Improved Design of Convex Hull Click (CHC) Graphical Password Scheme

By
Zohaib Shahid
NUST201464160MSEECS63114F

Supervisor
Dr. Shahzad Saleem
Department of Computing

A thesis submitted in partial fulfillment of the requirements for the degree of Masters in Information Security (MS IS)

In
School of Electrical Engineering and Computer Science,
National University of Sciences and Technology (NUST),
Islamabad, Pakistan.

(July 2018)

Approval

It is certified that the contents and form of the thesis entitled "**Improved Design of Convex Hull Click (CHC) Graphical Password Scheme**" submitted by **Zohaib Shahid** have been found satisfactory for the requirement of the degree.

Advisor: **Dr. Shahzad Saleem**

Signature: _____

Date: _____

Committee Member 1: **Dr. Mehreen Afzal**

Signature: _____
Date: _____

Committee Member 2: **Mr Ubaid-Ur-Rehman**

Signature: _____
Date: _____

Committee Member 3: **Mrs Hirra Anwar**

Signature: _____
Date: _____

Abstract

Passwords have always played a crucial role in cybersecurity. As known, alphanumeric passwords are commonly used for authentication but they suffer from issues of usability and shoulder-surfing. By introducing new practices, like obligatory inclusion of special characters for better security, it has become increasingly difficult for humans to remember passwords. This results in people choosing weak and easy-to-remember passwords which lead to security breaches. Graphical password schemes are a favorable alternative to textual passwords because research, in psychology, shows that humans are better at recognizing than recalling. Although graphical password schemes offer better usability, they are susceptible to shoulder-surfing too. Some graphical password schemes do exist, which are shoulder-surfing resistant and possess an appropriate degree of usability. Convex Hull Click (CHC) graphical password scheme is one such scheme which lessens the cognitive load on the user and mitigates shoulder-surfing more effectively, as compared to others. Although being still in its research phase, it holds great potential for use in the industry but like any other password scheme, it suffers from some attacks, which are, the brute-force attack and three probabilistic attacks. If the security issues of this password scheme are reduced while maintaining its ease-of-use, it can become a proper authentication scheme for the industry.
The main objective of this research was the development and analysis of improved versions of CHC password scheme with a suitable balance between security and usability. By studying and analyzing other graphical password schemes and their techniques for resisting attacks and providing good enough usability, two variants of CHC scheme, named Centroid-Oriented Convex Hull Click (CO-CHC) and Rogue CHC password schemes were developed. Both schemes tackle different issues of security of CHC password scheme. A usability study was done to analyze the variants and compare them with each other and with CHC scheme. The results showed that both variants have trade-offs but they improve CHC password scheme and present new directions for research on graphical password schemes.

Dedication

I am hugely thankful to Allah Almighty as He is the One who opened my mind to this research problem and helped me in producing a novel solution. Without His help, none of this would have been possible in the first place. First of all, I dedicate this work to my parents, who have always loved, supported and been my primary mentors in not just education, but in every area of my life. Their prayers and efforts have always shaped my life into a better form. A pat on the back, from them, has helped me a lot to stand up to every challenge in life. I cannot be more thankful to my wife for loving and supporting me throughout the tedious journey of research even when I was not able to give proper time to our family. Without her patience and help, it would not have been possible to carry out and conclude this work properly.
I thank my siblings for keeping my morale up throughout this long period of research, especially when it seemed that a proper solution cannot be reached. Lastly, I owe a lot to my friends and colleagues at KTH Information Security Research Lab, SEECS and NUST for helping out in brainstorming at every stage of research and never letting me down.

Certificate of Originality

I hereby declare that this submission is my own work and to the best of my knowledge it contains no materials previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any degree or diploma at NUST SEECS or at any other educational institute, except where due acknowledgement has been made in the thesis. Any contribution made to the research by others, with whom I have worked at NUST SEECS or elsewhere, is explicitly acknowledged in the thesis.

I also declare that the intellectual content of this thesis is the product of my own work, except for the assistance from others in the project's design and conception or in style, presentation and linguistics which has been acknowledged.

Author Name: **Zohaib Shahid**
Signature: _____

Acknowledgment

First of all, I acknowledge the commendable efforts and patience of Dr. Shahzad Saleem, Dr. Mehreen Afzal and sir Fahad Satti who helped in shaping this research idea from scratch, producing and analyzing a viable and feasible solution. I am immensely thankful to Mr. Hamza Rehman, Ms. Fatima Mahmud and Mr. Ali Azlan for their help and noteworthy effort in developing CHC password scheme and the variant password schemes and careful testing and analysis of them.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

Since a long time in the world of technology, there has always been a significant need for security of the data of users. Considering the systems, which store such sensitive data, the mainstream security procedure is identification and authentication on the part of the user (Brostoff and Sasse, 2000). In short, a proper access control is always in place to prevent illegitimate users from exploiting the data or the system. By going through identification, a legitimate user tells the system that he or she has the right to access a system and use the data, stored within. Now, the user has to assure the system that he or she is indeed a legitimate user. This is the most important part as the resilience of the authentication mechanism is tested. This is what security researchers strive to strengthen.

In practice, there are three main types of authentication, which are employed for security. These authentication mechanisms are also called human identification protocols (Matsumoto, 1991). The types of authentication are given below (Brostoff and Sasse, 2000; Perrig, 2000).

1. **Knowledge-based Authentication**: This type of authentication is related to knowing something or having it in one's memory, which is to be given to the computer system. The user knows and recalls a secret word or phrase called a password (alphanumeric or textual), which has to be shared with the computer system, in order to access the data (Brostoff and Sasse, 2000).

2. **Token-based Authentication**: The user possesses something physical, like a token, which has to be used to access a system. The common type of token is a card like an ATM card or smart card. The main requirement is that this token should not be stolen or if it is stolen, it should be very difficult to forge it (Brostoff and Sasse, 2000).

3. **Biometric Authentication**: Considering this type, the user has to use the uniqueness of his or her anatomy or behavior to get authenticated. When the characteristics of his or her anatomy match with the electronic equivalent of those characteristics in the computer system, he or she gains access. Such characteristics include, but are not limited to fingerprint, retina and voice.

As known, knowledge-based authentication is the most frequently used type of authentication. Unlike token-based authentication, where a belonging is required to get authenticated and it is a cause of inconvenience as people forget to carry their token sometimes, only a password is to be recalled to gain access. Also, the token may get lost or be stolen, which can lead to a potential security breach. Thus, in the case of token-based authentication, extra care and security has to be employed like knowing what has to be done if the token is lost. Biometric authentication is quite unique but there is extra cost as specialized devices have to be installed to authenticate the user (Perrig, 2000). There is always a considerable percentage of false negatives and false positives. So knowledge-based authentication is cost-effective as no extra hardware is required. This human identification protocol requires the user to use his or her cognitive ability, which is recalling of a suitable secure password, to get authenticated. According to (Matsumoto, 1991), a proper knowledge-based authentication has entities, which are, the prover (human) and the verifier (computer system). The verifier will prompt the prover for the password and will only accept that password if and only if that password matches with the registered counterpart in the system.

Security researchers have strived a lot to create better password systems or Leakage Resilient Password Systems (LRPS) to deal with threats. In textual passwords, there always have been a tradeoff between security and ease of remembering. New password practices include the inclusion of capital letters, small letters, numbers and special characters in the password to increase its strength. Proactive and reactive password checking has been introduced, in order to enable users to build better passwords and other important developments have followed. New and advanced attacks are carried out on alphanumeric password systems every day and they are more resilient accordingly.

There are problems of security and memorability with these passwords whose solutions seem to get increasingly complex (Wiedenbeck et al., 2005). If alphanumeric passwords are made more complex by adding numbers, special characters, uppercase and lowercase letters, it becomes very difficult to memorize such passwords. The users reject them and use meaningful and simple passwords, which are vulnerable to cyber-attacks (Perrig, 2000). It can

be said that textual password systems have not been developed with the human users in mind as their usability issues have increased a lot (Wiedenbeck et al., 2005). Another critical issue is that alphanumeric password systems are susceptible to shoulder-surfing. Even if the password is displayed in the form of special characters, on the screen, like on the screen of an ATM, the keyboard or the keypad is still visible to the adversary. Even if the keyboard or the keypad is hidden, an adversary can study the movements of the hands of the user and can guess the password.

As observed over the years, graphical password schemes have proven to be a good alternative to alphanumeric passwords. They also come under the category of knowledge-based authentication because basically, pictures have to be retained by one's memory to get authenticated. The images in a graphical password jog a user's memory and help him or her retain the secret better. Considering humans, it is much easier to recognize something or someone than to recall (Perrig, 2000). Since the first graphical password scheme, made by Blonder in 1996 (Wiedenbeck et al., 2005), a lot of graphical password schemes have been developed which deal with different issues of security and usability. Through experiments, it has been shown that the latest graphical password schemes are resistant to shoulder-surfing. So it can be said that the issues of security and memorability, faced by the textual passwords, have been solved by graphical password schemes, to some extent thus a potential solution can be provided by them. The details of how graphical password schemes have solved these problems, have been discussed later. During the study of the former research on graphical password schemes, a graphical password scheme named Convex Hull Click (CHC) scheme was found, which is still in its research phase but has been deemed to be shoulder-surfing resistant and easy to use. After studying this scheme further, it was found out that after some improvements, this password scheme could be used in the industry. These improvements involved making CHC scheme resistant to two known attacks while also making sure that the ease of use, offered by it, did not suffer. The two attacks are the Random Click Attack, a type of brute force attack faced by many types of graphical password schemes, and an attack based on a geometrical technique (specific to CHC scheme only). These attacks have been described in detail later.

Following this idea for the research thesis, two variants of CHC password scheme, named Centroid-Oriented Convex Hull Click (CO-CHC) scheme and Rogue CHC scheme were developed and analyzed along the parameters of efficiency, effectiveness and user satisfaction. This analysis was done by carrying out an in-depth usability study and a comparison was made between CHC password scheme and these variants. After analysis, it was found out that both variants had their trade-offs between security and usability like

CO-CHC scheme offered better security than Rogue CHC scheme but Rogue CHC scheme was easier to use. So it can be said that the balance between security and usability is hard to achieve but both schemes improved the current state of CHC graphical password scheme. Also, this research can be used to improve CHC scheme further, develop new and different graphical password schemes and help in achieving a suitable trade-off between security and usability.

This research thesis has been divided into 7 chapters. In Chapter 2, the development of different graphical password schemes, over the years, has been described. Convex Hull Click graphical password scheme and its flaws, in security, have been discussed in detail. Chapter 3 explains how design science methodology, which is a type of research methodology, was used to carry out this research. The two proposed variants, CO-CHC password scheme and Rogue CHC password scheme, have been described along with how they tackle the problems of CHC password scheme, in Chapter 4. In Chapter 5, it has been explained how the usability study, for the analysis of the variants, was set up and carried out. The usability study consisted of three phases, which have been described in detail in this chapter. With the help of graphs, the analysis of the variant password schemes and CHC password scheme has been elaborated and discussed in Chapter 6. Chapter 7 concludes this research along with some suggestions for further research in this area.

Chapter 2

Literature Review

This chapter explains about the types of graphical password schemes and how the idea of graphical password schemes came into being. It highlights different graphical password schemes, developed through the ages, and the problems tackled by every scheme. The developments till Convex Hull Click (CHC) scheme, which is the main emphasis of this research, are given. CHC scheme has been discussed in detail in this chapter, including the different attacks on it, and it has been explained how its improved version can be used as a suitable authentication scheme for the industry.

2.1 Human Identification Protocols

The basic concepts of human identification protocols and the involved mathematics, along with a comprehensive discussion on graphical passwords has been given by (Asghar, 2012). The details of basic attacks on human identification protocols and an adequate literature review of a number of different protocols, have been presented. The basic idea of developing a password scheme, whereby secure communication could be carried out over an insecure channel, was presented in (Matsumoto, 1991). It was emphasized that such a password system should be made where an eavesdropper will gain nothing by eavesdropping. A diagram, explaining the protocol, in (Matsumoto, 1991), is displayed in Figure 2.1. The user was only required to memorize a number to generate the answer so the negative load was quite less.

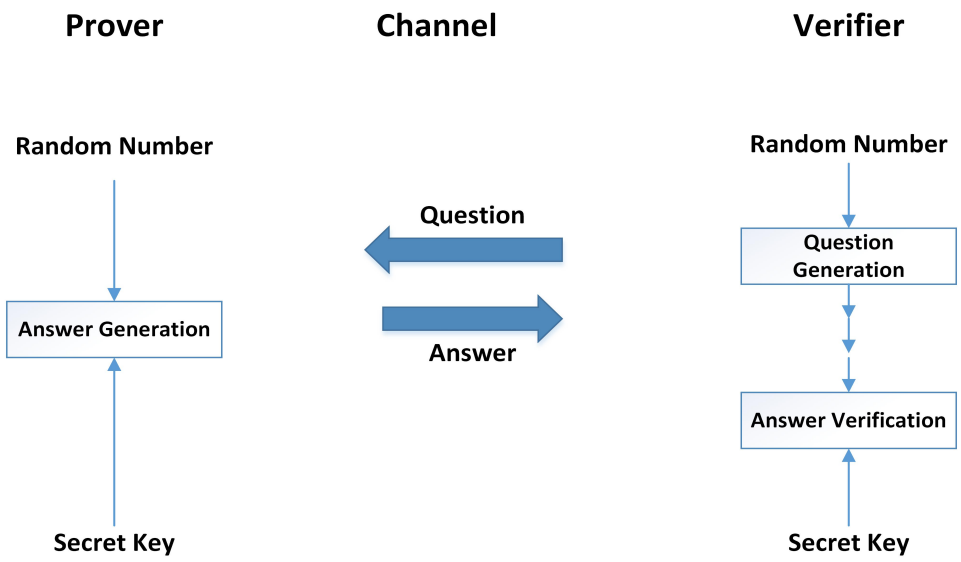


Figure 2.1: Authentication Protocol (Matsumoto, 1991)

An analysis of this scheme was done and two attacks, on this scheme, were proposed in (Wang et al., 1995). The attacks were the passive attack and the challenge replay attack. An adversary carries out the passive attack by observing the user's response to a challenge and tries to guess the secret key. In the challenge response attack, the attacker masquerades as the host, intercepts a valid challenge and replays it to the prover. After receiving a number of answers to the replayed challenges, the attacker analyzes the answers and tries to extract the secret key. The solution, given by the authors, was that the secret key should be randomized for every new session between the verifier and the prover. This would not allow the attacker to do guess work and get the secret key by analyzing the answers to the user.

A number of authors, afterwards, analyzed the password scheme of (Matsumoto, 1991) and proposed new attacks or suggested improvements. Considering the attacks on the original scheme, a new password scheme was proposed, along with analysis, in (Matsumoto, 1996). Also, two extended protocols were presented and analyzed. In (Hopper and Blum, 2001), the renowned Hopper-Blum (HB) protocol, based on an NP-hard problem was presented. The authors also showed how the protocol of (Matsumoto, 1991) can be broken after analyzing a few authentication sessions. A detailed cryptanalysis of the password scheme in (Matsumoto, 1996) was done and presented in (Li and Shum, 2003).

2.2 An Introduction to Graphical Passwords

Considering the threats faced by these protocols, researchers began looking more into developing graphical passwords. They wanted to present a suitable alternative to textual passwords. Some practical solutions were proposed. The first graphical password scheme was introduced by Blonder in 1996 (Wiedenbeck et al., 2005). In his scheme, the user had to click on some chosen regions of an image, presented on a screen, about which only he or she knew. The user would be logged in, if the correct regions were clicked on. Otherwise, the user would be rejected. The main types of graphical password schemes are given below (Li and Shum, 2005).

1. Selective Pictures Based password scheme
2. Point-and-Click password scheme
3. Drawing-based password scheme

Selective pictures based password schemes require the user to select his or her secret images or pass-images from many displayed decoy images. Such schemes include Passfaces (Brostoff and Sasse, 2000), Dej'a Vu (Perrig, 2000) and Visual Identification Protocol (VIP) (De Angeli et al., 2002). A user is required to click on previously chosen secret locations in an image, in the case of point-and-click password schemes. An example is Passpoints (Wiedenbeck et al., 2005). Considering drawing-based password schemes, a user has to draw a simple image to get authenticated, like in the case of the pattern recognition password scheme, which is commonly used in Android operating system. The most popular graphical password schemes are the pattern recognition password scheme in Android operating system and the picture password scheme in Windows operating system. In Figure 2.2, the different types of graphical passwords are shown.

