IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 9, Issue 6, Ver. II (Nov - Dec. 2014), PP 09-17
www.iosrjournals.org

Implementing 3D Graphical Password Schemes

Dr. Mcchester Odoh And Dr. Ihedigbo Chinedum E.
Department Of Computer Science Michael Opara University Of Agriculture, Umudike, Abia State

Abstract: *Beginning around 1999, numerous graphical password schemes have been proposed, motivated by the promise of improved password memorability and thus usability, while at the same time improving strength against guessing attacks. Like text passwords, graphical passwords are knowledge-based authentication mechanisms where users enter a shared secret as evidence of their identity. However, where text passwords involve alphanumeric and/or special keyboard characters, the idea behind graphical passwords is to leverage human memory for visual information, with the shared secret being related to or composed of images, parts of images, or sketches. Despite the large number of options for authentication, text passwords remain the most common choice for several reasons.*

Keywords: *3D, Graphical password, authentication, alphanumeric and special keyboard characters.*

I. Introduction

Authentication is the scientific process of establishing or confirming any entity as authentic, that is, proving if that claims made by, or, about the subject are true. This might involve confirming the identity of a person, tracing the origins of an artefact, ensuring that a product is what it's packaging and labelling claims to be, or assuring that a computer program is a trusted one. For example, when you show proper identification credentials to a bank teller, you are asking to be authenticated to act on behalf of the account holder. If your authentication request is approved, you become authorized to access the accounts of that account holder, but no others.

II. Authentication Methods

There are two techniques for doing this. The first is comparing the attributes of the object itself to what is known about objects of that origin. For example, an art expert might look for similarities in the style of painting, check the location and form of a signature, or compare the object to an old photograph. An archaeologist might use carbon dating to verifythe age of an artefact, do a chemical analysis of the materials used, or compare the style of construction or decoration to other artefacts of similar origin. The physics of sound and light, and comparison with a known physical environment, can be used to examine the authenticity of audio recordings, photographs, or videos [1].

The second technique relies on documentation or other external affirmations. For example, the rules of evidence in criminal courts often require establishing the chain of custody of evidence presented. This can be accomplished through a written evidence log, or by testimony from the police detectives and forensics staff that handled it. Some antiques are accompanied by certificates attesting to their authenticity. External records have their own problems of forgery and
perjury, and are also vulnerable to being separated from the artefact and lost.

Currency and other financial instruments commonly use the first type of authentication method. Bills, coins, and cheques incorporate hard -to-duplicate physical features, such as fine printing or engraving, distinctive feel, watermarks, and holographic imagery, which are easy for receivers to verify. Consumer goods such as pharmaceuticals, perfume, fashion clothing can use either type of authentication method to prevent counterfeit Goods from taking advantage of a popular brand's reputation (damaging the brand owner's sales and reputation). A trademark is a legally protected marking or other identifying feature which aids consumers in the identification of genuine brand-name goods. Normally the authentication scheme the user undergoes is particularly very lenient or very strict. Throughout the years authentication has been a very interesting approach. With all the means of technology developing, it can be very easy for 'others' to fabricate or to steal identity or to hack someone's password. Therefore many algorithms have come up each with an interesting approach toward calculation of a secret key. The algorithms are such based to pick a random number in the range of 10^6 and therefore the possibilities of the sane number coming is rare.

Currently, users are provided with major password stereotypes such as textual passwords, biometric scanning, tokens or cards (such as an ATM) etc .Mostly textual passwords follow an encryption algorithm as mentioned above. Biometric scanning is your "natural" signature and Cards or Tokens prove your validity. But some people hate to carry around their cards, some refuse to undergo strong Infrared (IR) exposure to their retina (Biometric scanning). Mostly textual passwords, nowadays, are kept very simple; say a word from the

dictionary or their pet names, girlfriend or boyfriend's name etc. [2] performed some tests and he could crack 10-15 passwords per day. Now with the technology change, fast processors and many tools on the Internet, this has become a Child's Play. Therefore we present this idea, the 3D passwords which are more customizable and very interesting way of authentication.

