Security and User Interface Usability of Graphical Authentication Systems – A Review

Hassan Umar Suru [#1], Pietro Murano [*2]
[#]School of Computing, Science and Engineering, University of Salford, Salford, UK
[*]Department of Computer Science, OsloMet - Oslo Metropolitan University, Oslo, Norway

Abstract

Alphanumeric text and PINs continue to be the dominant authentication methods in spite of the numerous concerns by security researchers of their inability to properly address usability and security flaws and to effectively combine usability and security. These flaws have, however, contributed to the growing research interest in the development and use of graphical authentication systems as alternatives to text based systems. Graphical passwords or graphical authentication systems are password systems that use images rather than characters or numbers in user authentication. In spite of the growing acceptance of graphical passwords, empirical studies have shown that graphical authentication systems have also inherited some of the flaws of text-based passwords. These flaws include predictability, vulnerability to observational attacks and the inability of systems to efficiently combine security with usability. Hence, there is a continued quest to find a 'system' that has both strong usability and strong security. This paper is a detailed review of the current state of research into graphical authentication systems. The paper considers in detail some of the mechanisms used in graphical authentication, along with the flaws and strengths of each. The paper also concludes with some suggested ways forward.

Keywords - *Graphical Authentication, graphical passwords, security, usability, user interface*

I. INTRODUCTION

This paper is a review on the evolution and evaluation of existing authentication systems. Over the years, the main method of authentication has been the use of alphanumeric text, which has been either predictable or difficult to remember [2]. In addition, the use of graphical images to complement text based passwords for improving their usability and security have been suggested [3]. The fact that users need to keep track of several accounts has made them resort to insecure behaviour such as the use of the same password for several accounts, use of common names, as well as writing down and sharing of passwords [4,5]. In order to address these problems, alternative password schemes have been suggested [4,6,7]. Among such schemes are graphical (or image based) passwords, as researchers believed that humans are better able to remember pictures than text [8, 9]. Several graphical systems have been developed and evaluated.

This paper is divided into two sections. The first section provides a general overview of the developmental trends in the design and proliferation of authentication systems focusing on the security and user interface usability issues in relation to these systems. The section also looks more closely into some of the most common user-related security issues, which include guessability, shoulder surfing (observability) and vulnerability to description. The second section takes a closer examination of three of the existing graphical authentication systems: the passpoints scheme, the passfaces scheme and déjà vu, a system that uses pictures and random art (abstract) images. Random art (abstract) images are coloured computer generated images that do not have a definite form. The section provides insight into important research findings related to the user interface usability and security of these systems.

This paper will not consider in any detail the algorithms or 'back-end' aspects of authentication systems. This review paper is principally about examining existing works (literature) in authentication systems along with their good and bad points in terms of security and usability.

II. REVIEW OF EXISTING AUTHENTICATION SYSTEMS

A. Overview of Existing Authentication Methods

In the literature, authentication methods have been developed and classified based on what is required of a systems user in the process of authentication. These methods include: 1) something you have (Token based authentication) [14, 15], 2) something you are (Biometric authentication) and 3) something you know (Knowledge based authentication).

Token-based authentication involves the use of additional devices such as key fobs, bank cards and tokens provided to the user for the process of authentication. However, token based systems, such as in ATM machines, are often combined with a knowledge-based component.

Biometric systems utilise human traits and characteristics in user authentication. Human fingerprints, palm scan, iris scan, facial scan and DNA are all used in biometric authentication. Gait and gaze based biometric systems have also been developed. Although biometric systems provide the

highest level of security, they mostly have usability issues such as being slow and sometimes unreliable as human physiology may change due to old age or ill health. Other problems with biometric systems include 'spoof attacks' [16] and 'template database leakage' [17]. They also mostly require the attachment of additional components to traditional computing systems and handheld devices, which are often very expensive.

The most widely used systems today are knowledge-basedsystems, which utilise something known only to the user for authentication. The most common of these techniques is the text based system that uses alphanumeric text and numeric PINs [18, 19, 20]. Considerable research has been conducted on the usage and performance of text based passwords including that on people's attitudes towards the selection of passwords, the strength and memorability of user chosen passwords, the number of passwords users have, as well as the use of passwords by corporations [18]. Graphical passwords were developed as an alternative to text-based systems and are subdivided into recognition based, recall based and cued recall-based systems [21, 22].

B. Overview of Recognition Based Systems

Recognition based graphical authentication systems are graphical systems that depend on the user's ability to recognise images selected earlier from a large collection of images. In each round of authentication, the user is presented with many images from which one is expected to recognise and correctly select the images that represent one's chosen password.

Several recognition-based schemes have been developed and evaluated. Among these is the déjà vu scheme developed by Dhamija and Perrig [4], which used the Hash Visualisation Technique [23] to generate a set of abstract images using a computer algorithm. The déjà vu scheme is an example of a grid-based type of recognition based graphical authentication system. To study the déjà vu scheme, the researchers developed system prototypes that were implemented and analysed in a study that involved interviews and web-based user studies. Two user studies were conducted using déjà vu systems that used photographs and random art images in which twenty research participants were recruited (11 males and 9 females) to compare the déjà vu system to traditional password based systems (passwords and PINs). A within user study was used with each user testing each of the four system prototypes presented, two for the déjà vu systems and another two for each of the textual and PIN based password systems. The tests were conducted in two sessions, one week apart. Although relatively slower in password creation and login time, memorability of the déjà vu system was better than in text based passwords and PINs. No login failure was recorded for the déjà vu system during the first session, unlike the passwords and PINs that recorded one failure (5%) each. After a week, the login failure had increased to seven (35%) for PIN and six (30%) for passwords while the déjà vu systems recorded two (10%) and one (5%) for the random art and photo based schemes. In spite of the improved memorability, a usability issue with the déjà vu system is that the seeds of each of the algorithms had to be stored separately to ensure that the exact image could be reproduced in the future. Another basic flaw of this work is the very low sample size. An improved version of this scheme was developed in [24]. Their Image Based Registration and Authentication System (IBRAS) used a function called a SHA-1 hash function. It was more secure and used less memory than the earlier version. Although similar in their storage of initial seeds, the main difference between the implementation of the IBRAS and the déjà vu system is that in the IBRAS, a user chooses and uses a single graphical authentication image. Although the déjà vu scheme performed well with its use of abstract images, researchers believe it is easier to remember images that have some meaning attached to them [21].

Researchers in [25] introduced and evaluated the Convex Hull Click (CHC) scheme. In this scheme, a participant selects a set of icons from a large set of icons during the registration stage. In each authentication round, the participant is expected to identify their pass-icons in every challenge set. An authentication round consists of several challenge sets. A challenge set is a set of images presented in an image grid containing some of the user's pass-icons and many decoy icons. The participant is expected to click inside any triangle (convex hull) formed by any subset of their pass-icons. The researchers conducted a usability study comprising of two sessions, one week apart, in a between user study with 15 participants (6 males and 9 females), mean age 37 (StdDev = 13.6) using a software prototype. The first session took about 15 minutes to collect data on the number of correct and incorrect logins, the number of correct and incorrect challenges, and the total time for each correct and incorrect login and challenge. Each participant was asked to authenticate themselves onto the system until able to get up to ten successful logins. Experimental results indicated the mean correctness of entries was 90.35%, the mean correctness of the challenge sets was 97.95%, and the mean time for correct password inputs was 71.66 seconds. Statistical evaluation of the results show a statistically significant smooth reduction in authentication times between the ten correct logins collected from participants. The results also indicated that participants whose challenge sets comprised of five pass-icons were faster in login times than those with three and four pass-icons in their challenge sets. No statistically significant correlation was identified between the login times of those with three and four pass-icons in their challenge sets. In the follow up session one week later, the participants were shown a list of 112 icons and told to identify the five pass-

icons they had used in the previous experiment. Only one of the participants was unable to identify all the five pass-icons, the participant was only able to identify four.

In order to compare with other recognition-based systems, the researchers detailed a number of experiments to compare the usability of the passfaces, déjà vu and the VIP schemes with alphanumeric PINs and passwords. The VIP scheme is a graphical PIN authentication system that is meant for use with both a PIN and an ATM card. The researchers discovered that although déjà vu compared better to the alphanumeric PINs and passwords in terms of memorability, the efficiency of déjà vu was lower due to the longer times it took to authenticate. Weinshall and Kirkpatrick proposed a number of graphical schemes in [26]. Their methods used picture, object and pseudo word recognition schemes with a considerably large number of images. With the aid of prototypes, they ran user trials that lasted for three months. They realized that for the picture-based model three aspects of their procedure made the largest influence on the accuracy and retention. These were choosing picture groups with a clear theme but individual distinctions, the number of training sessions, and the frequency of testing. Overall, the systems had good memorability as users could recognize their chosen images even after several weeks. The picture-based implementation, however, proved to be more effective than the others. While the pseudo- word model had a 70% success rate at the end of the three month period, the picture based model recorded about 90%.

Sobrado and Birget [27] proposed a number of shoulder surfing resistant schemes. Shoulder surfing is the ability to observe a user's password by simply looking over their shoulders [28]. Their models were an extension of the Convex Hull Scheme (CHC) proposed by Wiedenbeck et al. [25]. In their first approach, a user had to locate any three of their chosen password images and click inside the convex hull formed by those images. In the second approach, the user needed to position one of their chosen images in a movable frame, and then move the frame to align with any other two of the user's chosen images to authenticate. The researchers also introduced a third scheme in which the user had to locate any four of their chosen images and then click on the point of intersection of invisible lines joining the images placed at the opposite vertices of the quadrilateral formed by the four images. No details of experimentation with these schemes has been reported in the literature. To decrease guessability, the researchers suggested the use of thousands of images. According to the researchers, the number of possible passwords is a "Binomial Coefficient" $\left(\frac{n}{k}\right)$ (choose any K objects among N). Hence when N = 100 and K = 10, the number of possible passwords becomes $\left(\frac{1000}{10}\right) \approx 2.6 * 10^{23}$, which is a little more than the number of alphanumeric passwords of length 15. However, a large number of images on a small computer screen makes the screen highly compacted thereby creating usability issues. In fact, researchers in [30] discussed two significant drawbacks of this scheme. The first was a technical drawback in which the researchers developed a system prototype using 1000 icons as suggested in[27]. However due to the size of a standard computerscreen, it became impossible to distinguish one icon from the other. The second drawback was a "theoretical complication". Let K denote the number of user chosen pass-images, N the total number of images displayed on the screen and h the number of authentication screens for an authentication round. They argued that 10 pass icons (K) were suggested in [27] and that from a theoretical assumption: *"There is a constant c > 1, which depends only on the size of the screen used such that the probability of thecenter of the screen being in the convex hull of the K randomly placed pass-objects is greater than* $1 - \left(\frac{1}{C^k} - 1\right)$*".*This meant that if K objects are randomly placed on a computer screen, an attacker can play a wait- and-hunt. For each image (screen), the attacker may just click in the center of the screen and the probability of a successful login is $q = \left(1 - \frac{1}{C^k - 1}\right)^h$. For a standard sized screen, c ≈ 1.5, and thus, we have q ≈ 0.77 when K = 10, and h = 10 and q ≈ 0.45 when K = 10 and h = 30. Therefore, the K pass icons will have to be moved as a group all over a screen. This complicates analysis of the scheme, since a mouse click always gives an attacker some hint. Another drawback is that authentication in this system may be considerably slow due to the time it may take in locating the images, lowering the efficiency of the system.