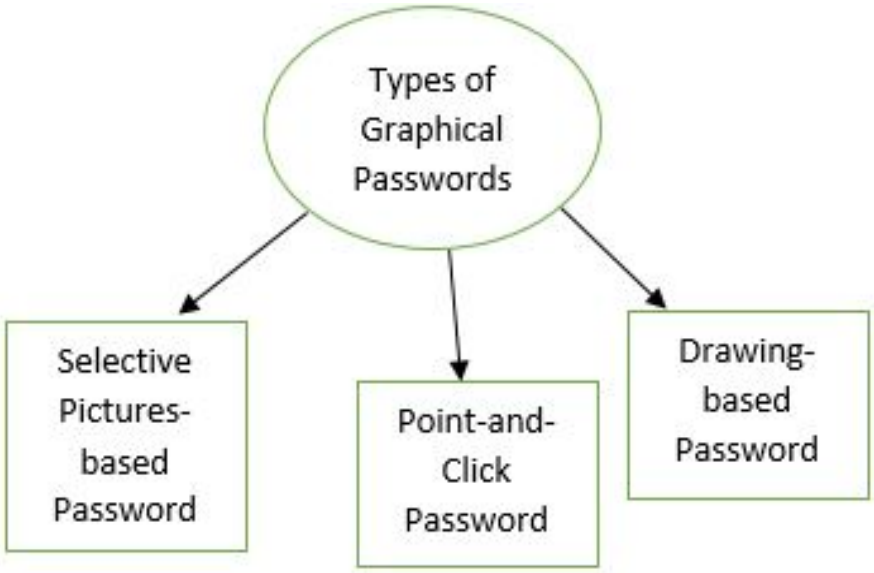


Figure 2.2: Types of Graphical Password Schemes

2.3 A Review of Graphical Password Schemes

Some early graphical password schemes were Passfaces, Dej'a Vu, VIP and Passpoints. These schemes were built on very simple concepts and were easy to understand. They have been discussed in detail in this section.

2.3.1 Passfaces

In Passfaces (Brostoff and Sasse, 2000), a user had to select and memorize 4 faces, out of a number of faces, which would be his or her secret, in the registration phase. In the authentication phase consisting of four rounds, with each round containing nine faces, the user had to select his or her secret face or "passface", to get authenticated. None of the faces were repeated and the positions of the faces were randomized, thus protecting against packet-sniffing. An example of a grid, used in Passfaces, is given in Figure 2.3.

Figure 2.3: An example of a grid used in Passfaces (Brostoff and Sasse, 2000)

2.3.2 Dej'a Vu

Considering Dej'a Vu (Perrig, 2000), the user had to create a portfolio of p secret images out of a set of sample images. Abstract images were used to provide some protection against guessing attacks because the adversary would not be able to know the user's choice, even if he or she had some personal information about the user. During the authentication phase of a single round, the prover had to select all of his or her secret images from a challenge set, containing n images, to log in. The example of a grid of images, used in Dej'a Vu, is displayed in Figure 2.4.

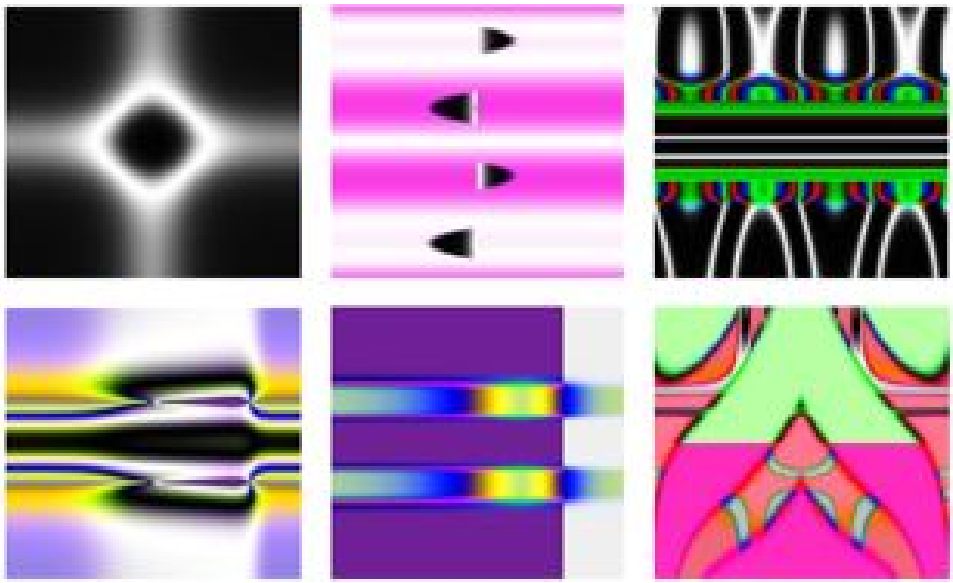


Figure 2.4: Authentication Grid in Dej'a Vu (Perrig, 2000)

2.3.3 Visual Identification Protocol and Passpoints

A graphical password scheme, built as an improvement of Dej'a Vu, was Visual Identification Protocol (VIP) (De Angeli et al., 2002). In this paper, three versions of this scheme, namely VIP1, VIP2 and VIP3 were proposed. All of these had varying qualities. VIP3 will be discussed here as it was the most complex of these three and explored the limit of the graphical approach, as stated in (De Angeli et al., 2005). Instead of allowing the user to make his or her own portfolio, the user was assigned a portfolio of eight secret pictures, which had to be memorized. By not allowing the user to select his or her portfolio, the simple guessable pictures were avoided. Also, as the user did not have to spend time in selecting the secret pictures, the efficiency of the system became better. In the authentication phase, consisting of only one round, a challenge set of sixteen images, containing twelve decoy and any four secret images, was displayed. In every authentication phase, the images used to be in a random order. The users had to select all of their secret images to get authenticated. The pictures were colourful, detailed and meaningful so they could be remembered better by the user. An example challenge set of pictures, used in VIP, is shown in Figure 2.5.

Figure 2.5: Challenge set of VIP (De Angeli et al., 2005)

Concerning Passpoints (Wiedenbeck et al., 2005), a user had to select a number of arbitrary points, in an image, as the password. To get authenticated, the user has to click on or close to all of the secret points.

2.3.4 Cognitive Authentication Scheme (CAS)

The 4 schemes, described previously, were quite practical and did not put a lot of cognitive load on the user but all of them were susceptible to shoulder-surfing. A skilled adversary could easily observe the sessions and know the images, in the case of Passfaces, Dej'a Vu and VIP, and click points, in the case of Passpoints, and compromise the password scheme. To cope with this problem, some solutions were proposed. In (Weinshall, 2006), Cognitive Authentication Scheme (CAS) was presented, which had 2 variants, namely the high-complexity query version and the low-complexity query version. In the high-complexity query version, the user had to memorize 30 pictures, which were fixed by the system, out of a set of 80 pictures. Then, a grid of these 80 pictures was presented to the user with a multiple-choice question at the top of the grid. Figure 2.6 shows the grid, of pictures, used in CAS.

Figure 2.6: Grid, in CAS, for authentication (Weinshall, 2006)

To get authenticated, the user had to make a mental path from the top-left picture, in the grid, to the bottom or the bottom-right end of the grid. If a secret picture is reached, the user should move one picture down. Otherwise, the user should move, one picture to the right. As seen in Figure 2.6, numbers are displayed on the bottom and right panels of the grid and there is one number alongside each image. When the user got to a picture at the bottom or the right-most end, the answer, to the MCQ, was the number alongside that picture. The distribution of the numbers (0, 1, 2 and 3) is such that the probability to reach any one of these numbers is 0.25.

Considering the low-complexity query, similarly, the user had to memorize a secret subset of fixed 60 pictures, out of 240 pictures. During the authentication round, 20 pictures were shown, with 10 pictures assigned with the value 0 and the rest of them assigned with the value 1. The user had to study the panel from left to right and find the first, second and the last picture of his or her secret subset. A multiple choice question, consisting of 2 options (0 or 1), was asked in this version. The user had to answer whether the majority of the values, associated with the pictures, was 0 or 1. The authors described two attacks, on this scheme, and the mechanisms to protect from them, namely the brute-force attack and the enumeration attack (statistical analysis attack). CAS had proved to be secure against shoulder-surfing as the attacker cannot see what path is being computed by the user.

2.3.5 Foxtail Protocol

Foxtail Protocol, a textual password protocol known for its stability and good performance, had been implemented in the form of a graphical password scheme (Li and Shum, 2005). The diagram of the implementation of this graphical password scheme is given in Figure 2.7.

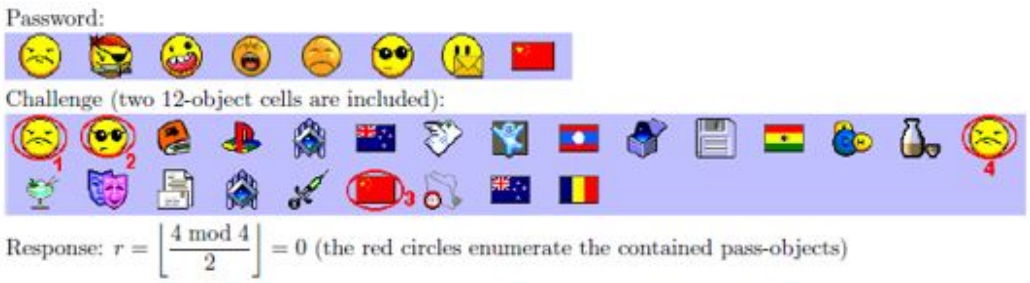


Figure 2.7: Graphical password, based on Foxtail (Li and Shum, 2005)

As shown in Figure 2.7, the user had to memorize the given small images as his or her secret images. In a challenge, the prover had to count the secret images given. Then, he or she would use the number in the relation, given in Figure 2.7, to calculate the response and send it to the verifier. The security of this protocol, against brute-force attacks and shoulder-surfing had been analyzed and shown to be quite satisfactory.

2.4 Development of Convex Hull Click (CHC) Password Scheme

Considering the growing problem of shoulder-surfing and the difficulty of use, a different type of graphical password scheme, named Triangle Scheme was suggested by the authors in (Sobrado and Birget, 2002). An image of the GUI of their scheme is displayed in Figure 2.8.

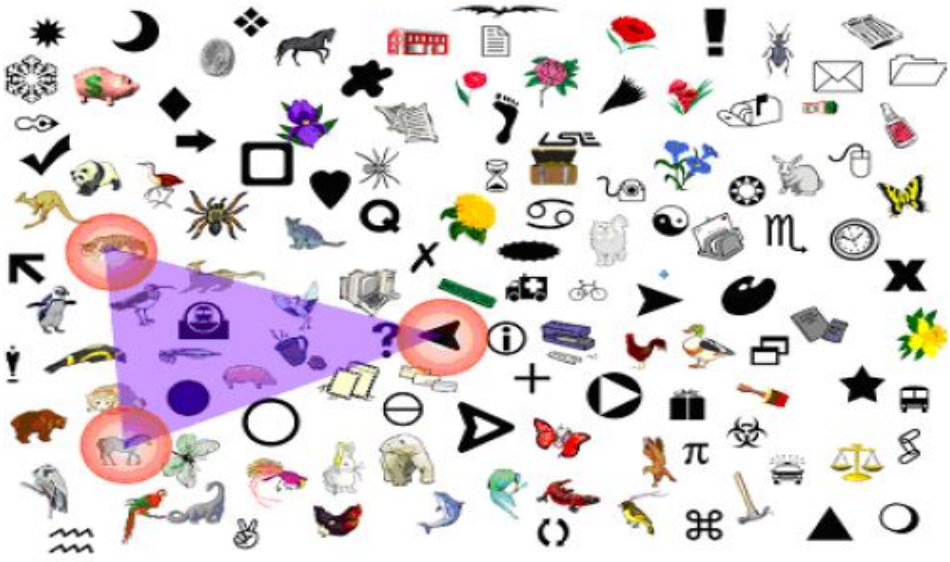


Figure 2.8: Triangle Scheme (Sobrado and Birget, 2002)

According to this scheme, a user selected three icons as the secret icons or pass-icons. The users had to identify their secret icons, which are marked red in Figure 2.8, among a number of icons displayed during a specific number of rounds of authentication. Please note that the secret icons were not marked like that when the scheme was used in real. This triangle was drawn mentally by the users and they had to click inside the invisible triangle to gain authentication. This scheme was made to be fun and easy-to-use and was shoulder-surfing resistant because the secret icons are not revealed directly to the attacker.

Based on Triangle Scheme, Convex Hull Click (CHC) Graphical Password Scheme was developed and introduced (Wiedenbeck et al., 2006). In Figure 2.9, an image of the user interface of this scheme is shown.

Figure 2.9: CHC Scheme with 4 pass-icons (Wiedenbeck et al., 2006)

In the setup phase of this scheme, a user had to select five pass-icons. The authentication phase consisted of ten rounds. During one authentication round, the users identified their pass-icons on the screen, made a mental convex hull, enclosing all the pass-icons and clicked in it to move to the next round.

CHC scheme was deemed to be shoulder-surfing resistant, easy-to-use and the cognitive load was not a lot as only five icons had to be memorized. The usability study indicated that many users, despite the long period of time spent in authentication, found this scheme to be quite practical. Nonetheless, some considerable attacks were carried out on CHC scheme. Their details are in the next section.

A variant of this scheme, named S3PAS, was also proposed (Zhao and Li, 2007). In this scheme, alphabets, numbers, special characters and other symbols were used instead of graphical icons. Four characters were selected by the user as the secret characters or pass-characters. At one time, only three out of four secret pass-characters were displayed. In a single round, a user had to click inside the triangle formed by his or her pass-characters, called pass-triangle. The user could also enter the character (session pass-character) seen inside the triangle. The GUI of this graphical password scheme is shown in Figure 2.10.

Figure 2.10: Graphical User Interface of S3PAS (Zhao and Li, 2007)

2.5 Attacks on CHC Password Scheme

CHC password scheme suffers, mainly, from two types of attacks, namely the brute force attack and statistical analysis attack or the probabilistic attack (Asghar, 2012; Asghar et al., 2013; Yan et al., 2012). These attacks have been explained in the subsections ahead.

2.5.1 Brute Force Attack

In the brute-force attack (Yan et al., 2012), an adversary would list all the possible combinations of the graphical icons, that is, combinations of five icons each, which could be used as the password. After making a verification algorithm, similar to the one used by the scheme, the adversary used it to test all the combinations. This process would be repeated until the set of passwords narrowed down to a single password. There are two important points for the success of this attack, which are as follows.

1. The verification algorithm, for the attack, should have the same efficiency as the verification algorithm for CHC protocol.

2. The average shrinking rate of the password set should be equal to **((Average success rate of the guessing attack) - 1)**.

Another type of brute force attack, which involves less working as compared to the technique described earlier, is the Random-Click attack. In this attack, the adversary makes a random click in every authentication round in the hope that he or she has clicked inside the convex hull. Although the chances of success of this attack are quite small but if a large convex hull is produced in every round, the chances of success can increase sufficiently. This attack is commonly faced by many other point-and-click graphical password schemes because the main principle of these password schemes is the clicking on a portion of the screen recognized by the user.

2.5.2 Probabilistic Decision Tree Attack

Considering the probabilistic decision tree attack (Yan et al., 2012), the adversary tries to determine the decision path of a user. A decision path is the decision process of the user which involves finding the secret graphical icons or the combination of the secret icons on the screen, in order to place a valid click point. The steps taken for this attack are given below.

1. Calculate all the possible combinations of the icons, that is, all possible combinations of three icons.
2. Make a score table containing two columns. One column is for listing the different combinations of icons and the other column is for listing the value of conditional probability for each combination.
3. Observe the challenge-response pairs.
4. Considering a single click-point, "C", note down all the possible combinations (decision paths) from the score table.
5. Assign a probability, based on a uniform distribution, to these combinations, $\mathbf{p(X)}$.
6. Calculate the sum of all individual values of probabilities, $\mathbf{p_c}$.
7. Find out the conditional probability of each decision path, $P(X|C) = p(X)/p_{\mathbf{c}}$.
8. Add this value of conditional probability in front of the concerned combination of icons in the score table.
9. Repeat the process for all rounds and keep filling the table.

As a result of this attack, an adversary has found the combinations with the high values of $P(X|C)$ because they contained one or more pass-icons. A higher value of $P(X|C)$ also means that one or more of the icons, in that combination, appeared often in the challenges. As every pass-icon had to appear in most of the challenges, this means that such combinations would definitely have some, if not all, of the pass-icons. Table 2.1 gives an example of a table made for this attack.

Table 2.1: Table for the Probabilistic Decision Tree Attack

Combination	Conditional Probability ($P(X\|C)$)
Combination 1	a
Combination 2	b
Combination 3	c
Combination 4	d

2.5.3 Counting the Number of Icons

In this statistical analysis attack (Asghar et al., 2013), an adversary made a score table of all the graphical icons, appearing on the screen. He or she counted the number of times, each icon appeared in each challenge and filled the table accordingly. Then he or she filtered out the icons, which occurred the most number of times, considering all the challenges. Most of such icons were the pass-icons because they have to appear in every challenge. Table 2.2 is an example of a table used for this attack.

