INTERNATIONAL JOURNAL OF ENGINEERING AND MANAGEMENT SCIENCES

www.scienceandnature.org

SECURED AUTHENTICATION: 3D PASSWORD

*** Duhan Pooja, Gupta Shilpi , Sangwan Sujata, & Gulati Vinita**
Department of Computer Science and Engineering, Dronacharya College Of Engineering, Gurgaon

ABSTRACT
Authentication is a process of validating who are you to whom you claimed to be or a process of identifying an individual, usually based on a username and password. We have many authentication schemes but they have some drawbacks. So 3D password is introduced. The 3-D password is a multifactor authentication scheme. It can combine all existing authentication schemes into a single 3-D virtual environment. This 3-D virtual environment contains several objects or items with which the user can interact. The type of interaction varies from one item to another. The 3-D password is constructed by observing the actions and interactions of the user and by observing the sequences of such actions. In other words, The 3D Password scheme is a new authentication scheme that combine RECOGNITION + RECALL+TOKENS+BIOMETRIC in one authentication system. 3D passwords are flexible and they provide unlimited passwords possibility. They are easy to Memorize and can be remembered in the form of short story. 3D passwords have many application areas such as Critical Servers, Nuclear and military Facilities, Airplanes and Jet Fighters, ATMs, Desktop and Laptop Logins, Web Authentication etc. In this research paper we have compared 3D password authentication system with existing system and discussed about implementation and working of 3D password system. Let us consider a 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. We assume that the user can navigate into the 3D virtual environment and interact with the objects using any input device such as a mouse, key board, fingerprint scanner, iris scanner, stylus, card reader, and microphone. We consider the sequence of those actions and interactions using the previous input devices as the user's 3D password. We have also provided security analysis against various attacks such as Brute Force Attack, Well-Studied Attack, Shoulder Surfing Attack, Timing attack etc.

KEYWORDS: Authentication, Biometrics, 3D password,

INTRODUCTION

The authentication system which we are using is mainly very light or very strict. Since many years it has become an interesting approach. With the development in means of technology, it has become very easy for 'others' to hack someone's password. Therefore many algorithms have come up each with an interesting approach toward calculation of a secret key. The algorithms are such based to pick a random number in the range of 10^6 and therefore the possibilities of the sane number coming is rare. We are provided with many password types such as textual passwords, biometric scanning, tokens or cards (such as an ATM) etc. But there are many weaknesses in current authentication systems.

When a person uses textual passwords, he likely chooses meaningful words from dictionary or their nick names, girlfriends etc which can be cracked easily. And if a password is hard to guess then it is hard to remember also. Users face difficulty in remembering a long and random appearing password and because of that they create small, simple, and insecure passwords that are easy to attack. Graphical passwords can also be used. Their strength comes from the fact that users can recall and recognize pictures more than words. Token based systems can also be used as way of authentication in banking systems and for entrance in laboratories. But smart cards or tokens are susceptible to loss or theft. Biometric scanning is your "natural" signature and Cards or Tokens prove your validity. Many years back Klein performed tests and he could crack almost 15 passwords per day. As the technology has changed many fast processors and tools are available on internet it has become very easy. So in this paper , we have introduced 3-d password scheme.

AUTHENTICATION

Authentication is a process of validating who are you to whom you claimed to be or a process of identifying an individual, usually based on a username and password.
Human Authentication Techniques are as follows:

- Knowledge Base (What you know)
- Token Based(what you have)
- Biometrics(what you are)
- Recognition Based(What you recognise)

Computer Authentication Techniques are as follows:

- Textual Passwords (Recall Based)-Recall what you have created before.
- Graphical Passwords (Recall Based + Recognition Based)
- Biometric schemes (fingerprints, voice recognition etc)

DRAWBACKS IN EXISTING AUTHENTICATION SYSTEM

Textual Password: Textual Passwords should be easy to remember at the same time hard to guess. But if a textual

password is hard to guess then it is very difficult to remember also. Full password space for 8 characters consisting of both numbers and characters is 2 *1014.From a research 25% of the passwords out of 15,000 users can guessed correctly by using brute force dictionary.

