iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** IV **Month of publication:** April 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

3D Graphical Password Authentication System

Mr. Rakesh Prakash Kumawat[1], Mr. SachinSampat Bhosale[2], Mr. PrashantPrabhakar Ratnaparkhi[3]
[1,2,3]*P.Dr.V.V.Patil Inst.of technology &Engg.(Polytechnic),Loni*

Abstract: ***Current authentication systems suffer from many weaknesses. Textual passwords are commonly used; however, users do not follow their requirements. Users tend to choose meaningful words from dictionaries, which make textual passwords easy to break and vulnerable to dictionary or brute force attacks. Many available graphical passwords have a password space that is less than or equal to the textual password space. Smart cards or tokens can be stolen. Many biometric authentications have been proposed; however, users tend to resist using biometrics because of their intrusiveness and the effect on their privacy. Moreover, biometrics cannot be revoked. In this paper, we present and evaluate our contribution, i.e., the 3-D password. The 3-D password is a multifactor authentication scheme. To be authenticated, we present a 3-D virtual environment where the user navigates and interacts with various objects. The sequence of actions and interactions toward the objects inside the 3-D environment constructs the user's 3-D password. The 3-D password can combine most existing authentication schemes such as textual passwords, graphical passwords, and various types of biometrics into a 3-D virtual environment. The design of the 3-D virtual environment and the type of objects selected determine the 3-D password key space.***
Keywords: Graphical passwords, PCCP, authentication, Security

I. INTRODUCTION

Today computer has become a integral part of our day today life. The computer applications from all sorts of areas from business to banking and many more. The applications hold data and details of all the transaction a organization does. So to protect the applications authentication techniques like textual passwords with various strengths are used which help to protect a application. The vulnerabilities of textual password to method like eves dropping, dictionary attack, social engineering and shoulder surfing are well known. Random and lengthy passwords can make the system secure. But the main problem is the difficulty of remembering those passwords. Studies have shown that users tend to pick short passwords or passwords that are easy to remember. Unfortunately, these passwords can be easily guessed or cracked. Biometric based authentication and Knowledge based authentication. Most of the web application provides knowledge based authentication which include alphanumeric password as well as graphical password. In today's changing world when we are having number of networks and personal account some sort of easy authentication schema need to be provided. This paper provide textual password related to graphical image and provide four cued point on 3D graphical image

II. LITERATURE SURVEY

Graphical password is an alternative solution to secure system rather than text based password. Reason behind is graphical pictures are more easily recalled than text. Graphical password schemes can be grouped into three general categories: recognition based, pure recall based, and cued recall based techniques

A. Click-based graphical passwords

Graphical password systems are a type of knowledge-based authentication that attempt to leverage the human memory for visual information. A comprehensive review of graphical passwords is available elsewhere. Of interest herein are cued-recall click-based graphical passwords (also known as loci metric). In such systems, users identify and target previously selected locations within one or more images. The images act as memory cues to aid recall. Example systems include PassPoints and Cued Click Points . In PassPoints, passwords consist of a sequence of four click-points on a given image. Users may select any pixels in the image as click-points for their password. To log in, they repeat the sequence of clicks in the correct order, within a system-defined tolerance square of the original click-points. Although PassPoints is relatively usable security weaknesses make passwords easier for attackers to predict

Password with different click-points results in a different image sequence. The claimed advantages are that password entry becomes a true cued-recall scenario, wherein each image triggers the memory of a corresponding clickpoint. Remembering the order of the

click-points is no longer a requirement on users, as the system presents the images one at a time. CCP also provides implicit feedback claimed to be useful only to legitimate users. When logging on, seeing an image they do not recognize alerts users that their previous click-point was incorrect and users may restart password entry. Explicit indication of authentication failure is only provided after the final click-point, to protect against incremental guessing attacks. User testing and analysis showed no evidence of patterns in CCP , so pattern-based attacks seem ineffective. Although attackers must perform proportionally more work to exploit hotspots, results showed that hotspots remained a problem.