Table 2.2: Table for the Counting Attack

Graphical Icons (n)	No. of Appearances
Icon 1	6
Icon 2	9
Icon 3	7
Icon 4	5

2.5.4 Attack based on a Geometrical Technique

This statistical analysis attack, described in (Asghar et al., 2013), used a quite intelligent approach to find the pass-icons. First of all, the attacker would make a score table for all the possible combinations of the icons. Then, he or she would observe a click-point in one round and capture a screenshot. A diagrammatical representation of this attack is given in Figure 2.11.

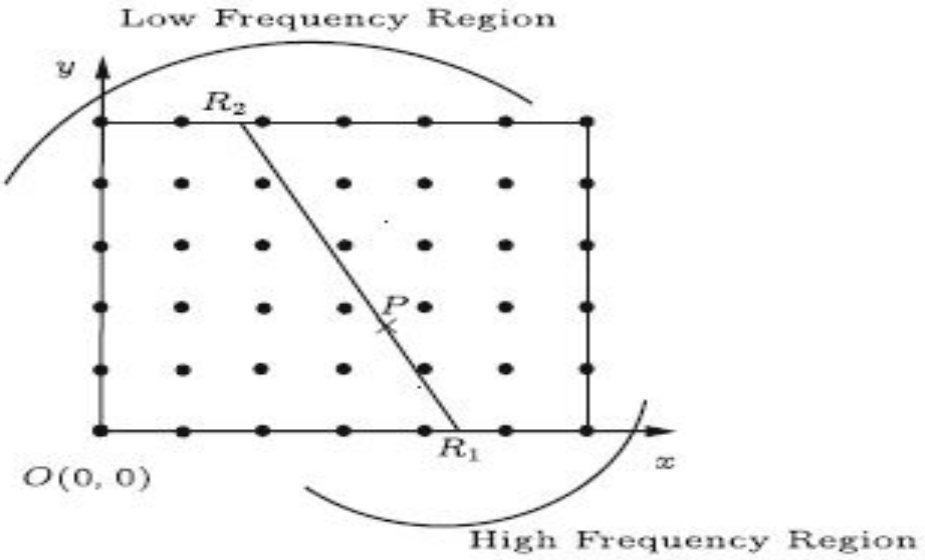


Figure 2.11: Geometrical Technique of attack on CHC scheme (Asghar et al., 2013)

As seen in Figure 2.11, a line would be drawn, by the adversary, through the click-point and the screenshot would be divided into 2 regions such that there was an equal number of icons in both of the regions. Then, the adversary would label the shorter segment of the line as R_1P and the longer segment as PR_2. The icons, near or around the shorter line segment, were the ones which had a higher number of occurrences over all challenges. Hence, the secret icons would be among those icons as they had to appear in all the challenges. This was also proven by the fact that the click-point was closer to the region of the screenshot, where the shorter line segment was. The icons, near the longer line segment, would have a less number of occurrences, considering all challenges. Therefore, these icons were mainly decoy icons. That was further verified by the click-point being away from that region of the screenshot. Thus, PR_2 was called the low-frequency region and R_1P was called the high-frequency region. This geometrical technique would

be carried out on all the captured screenshots of the rounds and the high-frequency region would be checked. The adversary would match the icons, in the high-frequency region, with the ones in the combinations in the score table. Eventually, he or she would come to know about the pass-icons.

2.5.5 Chosen Test Set Attack

An improved variant of the previous attack, the Chosen Test Set Attack, is also present. In this attack, only those challenge-response pairs (click-points) were considered, which were closest to the boundary of the grid of the icons. Such challenge-response pairs were known as the Test Sets. Considering those click-points, it could be said that some of the secret icons were near the boundary of the grid and would have a higher value of frequency of occurrence. Thus, only the combinations of icons, having the icons near those click-points, would be checked from the score table. The icon(s), which would be occurring with a high frequency, in the matched combinations, could be considered as the secret icons. The main advantage of this attack is that only some click-points would have to be considered and the effort to find the secret icons was reduced.

2.5.6 Analysis of CHC scheme and the Attacks on it

The main drawback of CHC scheme is that an attacker does not need to know all the pass-icons to impersonate the user. He or she can know about the other pass-icons by checking the type of pass-icons, already obtained. For example, if the pass-icons, obtained, are flags of countries, then the attacker will know that the other pass-icons will also be flags.

Considering the types of attacks carried out on CHC password scheme, it can be said that the probabilistic attacks pose a greater threat, as compared to the brute force attack. The brute force attack can be mitigated by limiting the number of attempts to log in, by the user. An example of limiting the number of attempts can be that if a user fails in at three attempts to log in, he or she locked out of the system. In probabilistic attacks, there is always a higher chance of finding the password icons because the set of icons, which has to be searched to obtain the password icons, is reduced by the methods of the attacks. By using the techniques of probability, a reduced set of icons, which has a higher frequency of occurrence, is obtained like in the case of the Probabilistic Decision Tree Attack. The same happens in the case of the attack, based on a geometrical technique and the Chosen Test Set Attack. The overall time, taken to crack the password, is reduced along with the effort. The initial effort will be a lot because all the possible combinations

of the icons have to be considered but the attack helps to eliminate many combinations of the graphical icons. An added advantage to the brute force attack and the statistical analysis attacks is that even if two password icons of the user are found out, the attacker can impersonate the user if he or she can understand the types of graphical icons, preferred by the user.
A way to reduce the chance of success of the probabilistic attacks and the brute force attack is to confuse the attacker. If the click-point is placed outside the convex hull, the number of icons, which can be considered as the password icons, will increase along with the effort of the attacker. As the user clicks away from the password icons, the attacker is diverged accordingly. The proposed improved schemes take help of this idea and will be explained later.

Chapter 3

Research Methodology

3.1 Research Approach

Considering the different kinds of password schemes, there are a lot of interconnected factors to consider. Although increased security is a critical need nowadays but the non-technical factors, that is, the human beings, have to be given equal importance. This is because human beings are the ones who are going to be the actual users of any method of authentication. Better security practices can only be developed and promoted if humans find a password scheme, either textual or graphical, to be psychologically acceptable. Therefore, the tradeoff between security and usability has to be developed in such a way that human beings can adapt easily to it. Another point to be remembered is that the majority of the users, of any password scheme, are not a part of a technical field like information technology. So the complexity has to be kept at such a level that all users (technical or laymen) find least difficulty in understanding the scheme. Thus, behavioral research, for studying the non-technical factors, was also made a part of this research. It was made sure that all factors, related to a graphical password scheme, are studied and a secure, yet practical solution is presented.

The research was divided into two phases. In the first phase, the basic concepts of human identification protocols were understood along with the idea of secure communication over an insecure channel. The problem of shoulder-surfing was studied. After understanding the different types of graphical passwords and their evolution through the years, Convex Hull Click (CHC) graphical password scheme was discovered. After studying this scheme and the attacks on it, two new graphical password schemes were developed with the idea of providing better security and usability. The second phase was the testing phase in which a detailed usability study of these schemes was done.

A set of university students were instructed to use the password schemes and some metrics were recorded. Later, these metrics were analyzed to assess the efficiency and effectiveness of the two variants. Through this behavioral research, a clear idea was obtained about the practicality of these schemes.

3.2 Relation of Design Science and the Presented Research

In this research, work has been done to solve a certain problem, that is, critical attacks on graphical password schemes. Two new variants of Convex Hull Click password scheme have been proposed and designed to counter shoulder-surfing. By doing an extensive usability study, the practicality of these variants has also been justified to some extent. Thus, an effort has been made to tackle the problem with the theoretical, as well as, practical aspect in mind. Such research, which aims to solve problems, can be done better by using "a design science approach" (Piirainen et al., 2010). According to (Wikipedia, 2017), in design science, the focus is on developing and evaluating the performance of a designed artifact with the target of improving the functional performance of the original artifact. The areas, where design science is most applied, are engineering and computer science. This is because when artifacts, like algorithms and human/computer interfaces are redesigned or reevaluated, the focus is on solving specific problems. According to (March and Smith, 1995), the difference between natural science and design science is that the former tries to understand reality while the latter attempts to create it. The products of design science approach serve human purposes, usually. The evaluation of these products is done to prove their performance, improvement, value and utility (March and Smith, 1995). The suggested technical solution, in this research, was tested for its utility, improvement and performance. In design science, innovation is the main part whereby new ideas, practices and products, are created for serving humans more efficiently (Denning, 1997). In this research, new password schemes were developed which would mitigate the mentioned attacks and also, be easy to use for humans. According to Aken, design science aims to solve improvement and construction problems, in order to implement an innovation (Aken, 2004).

The explanation, given by Aken, also corresponds with this thesis. One of the basic objectives of this research was the extension of the theoretical basis as an innovation. The extensions, here, were the new password schemes, built upon the idea of the original Convex Hull Click graphical

password scheme. These extensions tackle some specific attacks on the original password scheme while maintaining the ease-of-use and the game-like feel of the original scheme. Another innovation was to bring the attention of the research community towards development of graphical password schemes. Despite the problems of these schemes, if formidable effort is placed in developing them, they can surely be a good alternative to textual password schemes. In short, design science research methodology is chosen because it helps in testing both the theoretical and practical features of our designed artifacts. This work is focused on the "improvement problem", as discussed by Aken (Aken, 2004).

3.3 Process of Research

The research process, carried out, will be mapped onto the design science research process in this section. According to (Takeda et al., 1990), design science research process comprises of five sub-processes, which are listed below.

1. Awareness of the problem
2. Suggestion
3. Development
4. Evaluation
5. Conclusion

The same concepts about design science research are put forward in (Kuechler and Vaishnavi, 2004). The five different phases of design science research method have been shown in the form of Figures 3.1 and 3.2 (Takeda et al., 1990; Kuechler and Vaishnavi, 2004). These figures have helped in understanding this research method properly.

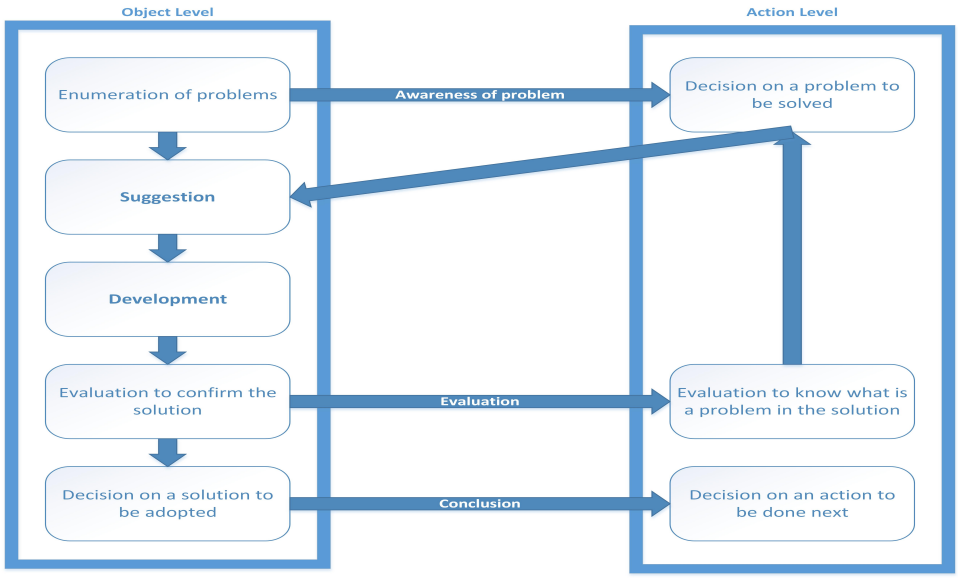


Figure 3.1: Design Cycle (Takeda et al., 1990)

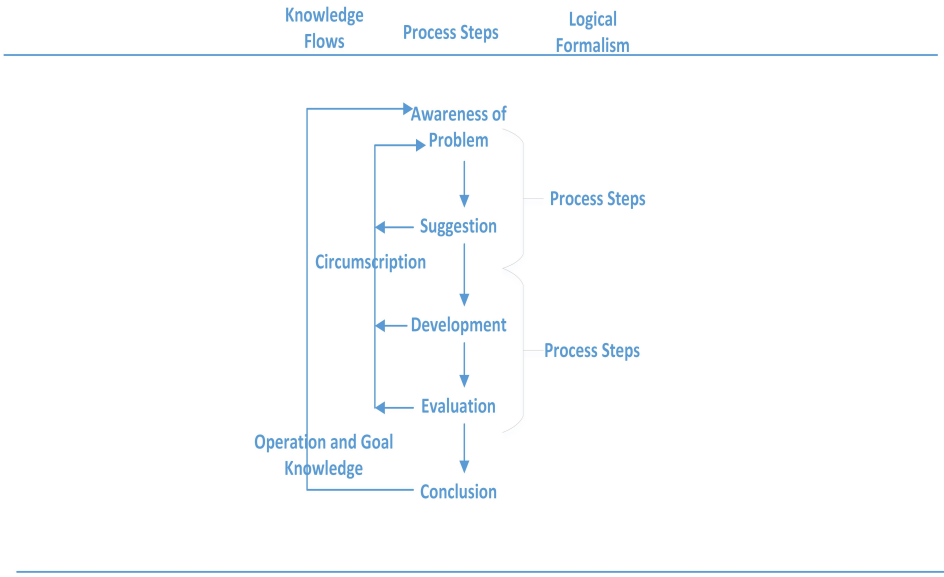


Figure 3.2: Reasoning in the Design Cycle (Kuechler and Vaishnavi, 2004)

3.3.1 Awareness of the Problem

During the first phase of design science research methodology, a researcher makes himself or herself familiar with the problem and its related domain. Also called "improvement research", design science research demands awareness of a problem so a suitable solution can be suggested to it (Kuechler and Vaishnavi, 2004). By comparing the object, under consideration, with its specifications, a problem is identified in this phase (Takeda et al., 1990). Studying and understanding the related domain was the first phase in this research. The basic concepts of human identification protocols or passwords were understood (Matsumoto, 1991; Asghar, 2012) . The problems of the popular alphanumeric passwords, such as shoulder-surfing and less psychological acceptability, were understood. The concepts of graphical passwords were built alongside. In order to understand the research done on graphical passwords, different graphical password schemes and the attacks, on them, were studied (Brostoff and Sasse, 2000; Perrig, 2000; De Angeli et al., 2002; Wiedenbeck et al., 2005; Weinshall, 2006; Li and Shum, 2005). Through this study, it came to be known that graphical password schemes also suffered from shoulder-surfing but they were more psychologically acceptable to users. There was a need for a password scheme which would mitigate the issue of shoulder-surfing, as well as, give a good degree of usability. Then, a graphical password scheme, named Convex Hull Click password scheme, was discovered (Wiedenbeck et al., 2006). It was deemed to be resistant to shoulder-surfing, fun and easy-to-use. The attacks, on this scheme, were understood with the aim of improving it for proper use in the industry (Yan et al., 2012; Asghar et al., 2013).

3.3.2 Suggestion

During the first phase, the knowledge base for the domain and the awareness of the problem was built. Based on these, a solution was suggested. In this phase, mainly, the following two steps were taken.

- For solving the problem, the required key concepts were suggested (Takeda et al., 1990).
- A solution, to the current problem, was inferred from the knowledge base of the domain (built during 'Awareness of the problem' phase) by using abduction (Kuechler and Vaishnavi, 2004).

The gathered knowledge helped in understanding graphical password schemes thoroughly along with their limitations and the attacks on them.

In addition, the tradeoff between security and usability was understood. Thus, two variant password schemes, based upon Convex Hull Click password scheme, were suggested. They tackled two different types of attacks. It was also made sure that the variants were as easy-to-use as the original password scheme.

3.3.3 Development

In this phase, the implementation of an artefact is done in the light of the suggestion phase (Kuechler and Vaishnavi, 2004). If anything unsolved comes up, the whole design cycle should be repeated (Takeda et al., 1990). The two suggested graphical password schemes were developed in this phase and prepared for testing. Following the method in (Wiedenbeck et al., 2006), a partial solution was also developed for the evaluation of the performance of the suggested solution. This partial solution would also help in finding out if any improvement can be made.

