Graphical authentication – an alternative to textual based authentication

Payel Bandyopadhyay
Department of Computer Science
University of Helsinki
Helsinki, Finland
Payel.Bandyopadhyay@cs.helsinki.fi

Abstract—Text based password consists of alphanumeric and special characters, which we often use while maintaining user accounts. But these text based passwords are often very difficult to remember and are vulnerable to various types of attacks. So researchers have come up with various alternatives to text based passwords, out of which graphical authentication is one of them. In this paper, I will be concentrating on graphical authentication as an alternative to text-based authentication. Graphical authentication contain images as a replacement to alphanumeric and special characters. Graphical password systems are also further categorised into recall, recognition and cued recall based systems. In this paper, I will be presenting a thorough survey of these three systems and also the possible attacks and drawbacks associated with these systems. At the end, I will also be presenting various new type of graphical systems that have been invented recently and will describe their advantages and disadvantages.

Keywords—Graphical authentication, Pure recall based systems, Recognition based systems, Cued recall based systems

I. INTRODUCTION

In today’s technological world, computers have gained prime importance in our lives. People always tend to keep their information secure. Obviously, we won’t be comfortable in sharing all our confidential work or information with others. So, to protect our confidential data we use passwords, which previously were only text-based means containing only alphanumeric and special characters. Passwords are used to protect ATM logins, computer logins, online account logins, folder logins and in many areas. But nowadays, a single user has numerous accounts online, uses more than one computer at the same time (like one for official purpose, one for personal purpose). Hence, each user has to maintain a lot of passwords which causes memorability issue [1] i.e. users tend to forget passwords frequently. Study results [2] have shown that, due to increasing number of passwords that each user has to maintain and also due to memorability issue, users rarely choose passwords that are difficult to guess and can be easily remembered at the same time. Hence, researchers have proposed alternatives to these text-based passwords. The three alternatives that have been found out are token based authentication, biometric based authentication and graphical based authentication.

In this paper, I will be focusing on graphical authentication as an alternative to text based authentication. Graphical authentication systems use pictures instead of alphanumeric and special characters as passwords. Dual coding theory [3] has shown the difference between visual and textual memory. The theory states that textual memory requires additional processing, so it is difficult to remember while images are easily memorised. Hence, graphical authentication have been invented with the assumption that as images can be easily remembered users will tend to choose variety and complex passwords which will be more secure from attackers. Graphical authentication systems are further categorised into three types – pure-recall based systems, cued-recall based systems, recognition based systems. In section II, I will be presenting about various authentication techniques. In section III, I will be presenting about the various criteria based on which each graphical systems will be analysed. In section IV, I will be presenting a thorough survey of these three types of graphical password systems that have been invented so far. At the last, in section V, I will also be presenting some newly developed graphical password systems and will try to critically analyse them based on the evaluation criteria discussed in section III.

II. TYPES OF AUTHENTICATION TECHNIQUES

At present the authentication techniques can be classified in three categories [4], [5]: Token based authentication, Biometric based authentication, Knowledge-based authentication.

A. Token based authentication

In token based authentication [4], [5], ‘tokens’ are used to authenticate users. Token contains a piece of data which is later on used to authenticate users possessing tokens. After a token has been validated then an user can access the desired service for which the token is responsible for. The night key that students of University of Helsinki possess, is an example of token. In general, bank cards, smart cards, key cards, e-passports are classic example of tokens. But the main disadvantage of token is that it can be easily stolen or lost or damaged. Hence, there is no way to restrict unauthorised users, possessing somebody’s else token, to access the desired service.
B. Biometric based authentication

In biometric based authentication [4], [5], users are authenticated with help of human characteristics like signature, speech, typing style, etc. Fingerprint, face recognition, iris scan are also used to authenticate users. Like Lenovo laptops have VeriFace recognition to authenticate the owner of a particular laptop. The main disadvantage of biometric authentication is that it is very expensive to deploy and authentication process is often very slow.

C. Knowledge-based authentication

Knowledge based authentication [4], [5] is widely used nowadays. It is further sub divided into text based or alphanumeric passwords and picture based or graphical passwords.

1) Alphanumeric or text based passwords: Alphanumeric authentication technique is most widely used nowadays. Here, a user maintains an username and an alphanumeric based text as password for an account. This combination of username and password is later on used to authenticate a particular user account. Like for accessing Facebook, each user creates an account during registration and later on while logging into the account the user verifies himself by providing the desired username and password, as provided during the registration process. Similarly, users maintain gmail accounts, yahoo accounts, University specific accounts, work based accounts, ATM accounts, accounts for using laptops, computers, etc.. As mentioned above, that dual coding theory states that human mind requires extra processing to remember and recall texts, hence these type of passwords are often very difficult to remember. Sasse et al. [1] conducted a survey where 144 people where enquired about the reason for re-setting their passwords and the number of passwords each user maintained. The results of the survey is shown in table 1. According to the survey results, users were divided into three groups: light use users (means users who used their passwords from once per year to just under once a month), medium use users (means users who used their passwords from once a month to once a day) and heavy use users (means users who used their passwords used more frequently than once a day). Hence generally, text based passwords are either simple enough so that it can be easily remembered, which makes the passwords vulnerable to attacks or very complex which causes memorability issues [1], [2]. Textual passwords that can be easily remembered and can be secure against attacks at the same time is very difficult to create, hence researchers proposed graphical authentication as an alternative to textual passwords.