Strengths Of 3d Passwords

Memorization: Users can memorize a 3D password as a "little" story which makes the password easy to remember:

- Flexibility: 3d passwords allows multi-factor authentication. Smart cards, biometrics and alpha numeric password can embedded in the 3d password technology
- Strength: A scenario in a 3D environment offers an almost unlimited combination of possibilities. As such system can have specific 3d world, hack are extremely difficult.
- The 3D password gives users the freedom of selecting what type of authentication techniques.
- Secrets are not easy to write down on paper.
- The scheme secrets should be difficult to share with others.
- Provide secrets that can be easily revoked or changed.

How 3d Password Works

Passwords are based on the principals of human memory. Generally, simple passwords are set so as to quickly recall them. The human memory, in this scheme has to undergo the task of recognition, recalling, biometrics or token based authentication. Once implemented and you log in to a secure site, the 3D password Graphic User Interface (GUI) opens up. This is an additional textual password which the user can simply put. Once he goes through the first authentication, a 3D virtual room will open on the screen. In our case, let's say a virtual garage. Now in a day to day garage, one will find all sorts of tools, equipment, etc. each of them having unique properties; same is applied here. The user will then interact with these properties accordingly. Each object in the 3D space, can be moved around in an (x,y,z) plane. That is the moving attribute of each object. This property is common to all the objects in the space. Suppose a user logs in and enters the garage. He sees and picks a screw-driver (initial position in xyz coordinates (5, 5, 5)) and moves it 5 places to his right (in XY plane i.e. (10, 5, 5).That can be identified as an authentication. Only the true user understands and recognizes the object which he has to choose among many. This is the Recall and Recognition part of human memory coming into play. Interestingly, a password can be set as approaching a radio and setting its frequency to a number that only the user knows. Security can be enhanced by the fact of including Cards and Biometric scanner as input. There can be levels of authentication a user can undergo. The More the confidentiality, the more the complex it becomes. In that scenario a virtual environment can be developed as a globe, a city or simply a garage.

III. Literature Review

Sensitive documents are been produced every minute of the day and it is amazing how password hacking has been a major threat to this information and data. D. V. Klein (1990), an ethical hacker with USENIX Security systems performed a password cracking test and he could crack an average of fifteen (15) textual passwords in one day. He then proposed the idea of 3D passwords and organised a workshop to this regard. "Foiling the cracker: A survey of, and, improvement to passwords security," in Proc. USENIX Security Workshop, 1990. Surveys of graphical passwords circa 2005 are available from Suo et al. and Monrose and Reiter. More recently, Hafiz et al. briefly summarize and categorize 12 schemes. Renaud reviews numerous graphical password systems and offers usability guidelines for their design. In this paper, comprehensive review of the first ten years of published research on graphical password was provided. Reflection clearly shows that the graphical nature of schemes does not by itself avoid the problems typical of text password systems. However, while this first generation of graphical password schemes presents some familiar problems, we see an emerging second generation beginning to leverage the graphical elements in new ways to avoid the old problems. These schemes have three main categories based on: recall, recognition, and cued-recall.

Tulving And Pearlstone Recall, Recognition, And Cued Recall

Tulving and Pearlstone explain that items in human memory may be available but not accessible for retrieval. Their results show that previously inaccessible information in a pure recall situation can be retrieved with the aid of a retrieval cue. Recall requires that a person remember information without cueing. With recognition, a person is provided with the information and has to decide whether this matches the information previously memorized. Several theories exist to explain the difference between recognition and recall memory, based on whether these are two unique processes or whether they are similar and differ only in their retrieval

difficulty. It is generally accepted, however, that recognition is an easier memory task than recall. In cued-recall, an external cue is provided to help remember information.