B. Human Authentication Technique

1) *Textual passwords:* Recall-based techniques require the user to repeat or reproduce a secret that the user created before. Recognition based techniques require the user to identify and recognize the secret, or part of it, that the user selected before. One of the most common recall-based authentication schemes used in the computer world is textual passwords. One major drawback of the textual password is its two conflicting requirements: the selection of passwords that are easy to remember and, at the same time, are hard to guess Klein collected the passwords of nearly 15 000 accounts that had alphanumerical passwords, and he reached the following observation: 25% of the passwords were guessed by using a small yet well-formed dictionary of 3 X 106 words. Furthermore, 21% of the passwords were guessed in the first week and 368 passwords were guessed within the first 15 min. Klein stated that by looking at these results in a system with about 50 accounts, the first account can be guessed in 2 min and 5–15 accounts can be guessed in the first day. Klein showed that even though the full textual password space for eight-character passwords consisting of letters and numbers is almost 2 X 1014 possible passwords, it is easy to crack 25% of the passwords by using only a small subset of the full password space. It is important to note that Klein's experiment was in 1990 when the processing capabilities, memory, networking, and other resources were very limited compared to today's technology
2) *Graphical passwords:* Various graphical password schemes have been proposed. Graphical passwords are based on the idea that users can recall and recognize pictures better than words. However, some of the graphical password schemes require a long time to be performed. Moreover, most of the graphical passwords can be easily observed or recorded while the legitimate user is performing the graphical password; thus, it is vulnerable to shoulder surfing attacks. Currently, most graphical passwords are still in their research phase and require more enhancements and usability studies to deploy them in the market
3) *Biometrics:* Many biometric schemes have been proposed; fingerprints, palm prints, hand geometry, face recognition, voice recognition, iris recognition, and retina recognition are all different biometric schemes. Each biometric recognition scheme has its advantages and disadvantages based on several factors such as consistency, uniqueness, and acceptability. One of the main drawbacks of applying biometrics is its intrusiveness upon a user's personal characteristic. Moreover, retina biometrical recognition schemes require the user to willingly subject their eyes to a low-intensity infrared light. In addition, most biometric systems require a special scanning device to authenticate users, which is not applicable for remote and Internet users
4) *3DPasswords:* The 3-D password is a multifactor authentication scheme. It can combine all existing authentication schemes into a single 3-D virtual environment. This 3-D virtual environment contains several objects or items with which the user can interact. The type of interaction varies from one item to another. The 3-D password is constructed by observing the actions and interactions of the user and by observing the sequences of such actions. It is the user's choice to select which type of authentication techniques will be part of their 3-D password. This is achieved through interacting only with the objects that acquire information that the user is comfortable in providing and ignoring the objects that request information that the user prefers not to provide. For example, if an item requests an iris scan and the user is not comfortable in providing such information, the user simply avoids interacting with that item. Moreover, giving the user the freedom of choice as to what type of authentication schemes will be part of their 3-D password and given the large number of objects and items in the environment, the number of possible 3-D passwords will increase. Thus, it becomes much more difficult for the attacker to guess the user's 3-D password

a) *3D Password Scheme:* In this section, we present a multifactor authentication scheme that combines the benefits of various authentication schemes. We attempted to satisfy the following requirements. The new scheme should not be either recall based or Recognition based only. Instead, the scheme should be a combination of recall- recognition-, biometrics-, and Token-based authentication schemes. Users ought to have the freedom to select whether the 3-D password will be solely recall-, biometrics-, recognition-, or token-based, or a combination of two schemes or more. This freedom of selection is necessary because users

are different and they have different requirements. Some users do not like to carry cards. Some users do not like to provide biometrical data, and some users have poor memories. Therefore, to ensure high user acceptability, the user's freedom of selection is important. The new scheme should provide secrets that are easy to remember and very difficult for intruders to guess. The new scheme should provide secrets that are not easy to write down on paper. Moreover, the scheme secrets should be difficult to share with others. The new scheme should provide secrets that can be easily revoked or changed. Based on the aforementioned requirements, we propose our contribution, i.e., the 3-D password authentication scheme.

