uOttawa

L'Université canadienne
Canada's university

FACULTÉ DES ÉTUDES SUPÉRIEURES ET POSTOCTORALES

uOttawa

L'Université canadienne
Canada's university

FACULTY OF GRADUATE AND POSDOCTORAL STUDIES

Fawaz Abdulaziz A. Alsulaiman
AUTEUR DE LA THÈSE / AUTHOR OF THESIS

M.C.S. (Master of Computer Science)
GRADE / DEGREE

School of Information Technology and Engineering
FACULTÉ, ÉCOLE, DÉPARTEMENT / FACULTY, SCHOOL, DEPARTMENT

Design and Development of a Three Dimensional Password Scheme

TITRE DE LA THÈSE / TITLE OF THESIS

Abdulmotaleb El Saddik
DIRECTEUR (DIRECTRICE) DE LA THÈSE / THESIS SUPERVISOR

CO-DIRECTEUR (CO-DIRECTRICE) DE LA THÈSE / THESIS CO-SUPERVISOR

EXAMINATEURS (EXAMINATRICES) DE LA THÈSE / THESIS EXAMINERS

Dorina Petriu

Jiying Zhao

Gary W. Slater
Le Doyen de la Faculté des études supérieures et postdoctorales / Dean of the Faculty of Graduate and Postdoctoral Studies

DESIGN AND DEVELOPMENT OF A THREE DIMENSIONAL PASSWORD SCHEME

By

Fawaz Abdulaziz A Alsulaiman

A thesis submitted to the University of Ottawa
in partial fulfillment of the requirements for
the degree of

Master of Computer Science

Ottawa-Carlton Institute of Computer Science

School of Information Technology and
Engineering

University of Ottawa
Ottawa, Canada

April, 2006

Your file Votre référence
ISBN: 978-0-494-18392-2
Our file Notre référence
ISBN: 978-0-494-18392-2

ABSTRACT

Current authentication systems suffer from many weaknesses. Textual passwords are common. However, users do not follow the requirements of a textual password system. Users tend to choose meaningful words from dictionaries, which make textual passwords easy to break and vulnerable to dictionary attacks or brute-force attacks. Many available graphical password schemes have a password space less or equal to the textual password space. Smart cards or tokens can be stolen. Although many biometrics authentications have been proposed, users tend to resist using biometric passwords because of their seeming intrusiveness and their affect on personal privacy. Moreover, biometric passwords cannot be revoked.

In this thesis, we propose and evaluate our contribution which is a new scheme of authentication. This new scheme is based on a three-dimensional virtual environment. Users navigate through the virtual environment and interact with items inside the three-dimensional virtual environment. The combination of all interactions, actions and inputs towards the items and towards the three-dimensional virtual environment constructs the user's 3D password. The 3D password combines most existing authentication schemes such as textual passwords, graphical passwords, token-based, and biometrics into one three-dimensional virtual environment. The 3D password's main application is the protection of critical resources and systems.

TABLE OF CONTENTS

LIST OF FIGURES

ACKNOWLEDGMENTS

I would like express my appreciation to my parents, family, wife, and daughter for their unlimited support throughout my life and for offering an appropriate environment allowing for my increased productivity and the quality of this research.

I would like to especially thank my supervisor Prof. Abdulmotaleb El Saddik for all his support, enthusiasm, and guidance.

I am thankful to King Saud University, Department of Computer Science for the scholarship that allowed me to pursue graduate studies in computer science at the University of Ottawa.

I would like to thank all my friends and family who waited patiently for me to complete my research.

I would like to thank those who participated and volunteered in testing the experimental three-dimensional password software. Their comments, suggestions, and feedback contributed much to the experiment and to my overall research.

To my parents, beloved wife, and my lovely daughter, Jude

GLOSSARY

3D Password: Three Dimensional Password.

3D Virtual Environment: The three dimensional Virtual Environment is the virtual environment that 3D Password system uses for performing the users 3D Password.

ATM: Auto Teller Machine.

Authentication is the process of validating who are you to whom you claimed to be.

AWASE-E: Image-based authentication system for mobile phones that use user's favorite images.

Biometrics is the science of using biological properties to identify individuals is the science of using biological properties to identify individuals.

Brute-Force Attack: is an attack where the attacker tries all possible passwords.

DAS: Draw A Secret. DAS is a knowledge-based graphical password where user draws something as a secret.

Déjà Vu: A graphical password scheme that requires the selection of random art portfolios as user's password.

Information Content: the entropy of the probability distribution over that space given by the relative frequencies of the passwords that users actually choose. It is a measure that determines how difficult the attack is.

MCR LAB: Multimedia Communications Research Laboratory, University of Ottawa, Ottawa, Ontario, Canada.

PassFaces: a graphical password scheme that require the selection of faces as a secret.

PDA's: Personal Digital Assistance such as Palm Pilot ™.

PIN: Personal Identification Number.

Shoulder Surfing Attack: Shoulder-surfing attack occurs when a person observes (via camera or recording) and notes the legitimate user's password or watches over the legitimate user's shoulder for the password

Well-Educated Attack: is an attack where the attacker tries to find the most probable passwords used and applies this knowledge for attacking user's passwords.

Chapter 1

INTRODUCTION

1.1 Objective and Motivation

Due to recent advancements in computer speeds and to the worldwide interconnected nature of computers, the need for an authentication scheme that cannot be cracked easily has increased dramatically. Since forcing users to use a specific authentication scheme might be resisted, user freedom in selection from a variety of password authentication scheme is motivating and commercially viable.

Textual passwords are the most common authentication techniques used in the computer world. Textual passwords have two conflicting requirements: passwords should be easy to remember and hard to guess. Users tend to ignore the second requirement, which leads to the creation of easy-to-break passwords. Most commonly, users face constant challenges in selecting and remembering textual passwords. For security reasons, an effective password authentication scheme should not be written down or shared with friends. Consequently, users usually select passwords that have linguistic meaning. Therefore, using dictionaries is the easiest way to crack a system protected by textual passwords.

The strength of graphical passwords comes from the fact that users can recall and recognize pictures more than words. Most graphical passwords are vulnerable to shoulder-surfing attacks, where an attacker observes or records the legitimate user's graphical password by camera. Moreover, many graphical passwords have a probable password space that is less or almost equal to that of textual passwords. Currently, many graphical password schemes are under study. However, it might be some time before they can be successfully applied in the real world.

Token-based systems such as ATMs are widely applied in the banking industry and in secured laboratory entrances. However, tokens are vulnerable to loss or to theft. Moreover, the user must remember to carry the token whenever access to a system or location is required.

Many biometric schemes have been released to consumers in recent years. Fingerprints, palm prints, hand geometry, face recognition, voice recognition, iris recognition, and retina recognition are all different biometrics schemes. Each biometric recognition scheme is different considering consistency, uniqueness, and acceptability. Users tend to resist some biometrics recognition schemes because of concerns for personal privacy. Moreover, iris and retina password recognition schemes require the user's to willingly expose their eyes to a laser beam. Also, in the case where a user's biometrical data has been forged, biometrics cannot be revoked.

The design of a password authentication scheme that can be revoked, that cannot be stolen, and that is easy to remember and to initiate is the primary objective of this research.

1.2 Thesis Contributions

The proposed three-Dimensional Password, or "3D Password" allow users to navigate through a three-dimensional virtual environment and interacts with virtual objects as a means of authentication. The user's actions, interactions, and inputs regarding the virtual objects and the three-dimensional environment are communicated and recorded as the user's 3D Password. The 3D authentication scheme is capable of combining some or all of the existing authentication schemes such as recognition-based systems, recall-based systems, tokens-based systems, and biometrics-recognition systems in one authentication scheme. The user has the freedom to select the appropriate authentication method. It is left to the users to choose a 3D Password that best suits their requirements.

The proposed password scheme presents a dramatic increase in the probable password space that surpasses existing password authentication schemes. The probable password space reflects the effort required by the attacker to crack or break the system.

A proof-of-concept 3D Password authentication system has been developed and tested. A set of user-specific 3D Passwords has been acquired and analyzed.

1.4. Thesis Organization

In this chapter, the objective and motivation for the current research is presented and the various authentication schemes are introduced. Then the thesis contribution, thesis organization, and publication resulting from this thesis are listed.

Chapter 2 presents the existing authentication schemes in depth. It starts with a discussion of the textual password. This section also examines biometric recognitions and token-based authentication schemes. Finally, the section explores various graphical passwords authentication schemes in detail.

Chapter 3 provides an overview of our contribution. In this section, we present 3D (three-dimensional) Passwords as a new authentication scheme. This chapter examines the system architecture and it presents guidelines on designing a three-dimensional, virtual environment for 3D Password.

Chapter 4 provides information regarding implementation issues. A proof-of-concept implementation is proposed. Furthermore, this section discusses 3D Password user interfaces.

Chapter 5 analyzes the security of the 3D Password. It studies three-dimensional passwords probable password spaces. Additionally, this chapter provides comparisons between three-dimensional passwords and some other existing authentication schemes. Finally, the section presents experiment results, and evaluation of the proposed scheme.

Chapter 6 summarizes the thesis. In concluding, the section presents recommendation for future work.

1.5 Publications Resulting from this Research

Resulting from the research undertaken in this thesis, two patent applications have been submitted for approval and one conference paper has been accepted and another conference paper has been submitted.

1. A patent application on Three Dimensional Password submitted to TTBE, University of Ottawa. October 2005.

2. A patent application on Collaborative Three Dimensional Password submitted to TTBE, University of Ottawa. January 2006.

3. Fawaz A Alsulaiman, Abdulmotaleb El Saddik. A Novel 3D Graphical Password Schema. IEEE International Conference on Virtual Environments, Human-Computer Interfaces, and measurement systems (VECIMS 2006). La coruna, Spain. 10-12 July 2006. (Accepted)

4. Fawaz A Alsulaiman, Abdulmotable El Saddik, Three dimensional Password for more secure authentication, The 2006 ACM Multimedia Conference, Santa Barbara, CA, USA. October 2006.

Chapter 2

RELATED WORK

In this chapter, various authentication schemes are introduced and discussed in detail. Shortcomings of textual passwords will be presented. Token-based system and biometric password systems will be explored. In addition, various knowledge-based and recognition-based graphical passwords will be presented and discussed.

2.1 Textual Password

Textual passwords are the most common authentication techniques used in the computer world. Textual passwords have two conflicting requirements: passwords should be easy to remember and difficult to crack.

Klein [KLEIN 1990] acquired a database of nearly 15,000 user accounts that had alphanumeric passwords, and stated that 25% of the passwords were cracked using a small, yet well-formed dictionary of (3×10^6) words. Furthermore, 21% of the passwords were uncovered in the first week and 368 passwords were uncovered within the first 15 minutes. Klein [KLEIN 1990] stated that by looking at these results in a system with about 50 accounts, the first account can be cracked in 2 minutes and 5 to 15 accounts in the first day.

Even though the full textual password space for 8-character passwords consisting of letters and numbers is almost (2×10^{14}) possible passwords, by using a small subset of the full space, 25% of the passwords were uncovered. Why? The user is often not careful in selecting their textual passwords and most users do not select random passwords.

According to the Vice-President of IT at Telesis Community Credit Union [GILHOOLY 2005], their security team ran a network password cracker as part of an enterprise security audit. They found that 80% of employee passwords were cracked within 30 seconds. Following this result, the security personnel advised the employees to create stronger passwords. After a few days, the team ran the network cracker again and found that 70% of employee passwords were cracked by the software.

An early study by Morris and Thompson [MORRIS and THOMPSON 1979] of 3289 user passwords showed that almost 30% of user passwords are four letters or less. Moreover, 86% of user passwords appear in various dictionaries and name lists. They tried to improve textual password authentication systems by offering some suggestions such as using slower encryption algorithms, forcing users to pick a random password, salting passwords, etc.

There are many available programs that crack textual passwords using dictionaries or brute-force attacks. For example, consider John the Ripper [OPENWALL PROJECT 2006], Alec Muffet (Crack version 4.1) [Muffett 1992], and Feldmeier and Karn [FELDMEIER and KARN 89].

Another study conducted by DHAMIJA AND PERRIG [DHAMIJA AND PERRIG 2000] examined over 30 users focusing on user behavior regarding textual passwords. The study revealed the following results:

- Users have only 1-7 unique passwords.
- The vast majority of participants write their passwords down.
- Most users do not change their passwords unless required by the system.
- The level of security education or training does not have any impact on the user's textual password selection behavior.
- Users who speak foreign languages use common names or words from their mother language as passwords.
- Almost all users share their bank PIN with family members and/or friends.

In his study, Klein [KLEIN 1990] proposes many solutions for selecting a safe password. Klein [KLEIN 1990] offers the following four solutions:

1. Run a password checker periodically to detect easy-to-guess passwords. Of course, this solution is considered to be both time and resource consuming.

2. Require users to change passwords frequently. However, users tend to choose passwords that relate to each other such as "FawazJan", "FawazFeb", "FawazMar"... etc.

3. Assign random passwords. However, since passwords can be difficult to remember, the user may write the password down, where it can be easily collected by someone else.

4. Use smart cards. However, the draw back to this solution is the cost of smart cards. In addition, it must be carried whenever the user wants to access the system.

To address the fact that users tend to choose simple passwords and that users usually use few unique passwords, Halderman et al. [Halderman et al. 2005] proposes a technique that uses a cryptographic hash function to compute passwords for many accounts by requiring only a single master password. For every site, a unique password is generated. The bottleneck of this approach is the master password. Once the master password is broken, all passwords are revealed.

Many authentication schemes have been proposed as alternatives for textual passwords. The alternative authentication systems include graphical passwords, biometric systems, and token based authentication systems. Figure 2.1 shows different authentication schemes classified by the type. We will begin with a brief description of token-based systems and biometric recognition systems. Then we will study graphical password authentication systems in depth.

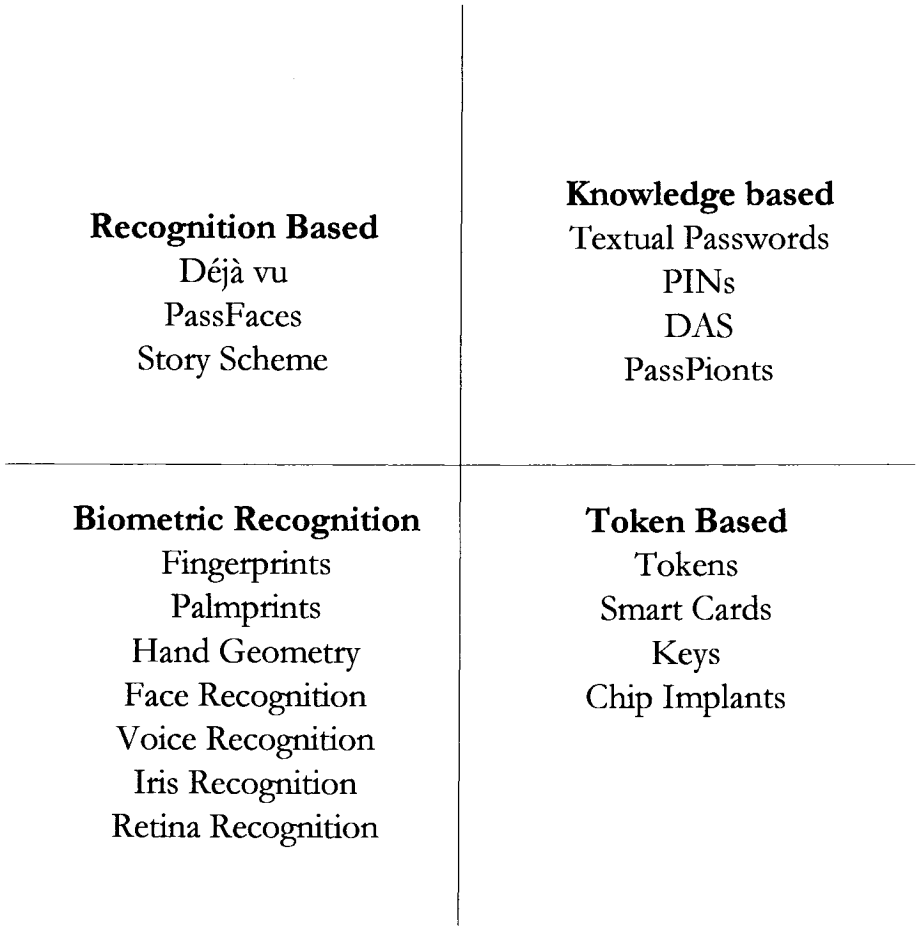

Figure 2.1: classification of existing authentication schemes based on the perception of Kaufman et al.[KAUFMAN et al. 2002] and Dhamija and Perrig [DHAMIJA AND PERRIG 2000]

2.2 Token-based systems

Token based systems are widely applied in banking systems and in laboratory entrances as a mean of password authentication.. Users are required to carry the token whenever access is required. Tokens such as Auto Teller Machine (ATM) cards are vulnerable to loss and/or theft. Personal Identification Numbers (PINs) are usually required to accomplish the authentication process. Therefore, token-based systems usually depend on knowledge-based authentication schemes to prevent impersonation.

2.3 Biometrics

Biometrics is the science of using biological properties to identify individuals [RSA LABORATORIES 2005]. Many biometric recognition schemes have been proposed. Every biometric recognition scheme is different considering consistency, uniqueness, and acceptability. Users tend to resist some biometrics recognition because of privacy-related issues.

Some human properties are vulnerable to change for different reasons such as aging, scaring, face makeup, new hairstyle, and illness (change of voice). People resist biometrics for different reasons. Research suggests that some users feel that keeping a copy of a user's fingerprints is not acceptable and is considered by many to be a threat to the user's privacy. In addition, some users resist the idea of a laser beam scanning their eyes as in the case of retina and iris recognition authentication systems, even if it is merely a camera.

Some biometrical data such as fingerprints and voice can be captured and forged easily. Figure 2.2 (Left) shows molds for artificial fingerprints. Figure 2.2 (right) shows fingerprints captured from a bullet. Moreover, it is easily to find the instruction on how to forge fingerprints [CHOAS COMPUTER CLUB 2004]. One critical disadvantage of biometrics is that the user's biometrical data cannot be revoked, which leads to a dilemma if the user's data has been forged. Therefore, biometrics is still not the perfect solution for authentication.

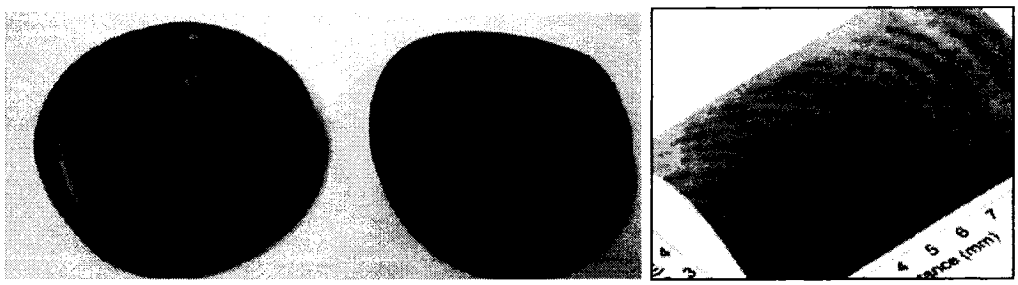

Figure 2.2: (Left) Molds for Artificial Fingerprint [ORTEGA-GARCIA 2002]. (Right) Fingerprint captured from a bullet. [BBC 2006]

2.3 Graphical Passwords

Graphical passwords started with the innovative work of Greg E. Blonder [BLONDER 1996]. For Blonder, graphical passwords have a predetermined image that the user selects or touches by tapping regions of the image and the sequence and the location of the touches constructs the user graphical password. Figure 2.3 below illustrates G. Blonder's [BLONDER 1996] idea. Graphical passwords are either recognition-based authentication schemes or knowledge-based authentication schemes.

Figure 2.3: An example of G. Blonder's graphical password system [BLONDER 1996]. The red circles represent tap regions that can be part of the user's authentication system. The sequence and the tap regions selected are interpreted as the graphical password.

PassPoints [WIEDENBECK et al. 2005a]; [WIEDENBECK et al. 2005b]; [WIEDENBECK et al. 2005c] graphical password system is based on Blonder's graphical password [BLONDER 1996] idea. However, it overcomes the limitations of Blonder's graphical password limitations of predefined region. PassPoints allows the user the option to click anywhere on the picture as PassPoints secret. The collection of the user's clicks is the user's PassPoints secret. Moreover, PassPoints can be applied on any picture chosen by the user. PassPoints does not capture the

exact pixel the user selects. However, it considers a range of pixels around the secret pixel as the user's PassPoints secret. This range of pixels is required because it is almost impossible for users to select the exact pixel originally chosen. Different tolerances such as 10× 10 pixels, 14 × 14 pixels, and 20 × 20 pixels were examined in the aforementioned studies. Figure 2.4 below illustrates the PassPoint authentication system.