In successful guessing attacks, attackers are able to either exhaustively search through the entire theoretical password space, or predict higher probability passwords (i.e., create a smaller dictionary of likely passwords) so as to obtain an acceptable success rate within a manageable number of guesses. Guessing attacks may be conducted online through the intended login interface or offline if some verifiable text (e.g., hashes) can be used to assess the correctness of guesses. Authentication systems with small theoretical password spaces or with identifiable patterns in user choice of passwords are especially vulnerable to guessing attacks. Password capture attacks involve directly obtaining the password, or part thereof, by capturing login credentials when entered by the user, or by tricking the user into divulging their password. Shoulder-surfing, phishing, and some kinds of malware are three common forms of capture attacks. Shoulder-surfing, phishing, and some kinds of malware are three common forms of capture attacks. In shoulder-surfing, credentials are captured by direct observation of the login process or through some external recording device such as a video camera. Phishing is a type of social engineering attack where users are tricked into entering their credentials at a fraudulent website that records users' input. Malware attacks use unauthorized software installed on client computers or servers to capture keyboard, mouse, or screen output, which is then parsed to find login credentials. Recall-based graphical password systems are occasionally referred to as draw-metric systems because users recall and reproduce a secret drawing. In these systems, users typically draw their password either on a blank canvas or on a grid (which may arguably act as a mild memory cue). Recall is a difficult memory task because retrieval is done without memory prompts or cues. Users sometimes devise ways of using the interface as a cue even though it is not intended as such, transforming the task into one of cued-recall, albeit one where the same cue is available to all users and to attackers.

Although there is currently no evidence of this happening with graphical passwords, it remains a plausible coping strategy if users can devise a way of relating a recall-based graphical password to a corresponding account name. A number of security vulnerabilities are common to most recall-based systems, as these systems share similar features. These systems are generally susceptible to shoulder surfing to the extent that in many cases, the entire drawing is visible on the screen as it is being entered, and thus an attacker need accurately observe or record only one login for the entire password to be revealed.

Some Graphical Recall-Based 3d Schemes

Bdas, Proposed By Dunphy And Yan

BDAS, proposed by Dunphy and Yan added background images to DAS to encourage users to create more complex passwords. In a comparison of BDAS to DAS using paper prototypes, they reported that the background image reduced the amount of symmetry within password images, and led users to choose longer passwords that were similarly memorable to the weaker DAS passwords. It is not known whether the background images introduced other types of predictable behaviour such as targeting similar areas of the images or image-specific patterns. GAO et al Proposed a modification to DAS where approximately correct drawings can be accepted, based on Levenshtein distance string matching and "trend quadrants" looking at the direction of pen strokes. As consequences of this approximation algorithm, a finer grid may be used, but the original password must be stored in a system-accessible manner (rather than hashed) to allow for comparison with the user's input.

Passdoodle

Passdoodle is similar to DAS, allowing users to create a freehand drawing as a password, but without a visible grid. The use of additional characteristics such as pen colour, number of pen strokes, and drawing speed were suggested to add variability to the doodles. Later, Govindarajulu and Madhvanath separately proposed a web-based password manager using a "master doodle" instead of a master password. The three Passdoodle studies focus on users' ability to recall and reproduce their doodles, and on the matching algorithms used to identify similar entries. While usability metrics such as login times or success rates are not reported, the scheme would likely require training of the recognition algorithm during password creation, to build an accurate model of the password. Pass-doodle passwords (the drawings themselves or a characterization thereof) must apparently be stored in a manner accessible to the system, as opposed to hashed, since the recognition algorithm requires access to both original and entered doodles to test if they are sufficiently similar.

Pass Shapes

Weiss and De Luca proposed a similar system, Pass-Shapes. Passwords are translated into alphanumeric characters based on 8 stroke directions, recognized at 45^{O} intervals.

