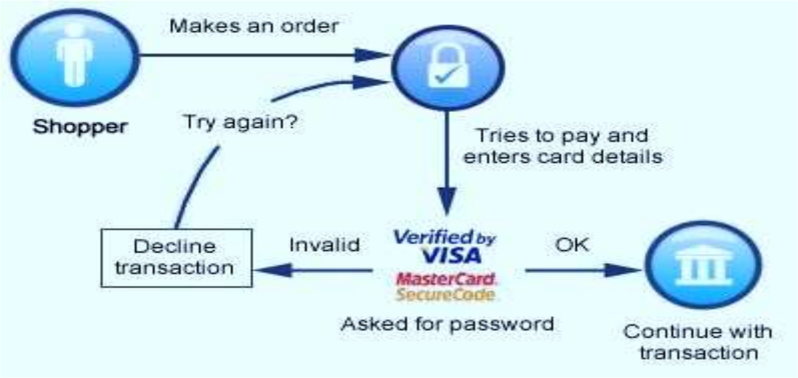

Figure 1. Security using 3D password

Textual passwords, biometric scanning, tokens or cards (such as an ATM), and other password models are now available to users. As previously stated, most textual passwords use an encryption method. Biometric scanning serves as your "natural" signature, while Cards or Tokens serve as proof of your identity. However, some people despise having to carry their cards with them, and others reject to have their retinas exposed to powerful IR (Biometric scanning). Nowadays, most textual passwords are kept basic, such as a phrase from the dictionary With the advancement of technology, fast computers, and a plethora of Internet-based applications, this has become a child's game.or their pet names. Klein used to do these tests and could crack 10-15 passwords every day.

As a result, we introduce our concept, 3D passwords, which are more personalised and a fun method to authenticate. Passwords are now predicated on the fact that humans have memory. Simple passwords are usually used so that they may be remembered easily. In our concept, the human memory must go through the processes of recognition, recall, biometrics, and token-based authentication. The 3D password GUI appears once you've implemented it and logged in to a secure site. This is a second textual password that the user can type in. A 3D virtual room will appear on the screen after he completes the first authentication. Let's imagine we're talking about a virtual garage.

APPLICATIONS

In comparison to other authentication techniques, the password space for a 3D password might be quite extensive. Protecting vital systems and resources is one of 3D password's key application domains.

1. Critical Servers: A textual password is commonly used to safeguard critical servers in many major enterprises. A sound replacement for a textual password is a 3D password authentication.
2. Airplanes and jet fighters: Because there is a risk of misusing planes and jet fighters for religious or political purposes, the use of such planes should be protected by a robust authentication mechanism.

3. Banking: 3D passwords, similar to credit card passwords for online transactions.

V. CONCLUSION

Textual and token-based passwords are now utilised for authentication and are subject to a variety of attacks. The 3D Password is a multi-featured, multi-factor authentication technique that integrates the advantages of existing authentication schemes into a single virtual 3D environment. The 3-D password is a relatively new authentication method that is still in its infancy. The user experience of the 3-D password will be enhanced and improved by designing various sorts of 3-D virtual settings, deciding on password spaces, and evaluating user input and experiences from such environments. The user's preferences and requirements for the purpose of creating a 3D password are reflected in the 3D password**.** The user's preferences and requirements for authentication are reflected in the 3D password, making 3D password usage user-friendly. In comparison to other authentication mechanisms, the 3D Password technique is more safe and trustworthy. We can make any system more secure by utilising 3d Password, and it will be advantageous for apps used in the business world, the government sector, and personal usage.

REFERENCES

1. http://www.ijesit.com/Volume%202/Issue%202/IJESIT2 0130 2_16.pdf
2. 3D Password: Minimal Utilization of Space and Vast Security Coupled with Biometrics for Secure Authentication.
3. http://www.ijater.com/Files/b8d368dffb71-4b45-95c5-0a7a4b266a1c_IJATER_05_15.pdf
4. Duhan Pooja, Gupta Shilpi, Sangwan Sujata, & Gulati Vinita "SECURED AUTHENTICATION: 3D PASSWORD" International Journal of Engineering and Management Studies
5. Alsulaiman, F.A.; El Saddik, A., "Three -for Secure" IEEE Transactions on Instrumentation and measurement, vol.57, no.9, pp 1929 - 1938.Sept. 2008.
6. Vishal Kolhe, Vipul Gunjal, Sayali Kalasakar, Pranjal Rathod "Secure Authentication with 3D Password" International Journal of Engineering Science and Innovative Technology (IJESIT)
7. 3D Password: A Novel Approach for More Secure Authentication. ttp://www.ijcset.com/docs/IJCSET14-05-02-080.pdf
8. S. Ranjitha "Secure Authentication with 3D Password" IFET College of Engineering