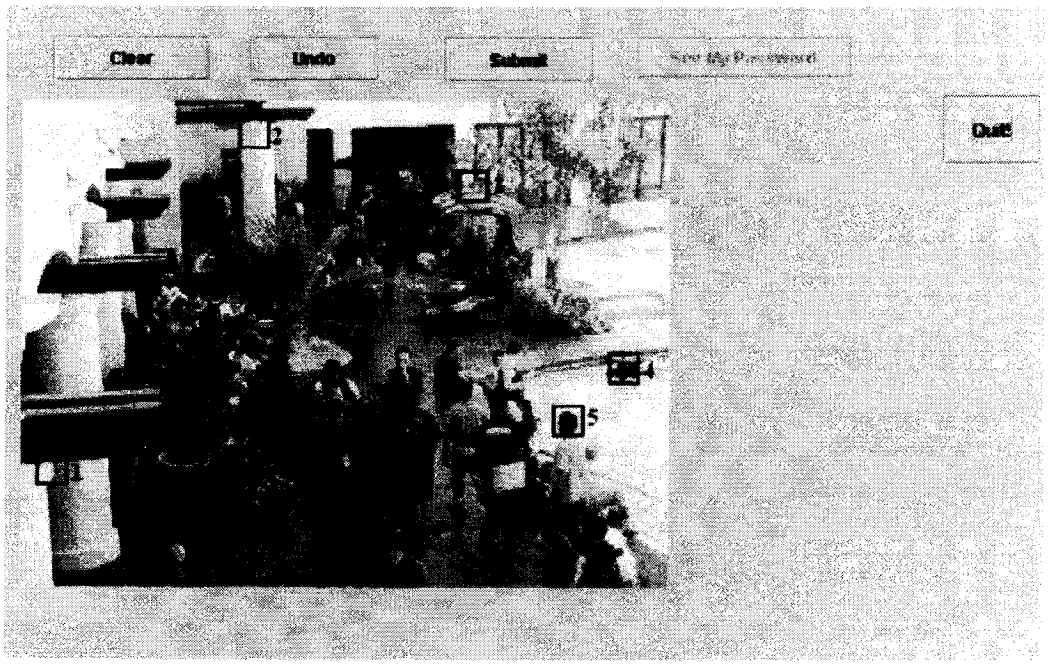

Figure 2.4 PassPoints authentication system. Numbers one to five illustrate user selection as a PassPoints secret. The square size illustrates the tolerance range from the original pixel [WIEDENBECK et al. 2005c].

PassFaces [REAL USER CORPORATION 2005] works simply by having the user select a subgroup of k faces from a group of n faces. For authentication, the system shows m faces and one of the faces belong to the subgroup k. The user has to do the selection many times in order to complete the authentication process. Figure 2.5 below show an example of PassFaces [REAL USER CORPORATION 2005].

According to Davis et al. [DAVIS et al. 2004] with PassFaces [REAL USER CORPORATION 2005], users tend to choose faces that reflect their own taste on face attractiveness, race, and gender. Moreover, according to Davis et al. [DAVIS et al. 2004] 10% of male passwords have been cracked in just two attempts. This result is due to the fact that

most male selections of PassFaces are females and they usually choose the best looking female among other faces.

Figure 2.5: PassFaces, users have to select a face as part of user secret.

Another authentication scheme is the story scheme [DAVIS et al. 2004] that requires the selection of objects (people, cars, foods, airplanes, landmarks, etc.) to form a storyline by selecting some pictures from a group of pictures. Story schemes are somehow similar to the PassFaces concept. However, instead of using faces as the user's secret, the user must select objects that form a story line. Figure 5.6 illustrates an example of the story authentication scheme. This scheme also may be affected by user taste, interests, and habits. For example, a sport car fan might select cars and any picture relevant to sport cars as a Story scheme secret. This may affect the security of the system to the degree that the system is rendered insecure as mentioned in Davis et al. [DAVIS et al. 2004].

Figure 2.6: A story authentication scheme where users have to select pictures that form a storyline as a secret [DAVIS et al. 2004].

Takada and Koike [TAKADA T. AND KOIKE H. 2003] propose A WASE-E. A WASE-E is a graphical password scheme applied over mobile phones. The user has k picture passwords. In order to login, the user has to select the correct image. If all images do not belongs to k pass images, then the user click on no pass-image. In order to gain access, the legitimate user has to solve the challenge four times. The password probable space is similar to numerical PINs. However, it relies on the fact that users usually do not select random numbers. Therefore, selection of pictures might be considered as random. However, according to Davis et al. [DAVIS et al. 2004] selection of pictures usually reflects the user's tastes and interests. Therefore, a broader security analysis study should be performed on comparing numerical PINs to A WASE-E system.

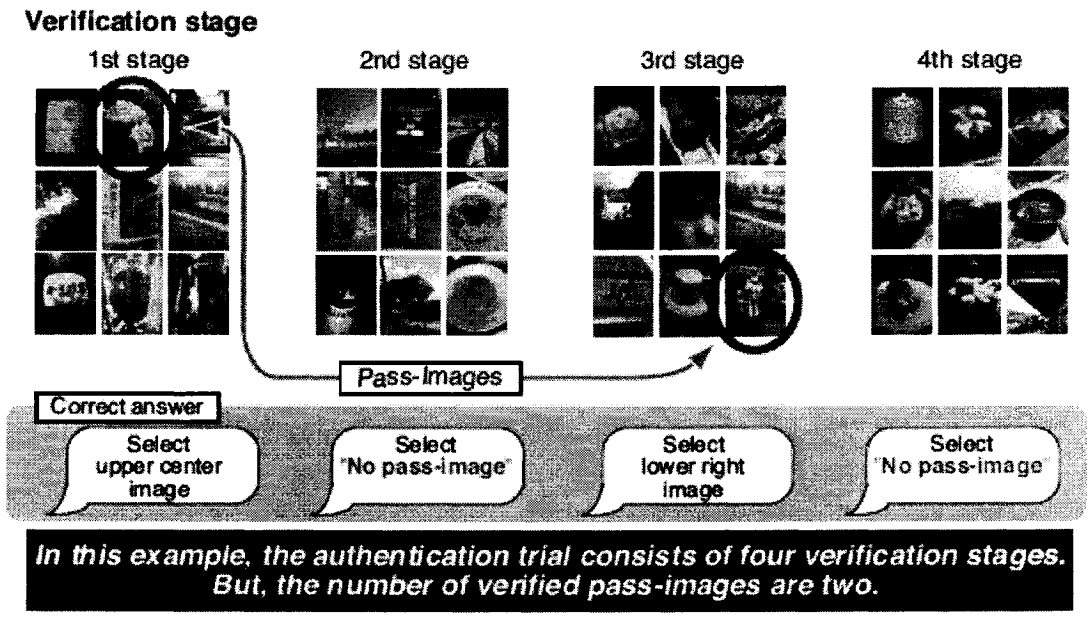

Figure 2.6: A WASE-E authentication system. The user either selects the correct image or no-pass image [TAKADA T. AND KOIKE H. 2003].

Rachna Dhamija et al. [DHAMIJA AND PERRIG 2000] proposed Déjà Vu, which is a system that authenticates users by choosing portfolios among decoy portfolios. These portfolios are randomized art portfolios. Each image is derived from an 8-byte seed. Therefore, an authentication server does not need to store the entire image. However, Déjà Vu is not protected from shoulder-surfing attacks. Figure 2.7 below shows a random art generated by Déjà vu.

One important feature of randomized art compared to photos is that photos are often selected according to user taste and background [DAVIS et al. 2004]. However, it is more difficult to know the user's taste for random arts.

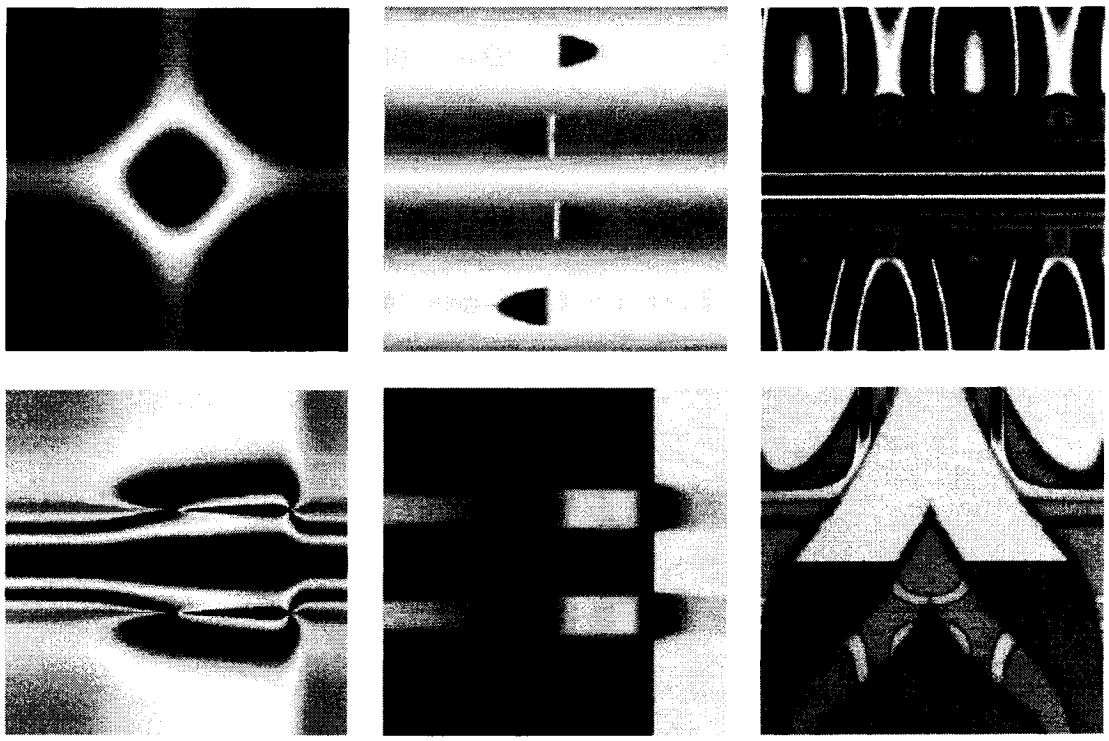

Figure 2.7: Examples of random arts generated by Déjà Vu System [DHAMIJA AND PERRIG 2000].

Ian Jermyn et al. [JERMYN et al. 1999] proposes a textual password scheme with graphical assistance. It decouples the temporal order of input and the position of the characters. Instead of entering the textual passwords from left to right, the user enters the same word in different ways. For example figure 2.8 shows four ways of writing the word "tomato". The underlying representation of such scheme can be represented as $\pi'(i) = (c, j)$ which means the i^{th} entry is the character c in position j. Therefore, the underlying representation of figure 2.8 (a) is $\pi'(0) = ('t',0)$, $\pi'(1) = ('o',1)$, $\pi'(2) = ('m',2)$, $\pi'(3) = ('a',3)$, $\pi'(4) = ('t',4)$, $\pi'(5) = ('o',5)$, while the underlying representation of figure 2.8 (d) is $\pi'(0) = ('t',7)$, $\pi'(1) = ('o',4)$, $\pi'(2) = ('m',0)$, $\pi'(3) = ('a',3)$, $\pi'(i) = (c, j)$, $\pi'(4) = ('t',1)$, $\pi'(5) = ('o',2)$. The two representations are different. Therefore, the same word can be written in different ways, which increases the probable password space by $m!/(m-k)!$ where m is the number of possible positions that enable k-character passwords to be written. The

main application of this authentication scheme is in "personal digital assistants" or PDAs such as Palm Pilot ™.

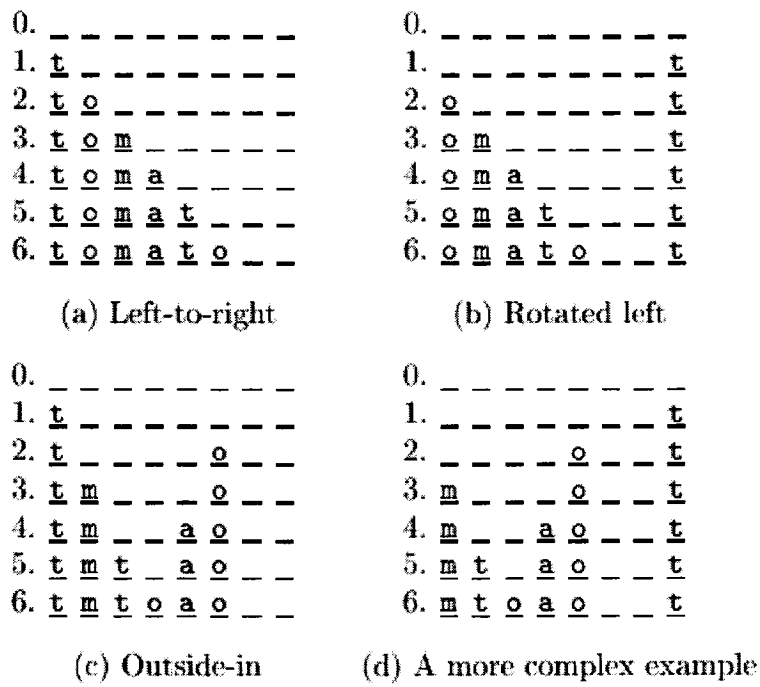

Figure 2.8: Textual passwords with graphical assistance. It decouples the position of inputs from the temporal order in which they occur. A word such as tomato can be written in many ways. (a) Shows the word tomato written from left-to-right. (b) Shows the word tomato after a shift left by one. (c) outside-in strategy. (d) Shows a more complex example [JERMYN et al. 1999].

Ian Jermyn et al. [JERMYN et al. 1999] proposes another graphical password scheme called Draw A Secret (DAS). DAS is simply drawing something on a grid as a secret. The secret draw is mapped into a sequence of strokes with two dimensional coordinates (x, y) in a grid. Figure 2.9 below is an example of DAS of (5 × 5) grid. Ian Jermyn et al. [JERMYN et al. 1999] discusses one implementation issue of this authentication scheme. The issue when the user's drawing falls between two squares or more. They suggested two solutions to such a problem. (a) Show the underlying representation of the user's drawing as (x, y) coordinates. (b) Forbid drawings that fall between two or more squares. DAS' main application is protecting handhelds devices and PDA's.

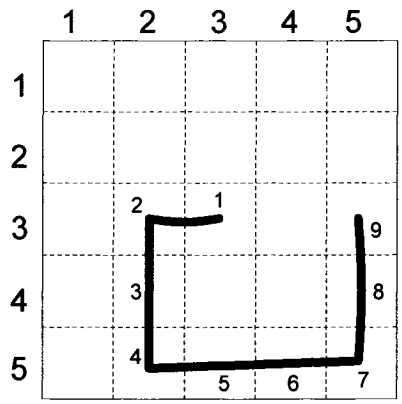

Figure 2.9: Inputs of DAS on a grid sized 5 × 5. The drawing is converted into (x, y) coordinates. By considering "pen up" = (6,6) the result of mapping process is (3,3), (3,2) , (4, 2) , (5, 2) , (5, 3) , (5, 4) , (5,5) , (4,5) , (3,5) , (6,6).

The size and the complexity of a DAS grid affect the probable password space. By increasing the grid size, the full password space increases. Moreover, there are limitations in grid complexity due to human nature. It becomes very difficult to recall where the drawing started and ended and where the middle points were when large grid sizes are used.

In order to increase DAS grid size TAO H. [TAO H. 2005a] [TAO H. 2005b] proposes adding four dots in the middle of the DAS grid that act as indicators for the user's drawings. Figure 2.10 illustrates the four dots and the dark horizontal and vertical lines that act as reference points and reference lines for DAS drawings. It is significant to note that the user's DAS secrets may be affected by the four reference points.

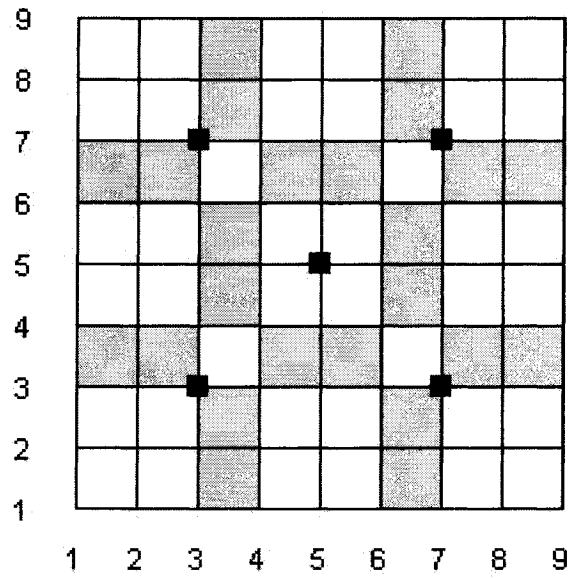

Figure 2.10: Passgo scheme where four points act as reference points for DAS secrets [TAO H. 2005b].

All previously mentioned graphical password authentication schemes suffer from shoulder-surfing attack. Shoulder-surfing attack occurs when a person observes (via camera or recording) and notes the legitimate user's password or watches over the legitimate user's shoulder for the password. Many shoulder-surfing resistant graphical passwords schemes have been proposed.

Sobardo S. and Birget J.C [SOBRADO AND BIRGET 2005a] [SOBRADO AND BIRGET 2005b] propose a shoulder-surfing resistant graphical password called the convex-hull scheme. The system displays N icons. The user has to select k icons as "the user's pass-icons". When the user tries to login, the system challenges the user by randomly choosing j where $3 \leq j \leq k$. The system shows n icons where $n \leq N$ and among these icons, it randomly distributes j icons. In order to login, the user has to observe where the j icons are and has to observe the convex-hull formed by these pass-icons. Then the user clicks anywhere inside the convex hull. The system challenges the user several times before granting access. Figure 2.11 illustrates the convex-hull scheme. Two critical drawbacks to this approach include the length of time required to login and the small probable password space resulting from this authentication scheme.

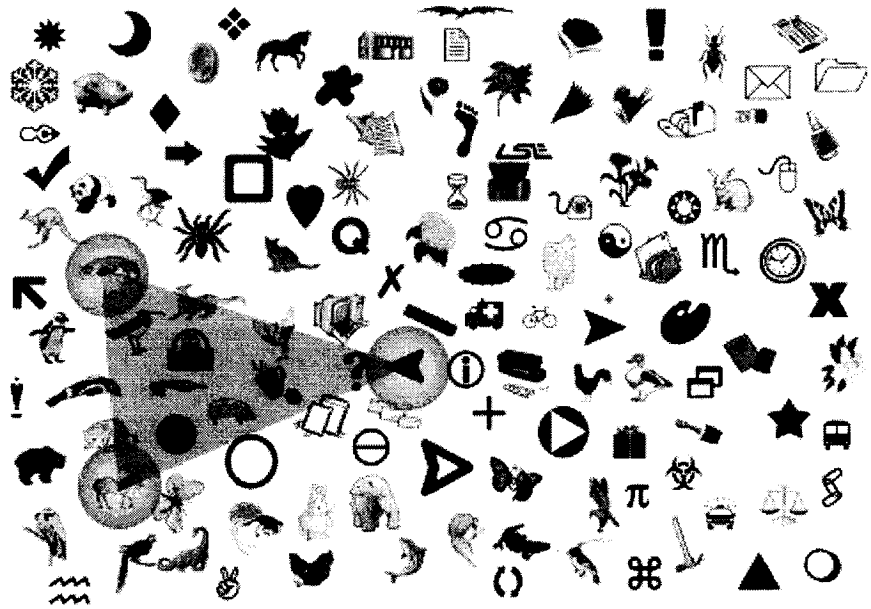

Figure 2.11: Convex-hull scheme. Shadowed area illustrates the possible locations for the system challenge [SOBRADO AND BIRGET 2005c].