Graphical Password

Graphical passwords came as users can recall and recognize pictures more then words. But most graphical passwords are susceptible for shoulder surfing attacks, where an attacker can observe or record the valid user graphical password by camera. The main weakness while applying biometric is its intrusiveness upon a users personnel characteristics. They require special scanning device to verify the user which is not acceptable for remote and internet users. Smart cards can be lost or stolen and the user has to carry the token whenever access required.

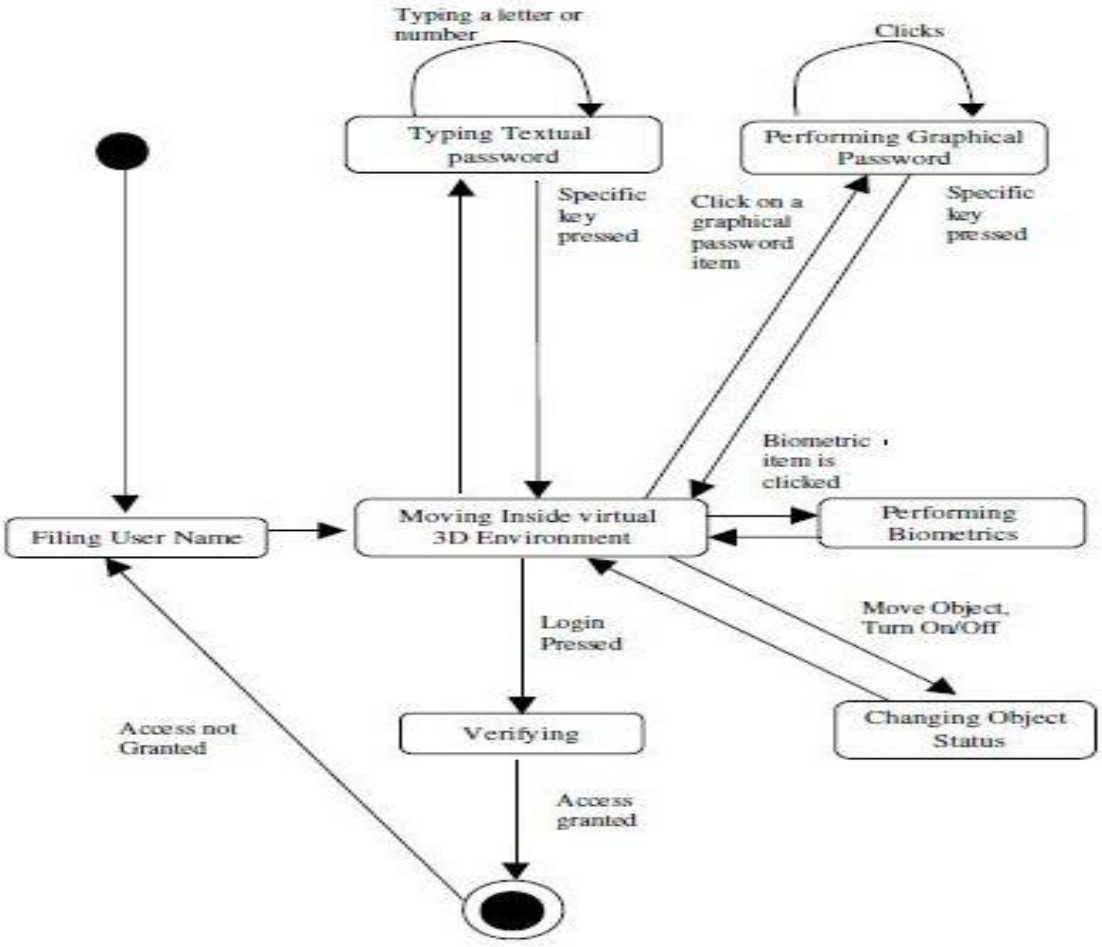
PROJECTED SYSTEM

The projected system is a multi factor authentication scheme which combines the advantages of other authentication schemes. Users can choose whether the 3D password will be only recall, biometrics, recognition, or token based, or a combination of two schemes or more. This choice of selection is necessary because users are different and they have different requirements. So, for surety of high user acceptability, the user's freedom of selection is essential. The following necessities are satisfied in proposed scheme:

1. The new scheme provide secrets that are easy to remember and very difficult for intruders to guess.
2. The new scheme provides secrets that are not easy to write down on paper. Moreover, the scheme secrets should be difficult to share with others.
3. The new scheme provides secrets that can be easily revoked or changed.