3.3.4 Evaluation

During the evaluation of the solution to find issues in performance and suggest further improvement, a new iteration of the design cycle is needed if any problem is found (Takeda et al., 1990). It should be remembered that, in a typical design science approach, the development, evaluation and suggestion phases are performed iteratively (Kuechler and Vaishnavi, 2004). A usability study, according to the one in (Wiedenbeck et al., 2006), was planned and carried out for finding out any issues with the usability of the variant password schemes. The usability study measured the effectiveness and efficiency of the developed password schemes. Effectiveness told about how much difficulty was faced by a user in the logins of a password scheme. The parameter of efficiency told about how much time was taken during the correct rounds and logins of the password schemes. This parameter helped in telling about the learning curve of the password schemes and the time taken by the users to get accustomed to the schemes. Through this usability study, it was found out that the newly developed password schemes did offer an adequate degree of security. The usability of one scheme was found to be better than the other.

3.3.5 Conclusion

This phase helps in offering a probable solution and/or changing the description of the objects (Takeda et al., 1990) and signals the end of a design

research project (Kuechler and Vaishnavi, 2004). The knowledge, obtained as an outcome of this research, was shared and disseminated in this phase. Particular solution, in the form of two new password schemes, were suggested along with a supporting usability study. These password schemes were built after proper consideration of the balance between security and usability. Also, one common attack and an attack, specific to CHC password scheme only, was tackled by the variant password schemes. Further research work can be carried out by modifying the techniques of geometry used in CHC scheme.

Chapter 4

Proposed Graphical Password Schemes

Convex Hull Click (CHC) Graphical Password Scheme holds great potential for research due to its usability and uniqueness. It can be developed into a strong alternative to other mainstream password schemes but just like with any password scheme, there are some critical issues. Even with the quality of being shoulder-surfing resistant, it is vulnerable to a significant number of attacks. As mentioned before, those attacks are the brute-force attack and some probabilistic attacks. Although the brute-force attack can be avoided by setting a specific number of password attempts, the probabilistic attacks cannot be avoided because they exploit some mathematical anomalies in the password scheme itself. Concerning the fast advances in cybersecurity in the world of today, attackers have evolved to become more intelligent. With their good knowledge of computing and mathematics, they can understand the mechanics of a password scheme and exploit the flaws within. Concerning CHC graphical password scheme, if a significant amount of research is put into it, a strong password scheme can be created for a variety of users.

It should be understood that there is a critical tradeoff between the security and usability of a password scheme. The security and usability, of a password scheme, have an inversely proportional relationship. The researchers of cyber security, have always strived to strike a balance between these two properties but it is a tedious task. Some compromise has to be made, always. Keeping the task of maintaining the delicate balance between security and usability, this research is directed towards developing better variants of the concerned password scheme. After understanding the working of this scheme and the attacks upon it, two variants of CHC scheme have been designed and implemented. These variants have been named Centroid Oriented Convex Hull Click (CO-CHC) and Rogue CHC graphical password schemes. These

variants have been developed with the point of overcoming some flaws of this scheme.

4.1 Centroid-Oriented Convex Hull Click (CO-CHC) Scheme

As observed in the original CHC scheme, the password icons, of a user, are distributed randomly in different rounds and convex hulls, of varying sizes, are produced. Given the varying sizes of these convex hulls, some of them take up a large portion of the login screen. Also, there are chances that such large convex hulls could be generated consecutively in all authentication rounds. Thus, such large convex hulls subject the scheme to the Random-Click Attack. Although the random-click attack is a type of brute force attack and has less chances of success, but with large convex hulls, its chance of success increases considerably. Centroid-Oriented Convex Hull Click (CHC) scheme has been developed with the target of eliminating the random-click attack. First of all, it should be remembered that as the convex hulls, produced here, are irregular polygons, they have a centroid, not a center like regular polygons. The centroid is so called because irregular closed polygons have a center of mass, just like humans, but no exact center themselves. The reason for the usage of this term, in the name of this variant, will be explained later.

First of all, it has to be known how to calculate the exact centroid of an irregular closed polygon. Consider an irregular polygon on a cartesian plane or a convex hull shown in Figure 4.1. Note that the last vertex (x_N, y_N) is considered to be the same as the first vertex because the polygon is closed.

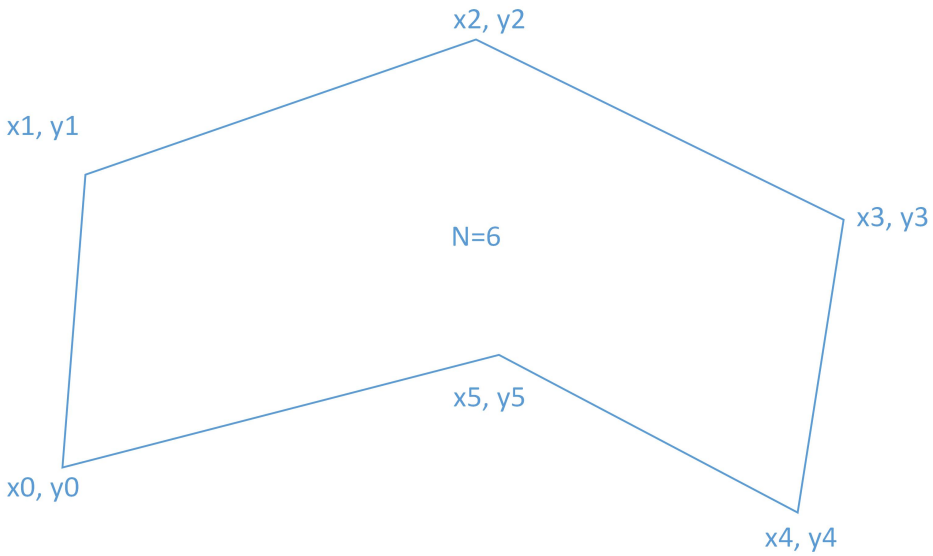


Figure 4.1: Irregular Polygon (Bourke, 2013)

To find the coordinates of the centroid of this polygon, first of all, the area is calculated by using Equation 4.1.

$$A = \frac{1}{2}\sum_{i=0}^{N-1}(x_i y_{i+1} - x_{i+1} y_i) \tag{4.1}$$

where A : Area of the polygon
N : Number of vertices of the polygon
x_i: x-coordinate of the i^{th} vertex of the polygon
y_i: y-coordinate of the i^{th} vertex of the polygon
x_{i+1}: x-coordinate of the $(i+1)^{th}$ vertex of the polygon
y_{i+1}: y-coordinate of the $(i+1)^{th}$ vertex of the polygon

Then, using the area of the polygon, the coordinates of the centroid are calculated by making use of Equations 4.2 and 4.3.

$$c_x = \frac{1}{6A}\sum_{i=0}^{N-1}(x_i + x_{i+1})(x_i y_{i+1} - x_{i+1} y_i) \tag{4.2}$$

$$c_y = \frac{1}{6A}\sum_{i=0}^{N-1}(y_i + y_{i+1})(x_i y_{i+1} - x_{i+1} y_i) \tag{4.3}$$

where c_x : X-coordinate of the centroid
c_y : Y-coordinate of the centroid
A : Area of the polygon
N : Number of vertices of the polygon
x_i: x-coordinate of the i^{th} vertex of the polygon
y_i: y-coordinate of the i^{th} vertex of the polygon
x_{i+1}: x-coordinate of the $(i+1)^{th}$ vertex of the polygon
y_{i+1}: y-coordinate of the $(i+1)^{th}$ vertex of the polygon

The main idea, behind CO-CHC scheme, is that if a person is asked to locate the centroid of an irregular closed polygon without using the mathematical technique, detailed previously, he or she can easily point out a probable centroid. Although it will not be accurate but it will be near the actual centroid. Keeping this in mind, CO-CHC scheme was developed where the main objective is that the user will make the invisible convex hull and not click anywhere inside it, but on the centroid of the convex hull. This variant has been designed to overcome the random-click attack on CHC scheme. As observed, most of the invisible convex hulls, in CHC scheme, take up a considerable portion of the login screen. An attacker might be able to get through multiple rounds of the scheme by clicking anywhere on the screen because of the big convex hulls. If a large area, for clicking, is provided for the ease of the user, it also becomes a vulnerability. Thus, CO-CHC scheme was designed to reduce the area, for clicking on the screen, while making sure that the user is able to locate that area easily. Figure 4.2 shows this scheme.

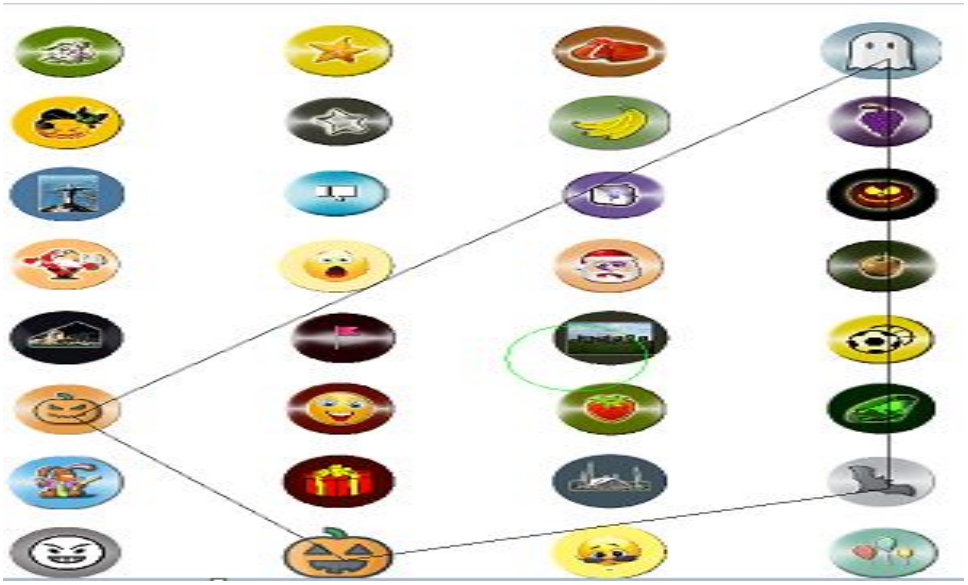


Figure 4.2: Centroid-Oriented (CO-CHC) Convex Hull Click Password Scheme

As displayed in the last figure, a convex hull is produced by the pass-icons and its centroid has been indicated. In the real-time implementation of this scheme, the lines and the centroid will not be drawn. The user will have to make the mental convex hull and click on the probable centroid. Now, it is known that due to the flawed human judgment, the exact centroid can never be found out except if a lucky guess works. Thus, a circle of a specific radius has been drawn, as shown in the figure, around the exact centroid to provide flexibility to the user. The exact centroid is calculated by the mathematical technique, detailed previously in this section. If the user clicks anywhere in the circle around the centroid, he or she will be able to get through one round of this scheme.
For setting the radius of this circle or the threshold, a test was conducted in which the users were asked to click on the probable centroid or the center of some convex hulls. Then, box-and-whisker plots, of the data, were made and the average value of the filtered values was calculated. This average value was set as the radius or the threshold within which the user could click.

4.2 Rogue Convex Hull Click Scheme

As indicated by the name, Rogue Convex Hull Click scheme is so named because it goes against the format of CHC scheme. The scheme will work like the original CHC scheme but, this time, after forming the convex hull, the user has to click outside it to get authenticated. Now, there are multiple points outside the convex hull where the click can be done so a format has been designed to assist the user. The main idea, behind the design, is to randomize the click point. This scheme has been designed to counteract the attack, which utilized a geometrical technique, as explained in Chapter 2. This attack involves statistical analysis. In this attack, the adversary used to study the location of the click point and find the possible password icons by doing calculations, on their probability of occurrence. Basically, the possible password icons were found through reverse engineering. Although this attack seems quite difficult to carry out, its probability of success is significant. This type of attack is successful because the click-point is always inside the convex hull. If the click-point is somewhere outside but near the convex hull, the attacker can get confused about the real location of the convex hull and the pass-icons. The main challenge, here, is that if the security is being increased, there will be a great fall in the usability but an effort has been made to hit a balance.
To make it easy for the users, four possible click points will be designated outside the convex hull. Figure 4.3 displays Rogue CHC scheme.

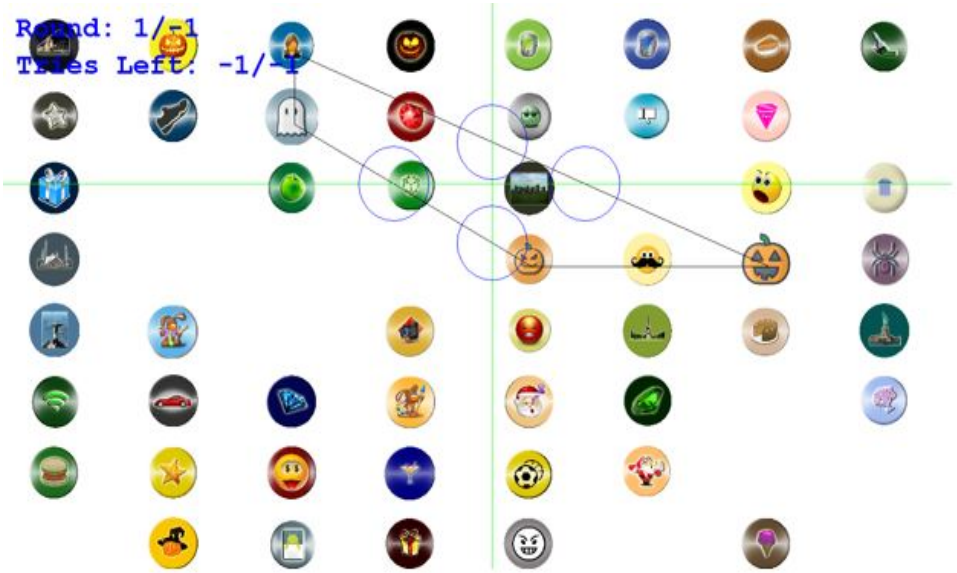


Figure 4.3: Rogue Convex Hull Click Password Scheme

As shown in Figure 4.3, the user will identify the pass-icons and make the convex hull first. Then, the user will locate the probable centroid and form imaginary horizontal and vertical axes on that point. After that, the user will locate the points at which the axes intersect the convex hull on the top, bottom, left and right sides. Finally, the user will have to click close to one of these points but outside and close to the boundary of the convex hull to get authenticated through one round. As seen here, the centroid will be used as a point of reference by the user so he or she is not unclear about where to click outside the convex hull.
To calculate the suitable distance from the convex hull for clicking, a test was carried out. The volunteers were asked to make a mental convex hull from a fixed number of pass-icons and locate the centroid. Then, they were asked to make the imaginary horizontal and vertical axes on that centroid and click on the top, bottom, left and right side of the convex hull but outside it. The distance between the point of the intersection and the click-point, given by the user, was calculated. The box-and-whisker plots were made and the average values of the threshold, concerning all four click-points, were calculated and incorporated. That average value will be the radius of the circles, shown outside the convex hull in Figure 4.3. If the user clicks within these circles, he or she will get through one round of authentication. The details of the testing procedure, including the development of the box-and-whisker plots for setting the threshold value of the radius, for CO-CHC scheme, and the

threshold value of clicking distance, for Rogue CHC scheme, and a usability study, for both schemes, have been given in Chapter 5.
It can be seen that in both schemes, there are lines, which make the boundaries of the convex hull, and circles for marking the areas to be clicked. These lines and circles have only been drawn to explain these schemes easily and will not be present in the actual implementation of these schemes. To support these variants, the number of pass-icons has been set at four to increase the memorability. Also, the size of the icons has been kept large for better visibility.

Chapter 5

Testing

As it is known that any password scheme has to be used by common people, who might or might not be tech-savvy, it is important to know about the usability of any developed password scheme. For our developed graphical passwords, two methods of testing were proposed initially. Out of these two methods, one was chosen. One method was that the strength of the graphical passwords should be tested by simulating the known attacks on it. An extensive mathematical analysis can be done to show that the new algorithms are resilient against the known attacks. The other method was carrying out an extensive usability study on these passwords. The evaluation of these passwords could be done on some metrics which are generally related to passwords. After studying both of these testing methods, it was decided that a proper usability study will be carried out on the passwords. It is believed that a good user evaluation of these graphical passwords can provide a deeper insight on how to make the password scheme more practical for use of a common man. As mentioned earlier, a common man has to use passwords on a daily basis so the emphasis on usability of the password is very important while keeping the security adequate. As all security researchers try, the maximum effort to strike a balance between the security and the usability of these passwords has been made. This usability study was based upon the one done by (Wiedenbeck et al., 2006) on the original CHC scheme and another one done by (De Angeli et al., 2002) on VIP graphical password scheme.