During login, Pass-Shapes can be drawn in a different size or location on the screen and still be translated into correct output provided the stroke direction is accurate. The password space is reduced since only

8 possible choices can be made with each stroke, giving a theoretical password space of size similar to PINs if the number of strokes is similar to the number of digits in a PIN. Lab-based studies show that memorability and login times are acceptable according to the authors, but no security analysis has been reported.

A similar scheme was proposed by Orozco et al [], using a haptic input device that measures pen pressure while users draw their password. While this is intended to help protect against shoulder-surfing (an observer would have difficulty distinguishing variances in pen pressure), their user study showed that users applied very little pen pressure and hardly lifted the pen while drawing. The differences were so small that the use of hepatics did not increase the difficulty of guessing passwords. Por et al. proposed modifying Pass-Go to include background images to aid memorability, optionally highlighting the user's input to facilitate password entry at times when shoulder-surfing is not a threat, and adding decoy input traces to confuse an observer.

Gridsure

Gridsure, a commercial product, displays a 5X5 grid of digits. For their password, users select and memorize a pattern consisting of an ordered subset of the 25 grid squares, and enter the corresponding digits therein using the keyboard. On subsequent logins, digits are randomly displayed within the grid cells and users enter the new sequence of digits found within the cells of their memorized pattern. In a summary of usability study posted online, the reported login success rate exceeds 92% after 36 days. An initial security analysis by Weber reported that grIDsure passwords were much more secure than traditional PINs, especially against shoulder-surfing. Independent analysis by Bond notes several weaknesses in the scheme. A grid-based system resembling a mini Pass-Go has also been deployed commercially for screen-unlock on Google Android cell phones. Rather than entering a 4-digit PIN, users touch-draw their password on a 3X3 grid. These later recall schemes offer design and understanding that goes beyond that in DAS. In particular, BDAS suggests that it might be possible to influence the user to select stronger passwords than they might otherwise. Also, the Pass-Go variant was implemented and tested in user studies, with results supporting its usability in practice; a comparison with the memorability of text passwords remains to be done.

IV. Recognition-Based 3d Password Schemes

Recognition-based systems, also known as cognometric systems or search metric systems, generally require that users memorize a portfolio of images during password creation, and then to log in, must recognize their images from among decoys. Humans have exceptional ability to recognize images previously seen, even those viewed very briefly. From a security perspective, such systems are not suitable replacements for text password schemes, as they have password spaces comparable in cardinality to only 4 or 5 digit PINs (assuming a set of images whose cardinality remains reasonable, with respect to usability). Recognition-based systems have been proposed using various types of images, most notably: faces, random art, everyday objects, and icons. Renaud discusses specific security and usability considerations, and offers usability design guidelines focusing on recognition-based systems.

Phishing attacks are somewhat more difficult with recognition-based systems because the system must present the correct set of images to the user before password entry.

This can be accomplished with a man-in-the-middle (MITM) attack, where the phishing site relays information between the legitimate site and the user in real-time; the phishing site would get the user to enter a username, pass this information to the legitimate site, retrieve the panel of images from that site and display these to the user on the phishing site, then relay the user's selections to the legitimate site. Thus the attacker gains access to the user's account.

V. Story Scheme

[6] developed a comparison system for PassFaces. Users first select a sequence of images for their portfolio. To log in, users are presented with one panel of images and they must identify their portfolio images from among decoys. Images in their user study contained everyday objects, places, or people. Story introduced a sequential component: users must select images in the correct order. To aid memorability, users were instructed to mentally construct a story to connect the images in their set. In the test system, a panel had 9 images and a password involved selecting a sequence of 4 images from this panel. Story was user-tested along with Faces in a field study; Davis et al. found that user choices in Story were more varied but still displayed exploitable patterns, such as differences between male and female choices. Users had more difficulty remembering Story passwords (≈ 85% success rate) and most frequently made ordering errors. Surveys with participants revealed that they were unlikely to have formulated a story as a memory aid, despite the designers' intentions; this may explain the high number of ordering errors. Different instructions or more user experience might possibly result in greater usage of a story strategy.

