Analysis Of Three-Dimensional Password Scheme

Chaitali A. Kurjekar, Shital D. Tatale, Sachin M. Inzalkar

Abstract— In this paper, We analyze and evaluate our contribution which is a new scheme of authentication. This scheme is depend on a virtual three-dimensional environment. Users negative through the virtual environment and interact with items inside the virtual three dimensional (3Dimentional) environment . The combination of all interactions, inputs and actions towards the items and the inputs action and interaction these are virtual three environment and it constructs the user's 3Dimentional password.and these 3Dimentional password combines most authentication schemes such as biometrics,textual passwords ,graphical passwords into one virtual three-dimensional environment. The important application of 3D password's is provide the protection of critical resources and systems.

Index Terms—:- Authentication Three Dimensional Virtual Environment, Biometrics Textual passwords ,Graphical passwords, Three dimensional passwords.

1 INTRODUCTION

Authentication is the process of Recgnization who you are to whom you claimed to be. In general,it Categorize in to four authentication techniques:

1. What you know (knowledge based)
2. What you have (token based).
3. What you are (biometrics).
4. What you recognize (recognition based).

Textual passwords are the authentication techniques used in the computer world. Textual password has two battle requirements: passwords should be very easy to remember and very hard to Recognized or guess. Klein [1] acquired a database of nearly 15,000 user accounts that had alpha numerical passwords, and stated that 25% of the passwords were guessed using a small, yet well formed dictionary of (3 × 106) words. Even though the full textual password for 8- character passwords consist of letters and numbers is almost (2 × 1014) passwords, using a very small subset of the full space, 25% of the passwords were guessed correctly. to this process user's are responsible in selecting their textual passwords & it is the fact that many users do not select random passwords.

Many graphical passwords have been show this paper. The strength of graphical passwords comes from the fact that users can recognize pictures more than words. Many graphical passwords are vulnerable for shoulder surfing attacks, where an attacker can observe the legitimate user's graphical password by camera. A study [5] concluded that the selection of faces in Pass Faces[4] can be affected by the gender attractiveness,and race of the selected face which results in an insecure scheme. Recently , many types of graphical passwords are under study yet, it might be some time before they can be applied in the real world. Token based systems such as ATMs are widely applied in banking systems and in laboratories entrances as a mean of authentication. However, tokens are vulnerable to theft. Moreover, the user has to carry the token whenever access required. Many biometric schemes have been show.Each biometric recognition scheme is different considering consistency, and acceptability uniqueness. Users tend to resist some biometrics recognition systems due to its intrusiveness to their privacy.The 3D password combine with all existing authentication schemes into one three-dimensional virtual environment. The three-dimensional virtual environment consists of many objects. Each item has different responses to actions. The user actions, interactions and i/ps towards the objects or towards the 3-dimensional virtual environment creates the user's 3D password.

The 3D password gives users the freedom of selectingwhat type of authentication techniques they want to beperformed as their 3D password. The 3D password has a very large number of passwords because of the high number of possible actions and interactions towards every object and towards the three dimensional virtual environment.

The remainder of this paper is organized as follows: Section II introduces the 3D password. Section III discusses about the security analysis. Section IV show the conclusions and future work.

2 3-D PASSWORD SCHEME

In this section,This paper shows a multifactor authentication scheme that combines the Advantages of different authentication schemes. attempted to satisfy the following requirements.

1) should not be either depend on recall or depend on recognition only. Instead, the scheme should be a combination of biometrics-, recognition-, recall-,and token-based authentication schemes.
2) Users ought to have the freedom to select whether the 3-D password will be solely recall-, biometrics-, recognition of two schemes or more. This freedom of selection is neces-

sary because users are different and they have different requirements. Some users do not like to provide biometrical data, and some users have not strong memories.Therefore,to ensure high user acceptability, and the user's freedom of selection is very important.

3) The new scheme should provide secrets that are not difficult to remember and very difficult to guess.
4) The new scheme should provide secrets not only difficult to write down on paper. But also difficult to share with others.
5) The new scheme should provide secrets that can be easily changed. Depend on the before describe requirements,This paper Anatyze contribution that is the 3-D password authentication scheme.

