INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

THREE-DIMENSIONAL PASSWORD SYSTEM IMPLEMENTATION TECHNIQUE

RONAK B. SINGH, ZEESHAN I. KHAN

1. **B.E, Department of CSE, IBSS College of Engineering, Amravati.**
2. **Asst. Prof., Department of CSE, IBSS College of Engineering, Amravati.**

Accepted Date:

27/02/2013

Publish Date:

01/04/2013

Keywords

3 D Password

System

Implementation

Corresponding Author

Mr. Ronak B. Singh

Abstract

The 3-D password is a multifactor authentication scheme that can combine most existing authentication schemes such as textual passwords, graphical passwords, and various types of biometrics into a 3-D virtual environment. The user navigates and interacts with various objects in 3-D virtual environment. The sequence of actions and interactions toward the objects inside the 3-D environment constructs the user's 3-D password. The method of implementing 3-D Password system after building 3-D virtual environment should be more secured to prevent possibility of security attacks.

I. INTRODUCTION

The Dramatic increase of computer usage has given rise to many security concerns. One major security concern is authentication, which is the process of validating who you are to whom you claimed to be. 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. 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 [1].

Now, in a 3-D virtual environment space of size $G \times G \times G$, the objects are distributed with unique (x, y, z) coordinates and saved with reference to those co-ordinates as a user's 3-D Password including the references of other authentication scheme if used [1]. But it is possible that attacker by using various methods of security attack can succeed in recovering those co-ordinates and thus a chance of recovering 3-D password increases as each co-ordinate represent some action in 3-D virtual environment. Hence, to avoid these we can represent each action of 3-D virtual environment as a unique code instead of (x, y, z) co-ordinates. And then, we can encrypt these unique codes and save as a user's 3-D password. So, if also attacker succeeds in recovering the password he will get the password in form of these unique codes which will fail him to find related action in 3-D virtual environment. A system carries records of all action and its corresponding unique code to verify user's 3-D password. Thus, it increases the security level of 3-D password system.

II. 3-D PASSWORD SCHEME

The multifactor authentication scheme that combines the benefits of various authentication schemes should satisfy the following requirements.

1) The new scheme should not be either recall based or recognition based only. Instead, the scheme should be a combination of recall, recognition, biometrics, and token-based authentication schemes.

2) Users ought to have the freedom to select whether the 3-D password will be solely recall, biometrics, recognition, or token-based, or a combination of two schemes or more. This freedom of selection is necessary because users are different and they have different requirements. Some users do not like to carry cards. Some users do not like to provide biometrical data, and some users have poor memories. Therefore, to ensure high user acceptability, the user's freedom of selection is important.

3) The new scheme should provide secrets that are easy to remember and very difficult for intruders to guess.

4) The new scheme should provide secrets that are not easy to write down on paper. Moreover, the scheme secrets should be difficult to share with others.

5) The new scheme should provide secrets that can be easily revoked or changed.

A. 3-D Password Overview

The 3-D password is a multifactor authentication scheme. The 3-D password presents a 3-D virtual environment containing various virtual objects. The user navigates through this environment and interacts with the objects. The 3-D password is simply the combination and the sequence of user interactions that occur in the 3-D virtual environment. The 3-D password can combine recognition, recall, token, and biometrics-based systems into one authentication scheme. This can be done by designing a 3-D virtual environment that contains objects that request information to be recalled, information to be recognized, tokens to be presented, and biometrical data to be verified.

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 3-D environment toward the virtual objects. Moreover, any user input (such as speaking in a specific location) in the virtual 3-D environment can be considered as a part of the 3-D 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 biometrical recognition device;
4. A paper or a white board that a user can write, sign, or draw on;
5. An automated teller machine (ATM) that requests a token;
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 book that can be moved from one place to another;
11. Any graphical password scheme;
12. Any real-life object;
13. Any upcoming authentication scheme.

To perform the legitimate 3-D password, the user must follow the same scenario performed by the legitimate user. This means interacting with the same objects that reside at the exact locations and perform the exact actions in the proper sequence [1].

B. 3-D Virtual Environment Design Guidelines

Designing a well-studied 3-D virtual environment affects the usability, effectiveness, and acceptability of a 3-D password system. Therefore, the first step in building a 3-D password system is to design a 3-D environment 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 3-D 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 with, by using common sense.