2) Graphical based passwords: Graphical passwords overcomes the problems of text based passwords and act as an alternative to it. As the name suggests, graphical based passwords deals with pictures or images either selected from a given panel of pictures provided on Graphical User Interface (GUI) or drawn by users themselves on the Graphical User Interface. According to dual coding theory [3], picture is easier to remember than text. Hence taking this assumption, if pictures are used as an alternative to text based passwords, then users will be tempted to choose variety and complex passwords for each user accounts. Graphical based password systems are also further categorised into three types: Pure recall based systems, Cued recall based systems and Recognition based systems.

   Pure recall based systems: In these types of systems, user has to draw his/her own password on the GUI during account registration process. During authentication of user account, user has to remember the password or draw the password on the GUI, without any clue. These systems are also known as drawmetric systems.

   Cued recall based systems: In these types of systems, user is provided with an image on the GUI and then user has to click on specific points of an image during account registration process. During account authentication, user is provided with the same image (i.e. the same picture that was provided during the registration process) and user has to click on same points as done during account registration process. These systems are also known as locimetric systems.

   Recognition based systems: In these types of systems, while creating an account (means during registration process), user has to choose pictures from a given a set of pictures in panel by panel. During account authentication, user has to choose the same set of pictures from a random set of pictures (also known as decoy picture), he has chosen earlier while creating the account. These systems are also known as cognometric systems.

III. Evaluation criteria

The graphical password systems are analysed using the following criteria: security and usability.
A. Security

Given a password, no matter whether it a text based or graphical based password, one question always arises in our mind - “Is the password secure enough to protect the user account?”. Hence, security [4], [3], [6] is always an issue when we discuss about passwords. As, the real implementation of graphical passwords haven’t been quite common till now, so practical cases of breaking passwords have been less reported. In this section, I have briefly discussed about some possible attacks in graphical authentication systems.

1) Shoulder-surfing attacks: In shoulder surfing attack [4], [3], [6], attackers captures the login details of users by some external recording devices such video or camera or by observation at the time of user logs into the account. For example, in ATMs people stand behind each other in a queue and hence can observe the pin numbers of user using the ATM from behind. Also, the ceiling and wall cameras can be used to record user log in sessions by attackers. Most of the recall based techniques are vulnerable to shoulder surfing attacks.

2) Phishing or social engineering attacks: In these types of attacks, attackers deceive the users to enter their login details in some recording fraud website. Phishing attacks [4], [3], [6] on pure recall based systems are similar to text based systems. But for attacking in cued recall based or recognition based systems attackers need to provide users with some specific images of their own. Phishing is a form of social engineering attack where users are asked to describe their passwords, like by making phone calls from fake help desk or credit card company.

3) Malware attacks: In malware attacks [4], [3], [6], attackers use unauthorised software to capture keyboard input through keystroke loggers, mouse clicks through mouse loggers and screen scrapers. It can also take screen shots of web page and parse it to find out the user login details. Graphical passwords are vulnerable to malware attacks as most of the graphical password systems use mouse logger and screen scraper for capture and often a keystroke logger for entering usernames.

4) Brute-force search attacks: The attackers of brute force search [4], [3], [6] attempt to search for the password until the correct password is found. Graphical passwords are somewhat resistant to brute force search attacks, if the password space is increased by increasing the picture library capacity. In general, recognition based graphical passwords have less password space than recall based graphical passwords. Text based passwords have space of $94^N$, where $N$ is the length of password and 94 is the number of printable characters. As, 94 is the maximum possible number, text based passwords are vulnerable to this type of attack.

5) Dictionary attacks: Dictionary attacks [4], [3], [6] are similar to brute force search attacks. In these types of attacks, attackers keep a dictionary of all possible passwords. Recognition base graphical passwords use mouse instead of keyboard input so it is less vulnerable to dictionary attack. For, recall based systems, there are chances of this type of attack but the probability is low as it is complicated to use automated dictionary.

B. Usability

Graphical passwords are recently emerging as an replacement to text based passwords. So the usability [3] feature plays an important role. The term ‘usability’ refers to the question that “whether graphical passwords can be conveniently used by the target users”? Usability is somewhat depended on target users [3]. Graphical passwords are dependent on the way the target users interact with the system, the number of times they use the system (as shown in Table I). Some systems also require good good visionary senses especially recognition based systems, some systems require good drawing skills like pure-recall based systems. So, graphical password systems should be build by taking into consideration the capabilities of targeted users. Usability is also depended on the following tasks performed by the target users:

- **Password creation [3]**: Password creation phase involves the registration phase. Attention should be given to the fact that “how much time does it takes to create the password”? If more time is needed in the registration then obviously users will be less reluctant to use the system.

- **Login [3]**: Login phase involves the authentication process. Graphical password systems should be build in such a manner that the login time is least otherwise users may be reluctant to use the systems. Memorability also plays an important factor in determining the login time.