3D PASSWORD SCHEME?

The 3D Password scheme is a new authentication scheme that combine RECOGNITION + RECALL+TOKENS+BIOMETRIC in one authentication system. The 3-D password is a multifactor authentication scheme. It can combine all existing authentication schemes into a single 3-D virtual environment. This 3-D virtual environment contains several objects or items with which the user can interact. The type of interaction varies from one item to another. The 3-D password is constructed by observing the actions and interactions of the user and by observing the sequences of such actions. It is the user's choice to select which type of authentication techniques will be part of their 3-D password.



State Diagram

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 the user prefers not to provide. For example, if an item requests an iris scan and the user is not comfortable in providing such information, the user simply avoids interacting with that item. Moreover, giving the user the freedom of choice as to what type of authentication schemes will be part of their 3-D password and given the large number of objects and items in the environment, the number of possible 3D passwords will increase. Thus, it becomes much more difficult for the attacker to guess the user's 3-D password

SYSTEM IMPLIMENTATION

The 3D password is a multi factor authentication scheme. The 3D password presents a 3D virtual environment containing various virtual objects. The user navigates through this environment and interacts with the objects. The 3D password is simply the combination and the sequence of user interactions that occur in the 3D virtual environment. The 3D password can combine recognition, recall, token, and biometrics based systems into one 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.

For example, the user can enter the virtual environment and type something on a computer that exists in (x1 , y1 , z1) position, then enter a room that has a fingerprint recognition device that exists in a position (x2 , y2 , z2) and provide his/her fingerprint. Then, the user can go to the virtual garage, open the car door, and turn on the radio to a specific channel. The combination and the sequence of the previous actions toward the specific objects construct the user's 3D password.

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

1. A computer with which the user can type.
2. A fingerprint reader that requires the user's fingerprint.
3. A biometric recognition device.
4. A paper or a white board that a user can write, sign, or draw on.
5. An ATM machine that requires a smart card and PIN.
6. A light that can be switched on/off.
7. A television or radio where channels can be selected.
8. A staple that can be punched.
9. A car that can be driven.
10. A chair that can be moved from one place to another.
11. Any graphical password scheme

WORKING

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 (x,y,z) coordinates. Assume 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 interactions with objects can be a mouse, a keyboard, stylus, a card reader, a microphone…etc.

For example, consider a user who navigates through the 3D virtual environment that consists of a ground and a classroom. Let us assume that the user is in the virtual ground and the user turns around to the door located in (9, 16, 80) and opens it. Then, the user closes the door. The user types "ANGEL" into a computer that exists in the position of (10, 5, 25). The user then walks over and turns off the light located in (15, 6, 20), and then goes to a white board located in (55, 3, 30) and draws just one dot in the (x,y) coordinate of the white board at the specific point of (420,170). The user then presses the login button. The initial representation of user actions in the 3Dvirtual environment can be recorded as follows:

(9, 16, 80) Action = Open the office door;
(9, 16, 80) Action = Close the office door;
(10, 5, 25) Action = Typing, "A";
(10, 5, 25) Action = Typing, "N";
(10, 5, 25) Action = Typing, "G";
(10, 5, 25) Action = Typing, "E";
(10, 5, 25) Action = Typing, "L";
(15, 6, 20) Action = Turning the Light Off;
(55, 3, 30) Action = drawing , point = (420,170);

3D PASSWORDS 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 users privacy.

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.

   How to Create 3D password for my master card?

