Chapter 2

3D PASSWORD SCHEME

2.1 3D-Password Overview

The three dimensional password (3D password) is a new authentication methodology that combines recognition, recall, what you have (tokens), and what you are (biometrics) in one authentication system. The idea is simply outlined as follows. The user navigates through a three dimensional virtual environment. The combination and the sequence of the users actions and interactions towards the objects in the three dimensional virtual environment constructs the users 3D password. Therefore, the user can walk in the virtual environment and type something on a computer that exist in (x_1, y_1, z_1) position, then walk into a room that has a white board that exist in a position (x_2, y_2,z_2) and draw something on the white board. The combination and the sequence of the previous two actions towards the specific objects construct the users 3D password. Users can navigate through a three dimensional virtual environment that can contain any virtual object.

Virtual objects can be of any type. We will list some possible objects to clarify the idea.
An object can be:

- A computer that the user can type in
- A white board that a user can draw on
- An ATM machine that requires a smart card and PIN
- A light that can be switched on/off
- Any biometric device
- Any Graphical password scheme
- Any Graphical password scheme
- Any real life object
- Any upcoming authentication scheme

2.2 3D Password Selection and Inputs

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) ϵ [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, styles, a card reader, a microphone etc.

User actions, interactions and inputs towards the objects and towards the three-dimensional virtual environment are mapped into a sequence of three-dimensional coordinates and actions, interactions and inputs. For example, consider a user navigates through the three-dimensional virtual environment and types ”AB” into a computer that exists in the position of (13, 2, 30). The user then walks over and turns off the light located in (20, 6, 12), 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 (530,250). The user then presses the login button. The representation of user actions, interactions and inputs towards the objects and the three-dimensional virtual environments can be represented as the following:

- (13, 2, 30) Action = Typing, ”A”,
- (20, 6, 12) Action = Turning the Light, Off,
- (55, 3, 30) Action = drawing, point = (530,250)

Two 3D passwords are equal to each other when the sequence of actions towards every specific object is equal and the actions themselves are equal towards the objects.

A three-dimensional virtual environments can be designed to include any virtual objects. The first step in building a 3D password system is designing the three-dimensional virtual environment. The selection of what objects to use, locations, and types of responses are very critical tasks. The design affects the strength, usability and performance of the 3D password. Figure given below shows an experimental three-dimensional environment.

Figure 2.1: 3D Login screen

Chapter 3

SECURITY ANALYSIS

Security analysis is a measure for determining how hard the attack is.Trying to have a scheme that has very large possible passwords is one of the important parts in resisting the attack on such a scheme.We will analyze 3D passwords by discovering how large the 3D password space is. Then we will analyze the knowledge distribution of the 3D password.

3.1 The Size of the 3D Password Space

First of all, by computing the size of the 3D Password space we count all possible 3D Passwords that have a certain number of (actions, interaction, and inputs) towards all objects that exist in the three-dimensional virtual environment. We assume that the probability of a 3D Password of a size greater than L_{max} is zero.

We will compute $\pi(L_{max}$, G)on a three-dimensional space (G × G × G) for a 3D Password of a length (number of actions interactions and inputs) of L_{max} or less.

AC represents possible actions towards the objects. The symbol π is defined as the total number of possible 3D Passwords that have a total number of actions, interactions, and inputs equal to L_{max} or less which is equal to:

$$\prod(L_{\max}, G) = \sum_{n=1}^{n=L\max} (m + g(AC))^{n}$$

O_{max} represent the total number of existing objects in the three-dimensional virtual environment. The number O_{max} can be determined based on the design of the three-dimensional virtual environment. The variable m represents all possible actions and interactions towards all existing objects O_i.

$$m = \sum_{i=1}^{i=O^{\max}} h(Oi, Ti, x_i, y_i, z_i)$$

where xi=xj , yi=yj, and zi=zj only if i=j

Where any new action, interaction, or inputs towards the objects or the three-dimensional virtual environment of length n can be accumulated.

g(AC) is the total number of actions, inputs towards the three-dimensional virtual environment excluding the actions towards the objects which are already counted by m . An example of g(AC) can be a user voice that can be considered as a part of user's 3D Password.

The function h (O_i, T_i, x, y, z) determines the number of possible actions and interactions towards the object Oi based on the object type (T_i). Possible object types are textual password objects, graphical password objects, DAS graphical passwords objects, fingerprint objects, etc. h (O_i, T_i, x, y, z)= f (O_i, T_i, x, y, z).