- **Password reset and password change [3]**: Users often change their password due to security concerns or reset their password due to memorability issue. So the graphical password systems should be build in such a manner that users can easily change or reset their passwords without any security threat and the changed password should be completely different from the previous one. In text based systems, the process of resetting the passwords is done either by only user-system interaction or with help of an third party verification like a message or phone call or email. Biddle et al. [3], claimed that such type of verification is difficult in implementing in graphical password systems, as it would pose social-engineering attacks. So, as a solution, they have proposed to use temporary non-graphical password during resetting process. But I think that, if graphical passwords also use the same process as used by text based password systems i.e. third party verification then the system won’t be vulnerable to social engineering attacks, as in third party verification security questions set during registration process will be asked to describe and not the passwords set during registration process.
IV. VARIOUS TYPES OF GRAPHICAL AUTHENTICATION SYSTEM

As mentioned earlier there are three types of graphical authentication systems: recognition based systems, pure-recall based systems and cued-recall based systems. In this section, I will be presenting briefly various types of graphical based systems. I will also be presenting the advantages and disadvantages of each system wherever possible.

A. Recognition based system

There are six types of recognition based systems: Dhamija and Perrig algorithm, Sobrado and Birget Algorithm, Man et al. Algorithm, Jansen et al. algorithm, Takada and Koike, Passface algorithm.

1) Dhamija and Perrig algorithm: In 2000, Dhamija and Perrig [3], [7], [8] proposed a graphical authentication model called ‘Deja Vu’ which was based on Hash Visualization Technique. During experimentation, in the registration process 20 users had to choose a set of 5 pictures from a given set of 25 random pictures as shown in figure 1. The participants were also required to form text based passwords, of atleast 6 characters long, simultaneously. After some time period, participants were asked to authenticate themselves using both graphical and text based techniques. The results showed that 90% of the participants could log in successfully using graphical passwords whereas only 70% of participants could log in successfully using text based passwords. The password space was evaluated as:

$$\binom{N}{M}$$

where N is the total number of images in the panel and M is the set of pictures chosen by the user. Hence, if N=25 and M=5, number of possible password combination is 53,130 which is equivalent to 2^{16}.

Critical analysis: Here, the above system is evaluated based on the evaluation criteria of section III. Security aspects: Dhamija et al. [8] have claimed that this system is secured from shoulder-surfing attacks. To prove their claim they have taken the 3 assumptions - that the images will be clearly visible only to the user and not to the attackers; the process of selecting the images is not visible to the attackers i.e. which keys relates to which images are hidden; the images in the user portfolio will be slightly changed in each authentication process. But I think that the first assumption is not valid as attackers in shoulder surfing attacks can easily see the random images from behind or clear observation of authentication process. Moreover, if the third claim is implied then it may cause usability issue, as slight change in the user portfolio may cause memorability issue, as random arts are quite confusing. The description of random pictures became a bottleneck for users, hence users couldn’t easily share their passwords with others hence this system was resistant to social engineering attacks [3]. No claims have been found regarding whether this system is resistant to malware attacks. But I think that this system is resistant to malware attacks. If we take the assumption 2 (as stated above), then even by taking the screen shots of authentication process attackers won’t be able to discover the password. Moreover, capturing the keyboard and mouse instance together at the same time is difficult. The probability of brute force attacks [8] is 1/(N M), where N is the total number of images in the panel and M is the set of pictures chosen by the user. So, if N=20 and M=5, then probability of brute force attacks are 1/15504. Hence, this system may deny access after few attempts to login to make the system resistant to brute force attacks. As, the number of possible password combination is 53,130 hence the probability of dictionary attacks is 1/53,130. As mentioned above, the system may deny access after few login attempts. Hence, the system is resistant to dictionary attacks [3]. Usability aspects: The authentication process may be slow [9] due to storage of bulk images in the server side, which is needed to be transferred over the network. I think, use of bright colors may be an issue for target users especially for color blinds as they cannot different between colors like red and green, which are used in this system. Moreover, I think that remembering the random arts may cause memorability issue.

2) Sobrado and Birget Algorithm: Sobrado and Birget developed many algorithms [4], [9], [10] to resist against shoulder surfing attacks. The first algorithm was called ‘triangle scheme’. In this scheme, user selected 3 images called as pass objects during registration phase. During authentication, a set of images were displayed on the UI out of which user had to select the three pass objects which formed a triangle and then had to click inside the triangle as shown in figure 2. To increase the password space and level of complexity of passwords, Sorado and Birget suggested to use 1000 images during authentication process and to repeat the process few times. The number of possible passwords are:

$$\binom{N}{K}$$
where K is the number of objects chosen and N is the total number of objects shown in UI. If, N=1000 and K=10, then number of possible password combinations are $2.6 \times 10^{23}$.

