ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol. 3 , No.1, Pages : 142– 148 (2014)
Special Issue of ICETETS 2014 - Held on 24-25 February, 2014 in Malla Reddy Institute of Engineering and Technology, Secunderabad– 14, AP, India

3D Password Authentication

S.Nikitha[1], Mr.L.Naresh Babu[2] ,V.S.Pratyusha[3]

[1,3] UNDER GRADUATE STUDENTS, DEPT OF C.S.E ,MALLA REDDY INSTITUTE OF ENGINEERING AND TECHNOLOGY, INDIA,singireddy.nikitha95@gmail.com, santoshi_pratyusha@yahoo.co.in

[2]ASSISTANT PROFESSOR, DEPT OF C.S.E MALLA REDDY INSTITUTE OF ENGINEERING AND TECHNOLOGY, INDIA,lellanaresh523@gmail.com

1.ABSTRACT

Users nowadays are provided with major password stereotypes such as textual passwords, biometric scanning, tokens or cards (such as an ATM) etc. Current authentication systems suffer from many weaknesses.

Textual passwords are commonly used; however, users do not follow their requirements. Users tend to choose meaningful words from dictionary or their pet names, girlfriends etc. Ten years back Klein performed such tests and he could crack 10-15 passwords per day. On the other hand, if a password is hard to guess, then it is often hard to remember. Users have difficulty remembering a password that is long and random appearing. So, they create short, simple, and insecure passwords that are susceptible to attack.Which make textual passwords easy to break and vulnerable to dictionary or brute force attacks.

Graphical passwords schemes have been proposed. The strength of graphical passwords comes from the fact that users can recall and recognize pictures more than words.Most graphical passwords are vulnerable for shoulder surfing attacks, where an attacker can observe or record the legitimate user's graphical password by camera. Token based systems such as ATMs are widely applied in banking systems and in laboratories entrances as a mean of authentication.

In this paper, we present and evaluate our contribution, i.e., the 3-D password. The 3-D password is a multifactor authentication scheme. To be authenticated, we present a 3-D virtual environment where the user navigates and interacts with various objects. The sequence of actions and interactions toward the objects inside the 3-D environment constructs the user's 3-D password. The 3-D password can combine most existing authentication schemes such as textual passwords, graphical passwords, and various types of biometrics into a 3-D virtual environment. The design of the 3-D virtual environment and the type of objects selected determine the 3-Dpassword key space

2. AUTHENTICATION

Authentication is the act of establishing or confirming something as authentic, that is, that claims made by or about the subject are true. This might involve confirming the identity of a person, tracing the origins of an artifact, ensuring that a product is what it's packaging and labeling claims to be, or assuring that a computer program is a trusted one.

For example, when you show proper identification credentials to a bank teller, you are asking to be authenticated to act on behalf of the account holder. If your authentication request is approved, you become authorized to access the accounts of that account holder, but no others.

3. AUTHENTICATION METHODS

The first is comparing the attributes of the object itself to what is known about objects of that origin. For example, an art expert might look for similarities in the style of painting, check the location and form of a signature, or compare the object to an old photograph. An archaeologist might use carbon dating to verify the age of an artifact, do a chemical analysis of the materials used, or compare the style of construction or decoration to other artifacts of similar origin. The physics of sound and light, and comparison with a known physical environment, can be used to examine the authenticity of audio recordings, photographs, or videos.

The second type relies on documentation or other external affirmations. For example, the rules of evidence in

criminal courts often require establishing the chain of custody of evidence presented. This can be accomplished through a written evidence log, or by testimony from the police detectives and forensics staff that handled it. Some antiques are accompanied by certificates attesting to their authenticity. External records have their own problems of forgery and perjury, and are also vulnerable to being separated from the artifact and lost.

Currency and other financial instruments commonly use the first type of authentication method. Bills, coins, and cheques incorporate hard-to-duplicate physical features, such as fine printing or engraving, distinctive feel, watermarks, and holographic imagery, which are easy for receivers to verify.

Consumer goods such as pharmaceuticals, perfume, fashion clothing can use either type of authentication method to prevent counterfeit goods from taking advantage of a popular brand's reputation (damaging the brand owner's sales and reputation). A trademark is a legally protected marking or other identifying feature which aids consumers in the identification of genuine brand-name goods.

4. BRIEF DESCRIPTION OF THE SYSTEM

The proposed system is a multi factor authentication scheme. It can combine all existing authentication schemes into a single 3Dvirtual environment. This 3D virtual environment contains several objects or items with which the user can interact. The user is presented with this 3D virtual environment where the user navigates and interacts with various objects. The sequence of actions and interactions toward the objects inside the 3D environment constructs the user's 3Dpassword.The 3D password can combine most existing authentication schemes such as textual passwords, graphical passwords, and various types of biometrics into a 3D virtual environment.