Hong et al. [HONG et al. 2004] proposed a challenge-response graphical password scheme that is resistant to spyware and resistant to shoulder-surfing attacks. The proposed graphical password scheme works in the following manner. The screen is divided into n grid. Icons are distributed among these n grids. The user must select k icons as pass-icons. Every pass-icon selected by the user has m variations. The legitimate user has to assign a string to each m variation of selected k icons. Therefore, the user will have k × m different strings assigned to every m variation of k icons. In order to login, the user must observe all icons shown in all grids. Then, the user must write down the string associated with all icons shown that belong to k (pass-icon set). Every time the legitimate user tries to login, a random subset of k is shown. Therefore, each time the user tries to login, the system requires different pass-strings. This is the result of showing different subset of k every time the user tries to login. Figure 2.12 shows k=4 pass-icons that has m = 4 variations and their assigned secret strings. Figure 2.13 shows the login screen of Hong et al.'s [HONG et al. 2004] graphical password scheme. In this graphical scheme, the user is required to recall k × m pass-strings associated with every variation of k pass icons. Therefore, it can be considered to be a knowledge-based authentication scheme.

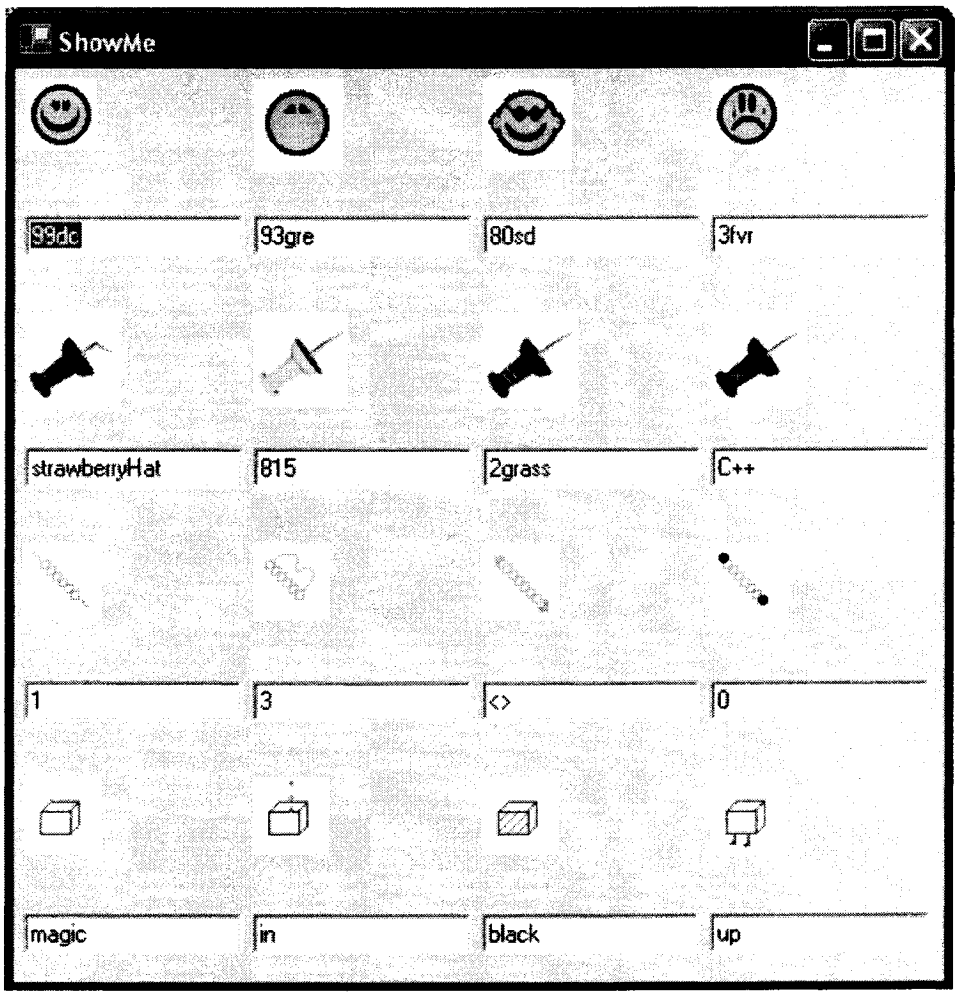

Figure 2.12: Four variations of four secret icons and their assigned secret stings [HONG et al. 2004].

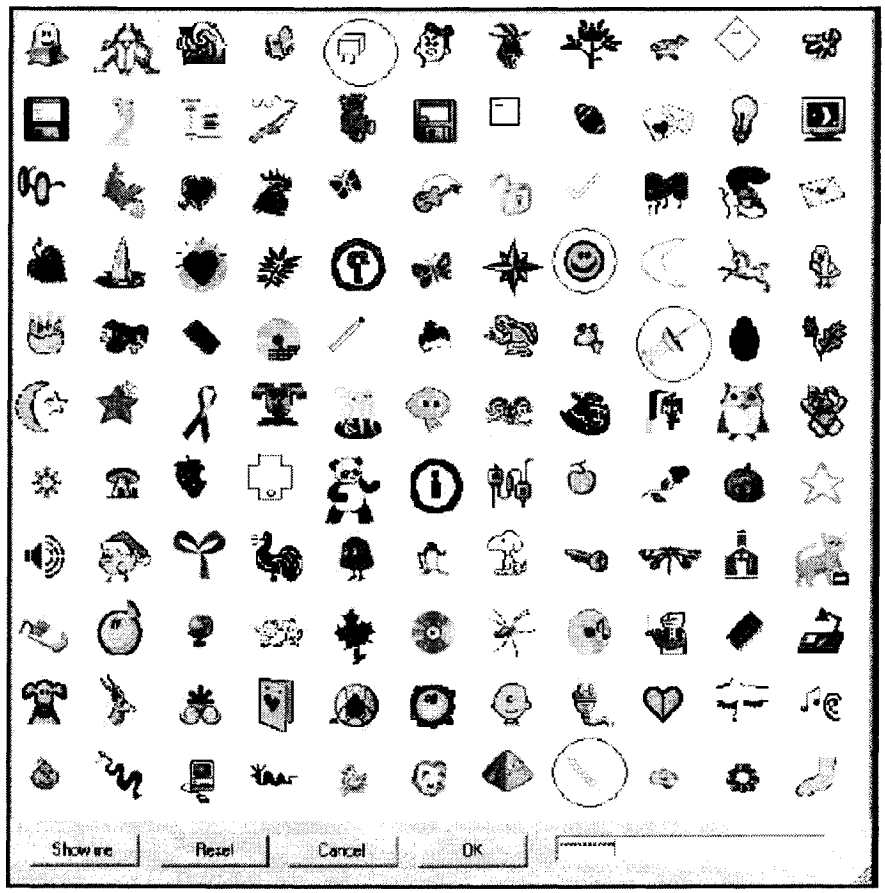

Figure 2.13: Login screen where the subset of pass-icons is circled. The pass-string is 99dc8151up [HONG et al. 2004].

Volker R. et al. [VOLKER et al. 2004] proposes an alternative PIN entry method called cognitive trapdoor games. This method is resistant to shoulder-surfing attacks. It challenges the user by asking him some questions that determines whether the user knows the right answer or not. It divides the numbers into white numbers and black numbers. The user must determine whether the secret number is among the white numbers or among the black numbers. The user must select the white button or the black button (depending on the secret digit, which will appear as a white number or a black number). The challenge is repeated many times for each secret digit. If the challenge is repeated four times for every digit and if we have a four digit PIN, the user must solve the challenge 16 times which is a time-consuming task. Figure 2.14 shows an example where the user must answer four answers about the secret digit 3.

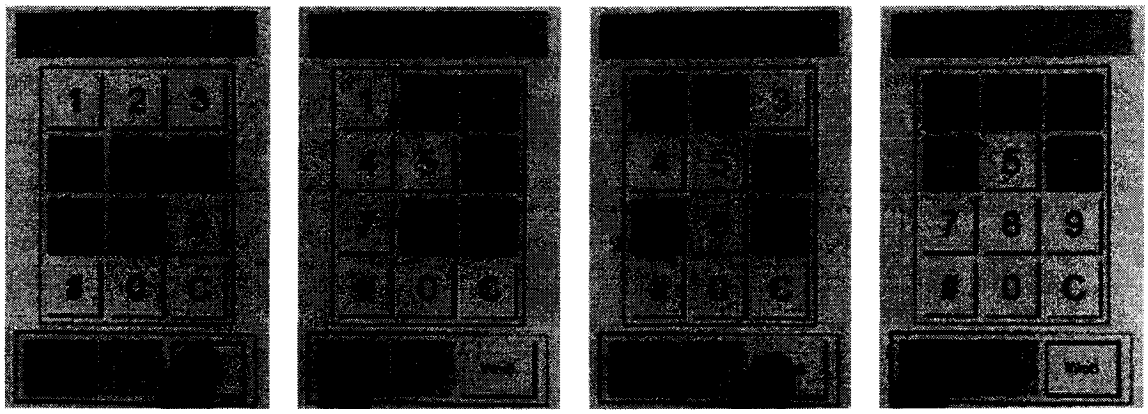

Figure 2.14: The digit 3 is the secret Pin. The user has to solve the challenge four times. [Volker et al 2004].

At this point, we have studied most graphical authentication schemes. Chapter 3 will discuss our contribution "Three-Dimensional Password" (3D Password). We believe that the current study represents a significant advancement in the world of authentication schemes.

Chapter 3

THREE DIMENSIONAL PASSWORD

In this chapter, we present a new scheme that addresses the shortcomings of the existing authentication schemes. We attempted to 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-based, recognition-based, biometrics, and token-based authentication schemes.

2. Users ought to have the freedom to select whether the 3D password used will be only recall-based, biometrics recognition-based, or token-based, or a combination of two schemes, or combination of all the different schemes. This freedom of selection is necessary due to the fact that users are different and they possess 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 will be difficult to share with others.

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

Based on the above requirements, we propose the Three-Dimensional Password (3D Password) authentication scheme.

3.1 Three Dimensional Password Overview

The idea of the proposed three-Dimensional Password (3D Password) is simply outlined as follows. The user navigates through a three-dimensional virtual environment. The combination and the sequence of the user's actions and interactions towards the objects in the three-dimensional virtual environment construct the user's 3D password. Therefore, the user can enter the virtual environment and type something on a computer that exists in (x_1, y_1, z_1) position, then enter a room that has a whiteboard that exists in a position (x_2, y_2, z_2) and draw something on the whiteboard. The combination and the sequence of the previous two actions towards the specific objects construct the user's 3D password. Moreover, any user input (such as speaking in a specific location) in the three-dimensional virtual environment can be considered as part of the 3D password.

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

1. a computer that the user can type in
2. a whiteboard that a user can draw on
3. an ATM machine that requires a smart card and PIN
4. a light that can be switched on/off
5. a TV where channels can be selected
6. a door that can be opened, closed, locked, and unlocked
7. a staple that can be punched
8. a fingerprint reader that requires the user's fingerprint
9. any biometric device
10. a car that can be driven
11. a book that can be moved from one place to another

12. any Graphical password scheme

13. any real life object

14. any upcoming authentication scheme

Moreover, in the three-dimensional virtual environment we can have two different computers in two different locations. Actions and interactions with the first computer are totally different than actions towards the second computer since each computer has a unique 3D position (x,y,z) in the three-dimensional virtual environment.

Each object or item in the three-dimensional virtual environment has its own

- (x, y, z) coordinates
- speed
- weight
- responses towards actions
- some other attributes

3.2 Three Dimensional 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 is 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 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 toward the objects and toward the three-dimensional virtual environment are mapped into a sequence of three-dimensional coordinates and actions, interactions, and inputs. For example, consider that a user navigates through the three-dimensional virtual environment and types "FALCON" 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 whiteboard located in (55, 3, 30) and draws just one dot in the (x, y) coordinate of the whiteboard at the specific point of (530, 250) (the user is not required to press the exact pixel but a point that is close to the original pixel). Then the user moves to another computer located in (220, 4, 77) and types "ADC". Then the user selects the login button. The representation of user actions, interactions, and inputs toward the objects and the three-dimensional virtual environments can be represented as the following:

(13, 2, 30) Action = Typing, "F",

(13, 2, 30) Action = Typing , "A",

(13, 2, 30) Action = Typing , "L",

(13, 2, 30) Action = Typing , "C",

(13, 2, 30) Action = Typing , "O",

(13, 2, 30) Action = Typing , "N",

(20, 6, 12) Action = Turning the Light, Off,

(55, 3, 30) Action = Drawing, point = (530, 250)

(220, 4, 77) Action = Typing, "A"

(220, 4, 77) Action = Typing, "D"

(220, 4, 77) Action = Typing, "C"

Two 3D Passwords are equal to each other when the sequence of actions towards each specific object is equal and the actions themselves are equal towards the objects. Figure 3.1

below shows a virtual computer that accepts textual passwords as a part of a user's 3D password.

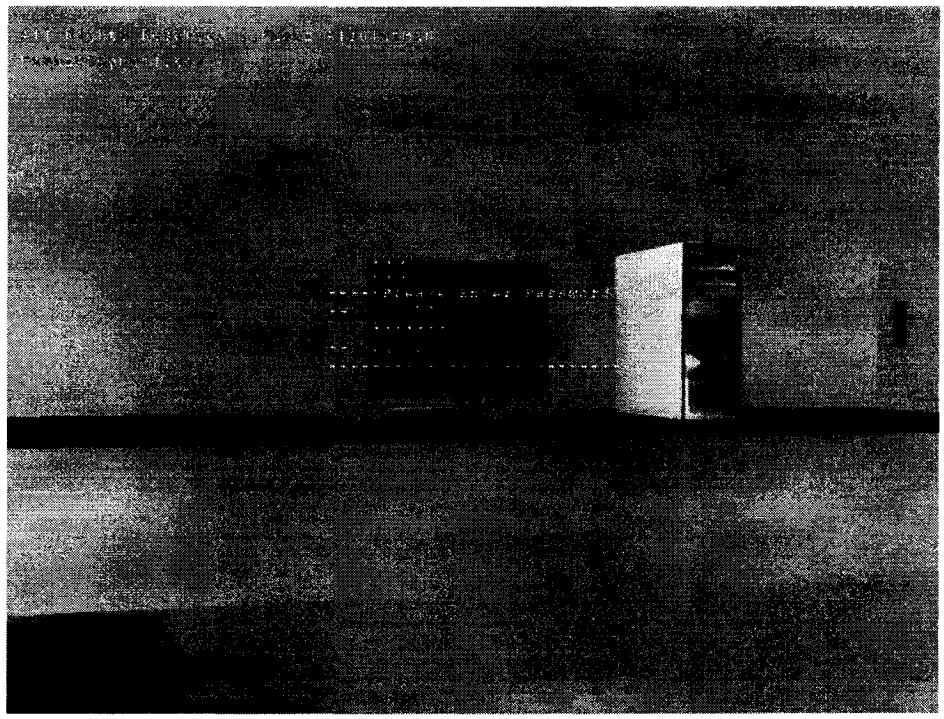

Figure 3.1: A snapshot of a proof-of-concept, three-dimensional virtual environment where the user is typing on a virtual computer as a part of the user's 3D password.

As described earlier, 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 include, which locations, and the types of responses to include are very critical tasks. The design of the three-dimensional virtual environment affects the overall strength, usability, and performance of the 3D password. Figure 3.2 shows an experimental three-dimensional environment. Guidelines on designing three-dimensional virtual environments are covered in section 3.5.

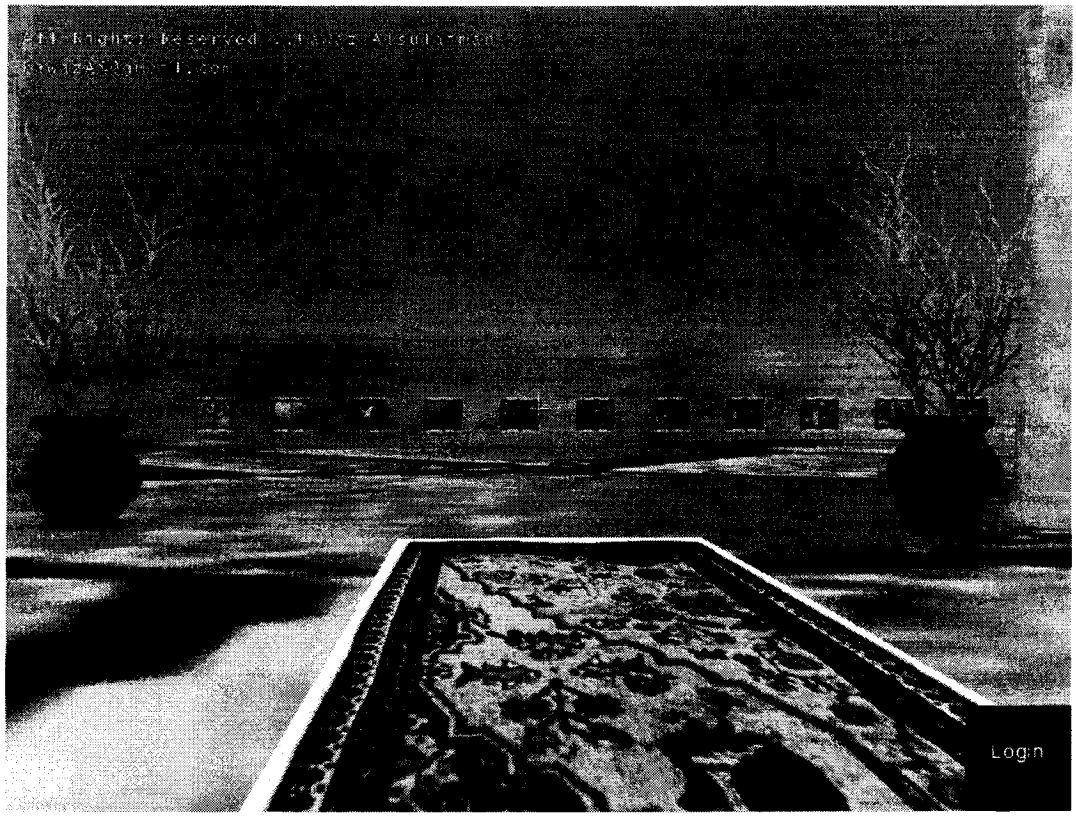

Figure 3.2: Snapshot 2 of the proof-of-concept three-dimensional virtual environment. A virtual art gallery that consist of 36 pictures and 6 computers, where users can navigate and interact with virtual objects by either typing or drawing.

Figure 3.3 illustrates 3D Password's possible selection of objects types. It covers all available existing schemes into one authentication scheme. Figure 3.4 shows a flowchart diagram of a possible 3D password. Notice that users have the freedom to choose any authentication scheme as part of their 3D password.

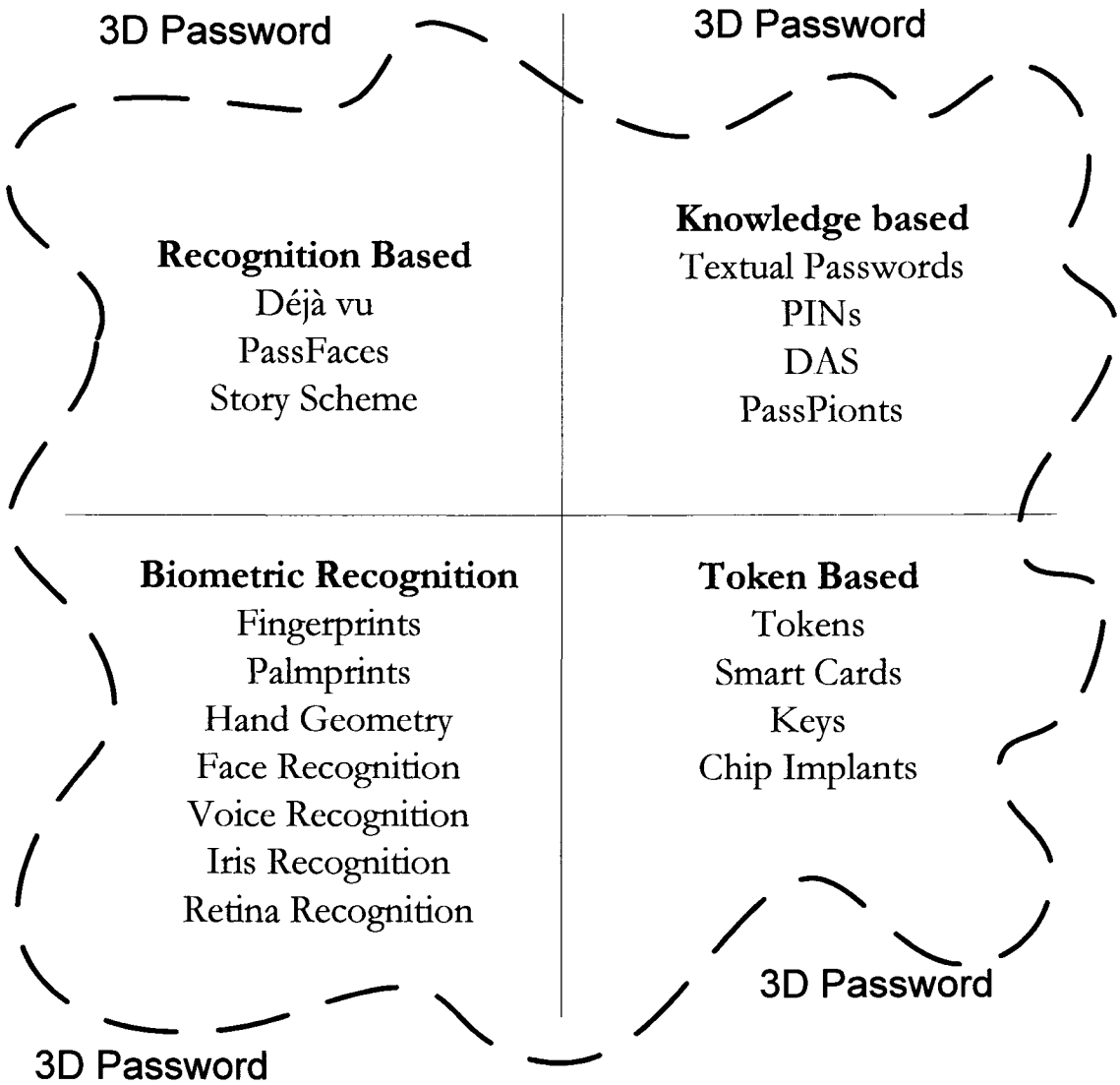

Figure 3.3: Authentication schemes divided into four categories. 3D Password can be any combination of any existing authentication schemes.