An algorithm for filtering distractor (doodle) images was suggested in [29]. The algorithm was used to filter out images due to their similarities based on the number of black and white regions as well as the number of joints possessed by each image. The aim of the algorithm was to identify similarities in distractor images to be presented as decoy images in the course of authentication. The assurance that simple doodle distractor images do not possess obvious similarities with the users pass images improves usability by reducing user input errors.

Man, et al. proposed a system [30] called WIW (where is Waldo?) which borrows its name form a popular puzzle game. In this scheme, the graphical interface is made up of several login images (called a scene). Each scene is made up of several objects from which a user selects their pass- objects and a set of perturbations. Each authentication round is performed such that a user is presented with several scenes depending on their exact selection. Each scene represents a challenge set in which a user is presented with their pass-objects and many decoy or non-pass-objects. The user is expected to identify and select their pass objects from a mixture of pass and non-

pass-objects contained in the scene. The perturbations are a number of variants developed for both the pass and non-pass objects such that during authentication the user can select any of the various perturbations (or variants) of their chosen images. A monitor's screen can be viewed as a rectangle with width a, and height b. Each scene is displayed on such a screen. For each scene, WIW renders two small icons of eye shape at$\left(\frac{a}{3},\frac{b}{2}\right)$ and $\left(\frac{2a}{3},\frac{b}{2}\right)$, respectively. These icons are designated as the left and the right eye. In the process of authentication, as the pass and non-pass objects are shuffled across each scene, the user has to relate the position of each of the designated eyes to the various positions of their pass objects within the scene. Although a prototype of the system was developed and experimentation was performed using a number of research participants, the methodology adopted for the experiment as well as the details of its results were not provided in the paper.

The system in [30] was improved upon by Hong et al. [31] in which every image had several variants and each variant was associated with a unique code. System users are presented with a scene during authentication, the scene containing pass object variants randomly selected and presented among many decoy images. To authenticate, a user types the code associated with their pass image variants and the relative position of their pass image among decoy images as observed on the computer screen. According to the researchers, the system proved resistant to shoulder surfing, although users had to both recognize their images as well as memorize the codes for the various image variants, which may affect the memorability and overall usability of the system. Although an experiment was reported to have been conducted by the researchers, the details of the experiment as well as its results were not reported. An improvement was also proposed in which a system user assigns their own codes to their preselected images. The need to memorize such codes, however, meant that it suffered the same fundamental usability flaws as the previous scheme.

The *passfaces* technique was developed by the Real User Corporation [32]. The idea came from the belief that humans find it extremely easy to remember the faces of other people even after prolonged periods of time. In the implementation of this scheme, a user is presented with a large database of human faces from which they are expected to select any four random faces. During authentication, the user is presented with four successive grids, and is expected to recognize and select their chosen faces among eight distractor face images. Considerable research has been done on the usability and security of the passfaces scheme.

Studies into the effectiveness of the passfaces scheme conducted by [33, 34] indicated that passfaces could easily be remembered even after a prolonged period of time. One of these was a within user study conducted by T. Valentine [33] involving 77 staff and students of Goldsmith's College to test the memorability of the passfaces scheme. All participants used the passfaces scheme to test three conditions. For the first condition, 29 participants were asked to login to the system every working day for a period of 2 weeks. The participants remembered their passwords in 99.98% of logins. The second condition used 29 participants to login after about 7 days of initial enrolment. Most (83%) of the participants were able to login on their first attempt. Everyone was, however, able to login on the third attempt. For the third condition, 19 participants were asked to login once after about 30 days of initial enrolment. In this condition too, 84% of participants were able to login on their first attempt, while all others were able to login by their third attempt. The passfaces scheme is also believed to withstand long-term recall as the study participants were asked to login to the systems after more than five months of their last use [34]. While 56 participants were able to participate in the follow up trial, 72% were able to login on their first attempt and 84% by the third attempt. It was also reported that the participants that used the everyday login condition could remember their passwords the best, with 87% remembering the passwords on the first attempt and 100% remembering them in the third attempt.

Other studies in [35] revealed that the login failure rate of passfaces was less than that of text-based passwords, but login time was longer. Davis et al. [32], however, discovered predictable patterns in the passfaces scheme as users were attracted to beautiful faces, faces of the opposite sex and members of their own race. In this study, the researchers analyzed observations collected during a roughly four month semester period of two universities in which two graphical password systems were used by 154 research participants. One of the schemes was a face based password system modelled after the passfaces scheme [32], while the other was a story scheme developed by the researchers. Each participant was randomly assigned one of the two graphical schemes. Each of the students used their graphical password to access published content that included their grades, class assignments, assignment solutions and reading materials through the use of Java enabled browsers. In total, 174 passwords were created during the semester, indicating that a number of students changed their passwords at least once during the study. A total of 2648 login attempts were recorded, out of which 2271 (85.76%) were successful logins. At the end of the semester, an exit questionnaire was used to both capture the demographics of the participants as well as the reasons why they each selected their faces (for the face scheme) or their chosen stories (for the story scheme). The results of the experiment revealed that in the face scheme, both males and females chose the faces of females significantly more often than the faces of males. In fact, over 68% of females and over 75% of males

selected female faces. It was also observed that when males chose the faces of females, they almost always chose the faces of models. This accounted for about 80% of male selection of female faces. This fact was also supported by participants' remarks in the research questionnaire. The researchers also recorded a significant correlation among members of the same race. Asian and Caucasian females selected faces of people from within their own race about 50% of the time. Caucasian males chose the faces of Caucasians over 60% of the time, while black males chose the faces of blacks about 90% of the time. With these results, the researchers refuted the argument that user-chosen graphical passwords of the face and story schemes are likely to offer additional security over text passwords without users being trained to select better passwords. System assigned passwords was suggested as a possible solution to the predictability problem. This, however, may render the system less memorable, hence negatively affecting its usability. Vulnerability of the passfaces scheme to descriptions was analyzed in [36]. The study was aimed at understanding the possibility of verbal descriptions on passfaces and how such vulnerabilities could be reduced. The study was conducted using images from the passfaces online demo using 45 face images (18 males and 27 females). The experiment evaluated three test conditions: random groups (the base condition) in which decoy face images for a target face image were selected randomly, visual groups in which decoy images for a target face image were selected based on visual similarities with a target face image and verbal groups in which decoy face images were selected based on verbal similarities with a target face image. The researchers recruited 56 participants (31 male and 25 female) with an average age of 22 (Standard dev. = 7) that conducted lab based trials. Five face grids were provided for each test condition out of which each participant was expected to identify a target face among decoy images assembled based on the criteria for the test condition in a within users study. A group of 18 contributors (9 males and 9 females) were recruited for the decoy image selection process. The results indicated that of all the 158 login attempts collectively made in the entirety of the experiment, only 13 (8%) were successful. That is, only 8% identified all five target face images in the five face grids of any particular test condition. The random groups had the highest login success rate and the verbal groups had the lowest. The average login success (out of 5) for the random groups was 3.57 (standard deviation = 0.91), for the visual groups was 2.87 (standard deviation = 1.07). The mean variation was statistically significant ($t=3.63$ $p< 0.0$). The average login success rate for the verbal group condition was 2.81 (standard deviation = 1.14). The mean variation between the verbal and the random conditions was also statistically significant ($t=3.64$ $p < 0.01$). The study concluded that passfaces could effectively be described and suggested the presentation of similar faces in a grid as an effective way of reducing facial disparity, and hence description. It is observed in [28] that keyboard entry was a better alternative in the implementation of the passfaces scheme in a study that compared the security of keyboard based versus mouse based data entry in the passfaces scheme.

A theme based set of graphical passwords [37-39] were proposed by Jansen et al. for mobile devices. In this system, a user selects images which represent themes (such as the sea, the forest, group of animals, etc.). Some themes comprise thumbnails of pictures which when put together will form a particular image, others comprise a set of similar images. A user selects a number of images in a sequence within this theme as their password. During authentication, the user needs to select their images within the theme in a definite order. The system also allowed users to submit and use their own set of images [38]. A method called "salting" was proposed to increase the security of the system against observational and specialized dictionary attacks. Salting is the process whereby the clear text value of an image password is prepended with a random numerical value *R*, called a salt. Through salting, the search space of an attacker is increased by a factor $2^{|R|}$ if the attacker does not know the salt. Although details of the system implementation were provided in [38], the researchers did not publish any details of any experiments or experimental results. The main limitation of this system was the fixed size of the mobile screen, which limited the number of thumbnails used, a great hindrance to the efficiency and usability of the system.

Another graphical scheme was proposed by Takada and Koike [40], which allowed a user to submit their favorite images to the server as their password. In each round of authentication, the user only needs to recognize the images they had submitted among other decoy images. If none of the user's images is presented on the screen, the user selects nothing. The idea of an online registration for every image submitted by the user as well as the use of image notifications as provided by the system greatly improve security. No experimental or design details were, however, reported for the system. Submitting one's own images greatly improves memorability, but also makes it easier for an intruder who knows the user to easily guess the password [35, 41], a great setback on security.

C. Overview of Recall Based Systems

Recall based systems are systems in which a user performs a series of actions during registration and is expected to repeat the actions, in the same order, during each authentication round. They are mainly divided into two subgroups: (1) Pure recall based systems (2) Cued recall based systems.

1. Pure Recall Based Systems

Pure recall based systems are systems in which a user is expected to fully recall a piece of action from past memory to authenticate. The majority of these systems present a blank touch sensitive screen during each authentication round upon which a user is expected to reproduce an image they had drawn earlier during registration.

A technique called Draw a Secret (or DAS) was proposed by Jermyn et al [42], which allowed users to draw their own pass images on a 2D grid using a touch sensitive screen. The coordinates of the drawn image on the grid are stored on the system in the order in which the drawing occurred. The user has to repeat the drawing in exactly the same order each time they want to authenticate. The password space for the DAS system is larger than the text password space. Another advantage of the DAS scheme is that since it is independent of any alphanumeric strings, it can well be used by speakers of any language.