The choice of what authentication schemes will be part of the user's 3D password reflects the user's preferences and requirements. A user who prefers to remember and recall a password might choose textual and graphical password as part of their 3D password. On the other hand users who have more difficulty with memory or recall might prefer to choose smart cards or biometrics as part of their 3D password. Moreover user who prefers to keep any kind of biometric data private might not interact with object that requires biometric information. Therefore it is the user's choice and decision to construct the desired and preferred 3D password.

5. INNOVATIVE COMPONENT

The proposed system is a multi factor authentication scheme that combines the benefits of various authentication schemes. Users have the freedom to select whether the 3D password will be solely recall, recognition, or token based, or combination of two schemes or more. This freedom of selection is necessary because users are different and they have different requirements. Therefore, to ensure high user acceptability, the user's freedom of selection is important.

The following requirements are satisfied in the 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.

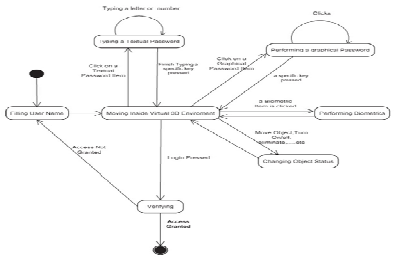
3. The new scheme provides secrets that can be easily revoked or changed.

6. 3D PASSWORD

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.

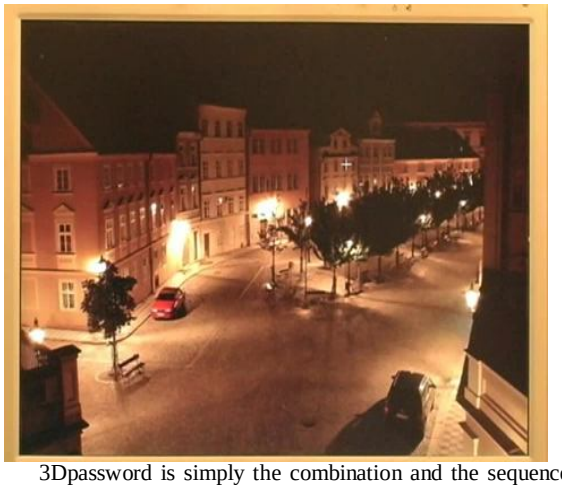
For example, if an item requests an iris scan and the user is not comfortable in providing such information, the user simply avoids interacting with that item. Moreover, giving the user the freedom of choice as to what type of authentication schemes will be part of their 3-D password and given the large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

7. STATE DIAGRAM



8. SYSTEM IMPLEMENTATION

The 3Dpassword is a multi factor authentication scheme. The 3Dpassword presents a 3Dvirtual environment containing various virtual objects. The user navigates through this environment and interacts with the objects. The



3Dpassword is simply the combination and the sequence of user interactions that occur in the 3Dvirtual environment.

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

Snapshot of a proof-of-concept 3-D virtual environment, where the user is typing a textual password on a virtual computer as a part of the user's 3-D password

Snapshot of an experimental 3-D virtual environment

9. 3-D VIRTUAL ENVIRONMENT DESIGN

The design of the 3 D virtual environments affects the usability, effectiveness, acceptability of 3D password. The first step in building a 3-Dpassword system is to design a 3-Denvironment that reflects the administration needs and the security requirements.

The design of 3-D virtual environments should follow these guidelines.

1) Real Life-Similarity- The prospective 3D virtual environment should reflect what people are used to seeing in real life. Objects used in virtual environments should be relatively similar in size to real objects (sized to scale). Possible actions and interactions toward virtual objects should reflect real life situations. Object responses should be realistic. The target should have a 3-D virtual environment that users can interact.

2) Object Uniqueness and Distinction-

Every virtual object or item in the 3-D virtual environment is different from any other virtual object. The uniqueness comes from the fact that every virtual object has its own attributes such as position. Thus, the prospective interaction with object 1 is not equal to the interaction with object2. However, having similar objects such as 20 computers in one place might confuse the user. Therefore, the design of the 3-D virtual environment should consider that every object should be distinguishable from other objects. Similarly, in designing a 3-Dvirtual environment, it should be easy for users to navigate through and to distinguish between objects. The distinguishing factor increases the user's recognition of objects. Therefore, it improves the system usability.