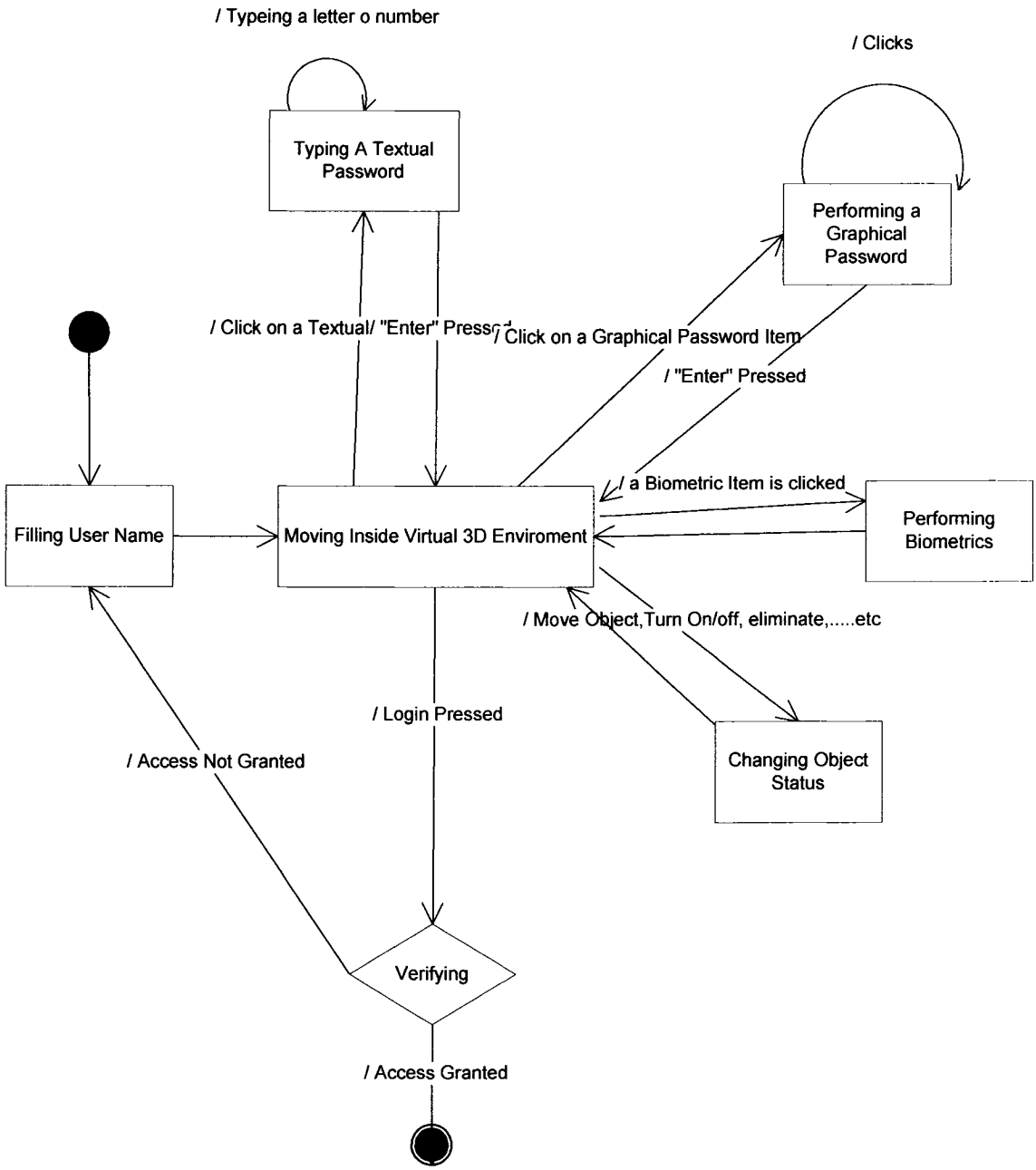

Figure 3.4: Flowchart diagram of a possible 3D Password application.

3.3 System Requirements

In this section we try to capture the system requirements through the use of Use-cases. For our system we have three use cases: a. Register. b. Sign-in. c. Change 3D Password.

A. Use-Case Specification-Register

1. Brief Description

This use case allows the user to register a new username/3D password pair to the system. The user is free to interact with any item as part of his/her 3D Password.

2 Actors

2.1 User

The user is any person wishing to access the protected system.

3. Flow of Events

3.1 Basic Flow

3.1.1 START

This use-case starts when the user chooses to create a new username.

3.1.1 FILL USERNAME

The user fills his username

3.1.2 OPERATING THREE-DIMENSIONAL VIRTUAL ENVIROMENT

The system will simulate a three dimensional virtual environment and the virtual user will be part of it.

3.1.3 NAVIGATING THROUGH THREE-DIMENSIONAL VIRTUAL ENVIRONMENT

The user navigates and walks inside the three dimensional virtual environment. The user has the capability to see the 3D items inside the three dimensional environment. The user selects 3D items among different 3D items inside the three-dimensional virtual environment. User selection of 3D items can be as much as the user wishes.

3.1.4 PERFORMING TEXTUAL PASSWORD

The system asks the user to enter a textual password as part of his 3D Password if the 3D item selected is of textual password type.

3.1.5 FININSH PERFROMING 3D PASSWORD

The user decides when he wants to finish performing his 3D Password by informing the system of his wish. This can be done by clicking a button "Done" shown to the user.

3.1.6 CONFIRMATION

The system confirms the user registration by informing the user that registering the username/3D Password pair has successfully created.

3.2 Alternative Flows (ONE)

3.2.1 ALREADY EXIST USERNAME

At FILL USERNAME if the user fills in a user name that already exists, the system informs the user that the username is already taken.

3.2.2 PERFORMING GRAPHICAL PASSWORD

the system asks the user to select points on the selected picture as a graphical password if the 3D item selected is of graphical password type. The system considers it as part of the user's 3D Password.

3.2.3 QUIT

The user has the capability to quit any time while performing his new 3D Password. However, quitting without completing the user's new 3D Password means the username/3D Password will not be registered.

B. Use-Case Specification-Sign In

1. Brief Description

This use case allows the user to login into the protected system. The user should perform the right 3D Password that belongs to his username in order to gain access.

2. Actors

2.1 User (Primary Actor)

The user is any person wishing to access the protected system.

2.2 Protected System (Secondary Actor)

The protected system is the system where the user wishes to grant access to.

3. Flow of Events

3.1 Basic Flow

3.1.1 START

This use-case starts when the user chooses to sign-in.

3.2.4 FILL USERNAME

The user fills his username

3.2.5 OPERATING THREE-DIMENSIONAL VIRTUAL ENVIROMENT

The system will simulate a three dimensional virtual environment and the virtual user will be part of it.

3.2.6 NAVIGATING THROUGH THREE-DIMENSIONAL VIRTUAL ENVIRONMENT

The user navigates and walks inside the three dimensional virtual environment. The user has the capability to see the 3D items inside the three dimensional environment. The user selects 3D items among different 3D items inside the three dimensional virtual environment. User selection of 3D items can be as much as the user wishes.

3.2.7 PERFORMING TEXTUAL PASSWORD

The system asks the user to enter a textual password as part of his 3D Password if the 3D item selected is of textual password type.

3.2.8 FININSH PERFROMING 3D PASSWORD

The user decides when he wants to finish performing his 3D Password by informing the system of his wish. This can be done by clicking a button "Login" shown to the user. If the performed 3D password is correct then the user access to the protected system will be granted.

3.3 Alternative Flows (ONE)

3.3.1 PERFORMING GRAPHICAL PASSWORD

The system asks the user to select points on the selected picture as a graphical password if the 3D item selected is of graphical password type. The system considers it as part of the user's 3D Password.

3.3.2 INCORRECT 3D PASSWORD

At FINISH PERFORMING 3D PASSWORD when the user finish performing his 3D Password and the 3D Password is incorrect then the user's access to the protected system will be denied.

3.3.3 QUIT

The user has the capability to quit any time while performing his new 3D Password. However, quitting without completing the user's new 3D Password means that the user access to the protected system will be denied.

C. Use-Case Specification-Change 3D Password

1. Brief Description

This use case allows the user to modify his old 3D Password into a new 3D Password. The user should perform the old 3D Password then perform the desired new 3D Password that belongs to his username.

2. Actors

2.1 User

The user is any person wishing to change his/her 3D Password.

3. Flow of Events

3.1 Basic Flow

3.1.1 START

This use-case starts when the user chooses to sign-in.

3.1.2 FILL USERNAME

The user fills his username

3.1.3 OPERATING THREE-DIMENSIONAL VIRTUAL ENVIROMENT

After filling the username, the system will simulate a three-dimensional virtual environment and the virtual user will be part of it.

3.1.4 NAVIGATING THROUGH THREE-DIMENSIONAL VIRTUAL ENVIRONMENT (OLD)

The user navigates and walks inside the three dimensional virtual environment. The user has the capability to see the 3D items inside the three dimensional environment. The user selects 3D items among different 3D items inside the three dimensional virtual environment. User selection of 3D items can be as much as the user wishes.

3.1.5 PERFORMING TEXTUAL PASSWORD (OLD)

For every selected 3D Item, if the 3D item is of textual password type then the system asks the user to enter a textual password as part of his 3D Password.

3.1.6 FININSH PERFROMING OLD 3D PASSWORD

The user decides when he wants to finish performing his old 3D Password by informing the system of his wish. This can be done by clicking a button "DONE" shown to the user.

3.1.7 NAVIGATING THROUGH THREE-DIMENSIONAL VIRTUAL ENVIRONMENT (NEW)

The user goes back to the three-dimensional virtual environment. The user has the capability to navigate and walk inside the three dimensional virtual environment. The user has the capability to see the 3D items inside the three dimensional environment.

3.1.8 SELECT A 3D ITEM (NEW)

The user selects 3D items among different 3D items inside the three-dimensional virtual environment. User selection of 3D items can be as much as the user wishes.

3.1.9 PERFORMING TEXTUAL PASSWORD (NEW)

The system asks the user to enter a textual password as part of his 3D Password if the 3D item selected is of textual password type.

3.1.10 FININSH PERFROMING NEW 3D PASSWORD

The user decides when he wants to finish performing his old 3D Password by informing the system of his wish. This can be done by clicking a button "UPDATE" shown to the user.

3.2 Alternative Flows (ONE)

3.2.2 PERFORMING GRAPHICAL PASSWORD

The system asks the user to select points on the selected picture as a graphical password if the 3D item selected is of graphical password type. The system considers it as part of the user's 3D Password.

3.2.3 INCORRECT OLD 3D PASSWORD

At FINISH PERFORMING OLD 3D PASSWORD when the user finish performing his old 3D Password and the 3D Password is incorrect then the system will notify the user that it is incorrect Old 3D password and the process of changing 3D Password failed.

3.2.4 QUIT

The user has the capability to quit anytime while performing his new 3D Password. However, quitting without completing the user's new 3D Password means that the user access to the protected system will be denied.

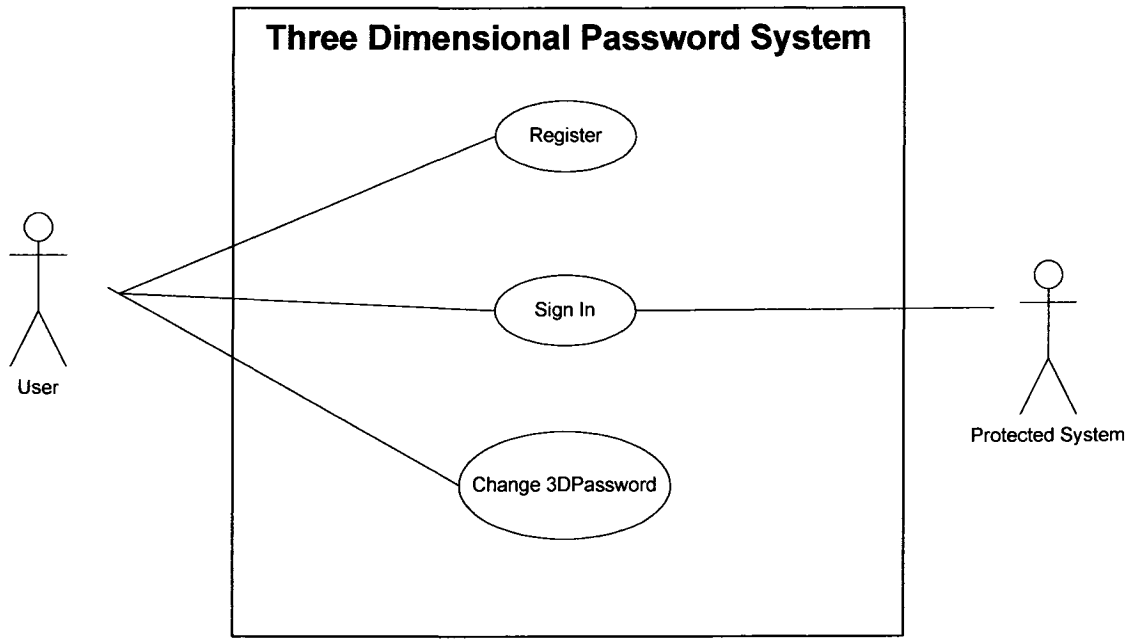

Figure 3.5: System use case Diagram

3.4 System Architecture

In this section, we describe the architecture of the three-dimensional password. Moreover, we will show the class diagram of 3D password. Then we will cover the collaboration diagrams that relate to our system use cases. Figure 3.6 shows the overall architectural view of the system. The system contains the following components:

- **Three-dimensional virtual environment author**: This component is very important. The three-dimensional virtual environment's author should be very easy to use by end-users. Administrators use this component to build and design three-dimensional virtual environments that satisfy the protected system requirements and user requirements. The selection of 3D items is made through this component. This component should be very simple to use because if it is not, then the administrators will likely use the default three-dimensional virtual environment or a design made by someone else. This design might not reflect all system requirements

- **Three-dimensional virtual environment:** The three-dimensional virtual environment is a virtual 3D world that a user can navigate through. In this

component, the navigation process should be specified. What devices should be used for navigation? It should also specify how to interact with 3D items. For example, we can specify a system where users use the keyboard as a means of interaction and navigation. There are many devices that can be used for interaction with objects and the three-dimensional virtual environment such as keyboard, mouse, styles, microphone, joystick, etc. Moreover, which 3D items should be used in the three-dimensional virtual environment should be specified. The 3D, virtual environment is constructed using 3D objects. 3D items can be a sofa, chair, table, TV, telephone, computer, picture, light, wall, door, car, book, pen, ground, or any object that we encounter in the real world. Moreover, the 3D items' responses towards the user's action should be specified. Among possible object types are textual passwords, graphical passwords, fingerprints recognition, voice recognition, iris recognition, smartcard reading, etc. The properties of the 3D objects should be specified carefully. Chapter 6 goes through implementation properties of 3D objects in more detail.

- **User**: The user can be represented as a 3D object in the three-dimensional virtual environment's component or it can be a separate component. We prefer separating the user as a different component from the 3D items for further use.

- **Observer:** This component observes the user's actions and interactions inside the three-dimensional virtual environment. It acts like a camera that captures the user's movements and actions towards 3D objects. This component is crucial because it determines what kinds of events the system should observe. For example, the system designer should specify whether user movements are considered as a part of 3D password or not. Also, it should specify what interactions and actions are counted as part of 3D password.

- **Verifier:** This component performs the verification process. It uses the observation information passed by the observer component. It compares the legitimate user 3D Password that is stored in the system with the information provided by the observer. If they are equal, then the user is authenticated. Otherwise, access is denied. Encryption can be a part of the verifier. It is up to the system designer to select the appropriate encryption algorithm.

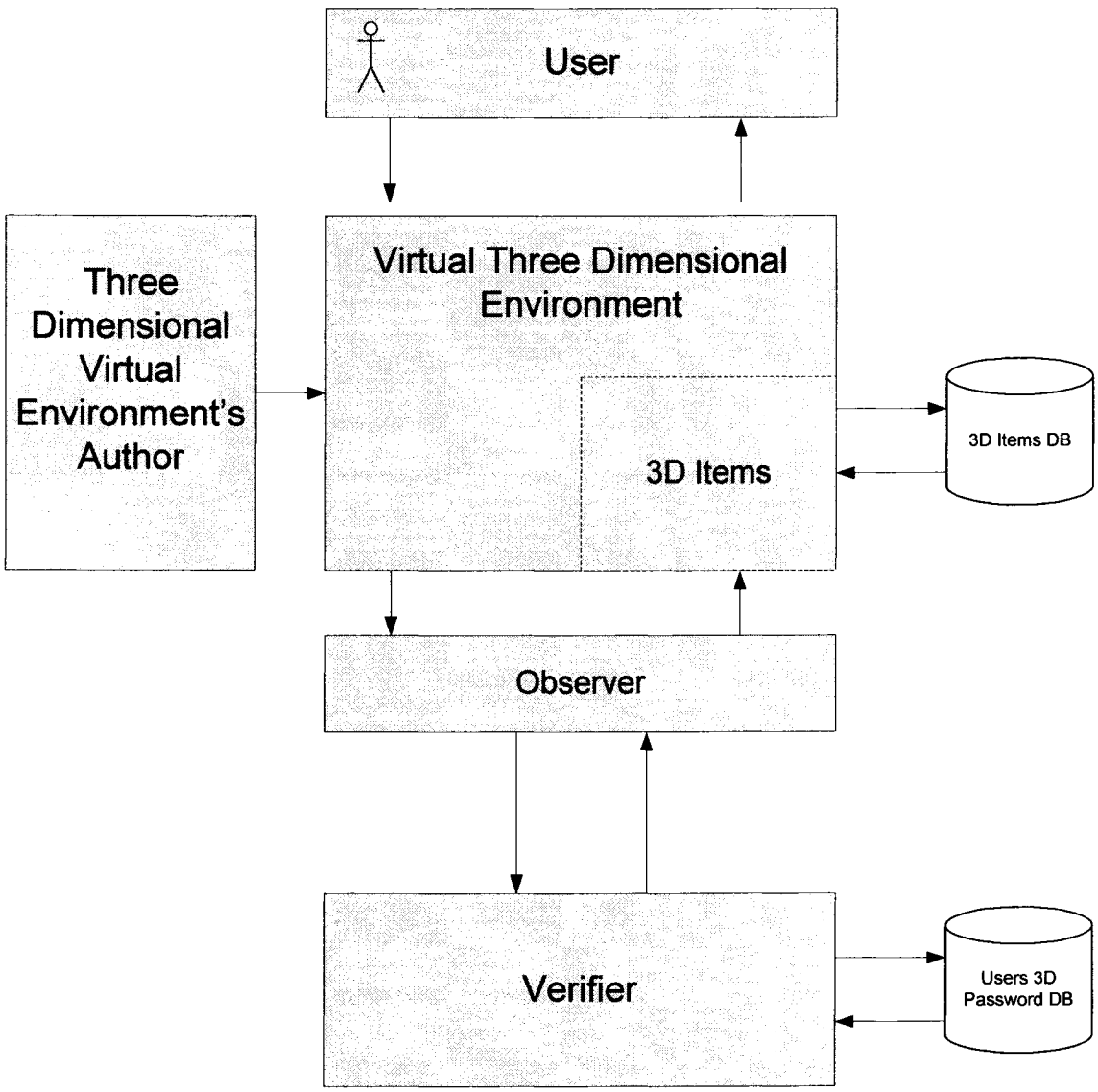

Figure 3.6: Block Diagram that represents the overall architectural view of the system

Figure 3.7 shows the class diagram of 3D Password. Figure 3.8 illustrates the collaboration diagram of 3D Password for Register use case. Figure 3.9 depicts the collaboration diagram of 3D password for Sign-in use case. Figure 3.10 is the collaboration diagram for Change 3D Password use case. We have taken into our consideration further development of 3D Password system that might have additional features.