A number of researchers have investigated the usability and security of the DAS password scheme. One was presented in [43]. In an analysis of the memorable password space of DAS, the researchers developed the concept of graphical dictionaries, which was used to study the susceptibility of the DAS scheme to brute force attacks. They postulated that since mirror symmetry had a significant position in human cognitive memory, it was possible to develop an attack dictionary based on symmetric patterns. A performance comparison of mirror symmetric and asymmetric images was also performed, which led to the conclusion that symmetric images were more preferred by system users, but were also less secure. Another study [44] investigated the impact of stroke count on DAS password strength and observed that the higher the stroke count the stronger the password. The study was aimed at investigating the relationship between the number of composite strokes, the dimensions of the grid and the length of the DAS password in the DAS password space. In doing this, the researchers introduced DAS password complexity properties based on pattern complexity factors which included password length, number of composite strokes (or the stroke count), symmetry, or the number of turns in each stroke. The study was to help understand if any of these factors could have an effect on the DAS password space such that it was possible to perform a brute force attack on a DAS password using a graphical dictionary. The study proved that when users choose images with less than five strokes with a password of length less than 13 on a 5 × 5 grid, instead of the maximum of 12 strokes, the password space of the DAS password is reduced from 58 bits to 40 bits. To further strengthen the DAS password, the researchers proposed the grid selection technique in which a user selects a small rectangular section of the grid as their drawing grid, which is then zoomed into before the password is created. This method significantly increased the password strength of the DAS system with an increase of up to 16 more bits. The researchers, however, did not report any user study. Dunphy et al. [45] also tried to improve the security of the DAS password through the introduction of background images in a method called Background DAS (or BDAS). In this method, a user first had to select a background image, and while the chosen image appears faintly at the background of their DAS grid, the user draws an image on the grid as is done in a normal DAS password. In two laboratory studies with paper-based prototypes, the researchers investigated the effects of background images on the memorability of the DAS password as well as the effects of background image choice on user performance in the BDAS password scheme. A total of 21 participants were recruited for the first experiment, 15 male and 6 female, aged between 18 and 50+ that cut across technical and non-technical disciplines. Participants were split into two groups, the control group that used a prototype representing the original DAS system and the BDAS group that used the BDAS prototype. Five picture images were used for the background and participants were allowed to use images of their choice. The results of the first study (the pilot study) revealed that 90% of the DAS group employed global symmetry as opposed to 50% in the BDAS group. In addition, 90% of the passwords used in the DAS scheme were centred within the grid as opposed to 70% in the BDAS scheme. The lengths of the passwords created by the BDAS users were significantly greater than those created by the DAS users. The t-test results showed $t=2.377$, $p<0.0$. These results imply that the users of the DAS scheme employed centralization and symmetry as a means to aid recall and that the BDAS users created longer passwords. In the second study, 46 participants were recruited, 32 male and 14 female with most participants between the ages of 18 and 25. While 20 participants had technical backgrounds, 26 were from non-technical disciplines. Participants were equally split into two groups as in the first study. The results from this study indicated that 43% of the BDAS group exhibited global symmetry as compared to 57% for the DAS group. In terms of image centering, 43% of the BDAS passwords exhibited image centering as against 87% for the DAS group. While the recall rate was better for the DAS password after the first five minutes (96% and 100%), the recall rates were the same at the end of the first week (95% for both). The study also indicated that the complexity of the passwords selected by the BDAS users was significantly higher than those for the DAS users with a t-test indicating $t=2.78$ $p < 0.01$. In spite of the increased complexity and length of the BDAS passwords over the DAS passwords, user performances in both systems were similar. Hence, the researchers concluded that in spite of its apparent increased complexity, the implementation of BDAS helped improve the memorability of DAS passwords.

Goldberg et al [46] proposed the passdoodle technique in which the user produces a small design or text on a touch screen. The researchers used a between-user design with 13 participants using paper prototypes to investigate the viability of the passdoodle scheme in user authentication through an understanding of the memorability and user preferences in comparing the passdoodle scheme to alphanumeric passwords. The study was divided into two login sessions one week apart to create and recall a username and one alphanumeric and one doodle password. Their studies observed that users could accurately remember how they drew complete graphical images, yet mostly forget the sequence in which the various components of the image were initially produced. Hence, the researchers observed that if the restriction of ordered login were removed for subsequent implementations of the passdoodle scheme, it would greatly enhance the usability and memorability of the system.

A further study to analyse the predictability of the DAS password was conducted in [47]. In spite of lacking any predictable patterns, it was discovered that at both the beginning and the end points of the password strokes, some characteristics such as rectangles, letters, numbers and crosses were common and that users generally preferred passwords that were predictable, hence insecure, in favour of memorability. In a paper based study with 16 participants, 10 male and 6 female, aimed at understanding if predictable patterns will appear in the implementation of the DAS password scheme, the researchers discovered that approximately 45% of the users chose symmetric passwords, 2/3 of which were mirror symmetric (reflective). Approximately 80% of users chose passwords composed of 1-3 strokes, 10% chose passwords composed of 4-6 strokes, and 10% of the users chose passwords with 6 or more strokes. With regards to the centering of passwords within grids, 56% of the passwords were centered, an additional 30% more were approximately centered, that is, centered on a set of cells adjacent to the central grid lines.

The signature scheme was proposed in [48]. In this scheme, a user is asked to draw their signature on a grid during the registration stage. The coordinates of this signature are immediately stored on the system and confirmed by a further verification stage before any round of authentication. The success of the scheme was satisfactory, as the users did not have to memorize their signatures. Users could also replicate their signatures with almost exact precision. To understand the distinguishing factors between user and imposter signatures, the researchers developed a set of signature writing parameters such as number of signature points, coordinates of points, signature writing time, velocity and acceleration and used these parameters against user and imposter signatures. The greatest variation was observed in the use of the acceleration parameter. This was then used in the experiments to differentiate user and imposter signatures. The researchers evaluated the system using two experiments; one with a static signature database in which signature data is registered into the system and kept in the system's database during the registration phase. The data is kept and used for user authentication until a new copy of the signature data is again registered onto the system and used to replace previous data. It was however discovered by the researchers that users become more efficient in the use of the scheme as the number of authentication cycles increased. The signatures became more accurate and took less time to write. Hence, in the second experiment, the researchers used a dynamic database in which the signature data in the system's database was changed occasionally and automatically by new signatures written by the users. In the static DB experiment, the successful verification rate was 91%, while the successful rejection rate was 92%, while in the dynamic DB experiment, the successful verification rate was 93% and the successful rejection rate was 96%. The signature scheme, however, needed proficiency with the stylus as well as the need for additional devices. Moreover, some tolerance threshold had to be set as the password is captured. This allows for better usability, while compromising security.

2. Cued Recall Based Systems

In cued recall based systems, a user is required to locate and click on a number of click points chosen earlier on an image. The image itself serves a cue and assists a user to recollect the series of actions carried out, since these actions were all carried out on the image. In pure recall based schemes, activities were done on an empty grid. The idea of click points was first proposed by Blonder [49]. In Blonder's design, an image was displayed on the screen, which had predefined click points. The user had to click on these points to register and do so in the same order anytime they intend to authenticate. However, some tolerance threshold is, provided for each click point. No experimental prototype of Blonder's scheme was ever developed. Hence, no user studies have ever been conducted.

Passlogix [50] developed a scheme based on repetitive actions, which a user had to choose such as preparing a meal or picking of cards as their password. Researchers have also proposed the variation of grid sizes [51] for grid-based systems during each authentication round to improve security. Through a web-based prototype, the researchers reported that the system was 92% resistant to shoulder surfing attacks. No details of experimentation and/or analysis were, however, reported. It was also reported in [52] that Microsoft proposed a graphical scheme in which users click on predefined areas on an image to register and authenticate. However, the details of the system were not, published.

The ideas of Blonder were further improved through the elimination of fixed boundaries and use of different images by Weidenbeck et al [53-55]. In their models, a user was allowed to click on any part of an image in any order to form their password with some tolerance allowed for each click point. The system adopted the quantization method proposed in [56] and with hundreds of click points to click from, it is believed to possess a large password space. The researchers reported an empirical study comparing the use of the PassPoints scheme to alphanumeric passwords. The participants were split into two groups that created and practiced either an alphanumeric or graphical password. The participants subsequently carried out three longitudinal trials to input their password over a period of 6 weeks. The results showed that the graphical password users created valid passwords with fewer difficulties than the alphanumeric users. However, the graphical password users also took longer and made more invalid password inputs than the alphanumeric password users during the practice sessions. In the longitudinal trials, the two groups performed similarly in the memorability of their passwords, but the graphical group took more time to input their passwords. The researchers also observed that an increase in the size of the image increased the number of available click points within the image thereby increasing both the security and usability of the image. The system of cued click points was also developed and studied in [56] as an optimized version of the click based password scheme. In this system, multiple click-based images are used with one click point per image. The next image is based on the previous click point. The system was tested with 24 participants in a lab study, which revealed that the system had considerable promise in both usability and security. From the results, the performance was very good in terms of speed, accuracy, and the error rate. Participants also preferred Cued Click Points (CCP) to PassPoints [55], claiming that selecting and remembering only one point per image was easier, and that seeing each of the images triggered their memory of where the corresponding click point was located. The researchers believed that CCP will provide greater security than PassPoints because the number of images involved increases the workload for attackers. The study, however, suggested further investigation into the memorability (usability) of this system and the problem of hotspots (security) through more elaborate and longitudinal trials. The effect of tolerance and image choice was studied in [54]. The tolerance study was conducted with 32 participants (undergraduate students), 22 males and 10 females. The mean age was 22.7 (SD = 1.33). The participants were divided into two groups with varying tolerance regions (error margins) of 10x10 pixels (.26cm2) and 14x14 pixels (.37cm2). The results showed that accurate memory of the password was greatly reduced when the tolerance was reduced from 14x14 to 10x10. It was observed that small tolerances can greatly increase the space of possible passwords and therefore make the passwords more secure. The nature of the images used in the system may also have a large effect on people's ability to remember their click points. It was observed that allowing users to choose their own images may lead to high memorability for the user, but may also result in images with poor security characteristics such as few click points or high guessability. The study revealed that countless images could be used in the implementation of the passpoints scheme. Further studies conducted in [55] showed that click-based graphical passwords had better security than text passwords, although user training may also take longer. The problem of hotspots in picture-based passwords was studied in [58]. The aim of the study was to explore popular points (hotspots) in click-based passwords and examine the strategies to predict and exploit them in guessing attacks. The researchers reported both short-term and long-term studies. The first was a lab controlled test with 43 participants and 17 diverse images and the second was a field trial involving 223 user accounts. The research discovered that hotspots existed in varying degrees from one image to another. The researchers explored the use of 'human computation' to predict hotspots from images and to generate two 'human seeded' attacks. The first was based on a first-order Markov model while the second was based on an independent probability model. Within 100 guesses, the first- order Markov model based attack reveals 4% of passwords in one image's data set and 10% of passwords in a second image's data set. The independent model based attack reveals 20% of passwords within 233 guesses in one image's data set and 36% of passwords within 231 guesses in a second image's data set. The researchers also evaluated the first-order Markov model based attack with cross-validation of the field study data, which revealed an average of 7-10% of user passwords within three guesses. The research concluded that all click based graphical passwords were predictable and hence vulnerable to online and offline attacks.

According to [52], a system of navigation through a virtual world for authentication was proposed by Adrian Perrig by which users could randomly create virtual environments and be authenticated by navigating through these virtual spaces. Although it is believed to have the potentials of creating strong passwords, there is, however, no documentation for this system. The use of mnemonics to aid recall have also been studied in [12, 59], where the use of mnemonics was incorporated into a number of graphical systems. In [59], a between-users retention test was conducted for multiple passwords for a control group (Group 0) using PIN based password entry, a graphical password group (Group 1), a group with graphical passwords with signature colour background for graphical images to augment

memorability (Group 2), a group with graphical passwords with mnemonic strategy to augment memorability (Group 3) and a group with graphical passwords with mnemonic strategy and colour background to augment memorability (Group 4) where each participant was randomly allocated one of the groups. The study was conducted over a period of four weeks and each participant was allocated five passwords. A total of 172 participants participated in the user study. Due to the high dropout rate, however, only 61 participants completed the study. The dropout rate was highest in group 0 in which some participants thought it was impossible to retain multiple PIN based passwords over a relatively long period of time. Their study results proved the superiority of retention of multiple graphical passwords over multiple PINs and that mnemonics could aid even the recall of multiple graphical passwords. The use of mnemonics and degraded images in a recognition-based system was also studied in [60]. This scheme, which borrowed its ideas from the story scheme, used a trace line across both the user's pass-images and the distractor images, to safeguard against the shoulder- surfing problem. In a between-user study with 20 participants (10 males and 10 females) with an age range of 20 to 30 years, the researchers compared the new scheme called CDS (meaning "Come from DAS and Story" scheme), with the story scheme in two login sessions, an initial session and a follow up session one week later. The mean password creation time was 42.9 seconds for the story scheme and 49.5 seconds for the CDS scheme. The mean login time was 9.2 seconds for the story scheme in the first session and 23.1 seconds in the second session, while it was 13.7 seconds for the CDS scheme in the first session and 19.8 seconds in the second session. The success rate for the CDS was 80% as compared to 60% for the story scheme. However, a comparison of the new scheme with the story scheme in terms of observational attacks, was not conducted in the research.

