International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN :2147-6799 www.ijisae.org Original Research Paper

Security Analysis of the Graphical Password-Based Authentication Systems with Different Attack Proofs

[1]Priti C. Golar, [2]Dr. Rika Sharma

Submitted: 27/05/2023 **Revised**: 08/07/2023 **Accepted**: 26/07/2023

Abstract: Graphical password authentication is an effective alternative to the textual based password as the text based passwords are difficult to be remembered. One of the disadvantage is that there are several attacks existing in these schemes that disrupts the integrity of the websites. In this paper, a detailed security analysis for various kinds of attacks existing in a graphical password authentication system is presented. Initially, the scenario of graphical authentication system along with its types are narrated. Then, the major security threats encountered in the graphical password authentication systems till date are explored. Based on the security threats arising in the authentication systems, the zero knowledge attack proof is formulated and the analysis is explained. More importance is given to the shoulder surfing attack and the proof is explained with the help of an application scenario. The introduced application scenario includes a 3D graphical password authentication system for website login. The scenario is proved to be shoulder surfing resistance using the zero knowledge proof protocol. With the analysis, it is proved that the graphical passwords are highly significant in maintaining the integrity of the websites.

Keywords: *Security, authentication, graphical password, recognition based graphical password, recall based graphical password, attack proof, shoulder surfing, zero knowledge proof.*

1. Introduction

In the modern world, smart devices are becoming common and integral part of our daily activities. People can store private information like financial information, PIN numbers, personal images, documents, contact details etc., on their smart devices. In USA, the customer report has found that approximately 34% of every smartphone vender either employ a simple code for locking the screen or have no security mechanism of their smartphone [1]. Meanwhile, about 36% of smartphone users utilize a fundamental 4-digit PIN for locking phones. Authentication of user plays a significant role to protect the data that have been stored [2]. Some of the authentication methods are based on password, smart cards, biometrics, public key infrastructure and so on [3]. Among the authentication methods [4], text-based passwords and password-based are the most common categories [5, 6]. It is the integration of special symbols, digits and alphabets because it is very simple to remember as well as can be altered to a distinctive number for key exchange protocols [7, 8]. In smart devices, text-based passwords are complex and incompetent due to limited screen size. For this reason, people are using small passwords that leads then susceptible to several attacks.

Additionally, when the password can be complex people requires to mark it down and tends to utilize single password for many devicesduring web application login [9]. Nevertheless, text-based is susceptible to several attacks like guessing attack, social engineering attack, brute force attack, shoulder surfing, dictionary cracking attack, password guessing attack, hotspot attack and so on [10, 11]. Therefore, an alternative graphical password has developed against text-based password for user authentication [12]. In the year 1996, the graphical password model was introduced by Blonder with the objective of minimizing the weakness of typical passwords and maximizing the security space [13]. The graphical password is recognized that humans normally contain better memory as well as recognition abilities for images compared to textual strings [14]. This remark has inspired the strategy of several graphical password models, which mostly encompass identifying or reproducing a sketch on images. In addition, when the number of acceptable images is huge enough, the password space of graphical password model can extent higher than alphanumeric password scheme, and so, the usage of graphical password may provide better resistant to various security attacks [15].

However, the prevailing graphical password models can be susceptible to different attacks such as brute force attack, smudge attack and shoulder surfing attacks and so on [16] [17]. Shoulder surfing, by employing direct

1Research scholar
Department of Computer Science & Engineering
Amity University
Raipur, (Chhattisgarh), India
priticgolar@gmail.com
2Associate Professor
Department of Computer Science & Engineering
Amity University
Raipur, (Chhattisgarh), India
rsharma1@rpr.amity.edu

observation schemes like video recorders, CC cameras or looking over someone's shoulder to obtain PINs, passwords as well as other sensitive personal data is a severe issue [18]. Moreover, one of the probable issue is gathering password through a malicious observer while entering the passwords by a user through classical input devices such as mouse, keyboard etc. Rather than hardware keyboards, the touch screens are more common in recent days because of providing conversant experience. However, the hacker will catch the password because of the smear left on the screen whereas, the remaining smear can be the side effects of touch screens. Frequently touched areas of the screen and latent smear can be applied to suppose a form of information leakage. Password guessing is considered as a strategy that includes trying to authenticate a specific user by systematically guessing of passwords.

On the other hand, brute attack is considered as one of the prominent attack that intents to analytically check each possible secret till the right one has been determined. In dictionary attack [19], the intruders try to crack a password-protection network, computer or other IT resources by analytically providing each word in the dictionary as a password till the exact one is determined [20]. While considering the hotspot attack, the suspicious Wi-Fi provider can utilize the hotspot itself for infecting the system with one or more threads. Many of the graphical password models have failed to challenge these attacks so discovering a solution to overcome these attack leftovers as an active study area.

The main contributions of the work are as follows:

- Presenting a detailed description about the security issues prevailing in the graphical password authentication systems.
- Elaborating the latest and important schemes established in literature in the sense of graphical password authentication systems.
- Presenting an application scenario to prove that the system is secure against different attacks and to introduce the advantages of the graphical password schemes.

1.1 Paper organization

The remainder of the paper is structured as follows: section 2 covers the graphical authentication schemes introduced in literature along with its types, section 3 discovers the important attacks existing in the graphical password authentication systems, section 4 provides the solutions for the discovered attacks along with attack proofs and section 5 concludes the paper.

2. Graphical Authentication Schemes

Graphical authentication is introduced as an effective alternative for text-based passwords claiming to the fact that the images can be much easily remembered compared to the texts. Based on its working, the graphical authentication systems can be classified into two such as recognition-based and recall-based schemes.