2.1 3-D Password Overview

The 3-D password is a multifactor authentication scheme. The 3-D password shows a 3-D virtual environment containing different virtual objects. The user navigates through this environment and also this user inteacts with the objects. The 3-D password is simply the combination and the sequence of user interactions and this interaction occure in the 3-D virtual environment. The 3-D password can combine token-, recognition-,and recall biometrics-based systems into one authentication. This can be done by designing a 3-D virtual environment that consist the objects that request information to be recall, information to be recognized, tokens to be presented, as wellas biometrical data to be verified. For example, the user can enter the virtual environment and type something on a computer that in (p1,q1,r1) position, then enter a room that has a fingerprint recognition device that exists in a position (p2, q2, r2) and provide his/her fingerprint. Then, the user can go to the open the car door, virtual garage,and turn on the radio to a specific channel. The combination and the sequence of the actions toward the specific objects construct the user's 3-D password.

Virtual objects can be any object that this paper encounter in real life. Any obvious actions and interactions toward the real-life objects can be done in the virtual 3-D environment toward the virtual objects.many times, any user input in the virtual 3-D environment can be considered as a part of the 3-D password. This paper have the following objects:

1) a computer with which the user can type;
2) who is the fingerprint reader that must to requires the user's fingerprint;
3) a biometrical recognition device is also important;
4) a white board that a user can write, sign, or on;
5) an automated teller machine (ATM) that requests a token;
6) a light that can be switched on/off;
7) a television channel or radio channels can be selected;
8) a stapler that can be punched;
9) a car that can be driven;
10) a book that can be from one place to another;
11) any graphical password scheme;
12) any real-life object;
13) any upcoming authentication scheme.

The action toward an object (assume a fingerprint recognition device) that exists in location (p1,q1, r1) is different from the actions toward a similar object (another fingerprint recognition device) that exists in location (p2, q2, r2), where $p1 \neq p2$, $q1 \neq$ q2, and $r1 \neq r2$. Therefore, to perform the legitimate 3-D password, the user must follow the same scenario performed by the legitimate user. That means interacting with the objects that reside at the exact locations and perform the exact actions in the proper sequence.

2.2 3-D Password Application

Because a 3-D password have a password space that is very large compared to other authentication the 3-D password's important application doains are protecting critical following.

1) *Critical servers:* Many large organizations have critical servers that are always protected by a textual password. A 3-D password authentication analyze a sound replacement for a textual password. Moreover, entrances to such places are usually protected by using access cards and sometime digit,PIN numbers. Therefore, a 3-D password can be used to protect such locations and protect the usage of such servers.

2) *military facilities and Nuclear:* This facilities should be protected by the most powerful authentication systems. The 3-D password has a very large password space, and so it can contain biometrics-, token-,Knowledge-based and recognition-, authentications in a single authentication system, it is a sound choice for high level security locations.

3) *Jetfighters and Airplans:* Because of the possible threat of misusing airplanes and jetfighters for religio-political agendas, usage of airplanes should be protected by a powerful authentication system. The 3-D password is recommended for these systems. In addition, 3-D passwords can be used for less critical systems because the 3-D virtual environment can be designed to any system's. A small 3-D virtual environment can be used in number of systems such as ATMs and also below given.

1) web authentication;
2) ATMs;
3) Personal digital assistant;
4) Desktop computer and laptop logins;

3 Security Analysis

This paper analyze and study how secure a system is, This paper have to consider how hard it is for the attacker to break such a system.

A possible mapped depend on the information content of a password space, which is defined in as "the entropy of the probability distribution over that space given by the relative

frequencies of the passwords that users choose." have seen that textual password space may be relatively large; however, an attacker only need a small subset of the full password space as Klein [1] observed to successfully break such an authentication system. As a paper result, it is important to have a scheme that has a very large possible password space as one factor for increasing the work required by the attacker to break the authentication system. Other factor is to find a scheme that has no previous or existing information or knowledge of the probable user password selection, which can also oppose the attack on such an authentication scheme.

scheme that has no previous or existing knowledge of the most probable user password selection, which can also resist the attack on such an authentication scheme.