In several studies, the combination of several graphical passwords has been explored. In [61], the researchers deployed the use of a recognition-based system in the first stage and a recall based system in the second stage of user authentication. A set of questions (three, specifically) were associated with the recall based phase. The questions help the user in knowing their click points as the click sequence is randomized in each authentication round. No user study was reported for this scheme.

D. Hybrid Authentications Schemes

A number of hybrid authentication systems have also been developed. These are systems that combine the elements of recall and recognition based authentication systems or text and graphical authentication systems in order to benefit from the usability and security advantages of both systems [62, 63]. A hybrid system for the generation of session-based passwords was presented in [62] and [64], and extended in [65]. The system combines graphical and text based authentication schemes, and during registration, a user needs to select both a graphical and a text-based password. To authenticate, the user has to correctly enter both the graphical and text based passwords. Two implementations of the system were proposed. In the first implementation, the user is presented with a text grid from which they choose their password from an intersection of the various rows and columns of the grid which represent their password, while the second implementation suggested the ranking of colors, both of which the user has to remember accurately. The mixing of upper and lower case letters and augmentation with special characters was suggested for the text-based password. Although the system is believed to be resistant to most common password security attacks, there is high likelihood that the system will suffer from usability issues. A usability evaluation has, however, not been conducted.

Another hybrid graphical scheme is presented in [63], which incorporates a recognition-based scheme with dynamic graphics. In this scheme, during the registration process, a user is presented with a 4x4 grid of images from which they select their chosen password images. Below each image, however, is a random three digit number, and at the bottom of the image grid is a text box. On selecting an image, the user needs to enter the three digit code for their chosen image in the text box. At the end of the selection of all password images, the textbox contains a string of digits, which represent the user's password that is saved by the system. The user thus has to remember the exact order in which the password images were chosen.

The authentication phase for this system is divided into two phases for each of the chosen password images. In the first phase, the user is presented with a 4x4 grid to select their password images. However, associated with each of the images and below each image is a colour ball. The user has to both recognise each of their chosen images in the grid as well as remember their associated colour balls. The colour balls associated with each image are randomly assigned per authentication session. In the second authentication phase, the user is presented with a 16x1 grid also with a colour ball associated with each of the images. However, the colour ball associated with each image in this grid is randomly reassigned according to a specific timeframe. The user has to recognise their first selected image and its associated colour ball in phase one and click on this image in phase two only at the time when the colour ball bears the same colour as that associated with it in phase one. The user then repeats phase two for all of their remaining images.

In this scheme, when images are presented in the grid for authentication in the first phase, a user is not expected to select any image, but to only observe the

colour of the balls below the images. The actual image selection is done in the second phase. This provides extra security to the system as an onlooker may not even understand that the first phase is actually a part of the authentication process. According to the researchers, the system has a large password space, high entropy and is resistant to most common password intruder attacks. Another parameter that enhances the security of this system is the time window within which a user has to select the image in the second phase when the coloured ball for the image seen in the first phase appears.

According to the researchers, the system had both good usability and good security as it was both easy to use and to remember as well as being resistant to common security attacks. However, one would expect that the need to memorize a set of images selected by the user in the registration phase as well as the colour balls allocated to each of the images in the first authentication phase, as well as the need to interact with two separate grids in the system's authentication phase creates additional burden for the usability of the system.

Many other hybrid graphical authentication systems have also been proposed. In [66], a system that uses shape and text is proposed. The system combines a traditional text based password with a shape drawn on a grid as in the DAS scheme. Although the system is believed to be strong against shoulder surfing and brute force attacks, the researchers themselves agree that the system suffers from several usability flaws. Another hybrid model is presented in [67] which combines a traditional password based authentication system with a recognition based graphical authentication system. The registration phase for the text and graphical passwords are done normally. A user enters their text-basedpassword, which consists of alphanumeric and special characters and then selects a number of images from an image grid. In the authentication phase, the user enters their alphanumeric password and then selects their chosen images from an image grid provided for the selection of the images. The image grid is, however, slightly different from the traditional image grid in which a user needs to click on their password images to select them. In the image grid for this system, below each image is assigned a unique number. This number is randomly assigned and changes in each authentication round. A selection panel is provided at the bottom of the image grid in which the numbers are arranged in ascending order from the smallest to the largest. A user selects an image by clicking on its corresponding digit in the selection panel. Hence, a user does not need to click directly on an image to select it, but to click on the digit that represents it in the selection panel. This is a strong mechanism against shoulder surfing attacks. The selection panel also helps a user keep track of the various pass images already selected, as the selected digits in the selection panel remain highlighted until the end of the authentication process. Although the system is believed to be strong against common password security threats, actual user studies to verify and analyse its security and usability potentials had not been conducted.

E. Two Factor Authentication

Discussed in the previous sections are the various authentication methods through which a legitimate user can authenticate onto a computing device. These include; token based authentication, biometric authentication and knowledge based authentication. Two factor authentication involves the use of any two of these methods in a single authentication system. A typical example is in the use of the bank ATM machine. The ATM smart card serves to provide the user ID and helps the machine understand which account(s) are being accessed. The user then enters their PIN (Personal Identification Number) to show that they are the legitimate owner of the designated account. Several authentication systems have been developed that adopt the two factor paradigm for user authentication. The most common of these systems include the use of smart cards [68] for physical access mechanisms, hardware tokens and OTP (One Time Password) for mobile and online applications. The most common security problem with smart-card based systems is the offline guessing attack [68]. The greatest usability problem associated with multifactor authentication systems is the need to carry additional device(s). Systems that combine biometric authentication such as fingerprint recognition with tokenized devices have also been proposed [69]. In [70], however, a gait based two factor system for mobile devices was proposed. Other researchers have proposed the use of three factor [71] and four factor [72] authentication systems as a means of improving upon the security of two factor authentication techniques. However, this increased complexity may add increased constraints on the usability of the systems.

F. Password Security Threats

A number of threats have significantly affected the use of text-based passwords. The exact extent of the effects of these threats on graphical passwords is not fully understood as the deployment of graphical passwords in real user environments is still undergoing research and is in its infancy. Some of these threats are:

1. Brute Force Attack

Brute force attack is the use of the brute force search algorithm to try all possible combinations of user passwords to gain access to a user's account. Since passwords are a combination of letters, numbers and special symbols, brute force attacks take a considerably long period of time. Hence, having a considerably large password space is a good defense strategy against brute force attacks. Graphical

passwords are believed to be more difficult to compromise than text based techniques as they are believed to possess a similar or sometimes even larger [42, 45, 48, 56] password spaces. Recall based techniques normally have larger password spaces than both the text and recognition based techniques. The dependency on mouse movements makes graphical passwords more resilient to brute force attacks than text-based methods.

2. Dictionary Attack

A dictionary attack is a password security threat in which the attacker repetitively tries a list of words, called a dictionary to gain access to a computing system. Unlike a brute force attack that uses all possible combinations, a dictionary attack uses a list of weak passwords that are insecurely used as passwords by system users. Although it is believed that dictionary attacks could be used against some recall based graphical passwords [48], it is definitely more complex to execute especially as they mostly involve the use of the mouse and not the keyboard.

3. Guessing Attacks

The ability to guess a user's password is common in text passwords and is further simplified by having some information about the user. Forming passwords with the names of family members or pets and known places or dates is therefore highly discouraged. Guessing is also possible in user defined passwords and password systems with predictable patterns such as the passfaces scheme [32] in which users select beautiful faces, faces of the opposite sex and of members of their own race. The DAS system [42] also showed predictability especially in symmetric and non-symmetric images, according to [47].

4. Spyware Attack

Spyware are mischievous programs or devices intended to "spy" or gather sensitive information from any system to which they are attached. They are normally used to spy on persons or organisations and may retransmit the information gathered to a third party. Keyloggers are hardware and software designed to keep track of and automatically log user keystrokes onto external media, while mouse trackers are software and hardware designed to capture and store mouse or cursor movement on the screen. Although, it is believed that keyloggers cannot be used against graphical passwords [30, 31], mouse trackers are seen as a potential risk.

5. Shoulder Surfing Attack

Shoulder surfing is the ability of an intruder to obtain useful password information by simply observing the user's actions from across the user's shoulder. Shoulder surfing is a potential risk in most graphical schemes [30, 31].

6. Smudge Attack

Most android phones and other mobile devices today use a form of authentication called a pattern lock [83] in which a user tracks a set of dots on the screen. The use of this system may sometimes lead to the pattern becoming traceable due the formation of oily deposits on the face of the phone over time. This pattern 'smudge' can be used by attackers as investigated by [73].

7. Social Engineering Attack

Social engineering is the ability to fraudulently obtain useful information from a person through pretext. Social engineers exploit human attributes of love, fear, respect, trust and pity to deceive system users into divulging sensitive information, which they later use to gain access into applications or devices. Phishing is the ability to impersonate an entity such as a bank to obtain personal security details from users. For password systems, however, social engineering is effective only if a user password could be described.

8. Vulnerability to Description

Vulnerability to description is the ability to clearly describe, verbally or in writing, the characteristic features of a user password. Text based passwords can mostly be effectively described, and it is a main concern that many graphical passwords can also be described. Vulnerability to verbal and written descriptions of various image types used as authenticators was studied in [36, 74].

G. The Evaluation of system Security

A visit to any bank, bank related website or ATM machine and one will be overwhelmed with messages asking bank customers to "protect" their accounts, card and token-based information and "not to disclose" any part of it to anyone. They are warned that the bank "will never ask" for sensitive information via telephone and that they should "beware" of persons or websites demanding sensitive banking information from them. Probably the only other message that is communicated along with these is the demand that the customer complies with the banks password policy. These are all messages that are seen every day and are meant for just one goal: to ensure that the bank account user "takes adequate care" of their own part of the security chain. The protection of password entry from keen observers is a counter-measure against observational attacks, the refusal to divulge sensitive account, card or token-based information is a counter- measure against social engineering attacks, while the use of "strong passwords" or password policies is a counter-measure against guessing attacks.

This section provides an overview of some of the main security concerns. These can include guessing attacks, shoulder surfing attacks and vulnerability to descriptions. Guessing attacks can be performed

either randomly (normally called blind guess) or based upon some valid information known to the intruder about the legitimate user (herein called hinted guess). Shoulder surfing or observational attack is the ability of an intruder to steal a user's authentication information by mere observation of the user's login session. Vulnerability to verbal and written description is the susceptibility of an authentication system to be breached by intruders for its reason of being easy to verbally describe or to write down [74]. In such systems, all the intruder needs to do is to obtain a verbal or written description of a user's password and the intruder uses the descriptions to break the password. Vulnerability to description is itself a factor that reflects the vulnerability of an authentication system to social engineering attacks. Social engineering attacks are efforts made by crafty intruders to convince unsuspecting legitimate system users to divulge sensitive security information to allow the intruder gain access to the system. Studies have considered the evaluation of these three security dimensions to be of equal significance in the design and implementation of authentication systems [75].