b) *3-D Password Overview:* The 3-D password is a multifactor authentication scheme. The 3-D password presents a 3-D virtual environment containing various virtual objects. The user navigates through this environment and interacts with the objects. The 3-D password is simply the combination and the sequence of user interactions that occur in the 3-D virtual environment. The 3-D password can combine recognition-, recall-, token-, and biometrics-based systems into one authentication scheme. This can be done by designing a 3-D virtual environment that contains objects that request information to be recalled, information to be recognized, tokens to be presented, and biometrical data to be verified. For example, the user can enter the virtual environment and type something on a computer that exists in (x1, y1, z1) position, then enter a room that has a fingerprint recognition device that exists in a position (x2, y2, z2) and provide his/her fingerprint. Then, the user can go to the virtual garage, open the car door, and turn on the radio to a specific channel. The combination and the sequence of the previous actions toward the specific objects construct the user's 3-D password. Virtual objects can be any object that we encounter in real life. Any obvious actions and interactions toward the real-life objects can be done in the virtual 3-D environment toward the virtual objects. Moreover, any user input (such as speaking in a specific location) in the virtual 3-D environment can be considered as a part of the 3-D password.

We can have the following objects:

i. A computer with which the user can type;
ii. A fingerprint reader that requires the user's fingerprint;
iii. A biometrical recognition device;
iv. A paper or a white board that a user can write, sign, or Draw on;
v. An automated teller machine (ATM) that requests a token;
vi. A light that can be switched on/off;
vii. A television or radio where channels can be selected;
viii. A staple that can be punched;
ix. A car that can be driven;
x. A book that can be moved from one place to another;
xi. Any graphical password scheme;
xii. Any real-life object;
xiii. Any upcoming authentication scheme.

The action toward an object (assume a fingerprint recognition device) that exists in location (x1, y1, z1) is different from the actions toward a similar object (another fingerprint recognition device) thatexists in location (x2, y2, z2), where x1!= x2, y1!= y2, and z1!= z2. Therefore, to perform the legitimate 3-D password, the user must follow the same scenario performed by the legitimate user. This means interacting with the same objects that reside at the exact locations and perform the exact actions in the proper sequence.

c) *3-D Password Selection and Inputs:* Let us consider a 3-D virtual environment space of size G x G x G. The 3-D environment space is represented by the coordinates (x, y, z) Є [1, . . . , G] x [1, . . . , G] x [1, . . . , G]. The objects are distributed in the 3-D virtual environment with unique (x, y, z) coordinates. We assume that the user can navigate into the 3-D virtual environment and interact with the objects using any input device such as a mouse, keyboard, fingerprint scanner, iris scanner, stylus, card reader, and microphone. We consider the sequence of those actions and interactions using the previous input devices as the user's 3-D password. For example, consider a user who navigates through the 3-D virtual environment that consists of an office and a meeting room. Let us assume that the user is in the virtual office and the user turns around to the door located in (10, 24, 91) and opens it. Then, the user closes the door. The user then finds a computer to the left, which exists in the position (4, 34, 18),And the user types "FALCON." Then, the user walks to the meeting room and picks up a pen located at (10, 24, 80) and draws only one dot in a paper located in (1, 18, 30), which is the dot (x, y) coordinate relative to the paper space is (330, 130).

The user then presses the login button. The initial representation of user actions in the 3-D virtual environment can be recorded as follows:

(10, 24, 91) Action = Open the office door;
(10, 24, 91) Action = Close the office door;

(4, 34, 18) Action = Typing, “F”;
(4, 34, 18) Action = Typing, “A”;
(4, 34, 18) Action = Typing, “L”;
(4, 34, 18) Action = Typing, “C”;
(4, 34, 18) Action = Typing, “O”;
(4, 34, 18) Action = Typing, “N”;
(10, 24, 80) Action = Pick up the pen;
(1, 18, 80) Action = Drawing, point = (330, 130).