   Our online payment will fail, if will create 3D password, so for generating 3D password, we have to go to our bank's website and then, click 3D secure service and then write our card number, CVV, pin no., and write our password and rewrite it and then click ok or submit. After this we will get thank you message. Like PNB, SBI also started 3D secure services for verified by Visa.Verified by Visa is a new service that will let you use a personal password with your State Bank of India

Visa card, giving you added assurance that only you can use your State Bank of India Visa card to make purchases over the Internet.

3. **Nuclear and military Facilities:** 3D password has a very large password space and since it combine 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 jetplanes can be misused for religion and political agendas, they should be protected by a powerful authentication scheme.
5. ATMs, Desktop and Laptop Logins, Web Authentication.

SECURITY ANALYSIS

Brute Force Attack

The attack is very difficult because

1. Time required to login may vary form 20s to 2 min therefore it is very time consuming.
2. Cost of Attack: A 3D Virtual environment may contain biometric object, the attacker has to forge all biometric information.

Well-Studied Attack

The attacker tries to find the highest probable distribution of 3D passwords. In order to launch such an attack, the attacker has to acquire knowledge of the most probable 3D password distributions. This is very difficult because the attacker has to study all the existing authentication schemes that are used in the 3D environment. It requires a study of the user's selection of objects for the 3D password. Moreover, a well studied attack is very hard to accomplish since the attacker has to perform a customized attack for every different 3D virtual environment design. This environment has a number of objects and types of object responses that differ from any other 3D virtual environment. Therefore, a carefully customized study is required to initialize an effective attack.

Shoulder Surfing Attack

An attacker uses a camera to record the user's 3D password or tries to watch the legitimate user while the 3D password is being performed. This attack is the most successful type of attack against 3D passwords and some other graphical passwords. However, the user's 3D password may contain biometric data or textual passwords that cannot be seen from behind. Therefore, we assume that the 3D password should be performed in a secure place where a shoulder surfing attack cannot be performed.

Timing Attack

The Attacker observes how long it takes the legitimate user to perform correct log in using 3D Password which gives an indication of 3-D Passwords length. This attack cannot be succesful since it gives the attacker mere hints.

CONCLUSION AND FUTURE WORK

In the existing system, Textual passwords and token-based passwords are the most common used authentication schemes. Many other schemes are also there like graphical password, biometric authentication scheme etc which are used in different fields. The main goal of this paper is to have a scheme which has a huge password space and which is a combination of any existing, or upcoming, authentication schemes into one scheme.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 provide their fingerprints if they do not wish to. 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 three-dimensional virtual environment can contain any objects that the administrator feels that the users are familiar with. For example, Cricket players can use a three dimensional virtual environment of a stadium where they can navigate and interact with objects that they are familiar with.

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.

The main application domains of 3D Password are critical systems and resources. Critical systems such as military facilities, critical servers and highly classified areas can be protected by 3D Password system with large three dimensional virtual environment. Moreover, Airplanes and jet fighters, ATM's and operating system's logins can also make use of 3D passwords to provide more secured authentication Finding a solution for shoulder surfing attacks on 3D passwords and other authentication schemes is a field of study.

REFERENCES

X. Suo, Y. Zhu, and G. S. Owen, "Graphical passwords: A survey," in Proc. 21st Annu. Comput. Security Appl. Conf., Dec. 5–9, 2005, pp. 463–472.

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

Daniel V.Klein. Foiling the Cracker: A Survey of, and Improvement to Passwords Security. Proceedings of the USENIX Security Workshop, 1990

NBC news, ATM Fraud: Banking on Your Money, Dateline Hidden Cameras Show Criminals Owning ATMs, Dec. 11, 2003.

Real User Corporation. The Science Behind Passfaces.http://www.realusers.com accessed October 2005.

[6] BBC news, Cash Machine Fraud up, Say Banks, Nov. 4, 2006.

Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, Nasir Memon. Authentication Using Graphical Passwords: Basic Results. In the Proceedings of Human-Computer Interaction International, Las Vegas, July 25-27, 2005.