According to [1], users are the weakest link in the system security chain. Some researchers argue [2, 79] that the idea of users selecting weak passwords is normally due to a lack of motivation in the use of the security systems provided. They believe that the bulk of the problem arises from the way security systems are designed and the lack of proper user orientation on their use.

Analyzing the Guessing Attack:This sectionprovides an insight into the need to provide algorithms that can effectively safeguard against guessing attacks in the design of authentication systems. In most security related literature, system users are always advised on the use of strong passwords to counter online and offline guessing attacks. However, guessing attacks are only possible when password systems are predictable, that is, when predictable patterns exist in password application by system users [80]. In a study in 2010, Zhang et al. found out that 41% of passwords from a university system could be cracked in just under three seconds each, when the cracker has some knowledge of expired passwords from the same account [81]. Predictable patterns in password use arise when users choose passwords that can be easily guessed [82]. Many organizations thus impose password policies to make passwords less predictable [83]. A study was conducted by Rainbow Technologies Inc. on the use of insecure passwords in a sample population of 3000 computing professionals, and it was discovered that most system users used insecure passwords. The need to maintain multiple passwords as well as the need to constantly change passwords had intensified the situation as more than 50% of the surveyed population reported having more than five passwords and more than 80% reported that their organizations had imposed policies forcing them to use 'non-words' as passwords or combinations of numbers and letters. This, in turn had forced the users to write down their passwords. Hence, 51% of the surveyed user population have reported that they need IT support help to gain access to their accounts and applications as they had forgotten their passwords. This trend essentially underscores the contention that has existed between usability and security in authentication systems in which the need to improve one has consistently diminished the other. A study conducted in [84] on the vulnerability of ATM PINs discovered that the mere knowledge of a user's birthday is enough to compromise from 1 out of every 11 to 1 out of every 18 ATM cards. In spite of this, researchers have continued to strive for more efficient password systems and better password policies. According to [85] "One weak spot is all it takes to open secured digital doors and online accounts causing untold damage and consequences". Poorly assigned and poorly used passwords remain the most important causes of password guessing attacks [86] which are among the greatest issues facing authentication systems today [87]. Several graphical based authentication systems have been developed to counter the guessing attack [88, 89, 90].

Since the use of passwords for the maintenance of online accounts is ubiquitous [86] and they are often the first and only line of defence [83], the continued search for a solution to the password guessing problem has become of paramount significance to system security researchers. Since online and offline guessing attacks have utilised various algorithms for text-based searches, researchers have confronted the problem through the use of complex cryptography and other security protocols [90, 91]. However, the idea of using brute force or dictionary attacks may not be applicable in graphical authentication schemes. Nonetheless, the appearance of predicable patterns in the use of most graphical authentication schemes makes them also vulnerable to guessing attacks. Graphical implementations such as the passfaces scheme, the passpoints scheme and even the DAS scheme have been found to have predictable patterns that render them susceptible to guessing attacks [92, 93, 94].

1. Analysing the Shoulder Surfing Problem:

Shoulder surfing is the act of looking over the shoulders of a system user while they are in the process of authentication so as to use the information obtained at a later time to gain access to the user's private resources [10]. This situation can occur typically in an office or busy public places such as shopping malls, bus stations, coffee shops, airports and train stations especially in crowded areas where the attacker takes an advantaged position in order to have a good view of the user's login session to be able to capture their required login details [25]. While keying in alphanumeric passwords on a computer

system, a typical attacker can observe the user's keyboard input from a vantage point. The same applies to PIN entries on ATM machines. In a typical graphical password, however, all the attacker needs to do is to observe the screen, and the user's only defence is to shield the screen during password entry. More complex forms of shoulder surfing include the use of additional devices like binoculars and low power telescopes or a video camera to capture or record user login entry. Apart from advising password users to be conscious of the threat and to shield their systems during password entry, little help can be rendered against shoulder surfing in most authentication systems [95]. Many organisations counter the problem of shoulder surfing through the use of 'two-factor authentication' in which password entry is complemented with the use of hardware tokens [95] that generate random digits to be used alongside traditional authentication methods. Since only the legitimate user possesses the hardware token, attempts toward shoulder surfing become a futile idea. Other systems incorporate mobile technology [96] with traditional password systems such that One-Time-PINs (OTPs), a set of digits, are sent to the user's telephone via the user's registered telephone number, and the OTP is used alongside normal authentication procedures. Shoulder surfing is regarded as one of the greatest concerns of information and computer security researchers since the evolution of text based passwords, it has been researched rigorously [10, 11, 25, 28, 30] and has been the impetus for the development of graphical authentication systems as alternatives to text based passwords [9, 30]. Most graphical authentication systems, however, are still prone to the shoulder surfing attack and this has led to the proliferation of different graphical authentication schemes to curb shoulder surfing as well as the development of various mechanisms to mitigate the shoulder surfing attack. A lot of effort has been put into the search for a promising solution to the shoulder surfing problem over the years, yet truly satisfactory solutions have not been found [25].This is because the search for the solution has opened up other salient issues. One of these is the fact that it is difficult combine security and usability on one system. The quest for more secure systems has rendered systems less usable while the quest for more usable systems has rendered systems less secure. Bridging this gap has continued to elude system security researchers over the years.

2. Description Vulnerabilities and Social Engineering Attacks

Vulnerability to verbaland written descriptions denote the ability of a system user to verbally describe their password to someone else, or to write a description of their password on paper for later use or for the use of another person. The storage of passwords has constituted a serious security issue in the applicability of text-based passwords for the following reasons: 1) it renders the password vulnerable to being stolen and used illegally. 2) It provides fertile grounds for social engineering attacks. Social engineering is the act exploiting human factors to persuade or convince a system user to divulge sensitive security information. Social engineering is considered one of the most serious and effective online attacks [97] and has gained significant academic importance [98]. In social engineering, an attacker pretends to be someone that can be trusted by the user such as their employer, or an employee from their bank to maliciously obtain sensitive information. Social engineering is a common threat in online or web applications. People engaged in social engineering technically rely on knowledge of human psychology to exploit human psychological weakness commonly known as human factors. One of the most common forms of social engineering attacks on the internet is called phishing. Phishing is a situation whereby an attacker uses malicious email or a website to pose as a trustworthy organisation. Phishing is a large threat on the internet and costs internet users and organisations millions of dollars each year [99]. It is estimated that for the year 2007 alone, the global cost of phishing attacks was about three hundred and twenty million dollars ($320m) [100]. Perpetrators of phishing attacks have consistently used malicious applications to pose as banks and financial institutions and use these applications to demand sensitive details from unsuspecting users [101]. This has continued to pose a severe threat to banking applications and institutions. The main problem with phishing attacks, which probably guarantees its success, is that it directly targets the human user.Hence, it is not hindered by all system security protocols [102]. In a study conducted in [103] to evaluate the trends in global phishing attacks in 2006, the researchers discovered that it was becoming a global issue with up to 31 regions being targeted in up to 16 different languages. Gartner [104] conducted a research survey in 2004 that included about 5,000 adult respondents to determine the trend of phishing attacks on US citizens. Extrapolating from the results, Gartner concluded that about 30 million people were absolutely sure they had been victims of a phishing attack, 27 million believed they had received what "looked like" a phishing attack, 35 million were unsure of an attack and 49 million were sure they had no such experience. Based on the statistics, nearly 11 million adults, which represented about 19% of those attacked, had actually clicked on the phishing e-mail, and, more shockingly, about 1.78 million remember providing sensitive personal or financial information to the phishing sites. In fact, the study concluded that U. S. banks and bank card issuers had lost about $1.2 billion in 2003. Gartner acknowledged that phishing attacks were causing a gradual erosion in consumer trust and may slow down U. S. commerce growth by 10% by 2007. Gartner then suggested the use of

phishing antidotes, which include the use of digitally signed emails and the provision of anti-phishing services.

In spite of their seriousness, phishing attacks are not possible if user passwords cannot be described. Hence, [105] suggests that to work against phishing attacks, systems must be developed that take human factors into consideration and be designed to preclude all vulnerability to phishing attacks. Other researchers [106, 107, 108] suggest that since social engineering is a user centered threat, its prevention should include security awareness and alert programs focused directly towards the system users that take into consideration the main security weaknesses that are continuously exploited by the social engineers.

H. Combining Usability and Security

Quite a significant research effort has been made in recent years in the area of graphical authentication systems. Most of this effort has, however, not been put in the development of novel and more secure and usable systems, or in bridging the gap between usability and security in existing systems, but on trying to make existing systems either more usable or more secure [109, 110]. However, some researchers have made the effort to look into the security/usability contention and have come up with a number of suggestions.

The Convex Hull Click (CHC) [25] was designed as a remedy against shoulder surfing attacks, which are prevalent in grid-based models of recognition, based graphical authentications schemes. The system worked by the use of small icons from which a user clicks inside an imaginary triangle formed by any three of the user's pass images. The system could allow a user to authenticate even in the presence of onlookers. Hence, the system greatly improved upon the security of traditional grid based systems. Since the system used many small icons, however, a user had to spend more time to authenticate and this was a usability problem.

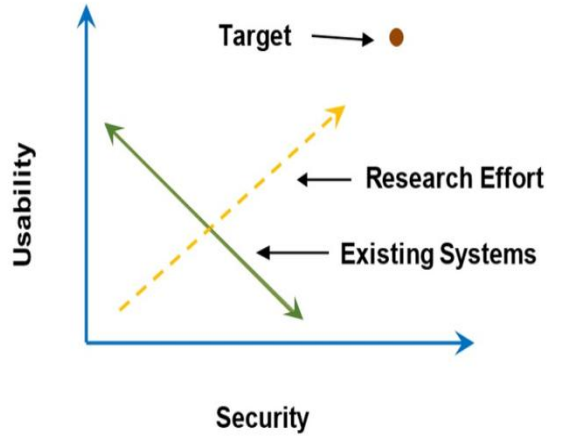

Fig. 1 Usability and Security (Modified from [116])

In the passfaces scheme [32], a suggested solution to the predictability problem [35,110], was the use of system assigned passwords. This improved the security, but reduced memorability, hence making the system less usable. Another enhancement to the passfaces scheme was proposed by [111] in which alphabetic letters were assigned to each of the passfaces images to allow for the replacement of the mouse with the keyboard. To increase usability, passwords were also composed with face images from separate grids of males and females or clowns and kids [112].

Image categorisation has been suggested in [113] where images are subdivided into groups and users select only the groups containing the images they will like to use to authenticate. A user only has to remember the category to which their chosen images belong and not the images themselves. Although the idea sounds plausible, the system is still not very secure. This is because if an intruder knows the image category selected by a user, they can easily recognise any image presented from that category.

The use of image synonyms was proposed in [114]. Image synonyms are varying images of the same object or class of objects. For example, there are different designs and models of a standing fan, and each can represent an image synonym of that object. Although not the same concept, image categorisation and image synonyms suffer the same problems. Anyone who knows that a user's pass image is a flower will likely select any flower presented to him if it is the only flower within the image set. The system will be secure, however, for an observer who observes the dimensions of an image during a user's authentication and will only accept the particular image they had observed.

Since graphical authentication is a new and evolving field [115], new models are being developed continuously with the hope of bridging the gap between usability and security. The target is a system that effectively combines usability and security. For now, no single method can claim to have bridged security and usability to a satisfactory level [54].According to [13] "An ideal authentication system should provide strong security while maintaining high usability – it should be usable everywhere, by everyone, without the need for any specific training".