2) Object uniqueness and distinction: Every virtual objector item in the 3-D virtual environment is different from many 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 object 2. 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. In designing a 3-D virtual 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-D virtual 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. The size of a 3-D environment should be carefully studied. A large 3-D virtual environment will increase the time required by the user to perform a 3-D password. Moreover, a large 3-D virtual environment can contain a large number of virtual objects. Therefore, the probable 3-D password 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 (items) 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 finger print 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 3-D virtual environment should consider what systems will be protected by a 3-D password. The number of objects and the types of objects that have been used in the 3-D virtual environment should reflect the importance of the protected system [1].

III. 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, which is defined in as "the entropy of the probability distribution over that space given by the relative frequencies of the passwords that users actually choose." We have seen that textual password space may be relatively large; however, an attacker might only need a small subset of the full password space as Klein observed to successfully break such an authentication system. As a result, it is important to have a scheme that has a very large possible password space as one factor for increasing the work required by the attacker to break the authentication system. Another factor is to find a scheme that has no previous or existing knowledge of the most probable user password selection, which can also resist the attack on such an authentication scheme.

Attacks and Countermeasures

To realize and understand how far an authentication scheme is secure, we have to consider all possible attack methods. We have to study whether the authentication scheme proposed is immune against such attacks or not. Moreover, if the proposed authentication scheme is not immune, we then have to find the counter measures that prevent such attacks. In this section, we try to cover most possible attacks and whether the attack is valid or not. Moreover, we try to propose countermeasures for such attacks.

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

1) Time required to login: The total time needed for a legitimate user to login may vary from 20 seconds to 2 min or more, depending on the number of interactions and actions, the size of the 3-D virtual environment, and the type of actions and interactions done by the user as a3-D password. Therefore, a brute force attack on a 3-Dpassword is very difficult and time consuming.

2) Cost of attacks: In a 3-D virtual environment that 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 the3-D password is more challenging. Moreover, the high number of possible 3-D password spaces leaves the attacker with almost no chance of breaking the 3-D password [1].

Well-Studied Attack: The attacker tries to find the highest probable distribution of 3-D passwords. However, to launch such an attack, the attacker has to acquire knowledge of the most probable 3-D password distributions. Acquiring such knowledge is very difficult because the attacker has to study all the existing authentication schemes that are used in the 3-D environment. Moreover, acquiring such knowledge may require forging all existing biometrical data and may require forging token-based data. In addition, it requires a study of the user's selection of objects, or a combination of objects, that the user will use as a 3-D 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. Every system can be protected by a 3-D password that is based on a unique 3-D virtual environment. This environment as 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 [1].

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 3-D passwords and some other graphical passwords. However, the user's 3-D password may contain biometrical data or textual passwords that cannot be seen from behind. The attacker may be required to take additional measures to break the legitimate user's 3-D password. Therefore, we assume that the 3-D password should be performed in a secure place where a shoulder surfing attack cannot be performed.

Timing Attack: In this attack, the attacker observes how long it takes the legitimate user to perform a correct sign-in using the3-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 3-D virtual environment is poorly designed [1].

IV. 3-D PASSWORD SYSTEM IMPLEMENTATION

All the possible actions that can occur in 3-D virtual environment are represented by unique codes which are saved separately in the system. Now, assume that we need to set a 3-D password for a particular user in 3-D virtual environment of Hard Rock café which consists of several authentication schemes.

We would set a 3-D password in a sequence which is represented by some corresponding code by system for some particular action as described below:

Authentication Scheme	*Unique Code*
1. Use Pass faces graphical password. (One human face selected)	DERON#
2. Select desired carom shot. (One carom shot is selected)	DEZEE#
3. Set textual password.	*********