5.1 Participants

The calculation of the sample size for any usability study is important because it has to be known how many users will be enough to get a proper

evaluation. The formula used for calculating the sample size (n) is given below.

$$n = \left\{(z_{\alpha/2} \times \sigma)/E\right\}^2 \tag{5.1}$$

where $z_{\alpha/2}$: Critical value (The positive value of 'z' at the vertical boundary of the area of $\alpha/2$ in the right tail of the standard normal distribution)
σ : Population Standard Deviation
E : Margin of Error

The value of population standard deviation was obtained from the usability study in (Wiedenbeck et al., 2006) as our graphical passwords are based upon CHC scheme. The critical value, at a degree of confidence of 95%, was used, that is, 1.96. Thus, keeping the margin of error at 3, which was acceptable, the sample size was calculated as shown below.

$$n = \left\{(1.96 \times 8.58)/3\right\}^2 = 31.4 \approx 30 \tag{5.2}$$

A sample size of 30 participants seemed to be significant to demonstrate the usability of the password scheme. So for this usability study, a group of university students was picked. The mean age was 21 years (Std Dev = 1.45). All of them were experienced computer users who used various gadgets like cellphones, tablets and PCs on a daily basis. After a survey of the estimated usage, in hours, of computers for work and personal activities on a daily basis, it was revealed that mean usage of the computers was 9 hours (Std Dev = 3.64).

5.2 Materials

At a research lab in the university, some PCs were set up to run the graphical password software, which was built in Java. The system, used for testing, showed up to 60 icons in a window of 1366×768 pixels. The number of icons, displayed in a challenge, varied from 50 to 60 icons. The number of pass-icons, designated for these password schemes, was four. This is lesser than the number of pass-icons, used for CHC scheme, because the dynamics of our developed scheme are different. The user is required to click on or near the centroid of the convex hull (CO-CHC scheme) or outside the convex hull (Rogue CHC scheme) so making a convex hull out of four pass-icons turned out to be much easier. Also, the cognitive load of these two schemes is more

as compared to CHC scheme so an effort was made to increase the easiness of making a convex hull. During a single login phase of either CO-CHC scheme or Rogue CHC scheme, there were five rounds of challenges in which all four pass-icons were displayed. A user has to get through all five challenges with three chances of error, as used in Equation 5.2. A challenge screen is displayed in Figure 5.1. Also, videos of the participants were made during the test to observe the reactions of the users towards the password schemes. This would, in turn, help in knowing about the level of user satisfaction.

Figure 5.1: Challenge Screen for CO-CHC and Rogue CHC Schemes

Before starting with the proper login phase, the users worked on the tutorials of these schemes, which were similar to the real challenges. The only difference was that the tutorials had no limit on challenges and the users could easily practice as much as they needed to. As shown in the tutorial login screen in Figure 5.2, the number of challenges is negative, which shows that a new challenge will be produced with every left-click. The program was exited only by using right-click.

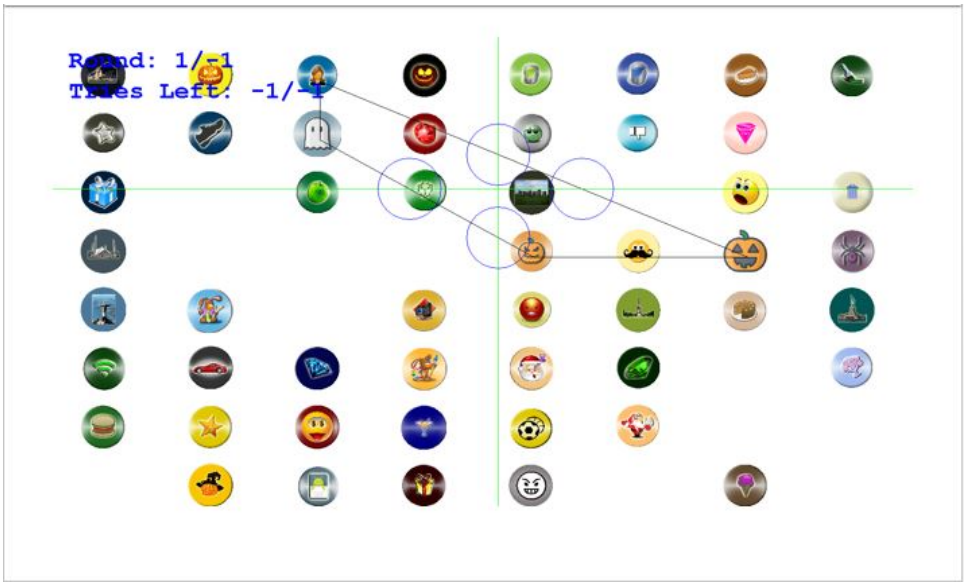


Figure 5.2: Tutorial Screen for CO-CHC and Rogue CHC Scheme

5.3 Procedure

For this usability study, the method of longitudinal testing was used. This test was based upon 3 phases. As the memorability issue of passwords is always a major concern, the experiments had to be spread over a period of time. Before starting with these tests, the participants were taught how to create convex hulls from 4 points or pass-icons.

5.3.1 First Phase or Test 1

The first phase was used for setting thresholds of clicking for Centroid-Oriented CHC scheme and Rogue CHC scheme. It was divided into stage 1 and stage 2. In stage 1, the clicking threshold of CO-CHC scheme was set while stage 2 determined the threshold for clicking in Rogue CHC scheme. In case of CO-CHC, a value of radius of the centroid had to be set as no human can click on the exact centroid of a convex hull. This value of radius could have been estimated and set by the researcher but as real human users have to use this scheme, the best approach was to have the radius set by the users themselves. The window used for setting the clicking threshold of CO-CHC scheme is displayed in Figure 5.3.

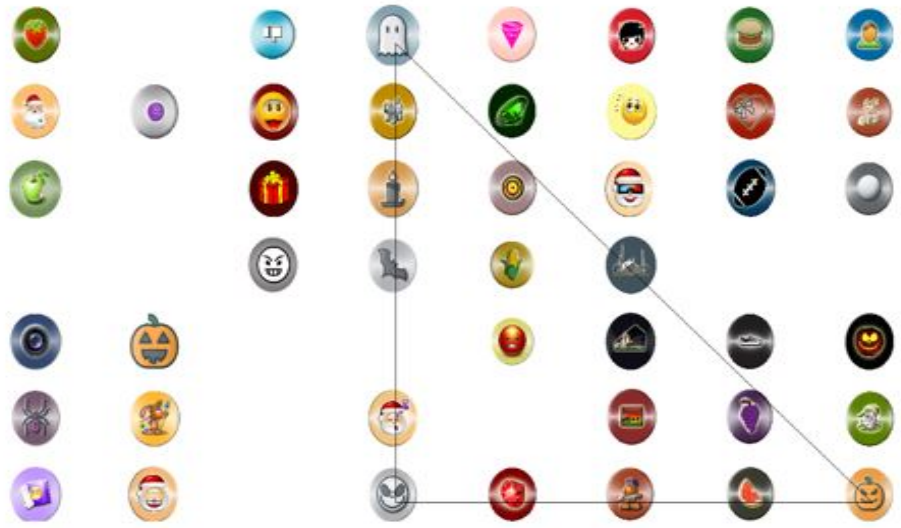


Figure 5.3: GUI for obtaining the input for clicking threshold in CO-CHC Scheme

In stage 1, there were 5 rounds and in each round, the user was shown a convex hull. He or she had to click on the probable centroid of the convex hull. After getting the values of the probable centroid from all the users, the individual distances between the user's centroid and the real centroid were calculated. Then, the box-and-whisker plot, for each round, was drawn to eliminate the outliers. For each round, the average of the individual values of distance was calculated. Following that, the mean value of these average values was calculated and set as the radius. The user had to click anywhere in that area around the centroid, bound by the radius, to get authenticated. The obtained value of the radius was 43.477 pixels. This value might seem very small for clicking correctly but such a value ensures less chances of a random click attack. Also, during the usability study, it was observed that when the users practiced enough, they were comfortable with this value of the radius. The box-and-whisker or box plots of all 5 rounds are shown in Figure 5.4.

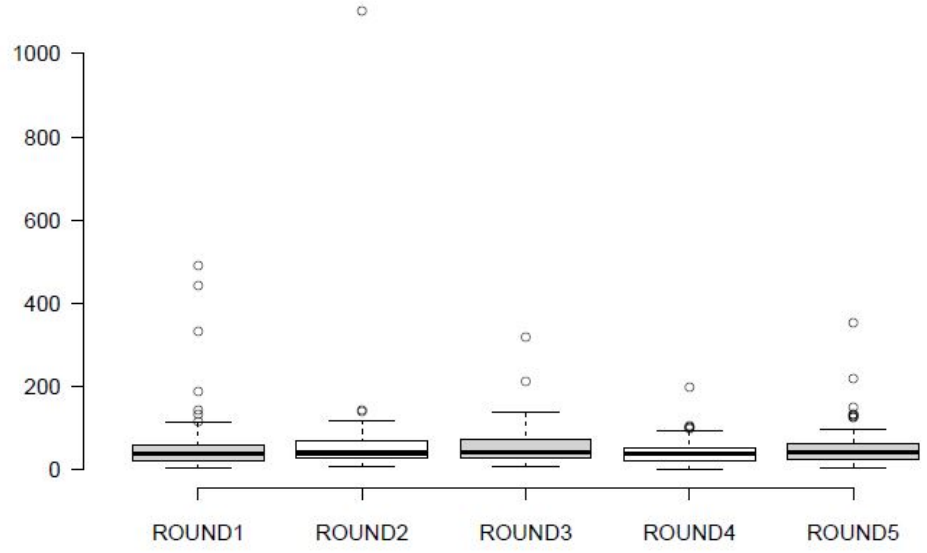


Figure 5.4: Box-and-whisker plots for setting the clicking threshold in CO-CHC scheme

In stage 2, a similar process was carried out to calculate the clicking thresholds on the left, right, top and bottom of the convex hull for Rogue CHC scheme. For Rogue CHC scheme, the graphical user interface is shown in Figure 5.5.

Figure 5.5: GUI for obtaining the input for clicking threshold in Rogue CHC Scheme

In stage 2, the pass-icons were highlighted in blue as shown in Figure 5.5. In 5 rounds of challenges, the user was instructed to locate the pass-icons and draw a mental convex hull. Then, the user had to locate the probable centroid of the invisible convex hull and click outside the convex hull. The clicks had to be on the top, bottom, left and right of the centroid but outside the hull and close to its boundary. The clicks had to be done in the order of top, bottom, left and right. After this stage, the distance between a click-point, like the top one, and the point at which a straight line, from the centroid, intersects the boundary of the convex hull on that side, was calculated. Then, the concerned box-and-whisker plots were constructed and the outliers were eliminated. It should be noted that for one clicking position, like top, 1 box plot was drawn per round. Hence, every clicking position had 5 box plots. After eliminating the outliers from each box plot, the average value of the values in that box plot was calculated. In this way, 5 values, of average, for the clicking positions, in 5 rounds were calculated. Then, the mean value of these 5 values was found out and used as the threshold. Thus, the 4 approximate values of distance for the top, bottom, left and right regions, from the boundary of the convex hull were calculated to be used in the experiments ahead. The values of the distance are shown below.

1. Distance for the Clicking Region on the Top of the Convex Hull =

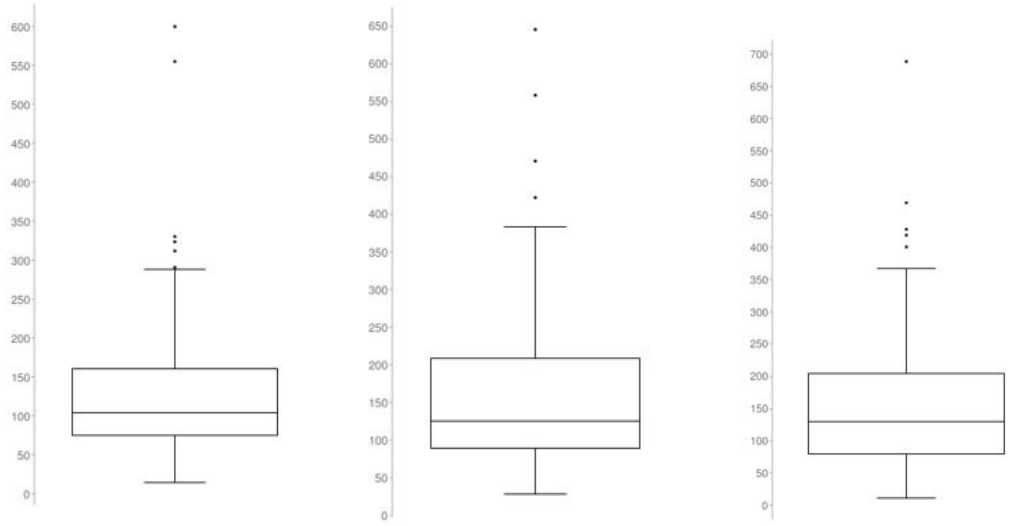
130.55 pixels

2. Distance for the Clicking Region at the Bottom of the Convex Hull = 116.31 pixels

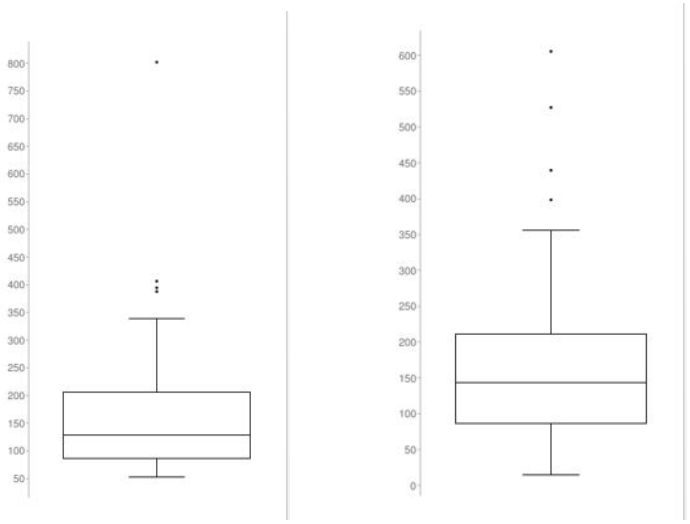
3. Distance for the Clicking Region on the Left of the Convex Hull = 204.48 pixels

4. Distance for the Clicking Region on the Right of the Convex Hull = 136.10 pixels

As seen, the calculated values of distance are quite large which give a large clicking space, thus making it easier for the user to click correctly. The box plots, of all rounds, for all the clicking regions, are shown in Figures 5.6, 5.7, 5.8 and 5.9. There is a need to emphasize here that all these calculated values for distance in both password schemes may vary due to changes in the test environment like changing the age group of users who will use the schemes and perform the tests. Please note that Appendix A contains the links to two separate Microsoft Excel files, stored online, which have the collected data and the calculations done for drawing the box plots for CO-CHC Scheme and Rogue CHC Scheme.