Figure 3 – (a) Snapshot of a proof-of-concept 3-D virtual environment, where the user is typing a textual password on a virtual computer as a part of the user’s 3-D password. (b) Snapshot of a proof-of-concept virtual art gallery, which contains 36 pictures and six computers

To simplify the idea of how a 3-D password works, Fig. 4 shows a state diagram of a possible 3-D password authentication system.

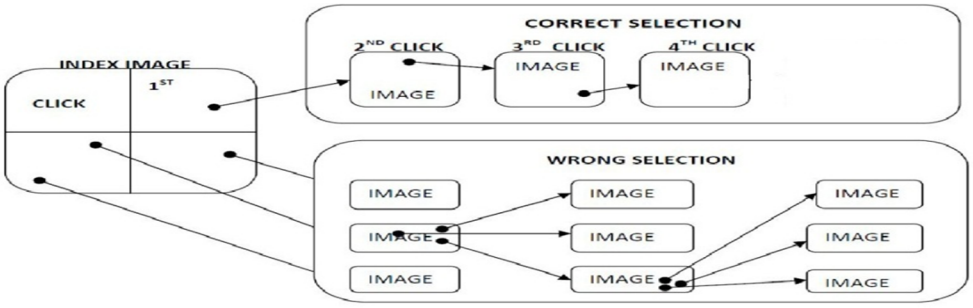
d) 3-D Virtual Environment Design Guidelines: Designing a well-studied 3-D virtual environment affects the usability, effectiveness, and acceptability of a 3-D password system. Therefore, the first step in building a 3-D password system is to design a 3-D environment that reflects the administration needs and the security requirements. The design of 3-D virtual environments should follow these guidelines.

(i) Real-life similarity: The prospective 3-D virtual environment should reflect what people are used to seeing in real life. Objects used in virtual environments should be relatively similar in size to real objects (sized to scale). Possible actions and interactions toward virtual objects should reflect real-life situations. Object responses should be realistic. The target should have a 3-D virtual environment that users can interact with, by using common sense

(ii) Object uniqueness and distinction: Every virtual object or item in the 3-D virtual environment is different from any other virtual object. The uniqueness comes from the fact that every virtual object has its own attributes such as position. Thus, the prospective interaction with object 1 is not equal to the interaction with object 2. However, having similar objects such as 20 computers in one place might confuse the user. Therefore, the design of the 3-D virtual environment should consider that every object should be distinguishable from other objects. A simple real-life example is home numbering. Assume that there are 20 or more homes that look like each other and the homes are not numbered. It would be difficult to distinguish which house was visited a month ago. Similarly, in designing a 3-D virtual environment, it should be easy for users to navigate through and to distinguish between objects. The distinguishing factor increases the user’s recognition of objects.

Therefore, it improves the system usability.

(iii) Three-dimensional virtual environment size: A 3-D virtual environment can depict a city or even the world. On the other hand, it can depict a space as focused as a single room or office. The size of a 3-D environment should be carefully studied. A large 3-D virtual environment will increase the time required by the user to perform a 3-D password.



Moreover, a large 3-D virtual environment can contain a large number of virtual objects. Therefore, the probable 3-D password space broadens. However, a small 3-D virtual environment usually contains only a few objects, and thus, performing a 3-D password will take less time.

(iv) Number of objects (items) and their types: Part of designing a 3-D virtual environment is determining the types of objects and how many objects should be placed in the environment. The types of objects reflect what kind of responses the object will have. For simplicity, we can consider requesting a textual password or a fingerprint as an object response type. Selecting the right object response types and the number of objects affects the probable password space of a 3-D password.

(v) System importance: The 3-D virtual environment should consider what systems will be protected by a 3-D password. The number of objects and the types of objects that have been used in the 3-D virtual environment should reflect the importance of the protected system.