**Critical analysis:** Here, the above system is evaluated based on the evaluation criteria of section III. Security aspects: The system is claimed to be resistant to shoulder surfing attack [10] in the following way: if one click point is seen by the attacker, then the attacker knows that the other K objects will form a triangle, inside which the click point will be there. Hence, K-tuples objects will be unlikely to be clicked by the attacker. Hence, if N=100 and K=10, then the ruled out K-tuples is

$$\binom{100}{10}$$

which is $>2 \times 10^{20}$. Hence, even if the attacker observes the login session, the attacker will hardly remember the exact objects. No claim haven’t been done yet regarding whether the system is resistant to phishing attacks and malware attacks. I think, that the system is resistant to phishing attacks, as the UI contains large number of objects i.e. N=100 or 1000, so it will be difficult for the users to describe the images distinctly from each other. I think that the system is resistant to malware attacks also, as even if the mouse clicks and keyboard inputs are recorded through respective loggers, then also the attacker cannot identify the password, as images are shown randomly in each authentication phase. Moreover, even if the screen shot of authentication phase is taken then also the attacker will unaware of the the triangle, as the triangle is invisible. Sobrado et al. [10] used the same fact as used in shoulder surfing attacks, to claim that this system is resistant to brute force and dictionary attacks. Due to the usage of large number of decoy images on the UI, the possibility of brute force attack is negligible. As mentioned above, that the possible number of passwords are $2.6 \times 10^{23}$, hence the probability of choosing the same passwords by two or more users is very less. Hence, the system is resistant to dictionary attacks. Usability: The user can easily create the password but the login process is extremely slow [4], as the user needs to first find the pass objects then needs to find out the invisible triangle formed by those pass objects and then the user needs to click inside that invisible triangle, which will take a lot of time. I think that, the user also needs to have good vision, which may be a bottleneck, as most users may suffer from eye problem. Moreover, I think that password resetting may also be a problem, as most of the images looks similar and hence resetting the password may confuse the user. The presence of too many decoy images may cause memorability issue [9].

The second algorithm proposed by Sobrado and Birget was called the ‘movable frame scheme’. In this scheme, a frame was first placed over a single pass object and then the frame was moved in a circular manner until the other two pass objects came inside the frame to form a single straight line as shown in figure 3. This step was repeated several times so that attackers couldn’t guess the password by randomly moving or clicking the frame.

**Critical analysis:** Security: Though Sobardo et al.[10] claimed that the system is also resistant to attacks as discussed above, but I think use of straight frame increases the likelihood of password guessing attacks. Usability: I think that this system also also suffered from the same usability problems as mentioned above. The main disadvantage of this scheme was that login process was too slow and confusing because of presence of too many non-pass objects or decoy images.

3) **Man, et al. algorithm:** In Man et al. algorithm [4], [11], user had to select many pass objects during the registration phase. Each pass object was unique in the sense that each pass object was represented by an unique code. Authentication was done using many login phases. In each phase, user had to select several pass objects from given set of decoy images on the UI and had to write the unique code corresponding to each variant of pass objects and also had to write a code to locate the exact position of the pass objects.
Critical analysis: Security: Man et al. [11] claimed that the system is resistant to shoulder surfing attack in the following way: that even if attacker observes the login session from behind then also it is difficult to find the actual password, as each image is associated with unique code, known only to the user. In [4] it is claimed that even video recording of authentication session won’t reveal the password as mouse click is not associated with this system. But I think that video recording can easily record the unique codes associated with each pass object, hence the system is vulnerable to shoulder surfing attacks. No valid claim has been found regarding the system vulnerability to other attacks. I think, this system that the system is resistant to social engineering attacks, as users may find it difficult to describe the pass objects distinctly from other decoy images, due to presence of large number of decoy images on the UI. Hence, even if the users describe the unique codes associated with each pass objects, it will be difficult for the attackers to find out the exact pass objects. I think that the system is resistant to malware attacks, as no mouse click is associated in the system. So, even if the keyboard input is captured, then also it will be difficult to relate it with the corresponding pass objects. The presence of large number of decoy images makes the system resistant to brute force attack, as the probability of searching the password is too low. The probability of using the same password by two or more users is very low, hence the system is resistant to dictionary attack. Usability: Users had to remember alphanumeric code corresponding to each variant of pass objects [4], which again brings back the problem of text based passwords. Also, this scheme was time consuming specially during registration process, as users have to remember the pass objects and then the unique code. Moreover, I think that the system may take large time for authentication process, as the user not only have to write codes corresponding to the pass objects but also have to write the exact location of the pass objects on the UI which is time consuming and requires lot of human mind processing and hence users may not prefer it.

4) Janson et al. algorithm: The algorithm proposed by Janson et al. [7], [12] was mainly useful in mobile devices. During registration process each user have to select a theme (like a dog, sea, scenery, etc) as the base for selecting password. Each theme was further divided into blocks and each user had to select a sequence of blocks as password. During authentication, user had to enter the previously selected images in each block in correct sequence.

Critical analysis: Security: In this scheme, password size was very small as compared to textual password as the number of block images was limited to 30 as shown in figure 5. Each image corresponded to a mathematical value and hence the whole password generated a numerical password of small size. Hence, the system is vulnerable to brute force and dictionary attacks [7]. Moreover, I think that this system was vulnerable to shoulder surfing attack - one could easily guess the password by observing a login session. This system was resistant to phishing attacks, as many blocks of images were identical so describing the images on each block was difficult. Usability: The passwords can be easily reset in this system [12], as users can easily reuse the same password but the values of each image was changed in the corresponding matrix as shown in the figure 6, but this may pose security threat. I think that the registration process takes very less time as the user only has to click on the images in a desired sequence. On the other hand, I think that the authentication process may take some time if the user forgets the order in which images was clicked. Hence, the user may suffer from memorability issue, as all the images were similar to each other.

5) Takada and Koike algorithm: Takada and Koike [9], [13] developed an algorithm similar to the one mentioned above. The difference was that here user could choose his/her own images, also called as pass images, during registration phase as shown in the figure 7. This system is also known as Awase-E. During authentication, user had to select a pass image from a given set of decoy images and nothing if no pass image was present in a particular round. In order to verify, the user had to complete all the rounds successfully as shown in figure 8.

Critical analysis: Takada and Koike [13] developed this
The system to maintain a balance between security and usability aspects. According to Takada and Koike [13] "The number of verification stages in Awase-E is variable. Awase-E, therefore, provides a flexible authentication framework that can handle various situations. For example, to emphasize security over usability, you could configure Awase-E such that a user must verifies 5 sets and must select a pass-image in 4 of the sets. On the contrary, if you put weight on usability over security, you can configure the process such that the user verifies only 3 sets and must select a pass-image in 1 of the sets." But, I think that this consideration cannot be taken as valid in case of graphical password system, as an ideal system will be one which will provide both security and usability at same time. Moreover, Takada and Koide haven’t taken into the consideration the other types of attacks. The system is highly vulnerable to shoulder surfing attack, as anyone observing the login phase can easily detect the password. Moreover, I think that the system is vulnerable to phishing attacks, as users can easily describe their passwords. Moreover, by recording the mouse clicks or keyboard inputs, attackers can easily detect the password. I think, if the number of sets of panels is increased, then the probability of brute force attack decreases. Use of own images limits the possibility of dictionary attack. But this scheme is not so secure as attacker knowing the user could easily predict the password by predicting which favourite image have been used by the user. Usability: Using own image helped user to remember password in a better way. If usability is priority then user can reduce the number of sets [13]. I think that the registration process may take sometime, as users had to take some time to think which image to be used so that it can’t be predicted easily by attackers. The authentication process doesn’t takes much time [13], as users needed to just click on the respective images. Authentication process was completed in at most N+1 times, where N is the number of sets or panels. Moreover, passwords can be easily reset [13], as users can use the same images as passwords but each image would correspond to different value matrix as shown in figure 6.

6) Passface: As the name suggests passface algorithm [3], [9], [14] was based on human faces developed by Real User Corporation. In passface, during registration each user had to choose a set of 4 human faces as his/her own portfolio. During authentication, a set of M faces were shown in each N rounds, where M=9 and N=4, out of which in each round only 1 face belonged to the user portfolio as shown in figure 9. User had to identify all the faces correctly in all the rounds for successful authentication. Possible password combination was M^n, where M is 9 and n is 4, is 6561 ∼ 2^{13}.

Critical analysis: This system is being claimed to provide high security against phishing attacks [14], as it will be extremely difficult to describe their passwords, as all the images belong to human figures. But I think, Passface password is easier to predict by attackers as user choice is influenced by race, gender of user and attractive faces in the set. Also, based on race and gender, users could easily describe their passwords, hence this system is vulnerable to phishing attacks. Study results [15] have shown that passface
implemented with keyboard is less vulnerable to ‘shoulder surfing’ attacks, as shown in table II. Moreover, the system is resistant to malware attacks [3] if keyboard is used for login, as recording both the keyboard input and screen shots at the same time is difficult. No study results have been found out regarding brute force or dictionary attacks. I think, the possibility of brute force attack is $1/2^{13}$. Probability of dictionary attack is also high, as same images are used. Usability: The registration time is 3-5 mins [14]. It is also claimed that the authentication time is also very low [3], [16]. But, I think authentication time may be longer due to memorability issue. Experiments conducted by Brostoff and Sasse [16] showed that human faces were easier to remember as shown in table III. But, if users have to maintain many accounts having passfaces as medium of creating passwords then it will be extremely difficult for users to remember the faces. Moreover, this will tend the users to use the same passwords in many accounts and hence this will result in dictionary attacks. Moreover, experiments conducted by Davis et al. [17] showed that passface took longer time to login than textual based passwords, hence users hesitated to use passfaces. Hence, this is a matter which contradicts the study results.

B. Pure-recall based system

There are five types of pure-recall based systems: Passdoodle, Draw-A-Secret, Grid-selection, Qualitative DAS (QDAS), Syukri Algorithm

![Figure 9. A screenshot of passface showing 9 faces out of which only 1 face belongs to user portfolio [9]](image)

1) Passdoodle: Goldberg et al. proposed passdoodle [18], [19] which was a type of pure recall based system where users had to draw either a figure or a text by their own with help of stylus on a touch sensitive screen, during registration process. While authenticating, users had to draw the same figure or text with same speed and accuracy without any hint. Figure 10 shows an example of passdoodle password. Only a finite number of computer identifiable doodles were possible.

**Critical analysis:** Security: Much claims regarding the security of this system haven’t been found out yet. I think that the system is resistant to shoulder surfing attack as even if the attacker observes the login session still the speed with which the user has drawn the password may vary. Hence, drawing the exact passwords is quite difficult. I think that this system is also resistant to phishing attacks as even if the users describe their passwords, describing the speed with which they had drawn their password is difficult to describe. I think that the system is vulnerable to malware attack as password can be easily guessed if mouse click is captured. No claims have been found regarding the brute force attack. It is claimed [18], [20] that the system is resistant to dictionary attack as users tend to generally draw the first letter of their names. But I think that even if the attackers can guess the password drawn, they cannot draw the exact password as the speed of drawing the passwords may vary. Usability: I think that users may find it difficult to draw on touch sensitive screens, hence possibility of delay in registration process may happen. Also authentication process may require long time as study results [19] have shown that users tend to forget the order in which they drew their password.

2) Draw A Secret: Draw A Secret also known as DAS [18], proposed in 1999, was same as above discussed scheme. The only difference was that 2 dimensional grid structure was used here as a background to draw the figure
Table III
MEMORABILITY OF PASSWORDS AND PASSFACES OVER DIFFERENT INTERVALS [16]

<table>
<thead>
<tr>
<th>Interval</th>
<th>Passwords (%) remembered</th>
<th>Passfaces (%) remembered</th>
<th>Study</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 day</td>
<td>-</td>
<td>99.98 (1st attempt)</td>
<td>Valentine, 1998</td>
</tr>
<tr>
<td>1 week</td>
<td>-</td>
<td>100 (by 3rd attempt)</td>
<td>Valentine, 1998</td>
</tr>
<tr>
<td>2 weeks</td>
<td>77 (1st attempt)</td>
<td>-</td>
<td>Bunnell et al. 1997</td>
</tr>
<tr>
<td>1 month</td>
<td>-</td>
<td>100 (by 3rd attempt)</td>
<td>Valentine, 1998</td>
</tr>
<tr>
<td>3 months</td>
<td>35 (1st attempt)</td>
<td>-</td>
<td>Zviran and Haga, 1993</td>
</tr>
<tr>
<td>3 months</td>
<td>27.2 (1st attempt)</td>
<td>-</td>
<td>Zviran and Haga, 1993</td>
</tr>
<tr>
<td>5 months</td>
<td>-</td>
<td>72 (by 3rd attempt)</td>
<td>Valentine, 1998</td>
</tr>
</tbody>
</table>

Figure 10. A screenshot of Passdoodle [18]

<table>
<thead>
<tr>
<th>Group</th>
<th>Strokes</th>
<th>Password length</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Avg</td>
<td>s.d.</td>
</tr>
<tr>
<td>BDAS</td>
<td>5.75</td>
<td>2.6</td>
</tr>
<tr>
<td>DAS</td>
<td>2.28</td>
<td>0.5</td>
</tr>
</tbody>
</table>

Figure 11. A screenshot of DAS scheme[18]

3) Grid Selection: According to Thorpe and van Oorschot, stroke count was directly proportional to password space. Users of DAS tend to choose fewer strokes, which weakened the password strengths. So, in order to increase complexity, grid selection [18] was introduced in 2004. In this scheme, during registration process users had to select n*n grid from a given set of larger grids as shown in figure 12. Then user had to draw his/her own password on the selected grid in a similar manner as DAS. During authentication, user had to first choose the correct grid, which was chosen in registration phase and then had to draw the password in correct order.

Critical analysis: The introduction of grid selection increased the password space to 16 bits, hence passwords of this scheme were much secure. It was also somewhat resistant to phishing attack, as explaining the exact grid selected would be difficult for users to describe. The system was also resistant to shoulder surfing attacks, visibility of exact grid selection out of similar grids would be difficult. It just increased complexity of DAS but the actual loopholes of DAS was unsolved. Also, remembering exactly which grid was selected could be a memorability issue.

4) Qualitative DAS: Qualitative DAS [18], [22] also known as QDAS, was an extension of DAS scheme described above. In QDAS, dynamic grid transformation was used and each stroke was encoded. Figure 13 shows a screenshot of QDAS. The password space is $2.8 \times 10^{14}$.

Critical analysis: Security: It is claimed that the system is...
resistant to shoulder surfing attack [22] in the following way: the drawing of the password is dependent on the starting cell number and the exact direction of change of strokes. But I think, in this way shoulder surfing attack can be reduced if attacker is behind the user and observing the password. As, in this way remembering the exact starting grid point and the grid points where the change of strokes occurred is difficult. But, if the authentication session is recorded then I think attacker can easily identify these grid locations. Claims regarding the vulnerability of other attacks haven’t been analysed yet. I think that the system is vulnerable to phishing attack, as user can easily describe the figure drawn the corresponding grid cell numbers. I think that the probability of malware attack is also high if mouse click is recorded using mouse loggers. As the password space is high, I think that the probability of brute force attack is very low $\frac{1}{2.8 \times 10^{14}}$. Usability: It is claimed that the memorability of users using this system is average [22]. Other discussion regarding usability aspects haven’t been found yet. I think that the registration time may take some time, as users have to draw on UI and most users are not acquainted with that. Moreover, I think that remembering the exact grid locations may be an memorability issue, though this is contradicting the claim of the study results of [22], hence authentication process may be longer.

5) **Syukri Algorithm:** Syukri algorithm [18] dealt with user signature drawn by mouse on UI as passwords. During registration, each user had to draw his/her own signature and the system parsed the signature to either increase the signature size or reduce the signature size (in some cases rotation was also done) and then the signature was saved in database of system. During authentication, each user had to draw the signature in the same manner. Geometric average means and dynamic update of database was used to verify the signatures of user input and one in database. Figure 14 shows an example of Syukri scheme.

**Critical analysis:** In this scheme, user could easily remembered their own signatures. It was secure in the sense that signatures were hard to be copied. The main problem of this scheme was that users found difficulty in drawing signatures with mouse on UI. Also, drawing exactly the same signature on each authentication process took a long time.

C. Cued-recall based system

There are 8 types of cued-recall based system: Blonder, PassPoint, PassMap, BackgroundDAS, Passlogix v-Go, VisKey SFR.

1) **Blonder:** Blonder [18] scheme was proposed by Greg E. Blonder in 1996. During registration user had to select a image and had to click on some specific regions marked by some boundaries. During authentication, the pre-determined image was shown to the user, out which the user had to click on the pre-selected areas or locations as shown in figure 15.

**Critical analysis:** The region of pre-determined click was very small, so long password was necessary for better security. Moreover, this pre-determined click used simple cartoon pictures instead of complex real world pictures.

2) **PassPoint:** In 2005 PassPoint [18] was proposed, which covered some of the loop holes of Blonder scheme. In this scheme, real life image was used which increased password security. Unlikely to blonder scheme, the region
where users could click was not pre-determined, as shown in figure 16. During registration, user clicked on any location of the image. While authentication, user needed to click nearby previously selected points (should be within a tolerated region).

**Critical analysis:** In this scheme, users could easily create their own passwords. The scheme suffered from shoulder surfing attack. Increasing the tolerated region size was a loophole as it would decrease the password space size. Users had difficulty in remembering the passwords.

3) **BackgroundDAS:** As the name suggests, BackgroundDAS [18], proposed in 2007, was an extension of DAS. Users had to draw their passwords on grid containing a background image, as shown in figure 17. The background image was introduced with the assumption that it will help users to better remember their passwords in the following ways - users could select a point of background image to start drawing their own passwords or users could draw an image related to the background strokes or both, though this could increase brute force attack possibility.

**Critical analysis:** This scheme suffered from shoulder surfing attacks and large number of passwords could interfere with each other. Memorability was also an issue in this scheme.

4) **PassMap:** Considering the fact that, users suffer from memorability issue in case of complex passwords and simple passwords are easy to break, PassMap [18] was proposed by Roman in 2007, which used geographical maps as images used for passwords. Suppose the map of Europe is provided to the user during registration phase and the user has to select places (like Eiffel Tower in Paris, Suomenlina in Finland, etc.) as points to form a password, as shown in figure 18.

**Critical analysis:** This scheme was build on the assumption that places could be easily memorised by users hence passwords would be easier to remember. This scheme was resistant to shoulder surfing attack. This scheme suffered from brute force and dictionary attacks, as users tend to choose world famous destinations as points of passwords. In this scheme, users could easily describe their passwords hence the system was extremely vulnerable to phishing attacks.

5) **Passlogix v-Go:** In 2008, Passlogix Inc. a security based company of USA developed Passlogix v-GO [18] scheme. This scheme, allowed user to select the background image of his/her own choice like kitchen, clubroom, etc. out of which the user had to select a sequence of events in chronological order as password. For example, if the background image was kitchen or any room, as shown in figure 19, then the user could first choose to pick vegetables, then pick the cutting utensils, then put them in a bowl and then in oven. This series of events represented as a password.

**Critical analysis:** In this scheme, passwords were easier to remember as it directly correlated with user’s regular life activities. The password size was small in this scheme. Passwords could be guessable in the sense that vegetables were always kept in the fridge, there’s a certain area to keep bowls and cutting utensils which lead to brute force attacks. Moreover, the set of images like kitchen or clubroom was pre-determined and always same which lead to dictionary attack. In this scheme, users could easily describe their passwords which lead to phishing attacks.
6) **VisKey SFR**: VisKey [18], proposed by a German company SFR, was mainly targeted for mobile devices. During registration, user was provided with an image on which the user had to click on certain locations of the image in a sequence. For authentication, user had to click the same locations in correct order, as shown in figure 20.

**Critical analysis**: In this scheme, it was not necessary to click on the exact location, a click within a certain range of area (previously specified by the user) was tolerated. So, users needed less time for authentication. The input tolerance range of the scheme was a bottleneck, as experiments showed that it was difficult for the users to click on specific tolerance areas, so users could specify their own tolerate region of clicks which imposed security issue. Moreover, the scheme was vulnerable to brute force attacks.

D. **Some real-life practical application of graphical authentication systems**

Some real-life practical application of Pure recall based systems [3] includes - Google Andriod cell phones have implemented grid system (mini Pass-Go system), BlackBerry uses pattern lock, Andriod screen unlock system is vulnerable to smudge-attack (pattern id detected by finger impression left on the screen).