3) Three Dimensional Virtual Environment Size-

A 3-Dvirtual 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. A large 3¬D virtual environment will increase the time required by the user to perform a 3-Dpassword. Moreover, a large3-Dvirtual environment can contain a large number of virtual objects. Therefore, the probable 3-Dpassword space broadens. However, a small 3-D virtual environment usually contains only a few objects, and thus, performing a 3-D password will take less time.

4) Number of Objects and Their Types-

Part of designing a 3-D virtual environment is determining the types of objects and how many objects should be placed in the environment. The types of objects reflect what kind of responses the object will have. For simplicity, we can consider requesting a textual password or a fingerprint as an object response type. Selecting the right object response types and the number of objects affects the probable password space of a 3-D password.

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.

10. APPLICATIONS

The 3D password can have a password space that is very large compared to other authentication schemes, so the 3-D password's main application domains are protecting critical systems and resources.

1. Critical Servers-

Many large organizations have critical servers that are usually protected by a textual password. 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 3-D 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.

3. Airplanes and Jet Fighters-

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

In addition, 3-D passwords can be used in less critical systems because the 3D virtual environment can be designed to fit to any system needs. A small virtual environment can be used in the following systems like

Some other applications are:

- ATM
- Desktop Computers & laptop logins
- Web Authentication

11. SECURITY ANALYSIS

To analyze and study how secure a system is, we have to consider,

- ***How hard it is for the attacker to break such a system***

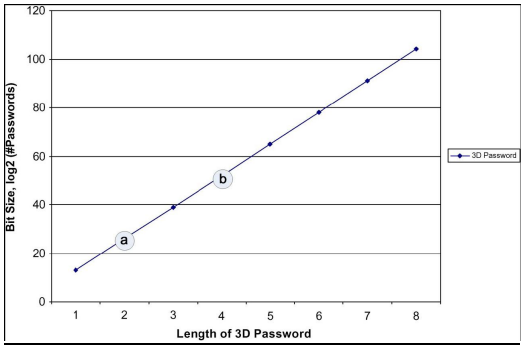
A Possible measurement is based on the information content of a password space. The textual password space may be relatively large; however, an attacker might only need a small subset of the full password space is observed to successfully break such an authentication system. It is important to have a scheme that has a very large possible password space which increases the work required by the attacker to break the authentication system. Find a scheme

that has no previous or existing knowledge of the most probable user password selection.

- ***Common guidelines for choosing good passwords are designed to make passwords less easily discovered by intelligent guessing:***

- Include numbers, symbols, upper and lowercase letters in passwords if allowed by the system
- Password length should be around 12 to 14 characters if permitted, and longer still if possible while remaining memorable
- If the system recognizes case as significant, use capital and lower-case letters
- Avoid any password based on repetition, dictionary words, letter or number sequences, usernames, relative or pet names, romantic links (current or past), or biographical information (e.g., dates, ID numbers, ancestors names or dates, ...)
- Password should be easy to remember for the user, and not force insecure actions (e.g., the very bad and insecure practice of writing the password down on a Post-It note stuck to the monitor)

3D PASSWORD SPACE SIZE



To determine 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.

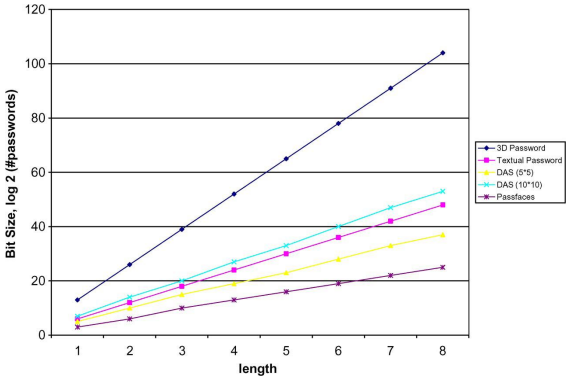


FIG: Password space of the 3-D password, textual password, Pass faces, and DAS with grid sizes of 5 × 5 and 10 × 10. Length is the number of actions and interactions for a 3-D password, the number of characters for textual passwords, the number of selections for Pass faces, and the number of points that represent the strokes for DAS. The length is up to eight.

Fig: Observing the number of possible actions/interactions of a 3-D password within a 3-D environment specified in Section V-A compared to the two critical Points of textual passwords. Point "a" is the bit size of Klein [2] (3 × 106) dictionary of eight-character textual passwords. Point "b" represents the full passwordspace of eight-character textual passwords.