Each object of a certain type (T) has its own formula f that determines the possible actions and interactions the object can accept. If we assume that an object "Keyboard" in location x=S_0, y= S_1, z= S_2 of type = textual password, then the possible actions will be the size of possible letters and numbers that can be typed using the "Keyboard", which is almost 93 possibilities. T can also be a type of object that accepts DAS [9] (so the user can draw something). Depending on the argument of this object type, the actions and interactions towards the objects can be determined. The more possibilities the function f has, the larger the 3D Password space can be.

We noticed that by increasing the number of objects in the three-dimensional virtual environment, the 3D password space increases exponentially. The design of the three-dimensional virtual environments is the key for the 3D password space. Figure (3.1) illustrate the key size space of a possible 3D password as in comparison with PassFaces, DAS of grid 5×5, DAS of grid 10×10 and textual password. We noticed the huge difference between the 3D password space and other authentication schemes.

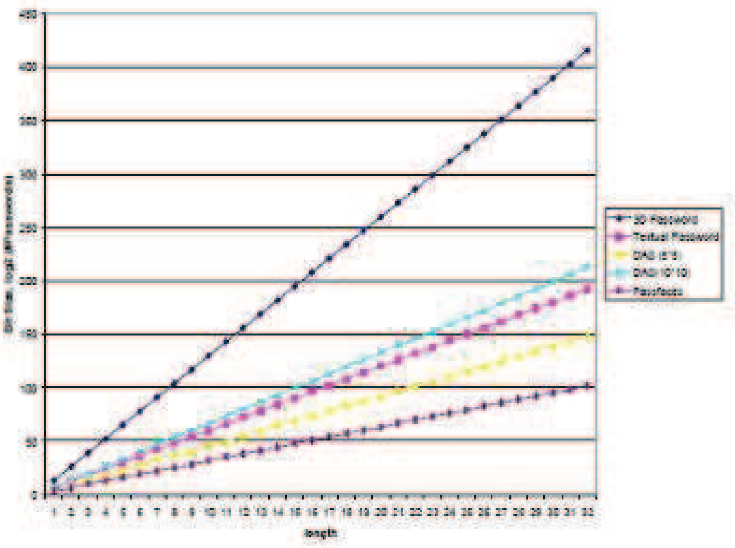

Figure 3.1: A comparison between the full password space of 3D Password, Textual Password, PassFaces of size (3×3 possible faces each turn), DAS of grid size (5× 5), and DAS of grid size (10 × 10). The length represents the number of characters for the textual passwords, the number of actions, interactions and inputs towards the objects for the 3D password, the number of selections for Passfaces, and the number of points that represent the strokes for DAS. The length is up to 32 (characters/actions, interactions, and inputs/selections).

3.2 3D Password Distribution Knowledge

Having knowledge about the most probable textual passwords is the key behind dictionary attacks. Any authentication scheme is affected by the knowledge distribution of the users secrets .

Knowledge about the users selection of three-dimensional passwords is not available, up to now, to the attacker. Moreover, having different kinds of authentication schemes in one virtual environment causes the task to be more difficult for the attacker. However, in order to acquire such knowledge, the attacker must have knowledge about every single authentication scheme and what are the most probable passwords using this specific authentication scheme. This knowledge, for example, should cover the users most probable selection of textual passwords, different kinds of graphical passwords, and knowledge about the users biometrical data. Moreover, knowledge about the design of a three-dimensional virtual environment is required in order for the attacker to launch a customized attack.

Chapter 4

EXPERIMENTAL RESULTS

As a proof of concept we have built an experimental three-dimensional virtual environment that consist of many objects. Objects initially have two kinds of responses to reactions, they are, objects that accept textual passwords and objects that accept graphical passwords. Almost 30 users have tested the experimental environment.

4.1 Experimental Virtual Three-Dimensional Environme

We have built a small experimental three-dimensional virtual environmentas as seen in figure(3.1). The three-dimensional virtual environment is simply an art gallery that the user can walk into. It consists of the following virtual objects:

1. 6 computers that accept textual passwords
2. 36 pictures that the users can click on, anywhere in the picture, as a part of their 3D password.

Chapter 5

CONCLUSION AND FUTURE WORK

Textual passwords and token-based passwords are the most common used 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. Users do not have to carry cards if they do not want to. Users have the choice to model their 3D password according to their needs and their preferences.

A 3D passwords 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 3D password is in its infancy. 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, 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 users 3D password might show the practical strength of a 3D password.Finding a solution for shoulder surfing attacks on 3D passwords and other authentication schemes is also a field of study.

References

[1] Alsulaiman, F.A. Saddik, A.E, A Novel 3D Graphical Password Schema, ieee july 2006,

[2] N. D. Georganas, M. Goldberg and S. Cohn-Sfetcu, 3D Password, 2007,