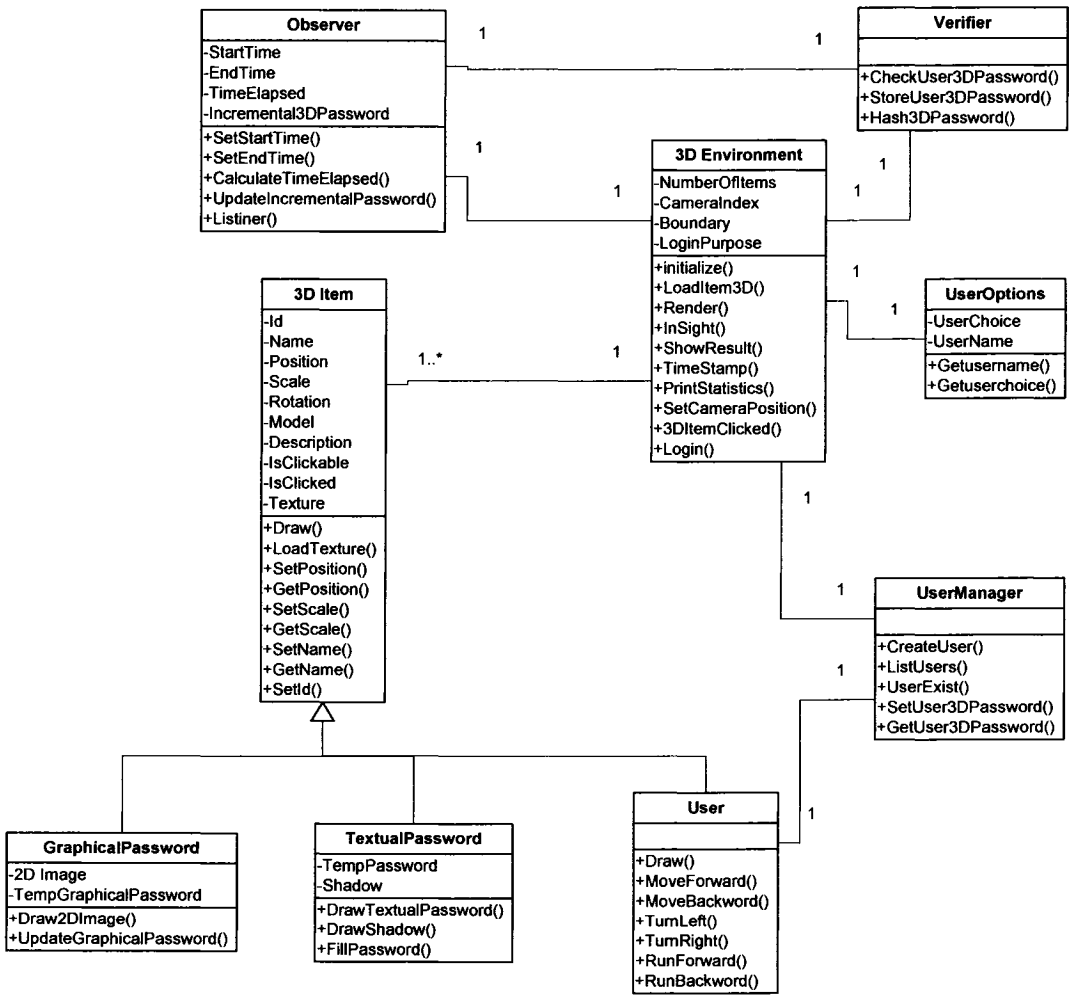

Figure 3.7: Class Diagram of 3D Password

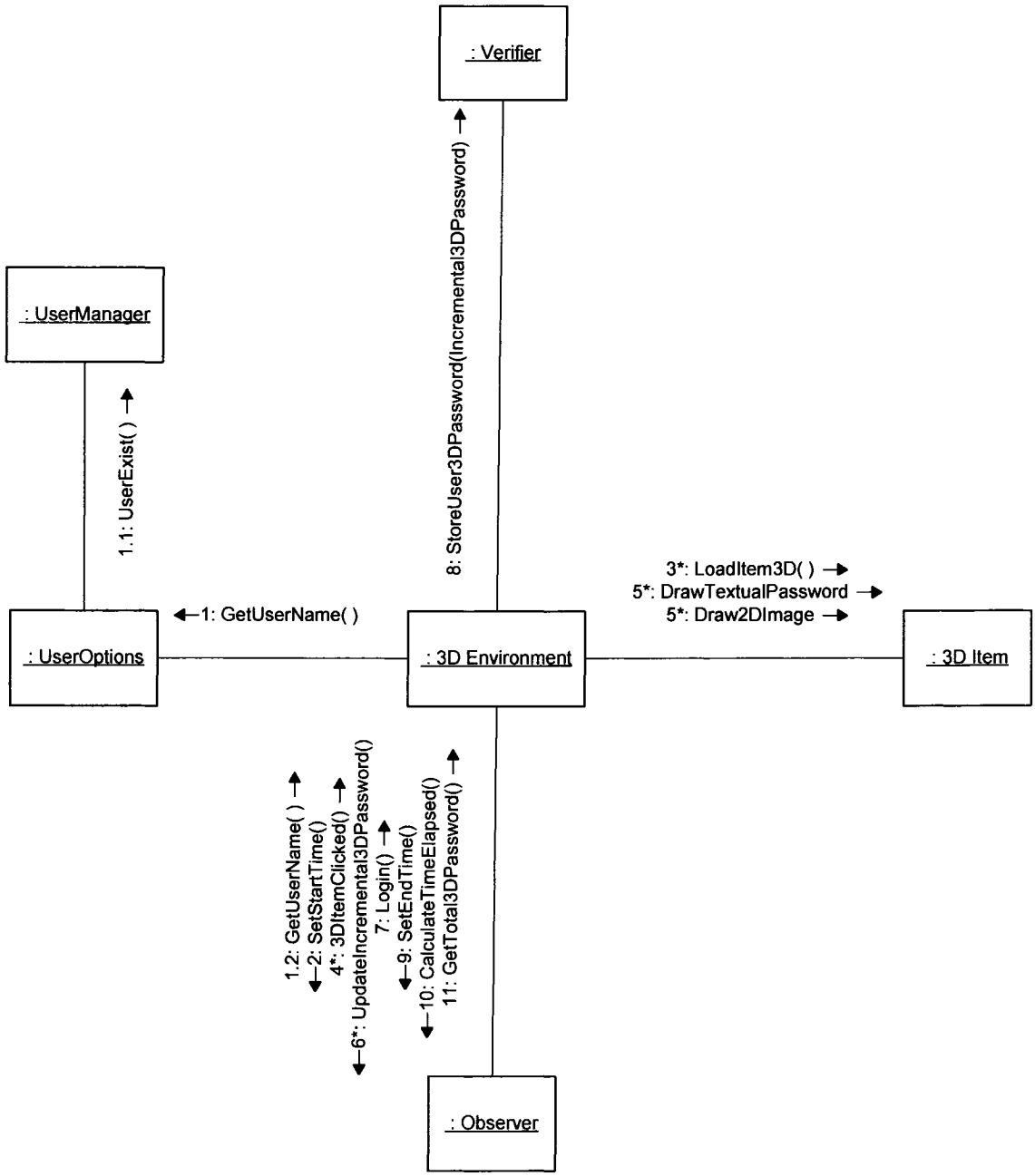

Figure 3.8: Collaboration Diagram for Register use case

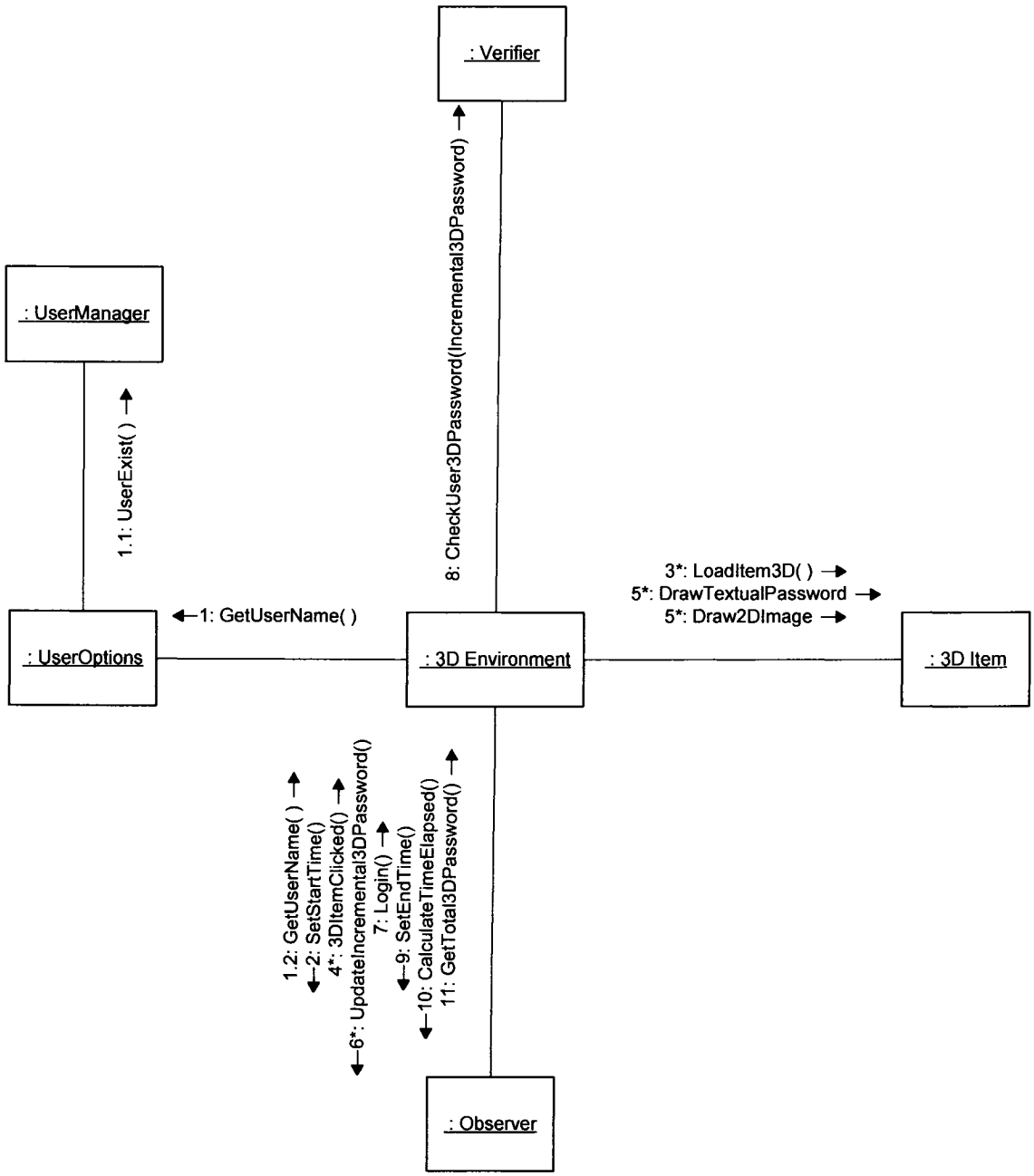

Figure 3.9: Collaboration diagram for Sign-in Use case

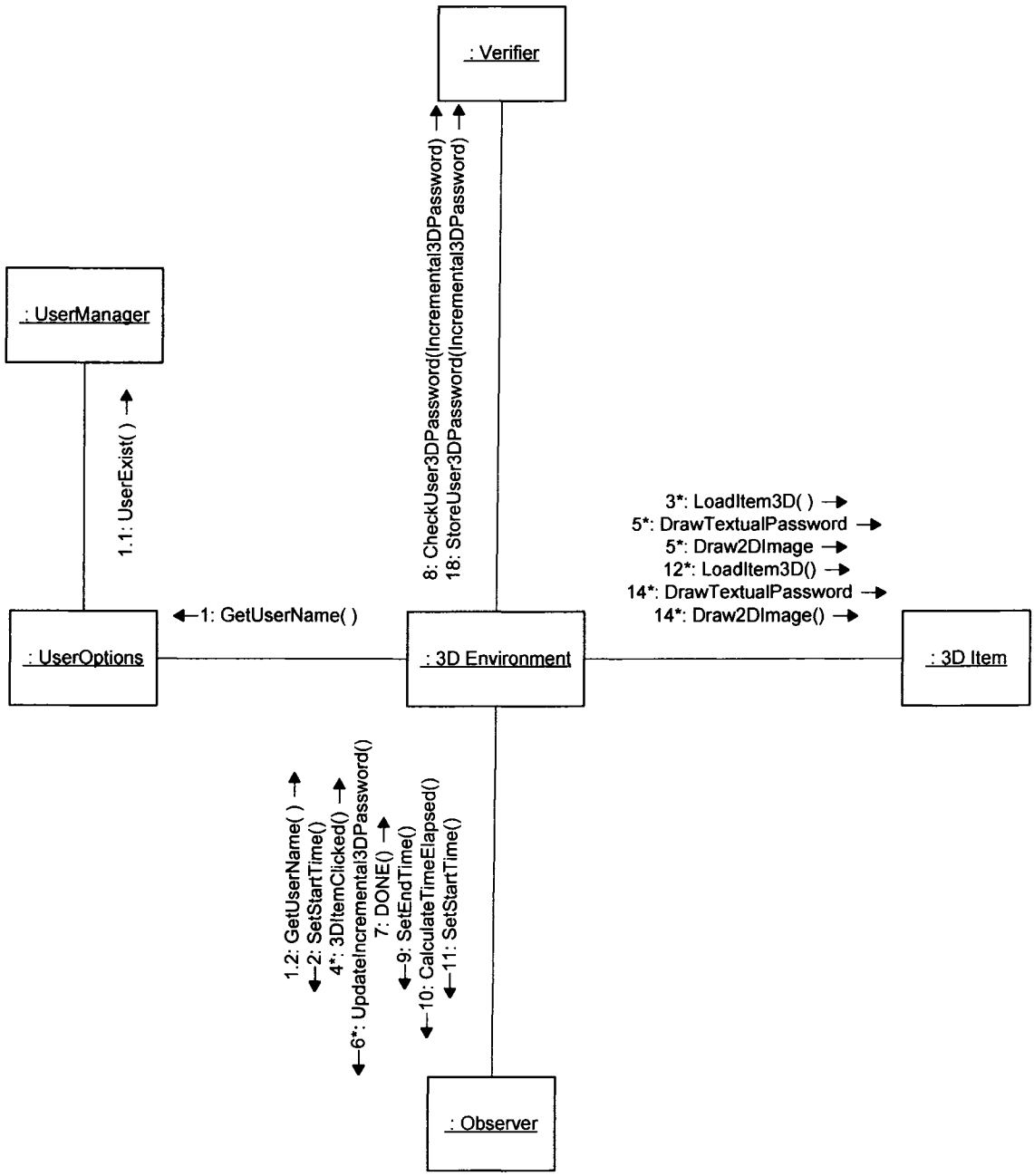

Figure 3.10: Collaboration Diagram for Change 3D Password use case.

3.5 Three Dimensional Password Design Guidelines

Designing a three-dimensional virtual environment effect the usability, effectiveness, and acceptability of a 3D Password system. Therefore, the first step in building a 3D password

system is to design a three-dimensional environment that reflects the administration needs and the level of security requirements. The design of three-dimensional virtual environments should follow these guidelines:

1. **Real Life Similarity:** The prospective three-dimensional 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 towards virtual objects should reflect real life situations. Object responses should be realistic. The goal is to have a three-dimensional virtual environment that users can interact with by using commonsense.

2. **Object Uniqueness and Distinction:** Every virtual object or item in the three-dimensional virtual environment is different from any other virtual object. The uniqueness comes from the fact that every virtual object has its own 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 three-dimensional virtual environment should consider that every object should be distinguishable from other objects. The designer of such an environment should use commonsense and all possible means of distinguishing every object or group of objects from each other. A simple, real life example is home numbering. Assume that 20 homes or more are similar to each other, and the homes are not numbered. Does this design increase distinction or not? Similarly, in designing a three-dimensional virtual environment, the environment should be easy for users to navigate through and easy to distinguish between objects. The distinguishing factor increases the user's recognition of objects. Therefore, it improves the 3D Password performance.

3. Objects that Looks alike but are not the same: This property is a little tricky. In three-dimensional virtual environments design objects should be unique and distinct. However, in order to prevent users recording or sharing their 3D Passwords with other people, objects should look similar to each other. Figure 3.11 shows an example of two pictures that are different. However, they are somehow similar to each other (both present faces).

Figure 3.11: Two different pictures. However, they have some similar features such as the two pictures present several faces.

Figure 3.11 shows two different pictures that have some similar features. Both feature faces. This kind of similarity is one method used to prevent sharing three-dimensional passwords with other users such as friends. In describing the 3D Password, the three-dimensional environment contains pictures that have similar features and thus the user must be more descriptive in describing all similar and non-similar features. This process is difficult to do and so users are less likely to share their 3D Passwords. Figure 3.12 shows another example of two different pictures that have some similar features.

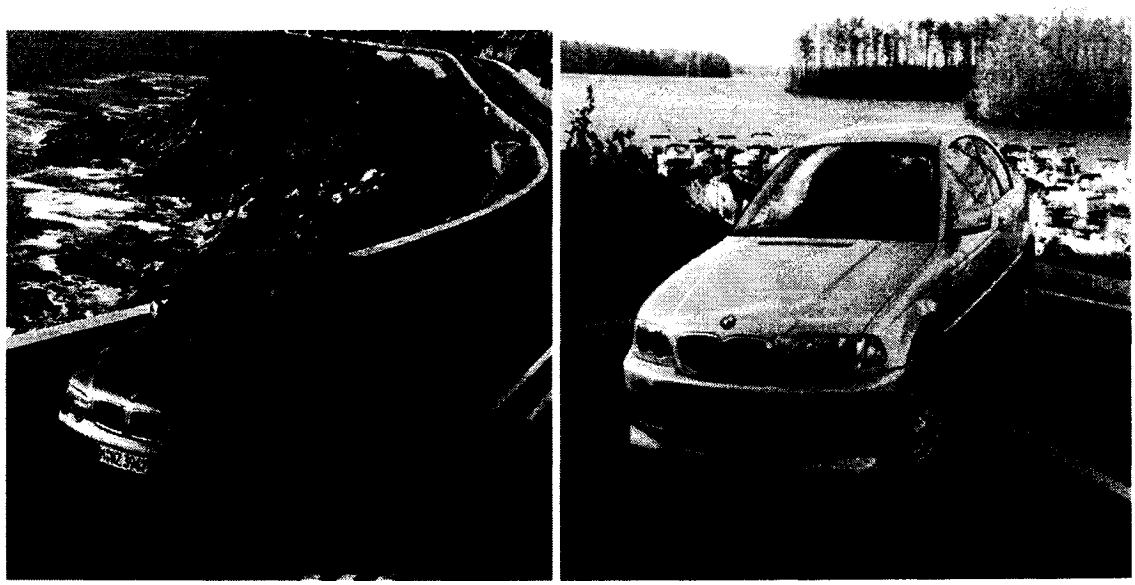

Figure 3.12: Two different pictures that have some similar features.