3.1 3-D Password Space Size

One it is the most important factor to determine how difficult it is to launch an attack on an authentication system is the size of the password space. To determine the 3-D password space,to count all possible 3-D passwords that have a certain number of inputs ,interactions,and actions and all objects that exist in the 3-D virtual environment.This paper assume that the length of the 3-D password is *Le*max, and the probability of the 3-D password of size is greater than *Le*max is zero.(length indicated by Le)

To mapped the 3-D password space, This paper will calculate $\pi(Le\max, G)$ on a 3-D virtual environment that has the space ($G \times G \times G$) for a 3-D password of a length (number of actions, interactions, and inputs) of *Le*max or less. In the following expression, *AC* indicates the possible actions the 3-D

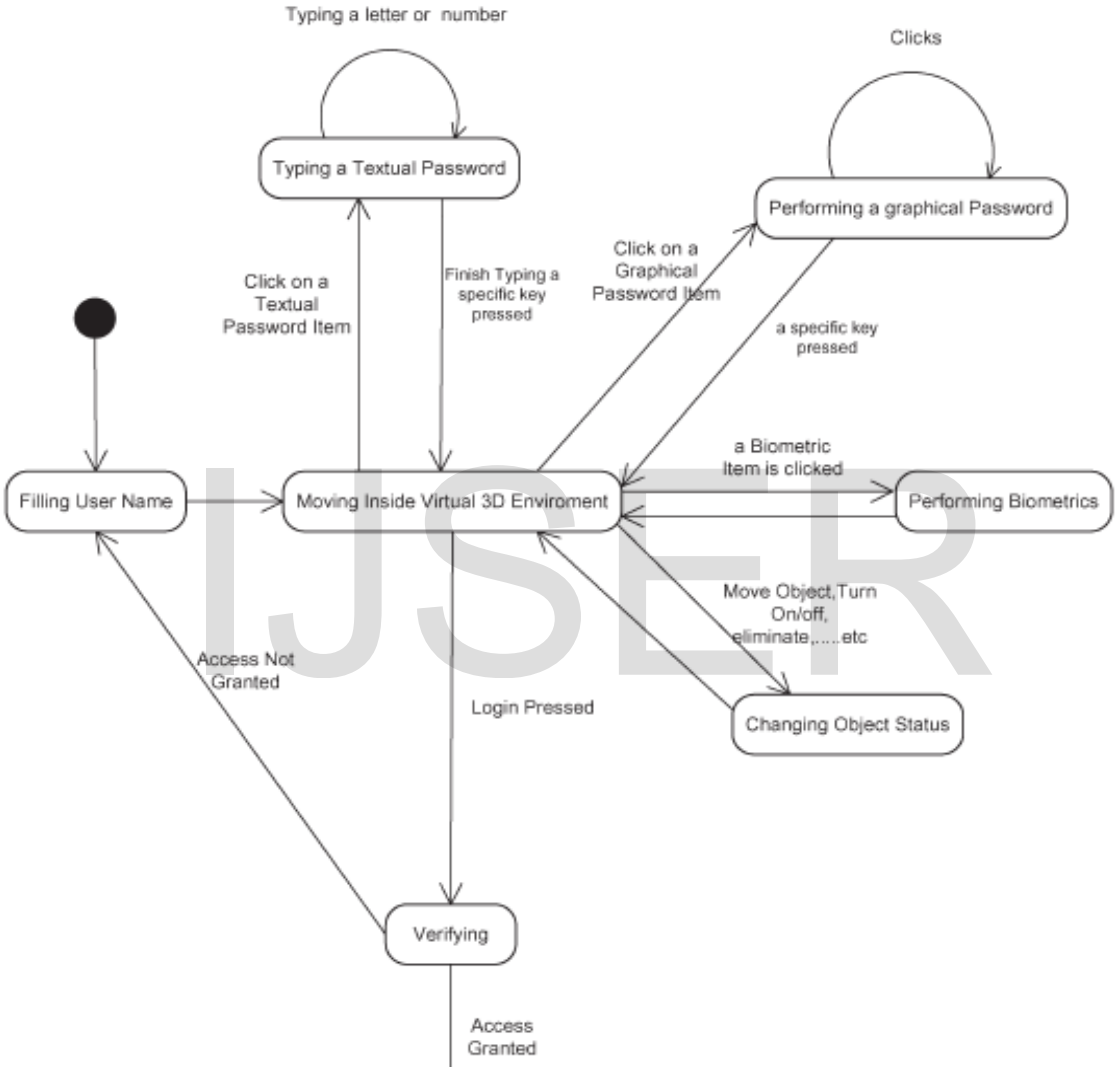


Fig. 1. State diagram of a possible 3-D password application.

virtual environment, whereas π indicate the total number of possible 3-D passwords of length *Le*max or less:

$$\pi(L_{max}, G) = \sum_{m=1}^{m=L_{max}} (m + g(AC)). \quad (1)$$

In the following expression (2), Omax is the number of objects in the 3-D virtual environment:

$$m = \sum_{i=1}^{i=O^{max}} h(O_i, T_i, x_i, y_i, z_i) \quad (2)$$

where xi = xj , yi = yj , and zi = zj , only if i = j. The design of the 3-D environment will determine the value of Omax. The variable m represents all possible actions and interactions toward all existing objects Oi.However, g(AC) counts the total number of actions and inputs toward the 3-D virtual environment, whereas m, as we mentioned before, counts the actions and interactions toward the objects. An example of g(AC) can be a user movement pattern, which can be considered as a part of the user's 3-D password. The function is the number of possible actions and interactions toward the object Oi based on the object type Ti.