ADVANTAGES

Easiness to memorize: Users can memorize a 3D password as a "little" story which makes the password easy to remember

- **Flexibility**: 3d passwords allows multi-factor authentication. Smart cards, biometrics and alpha num password can embedded in the 3d password technology
- **Strength**: A scenario in a 3D environment offers as almost unlimited combination of possibilities. As such system can have specific 3d world, hack are extremely difficult.
- The 3D password gives users the freedom of selecting what type of authentication techniques.
- Secrets those are not easy to write down on paper.
- The scheme secrets should be difficult to share with others.
- Provide secrets that can be easily revoked or changed.

12. ATTACKS

1) Brute Force Attack- The attacker has to try all possible 3D passwords. This kind of attack is very difficult for the following reasons.

Time required to login- The total time needed for a legitimate user to login may vary depending on the number of interactions and actions, the size of the 3-D virtual environment, and the type of actions and interactions. Therefore, a brute force attack on a 3-D password is very difficult and time consuming.

Cost of attacks –The 3-D virtual environment contains biometric recognition objects and token based objects. The attacker has to forge all possible biometric information and forge all the required tokens. The cost of forging such information is very high; therefore cracking the 3D password is more challenging. The high number of possible 3D password spaces leaves the attacker with almost no chance of breaking the 3-D password.

2)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 3-D 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 3-D virtual environment design. This environment has a number of objects and types of object responses that differ from any other 3-D virtual environment. Therefore, a carefully customized study is required to initialize an effective attack

3) Shoulder Surfing Attack- An attacker uses a camera to record the user's 3-D password or tries to watch the legitimate user while the 3-D 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 3-D password may contain biometric data or textual passwords that cannot be seen from behind. Therefore, we assume that the 3-D password should be performed in a secure place where a shoulder surfing attack cannot be performed.

4) Timing Attack-

In this attack, the attacker observes how long it takes the legitimate user to perform a correct sign-in using the 3-D password. This observation gives the attacker an indication of the legitimate user's 3-D password length. However, this kind of attack alone cannot be very successful since it gives the attacker mere hints. Therefore, it would probably be launched as part of a well studied or brute force attack. Timing attacks can be very effective if the 3D virtual environment is poorly designed.

13. CONCLUSION

There are many authentication schemes in the current state. Some of them are based on user's physical and behavioral properties, and some other authentication schemes are based on user's knowledge such as textual and graphical passwords. Moreover, there are some other important authentication schemes that are based on what you have, such as smart cards. Among the various authentication schemes, textual password and token-based schemes, or the combination of both, are commonly applied.

The 3-D password is a multifactor authentication scheme that combines these various authentication schemes into a single3-D virtual environment. The virtual environment can contain any existing authentication scheme or even any upcoming authentication schemes by adding it as a response to actions performed on an object. Therefore, the resulted password space becomes very large compared to any existing authentication schemes.

The design of the 3-D virtual environment, the selections of objects inside the environment, and the object's type reflect the resulted password space. It is the task of the system administrator to design the environment and to select the appropriate object that reflects the protected system requirements. Additionally, designing a simple and easy to use 3-D virtual environment is a factor that leads to a higher user acceptability of a 3-D password system.

The choice of what authentication schemes will be part of the user's 3-D password reflects the user's preferences and requirements. A user who prefers to remember and recall a password might choose textual and graphical passwords apart of their 3-D password. On the other hand, user's who have more difficulty with memory or recall might prefer to choose smart cards or biometrics as part of their 3-D

password. Moreover, users who prefer to keep any kind of biometrical data private might not interact with objects that require biometric information. Therefore, it is the user's choice and decision to construct the desired and preferred 3-D password.

14. FUTURE WORK

Textual passwords and token-based passwords are the most common user authentication schemes. However, many different schemes have been used in specific fields. Other schemes are under study yet they have never been applied in the real world. The motivation of this work is to have a scheme that has a huge password space while also being a combination of any existing, or upcoming, authentication schemes into one scheme. A 3D password gives the user the choice of modeling his 3D password to contain any authentication scheme that the user prefers. Users do not have to provide their fingerprints if they do not wish to.

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, football 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 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, a small three-dimensional virtual environment can be used to protect less critical systems such as handhelds, ATM's and operating system's logins.

Acquiring the knowledge of the probable distribution of a user's 3D password might show the practical strength of a 3D password. Moreover, finding a solution for shoulder surfing attacks on 3D passwords and other authentication schemes is also a field of study.

15. REFERENCES

- 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
- Greg E. Blonder, Graphical Password, United State Patent 5559961
- Rachna Dhamija, Adrian Perrig, Déjà Vu: A User Study Using Images for Authentication. 2000, Denver, Colorado, pages 45-58.