III. PROPOSED SYSTEM

The 3-D password is a multifactor authentication scheme. The 3-D password presents a 3-D virtual environment containing various virtual objects. The user navigates through this environment and interacts with the objects. The 3-D password is simply the combination and the sequence of user interactions that occur in the 3-D virtual environment. The 3-D password can combine recognition-, recall-, token-, and biometrics-based systems into one authentication scheme. This can be done by designing a 3-D virtual environment that contains objects that request information to be recalled, information to be recognized, tokens to be presented, and biometrical data to be verified. Forexample, the user can enter the virtual environment and type something on a computer that exists in (x1, y1, z1) position, then enter a room that has a fingerprint recognition device that exists in a position (x2, y2, z2) and provide his/her fingerprint. Then, the user can go to the virtual garage, open the car door, and turn on the radio to a specific channel. The combination and the sequence of the previous actions toward the specific objects construct the user's 3-D password.

Different users might be select same images. Same images could be reused by two different users, highest probability of collision may be occurs. With the help of inclusion-exclusion principle will be minimized. PCCP reportedly removes major concerns related to common patterns and hotspots. PCCP use a grid-based discretization algorithm to find out whether login click-points are within that tolerance area. In system-side storage for verification, these passwords can be hashed; additional information such as a grid identifier (for each click-point), however, is stored in a manner accessible to the system, to allow the system to use the appropriate grid to verify login attempts. It is unclear if attackers gaining access to the server-side storage can use these grid identifiers to their advantage

A. 3D Password Applications

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

1) Critical servers: Many large organizations have critical servers that are usually protected by a textual password. A 3-D

password authentication proposes a sound replacement for a textual password. Moreover, entrances to such locations are usually protected by access cards and sometimes PIN numbers. Therefore, a 3-D password can be used to protect the entrance to such locations and protect the usage of such servers.

2) *Nuclear and military facilities:* Such facilities should be protected by the most powerful authentication systems. The 3-D password has a very large probable password space, and since it can contain token-, biometrics-, recognition-, and knowledge-based authentications in a single authentication system, it is a sound choice for high level security locations.
3) *Airplanes and jetfighters:* Because of the possible threat of misusing airplanes and jetfighters for religion-political agendas, usage of such 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 in less critical systems because the 3-D virtual environment can be designed to fit any system's needs. A small 3-D virtual environment can be used in many systems, including the following:

ATMs;
Personal digital assistants;
Desktop computers and laptop logins;
Web authentication

IV. ADVANTAGES

Graphical password provides more security than alphanumeric password. Most of the alphanumeric authentication chooses a plain text or easy password to avoiding the confusion. whenever we confirm the alphanumeric password there is some hint option provided, using this hackers can easily gain entry to the system in less time. Most of the system provides image related password i.e. Graphical password. In this method selectable images are used , user can have more number of images on each page and among all of this password is selected. Images are different for each case, so if hackers try to match the each combination to find the correct password it will take millions of year. In alphanumeric password eight characters password is needed to gain entry of particular system, but in graphical password user have to select the images that in front of him/her and confirm the password. Whenever user pass through the authentication process it is easy to remember images whatever they have chosen previously. Graphical password is providing more memorable password than alphanumeric password which can reduce the burden on brain of user.

V. CONCLUSION AND FUTURE WORK

There are many authentication schemes In the current state. Some of them are based on user's physical and behavioral properties, and some other authentication schemes are based on user's knowledge such as textual and graphical passwords. Moreover, there are some other important authentication schemes that are based on what you have, such as smart cards. Among the various authentication schemes, textual password and token-based schemes, or the combination of both, are commonly applied. However, as mentioned before, both authentication schemes are vulnerable to certain attacks. Moreover, there are many authentication schemes that are currently under study and they may require additional time and effort to be applicable for commercial use.