Cued-Recall Systems

Cued-recall systems typically require that users remember and target specific locations within a presented image. This feature, intended to reduce the memory load on users, is an easier memory task than pure recall. Such systems may also be called locimetric [25] due to their reliance on identifying specific locations. This is a different memory task than simply recognizing an image as a whole. Hollingworth and Henderson show that people retain accurate, detailed, visual memories of objects to which they previously attended in visual scenes; this suggests that users may be able to accurately remember specific parts of an image as their password if they initially focused on them. In an ideal design, the cue in an authentication system is helpful only to legitimate users (not to attackers trying to guess a password).

System Implimentation

As previously stated, it is a multi-factor authentication scheme. The 3D password presents a 3D virtual environment containing various virtual objects. The user navigates through this environment and interacts with the objects. The 3D password is simply the combination of the sequence of user interactions that occur in the 3D virtual environment. The 3D password can combine recognition, recall, token, and biometrics based systems into one authentication scheme. This can be done by designing a 3D virtual environment that contains objects that request information to be recalled, information to be recognized, tokens to be presented, and biometric 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 pos’’’’’ition (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 3D 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 3D environment toward the virtual objects. Moreover, any user input (such as speaking in a specific location) in the virtual 3D environment can be considered as a part of the 3D password.

We can have the following objects in our garage:

1) A computer with which the user can type;
2) A fingerprint reader that requires the user’s fingerprint;
3) A biometric recognition device;
4) A paper or a white board that a user can write, sign, or draw on;
5) An automated teller machine (ATM) that requests a token;
6) A light that can be switched on/off;
7) A television or radio where channels can be selected;
8) A staple that can be punched;
9) A car that can be driven;
10) A book that can be moved 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 (x1, y1, z1) is different from the actions toward a similar object (another fingerprint recognition device) that exists in location (x2 , y2 , z2), where x1 = x2 , y1 = y2 , and z1 = z2 . Therefore, to perform the legitimate 3D 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.

3d Password Selections And Input

Let us consider a 3D virtual environment space of size G ×G × G. The 3D environment space is represented by the coordinates (x, y, z) ∈ [1, 2 . . . , G] × [1, 2 . . . , G] ×[1, 2 . . . , G]. The objects are distributed in the 3D virtual environment with unique (x, y, z) coordinates. We assume that the user can navigate into the 3D virtual environment and interact with the objects using any input device such as a mouse, key board, 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 3D password.

Consider a user who navigates through the 3D 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''Dvirtual 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";

3d Virtual Environment Design Guidelines

The design of the 3 D virtual environments affects the usability, effectiveness, acceptability of 3D password. The first step in building a 3D password system is to design a 3D environment that reflects the administration needs and the security requirements. The design of 3D virtual environments should follow these guidelines.

1) **Real Life Similarity**: The prospective 3D 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 3D virtual environment that users can interact