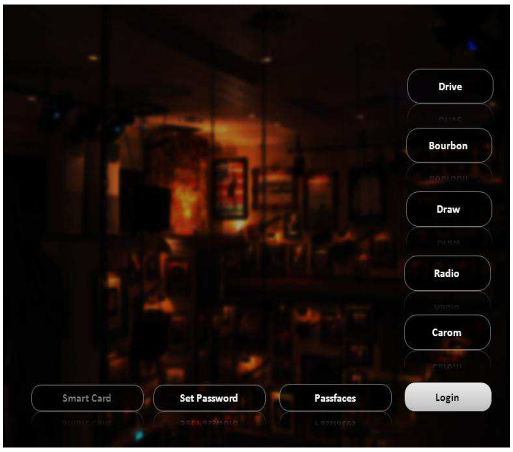
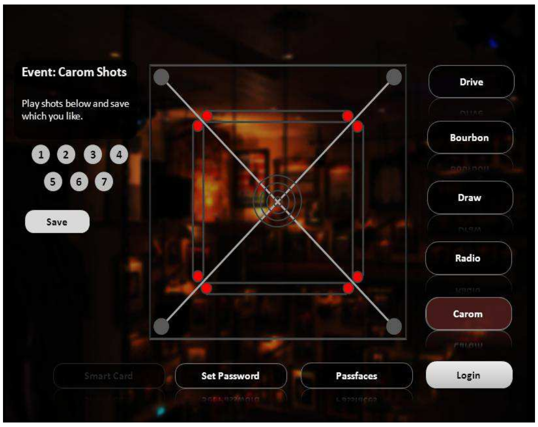


Fig. 1: Snapshot of a 3-D virtual environment of Hard Rock Cafe, where the user can use a Passfaces graphical password, set a textual password, set radio frequency, select desired carom shot as a part of the user's 3-D password.

1. Passfaces graphical password: Consider use choose passfaces as his/her first authentication scheme as a part of his/her 3-D password. The user will be asked to choose one image of human faces from a face database as their future password. In the authentication stage, the user sees a grid of nine faces or more faces, consisting of one face previously chosen by the user and eight decoy faces. The user recognizes and clicks anywhere on the known face. The user is authenticated if he/she correctly identifies the face. The technique is based on the assumption that people can recall human faces easier than other pictures [2].


Event: Carom Shots

Play shots below and save which you like.

So when user selects the face, its corresponding code, say, *DERON#* is saved as part of user's 3-D password.

2. Select desired carom shot: In this event user has to select one carom shot according to his/her liking out of fix seven carom shots. So when user save particular shot its corresponding code, say, *DEZEE#* is saved as a second action of user's 3-D Password.

Fig. 2: User saves a desired a carom shot as a second action of 3-D password in 3-D virtual environment of Hard Rock Café

3. ***Set textual password:*** User sets a textual password as a third activity of 3-D password and it is encrypted and saved.

Now, we had set a 3-D password using three authentication schemes which is represented by unique code as,

DERON#^DEZEE#^^BONBOUR11#

Now, user will always form this unique code inside the system in order to access his/her account. So if attacker recovers this code even, he will not be able to identify user's 3-D password. This unique code can again be encrypted by various methods to increase security level and then decrypted as required for login process.

Also, user can be put in time limit to complete all action and interaction in 3-D virtual environment according to the time of his/her 3-D password avoiding attacker to try some probabilities. If the user fails to give correct 3-D password three times, there can be system to block his/her account.

V. CONCLUSION AND FUTURE WORK

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. However, as mentioned before, both authentication schemes are vulnerable to certain attacks. Moreover, there are many authentication schemes that are currently under study and they may require additional time and effort to be applicable for commercial use.

The 3-D password is a multifactor authentication scheme that combines these various authentication schemes into a single 3-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 as part of their 3-D 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 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.

The 3-D password is still in its early stages. Designing various kinds of 3-D virtual environments, deciding on password spaces, and interpreting user feedback and experiences from such environments will result in enhancing and improving the user experience of the 3-D password. Moreover, gathering attackers from different backgrounds to break the system is one of the future works that will lead to system improvement and prove the complexity of breaking a 3-D password. Moreover, it will demonstrate how the attackers will acquire the knowledge of the most probable 3-D passwords to launch their attacks.

Shoulder surfing attacks are still possible and effective against 3-D passwords. Therefore, a proper solution is a field of research.

VI. REFERENCES

1. IEEE Transactions on Instrumentations and Measurement, "***Three Dimensional***

Password for more Secure Authentication" by Fawaz Alsulaiman and Abdulmotaleb El Saddik.

2. IEEE International Conference Virtual Environment, Human Computer-Interfaces and Measurement Systems, "***A Novel 3D Graphical Password Schema***" by Fawaz Alsulaiman and Abdulmotaleb El Saddik.

3. "***Graphical Passwords: A Survey***" by Xiaoyuan Suo, Ying Zhu and G. Scott. Owen, Department of Computer Science, Georgia State University.