The 3-D password is a multifactor authentication scheme that combines these various authentication schemes into a single 3-D virtual environment. The virtual environment can contain any existing authentication scheme or even any upcoming authentication schemes by adding it as a response to actions performed on an object. Therefore, the resulted password space becomes very large compared to any existing authentication schemes.

The design of the 3-D virtual environment, the selections of objects inside the environment, and the object'stype reflect the resulted password space. It is the task of the system administrator to design the environment and to select the appropriate object that reflects the protected system requirements. Additionally, designing a simple and easy to use 3-D virtual environment is a factor that leads to a higher user acceptability of a 3-D password system.

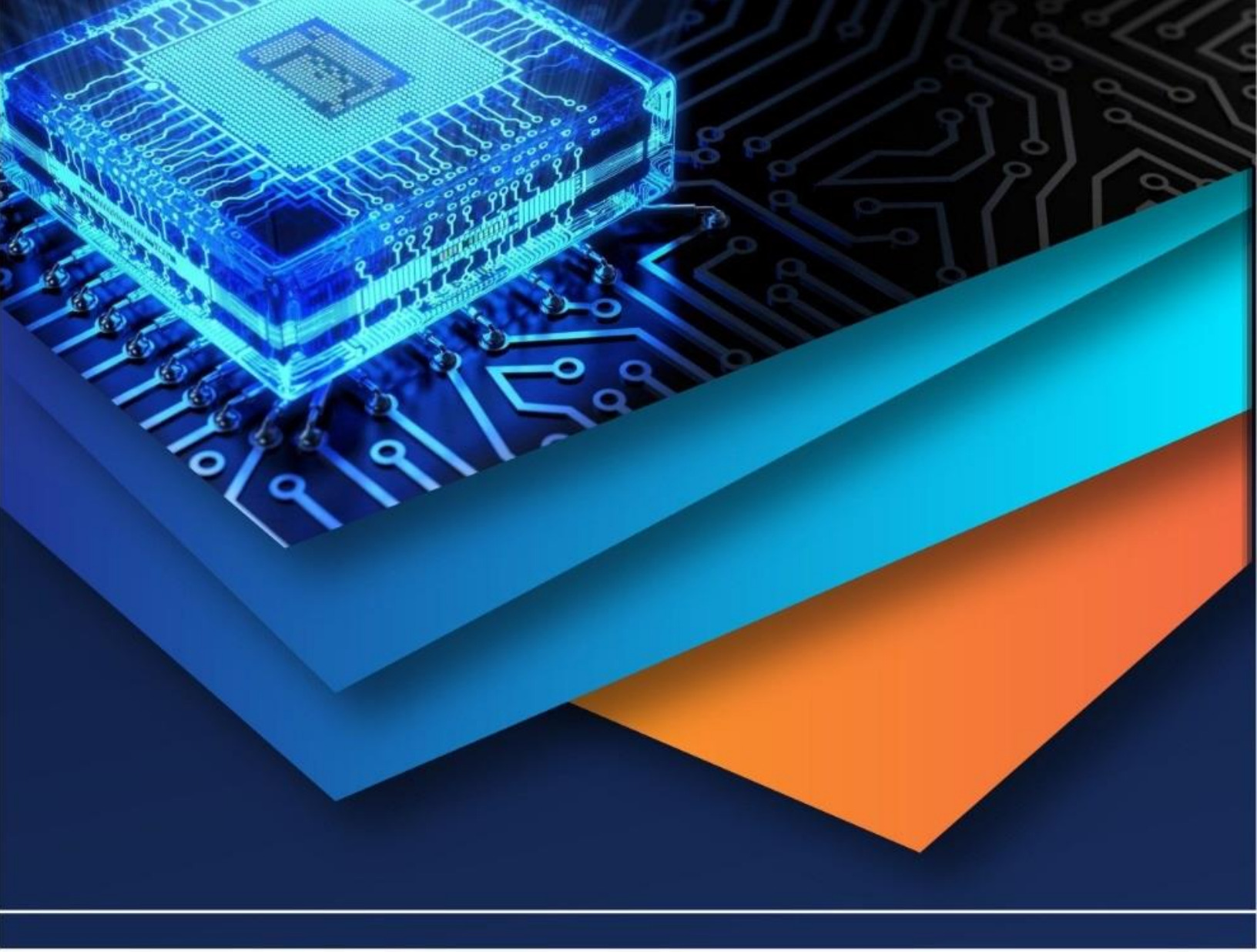
The choice of what authentication schemes will be part of the user's 3-D password reflects the user's preferences and requirements. A user who prefers to remember and recall a password might choose textualand graphical passwords as part of their 3-D password. On the other hand, users who have more difficulty with memory or recall might prefer to choose smart cards or biometrics as part of their 3-D password. Moreover, users who prefer to keep any kind of biometrical data private might not interact with objects that require biometric information. Therefore, it is the user's choice and decision to construct the desired and preferred 3-D password.