2.1 Recognition-based schemes

In this scheme, a set of images are presented to the users and they are allowed to select some images in the registration phase. The authentication gets completed when the user exactly selects the images that are already selected in the registration phase in the same order. Several techniques are established in literature for recognition-based authentication to attain higher performance globally. Among the existing schemes, passface[21] scheme is one of the most popular scheme that is based on choices. In this scheme, the authentication is done by making the users select images from a set of facial images. This is inspired from the concept that the human brain can remember human faces easily than the other objects. Another popular recognition-based scheme is the Déjà vu scheme [22] where a subset of images are selected by the users to construct a portfolio. Then for the login, the users are required to recall the subset of images chosen from a sample of decoy images. A panel of 25 images are provided as a set of decoy images to the user and they are allowed to select a total of 5 images that is from their portfolio. When the user selects all the images in the portfolio accurately, the process is termed to be successful. Though the % of success rate in this scheme is high, it takes a lot of time to get completed as the login time of the users are high and the network traffic is high due to delays. Even if the size of the password space is small, it is difficult for the users to exactly remember the chosen images in all cases. Also, the time taken in this scheme to create a password is 60 seconds whereas, for the textual based schemes is only 25 seconds.

To deal with one of the most important security issue called shoulder surfing, a scheme has been introduced known as the triangle scheme [23]. In this algorithm, the login phase is regulated where the users are required to select the pass-images that are selected at the time of registration. The users are required to select a total of 3 images to form a triangle shape in the password space to complete the authentication. Security is attained by enlarging the password space with more number of images so that the password would be harder to be predicted by the attackers. All the objects displayed in the password space varied sufficiently for the users to easily figure out the difference. One of the demerit of this scheme is that if the number of objects are very high,

it would be difficult for the users to exactly figure out the objects whereas, if the space is smaller, it would potentially be easier for the attackers to hack. Another scheme called the imagepass scheme [24] utilized single-object images to form the graphical password. The username can be selected by the user based on the preferred choice by the user. A graphical choice grid with images is displayed in the screen where the users can make graphical choice. When the images available does not match the user interest, they are allowed to load new set of images to make selection. A minimum of 4 images can be selected by the user and after enrolment, a set of 16 images with system chosen decoy and user chosen images are attached forever with the username. One of the demerit of the method is that the server is required to store a huge amount of images that makes the authentication process time consuming.

Another recognition-based methodology specifically designed for handheld devices is introduced in [25]. At the time of initial registration, the user is allowed to select a theme to acquire the thumbnail images and then, the order of the thumbnail images is utilized to create the password. After turning on the device, the user is requested to enter the exact order of the chosen thumbnails to complete login. To overcome the problem of small search space, another step where the users are allowed to simultaneously select two thumbnails is followed. The complexity in memorizing the password is one of the disadvantage of this method. A strategy to promote security against the shoulder-surfing attack is introduced in [26] known as the WYSWYE scheme. The term WYSWYE is an acronym for "Where You See is What You Enter". This is one of the easiest method that is based on tabular based reductions and pattern identification. It extracts the pattern of images within the grid and then maps the pattern to another grid. This method utilizes a challenge grid with decoy images and a response grid for the users to identify the password patterns. Though this method is effective than most other recognition-based strategies, the process of image selection is time consuming and hard for the users.

2.2 Recall-based schemes

In these schemes, the users should recall and reproduce the images that are earlier chosen or created by them at the time of registration. This scheme is again subdivided into two such as pure recall-based and cued recall-based schemes. In the former type, no clue is provided to the user while recalling or reproducing a password and in the latter type, a clue is provided to the user to recall a password. In case of cued recall, the user is provided with some hints to remember the password and is easier than the other type. Some the techniques under the recall-based schemes are reviewed below:

Passdoodle [27] is one of the popular recall-based technique that falls under the pure-recall based technique. This scheme involves handwritten text that is drawn on a touch sensitive screen using stylus. It has been proven that the doodles are harder to crack as there are a larger count of possible doodles available theoretically compared to other textual passwords. The problem of recognizing the password limits its widespread usage. Also, only a minimum number of machine identifiable doodles can be made that limits the system from recognizing the identifiable features from the doodles. Also, these techniques keep doodles as the only means of identification. When it comes to security, a threshold value of similarity is required to be set for the doodles drawn by the user to prevent unauthorized access. Another pure recall-based scheme called draw a secret (DAS) [28]where a user has to draw a simple picture over a 2D grid. An interface to the scheme is a rectangular grid where each cell in the grid is denoted using discrete rectangular coordinates (x, y). In this method, the user draws a stroke inside the cells of the grid and in the login phase, if the user draws the same stroke in the same sequence of cells, then the user is authenticated.

Another similar methodology is the qualitative DAS (QDAS) [29] which is an advanced version of DAS is a result of encoding every stroke in the grid. The encoding involves the starting cell along with the sequence of direction changes in the stroke comparative to the grid. Change in the direction indicates the change of the pen crossing a cell boundary compared to the cross in the previous cell boundary. It has also been observed in that research that the image containing more hotspot can be effectively used as a background image. Unlike the other methods, another method called Syukri algorithm [30] where users can draw their signatures using mouse has been introduced. This algorithm involved two main stages such as registration and verification. The user is asked to draw the signature in the registration phase and the signature area is extracted where, enlarging and scaling operations are performed. In the verification phase, the input is obtained and the signature parameters are extracted. Taking geometric average means and dynamic update of database, the verification procedure is conducted. The main significance of the approach is that the users are not required to remember the signatures whereas, the signatures are hard to be copied.