V. **NEWLY DEVELOPED GRAPHICAL PASSWORD BASED SYSTEMS**

Here, I will write about some newly developed graphical password based systems and will try to critically analyse them. The systems that I have critically analysed are Action-Based Graphical Password: Click-a-Secret and A hybrid recognition and recall based approach in graphical passwords.

A. **Action-Based Graphical Password: Click-a-Secret**

Click-A-Secret approach [23] is developed by Éluard, Maetz and Alessio in 2011 as a combination of cued recall based systems and recognition based systems. During registration process, user is provided with an image (previously stored in the system) which is modified by the user based on available Gecu (Graphical Element Chosen by User), to create user’s own personal image. Gecu refers to particular objects in the image which can be modified with alternate versions of it. Figure 21 shows an example of Gecu with its alternate versions. Number of Gecus and its alternate versions are predefined. Hence the final personal image formed by the user is different from the previous image displayed to the user as shown in figure 22. During registration, user is also provided with a practice phase where the user can practice to remember the password while login. In the following paragraphs, I have presented my analysis. The flow of the enrolment process is shown in figure 23.

**Critical analysis**: Usage of keyboard is not required in this scheme. Hence, it can be easily used on touch screens. A practice phase is involved which helps the user to remember the password in a better way. It is resistant to shoulder surfing attacks as anyone viewing from a certain distance won’t be able to view the password clearly as it is difficult to differentiate between different variants of Gecus but is vulnerable to recording the login session via a camera or video. According to me, this system suffers from both security and usability issue as described further. Security issues: Addition of predefined Gecu and its various alternatives may lead to guessing attacks like brute force attacks, even with the fact that it has high secret space. Given an image, user can easily describe the changes which makes it vulnerable to phising attacks. Usability issue: It may take a long time to create the password, so users may avoid to use this type of system. Moreover, remembering the passwords may become an issue even after implementing the practice phase, as most of the users will tend to avoid practice phase. Moreover, remembering all the Gecus with its correct variants may become a problem for users to remember.

Proposed solutions/modifications: If the "Click-A-Secret approach" is modified in such a way that user is allowed to do the changes in the image by his own, means Gecu’s variants are not predefined, then it can solve the memorability issue. This change can also make the system resistant to brute force attack - if the system doesn’t store the variants of Gecu then attackers cannot try different possibilities of passwords. Even, after implementing this change the system will remain vulnerable to phising attacks, as user can easily describe the changes done in the Gecus.
B. A hybrid recognition and recall based approach in graphical passwords

A hybrid recognition and recall based approach in graphical passwords [24] is a combination of recognition and recall based systems. In the registration process user have to select a minimum of three images from a set of given images on the UI. The authentication process involves two phase. At first the user is provided with a panel of images containing both the user password images and decoy images. Out of this panel user has to identify the images belonging to the user password and have to remember the position of those images, as shown in figure 24. The second panel consists of random numbers in each grid and user has to select numbers in correct sequence corresponding to the location of the user password images in the previous panel as shown in figure 25. The number of possible password combination for 4 images are represented by:

\[
\sum P.Comm = (14 - L_c.A) \times (15 - L_c.B) \times (16 - L_c.C) \times (17 - L_c.D)
\]

where P.Comm = Password combinations; \(L_c\) = Location within the password grid; A, B, C, D = Password images in sequence.

**Critical analysis:** Security: Zangooei et al. [24] have conducted a experiment to prove that the system is resistant to brute force attack. In the experiment, a user was asked to login using this scheme (using 4 images as password) and 2 other participants were asked to observe the login session from behind. This step was repeated 10 times, using different participants as attackers standing in different distances. The experiments results are shown in the table V. The results showed that out of 20 attackers only 3 attackers were able to guess the first 3 letters of the second panel while only 1 attacker was able to detect only the first character of the second set of letters. Hence, the experiment stated that the system is highly resistant to shoulder surfing attacks. Discussion regarding other types of attacks haven’t been found yet. I think that the system is highly vulnerable to phishing attack as users can easily describe the images, as each image is clearly distinct from the other. Hence, as the numbers are generated randomly in the second panel, so with only the knowledge of images attackers can easily find the password. I think that the system is secured against malware attack, as even if the keyboard input is captured it won’t reveal the actual images i.e. the actual password. It is claimed that the system is resistant to brute force attack [24] as the system only allows 3 login attempts at a instance. I think that the system is vulnerable to dictionary attack, as probability of choosing the same password from a set of
16 images is very high. Usability: The study results [24] as shown in table V showed that the users can easily create the password during registration process. The authentication process was also fast as users could easily remember the password.

VI. CONCLUSION

Taking the loopholes of alphanumeric passwords, graphical authentication is an emerging solution. Presently, graphical password techniques can be classified into three types: recognition-based, pure recall-based and cued recall based. As presented in this paper, the existing graphical passwords systems suffer from usability and security issues. To overcome these problems, many authors have proposed newly developed graphical password systems but those systems either solves security issues or usability issues. None of the systems provides both together. Emphasis should be given in building a system which is both user friendly and is completely secure. Otherwise, users will be reluctant to use graphical authentication systems. Hence, graphical authentication system is still an interesting area of research.

REFERENCES