The 3-D password is still in its early stages. Designing various kinds of 3-D virtual environments, deciding on password spaces, and

interpreting user feedback and experiences from such environments will result in enhancing and improving the user experience of the 3-D password

REFERENCES

[1] X. Suo, Y. Zhu, and G. S. Owen, "Graphical passwords: A survey," in Proc. 21st Annu.Comput. Security Appl. Conf., Dec. 5–9, 2005, pp. 463–472.
[2] D. V. Klein, "Foiling the cracker: A survey of, and improvement to passwords security," in Proc. USENIX Security Workshop, 1990, pp. 5–14. Authorized licensed use limited to: IEEEXplore. downloaded on March 5, 2009 at 02:38 from IEEE Xplore. Restrictions apply. 1938 IEEE TRANSACTIONS ON INSTRUMENTATION AND MEASUREMENT, VOL. 57, NO. 9, SEPTEMBER 2008
[3] NBC news, ATM Fraud: Banking on Your Money, Dateline Hidden Cameras Show CriminalsOwning ATMs, Dec. 11, 2003.
[4] T. Kitten, Keeping an Eye on the ATM. (2005, Jul. 11). [Online] Available: ATMMarketPlace.com
[5] BBC news, Cash Machine Fraud up, Say Banks, Nov. 4, 2006.
[6] G. E. Blonder, "Graphical password," U.S. Patent 5 559 961, Sep. 24, 1996.
[7] R. Dhamija and A. Perrig, "Déjà Vu: A user study using images for authentication," in Proc.9th USINEX Security Symp., Denver, CO, Aug. 2000, pp. 45–58.
[8] Real User Corporation, The Science Behind Passfaces. (2005, Oct.). [Online]. Available: http://www.realusers.com
[9] D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes," in Proc. 13th USENIX Security Symp., San Diego, CA, Aug. 2004, pp. 1–14.
[10] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Effects of tolerance and image choice," in Proc. Symp. Usable PrivacySecurity, Pittsburgh, PA, Jul. 2005, pp. 1–12.
[11] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Basic results," in Proc. Human-Comput. Interaction Int., Las Vegas, NV, Jul. 25–27, 2005.
[12] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system," Int. J. Human-Comput. Stud. (SpecialIssue on HCI Research in Privacy and Security), vol. 63, no. 1/2, pp. 102–127, Jul.2005.Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The design and analysis of graphical passwords," in Proc. 8th USENIX Security Symp., Washington DC, Aug. 1999, pp. 1–14.
[13] J. Thorpe and P. C. van Oorschot, "Graphical dictionaries and the memorable space of graphical passwords," in Proc. USENIX Security, San Diego, CA, Aug. 9–13, 2004, p. 10.
[14] Adams and M. A. Sasse, "Users are not the enemy: Why users compromise computer security mechanisms and how to take remedial measures,"Commun. ACM, vol. 42, no. 12, pp. 40–46, Dec. 1999.
[15] Authentication for Session Password Using Colour and Images by jai patel,SNJB's COE Computer Engineering Department, University Of Pune.Ganeshkhind,Pune



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY