A 3D Graphical Based Password Security

Dr. K.Kiran Kumar
Department of IT
Bapatla Engineering College
Bapatla, India

T.N.V.Pandu Ranga Rao
Department of IT
Bapatla Engineering College
Bapatla, India

T.Chittaranjan
Department of IT
Bapatla Engineering College
Bapatla, India

***ABSTRACT*—In this paper, we propose and evaluate a scheme which is based on a virtual three-dimensional environment. Passwords provide security mechanism for authentication and protection services against unwanted access to resources. A graphical based password is one promising alternatives of textual passwords. According to human psychology, humans are able to remember pictures easily. In this paper, we have proposed a new hybrid graphical password based system, which is a combination of recognition and recall based techniques that offers many advantages over the existing systems and may be more convenient for the user. Our scheme is resistant to shoulder surfing attack and many other attacks on graphical passwords. This scheme is proposed for smart mobile devices (like smart phones i.e. ipod, iphone, PDAs etc).**

Keywords – Three dimensional passwords; Textual passwords, Graphical passwords; authentication; biometric;, Three Dimensional Virtual Environment.

I. INTRODUCTION

Authentication is the process of validating who you are to whom you claimed to be. In general, there are four human 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 most common authentication techniques used in the computer world. Textual password has two conflicting requirements: passwords should be easy to remember and hard to guess. Klein acquired a database of nearly 15,000 user accounts that had alphanumerical passwords, and stated that 25% of the passwords were guessed using a small, yet well-formed dictionary of (3×10^6) words. 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 guessed correctly. This fact is due to the user's carelessness in selecting their textual passwords and to the fact that most users do not select random passwords[2].

Many graphical passwords schemes have been proposed. The strength of graphical passwords comes from the fact that users can recall and recognize pictures more than words. Most graphical passwords are vulnerable for shoulder surfing attacks, where an attacker can observe or record the legitimate user's graphical password by camera. A study concluded that the selection of faces in Pass Faces can be affected by the attractiveness, gender and race of the selected face which results in an insecure scheme. Currently, 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 loss or theft. Moreover, the user has to carry the token whenever access required. Many biometric schemes have been proposed. Each biometric recognition scheme is different considering consistency, uniqueness, and acceptability. Users tend to resist some biometrics recognition systems due to its intrusiveness to their privacy.

The 3D password combines all existing authentication schemes into one three-dimensional virtual environment. The three-dimensional virtual environment consists of many items or objects. Each item has different responses to actions. The user actions, interactions and inputs towards the objects or towards the three-dimensional virtual environment creates the user's 3D password. The 3D password gives users the freedom of selecting what type of authentication techniques they want to be performed as their 3D password. The 3D password has a large number of possible 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 Scheme. Section III discusses the security analysis. Section IV specifies Classification of Graphical Password Based Systems. Section V discusses the advantages. Section VI discuses the disadvantages. Section VII discusses conclusion and future work.

II. 3D PASSWORD SCHEME

In this section we present a new scheme that addresses the shortcomings of the existing authentication schemes.

A. 3D Password Overview

The three dimensional password (3D password) is a new authentication[6] methodology that combines recognition, recall, what you have (tokens), and what you are (biometrics) in one authentication system. The idea is simply outlined as follows. The user navigates through a three dimensional virtual environment. The combination and the sequence of the user's actions and interactions towards the objects in the three dimensional virtual environment constructs the user's 3D password. Therefore, the user can walk in the virtual environment and type something on a computer that exist in (x1, y1, z1) position, then walk into a room that has a white board that exist in a position (x2, y2, z2) and draw something on the white board. The combination and the sequence of the previous two actions towards the specific objects construct the user's 3D password. Users can navigate through a three- dimensional virtual environment that can contain any virtual object. Virtual objects can be of any type. We will list some possible objects to clarify the idea.