The cued recall-based schemes are reviewed here: PassPoint [31] is a cued recall-based scheme where a painting or picture with more possible click points (CPs) is used. The role of this picture is to help the user in remembering the CP. The user is allowed to choose different number of CPs from a single image in the registration phase and for login, the user is required to

select CPs in the same order within a particular tolerance area to match with the previously selected CPs. This method is capable of achieving higher entropy as there are more than hundreds of possible CPs that can be remembered in a challenge image. One of the main advantage of the method is that there is no requirement of artificial predefined CPs with well-specified boundaries. Another method known as background DAS (BDAS) [32] which is an improved version of DAS is introduced by adding an additional background image along with the drawing grid to acquire cued recall. This method is based on the users' secret in mind in selecting a particular point from the background image to draw the password. Based on the technique called "repeating a sequence of actions", a new method was put forth called Passlogix v-Go [33]that produces a password by chronological situation. Based on an environment, the background image is selected by the user and a series of items can be dragged to create a password. One of the disadvantage of this method is that the password becomes guessable when the environment space is small with limited items.

3. Attacks in Graphical Password Authentication Systems

Being a potential alternative to the text-based password systems, graphical authentication systems proved to be secure against different types of attacks. There are several attacks that arise in the graphical password authentication frameworks. The ultimate aim of any attack in an authentication system is to crack the user password and to acquire illegal access to sensitive information. These attacks are required to be identified and sorted out to ensure privacy and security to the users associated with the website login. A brief overview about the common attacks in the graphical authentication systems is provided below:

3.1 Brute force attack

Brute force is one of the common and most popular attack in the graphical password authentication systems where the attacker submits multiple passphrases and passwords with an aim of guessing the actual password. The hacker keeps checking the password until it matches with the original password created by the targeted user. The brute force attack is based on trial and error that is encountered to crack encryption keys, login credentials and passwords. Though this is an old attack, it is still followed and is effective among the hackers. There are five different types of brute force attacks as follows:

- ✓ Simple brute force attacks
- ✓ Hybrid brute force attacks
- ✓ Reverse brute force attacks
- ✓ Dictionary attacks
- ✓ Credential stuffing

3.1.1 Simple brute force attack: This is one of the common attack that is encountered by a hacker to obtain the login credentials of the user without the use of any software. This is carried out typically using PIN numbers or standard password combinations. This attack is termed as simple as it take advantage of the passwords that are simple and is guessable. The users following poor password etiquette and using the same password for different websites are prone to this attack.

*3.1.2 Hybrid brute force attack:*This type of attack is developed as a consequence of combining simple brute force attack with the dictionary attack. This attack is implemented by discovering the account login of a user by knowing their username. The exact password is obtained by the hacker based on some experiments with a letter, character and number combinations. This type of attack allows the hackers to predict passwords that are formed as a combination of letters, numbers, characters or random years.

*3.1.3 Reversebrute force attack:*This attack is formulated with the help of a known password acquired as a consequence of network breach. After that, a matching login credential is discovered by the hackers from a list of millions of usernames. Sometimes a weak password is also used by them to search in the database consisting of usernames.

*3.1.4 Dictionary attack:*This is a basic procedure of brute force attack in which a target is chosen initially and multiple tests are carried out on that target's username. The term dictionary attack is because of the usage of dictionaries by hackers to use multiple words to crack the password amended with numbers and special characters.

*3.1.5 Credential stuffing:*This type of attack search for users' credentials by taking advantage of their weak password etiquettes. The attackers make use of the already collected password and username combinations in other websites to gain additional access to other user accounts. This attack attains a higher success rate if the users use similar username and password for multiple accounts and social media profiles.

3.2 Shoulder surfing attack

Shoulder surfing or eavesdropping attack is the most common attack in any graphical password authentication systems and is one of the most successfully encountered attack. This attack is physically encountered where the attacker can physically view the keypad and device screen to acquire personal information of the users. For successful application of this attack, it is required for the attacker to stay close to the target. The victims are spied by the attackers via miniature cameras, binoculars or

other optical devices to obtain their credentials. In case of graphical authentication systems, the attackers tries to capture some snaps of the users' screen to obtain the password. There are several methodologies published in literature to deal with the shoulder surfing attack so that a better scenario for the authentication systems can be developed.

3.3 Replay attack

In this attack, an attacker detects a data transmission in a network and make it repeated or delayed using some fraudulent activity. This kind of delay is either created by the sender or by the malicious intruder who intercepts and retransmits the data. This attack is intended to fool the participants in the network who carried out data transmission into believing that they have successfully completed the task. This type of attack helps the attackers to gain access to the network and to acquire information that cannot be easily accessed or else complete a duplicate transaction.

3.4 Hotspot guessing attack

In the graphical password authentication systems, the CP based scheme is highly popular. In these schemes, the users rely on a sequence of points in the image to generate the password. The in-depth examination of these schemes proved that these schemes are vulnerable to predictability. Particular points in the image are more likely to be selected by the users that become the hotspots of the image. These hotspots can sometimes be predicted by the attackers to guess the password of the users. Some images consists of definite hotspots that can be easily predicted by the attackers. In some other images with abstract shapes in the background are also affected by the hotspot guessing attack problem that puts the practicality of click-based schemes under question.

3.5 Spyware attack

Spyware is a malicious software developed intentionally to gather information about the targeted user and sending to other user in view of harming the targeted user. For instance, the violating target user's privacy policies and causing damage to the devices' security. There are different types of spywares such as spybots, hijackers and keyloggers. Spyware based attacks is although uncommon in graphical authentication systems due to the complexities in exactly capturing the movements of mouse. The combinations of captcha along with pass images can be considered to be resistant against the spyware attacks.