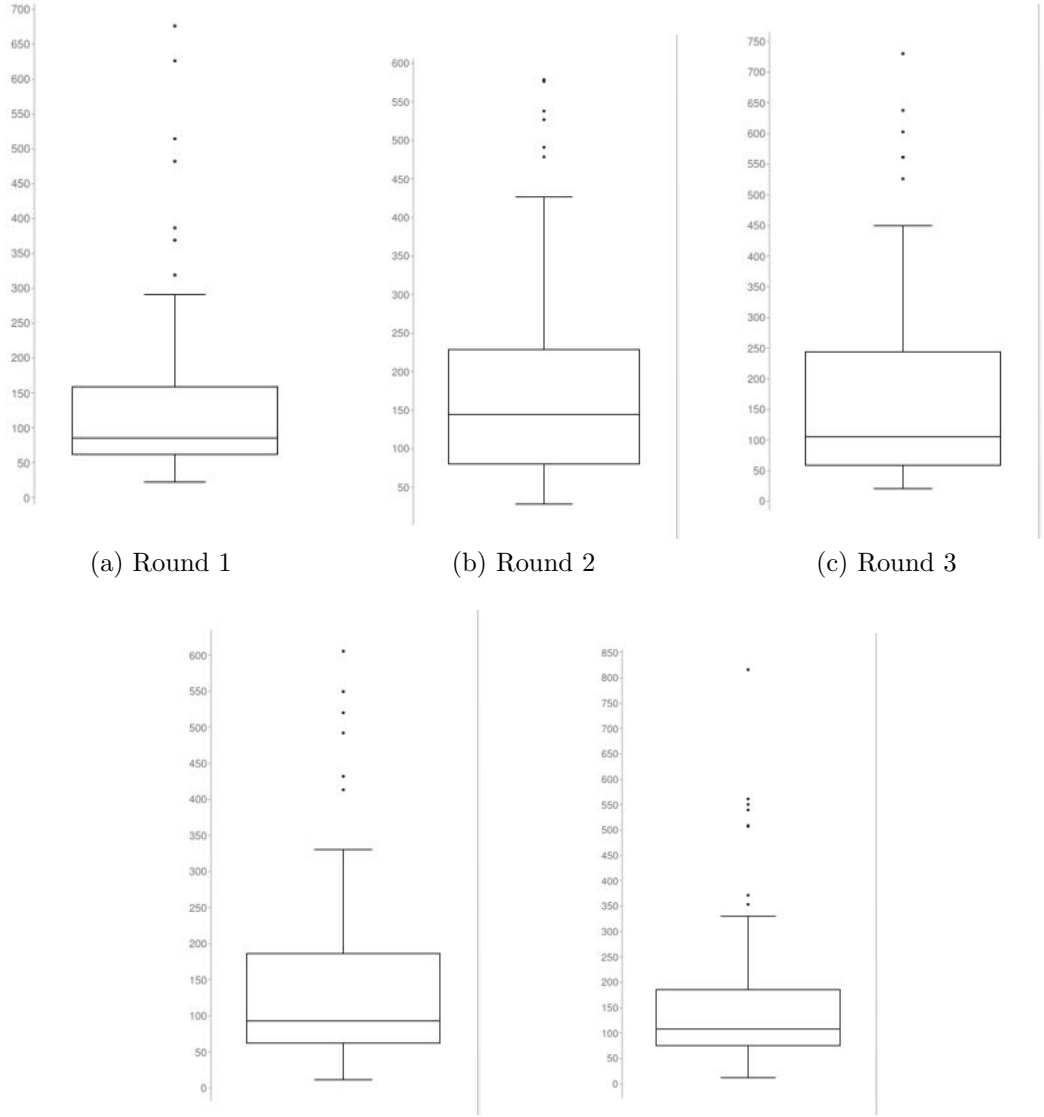


(a) Round 1 (b) Round 2 (c) Round 3



(d) Round 4 (e) Round 5

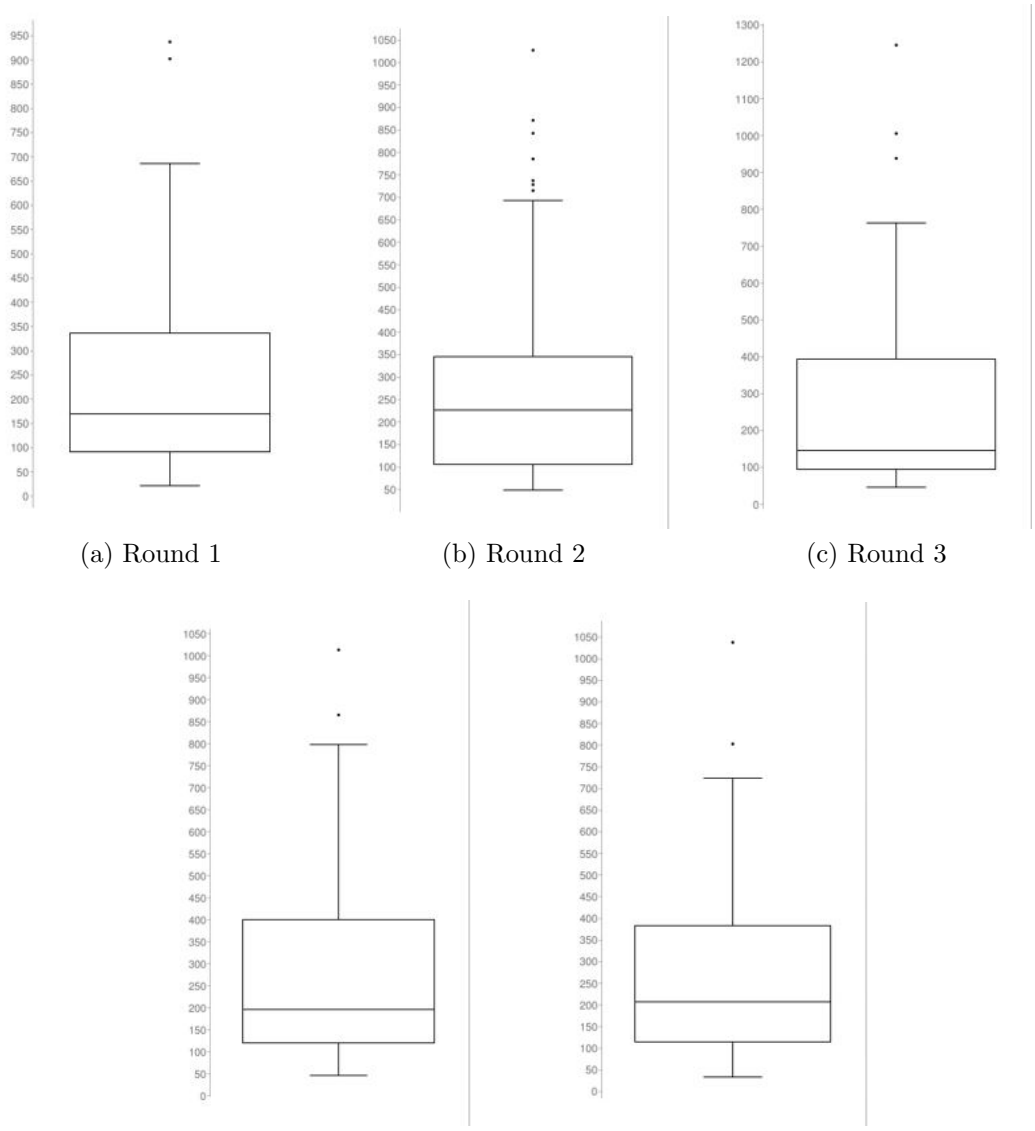
Figure 5.6: Box-and-whisker Plots for the Clicking Region on the Top of the Convex Hull



(a) Round 1 (b) Round 2 (c) Round 3

(d) Round 4 (e) Round 5

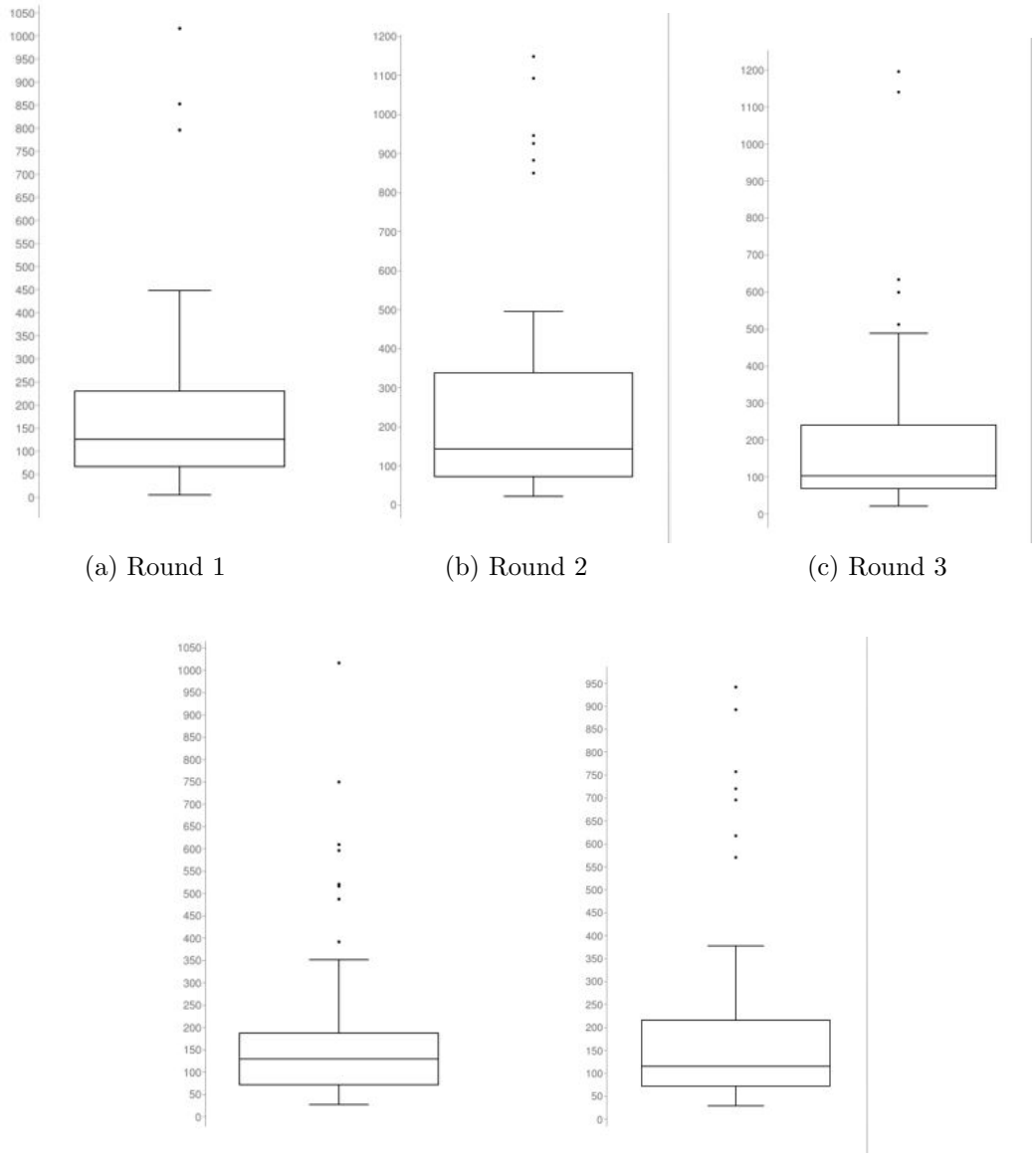
Figure 5.7: Box-and-whisker Plots for the Clicking Region at the Bottom of the Convex Hull



(a) Round 1 (b) Round 2 (c) Round 3

(d) Round 4 (e) Round 5

Figure 5.8: Box-and-whisker Plots for the Clicking Region on the Left of the Convex Hull



(a) Round 1 (b) Round 2 (c) Round 3

(d) Round 4 (e) Round 5

Figure 5.9: Box-and-whisker Plots for the Clicking Region on the Right of the Convex Hull

5.3.2 Second Phase or Test 2

After incorporating these results, the participants were called for the 2nd phase of the testing in which they had to use the password schemes. A participant had to choose his or her 4 password icons out of more than 100

icons. Then, they had to get 5 successful logins of CHC, CO-CHC and Rogue CHC scheme. A participant had to keep authenticating himself or herself until 5 successful logins were achieved for all the schemes. As mentioned earlier, each login consists of 5 rounds of challenges with 3 chances of error. Through this test, the following data was collected.

1. Number of successful and unsuccessful logins
2. Number of successful and unsuccessful challenges
3. The time taken for the successful and unsuccessful logins and challenges

5.3.3 Third Phase or Test 3

The analysis, based on this data, was used to determine the usability of the schemes. A week later, the participants were called for the third test or the memorability test. They had to identify their pass-icons out of a grid of more than 100 icons. The time taken by each participant to identify their icons and how many of the chosen icons were correct, was collected. The GUI used for test 3 is shown in Figure 5.10.

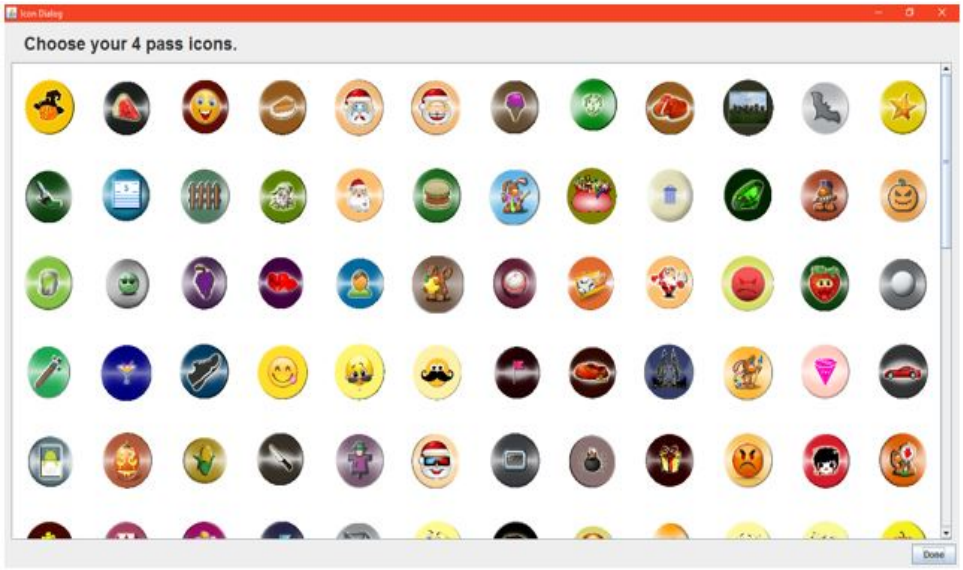


Figure 5.10: GUI for the Memorability Test

Chapter 6

Analysis

Considering all the participants, they were able to get their successful logins of both schemes. Some took more time than others. Some even had to appear more than two times to complete their successful logins. Many factors like mood, degree of concentration and failure in following the instructions properly, had to be considered too. Thus, it can be said that there was a diversity of parameters to be considered for the analysis. In this case, after taking much into consideration, the factors considered were how fast a user got himself or herself authenticated and in doing so, how many times was he or she unsuccessful. This will also indicate the learning curve of the password schemes. Also, the degree of satisfaction of the users, with the password scheme, had to be measured as well. Keeping these factors in mind, the analysis was done along the lines of efficiency, effectiveness and user satisfaction.

Here, effectiveness is associated with the number of right and wrong tries and how clear was the user, about the usage of the schemes. Efficiency is related to the measurement of the speed of data entry. User satisfaction tells about how users felt while learning and using the password schemes. While "Effectiveness" and "Efficiency" were quantitative measures, "User Satisfaction" was more of a qualitative measure. The feedback of every participant was taken for determining the level of comfort and for further improvement of the schemes. The sections, given ahead, tell about how these metrics were measured along with what can be derived from these measurements. In all the considered parameters, the measurements with CHC scheme were considered as a reference for the two newly developed password schemes.

6.1 Effectiveness

This metric measures the degree to which a user was successful and how much difficult he or she faced in achieving his or her 5 logins. It was measured in the form of mean percentage correctness of logins and challenges and the mean percentage error of logins. The mean percentage correctness of logins indicates the average number of correct logins achieved by a participant while getting to the required number of correct logins. The mean percentage correctness of challenges tells about the average number of correct challenges of a user in the correct logins. In contrast, the mean percentage error of logins tells about the number of incorrect logins of a user while achieving the 5 correct logins. Figures 6.1 and 6.2 show the bar graphs of these stats.

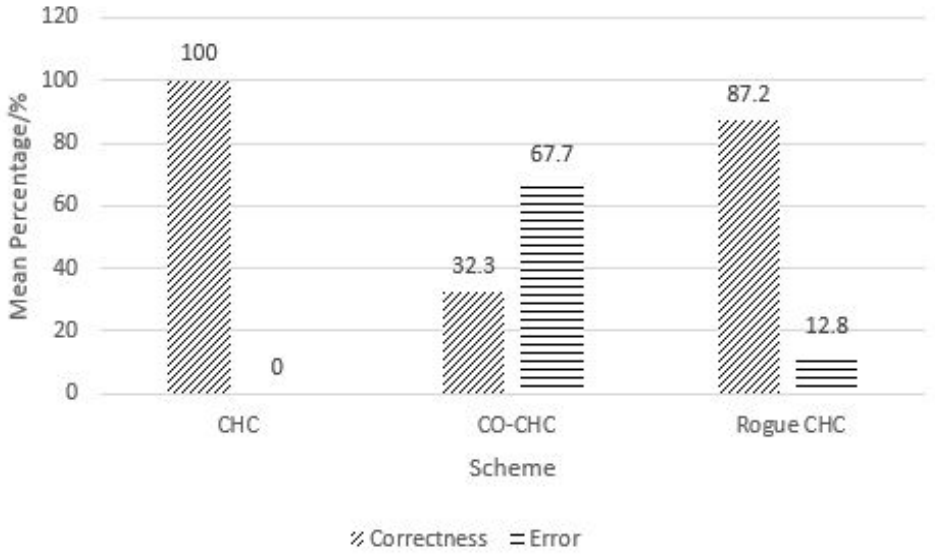


Figure 6.1: Mean Percentage Correctness & Error of the Logins

The values of mean percentage (correctness) of logins, for all three schemes, are given below.