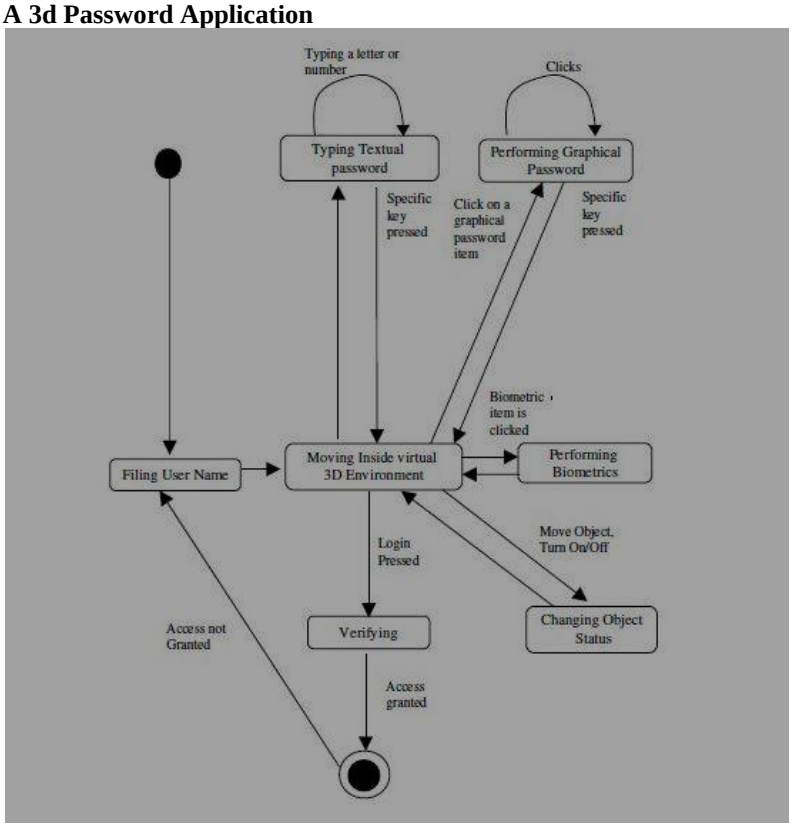
2) **Object uniqueness and distinction**: Every virtual object or item in the 3D virtual environment is different from any other virtual object. The uniqueness comes from the fact that every virtual object has its own attributes such as position. Thus, the prospective interaction with object 1 is not 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' 3D virtual environment should consider that every object should be distinguishable from other objects. Similarly, in designing a 3D 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.

3) **Three Dimensional Virtual Environment Size**: A 3D 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. A large 3D virtual environment will increase the time required by the user to perform a 3D password. Moreover, a large 3D virtual environment can contain a large number of virtual objects. Therefore, the probable 3D password space broadens. However, a small 3D virtual environment usually contains only a few objects, and thus, performing a 3D password will take less time.

4) **Number of objects and their types**: Part of designing a 3D 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 3D password.

5) **System Importance:** The 3D virtual environment should consider what systems will be protected by a 3D password. The number of objects and the types of objects that Have been used in the 3D 'virtual environment should reflect the importance of the protected system.

State Diagram Of A 3d Password Application



Source: Graphical Passwords: Learning from the First Generation
Robert Biddle, Sonia Chiasson, P.C. van Oorschot

3d Password Distribution Knowledge

Users tend to use meaningful words for textual passwords. Therefore finding these different words from dictionary is a relatively simple task which yields a high success rate for breaking textual passwords. Pass faces users tend to choose faces that reflect their own taste on facial attractiveness, race, and gender. Every user has different requirements and preferences when selecting the appropriate 3D Password. This fact will increase the effort required to find a pattern of user's highly selected 3D password. In addition, since the 3D password combines several authentication schemes into a single authentication environment, the attacker has to study every single authentication scheme and has to discover what the most probable selected secrets are. Since every 3D password system can be designed according to the protected system requirements, the attacker has to separately study every 3D password system. Therefore, more effort is required to build the knowledge of most probable 3D passwords.

Attacks And Counter-Measures

To realize and understand how far 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, we then 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. Some of these attacks include but not limited:

1) Brute Force Attack: The attacker has to try all possible 3D passwords. This kind of attack is very difficult for the following reasons.

a. **Time required to login**. The total time needed for a legitimate user to login may vary depending on the number of interactions and actions, the size of the 3D virtual environment, and the type of actions and interactions. Therefore, a brute force attack on a 3D password is very difficult and time consuming

b. **Cost of carrying out such attacks**: the 3D virtual environment contains biometric recognition objects and token based objects. The attacker has to forge all possible biometric information and forge all the required tokens. The cost of forging such information is very high; therefore cracking the 3D password is more

challenging. The high number of possible 3D password spaces leaves the attacker with almost no chance of breaking the 3D password.