Figure 1 presents a modified version of the diagram presented in [116] that depicts the trade-off between usability and security. The diagram shows the trade-off between usability and security in existing systems such that improving the security aspects of systems often renders the systems unusable, while improving the usability aspects normally renders the systems unsecure. The target is to design and implement systems that are both highly usable and highly secure, which has been the drive of the research effort in this field. The target is at some intersection of usability and security where both usability and security are considerably high.

III.A CLOSER LOOK AT SOME EXISTING GRAPHICAL MODELS

This section provides an overview of the implementation and analysis of some of the graphical authentication algorithms discussed in the literature. Research in the field of graphical authentication systems has consistently focused on identifying the various usability and security challenges of various implementations through field and lab based experiments using sample user populations. While usability ascertains system strengths and weaknesses in relation to a number of usability metrics which include effectiveness, efficiency and user satisfaction, security has been evaluated through the study of vulnerability parameters such as vulnerability to guessing attacks, vulnerability to shoulder surfing attacks, vulnerability to description, etc. Hence, in this section, some of the most researched graphical authentication models are cross-examined on security and usability in the context of existing literature.

A. The Passpoints Scheme

The passpoints graphical authentication system is a click based graphical authentication system. The system extended the ideas proposed and developed by Blonder [49], which was the pioneering model in the design and implementation of graphical authentication systems. In this system, a user is presented with an image on the computer screen during registration and is expected to select a number of 'click points' from the image in a definite order as their password. The user is then expected to click on these click points in exactly the same order as they did during registration in order to authenticate. The click points scheme is considered a cued recall based system and is one of the most studied graphical authentication systems today [60]. The difference between the new system and the system proposed by Blonder is that this system does not impose any restrictions on click points. The Blonder model provided fixed regions within an image within which a user had to click to select their password. Clicking anywhere outside the regions provided, even though still within the body of the image, is not recognised or recorded by the system. The new model, however, allowed users to click freely from any location within the image to select their passwords.

A study conducted in [54] examined the extent to which tolerance and image choice could affect user performance. Tolerance means the area (in pixels) surrounding a given point selected as password, within which user selection could be accepted as valid. Results of the study revealed that accurate memory of the password was strongly reduced when a small tolerance (10x10 pixels) was used around a user's password points. This happens because memory of the precise location of the user's passpoint reduces as time elapses. Hence, from the usability perspective, it is safe to say that increased tolerance meant increased usability for users. In the study on image choice, four images of everyday objects were used. The study revealed few significant differences in user performance between the images used. The study also revealed that many images may support memorability in click based graphical password systems.

The performance of the passpoints based system in comparison to other authentication systems has also been studied. In a study conducted in [55], the usability of the passpoints scheme was compared to that of alphanumeric passwords. Study participants were divided into two groups and asked to create and use passwords with passpoints and alphanumeric text over a period of six weeks. Study results indicated that users created their passwords with less difficulty while using graphical passwords. During the practice stage, however, users of the passpoints scheme took longer to login to their systems and made more errors than those with the text-based passwords. The two groups performed similarly in terms of memorability in the longitudinal trials, although the graphical system users took more time to login. Although the study results indicate the tendency for improved usability in the use of the passpoints scheme over alphanumeric passwords, this was in contrast to the results that compared the usability of both systems.

The best images suitable for click based passwords and the passpoint selection choices made by users was studied in [117]. The model predicts the probability of the likely click points of users to help predict the entropy of click points in the graphical password formed from a given image. The model also allows the evaluation of the suitability of an image for use in a click based graphical password helping to analyse the possibility of dictionary attacks on the system. In the study, predictions made using the model were compared to the choices made by actual human users. The study revealed that user choices could be modelled and were thus predictable. The study suggests further work along this direction to help improve the security of click based passwords. The study is further corroborated by another study in [110] that investigated the presence of predictable patterns in click based authentication systems. This study further confirmed that user interface design in graphical authentication systems could encourage secure or insecure behaviour among users and that user-selected passwords varied considerably in their predictability. The analysis of user selected click points among various image types suggests that click points were predictable. The study also investigated the implementations of the Cued Click Points (CCP) [57] and Persuasive Cued Click Points (PCCP) [118] algorithms and realized that they were indistinguishable from those of a randomly generated simulated dataset. These results indicated that these extended models of the passpoints scheme were less susceptible to guessing attacks than the original model.

Research in [93] studied the effect of multiple password interference on the usability of textual and click based graphical passwords. In this one-hour (short-term) laboratory study, the researchers aimed at comparing the recall of multiple text based passwords to the recall of multiple click-based passwords. The researchers concluded that users of the multiple click-based passwords did significantly better than those with text based passwords. The users of the click-based passwords made fewer errors than those with text passwords and did not engage in insecure behaviour such as the use of passwords directly related to account names and the use of the same passwords across multiple accounts as found in those with text-based passwords. After a period of two weeks, the researchers observed that the login success rates were not statistically different for both participant groups, yet the group with the graphical passwords made less recall errors than those with text passwords. The study confirmed that those with multiple click-based passwords were less susceptible to password interference in the short term, but had similar usability with text-based passwords in other respects.

B. The Passfaces Scheme

The passfaces scheme is a recognition based graphical authentication scheme developed by Real User Inc. [32] and commercialized in the year 2000. The system was developed as a form of two-factor authentication to be used alongside traditional text based authentication systems. The system also offers two way authentication composed of user-to-site and site-to-user to mitigate against phishing attacks. While using the passfaces scheme, a system user first goes through the registration phase, in which they are asked to select a number of face images from a large image pool. In each subsequent authentication round, they are presented with an image grid containing one of their chosen images and eight decoy images. The user is expected to recognise and select their pass-image for each step in the order in which they had selected them in the registration phase.

A significant body of research has been conducted on the passfaces scheme. A study reported in [35] compared the performance of the passfaces scheme with that of alphanumeric passwords. The study used 34 students in a three months field trial. The researchers recorded fewer login errors in the passfaces scheme than in the alphanumeric passwords, indicating that the Passfaces scheme had better memorability than the passwords. However, the researchers also reported that the passfaces system took a longer time to execute than the passwords, and hence users of the passfaces scheme took longer times to commence their jobs. This in turn created a motivational problem for users of the passfaces scheme as they logged in to the system less often than those that used the passwords.

The study also reported an earlier study by T. Valentine involving 77 staff and students of Goldsmith's College, University ofLondon, to study the memorability of the passfaces scheme. All study participants used the passfaces scheme to test three conditions. For the first condition, 29 participants were asked to login to the system every working day continuously for a period of 2 weeks. These participants remembered their passwords in 99.98% of logins. The second condition used 29 participants to login after about 7 days of the initial enrolment. Most (83%) of the participants were able to login on their first attempt. Everyone was, however, able to login on the third attempt. For the third condition, 19 participants were asked to login once after about 30 days of the initial enrolment. In this condition too, 84% of the participants were able to login on their first attempt, while others were able to login by their third attempt. The passfaces scheme was also tested against long-term recall as the study participants were asked to login to the systems after more than five months of their last use. From the actual study participants, 56 participants were able to participate in the follow up trial, 72% were able to login on their first attempt and 84% by the third attempt. The study also reported that the participants that used the everyday login condition could remember their passwords the best, with 87% remembering the passwords in the first attempt and 100% remembering them in the third attempt.

Researchers in [36] conducted a study to ascertain the susceptibility of images in the passfaces scheme to verbal and written descriptions. The study sought to evaluate approaches by which such vulnerabilities (if they existed) could be reduced as well as to understand if any predictable patterns did exist between how male and female participants described and interpreted the descriptions of facial images. In this study, 45 facial images were obtained from the passfaces website and grouped into three subgroups. The first group contained images that were placed at random, without any consideration. The second group contained images placed together due to visual similarities to a target face image and the third group contained images placed together due to written similarities to a target face image. The study discovered that the study participants did worse in distinguishing a target image where images were grouped based on visual and verbal similarities. The study suggested that the passfaces scheme could be further secured by grouping images due to verbal and written similarities. Subtle differences were also uncovered between male and female groups in relation to how they describe images and how they interpret the descriptions of others.

Researchers in [119] conducted a three week study to compare the usability of passfaces and PINs among older and younger adults. In the study, two test groups of older and younger adults were deployed to use a PIN based system for a time, and then use two

face-based graphical authentication systems of young versus old faces. Although, as expected the younger study group performed better in all the authentication systems provided, the older user group did considerably better in recognizing the older faces in the graphical systems. The study suggested that an age-appropriate implementation of the passfaces scheme will yield better usability among different age-related user groups.

C. Abstract Images (Déjà vu)

The déjà vu scheme used abstract images for user authentication and was proposed by Dhamija and Perrig [4]. It is another well researched recognition based graphical authentication system. Déjà vu was proposed to mitigate the issues of text based authentication systems especially in terms of memorability, as it is believed that humans have an excellent ability to remember previously seen images. The researchers implemented the déjà vu scheme to conduct a user study that compares it to text-based passwords.

In the déjà vu scheme, a user creates their image portfolio by selecting five images from a large set of images [25]. To authenticate, the system presents the user with a 'challenge set', an image grid, of 25 images, 5 of which are the user's password images and the rest 20 are decoy images. All the user needs to do to authenticate is to locate and click on their five pass images. In order to prevent the existence of predictable patterns in image selection, the researchers used Andrej Bauer's Random Art to generate random art images. Given an initial seed, the system generates a mathematical formula, which defines the colour value of each pixel in the image plane. The system does not store the images, but uses the stored seed to regenerate the image whenever needed. The researchers chose to use abstract images generated from the seeds to improve the security of the system, as users are unable to describe their images to others.

The research findings indicated that 90% of the users were able to successfully authenticate with déjà vu throughout the user study as opposed to 70% for traditional passwords. The researchers outlined potential areas for the application of the déjà vu scheme on PDAs, ATM machines and websites. The main drawback of the system was the need for the server to store the seed for each of the images that form the user's portfolio.

As reported in [25], a comparative evaluation was carried out between déjà vu, six character alphanumeric password and four digit PINs to compare the usability of each of these schemes. After initial training in password selection and the authentication procedure, participants using the déjà vu scheme using pictures and abstract images were all able to login successfully, while users of the alphanumeric passwords and PINs both realized 5% failure rates. In a follow-up trial a week later, déjà vu users with pictures and abstract images realized 5% and 10% failure rates respectively, while the users of PINs and alphanumeric text realized 30% and 35% failure rates respectively. In spite of the advantage in memorability, déjà vu had a relatively lower efficiency as it took approximate 30 seconds to login.

IV. CONCLUSIONS

This paper achieves a considerable review of available literature on the design, implementation and research trends in graphical authentication. This paper has also provided insight into existing security concerns brought about by either system design or user behaviour. Although some systems have done considerably better than others in terms of both security and usability, it is important to note that from the details presented in the current literature, no existing system is devoid of either security or usability issues that need to be addressed.

Therefore, there is still a strong need to discover methods or approaches to authentication that can be both highly usable and very secure. New prototypes would need to be developed and evaluated for their security and usability. One possible approach is to bridge some of the shortcomings in some of the systems discussed above by developing more hybrid approaches that aim to remove the current security and usability shortcomings. Hence, we suggest a more user centric approach to security by providing a system that can effectively mitigate the security issues that relate to user behaviour, while still providing good usability [76, 77, 78]. The success of such systems will guarantee that organisations do not have to worry about what legitimate system users might do to jeopardize the security of their accounts or the entire system.