1. CHC = 100% (Std Dev = 0)
2. CO-CHC = 32.3% (Std Dev = 19.7)
3. Rogue CHC = 87.2% (Std Dev = 15.5)

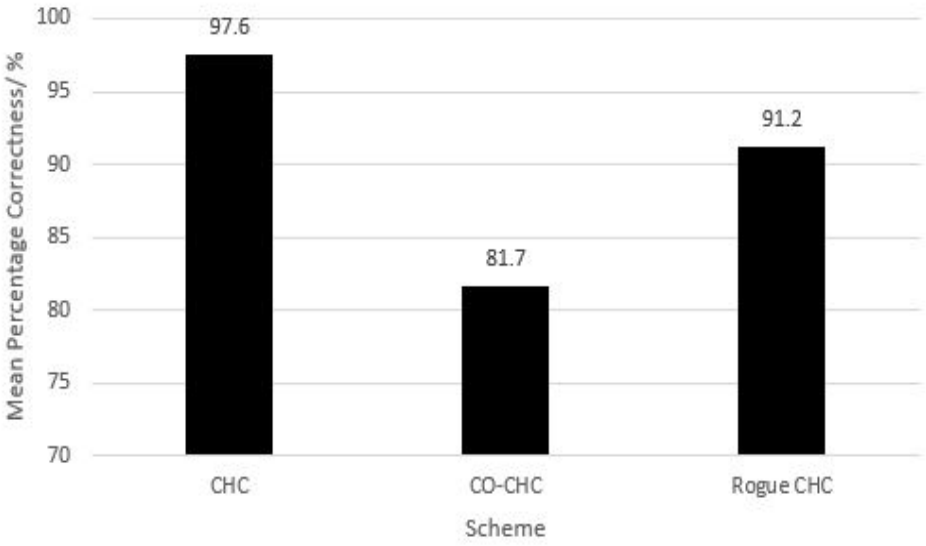


Figure 6.2: Mean Percentage Correctness of the Challenges

The values of mean percentage (correctness) for challenges for all three schemes are given below.

1. CHC = 97.6% (Std Dev = 3.23)
2. CO-CHC = 81.7% (Std Dev = 5.16)
3. Rogue CHC = 91.2% (Std Dev = 6.32)

All the participants, of this study, were able to achieve their 5 logins. Some took more time and turns than others. For example, in the case of CO-CHC, it took one participant, more than 70 logins, to get 5 correct logins. According to Figures 6.1 and 6.2, it can be said that the participants had a lot of ease in using CHC scheme because it did not require much mental effort. Actually, they found it quite fun to use. As it just required them to trace out a convex hull and click anywhere inside, it was very easy for them. In the same figure, in comparison with CHC scheme, the mean percentage correctness of the logins in CO-CHC is quite low while its mean percentage error is considerably high. It can be deduced that the participants faced a lot of difficulty in learning this scheme and thus, did not achieve the 5 correct logins easily. It was observed that when the participants were required to click in a specific area, that is, the centroid, it took them a lot of time to compute that area and click in it. Hence, on average, it took the

participants a large number of logins to get their required correct logins and it did become frustrating for most of them. This high mean percentage of error can also be attributed to the fact that the clicking threshold, for the centroid, calculated in Test 1, was quite small. It was around 44 pixels so it is quite difficult for a human eye to achieve that precision and coordinate to click in the correct area. Also, it was observed that the participants, who understood the concept of the center of mass or centroid better, were able to login correctly much easily, as compared to others. As compared to the mean percentage correctness (logins), the mean percentage correctness (challenges) of CO-CHC scheme does show some potential of being practical as it's quite near to the values of CHC and Rogue CHC scheme.
In contrast, a very high value of mean percentage correctness was achieved in the case of Rogue CHC scheme. This shows that the users had a lot of ease in achieving their 5 correct logins and learned the scheme fast. This can also be due to the fact that the clicking thresholds, calculated for Rogue CHC, were quite large and the participants had been given 4 options as to where they could click. Although the random click attack could be effective here but the variations in the shape of the convex hulls and the positions of the clicking areas do contribute in making the scheme secure. The low value of mean percentage error shows that this scheme can be considered practical for common usage. Also, its mean percentage correctness (challenges) is quite near to that of CHC scheme, thus, bringing its usability to the same level.

6.2 Efficiency

This parameter was evaluated by measuring the time taken for the correct logins and challenges. By observing the values of time, the degree of comfort of the users with the password scheme can also be known. Figure 6.3 and Figure 6.4 show the mean time taken to log in and the mean time taken to get through a challenge.

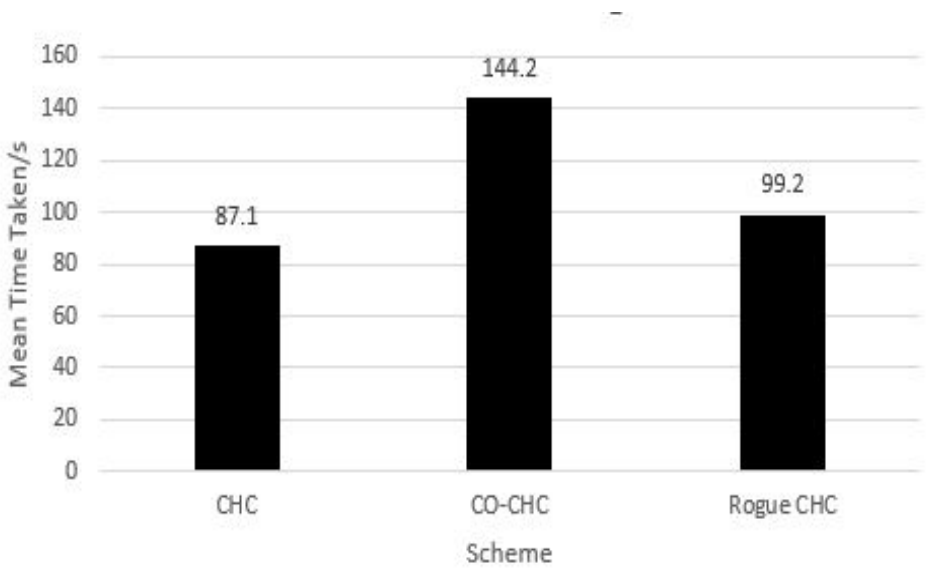


Figure 6.3: Mean Time Taken to Log In

The values of mean time taken to log in for all three schemes are listed below.

1. CHC = 87.1s (Std Dev = 34.1)(Range = 41.03s-196.95s)
2. CO-CHC = 144.2s (Std Dev = 50)(Range = 69.07s-278.08s)
3. Rogue CHC = 99.2s (Std Dev = 45.1)(Range = 47.4s-288.4s)

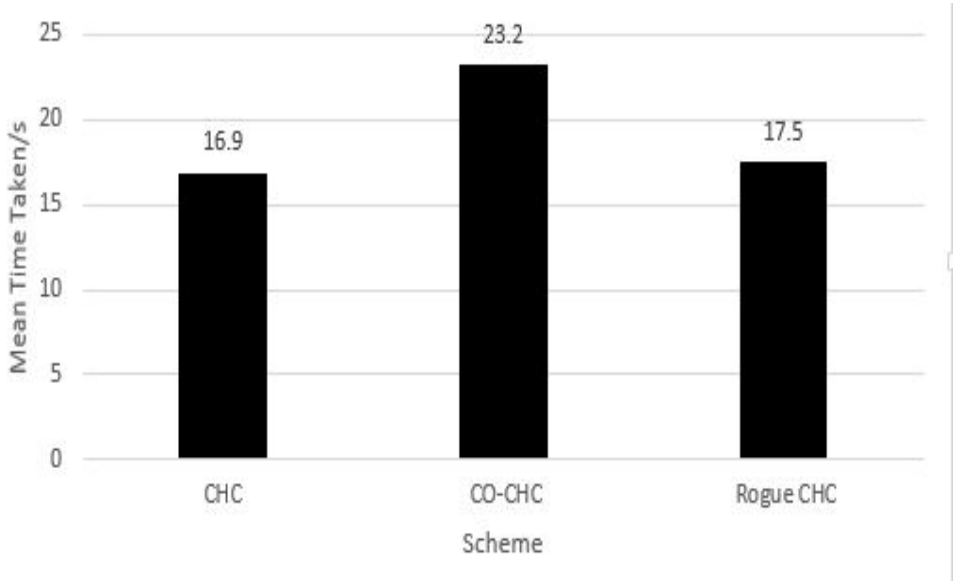


Figure 6.4: Mean Time Taken to get a Challenge Correct

The values of mean time taken, across challenges, for all three schemes are given below.

1. CHC = 16.9s (Std Dev = 6.57)(Range = 8.21s-38.9s)
2. CO-CHC = 23.2s (Std Dev = 8.22)(Range = 10.08s-41.9s)
3. Rogue CHC = 17.5s (Std Dev = 8.01)(Range = 8.53s-52.1s)

As observed in the graph for the mean time taken to log in, the participants had a tough time in getting a correct login of CO-CHC scheme, which took more than 2 minutes on average. This amount of time taken can also be attributed to the fact that the participants had to work a lot to compute the centroid and click in the correct location. Also, as compared to Rogue CHC scheme, it took a lot of mental effort and time to get 5 correct logins of CO-CHC scheme. On average, every participant, even the focused one, took at least one hour. On the other hand, the mean time taken to log in for Rogue CHC scheme is quite near to that of CHC scheme which shows that the participants found it quite easier to log in using Rogue CHC scheme.The same trend is shown by the bar graph of the mean time taken for a challenge. As mentioned earlier, the less time taken in a login and in a challenge of Rogue CHC can be attributed to the large clicking thresholds and the multiple number of locations for clicking. Now, to see how well a

participant learned a scheme and gained confidence while using it, the trend of mean time taken across 5 correct logins, of each scheme, was obtained. Figures 6.5, 6.6 and 6.7 show these trends in the form of bar graphs.

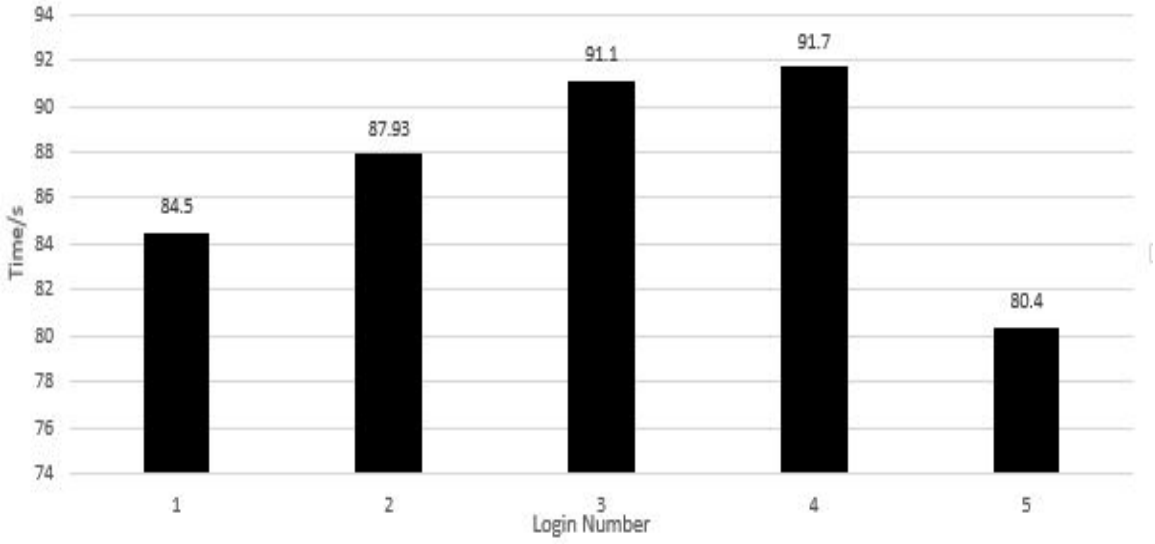


Figure 6.5: Mean Time Taken across five Correct Logins (CHC Scheme)

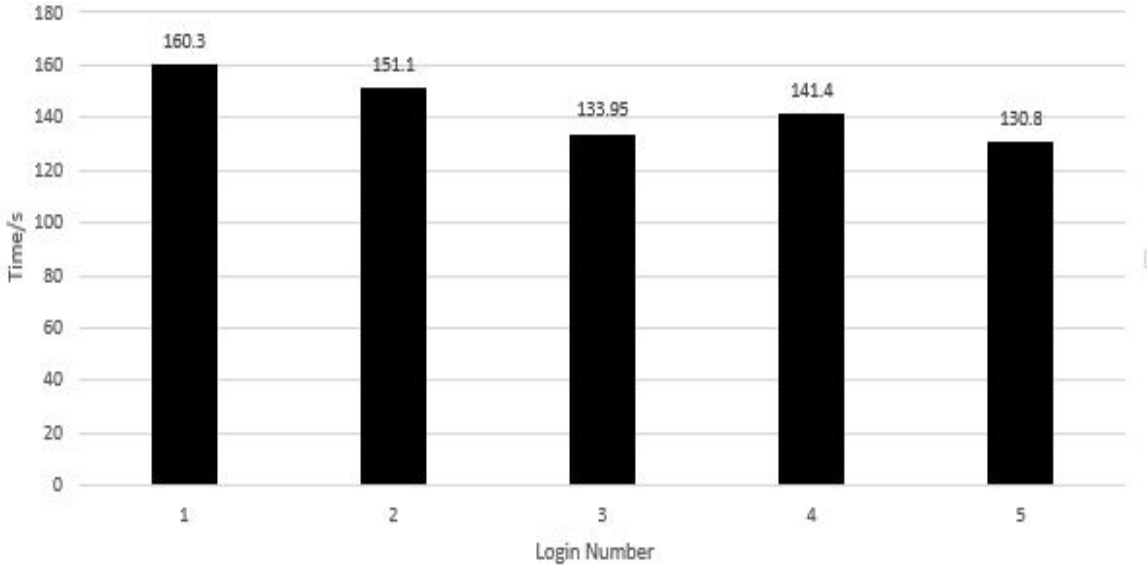


Figure 6.6: Mean Time Taken across five Correct Logins (CO-CHC Scheme)

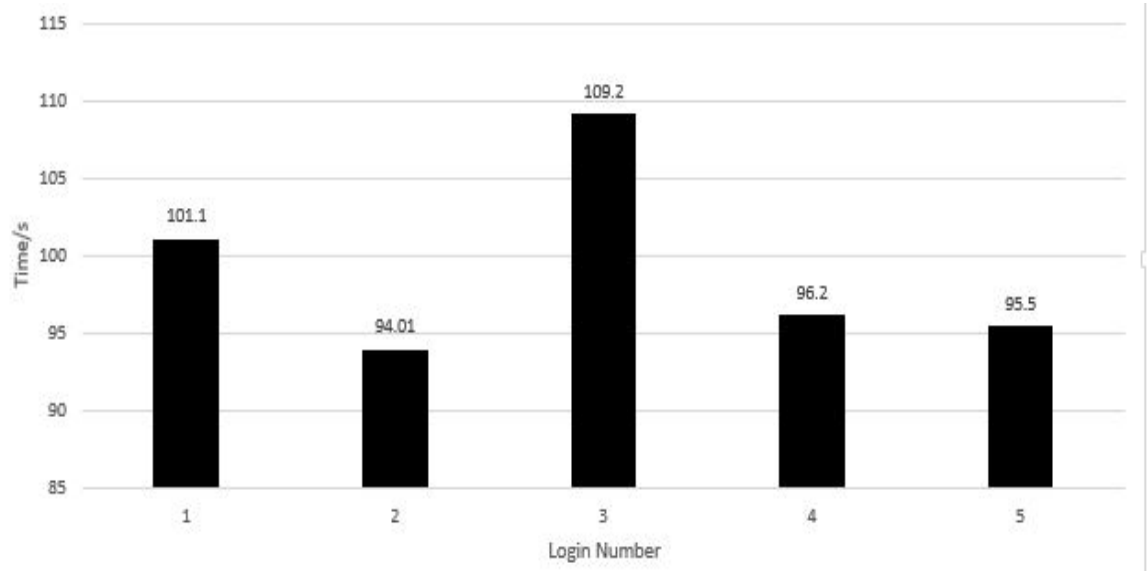


Figure 6.7: Mean Time Taken across five Correct Logins (Rogue CHC Scheme)

For CHC scheme, it can be seen that the mean time taken, to log in, increases till the fourth login. The reason can be that the participants might

have had to spend more time in finding their secret icons. The developed algorithm made sure that all of the login screen was used for the placement of the icons, in every round, so the same icon would not land in the same location more than once. Hence, more time might have been consumed in locating all the secret icons in every round. Still, it is observed that the mean time taken, for the fifth round, is quite less so it can be said that the participants got used to the scheme quickly. Considering CO-CHC scheme, despite of the difficulty in using it, there is a gentle downward trend in the mean time taken in a single login. Therefore, it can be deduced that the participants got more confident with every correct login and the practicality of the scheme can be observed. In the graph for Rogue CHC scheme, the mean time taken, for a single login, decreases till the 5th login in an irregular manner. The rise in the mean time taken, during the 3rd login, can be a result of over-confidence or more time spent in locating the secret icons. Still, the fall afterwards, indicates that the participants did find it quite easy to use, eventually. As observed, Rogue CHC scheme is the one which has figures, lying quite close, to the figures of CHC scheme. Its learning curve is supposedly less as compared to CO-CHC scheme. Please note that the link to the Microsoft Excel file (stored online), related to Test 2, which contains the collected data, the graphs in sections 6.1 and 6.2 and the calculations, is given in Appendix A.