2) Well-Studied Attack: The attacker tries to find the highest probable distribution of 3D passwords. In order to launch such an attack, the attacker has to acquire knowledge of the most probable 3D password distributions. This is very difficult because the attacker has to study all the existing authentication schemes that are used in the 3D environment. It requires a study of the user's selection of objects for the 3D password. Moreover, a well-studied attack is very hard to accomplish since the attacker has to perform a customized attack for every different 3D virtual environment design. This environment has a number of objects and types of object responses that differ from any other 3D virtual environment. Therefore, a carefully customized study is required to initialize an effective attack.

3) 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 biometric data or textual passwords that cannot be seen from behind. Therefore, we assume that the 3D password should be performed in a secure place where a shoulder surfing attack cannot be performed.

4) Timing Attack: In this attack, the attacker observes how long it takes the legitimate user to perform a correct "sign in" using the 3D password. This observation gives the attacker an indication of the legitimate user's 3D password length. However, this kind of attack alone cannot be very successful since it gives the attacker mere hints. Therefore, it would probably be launched as part of a well-studied or brute force attack. Timing attacks can be very effective if the 3D virtual environment is poorly designed.

VI. Conclusion

Since the 3D password scheme is a multi-factor authentication scheme that combines the various authentication schemes into a single 3D virtual environment; the virtual environment can contain any existing authentication scheme or even any upcoming authentication schemes by simply adding it as a response to actions performed on an object. Therefore, the resulting password space becomes very large compared to any existing authentication schemes. The design of the 3D virtual environment, the selection of objects inside the environment and the object's type 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. Designing a simple and easy to use 3D virtual environment is a factor that leads to a higher user acceptability of a 3D password system. The choice of what authentication scheme will be part of user's 3D password reflects the user's preferences and requirements, depending on the prevailing security requirement.

References

[1]. A. De Angeli, L. Coventry, G. Johnson, and K. Renaud, "Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems," International Journal of Human-Computer Studies, vol. 63, no. 1-2, pp. 128–152, 2005.

[2]. A. Paivio, Mind and Its Evolution: A Dual Coding Theoretical Approach.Lawrence Erlbaum: Mahwah, N.J., 2006.

[3]. A. Paivio, T. Rogers, and P. C. Smythe, "Why are pictures easier to recall than words?" Psychonomic Science, vol. 11, no. 4, pp. 137–138,1968.

[4]. B. Kirkpatrick, "An experimental study of memory," PsychologicalReview, vol. 1, pp. 602–609, 1894.

[5]. C. Herley, P. van Oorschot, and A. Patrick, "Passwords: If We're So Smart, Why Are We Still Using Them?" in Financial Cryptography and Data Security, LNCS 5628, Springer, 2009.

[6]. D. Klein, "Foiling the cracker: A survey of, and improvements to, password security," in 2nd USENIX Security Workshop, 1990.

[7]. E. Tulving and Z. Pearlstone, "Availability versus accessibility of information in memory for words," Journal of Verbal Learning and Verbal Behavior, vol. 5, pp. 381–391, 1966.

[8]. E. Tulving and M. Watkins, "Continuity between recall and recognition," American Journal of Psych., vol. 86, no. 4, pp. 739–748, 1973.

[9]. F. Craik and J. McDowd, "Age differences in recall and recognition," Journal of Experimental Psychology: Learning, Memory, and Cognition, vol. 13, no. 3, pp. 474–479, July 1987.

[10]. F. Monrose and M. Reiter, "Graphical passwords," in Security and Usability: Designing Secure Systems That People Can Use, L. Cranor and S. Garfinkel, Eds. O'Reilly Media, 2005, ch. 9, pp. 157–174.