$$h(O_i, T_i, x_i, y_i, z_i) = f(O_i, T_i, x_i, y_i, z_i) \quad (3)$$

is the number of possible actions and interactions toward the object *Oi* depend on the object type *Ti*. Object types can be textual password objects, DAS objects, or any authentication scheme. The function *f* is determined from the object type. It counts the possible actions and interactions that the object can accept. If assume that an object "Keyboard" is in location (*p*0, *q*0, *r*0) of type = textual password, *f* will count the possible all characters and numbers that can be typed, which is around 93 possibilities. Describe before, an object type is one of the important factors that affects the overall password space. Therefore, higher outputs of function *f* mean larger 3-D password space size.

From the previous equations, observe that the number of objects and the type of actions and interactions determines the probable password space. Therefore, the design of the 3-D virtual environment is a very critical part of the 3-D password system. $\pi(Le_{max}, G) = \sum_{m=1}^{m=Le_{max}} (m + g(AC))$. (1)

In the following expression (2), *O*max := OMAX is the number of
objects in the 3-D virtual environment:

$$m = \sum_{i=1}^{i=O^{max}} h(O_i, T_i, p_i q_i, r_i) \quad (2)$$

where *pi* = *pj* , *qi* = *qj* , and *ri* =r*j* , only if *i* = *j*. The design of the 3-D environment will determine the value of *O*max. The variable *m* indicates all possible actions and interactions toward

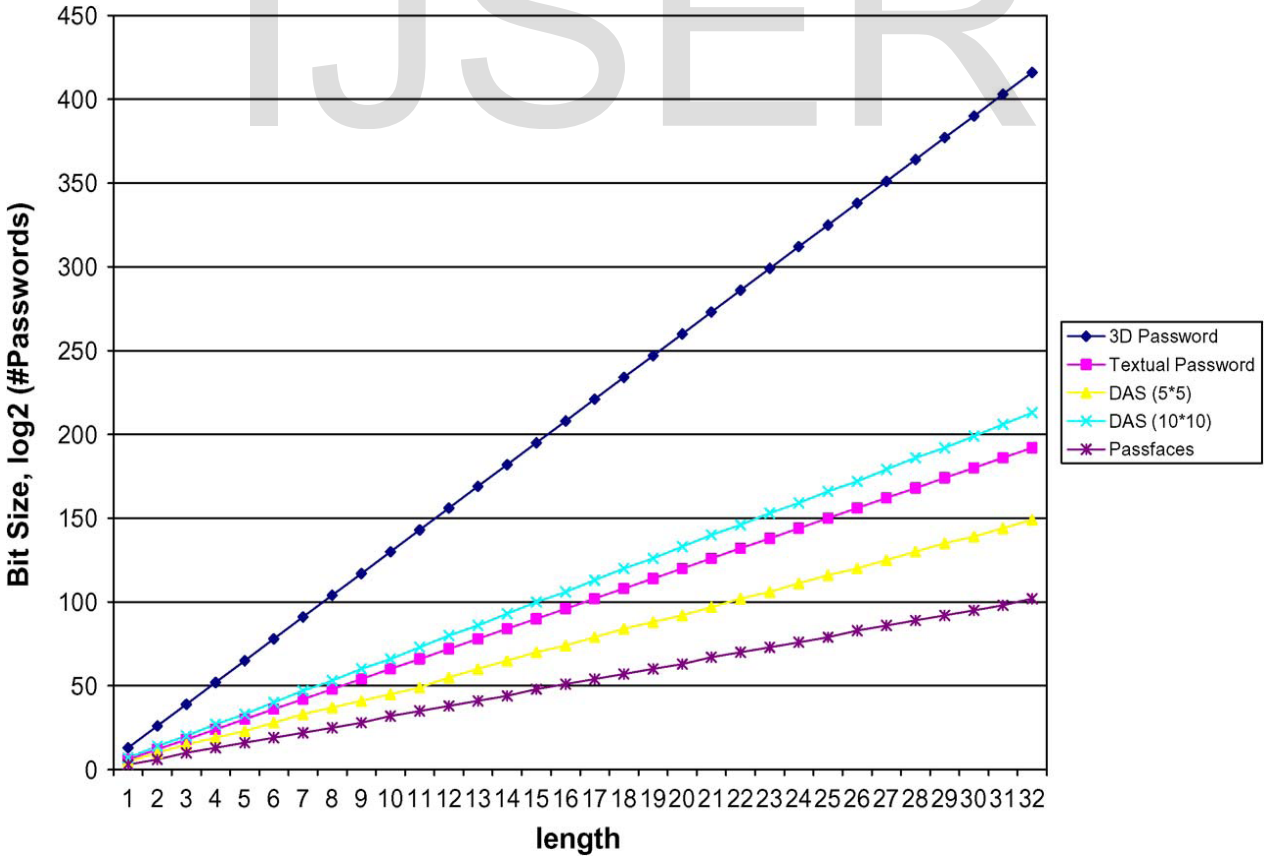
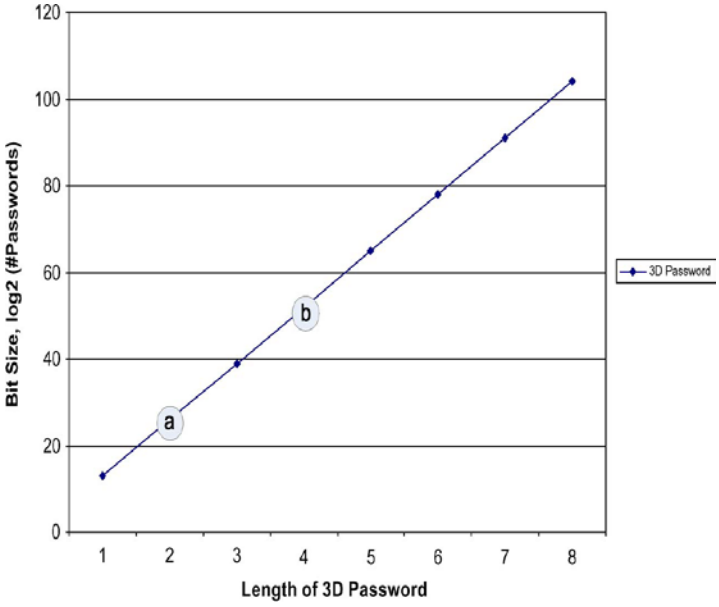