4. **Three-dimensional virtual environment size:** A three-dimensional 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 three-dimensional environment should be studied carefully. A large three-dimensional virtual environment will increase the time needed by the user to perform a 3D Password. Moreover, a large three-dimensional virtual environment can contain a large number of virtual objects. Therefore, the probable 3D password space becomes broadens. However, a small three-dimensional virtual environment usually contains a few objects and so performing a 3D Password will take less time.

5. **Number of objects (items) and their types:** A part of designing a three-dimensional 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. To simplify, we can say a type of object response can be requesting a textual password or requesting a fingerprint. Selecting the right object response types affects the probable password space of a 3D Password. Moreover, the number of objects also affects the probable space of the 3D Password.

6. **System importance:** The three-dimensional virtual environment should consider what kind of systems will be protected by a 3D Password. The number of objects and the types of objects that have been used in the three-dimensional virtual environment should reflect the importance of the protected system.

3.5 Applications of 3D Passwords

Due to the fact that a 3D Password can have a password space that is very large compared to other authentication schemes, 3D Password's main application domains are critical systems and resources. Possible critical applications include:

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. Moreover, entrance to such locations that are usually protected by cards and PIN numbers can also be protected by a 3D Password. Therefore, a 3D Password can be used to protect the entrance to such locations and the usage of such servers.

Nuclear and military facilities: Such facilities should be protected by the most powerful authentication systems. A 3D Password has a very large probable password space and since it can contain token-based, biometrics recognition-based, knowledge-based and recognition-based authentication in one authentication system, it is a sound choice for high-level security locations.

Airplanes and jetfighters: Because of the possible threat of misusing airplanes and jetfighters for religio-political agendas, usage of such airplanes should be protected by a powerful authentication system. A 3D Password is recommended for these systems.

Meeting rooms: Most meeting rooms are protected with token-based authentication systems or with biometrics recognition systems. However, token-based systems can be stolen or lost and some biometrical data can be forged. Therefore, 3D Password offers a sound replacement to such systems. Regular meetings rooms can still use token-based system because 3D Password can take up to one minute per person for authentication, which is sometimes not preferable.

Moreover, 3D Passwords can be used in less critical systems because the three-dimensional virtual environment can be designed to fit any system's needs. A small three-dimensional virtual environment can be used in many systems including:

1. ATM machines
2. PDAs
3. television, internet, and gaming parental control systems
4. network routers and firewalls
5. hotel safe boxes
6. desktop computers and laptop logins
7. web authentication
8. bank safety deposit boxes

Chapter 4

IMPLEMENTATION

In this chapter we will talk about the implementation of 3D Password. We will describe the main components of our system. Moreover, we will demonstrate some implementation details.

As a proof-of-concept, we have implemented a three-dimensional virtual environment using Java and JOJL [LIGHT WIEGHT JAVA GAME LIBERARY 2005]; [JOGL API PROJECT 2005]. We have included two kinds of authentication schemes inside 3D Password, namely textual passwords and graphical passwords.

4.1 System Components

Our implementation of 3D Password is divided into four main components. Figure 3.6 shows the main components. We will try to describe the necessary issues regarding the implementation of such components (our implementation did not cover the three dimensional password author component)

1. **Three-Dimensional Virtual Environment:** The three-dimensional virtual environment is a virtual 3D world within which a user can navigate. In order to navigate, the user must use the arrow keys, some keyboard keys, and a mouse. The three-dimensional virtual environment is made up of 3D objects. 3D objects can include: sofas, chairs, tables, TVs, telephones, computers, pictures, lights, walls, doors, cars, books, pens, ground, or any object that the user encounters in the real world.

Each 3D object has properties, which include:

- **Position:** The location is represented in (x, y, z) coordinates.

- **Orientation:** The orientation is represented in the angle of the 3D item or object. This property determines whether the 3D item faces the north or the south or any specific angle.

- **Weight:** For realism, each 3D object has its own weight.

- **Speed:** This feature determines how fast the 3D item or object is moving.

- **Acceleration**

- **Responses to actions:** Determines responses towards actions that occur to specified 3D objects.

- **Visibility:** Determines whether the item is visible or not. Moreover, it determines the distance from which the 3D object can be seen. We have added this feature to enhance the performance of our system. The user cannot see 3D items that are located very far away. However, if the 3D item is close enough, then the user can see it.

There are three types of responses towards actions in our system:

a. **Textual password response**: 3D items that have a textual password response require textual input from the user. The user's textual input is shadowed to prevent shoulder-surfing attacks. Many 3D items can have textual password responses. For example: desktop computers, PDAs, laptops, keyboards, and calculators.

b. **Graphical password response**: 3D items that have a graphical password response show a 2D image to the user. The user clicks on some points on the image as part of the user's 3D password. The image is divided into a grid. The image is divided into small squares. The size of each square is 64 pixels × 64 pixels. Therefore, we determine which square the user clicks as part of the user's 3D password.

c. **No response:** 3D items or objects that are part of three-dimensional virtual environments. However, those items do not have any response towards any actions. Some examples of such 3D items are walls, sky, ground, trees, and windows.

The designer of the three-dimensional environment specifies which items do not have responses and which 3D items have textual or graphical password responses.

4.2 Experimental Three-dimensional virtual Environment

We have built a small experimental three-dimensional virtual environment. The three-dimensional virtual environment is simply an art gallery that the user can walk into. It consists of the following virtual objects:

1. Six 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.

The pictures and the computers are scattered in the three-dimensional virtual environment as illustrated in Figure 4.1 below.

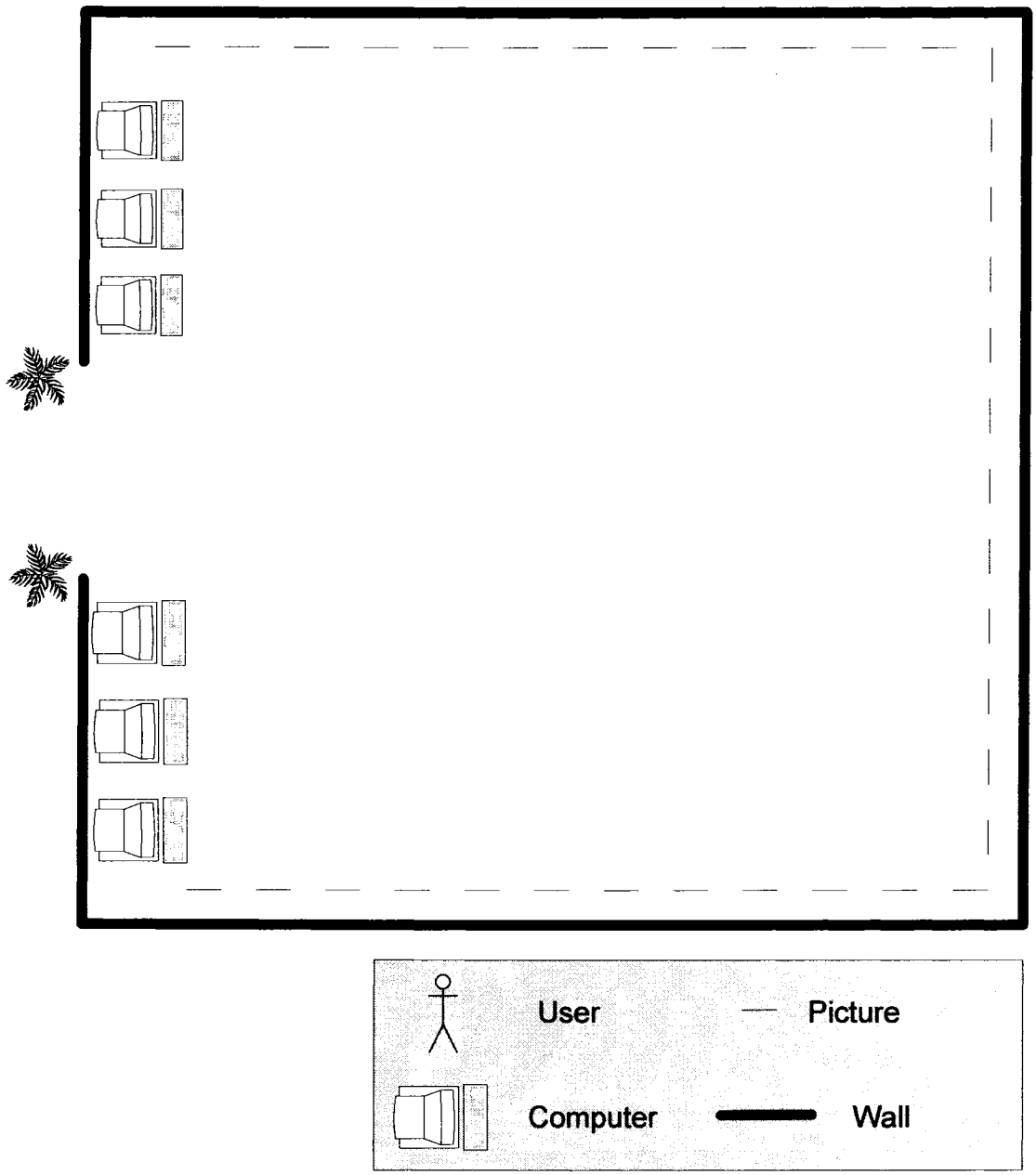

Figure 4.1 A proof-of-concept three-dimensional virtual environment's design

Figure 4.1 illustrates the three-dimensional virtual environment's design. There are six computers that accept textual passwords and 36 pictures. The user may navigate through the three-dimensional virtual environment and type something on any computer and click anywhere on the picture as part of the user 3D Password. The design of the three-dimensional virtual environment followed the guidelines mentioned in section 3.4 of this thesis.

4.3 User Interface

We tried to simplify the user interface for higher usability. Figure 4.2 shows a snapshot where users have to type their username. At this moment, we do not notify the user if the username exists or not. We hide this information to prevent any attacks on our system. Finding a legitimate username is the attacker's first step.

At the same screen we expect the user to select the purpose of login. Figure 4.3 shows three possible selections: login, create a new user, or change user 3D Password. If the user selects change user 3D password then the user has to perform the old 3D Password. Then, if the old 3D Password is correct, the user then performs the new 3D Password and we discard the old 3D Password.

Figure 4.2 User must type the username as the first step in performing 3D Password.

Figure 4.4 shows a snapshot of the three-dimensional virtual environment. The user can navigate through the three-dimensional virtual environment and interact and select any picture to enter a graphical password. When the user clicks on a picture, the picture becomes a full screen picture and the user may select any interesting points on the selected picture. The selected points of the specific picture become as a part of the user's 3D Password. As described previously, the picture is divided into a grid. Each square is of size 64 × 64 pixels. Therefore, the user does not have to click on the exact pixel, which is impossible, but the user should click on a point that is very close to the original point.

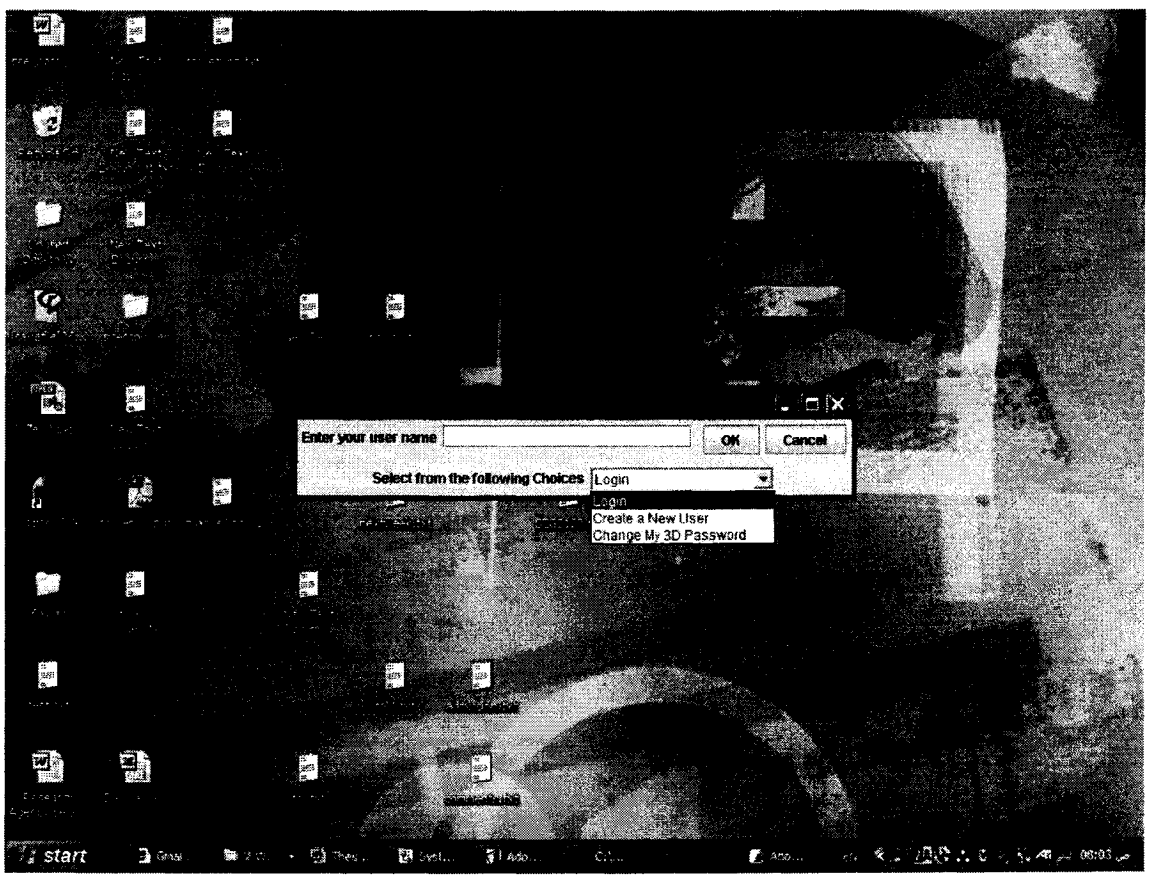

Figure 4.3: The user may select whether to login, create a new username, or change the 3D Password.

The login button is located on the bottom right (corner) of the screen as shown in figure 4.4 and figure 4.5. We tried to make the user interaction as simple as possible. The user must navigate through the three-dimensional virtual environment and interact with objects. Once the user finishes performing the 3D Password, he/she must click on the login button. Access

on the system depends on the verification process. The decision of granting access or denying access is made based on the correctness of the user's 3D Password.

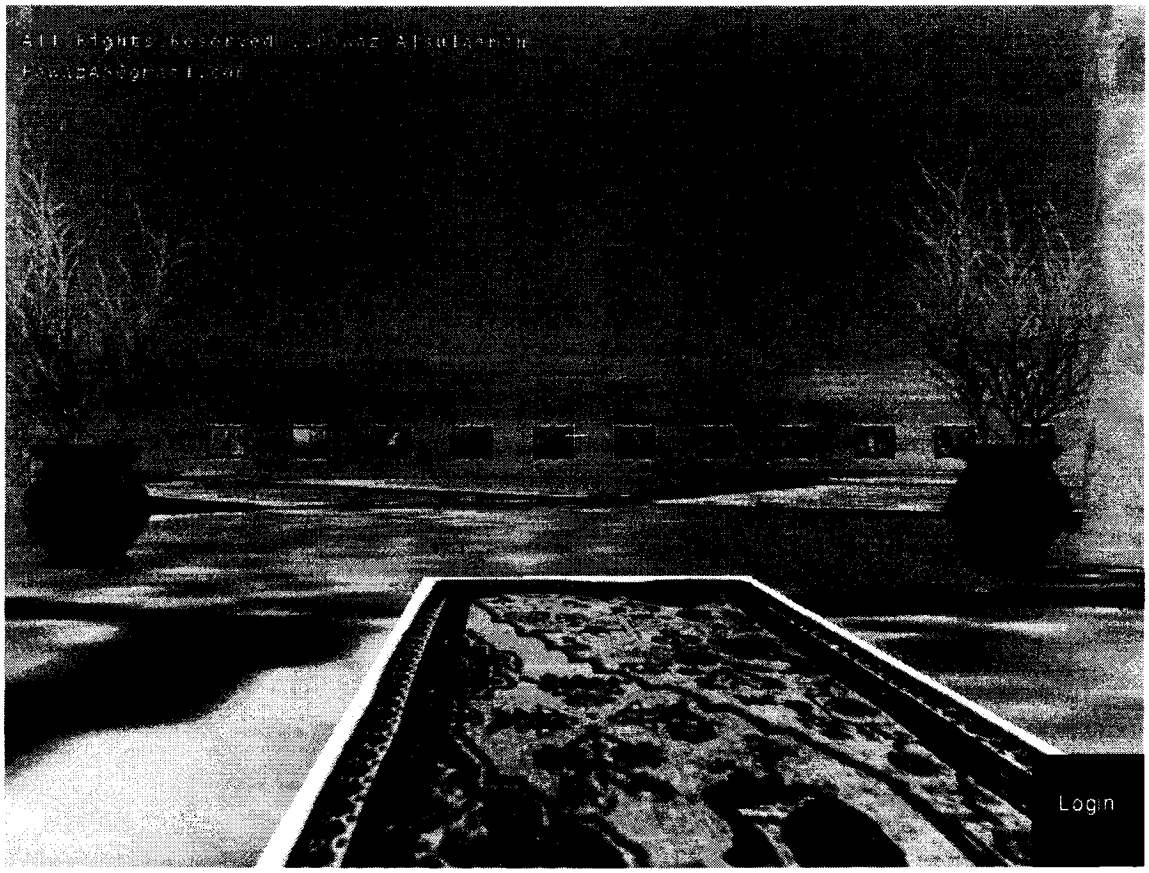

Figure 4.4: User navigates through the three-dimensional virtual environment. User can select any picture as part of his/her 3D Password.

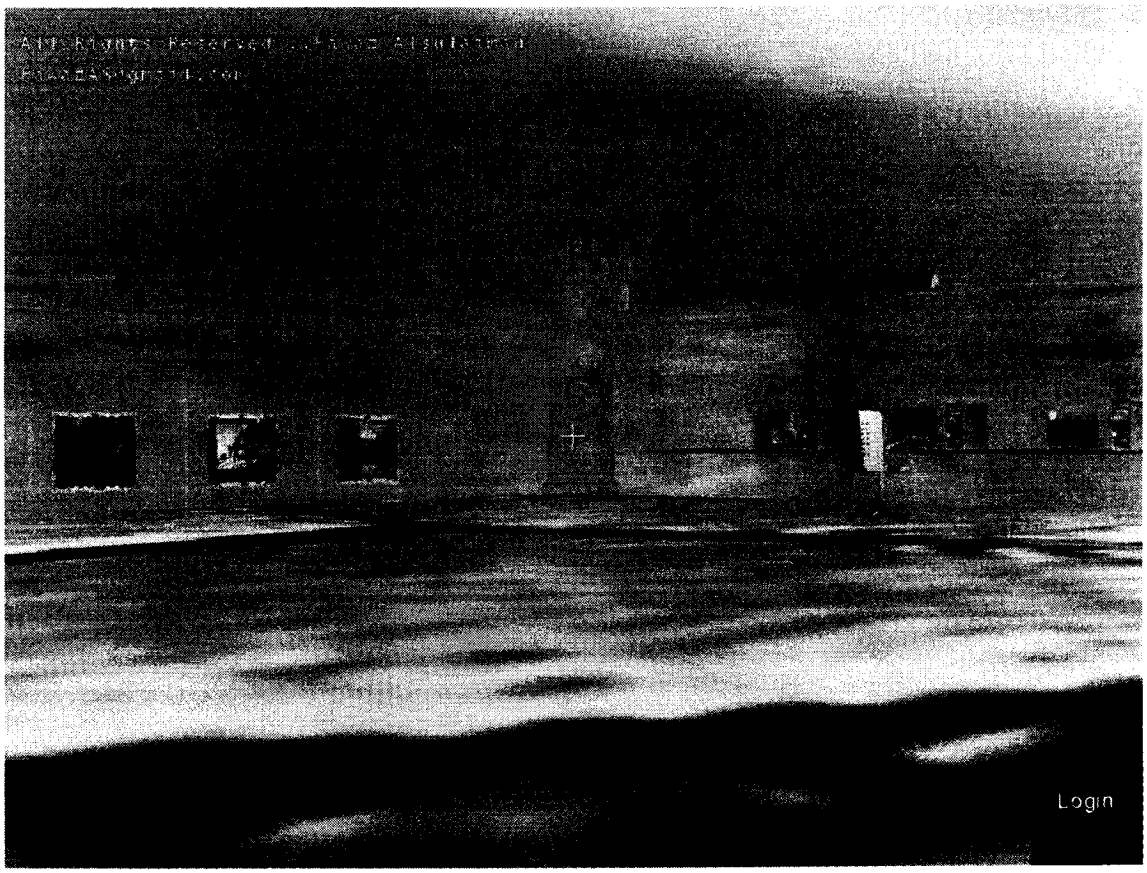

Figure 4.5: User can interact with computers or pictures as a part of user's 3D Password. Login button is on the right bottom corner.

Chapter 5

EXPERIMENTAL RESULTS

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

In this chapter we will start with the experimental three-dimensional virtual environment's design. Then we will show the results of testing such system. Finally, we present the users feedback about existing authentication schemes and our 3D Password.

5.1 Experimental setup

We have used a testing machine with the following specifications: 1.80 GHz Pentium® M Centrino™ with 512MB RAM, and ATI Mobility Radeon 9600 video card.

Almost 30 graduate and undergraduate students have tested the experimental 3D Password. Most of them are SEG 3210 students and MCR LAB (Multimedia Communications Research Laboratory) members. The experimental testing was held on an MCR LAB using the machine specified above.

5.3 Security Analysis

The information content of a password space is defined in Jermyn et al. [JERMYN et al. 1999] as "the entropy of the probability distribution over that space given by the relative frequencies of the passwords that users actually choose". It is a measure that determines how difficult the attack is. Even thought textual password space may be relatively large, an attacker might just need a small subset of the full password space as Klein [KLEIN 1990] observed. However, trying to have a scheme that has a very large possible password space is one of the important parts in resisting the attack on such a scheme. Another factor is trying 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 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.

5.3.1 The Size of the 3D Password Probable 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 $\prod(L_{max}, G)$ 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 environment. The symbol $\prod$ 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:

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

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 Oi.

$$m = \sum_{i=1}^{i=O^{max}} h(Oi, Ti, x_i, y_i, z_i) \quad \text{where } x_i=x_j,\ y_i=y_j, \text{ and } z_i=z_j \text{ only if } i=j \tag{2}$$

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 $h(Oi, Ti, x_i, y_i, z_i)$ determines the number of possible actions and interactions towards the object Oi based on the object type (Ti). Possible object types are textual password objects, graphical password objects, DAS [JERMYN et al. 1999] graphical passwords objects, fingerprint objects, etc.

$$h(Oi, Ti, x_i, y_i, z_i) = f(Oi, Ti, x_i, y_i, z_i) \tag{3}$$

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 [JERMYN et al. 1999] (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 5.1 and Figure 5.2 illustrate the key size space of a possible 3D Password as specified in section 3.4 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 5.3 shows the points where the 3D Password exceeds two important textual password points. Point (a) shows that by having only two actions and interactions as a 3D Password, the 3D Password exceeds the number of textual passwords used by Klein [KLEIN 1990] to break 25% of textual passwords of 8 characters. Point (b) represents the full textual password space of 8 characters or less. It shows that by performing only four interactions, actions, and inputs as a 3D Password, the 3D Password space exceeds the full textual passwords of 8 characters or less.

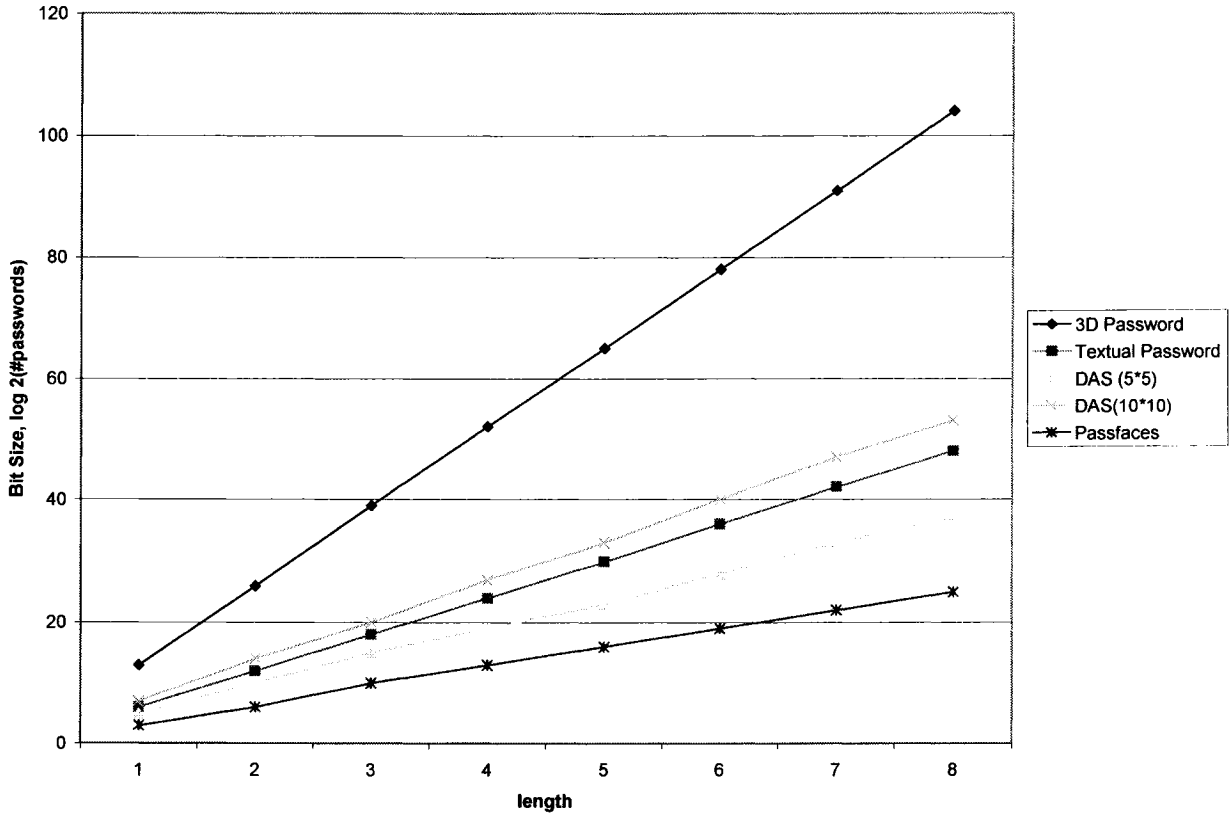

Figure 5.1: Comparison between the full password spaces of 3D Password, Textual password, PassFaces, DAS of grid size (5× 5), DAS of grid size (10 × 10). The length represents the number of characters for textual passwords, the number of actions, interactions, and inputs towards the objects in the 3D Password, the number of selections for PassFaces, and the number of points that represent the strokes for Draw A Secret (DAS). The length is up to 8 (characters/actions, interactions, inputs/selections). The 3D Password virtual environment is as Specified in Section (3.4)

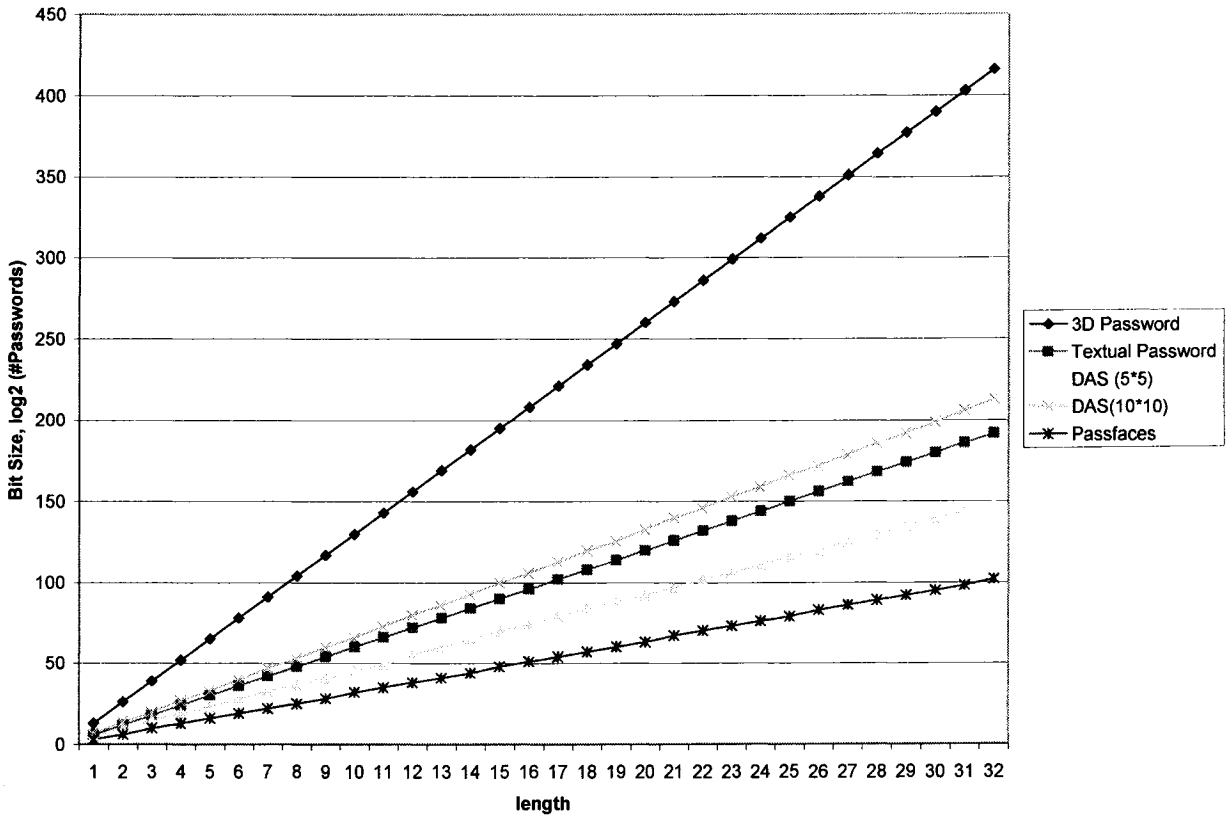

Figure 5.2: A comparison between the full password spaces of 3D Password, textual password, PassFaces of size (3×3 possible faces each turn), DAS of grid size (5× 5), and DAS of grid size (10 × 10). The length represents the number of characters for the textual passwords, the number of actions, interactions, 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). The 3D Password virtual environment is as specified in Section (3.4). We can see how the 3D Password's possible passwords are much larger than most existing authentication schemes.

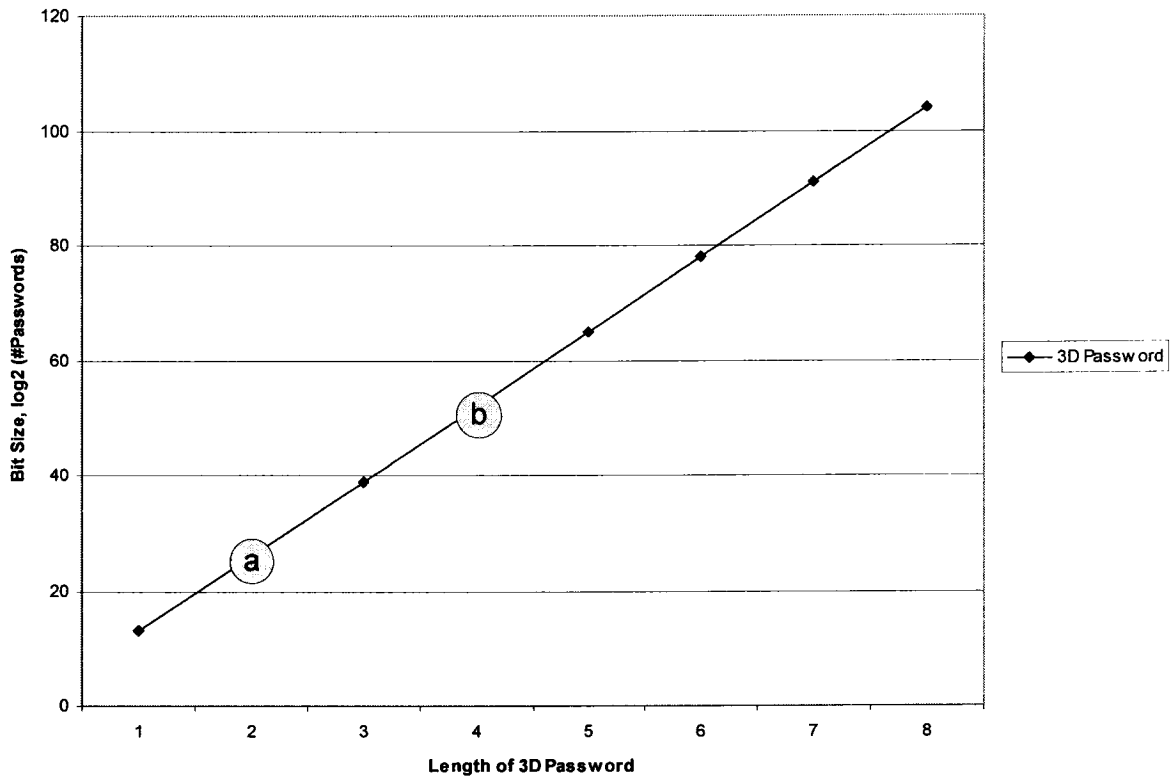

Figure 5.3: Observing the number of possible actions/interactions of a 3D Password within a three-dimensional environment specified in Section 3.4 Compared to the two critical points of textual passwords. Point "a" is the Bit size of Klein [KLEIN 1990] (3×10^6) dictionary of 8 character textual passwords. Point b represents the full password space of 8-character textual passwords.

5.3.2 Three Dimensional Password Distribution Knowledge

Having knowledge about the most probable textual passwords is the key behind dictionary attacks. Klein [KLEIN 1990] used a small set of (3×10^6) words that have a high probability of usage among users. The question is how has such information (high probable passwords) been found and why? Users tend to choose words that have meaning, such as places, names, famous people's names, actor's names, sports terms, biological terminologies, etc. Therefore, finding these different words from the dictionary is a relatively simple task. Using such knowledge yields a high success rate for breaking textual passwords. Any authentication

scheme is affected by the knowledge distribution of the user's secrets. According to Davis et al. [DAVIS et al. 2004] PassFaces [REAL USER CORPORATION 2005] users tend to choose faces that reflects their own taste on face attractiveness, race, and gender. Moreover, 10% of male passwords have been guessed in only two guesses. Another study [THORPE AND OORSCHOT 2004] regarding user selection of DAS [JERMYN et al. 1999] concluded for their secret passwords, users tend to draw things that have a meaning, which simplifies the attacker's task.

Currently, knowledge about the user's selection of three-dimensional passwords is not available to the attacker. Moreover, having different kinds of authentication schemes in one virtual environment causes the task to be more difficult for the attacker. In order to acquire such knowledge, the attacker must have knowledge about every single authentication scheme and knowledge of the most probable passwords using this specific authentication scheme. This knowledge, for example, should cover the user's most probable selection of textual passwords, different kinds of graphical passwords, and knowledge about the user's biometrical data. This knowledge is required because every object in a 3D Password can belong to a different authentication scheme. Moreover, knowledge about the design of a three-dimensional virtual environment is required in order for the attacker to launch a customized attack.

5.3.3 Attacks and Countermeasures

In order to realize and understand how 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 then we have to find the countermeasures 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 3D Passwords. This kind of attack is very difficult for the following reasons:

1. Time needed to login: The total time needed for a legitimate user to login may vary from 20 seconds to two minutes or more depending on the number of interactions and actions, size of

three-dimensional virtual environment, and the kinds of actions and interactions done by the user as a 3D Password.

Therefore, a brute force attack on a 3D Password is very difficult and time-consuming.

2. Cost of attacks: In a three-dimensional virtual environment that contains biometrics recognition objects and token-based objects, the attacker has to forge all possible biometrics information and forge all the required tokens. The cost of forging such information is very high, making an attack of 3D Password more challenging. Moreover, the high number of possible 3D Password spaces (as shown in table 7.1) leaves the attacker with almost no chance of breaking the 3D Password.

Well-studied attack: the attacker tries to find the highest probable distribution of 3D Passwords. However, to launch such an attack the attacker has to acquire knowledge of the most probable 3D Password distributions. Acquiring such knowledge is very difficult because the attacker has to study all the existing authentication schemes that are used in the three-dimensional environment. Moreover, acquiring such knowledge may require forging all existing biometrical data and may require forging token-based data. Also, it requires a study of the user's selection of objects, or a combination of objects, that the user will use as a 3D Password.

A well-studied attack is very hard to accomplish since the attacker has to perform a customized attack for every different, three-dimensional virtual environment design. Every system can be protected by a 3D Password that is based on a unique three-dimensional virtual environment. This environment has a number of objects and types of object responses that differ from any other three-dimensional 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 biometrical data or textual passwords that cannot be seen from behind. The attacker may be required to take additional measures in

order to break the legitimate user's 3D Password. Therefore, we assume that the 3D 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 for the legitimate user to perform a correct login using 3D Password. This observation gives the attacker an indication of what the legitimate user's 3D Password length. However, this kind of attack cannot be launched alone since it gives the attacker mere hints. Therefore, it would probably be launched as part of well-studied attack or brute-force attack.

Timing attacks can be very effective if the three-dimensional virtual environment is poorly designed. For example figure 5.4 below illustrates a poor three-dimensional virtual environment design. A timing attack is very effective against such three-dimensional virtual environments. Notice the location of the start point and notice how long it takes to navigate and walk to computer B from the start point. The attacker simply observes how long it takes for a legitimate user to login. If the time is less than two minutes then the user likely interacted and typed into computer A. Therefore, the attacker eliminates the possibility of typing on computer B. However, if the time is more than two minutes then the user's 3D Password is a combination of typing on computer A and B or just typing on computer B.

In order to countermeasure the timing attack, the virtual environment's design should be done in such a manner that interactions and actions towards some 3D items do not give any clue to the user.

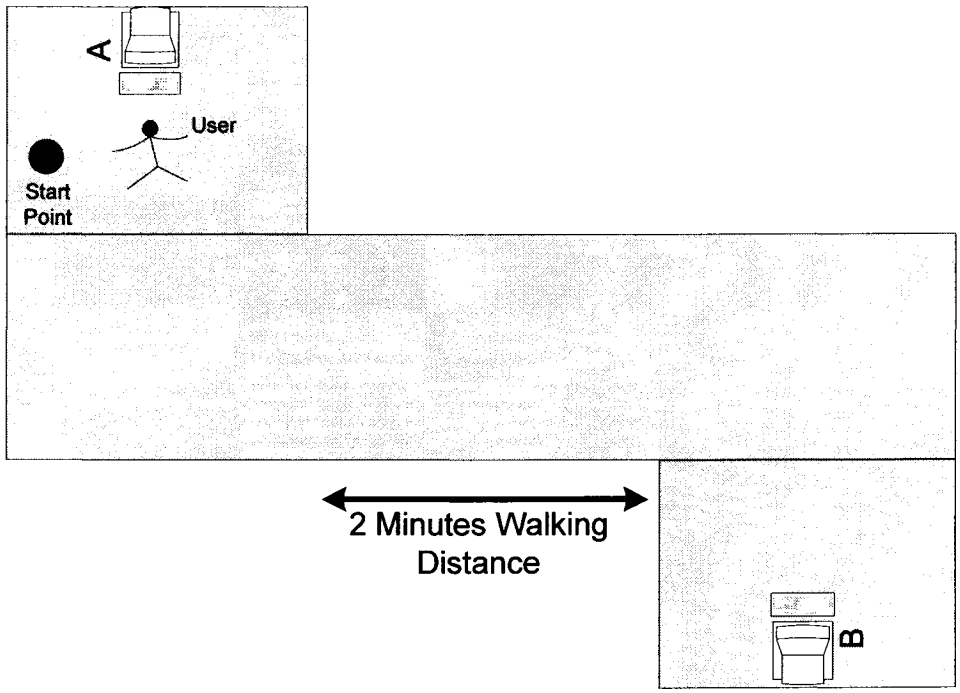

Figure 5.4: A poorly designed three-dimensional virtual environment, which is vulnerable to timing attack.

Table 5.1: Number of possible 3D Passwords of total length L_{max} in a three-dimensional virtual environment as specified in section 3.4

# of Actions, Interactions and Inputs (L_{max})	Log_2 (# of 3D passwords)	# of Actions, Interactions and Inputs (L_{max})	Log_2 (# of 3D passwords)
1	13	17	221
2	26	18	234
3	39	19	247
4	52	20	260
5	65	21	273
6	78	22	286
7	91	23	299
8	104	24	312
9	117	25	325
10	130	26	338
11	143	27	351
12	156	28	364
13	169	29	377
14	182	30	390
15	195	31	403
16	208	32	416

5.4 Three Dimensional Password Evaluation

Almost 30 users have tested our 3D Password. We endeavored to capture some statistical information based on the experimental three-dimensional virtual environment. There are two important issues that evaluate the performance of 3D Password. 1) The length of users' 3D Passwords. 2) The time needed to login. We will attempt to describe both points in more detail.

5.4.1 User's distribution of Three Dimensional Password length

This point is very important because it determines the user's behavior when selecting a 3D Password. We did not ask the users under study to create a 3D Password of a specific length. Every user created his 3D Password freely without any restrictions or hints. Figure 5.4 shows the users' distribution of their 3D Passwords. We observed that most users select 3D Passwords of length 5 to 6. This is an excellent result since as we have seen in figure 5.3, 3D

Password surpasses the full textual password space if 3D Password has a length of almost 4 (actions/interactions/inputs). Therefore, most of the users' 3D Passwords had password spaces greater than the full 8-characters textual password space. Moreover, we observed that only less than 4% of users have chosen a 3D password of length less than 2. This means almost 97% of users surpass the dictionary size that Klein [KLEIN 1990] used to crack almost 25% of users textual passwords. Therefore, the results shows that 3D Password have decreases the percentage (from 25% to 4%) of users passwords that have a password space equal to the dictionary size of Klein [KLEIN 1990].

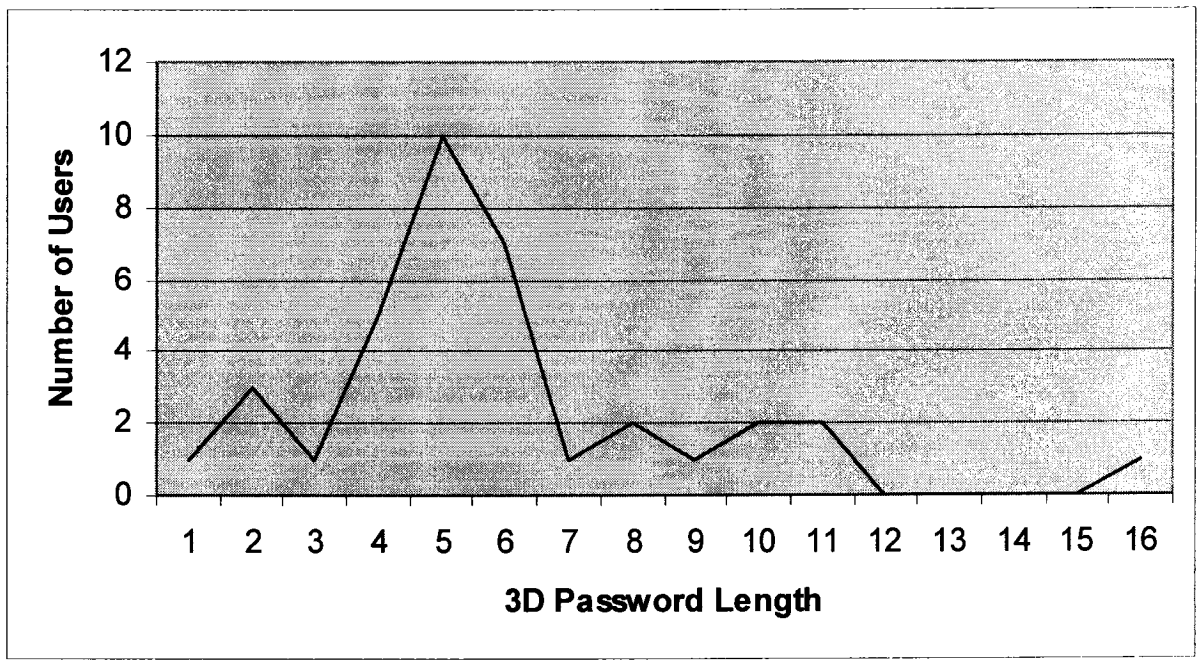

Figure 5.5: The distribution of user's 3D Password length. Length of 3D Password represents actions, interactions, and inputs toward 3D items and three-dimensional virtual environment.

5.4.2 Time required to perform 3D password

We observed the time required to login for first-attempt users and the second-attempt users. We noticed a decrease in the time required to perform 3D Password. This means users

become familiar with the system over time. Therefore, time required to login decreases over time as shown in figure 5.6 below

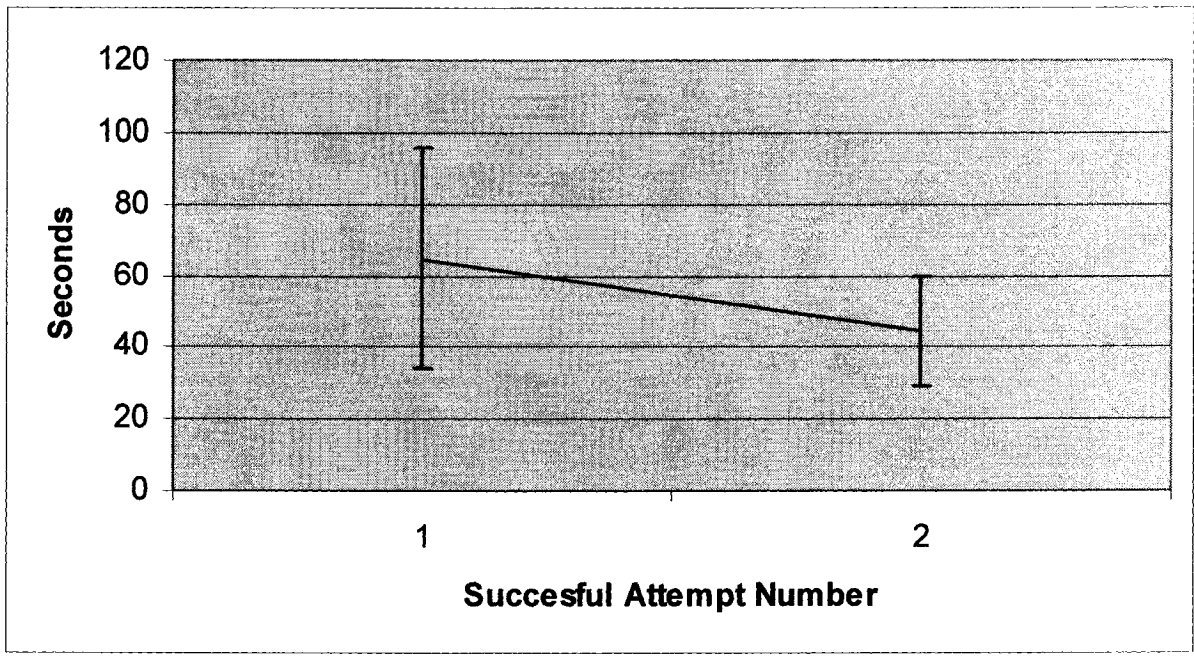

Figure 5.6: Users' average time required to login based on first and second attempt.

The relation of required time to login and the 3D Password's length is shown in figure 5.7. It is obvious that a large 3D Password requires more time to perform than a small 3D Password. However, length of time also depends on what kind of interactions and actions the user includes in the 3D Password. Performing textual password might require less time than performing a graphical password. Moreover, it depends on user's choice of 3D items as their 3D Password.

The time required to login is a very critical issue. Performing the authentication process is sometimes not feasible due to time constraints. However, the length of time required for performing authentication depends on what application we are applying our system and what resources will be protected.

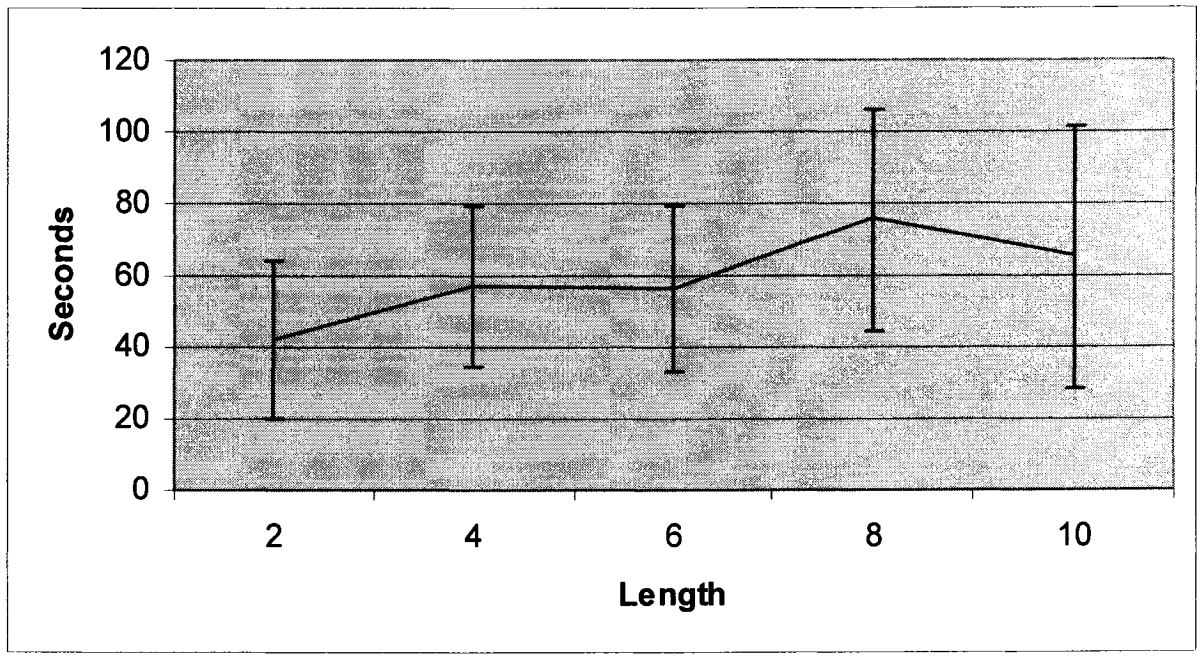

Figure 5.7: Average Time required to login based on user's 3D Password length.

5.6 User's Questionnaire feedbacks

We conducted a user study on 3D passwords using the experimental three-dimensional virtual environments. The study reviewed the usage of textual passwords and other authentication schemes. The users varied in age, sex and education level. Even though we believe it is a small set of users, the study produced some distinct results compared to previous studies [JERMYN et al. 1999] [ADAMS and SASSE 1999]. We have the following observations regarding textual passwords, 3D passwords and other authentication schemes:

- Most users who uses textual passwords of 9-12 character lengths or who use random characters as a password have only 1-3 unique passwords.

- More than 50% of user's textual passwords are 8 characters or less.

- Almost 25% of users use meaningful words as their textual passwords.

- Almost 75% of users use meaningful words or partially meaningful words as their textual passwords. In contrast, only 25% of users use random characters and letters as textual passwords.

- Over 40% of users have only 1-3 unique textual passwords and over 90% have 8 unique textual passwords or less.

- Over 90% of users do not change their textual passwords unless they are required to by system.

- Over 95% of users under study have never used any graphical password scheme as a means of authentication.

- Most users feel that 3D passwords are highly acceptable.

- Most users believe that there is no threat to personal privacy by using a 3D password as an authentication scheme.

5.7 Three Dimensional Password Features Evaluation

In order to complete the picture of evaluating 3D password, we tried to evaluate 3D password compared to other authentication schemes. We notice that 3D password combines recognition-based, knowledge-based, biometrics-based and token-based in one authentication scheme. Moreover, the user has the freedom to shape his/her 3D password to include any authentication schemes that he prefers and discard not preferable authentication schemes. Table 5.2 shows the comparison between different authentication schemes.

Users usually highly accept textual password, PassFaces, DAS and tokens because it does not affect their privacy. This observation can be seen by the common use of textual passwords

and tokens-based systems. However, users' acceptability decreases if the system affects users' privacy or health.

Fingerprints, face, hand geometry, and voice might change over the time due to several reasons. Therefore, we labeled their permanency as Low or Medium. Moreover, most biometrics cannot be revoked which can be considered a critical drawback of such systems.

We tried to mention the barriers of universality for every authentication scheme. Such barriers should be carefully considered before applying any authentication system.

Table 5.2: Comparison of several authentication schemes (assessments based on our perceptions).

	Acceptability	Distinctiveness	Permanence	Revoke	Barriers to Universality	Token based	Recognition based	Knowledge based	Bioemtrics based
Textual Password	High	Medium	high	√	None			√	
Pass Faces	High	Low	high	√	visual impairment		√		
DAS	High	Medium	high	√	visual impairment			√	
Fingerprints	Medium	high	medium		hand or finger impairment				√
Face	High	low	low		None				√
Hand Geometry	Medium	Medium	medium		hand impairment				√
Iris	Low	high	high		visual impairment				√
Retina	Low	high	high		visual impairment				√
Voice	High	medium	medium		speech impairment				√
3D Password	High	high	high	√	visual impairment	√	√	√	√
smart cards	high	high	high	√	Loss or theft	√		√	

Chapter 6

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. The motivation of this work is to propose a scheme that has a huge password space while also combining any existing or upcoming authentication schemes into one scheme.

3D Password gives the user the choice of modeling his/her 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 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 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 of the system using a large number of people is required. Moreover, we have to observe and study whether a legitimate user is apt to forget his/her 3D Password over a longer period of time.

We are interested in examining different three-dimensional virtual environments and their affects on users' behavior in selecting 3D Passwords and the affect on the resulting probable password space.

We are also interested in adding objects from different authentication schemes in the experimental three-dimensional environment. Objects can be fingerprints, iris recognition systems, token-based systems, etc. A study on the most popular objects for users will offer insight into the user's preferences when using such authentication scheme. It will show that if a specific authentication scheme is undesirable then it will not be part users 3D Password.

Acquiring the knowledge of the probable distribution of a user's 3D Password using different three-dimensional virtual environments that include different objects will show the practical strength of the 3D Password authentication scheme. It will demonstrate whether it is possible to build 3D Password dictionaries to launch a 3D Password dictionary attack.

Moreover, finding a practical solution for shoulder-surfing attacks on 3D Passwords and other authentication schemes requires additional research.

REFERENCES

ADAMS, A. AND SASSE, M. A 1999. Users are not the enemy: Why users compromise computer security mechanisms and how to take remedial measures. Communications of the ACM, vol.42, no.12, pp. 40-46. December 1999.

BLONDER Greg E. 1996. United State Patent 5559961, September 1996

BBC 2006. Fingerprints hide lifestyle clues.
http://news.bbc.co.uk/2/hi/technology/4857114.stm. April 2006.

CHOAS COMPUTER CLUB 2004. How to fake fingerprints? http://www.ccc.de/biometrie/fingerabdruck_kopieren.xml?language=en. October, 2004.

GILHOOLY, K. 2005. Biometrics: Getting Back to Business. In Computerworld. http://www.computerworld.com/securitytopics/security/story/0,10801,101557,00.html. May 2005.

DAUGMAN J.G. 1993. High Confidence Visual Recognition of Persons by a Test of Statistical Independence. IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 15, No. 11, pp. 1148-1161, November 1993.

DAVIS D., MONROSE F., AND REITER M. K. 2004. On user choice in Graphical Password Schemes. In Proceedings of the 13th USENIX Security Symposium, San Diego, August 2004.

DHAMIJA R., AND PERRIG A. 2000. Déjà Vu: A User Study Using Images for Authentication. 9th USINEX Security Symposium, Denver, Colorado, August 2000.

FELDMEIER D.C and KARN P.R. 1989. Unix Password Security - Ten years later. Proceedings of Crypto'89, published as Lecture Notes in Computer Science, Springer-Verlag, no.435, pp.44-63.

GLOSSARY OF EYE AND VISION TERMS 2005. http://www.eyeglossary.net . Site accessed December 2005.

HALDERMAN J.A. , WATERS B., AND FELTEN E.W 2005. A Convenient Method for Securely Managing Passwords. In Proceedings of the 14th International World Wide Web Conference (WWW 2005). Chiba, Japan, May 10-14, 2005.

HONG D., MAN S., HAWES B., AND MATHEWS M., A password scheme strongly resistant to spyware. Proceedings of 2004's international conference on security and management, pp. 94-100, Las Vergas NV, USA, June 2004.

JERMYN I., MAYER A., MONROSE F., REITER M. K., AND RUBIN A. 1999. The Design and Analysis of Graphical Passwords. Proceedings of the 8th USENIX Security Symposium, pp. 1-14, Washington, D.C., USA, August 23-26, 1999

JOGL API PROJECT 2005. https://jogl.dev.java.net , site accessed November 2005.

KAUFMAN, C., PERLMAN, R., AND SPECINER, M. 2002. Network Security: Private Communication in a Public World, Prentice Hall, Second Edition, p. 237.

KLEIN, D.V., 1990. Foiling the Cracker: A Survey of, and Improvement to Passwords Security. Proceedings of the USENIX Security Workshop, pp. 5-14, August 1990.

LIGHT WIEGHT JAVA GAME LIBERARY 2005. http://www.lwjgl.org . Site accessed November 2005.

MOORE, G. 2005. The History of Fingerprints, site accessed 8 May 2005, http://onin.com/fp/fphistory.html

MORRIS R. and THOMPSON K. 1979. Communications of the ACM. vol. 22, no. 11, pp. 594 - 597, November 1979.

MUFFETT A.D.C. 1992. "Crack Version 4.1". A Sensible Password Checker for Unix. July 1992.

OPENWALL PROJECT 2006. John the Ripper password cracker. http://www.openwall.com/john , site accessed February 2006.

ORTEGA-GARCIA J., GONZALEZ-RODRIQUEZ J., SIMON-ZORITA D., AND CRUZ-LIANAS S. 2002. From Biometrics technology to applications regarding face, voice, signature and fingerprint recognition. Chapter 12 in Biometrics Solutions for Authentication in an E-World, (D. Zhang, ed.), Kluwer Academic Publishers, vol. 697, pp. 289-337, July 2002.

R&T SYSTEMS 2005. http://www.rnts.co.kr/homepage/biometrics/readiris.asp, site accessed December 2005.

REAL USER CORPORATION 2005. The Science Behind Passfaces. http://www.realusers.com , site accessed October 2005.

RSA LABORATORIES 2005. http://www.rsasecurity.com/rsalabs/faq/B.html. Site accessed May 2005.

SOBRADO L., AND BIRGET J.C. 2005a. Shoulder-surfing resistant graphical passwords-draft.

SOBRADO L., AND BIRGET J.C. 2005b. Graphical password on interactive simulation. http://clam.rutgers.edu/~lsobrado/graphicalpassword. Site accessed October 2005.

SOBRADO L. AND BIRGET J.C. 2005c. Graphical Passwords. http://rutgersscholar.rutgers.edu/volume04/sobrbirg/sobrbirg.htm. Site accessed October 2005.

TAKADA T. AND KOIKE H. 2003. Awase-E: Image-based Authentication for Mobile Phones using User's Favorite Images, Proceedings on MobileHCI 2003. pp. 347-351, Udine, Italy, September 2003.

TAO H. 2005a. Patent application number CA2495445-A1. July 2005.

TAO H. 2005b. http://www.passgo.ca. Site accessed October 2005.

THORPE J., AND OORSCHOT V. 2004. Graphical Dictionaries and the Memorable Space of Graphical Passwords. USENIX Security 2004, San Diego, August 9-13, 2004

WIEDENBECK S., WATERS J., BIRGET J., BRODSKIY A., AND MEMON N. 2005 a. Authentication using graphical passwords: effects of tolerance and image choice. In the Proceedings of the 2005 symposium on Usable privacy and security, pp. 1 – 12, Pittsburgh, Pennsylvania, July 2005.

WIEDENBECK S., WATERS J., BIRGET J., BRODSKIY A., AND MEMON N. 2005 b. Authentication Using Graphical Passwords: Basic Results. In the Proceedings of Human-Computer Interaction International, Las Vegas, July 25-27, 2005.

WIEDENBECK S., WATERS J., BIRGET J., BRODSKIY A., AND MEMON N. 2005 c. PassPoints: Design and longitudinal evaluation of a graphical password system', International Journal of Human-Computer Studies (Special Issue on HCI Research in Privacy and Security), vol.63, no.1-2, pp.102-127, July 2005.

WOODWARD, J.D., ORLANS N.M., AND HIGGINS P. T. 2003. Biometrics: Identity Assurance in the Information Age. McGrawHill, 2003.

VOLKER R., RICHTER K., AND FREIDINGER 2004. A PIN entry method resilient against shoulder surfing. In Proceedings of the 11th ACM Conference on Computer and Communications Security, Washington, DC, USA. October 2004