[11]. I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords," in 8th USENIX Security Symposium, August 1999.

[12]. J. Anderson and G. Bower, "Recognition and retrieval processes in free recall," Psychological Review, vol. 79, no. 2, pp. 97–123, March 1972.

[13]. J. Bentley and C. Mallows, "How much assurance does a PIN provide?" in Human Interactive Proofs (HIP), LNCS 3517, Springer-Verlag, H. Baird and D. Lopresti, Eds., 2005, pp. 111–126.

[14]. J. G. W. Raaijmakers and R. M. Shiffrin, "Models for recall and recognition," Annual Reviews Psych., vol. 43, pp. 205–234, January 1992.

[15]. J. Yan, A. Blackwell, R. Anderson, and A. Grant, "Password memorability and security: Empirical results," IEEE Security & Privacy Magazine, vol. 2, no. 5, pp. 25–31, 2004.

[16]. K. Renaud, "Evaluating authentication mechanisms," in Security and Usability: Designing Secure Systems That People Can Use, L. Cranor and S. Garfinkel, Eds. O'Reilly Media, 2005, ch. 6, pp. 103–128.

[17]. K. Renaud, "Guidelines for designing graphical authentication mechanism interfaces," International Journal of Information and Computer Security, vol. 3, no. 1, pp. 60–85, June 2009.

[18]. K.-P. L. Vu, R. Proctor, A. Bhargav-Spantzel, B.-L. Tai, J. Cook, and E. Schultz, "Improving password security and memorability to protect personal and organizational information," International Journal of Human-Computer Studies, vol. 65, pp. 744–757, 2007.
[19]. L. Gong, M. Lomas, R. Needham, and J. Saltzer, "Protecting poorly chosen secrets from guessing attacks," IEEE Journal on Selected Areas in Communications, vol. 11, no. 5, pp. 648–656, June 1993.
[20]. M. A. Sasse, S. Brostoff, and D. Weirich, "Transforming the 'weakest link' – a human/computer interaction approach to usable and effective security," BT Tech. Journal, vol. 19, no. 3, pp. 122–131, July 2001.
[21]. M. D. Hafiz, A. H. Abdullah, N. Ithnin, and H. K. Mammi, "Towards identifying usability and security features of graphical password in knowledge based authentication technique," in Second Asia International Conf. on Modelling & Simulation. IEEE, 2008, pp. 396–403.
[22]. R. Morris and K. Thompson, "Password Security: A Case History," Communicaitons of the ACM, vol. 22, no. 11, pp. 594–597, 1979.
[23]. R. Shepard, "Recognition memory for words, sentences, and pictures,"Journal of Verbal Learning and Verbal Behavior, vol. 6, pp. 156–163, 1967.
[24]. S. Chiasson, A. Forget, E. Stobert, P. C. van Oorschot, and R. Biddle, "Multiple password interference in text and click-based graphical passwords." in ACM Computer and Communications Security (CCS), November 2009.
[25]. S. Chiasson, "Usable authentication and click-based graphical passwords ,"Ph.D. dissertation, School of Computer Science, Carleton University, December 2008.
[26]. S. Madigan, "Picture memory," in Imagery, Memory, and Cognition: Essays in Honor of Allan Paivio, J. Yuille, Ed. Lawrence Erlbaum Associates, 1983, ch. 3, pp. 65–89.
[27]. T. Kitten, Keeping an Eye on the ATM. (2005, Jul. 11). [Online]. Available: ATMMarketPlace.com.
[28]. W. Kintsch, "Models for free recall and recognition," in Models of Human Memory, D. Norman, Ed. Academic Press: New York, 1970.
[29]. X. Suo, Y. Zhu, and G. Owen, "Graphical passwords: A survey," in Annual Computer Security Applications Conf. (ACSAC), Dec. 2005.
[30]. BBC news, Cash Machine Fraud up, Say Banks, Nov. 4, 2006.