1. An object can be:
2. A machine that the user can type
3. A white paper that a user can draw on
4. An machine that requires a smart card
5. A Sensor
6. Any biometric device
7. Any Graphical password scheme
8. Any Virtual object
9. Any upcoming authentication scheme

Moreover, in the virtual three-dimensional environment we can have two different computers in two different locations[13]. Actions and interactions with the first computer is totally different than actions towards the second computer since each computer has a (x,y,z) position in the three-dimensional virtual environment. Each object in the virtual three-dimensional environment has its own (x,y,z) coordinates, speed, weight and responses toward actions.

B. 3D Password Selection and Inputs

Consider a three dimensional virtual environment space that is of the size G×G×G. Each point in the three dimensional environment space represented by the coordinates (x, y, z) [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[9][7] and can see the objects and interact with the objects. The input device for interactions with objects can be a mouse, a keyboard, styles, a card reader, a microphone …etc.

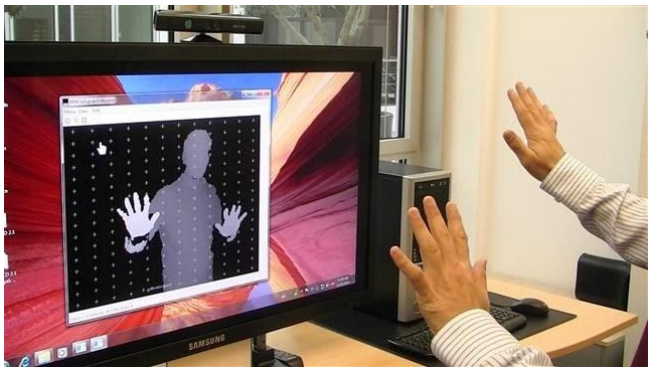
User actions, interactions and inputs towards the objects and towards the three-dimensional virtual environment are mapped into a sequence of three-dimensional coordinates and actions, interactions and inputs. For example, consider a user navigates through the three-dimensional virtual environment and types "10" into a computer that exists in the position of (13, 2, 30). The user then walks over and turns off the light located in (20, 6,12), and then goes to a white board located in (55,3,30) and draws just one dot in the (x,y) coordinate of the white board at the specific point of (530,250)[12]. The user then presses the login button. The representation of user actions, interactions and inputs towards the objects and the three-dimensional virtual environments can be represented as the following:

(13,2,30) Action = Typing, "1",

(13,2,30) Action = Typing , "0",

(20,6,12) Action = Turning the Light, Off, (55,3,30) Action = drawing , point = (530,250)

Two 3D passwords are equal to each other when the sequence of actions towards every specific object are equal and the actions themselves are equal towards the objects. 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[5]. The selection of what objects to use, locations, and types of responses are very critical tasks. The design affects the strength, usability and performance of the 3D password. Figure shows an experimental three-dimensional environment.



III. SECURITY ANALYSIS

The information content of a password space defined in [9] 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 hard the attack is. However, trying to have a scheme that has very large possible passwords is

one of the important parts in resisting the attack on such a scheme. We will analyze 3D passwords by discovering how large the 3D password space is. Then we will analyze the knowledge distribution of the 3D password.

A. The Size of the 3D Password Space

First of all, by computing the size of the 3D Password space we count all possible 3D Passwords that have a certain number of (actions, interaction, and inputs) towards all objects that exist in the three-dimensional virtual environment. We assume that the probability of a 3D Password of a size greater than Lmax is zero[4].

We will compute – (Lmax , G)on a three-dimensional space (G × G × G) for a 3D Password of a length (number of actions interactions and inputs) of Lmax or less. AC represents possible actions towards the objects. The symbol – is defined as the total number of possible 3D Passwords that have a total number of actions, interactions, and inputs equal to Lmax or less which is equal to:

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

Omax represent the total number of existing objects in the three-dimensional virtual environment. The number Omax 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 .

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

where xi=xj , yi=yj, and zi=zj only if i=j (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[8] 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 consideredas a part of user's 3D Password.

The function h(Oi,Ti, xi , yi , zi) 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[9] graphical passwords objects, fingerprint objects, etc.

h(Oi,Ti, xi , yi , zi) =f (Oi,Ti, xi , yi , zi) (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=S0, y= S1, z= S2 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 [10] (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[7][9], the 3D password space increases exponentially. The design of the three- dimensional virtual environments is the key for the 3D password space.

B. 3D Password Distribution Knowledge

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

IV. CLASSIFICATION OF GRAPHICAL PASSWORD BASED SYSTEMS

Graphical based passwords schemes can be broadly classified into four main categories: First is Recognition based Systems which are also known as Cognometric Systems or Search metric Systems[14]. Recognition based techniques involve identifying whether one has seen an image before. The user must only be able to recognize previously seen images, not generate them unaided from memory. Second is Pure Recall based systems which are also known as Drawn metric Systems. In pure recall-based methods the user has to reproduce something that he or she created or selected earlier during the registration stage. Third is Cued Recall[1] based systems which are also called Iconmetric Systems. In cued recall-based methods, a user is provided with a hint so that he or she can recall his his/her password. Fourth is

Hybrid systems[4] which are typically the combination of two or more schemes. Like recognition and recall based or textual with graphical password schemes.

V. ADVANTAGES OF 3-D PASSWORD

1. The new scheme provide secrets that are easy to remember and very difficult for intruders to guess. [3][5]
2. The new scheme provides secrets that are not easy to write down on paper. Moreover, the scheme secrets should be difficult to share with others.[6]
3. The new scheme provides secrets that can be easily revoked or changed

VI. DISADVANTAGES OF 3-D PASSWORD

1. As compare to traditional password approach this approach will definitely take more time to do user authentication [8].
2. More storage space required because it needs to save images which is large binary objects [10].
3. More costly due to required devices like web cam, finger print device etc. [3][5]
4. More complex than previous authentication schemes.

VII. CONCLUSION

The core element of computational trust is identity. Currently many authentication methods and techniques are available but each with its own advantages and shortcomings. There is a growing interest in using pictures as passwords rather than text passwords but very little research has been done on graphical based passwords so far. In view of the above, we have proposed authentication system which is based on graphical password schemes. Although our system aims to reduce the problems with existing graphical based password schemes but it has also some limitations and issues like all the other graphical based password techniques. Moreover, a small three- dimensional virtual environment can be used to protect less critical systems such as handhelds, ATM's and operating system's logins. Acquiring the knowledge of the probable distribution of a user's 3D password might show the practical strength of a 3D password. Moreover, finding a solution for shoulder surfing attacks on 3D passwords and other authentication schemes is also a field of study.To conclude, we need our authentication systems to be more secure, reliable and robust as there is always a place for improvement. Currently we are working on the System Implementation and Evaluation. In future some other important things regarding the performance of our system will be investigated like User Adoptability and Usability and Security of our system.

REFERENCES

[1] Daniel V.Klein. Foiling the Cracker: A Survey of, and Improvement to Passwords Security. Proceedings of the USENIX Security Workshop, 1990

[2] Greg E. Blonder, Graphical Password, 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. Authentication 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(12):40-46.

[12] Tejal Kognule and Yugandhara Thumbre and Snehal Kognule, ―3D password‖, International Journal of Computer Applications (IJCA), 2012.

[13] A.B.Gadicha , V.B.Gadicha , ―Virtual Realization using 3D Password‖, in International Journal of Electronics and Computer Science Engineering, ISSN 2277-1956/V1N2-216-222.

[14] Fawaz A. Alsulaiman and Abdulmotaleb El Saddik, "A Novel 3D Graphical Password Schema‖, IEEE International Conference on Virtual Environments, Human-Computer Interfaces, and Measurement Systems, July 2006.

[15] Duhan Pooja, Gupta Shilpi , Sangwan Sujata, & Gulati Vinita, ―SECURED AUTHENTICATION: 3D PASSWORD‖, I.J.E.M.S., VOL.3(2),242 – 245, 2012.

[16] Grover Aman, Narang Winnie, ―4-D Password: Strengthening the Authentication Scene‖, International Journal of Scientific & Engineering Research, Volume 3, Issue 10, October-2012