Fig. 2. Password space of the 3-D password, textual password, Passfaces, and DAS with grid sizes of 5 * 5 and 10 * 10. Length is the number of actions and interactions for a 3-D password, the number of charcters for textual passwords, the number of selections for passfaces, and the number of points that represent the strokes for DAS. The length is up to eight (Characters/actions, interactions, input/selections). The 3-D password vitual environment is as specified in Section V-A; bit size is the log2 of the entire probable password space.

all existing objects *Oi*.and *g*(*AC*) counts the all number of actions and inputs toward the 3-D virtual environment, whereas *m*, as show before, counts the interactions and actions toward the objects. An example of *g*(*AC*) can be a user movement pattern, which is the a part of the user's 3-D password. And The function of this as follows.

$$h(Oi, Ti, pi, qi, ri) = f(Oi, Ti, pi, qi, ri) \quad (3)$$

is the number of possible actions and interactions toward the object *Oi* depend on the object type *Ti*. Object types can be textual password objects, DAS objects, or any authentication scheme. The function *f* is determined from the object type. It counts the possible actions and interactions that the object can accept. If assume that an object "Keyboard" is in location (*p*0, *q*0, *r*0) of type = textual password, *f* will count the possible all characters and numbers that can be typed, which is around 93 possibilities. Describe before, an object type is one of the important factors that affects the overall password space. Therefore, higher outputs of function *f* mean larger 3-D password space size. From the previous equations, observe that the number of objects and the type of actions and interactions determines the probable password space. Therefore, the design of the 3-D virtual environment is a very critical part of the 3-D password system. Figs. 4 and 5 illustrate the resulting password space of the proposed 3-D password compared to Passfaces, textual password, and DAS of a grid of 5 × 5 and 10 × 10, respectively. Notice the difference between a 3-D password built on a simple 3-D virtual environment compared to the other authentication schemes.



character textual passwords. Point "b" represents the full password space of eight-character textual passwords.

3.2 3-D Password Distribution Knowledge

Having knowledge about the most probable textual passwords is the key behind dictionary attacks. Any authentications effect on the knowledge distribution of the user's secrets Knowledge about the user's selection of three-dimensional passwords and three dimensional password is not available, till up to now, to the attacker. Moreover, having various kinds of authentication schemes in one virtual environment causes this task is more difficult for the attacker to attack on it . However, in order to acquire such information,knowledge, the attacker must have knowledge and total information about every single authentication scheme and what are the most probable passwords using this specific authentication scheme. This knowledge, for example, should cover the user's most probable selection of textual passwords, various kinds of graphical passwords, and knowledge about the user's biometrical data. Most of the time knowledge about the design of a three-dimensional virtual environment is required in order for the attacker to launch attack.

3.3 Experimental Virtual 3-D

Environment This paper have built a small experimental three-dimensional virtual environment. The 3-dimensional virtual environment is simply an art gallery that the user can walk into. It consists of the following virtual objects:

1. 6 computers that take accept textual passwords
2. 36 pictures where user can click on anywhere in that picture, and this is the part 3D password

The pictures as well as computers are scattered in the three-dimensional virtual environment.

4 Conclusion Future Work

Textual passwords and token-based passwords are the most commonly used authentication schemes. However, many different schemes and it has been used in specific fields. Other schemes are under study yet have never been applied in the real world. The motivation of this work is to have a scheme that has a wide range of password space while also used a combination of any existing alphabate or number, or upcoming, authentication schemes into one scheme.