Another test, to observe the efficiency of the schemes, was the Memorability Test or Test 3, which was carried a week after Test 2 had been performed by a participant. Unlike alphanumeric passwords, graphical password schemes require users to memorize graphical objects or pictures. Considering this differentiating aspect, it had to be observed whether the users remembered their secret icons after a week of not using the password scheme at all. This test will also show whether the participants are more comfortable with memorizing letters (and other alphanumeric characters) or pictures. The results of Test 3 are shown in Figure 6.8.

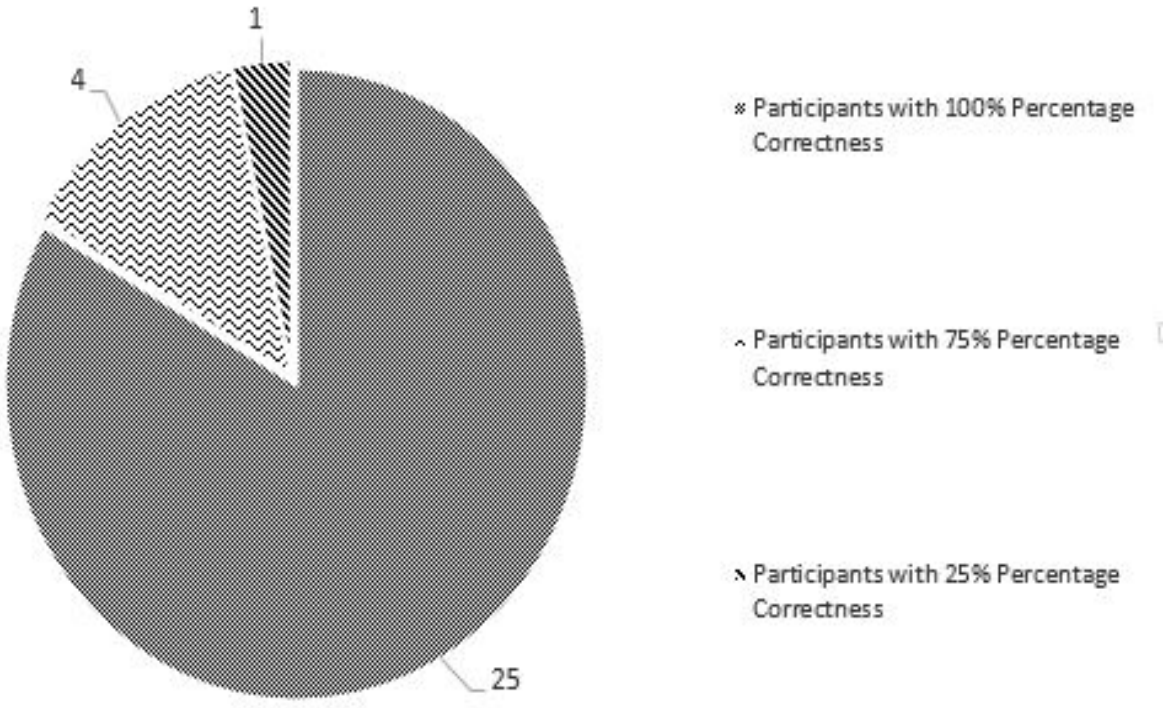


Figure 6.8: Result of the Memorability Test

As seen here, the results show that more than half of the users remembered their secret icons. This can be related to the fact that every participant spent a lot of time on the tutorials. Also, there was a significant number of incorrect logins for CO-CHC scheme and the repetition lead to better memorizing of the secret icons. This test proves that the psychological fact about the human mind being able to recognize properly than recall, is indeed correct. Therefore, users have less issues of usability with graphical password schemes. Appendix A contains the link to the file (stored online), in Microsoft Excel, which has the results of Test 3 along with the calculations done.

6.3 User Satisfaction

This parameter indicates the level of comfort and the ease felt by the participants, while using the schemes. The feedback of the users is always important for improving an authentication method, in terms of usability. After

Test 3, every participant was asked about the experience, with the password schemes, and how the schemes could be improved further and where they could be used. Video recording did help a lot in determining the user experience. It was observed that the participants had a tough time while learning and using CO-CHC scheme. They seemed to get frustrated at getting consecutive incorrect logins. The frustration did play a role in increased amount of time in getting correct logins. Some participants preferred having a second go at CO-CHC scheme at some other time due to their commitments or just so, they could be mentally fresh while trying again. They were instructed to appear the very next day so no considerable irregularity would come in the test results. Nonetheless, once any participant got the third login correct, for CO-CHC scheme, he or she felt more confident and had less difficulty in achieving the rest of the correct logins.
Considering Rogue CHC scheme, the participants took less time and were more confident as they did their logins quickly. The main factor was that they had a lot of practice with locating the centroid, in CO-CHC scheme, so it was easy for them to learn Rogue CHC scheme. A significant mental effort was required here as well but the large clicking thresholds lead to more ease for the participants. Considering the application, the opinion was that the password schemes were indeed secure but they should be used in areas where infrequent logins are required. The participants found the schemes to be game-like and with every successful login, they tried doing the next one in less time or tried beating their previous time. Any participant, with better focus or recognition of shapes or the concept of the centroid, achieved the correct logins in less time. For example, a participant, who was a regular player of First Person Shooter (FPS) games, completed his logins in less time. The reason can be that such games require the user to be precise while clicking so that practice helped in better estimation of the centroid and thus, less login time. Overall, the participants preferred Rogue CHC scheme for use in real-life applications.

6.4 Analysis in a Nutshell

After extensive usability testing and viewing its results, it can be easily observed that the participants were more comfortable with using Rogue CHC scheme. It was seen that the learning curve, of Rogue CHC scheme, was less as compared to the one with CO-CHC password scheme but it should be remembered that as independent password schemes, their learning curves are considerable. It will take a significant amount of time and effort to get used to any of them. Considering their application, till now, it can be concluded

that they will be of good use in high-security areas only where less frequent logins are required like a vault containing secret classified documents which are used less. Although these test results help in knowing the potential of these variants a lot but testing other parameters like different age groups will be very useful. This is because every parameter will define different qualities of the variants and contribute to their improvement. A good usability study, being the focus of this research, did help in finding out the potential of practical usage of these password schemes but it does not tell about the resilience of these schemes. To measure the security and the resistance of these schemes to attacks, attack simulations will prove to be very helpful and assist in reaching a proper conclusion, concerning the trade-off between security and usability.

Chapter 7

Conclusion and Future Work

7.1 Conclusion

Since years, in the world of technology, passwords have been considered as the most common and most attacked mode of authentication. A lot of research has gone into alphanumeric passwords. Although the security of alphanumeric passwords has increased but their overall complexity has also surged. As a password is something which is used quite a lot by laymen, so it has to be psychologically acceptable. Another critical problem, found with textual passwords, is shoulder-surfing.
Considering that, graphical password schemes were developed and a whole new area of research, in password schemes, opened up. They were found to be more psychologically acceptable, as compared to textual passwords, but they also suffered from shoulder-surfing. This problem still existed because now, the user was interacting with objects on the screen by clicking or touching, which is more visible to an adversary. The problem of shoulder-surfing, in the case of textual passwords, could still be controlled by instructing the users to hide the keyboard while typing the password. Considering graphical passwords, the option of hiding or obscuring the screen, in the same manner, is just not possible because it will create a hindrance for the user.
During the period of year 1996 to 2010, a lot of research went into the development of useful graphical passwords. Some shoulder-surfing resistant graphical passwords were also developed in this period but the cognitive load, placed by them on the user, was a lot. In 2006, a point-and-click graphical password scheme named Convex Hull Click (CHC) scheme was developed (Wiedenbeck et al., 2006). By clicking in the imaginary convex hull, made by the secret icons of the user, this scheme mitigated shoulder-surfing to some extent and provided good usability through its game-like interface.

This scheme also took more time, as compared to textual password schemes, but a layman user found this scheme fun to use so this tradeoff got covered to some extent. It still became a subject of some statistical analysis attacks and the brute force attack (Asghar, 2012; Asghar et al., 2013; Yan et al., 2012). Although this scheme is still in its research phase, it carries a good potential to be used in the industry, that is, in regions where a high level of security is required.

Thus, this research focused on producing two variants of this scheme, named Centroid-Oriented CHC (CO-CHC) scheme and Rogue CHC scheme. In CHC password scheme, large convex hulls can also be produced due to the random placing of the secret icons in every authentication round. These large convex hulls cover the whole screen, and contribute in the success of the random-click attack, which is a type of brute force attack. CO-CHC scheme introduces clicking on a reduced probable area around the centroid of the convex hull, thus leading to less chance of the random click attack. Rogue CHC scheme mitigated a statistical analysis attack whereby the adversary used a technique, based upon geometry, to discover the secret icons once he or she had the screenshot of the click point. Thus, the attacker would come to know about the positions of the convex hulls, being produced, after discovering the secret icons. As the click point is always inside the convex hull and led to this attack, it was placed outside at certain distances from the convex hull in Rogue CHC scheme. As the convex hull had four sides due to four secret icons, there were four probable click points to allow the user more ease. As the click points were outside now, the adversary had to work on more combinations of the secret icons so the attack was made seemingly difficult.

Although these schemes were more secure but their usability had to be found out properly because in the real world, it would be used by people, other than those with technical knowledge, too. Thus, a proper usability study, with 30 participants, was done. The effectiveness and efficiency of these schemes was found out. The way the participants dealt with the learning curve, of these schemes, was observed. After the analysis of the results, it was found out that Rogue CHC scheme has got more potential for practical usage, as compared to CO-CHC scheme, because the participants were more comfortable with its usage. They were more at ease with having more than one click point to consider. Thus, their response time was faster but it should be remembered that both schemes have their pros and cons and their application will differ. Another main target of this research is to bring the attention of the research community towards graphical password schemes because they can be a good alternative to textual password schemes in many areas.

7.2 Future Work

Although the tradeoff between security and usability has been taken care of, there are still many factors to consider. Having more click points in Rogue CHC scheme does help the user but it leads to decreased security as random click attack can be carried out easily. Considering both variants, a more refined usability study can be carried out. This usability study was carried out with university students but a better usability study can be done in an office environment. Also, by utilizing advanced knowledge of geometry and development of graphics, more variants can be built and tested. This research was focused more on usability. An appropriate research direction, for testing the resilience of CO-CHC scheme and Rogue scheme, would be rerunning the statistical analysis attacks, mentioned in this research, on them. By doing this, one will be able to observe and analyze the difference between CHC password scheme and the newly formed variants formally.

Appendix A

Links to Data Collected for Testing and Analysis

This appendix contains links, on Google Drive, of Microsoft Excel files, which contain the collected raw data and the analysis done during the three tests of the usability study. The calculations were done by using the built-in and some user-defined mathematical formulas in Microsoft Excel. The graphs, shown in this thesis, are contained in the file related to Test 2. These links have been given for verification of the results and assistance in further research. The links are given below.

1. Collected Data and Analysis for Test 1 (Centroid-Oriented CHC Scheme): https://drive.google.com/file/d/1EX4fFgc0OvVgTfUcZfZAzSG9p500RQK2/view?usp=sharing

2. Collected Data and Analysis for Test 1 (Rogue CHC Scheme): https://drive.google.com/file/d/1x0u7OIzIUHK1SPh8ZJqmuVvd1P37tO6D/view?usp=sharing

3. Collected Data and Analysis for Test 2 (All Schemes): https://drive.google.com/file/d/1B2NN8cZ5KRP9VWoO-bPur0xEfkM8h2u0/view?usp=sharing

4. Collected Data and Analysis for Test 3: https://drive.google.com/file/d/15wSzWFsrAJChIMKRtamteKmxRWrb22sy/view?usp=sharing

Bibliography

Aken, J. E. v. (2004). Management research based on the paradigm of the design sciences: the quest for field-tested and grounded technological rules. *Journal of management studies*, 41(2):219–246.

Asghar, H. J. (2012). *Design and Analysis of Human Identification Protocols*. PhD thesis, Macquarie University.

Asghar, H. J., Li, S., Pieprzyk, J., and Wang, H. (2013). Cryptanalysis of the convex hull click human identification protocol. *International Journal of Information Security*, 12(2):83–96.

Bourke, P. (2013). Calculating the area and centroid of a polygon. www.seas.upenn.edu/{~}sys502/extra.../PolygonAreaandCentroid.pdf{%}0A.

Brostoff, S. and Sasse, M. A. (2000). Are Passfaces More Usable than Passwords? A Field Trial Investigation. *People and Computers*, pages 1–20.

De Angeli, A., Coutts, M., Coventry, L., Johnson, G. I., Cameron, D., and Fischer, M. H. (2002). VIP: a visual approach to user authentication. *Proceedings of the Working Conference on Advanced Visual Interfaces*, pages 316–323.

De Angeli, A., Coventry, L., Johnson, G., and Renaud, K. (2005). Is a picture really worth a thousand words? exploring the feasibility of graphical authentication systems. *International journal of human-computer studies*, 63(1-2):128–152.

Denning, P. J. (1997). A new social contract for research. *Communications of the ACM*, 40(2):132–134.

Hopper, N. J. and Blum, M. (2001). Secure Human Identification Protocols. *Asiacrypt*, pages 52–66.

Kuechler, B. and Vaishnavi, V. (2004). Design science research in information systems. *URI: http://www. desrist. org/design-research-in-information-systems/. Online*.

Li, S. and Shum, H.-Y. (2003). Secure Human-Computer Identification (Interface) Systems against Peeping Attacks (SecHCI): A Survey. *IACR Cryptology ePrint Archive: Report 2005/268*, (1):268.

Li, S. and Shum, H.-Y. (2005). Secure Human-Computer Identification

(Interface) Systems against Peeping Attacks: SecHCI. *IACR Cryptology ePrint Archive: Report 2005/268*, 2005:268.

March, S. T. and Smith, G. F. (1995). Design and natural science research on information technology. *Decision support systems*, 15(4):251–266.

Matsumoto, T. (1991). Human Identification Through Insecure Channel. *Eurocrypt*, 547:409–421.

Matsumoto, T. (1996). Human-computer cryptography: an attempt. *Proceedings of the ACM Conference on Computer and Communications Security*, pages 68–75.

Perrig, A. (2000). 9th USENIX Security Symposium Dej'a Vu : A User Study Using Images for Authentication. In *Proceedings of the 9th USENIX Security Symposium*.

Piirainen, K., Gonzalez, R., and Kolfschoten, G. (2010). Quo vadis, design science?–a survey of literature. *Global Perspectives on Design Science Research*, pages 93–108.

Sobrado, L. and Birget, J.-C. (2002). Graphical passwords. *Rutgers Scholar*, 4(4).

Takeda, H., Veerkamp, P., and Yoshikawa, H. (1990). Modeling design process. *AI magazine*, 11(4):37.

Wang, C.-H., Hwang, T., and Tsai, J.-J. (1995). On the Matsumoto and Imai's Human Identification Scheme. *Eurocrypt*, 921:382–392.

Weinshall, D. (2006). Cognitive authentication schemes safe against spyware (short paper). *Proceedings - IEEE Symposium on Security and Privacy*, 2006(May):295–300.

Wiedenbeck, S., Waters, J., Birget, J. C., Brodskiy, A., and Memon, N. (2005). PassPoints: Design and longitudinal evaluation of a graphical password system. *International Journal of Human Computer Studies*, 63(1-2):102–127.

Wiedenbeck, S., Waters, J., Sobrado, L., and Birget, J.-C. (2006). Design and Evaluation of a Shoulder-Surfing Resistant Graphical Password Scheme. *In the proceedings of the working conference on Advanced visual interfaces (AVI'06)*, pages 177–184.

Wikipedia (2017). Design science (methodology) - Wikipedia. https://en.wikipedia.org/wiki/Design{_}science{_}(methodology). 2017-11-07.

Yan, Q., Han, J., Li, Y., and Deng, R. H. (2012). On Limitations of Designing Leakage-Resilient Password Systems : Attacks , Principles and Usability. *19th Network & Distributed System Security Symposium (NDSS)*.

Zhao, H. and Li, X. (2007). S3PAS : A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme. In *21st International Conference on Advanced Information Networking and Applications Workshops*.