Furthermore, some of the studies discussed above appear to indicate that the proposed approaches have not been evaluated rigorously enough. We therefore propose that any future work in this area must document clearly rigorous evaluations that cover both the security aspects and usability issues that affect many users.

REFERENCES

[1] S. Patrick, A. C. Long and S. Flinn "HCI and Security Systems," presented at CHI, Extended Abstracts (Workshops). Ft. Lauderdale, Florida, USA, 2003.

[2] A. Adams, and M. A. Sasse, "Users are not the enemy". Communications of the ACM, 42(12), 40-46, 1999.

[3] M. A. F. Al-Husainy and R. A. Malih "Using Emoji Pictures to Strengthen the Immunity of Passwords against Attackers" European Scientific Journal vol.11, No.30 October 2015

[4] R. Dhamija and A Perrig "Déjà Vu-A User Study: Using Images for Authentication" In USENIX Security Symposium vol. 9, August, 2000.

[5] W. C. Summers and E. Bosworth, "Password policy: the good, the bad, and the ugly," In Proceedings of the winter international symposium on Information and communication technologies, Cancun, Mexico, 2004.

[6] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano. "The quest to replace passwords: a framework for

comparative evaluation of web authentication schemes". In IEEE Symposium on Security and Privacy, 2012
[7] A. Jain, L. Hong, and S. Pankanti, "Biometric identification," Communications of the ACM, vol. 33, pp. 168-176, 2000.
[8] R. N. Shepard, "Recognition memory for words, sentences, and pictures," Journal of Verbal Learning and Verbal Behavior, vol. 6, pp. 156-163, 1967.
[9] S. Saeed and M. S. Umar. "A hybrid graphical user authentication scheme." In Communication, Control and Intelligent Systems (CCIS), (pp. 411-415). IEEE. November, 2015.
[10] P. Dunphy, A. P Heiner, and N Asokan. "A closer look at recognition based graphical passwords on mobile devices". In Proceedings of the Sixth Symposium on Usable Privacy and Security (p. 3). ACM, July, 2010.
[11] C. Singh and L. Singh "Investigating the Combination of Text and Graphical Passwords for a more secure and usable experience". International Journal of Network Security & Its Applications (IJNSA), 3(2), March 2011.
[12] S. Chowdhury, R. Poet and L. Mackenzie. "A study of mnemonic image passwords." In Privacy, Security and Trust (PST), 2014 Twelfth Annual International Conference on, pp. 207-214. IEEE, 2014.
[13] E. Hayashi, R Dhamija, N. Christin, and A. Perrig. "Use your illusion: secure authentication usable anywhere". In Proceedings of the 4th Symposium on Usable Privacy and Security (pp. 35-45). ACM, July, 2008.
[14] B. Coskun and C. Herley "Can "Something You Know" Be Saved?" In ISC (Vol. 8, pp. 421-440). September, 2008.
[15] A. De Luca, M. Denzel and H. Hussmann "Look into my eyes!: Can you guess my password?." In Proceedings of the 5th Symposium on Usable Privacy and Security (p. 7). ACM. July, 2009.
[16] D. Gafurov, E. Snekkenes and P. Bours "Spoof attacks on gait authentication system". IEEE Transactions on Information Forensics and Security, 2(3), Special Issue on Human Detection and Recognition. 2007
[17] M. Babaeizadeh, M. Bakhtiari and A. M. Mohammed "Authentication Methods in Cloud Computing: A Survey" Research Journal of Applied Sciences, Engineering and Technology 9(8): 655-664, 2015
[18] E. Hayashi and J. I. Hong, "A Diary Study of Password Usage in Daily Life," In Proceedings of the 29th Annual Conference on Human Factors in Computing Systems, Vancouver, BC, Canada, May 2011.
[19] M. D. H. Abdullah, A. H. Abdullah, N. Ithnin, and H. K. Mammi, "Towards identifying usability and security features of graphical password in knowledge based authentication technique". In Modeling & Simulation. AICMS 08. Second Asia International Conference on (pp. 396-403). IEEE, May 2008.
[20] G. Devansh "A new approach of authentication in graphical systems using ASCII submission of values."Wireless Communications and Mobile Computing Conference (IWCMC), 2017 13th International. IEEE, 2017.
[21] H. Zhao and X. Li "S3PAS: A scalable shoulder-surfing resistant textual-graphical password authentication scheme." In Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on (Vol. 2, pp. 467-472). IEEE, May 2007.
[22] S. Saeed and M. S. Umar. "A hybrid graphical user authentication scheme." In Communication, Control and Intelligent Systems (CCIS), (pp. 411-415). IEEE. November, 2015.
[23] A. Perrig and D. Song, "Hash Visualization: A New Technique to Improve Real-World Security", In Proceedings of the 1999 International Workshop on Cryptographic Techniques and E-Commerce, 1999.
[24] S. Akula and V. Devisetty, "Image Based Registration and Authentication System," In Proceedings of Midwest Instruction and Computing Symposium, 2004.
[25] S. Wiedenbeck, J. Waters, L. Sobrado, and J. C. Birget "Design and evaluation of a shoulder-surfing resistant graphical password scheme." In Proceedings of the working conference on Advanced visual interfaces (pp. 177-184). ACM, May 2006.
[26] D. Weinshall and S. Kirkpatrick, "Passwords You'll Never Forget, but Can't Recall," In Proceedings of the Conference on Human Factors in Computing Systems (CHI). Vienna, Austria: ACM, pp. 1399-1402., 2004
[27] L. Sobrado and J. C. Birget, "Graphical passwords", The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4, 2002.
[28] F. Tari, A. Ozok and S. H. Holden. "A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords". In Proceedings of the second symposium on Usable privacy and security (pp. 56-66). ACM. July, 2006.
[29] R. Poet and K. Renaud. "A Mechanism for Filtering Distractors for Graphical Passwords". In 13th Conference of the International Graphonomics Society Melbourne, Australia, volume 11, pg 14, 2007
[30] S. Man, D. Hong, and M. Mathews, "A shoulder surfing resistant graphical password scheme – WIW" in Proceedings of International conference on security and management. Las Vegas, NV, 2003.
[31] D. Hong, S. Man, B. Hawes, and M. Mathews, "A password scheme strongly resistant to spyware," in Proceedings of International conference on security and management. Las Vergas, NV, 2004.
[32] Passfaces: Two factor authentication for the enterprise". [Available online] at www.realuser.com, (Accessed July 2015)
[33] T. Valentine, "An evaluation of the Passface personal authentication system," Technical Report, Goldsmiths College, University of London, 1998.
[34] T. Valentine, "Memory for Passfaces after a Long Delay," Technical Report, Goldsmiths College, University of London, 1999.
[35] S. Brostoff and M. A. Sasse, "Are Passfaces more usable than passwords: a field trial investigation," in People and Computers XIV - Usability or Else: Proceedings of HCI. Sunderland, UK: Springer-Verlag, 2000.
[36] P. Dunphy, J. Nicholson, and P. Olivier. "Securing passfaces for description." In Proceedings of the 4th symposium on Usable privacy and security, pp. 24-35. ACM, 2008.
[37] W. Jansen, "Authenticating Mobile Device Users through Image Selection," in Data Security, 2004.
[38] W. Jansen, S. Gavrila, V. Korolev, R. Ayers, and R. Swanstrom, "Picture Password: A Visual Login Technique for Mobile Devices," National Institute of Standards and Technology Interagency Report NISTIR 7030, 2003.
[39] W. A. Jansen, "Authenticating Users on Handheld Devices," in Proceedings of Canadian Information Technology Security Symposium, 2003.
[40] T. Takada and H. Koike, "Awase-E: Image-based Authentication for Mobile Phones using User's Favorite Images," In Human-Computer Interaction with Mobile Devices and Services, vol. 2795 / 2003: Springer-Verlag GmbH, 2003, pp. pp. 347 - 351.
[41] X. Suo, Y. Zhu and G. S. Owen Graphical passwords: A survey. In 21st annual Computer security applications conference (pp. 10-pp). IEEE, 2005.
[42] I. H. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The Design and Analysis of Graphical Passwords," In Proceedings of the 8th USENIX Security Symposium, 1999.
[43] J. Thorpe and P. C. v. Oorschot, "Graphical Dictionaries and the Memorable Space of Graphical Passwords," In Proceedings of the 13th USENIX Security Symposium. San Deigo, USA: USENIX, 2004.
[44] J. Thorpe and P. C. van Oorschot, "Towards Secure Design Choices for Implementing Graphical Passwords," in 20th Annual Computer Security Applications Conference (ACSAC). Tucson, USA. IEEE, 2004.
[45] P. Dunphy, and J. Yan. "Do background images improve Draw a Secret graphical passwords?" In Proceedings of the