A 3D password choice to the user to choose of modeling his 3D password to contain any authentication scheme that the user prefers. Users do not have to provide their fingerprints if they do not wish to. and also 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, and this virtual environment is designed by the system administrator. The three-dimensional virtual environment can contain any objects that the administrator person feels that the users are familiar with. For example, football players can use a three -dimensional virtual environment of a stadium where they can

navigate and interact with objects that they are familiar with.A study on a large number of people is required. and looking at designing different three-dimensional virtual environments that contain objects of all possible authentication schemes. The important application domains of 3D Password are critical systems and resources. Critical systems such as military facilities, Airplans. critical servers and highly classified areas can be protected by 3D Password system with large three-dimensional virtual environment. a small three-dimensional virtual environment can be used to protect less critical systems like handhelds, ATM's and operating system's logins.

ACKNOWLEDGMENT

The authors express their gratitude to Prof.S.M. Inzalkar Department of Computer Science and Engineering, Jawaharlal Darda Engineering and Technology,(JDIET) Yavatmal (Maharashtra, India), for his valuable suggestions in the organization and development of this paper. The authors also acknowledge the management of JDIET, for their constant encouragement in completing this work.

REFERENCES

[1] DANIEL V.KLEIN. FOILING THE CRACKER: A SURVEY OF, AND IMPROVEMENT TO PASSWORDS SECURITY. PROCEEDINGS OF THE USENIX SECURITY PURPOSE WORKSHOP, 1990

[2] GREG E. BLONDER, GRAPHICAL PW, UNITED STATE PATENT 5559961, SEPTEMBER 1996.

[3] RACHNA DHAMIJA, ADRIAN PERRIG, DÉJÀ VU: A USER STUDY USING IMAGES FOR AUTHENTICATION. IN THE 9TH USINEX SECURITY SYMPOSIUM, AUGUST 2000, DENVER, COLORADO, PAGES 45-58.

[4] REAL USER CORPORATION. THE SCIENCE BEHIND PASSFACES.HTTP://WWW.REALUSERS.COM ACCESSED OCTOBER 2005.

[5] DARREN DAVIS, FABIAN MONROSE, AND MICHAEL K. REITER. ON USER CHOICE IN GRAPHICAL PASSWORD SCHEMES. IN PROCEEDINGS OF THE 13TH USENIX SECURITY SYMPOSIUM, SAN DIEGO, AUGUST, 2004.

[6] SUSAN WIEDENBECK, JIM WATERS, JEAN-CAMILLE BIRGET, ALEX BRODSKIY, NASIR MEMON. AUTHENTICATION USING GRAPHICAL PASSWORDS: EFFECTS OF TOLERANCE AND IMAGE CHOICE. IN THE PROCEEDINGS OF THE 2005 SYMPOSIUM ON USABLE PRIVACY AND SECURITY, PITTSBURGH, PENNSYLVANIA, JULY 2005,PAGES: 1 – 12

[7] SUSAN WIEDENBECK, JIM WATERS, JEAN-CAMILLE BIRGET, ALEX BRODSKIY, NASIR MEMON.USING GRAPHICAL PASSWORDS: BASIC RESULTS. IN THE PROCEEDINGS OF HUMAN-COMPUTER INTERACTION INTERNATIONAL, LAS VEGAS, JULY 25-27, 2005.

[8] SUSAN WIEDENBECK, JIM WATERS, JEAN-CAMILLE BIRGET, ALEX BRODSKIY, NASIR. MEMON. 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), 63 (2005) 102-127.

[9] IAN JERMYN, ALAIN MAYER, FABIAN MONROSE, MICHAEL K. REITER, AND AVIEL D. RUBIN. THE DESIGN AND ANALYSIS OF GRAPHICAL PASSWORDS, IN PROCEEDINGS OF THE 8TH USENIX SECURITY SYMPOSIUM, AUGUST, WASHINGTON DC, 1999.

[10] J. THORPE, P.C. VAN OORSCHOT. GRAPHICAL DICTIONARIES AND THE MEMORABLE SPACE OF GRAPHICAL PASSWORDS. USENIX SECURITY 2004, SAN DIEGO, AUGUST 9-13, 2004.

[11] 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, 42(12D):40-46.