4. Solutions for the Attacks Based on Proofs

There are several techniques and protocols introduced to demonstrate the effectiveness of the authentication systems in overcoming different website attacks. Some of the major proofs are explained under this section. The proofs for the security attacks existing in the graphical authentication system can be better explained under an application scenario.

4.1 3D Application scenario

Consider a website login where the user is asked to submit the credentials in the initial registration form. The initial page of the considered authentication system is displayed in Figure 1.

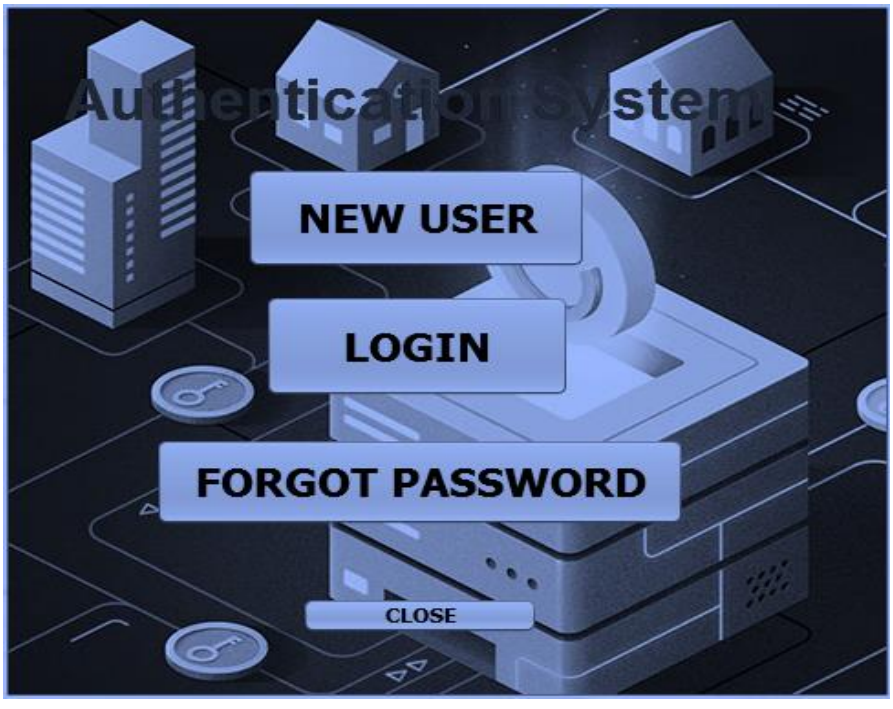

Fig 1: Initial page of the authentication system

The initial page of authentication system visible for the user consists of buttons like new user, login and forgot password with a close button at the end. For a new user entering the website for the 1st time, a registration form gets opened. The registration form obtains details such as the user's name, gender, age, occupation, contact number and e-mail id. The registration form is shown in Figure 2.

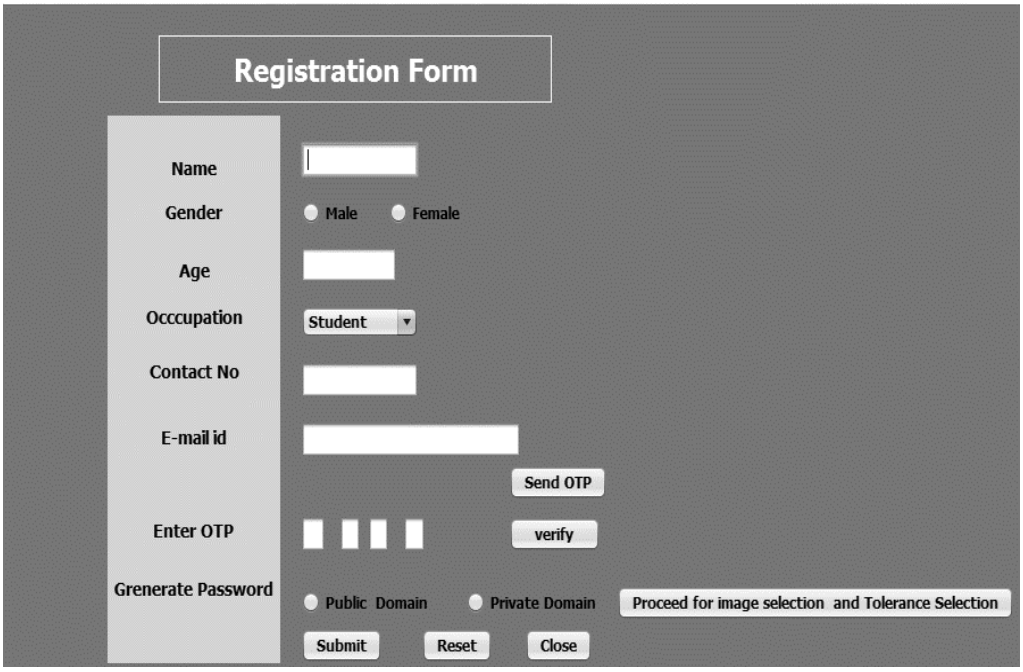

Fig 2: Registration form for user login

After obtaining the user credentials, an OTP will be sent to the user's registered mobile number. The user is asked to enter the OTP to complete the registration phase. After verification of OTP, password will be generated based on the CPs obtained from the user. For this, the user is asked to select either the private or public domain images. If the user selects the private domain images, then the user can upload the images of their interest saved in the system. Otherwise, in case of public domain images, the system randomly displays a set of images along with some threshold area for CP selection.

A threshold with option such as 50*50 or 25*25 can be selected by the user and then the password can be set by selecting a sequence of CPs from different images of their choice. The selected region in the image is highlighted in red colour square shape to confirm the area selected by the user. This helps the user to accurately differentiate the regions of the image from the selected region. The password is generated from the CPs based on the x and y coordinates of the point selected along with the image id.

#	UserName	Gender	Age	Occupation	ContactNo	EmailId	UserID	ChoiceOfImage	Password
1	Priti	Female	30	Other	2315843608	priti@gmail.com	Priti	private	img 11.81.91:img 9.102.114:img 5.92.167:img 6.57.160
2	Rudra	Female	29	Doctor	6315610674	rudra@gmail.com	Rudra	private	img 13.99.83:img 14.129.55:img 9.44.186:img 0.198.11
3	Raghav	Male	37	Prefessional	7654337518	raghav@gmail.com	Raghav	public	15.6.140:5.157.280:7.147.242:14.221.289
4	Komal	Male	46	Prefessional	0201427401	komal@gmail.com	Komal	private	img 13.150.76:img 0.100.181:img 3.130.130:img 2.71.106
5	Seema	Female	24	Faculty	6506520925	seema@gmail.com	Seema	private	img 10.113.130:img 12.86.5:img 9.191.10:img 5.146.136:img 4....
6	Sarika	Female	46	Faculty	3988318349	sarika@gmail.com	Sarika	public	14.299.127
7	Ruku	Female	31	Faculty	2622017298	ruku@gmail.com	Ruku	private	img 11.138.185
8	Vishu	Male	45	Doctor	4961405774	vishu@gmail.com	Vishu	public	9.204.300:11.231.48:17.318.163
9	Ritik	Male	31	Prefessional	7197985944	ritik@gmail.com	Ritik	public	4.210.175:6.303.178:2.283.346:15.191.315:16.175.155:17.10...
10	Ritika	Female	34	Faculty	4230741602	ritika@gmail.com	Ritika	private	img 1.181.39:img 1.156.36
11	Shruti	Female	39	Doctor	3651491632	shruti@gmail.com	Shruti	public	9.344.122:0.290.321:7.241.105:10.278.305
12	Mala	Female	32	Faculty	8800427576	mala@gmail.com	Mala	private	img 6.140.10:img 11.12.129:img 5.56.155:img 1.84.8:img 5.112...
13	Rohan	Male	24	Prefessional	0400505001	rohan@gmail.com	Rohan	private	img 0.74.185:img 14.171.117:img 5.61.151:img 10.111.134
14	Mintu	Female	27	Doctor	2763163857	mintu@gmail.com	Mintu	private	img 5.149.127:img 2.129.146
15	Neela	Female	22	Doctor	9910234851	neela@gmail.com	Neela	private	img 3.131.52:img 11.79.37:img 0.0.43:img 8.45.103:img 0.195....

Fig 3: Database for storing the password

The users are then trained with the sequential steps of registration to demonstrate the success ratio of the application. After training, the credentials obtained from each user along with the password are stored in the database as shown in Figure 3.

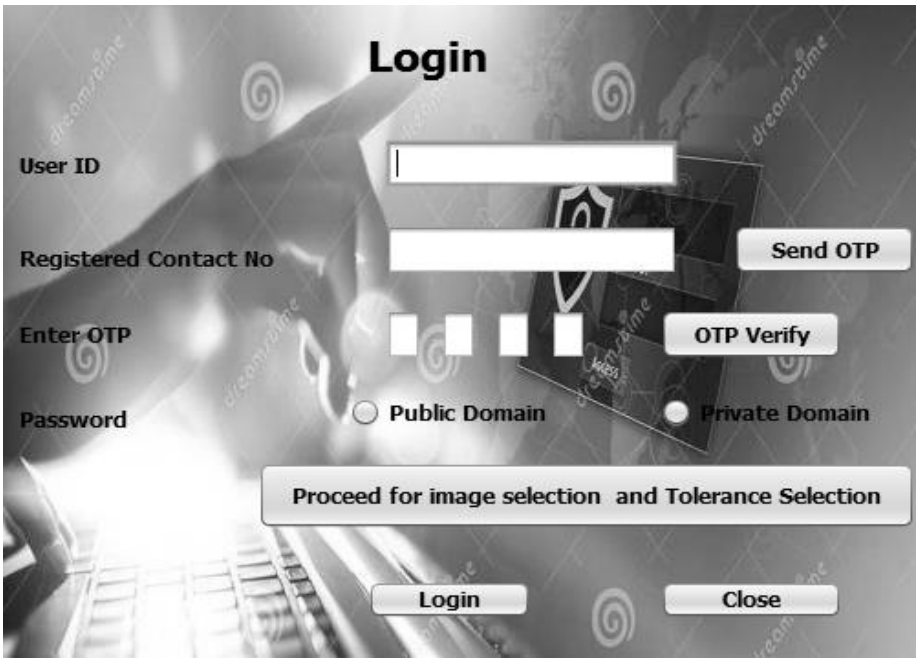

Fig 4: Login page for the authentication system

After the registration phase, the login phase is initiated where the user is provided with a login form as in Figure 4. The login form ask about the user credentials such as user id and registered contact number and an OTP is sent to the number. After verification of OTP, the password is required to be verified. For this purpose, the system displays some images that are selected by the user in the registration phase along with some random images as in Figure 6.

Some random images are provided along with the selected images to enhance the overall security of the network. The user is then asked to select the images accurately that are already selected by the user in the registration phase for CP generation.

After selecting the required images, the user is provided with a 3D cube structure where each of the faces of the cube displays one selected image by the user. The selection is restricted to a maximum of 6 images as the cube consists of only 6 faces. If the user selects less than 6 images in the last screen, then the remaining faces of the cube is filled with random images selected by the system. From the cubic structure, the user is asked to select the CPs previously selected by the user in the registration phase.

If the CPs selected by the user in the login phase matches with the CPs selected in the registration phase, then the authentication process is termed to be successful. Otherwise, 3 chances are provided to the user and then forgot password option is provided to set the password again.

In the above application scenario, the graphical password is generated based on CP selection. A sequence of CPs selected from multiple images are selected in the same order under a given threshold area in the 3D environment to complete the authentication process. In general, the CP selection based graphical authentication system is vulnerable to several types of attacks and the considered application scenario is evaluated with the help of certain significant proofs.

4.2 Zero knowledge proof

Zero knowledge protocol [34] is one of the popular protocol used to prove that an authentication system is shoulder surfing resistant. The major fact about the protocol is that it is trivial to prove that a party possess knowledge about an information by just revealing it whereas, the challenge is to prove that possession without using any additional information or without revealing the information. A special case in the protocol is that it consists of a fact that the party possess the secret information. Another case is that the interactive zero knowledge protocol requires interaction between the party proving the knowledge and the validator validating the proof.

Consider that the party needed to prove the secret information as party 1 and the validator to validate the secret information as party 2. Without revealing the secret information to party 2, it is important for party 1 to prove the knowledge it has. To achieve this objective, it is required for party 1 to solve a “hard problem”. Here, “hard problem” takes the definition that it is simple to solve if the secret is known and extremely hard if it is unknown. Thus, by solving this problem, party 1 can prove their knowledge to party 2. It is noteworthy that the hard problem is required to be carefully designed such that party 2 is unable to obtain any information

about the secret by observing the solution of party 1.To attain such scenario, party 1 can authenticate itself to party 2 and also avoids revealing the secret to the shoulder surfer (S).

4.2.1 Depiction

At this stage, it is important to design the hard problem so that the above scenario could be well explained. It is also important that the designed hard problem is secure and is without any complexities in the authentication process. Initially perform random clustering of the CPs in the image that is visible in the screen. Then, the hard problem lies in the selection of the required CP that is selected by the user at a particular image in a particular order. Here, it is considered that party 1 is aware of the CP and S is unaware of the required CP from a particular image. Since party 1 is aware of the CP, it is easy for it to choose the exact CP from the image whereas, S is unaware of the CP is has no clue about how to select the right CP from the image.

4.2.2 Analysis

The security of the system is verified here in terms of password entropy and shoulder-surfing resistance. The mathematical formulation to compute password entropy can be given as follows:

$$En(X) = N * \log_2(N * C * R) \tag{1}$$

where, N indicates the total number of images, C represents the total click points selected from the image and R indicates the total number of runs. Based on the value of the password entropy, it is depicted that the third party can make random guessing of the password. When the value of the password entropy is high, it is obvious that the S is unable to guess the password. This analysis proves that a trade-off is achieved between the shoulder surfing and password guessing attacks.

The shoulder surfing resistance is proved by evaluating the considered application scenario based on the number of attempts needed for S to identify the exact password. The best case for S occurs when it is able to identify the exact password in the second observation. This occurs when the CP is put on different clusters for every round without any overlapping with other CPs. If this scenario is encountered, then S is able to interpret the right password after observing the scenario twice. Also, in the worst case, it takes infinite number of observations for S to interpret the right password due to the existence of overlapping of the CPs from different images.

Based on the best and worst case scenarios, it is important to identify the approximate number of observations needed to discover the exact password. Let $\wp_s(M)$ indicates the probability for S to reveal the password after observing the scenario for M number of observations. Thus, the probability of revealing all the CPs to S in <=M observations can be given as follows:

$$\wp_l(\mu \le M) = \left[\sum_{\mu=1}^{M} \wp_s(M)\right]^N \tag{2}$$

From the above formulation, the probability of revealing all the CPs in M observations can be identified. This can be mathematically given as follows:

$$\wp_l(M) = \wp_l(\mu \le M) - \wp(\mu \le M - 1) \tag{3}$$

The total count of observations required for S to identify the password can be computed using the above formulations as follows:

$$\overline{M}_l = \sum_{\mu=1}^{\infty} \mu \wp_l(\mu) \tag{4}$$

In general, it is complex to identify the value for $\wp_s(M)$. Let us consider $|C_P|$ as the CP list selected by a particular user for login and κ be the clustered subsets of CPs so that κ divides $|C_P|$. For instance, consider the value for $|C_P|$ as 4 and κ as 2. The value for $\wp_s(M)$ can now be calculated as follows:

$$\wp_s(M) = (2/3) * (1/3)^{M-2} \tag{5}$$

Based on the formulation, the average number of observations required for an attacker with $N = 4$ is obtained as 3.39. This means that S requires more than 3 observations of the scenario to interpret the actual password. Though it is the considered case, it is nearly impossible for S to actually interpret the right password in reality. Thus, the presented application scenario can be considered to be resistant to the shoulder surfing attack. Also, the success probability for shoulder surfing can be further reduced by increasing the size of the CP list or by increasing the total number of rounds.

4.3 Convex hull algorithm proof

The convex hull algorithm [35] is an enhanced version of the triangle scheme used to prove that a graphical authentication system is resistant to shoulder surfing attacks. Under a complex scenario, this algorithm is used to prove that a system is resistant to the attack in a much accurate manner. This proof protects the graphical

password scheme from shoulder surfing based on direct observation and video recording. The convex hull algorithm is utilized in the authentication phase to identify the convex polygon fenced by password CPs. The users' authentication takes place within the region of the convex polygon. After this step, the users are allowed to choose points within the polygon structure rather than directly selecting the CPs. Since the location for CPs are randomly generated, the convex polygon's region is also different. Apart from this, not all the CPs are simultaneously displayed on the screen. A minimum of three CPs are chosen by the user for convex polygon construction. The CPs are required to be identified by the users and they should click on some random points within the region to complete the authentication.

When a shoulder surfer observes the login of the user, it is highly difficult for him/her to recognize the actual CPs selected as the users are allowed to randomly select the regions in the space. While the user is aware of the CPs they have selected in the registration phase, they can easily localize the regions covering the required CPs. On the other hand, it is highly difficult for the attackers to obtain the password as they are unaware of the CP as well the region where the CP is located. The convex hull polygon is drawn in the password space by connecting the CPs and a minimum of 3 CPs results in an exact polygon. In some cases of accidental logins, some main modifications are required to be carried out in the scheme. The probability of being within the convex hull is set to same in almost the entire region of the polygon except on the borders. Also, multiple challenges are provided to the user to complete the entire login phase for successful authentication. Though this algorithm is time consuming, it has proved to withstand weak shoulder surfing attacks.

5. Conclusion

In this paper, a detailed security analysis is presented while exploring different attack scenarios in the websites. Initially, the authentication schemes that are introduced in literature based on the recognition and recall based schemes are analysed. Then, the major security threats associated with the authentication schemes are explored. An application scenario is then introduced to prove that the system is secured against the shoulder surfing attack. The zero knowledge proof protocol is then utilized to prove that the system is secured against the attack in all the scenarios. The advantage of the CP selection in protecting the credentials of the user and the dominance of it over the other schemes is realized through the analysis. In future, it is planned to introduce a new graphical password authentication scheme exploring the 3D environment and developing multiple 3D structures for password generation.

References

[1] Faraji, Sepideh, and Kooroush Manochehri. "Attack Resistant Graphical Password Authentication Method Against Shoulder Surfing, Smudge and Brute Force Attacks." Smudge and Brute Force Attacks.

[2] Ho, Yean Li, Siong Hoe Lau, and Afizan Azman. "Comparison Between BlindLogin and Other Graphical Password Authentication Systems." In International Conference on Advances in Cyber Security, pp. 235-246. Springer, Singapore, 2019.

[3] Kovalan, Krishnapriyaa, Siti Zobidah Omar, Lian Tang, Jusang Bolong, Rusli Abdullah, Akmar Hayati Ahmad Ghazali, and Muhammad Adnan Pitchan. "A Systematic Literature Review of the Types of Authentication Safety Practices among Internet Users." International Journal of Advanced Computer Science and Applications 12, no. 7 (2021).

[4] Kamegne, Yvonne, Eric Owusu, and Joyram Chakraborty. "Bridging the Gap Between Usability and Security: Cultural Adaptation of a Graphical User Authentication." In International Conference on Human-Computer Interaction, pp. 260-269. Springer, Cham, 2022.

[5] Edward, Audu Lovingkindness, Hassan Umar Suru, and Jasmyne Okudo. "Position-Based Multi-Layer Graphical User Authentication System." American Journal of Software Engineering and Applications 11, no. 1 (2022): 1-11.

[6] Khodadadi, Touraj, Yashar Javadianasl, Faranak Rabiei, Mojtaba Alizadeh, Mazdak Zamani, and Saman ShojaeChaeikar. "A Novel Graphical Password Authentication Scheme with Improved Usability." In 2021 4th International Symposium on Advanced Electrical and Communication Technologies (ISAECT), pp. 01-04. IEEE, 2021.

[7] Shah, Abhishek Narayan, Dipti Anand, Sabyasachi Samanta, and Dipankar Dey. "Graphical Password Authentication System Using Modified Intuitive Approach." Int. J. HIT. TRANSC: ECCN. Vol 7, no. 2A (2021): 64-71.

[8] Yadav, Bipin, Kaptan Singh, and Amit Saxena. "Video Based Graphical Password Authentication System." In International Conference on Network Security and Blockchain Technology, pp. 78-90. Springer, Singapore, 2022.

[9] Sreelekshmi, K. U., Soja Sam, T. T. Samjeevan, and Sneha Mathew. "Web based Graphical Password Authentication System."

[10] Arun Kumar, S., R. Ramya, R. Rashika, and R. Renu. "A survey on graphical authentication system resisting shoulder surfing attack." In Advances in Artificial Intelligence and Data Engineering, pp. 761-770. Springer, Singapore, 2021.

[11] Isah Atsu, Sani Suleman, John Kolo Alhassan, and Abdulmalik Danlami Mohammed. "A SURVEY ON GRAPHICAL BASED AUTHENTICATION MODEL FOR SECURE ELECTRONIC PAYMENT." International Conference on Emerging Applications and Technologies for Industry 4.0| EATI 2020, 2020.

[12] Patel, Shikhar Singh, Akarsh Jaiswal, Yash Arora, and Bharti Sharma. "Survey on Graphical Password Authentication System." Data Intelligence and Cognitive Informatics (2021): 699-708.

[13] Ho, Yean Li, Siong Hoe Lau, and Afizan Azman. "Comparison Between BlindLogin and Other Graphical Password Authentication Systems." In International Conference on Advances in Cyber Security, pp. 235-246. Springer, Singapore, 2019.

[14] Juneja, Kapil. "An XML transformed method to improve effectiveness of graphical password authentication." Journal of King Saud University-Computer and Information Sciences 32, no. 1 (2020): 11-23.

[15] Parish, Zach, Amirali Salehi-Abari, and Julie Thorpe. "A study on priming methods for graphical passwords." Journal of Information Security and Applications 62 (2021): 102913.

[16] Yang, Gi-Chul. "Development status and prospects of graphical password authentication system in Korea." KSII Transactions on Internet and Information Systems (TIIS) 13, no. 11 (2019): 5755-5772.

[17] Abdalkareem, Zahraa A., Omar Z. Akif, Firas A. Abdulatif, A. Amiza, and PhaklenEhkan. "Graphical password based mouse behavior technique." In Journal of Physics: Conference Series, vol. 1755, no. 1, p. 012021. IOP Publishing, 2021.

[18] Abass, Islam Abdalla Mohamed, Loay F. Hussein, and Anis Ben Aissa. "New Textual Authentication Method to Resistant Shoulder-Surfing Attack." International Journal of Advanced Computer Science and Applications 13, no. 1 (2022).

[19] Gopali, Saroj, Pranaya Sharma, Praveen Kumar Khethavath, and Doyel Pal. "HyPA: A Hybrid Password-Based Authentication Mechanism." In Future of Information and Communication Conference, pp. 651-665. Springer, Cham, 2021.

[20] Zouave, Erik, Marc Bruce, Kajsa Colde, Margarita Jaitner, Ioana Rodhe, and Tommy Gustafsson. "Artificially intelligent cyberattacks." (2020): 50.

[21] Biddle, Robert, Sonia Chiasson, and Paul C. Van Oorschot. "Graphical passwords: Learning from the first generation." *Ottawa, Canada: School of Computer Science, Carleton University* (2009).

[22] Dhamija, Rachna, and Adrian Perrig. "Deja {Vu--A} User Study: Using Images for Authentication." In *9th USENIX Security Symposium (USENIX Security 00)*. 2000.

[23] Wiedenbeck, Susan, Jim Waters, Leonardo Sobrado, and Jean-Camille 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. 2006.

[24] Mihajlov, Martin, Borka Jerman-Blazic, and Marko Ilievski. "Recognition-based graphical authentication with single-object images." In *2011 Developments in E-systems Engineering*, pp. 203-208. IEEE, 2011.

[25] Jansen, Wayne. "Authenticating users on handheld devices." In *Proceedings of the Canadian Information Technology Security Symposium*, pp. 1-12. 2003.

[26] Khot, Rohit Ashok, Ponnurangam Kumaraguru, and Kannan Srinathan. "WYSWYE: shoulder surfing defense for recognition based graphical passwords." In *Proceedings of the 24th Australian Computer-Human Interaction Conference*, pp. 285-294. 2012.

[27] Varenhorst, Christopher, M. V. Kleek, and Larry Rudolph. "Passdoodles: A lightweight authentication method." *Research Science Institute* (2004): 1-11.

[28] Jermyn, Ian, Alain Mayer, Fabian Monrose, Michael K. Reiter, and Aviel Rubin. "The design and analysis of graphical passwords." In *8th USENIX Security Symposium (USENIX Security 99)*. 1999.

[29] Lin, Di, Paul Dunphy, Patrick Olivier, and Jeff Yan. "Graphical passwords & qualitative spatial relations." In *Proceedings of the 3rd Symposium on Usable Privacy and Security*, pp. 161-162. 2007.

[30] Eljetlawi, Ali Mohamed. "Study and develop a new graphical password system." PhD diss., UniversitiTeknologi Malaysia, 2008.

[31] Wiedenbeck, Susan, Jim Waters, Jean-Camille Birget, Alex Brodskiy, and Nasir Memon. "PassPoints: Design and longitudinal evaluation of a graphical password system." *International journal of human-computer studies* 63, no. 1-2 (2005): 102-127.

[32] Dunphy, Paul, and Jeff 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. 2007.

[33] Hafiz, Muhammad Daniel, Abdul Hanan Abdullah, NorafidaIthnin, and Hazinah Kutty Mammi. "Towards identifying usability and security features of graphical password in knowledge based authentication technique." In *2008 Second Asia International Conference on Modelling & Simulation (AMS)*, pp. 396-403. IEEE, 2008.

[34] Li, Zhi, Qibin Sun, Yong Lian, and Daniele D. Giusto. "An association-based graphical password design resistant to shoulder-surfing attack." In *2005 IEEE international conference on multimedia and expo*, pp. 245-248. IEEE, 2005.

[35] Gamby, Ask Neve, and Jyrki Katajainen. "Convex-hull algorithms: Implementation, testing, and experimentation." *Algorithms* 11, no. 12 (2018): 195.

[36] Mr. Rahul Sharma. (2018). Monitoring of Drainage System in Urban Using Device Free Localization Neural Networks and Cloud computing. International Journal of New Practices in Management and Engineering, 7(04), 08 - 14. https://doi.org/10.17762/ijnpme.v7i04.69

[37] Mwangi , J., Cohen, D., Silva, C., Min-ji, K., & Suzuki, H. Improving Fraud Detection in Financial Transactions with Machine Learning. Kuwait Journal of Machine Learning, 1(4). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/148

[38] Kathole, A. B., Katti, J., Dhabliya, D., Deshpande, V., Rajawat, A. S., Goyal, S. B., .Suciu, G. (2022). Energy-aware UAV based on blockchain model using IoE application in 6G network-driven cybertwin. Energies, 15(21) doi:10.3390/en15218304