14th ACM conference on Computer and communications security, pp. 36-47. ACM, 2007.
[46] J. Goldberg, J. Hagman, and V. Sazawal, "Doodling Our Way to Better Authentication," In Proceedings of Human Factors in Computing Systems (CHI), Minneapolis, Minnesota, USA, 2002.
[47] D. Nali and J. Thorpe, "Analyzing User Choice in Graphical Passwords," Technical Report, School of Information Technology and Engineering, University of Ottawa, Canada, May 2004.
[48] A. F. Syukri, E. Okamoto, and M. Mambo, "A User Identification System Using Signature Written with Mouse," In Third Australasian Conference on Information Security and Privacy (ACISP): Springer- Verlag Lecture Notes in Computer Science (1438), pp. 403441, 1998
[49] G. E. Blonder, "Graphical passwords," in Lucent Technologies, Inc., Murray Hill, NJ, U.S. Patent, Ed. United States, 16.
[50] M. R. Albayati and A. H. Lashkari. "A New Graphical Password Based on Decoy Image Portions (GP-DIP). In International Conference on Mathematics and Computers in Sciences and in Industry (MCSI), 2014 (pp. 295-298). IEEE. September, 2014.
[51] A. H Lashkari, A. Gani, L. G Sabet, & S. Farmand "A new algorithm on Graphical User Authentication (GUA) based on multi-line grids" In Scientific Research and Essays, 5(24), 3865-3875., 2010.
[52] D. Paulson, "Taking a Graphical Approach to the Password," Computer, vol. 35, pp. 19, 2002.
[53] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Basic results," In Human-Computer Interaction International (HCII 2005). Las Vegas, NV, 2005.
[54] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Effects of tolerance and image choice," In Symposium on Usable Privacy and Security (SOUPS). Carnegie-Mellon University, Pittsburgh, 2005.
[55] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system, "International Journal of Human Computer Studies 63(1), 102-127, 2005 .
[56] J. C. Birget, D. Hong, and N. Memon, "Robust discretization, with an application to graphical passwords," Cryptology ePrint archive, 2003.
[57] S Chiasson, van P. C. Oorschot, and R. Biddle. "Graphical password authentication using cued click points". In Computer Security–ESORICS 2007 (pp. 359-374). Springer Berlin Heidelberg, 2007.
[58] P. C. van Oorschot and J. Thorpe. "Exploiting predictability in click-based graphical passwords", Journal of Computer Security: 19(4):669–702, 2011.
[59] W. Moncur, and G. Leplâtre. "Pictures at the ATM: exploring the usability of multiple graphical passwords". In Proceedings of the SIGCHI conference on Human factors in computing systems (pp. 887-894). ACM. April, 2007.
[60] H. Gao, Z. Ren, X. Chang, X. Liu and U. Aickelin, "A New Graphical Password Scheme Resistant to Shoulder-Surfing", International Conference on Cyberworlds. 2010, IEEE: Singapore pp. 194 – 199, 2010.
[61] A. Haque and B. Imam "A New Graphical Password: Combination of Recall and Recognition Based Approach" International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol: 8, No:2, 2014
[62] M. Sreelatha, M. Shashi, M. Anirudh, et al. "Authentication schemes for session passwords using color and images." In International Journal of Network Security & Its Applications, 3(3), 111-119. 2011.
[63] S. Saeed and M. S. Umar "A hybrid graphical user authentication scheme". In Communication, Control and Intelligent Systems (CCIS), (pp. 411-415). IEEE, November 2015.
[64] N. P. Sachin, D. V. Panjabi "An Overview: Passwords using Text, Color and Images Techniques Discussion, Implementation and Comparison". In International Journal of Computer Applications (0975 – 8887) National Conference on Emerging Trends in Computer Technology NCETCT, 2014.
[65] M. S. Tidke, M. N. Khan and M. S. Balpande "Password Authentication Using Text and Colors." Computer Engineering, Rtm Nagpur University, MietBhandara. 2015.
[66] Z. Zheng, X. Liu, L. Yin and Z. Liu "A Hybrid Password Authentication Scheme Based on Shape and Text". JCP, 5(5), 765-772. 2010
[67] P. C. Van Oorschot, and T. Wan "TwoStep: An Authentication Method Combining Text and Graphical Passwords". MCETECH, 233-239. 2009.
[68] G. Yang, D. S. Wong, H. Wang and X. Deng "Two-factor mutual authentication based on smart cards and passwords" Journal of Computer and System Sciences, 74(7), 1160-1172, 2008.
[69] A. T. B. Jin, D. N. C. Ling and A. Goh, "Biohashing: two factor authentication featuring fingerprint data and tokenized random number." Pattern recognition, 37(11), 2245-2255., 2004.
[70] T. Hoang and D. Choi "Secure and privacy enhanced gait authentication on smart phone" The Scientific World Journal, 2014.
[71] S. Abu-Nimeh, "Three-Factor Authentication." In Encyclopedia of Cryptography and Security (pp. 1287-1288), Springer, US. 2011.
[72] J. Brainard, A. Juels, R. L Rivest, et al. "Fourth-factor authentication: somebody you know". In Proceedings of the 13th ACM conference on Computer and communications security (pp. 168-178). ACM. October, 2006.
[73] E. von Zezschwitz, A. Koslow, A. De Luca and H. Hussmann. "Making graphic-based authentication secure against smudge attacks". In Proceedings of the International Conference on Intelligent User Interfaces 277–286., 2013.
[74] S. Chowdhury, R. Poet, and L. Mackenzie "Exploring the Guessability of Image Passwords Using Verbal Descriptions". In Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on (pp. 768- 775). IEEE, July 2013.
[75] 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, 63(1), 128-152. 2005
[76] M. E. Zurko and R. T. Simon "User-centered security". In Proceedings of the 1996 workshop on new security paradigms (pp. 27-33). ACM. September, 1996.
[77] M. A. Sasse, S. Brostoff, and D. Weirich "Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security." BT technology journal, 19(3), 122-131. 2001.
[78] S. L. Pfleeger, M. A. Sasse and A. Furnham "From weakest link to security hero: Transforming staff security behavior." Journal of Homeland Security and Emergency Management, 11(4), 489-510. 2014.
[79] A. Adams and M. A. Sasse "Users are not the enemy". In Communications of the ACM, 42(12), 40-46. 1999.
[80] K. Renaud, P. Mayer, M. Volkamer, and J. Maguire "Are graphical authentication mechanisms as strong as passwords?" In Federated Conference on Computer Science and Information Systems (FedCSIS), (pp. 837-844). IEEE, September 2013.
[81] S. Komanduri, R. Shay, P. G. Kelley et al. "Of passwords and people: measuring the effect of password-composition policies." In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 2595-2604). ACM. May, 2011
[82] L. Lamport "Password authentication with insecure communication" In Communications of the ACM, 24 (11), 770-772. 1981.
[83] W. C. Summers and E. Bosworth. "Password policy: the good, the bad, and the ugly." In Proceedings of the winter international symposium on Information and communication technologies, pp. 1-6. Trinity College Dublin, 2004.

[84] J. Bonneau, S. Preibusch and R. J. Anderson "A Birthday Present Every Eleven Wallets? The Security of Customer-Chosen Banking PINs". In Financial Cryptography (Vol. 7397, pp. 25-40). March, 2012

[85] B. Ives, K. R. Walsh and H. Schneider "The domino effect of password reuse." In Communications of the ACM, 47(4), 75-78. 2004.

[86] M. Golla, D. V. Bailey and M. Dürmuth "I want my money back! Limiting Online Password-Guessing Financially." In Symposium on Usable Privacy and Security (SOUPS). July, 2017.

[87] G. C. Kessler "Passwords – strengths and weaknesses" Online Available at https://www.garykessler.net/library/password.html Accessed October, 15th 2017.

[88] L. Gong "Optimal Authentication Protocols Resistant to Password Guessing Attacks." In Proceedings of the Computer Security Foundations Workshop, 1995. Eighth IEEE (pp. 24-29). IEEE. June, 1995.

[89] P. Biswas, M. M. Patil, and M. Biswas "Reduction of Password Guessing Attacks using Click Point". In International Journal of Computer Applications (IJCA) (0975 – 8887) Proceedings on Emerging Trends in Electronics and Telecommunication Engineering (NCET). 2013.

[90] T. Kwon and J. Song "Efficient and secure password-based authentication protocols against guessing attacks" Computer communications, 21(9), 853-861, 1998.

[91] S. M. Bellovin and M. Merritt "Encrypted key exchange: Password-based protocols secure against dictionary attacks" In Research in Security and Privacy, 1992. Proceedings, 1992 IEEE Computer Society Symposium on(pp. 72-84). IEEE. May, 1992.

[92] H. K. Sarohi, and F. U. Khan "Graphical password authentication schemes: current status and key issues". Int. Journal of Engineering and Innovative Technol. (IJEIT), 10(2). 2013.

[93] S. Chiasson, A. Forget, E. Stobert et al., "Multiple password interference in text passwords and click-based graphical passwords" In Proceedings of the 16th ACM conference on Computer and communications security (pp. 500-511). ACM. November, 2009.

[94] K. Chalkias, A. Alexiadis, and G. Stephanides "A multi-grid graphical password scheme" In Proceedings of the 6th International Conference on Artificial Intelligence and Digital Communications, Thessaloniki, (pp. 1-11). Greece, August, 2006.

[95] A. H. Lashkari, S. Farmand, D. Zakaria et al. "Shoulder surfing attack in graphical password authentication."arXiv preprint arXiv:0912.0951. 2009.

[96] F. Aloul, S. Zahidi and W. El-Hajj "Two factor authentication using mobile phones." In Computer Systems and Applications, 2009. AICCSA 2009. IEEE/ACS International Conference on (pp. 641-644). IEEE. May, 2009.

[97] K. Krombholz, H. Hobel, M. Huber, and E. Weippl "Advanced social engineering attacks" In Journal of Information Security and applications, 22, 113-122. 2015.

[98] K. Ivaturi and L. Janczewski "A taxonomy for social engineering attacks." In International Conference on Information Resources Management. Centre for Information Technology, Organizations, and People. June, 2011.

[99] R. B. Basnet, S. Mukkamala, and A. H. Sung "Detection of Phishing Attacks: A Machine Learning Approach" In Soft Computing Applications in Industry, 226, 373-383. 2008.

[100] A. Ross et al. "Measuring the cost of cybercrime" In 11th Workshop on the Economics of Information Security, Berlin, Germany. June, 2012.

[101] S. Garera, N. Provos, M. Chew and A. D. Rubin "A framework for detection and measurement of phishing attacks." In Proceedings of the 2007 ACM workshop on Recurring malcode (pp. 1-8). ACM. November, 2007.

[102] J. Hong "The Current state of phishing attacks" In Communications of the ACM, 55(1), 74-81. 2012.

[103] Z. Ramzan, and C. Wüest "Phishing Attacks: Analyzing Trends in 2006" In CEAS. August, 2007.

[104] A. Litan "Phishing attack victims likely targets for identity theft" Online available at https://www.social-engineer.org/wiki/archives/IdTheif/IdTheif-phishing_attack.pdf Accessed 15 November, 2017.

[105] M. Jakobsson "Modeling and preventing phishing attacks" In Financial Cryptography (Vol. 5). February, 2005.

[106] P. P. Ray "Ray's scheme: Graphical password based hybrid authentication system for smart hand held devices." In Journal of Information engineering and Applications, 2(2), 1-12. 2012.

[107] N. A. G. Arachchilage and S. Love "Security awareness of computer users: A phishing threat avoidance perspective" Computers in Human Behavior, 38, 304-312. 2014.

[108] F. A. Aloul "Information security awareness in UAE: A survey paper." In Internet Technology and Secured Transactions (ICITST), 2010 International Conference for (pp. 1-6). IEEE. November, 2010

[109] M. Masrom, F. Towhidi, and A. H Lashkari. "Pure and cued recall-based graphical user authentication". In 3rd International Conference on Application of Information and Communication Technologies, 2009. AICT 2009. (pp. 1-6). IEEE, October 2009.

[110] A. H. Lashkari, R. Saleh, F. Towhidi, and S. Farmand. "A complete comparison on Pure and Cued Recall-Based Graphical User Authentication Algorithms". In Second International Conference on Computer and Electrical Engineering. 2009; Volume 1():527 - 542. IEEE., 2009

[111] S. Chiasson, A. Forget, R. Biddle, and P. C van Oorschot. "User interface design affects security: Patterns in click-based graphical passwords". International Journal of Information Security, 8(6), 387-398. 2009.

[112] F. Towhidi, M. Masrom and A. A. Manaf. "An enhancement on Passface graphical password authentication". Journal of Basic and Applied Scientific Research, vol. 2, no. 2, 2013

[113] R. English, "Modelling the security of recognition-based graphical password schemes," PhD Thesis, School of Computing Science, University of Glasgow., Glasgow, 2012.

[114] J. W. Sparks, "The Impact of Image Synonyms in Graphical-Based Authentication Systems" PhD Thesis, College of Engineering and Computing, Nova Southeastern University, Florida, USA, March 2015.

[115] Y. Meng, and L. Wenjuan. "Enhancing click-draw based graphical passwords using multi- touch on mobile phones." In IFIP International Information Security Conference, pp. 55-68. Springer, Berlin, Heidelberg, 2013.

[116] R. Biddle, S. Chiasson and P. C. Van Oorschot "Graphical passwords: Learning from the first twelve years. ACM Computing Surveys (CSUR), 44(4), 19. 2012

[117] A. E. Dirik, N. Memon and J. C. Birget "Modeling user choice in the PassPoints graphical password scheme" In Proceedings of the 3rd symposium on Usable privacy and security (pp. 20-28). ACM. July, 2007

[118] S. Chiasson, E. Stobert, A. Forget et al. "Persuasive cued click-points: Design, implementation, and evaluation of a knowledge-based authentication mechanism." In IEEE Transactions on Dependable and Secure Computing, 9(2), 222-235., 2012.

[119] J. Nicholson, L. Coventry and P. Briggs "Age-related performance issues for PIN and face-based authentication systems." In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 323-332). ACM. April, 2013.