Chapter 5: Click to Zoom-Inside Authentication

In this Chapter we propose and evaluate the usability and security of Click to Zoom-inside (CTZ); a new graphical password authentication mechanism. Users have to click six times on one point in some given specific regions (pass regions) shown with dotted lines in a theme image displayed on the screen. The selected region is then zoom to create a next image. Exactly, we are not going to zoom the region object of the theme image up to six times; rather we are replacing the image with another image of the same object in big size. The next image is based on the previous click-region. We secure our scheme from shoulder surfer attacking by using WIW scheme with our scheme. We also present the results of an initial user study which revealed positive results. Performance was very good in terms of speed, accuracy, and number of errors in recognizing the images. We can also demonstrate that CTZ provides greater security than Pass Points because the number of images increases the workload for attackers also it is more user friendly and attractive than other competitive schemes. It is just parallel to Click Click Scheme. It meets the today’s requirement of extremely high security.

5.1 Introduction

Today, s network environment is full of dangerous attackers, hackers, crackers, and spammers. Authentication, authorization and auditing are the most important issues of security on data communication. In particular, the user authentication is indispensable to every person living closest friends, but also a key area of security research. Authentication system is based on the passwords which use the alphanumeric for authentication and identifier. Many authentication techniques including biometrics and smart card are the possible and useable applications. The authentication security can be increased, but sometime the passwords seem to remain dominant due to the drawbacks of reliability, security, or cost of other techniques. Biometric techniques make use of physiological or behavioral characteristics to be their identities. Authentication may be secure, but it still needs to resolve the security usability and balance for general usage. And, smart card also needs to type
passwords for user authentication. Here, we propose a new graphical password authentication protocol to solve this problem.

Graphical password technique is one of methods which may provide more secure and more efficiency system for authentication. Usable and easy memorization is the main research issues of graphical password authentication. Patrick, et al. [1] demonstrated that there are three key areas where human-computer relations are important: authentication, security operations, and developing secure systems. For authentication purposes, in various environments, we generally use a text (alphanumeric) based password authentication mechanism. The vulnerabilities of this methodology have been well known. However, there are certain problems we are facing with alphanumeric system. Studies have shown that users tend to pick short passwords or passwords that are easy to remember, however, these passwords can also be easily guessed or broken because of their less prediction space. User Studies showed that user tend to write down or use the same passwords for different accounts, as user can remember only a limited number of passwords [2, 3]. Studies also showing that pictures are generally easier to remember or recognize than text. In this context Graphical password schemes are developing very fast with the hope of possible alternative to text based authentication.

The number of Graphical password schemes is available to show their relative assessment and accountability over text based (alphanumeric) authentication. Current research and user study have shown that text-based pass-words are weighed down on the basis of memorability, usability and security problems that make them less trusted for authentication purposes. Though the text based authentication take less time for the process and occupy usually less space in memory. Dictionary attack, Brute Force Search, Guess, Spyware, Shoulder Surfing etc. are some possible password hacking mechanism may be used to crack the security based on text based authentication. Perrig and Song [4] developed graphical password system in which user can pick several picture out of many choices. The problem with this mechanism was that it takes much time for processing and occupies much larger space in memory than text. Brute Force Search, Guess & Shoulder Surfing etc. may be the possible attacks on this mechanism. Sobrado and Birget [5] provides pre-register picture objects to user and user has to click within the area bounded by picture objects. It is faster in
process but may be hard to remember if the large numbers of objects are involved. Brute Force Search & Guess are the two possible attacks with the mechanism.

Man, et al. [6] & Hong et al. [7] developed another mechanism in which user has to type in the code of pre-register objects. It is faster but less in memorability because user has to remember both picture objects with their code; it is much more difficult than text. Brute Force Search & Spyware may be the two possible attack for such mechanism. Passface [8] mechanism had been developed to recognize and pick pre-registered picture. It takes longer time than text and the choices are still easily predictable. Dictionary attack, Brute Force Search, Guess, Shoulder Surfing are some possible attacks, a hacker can use. According to Jansen et al. [9-11] user has to register a sequence of images. It is slower than text based mechanisms. Brute Force Search, Guess, Shoulder Surfing may be some possible attacks on the mechanism. Takada and Koike [12] developed mechanism in which user has to remember and click to some pre-registered pictures. The users are also free to choose any of their favorite images. It has high memorability with slower than text based authentication. Force Search, Guess, Shoulder Surfing may be some possible attacks on the mechanism.

According to Jermyn et al. [13], Thorpe and Van Oorschot [14, 15] users has to draw anything of their choice on 2D grid in some sequence. Users study showed that the drawing sequence is hard to remember. Dictionary attack & Shoulder Surfing are possible attacks on the mechanism. In Syukri, et al. [16] developed mechanism user has to draw their signature with the help of mice. It is very easy to remember and hard to recognize also it needs a very reliable signature recognition program. Dictionary attack, Guess & Shoulder Surfing are possible attacks on the mechanism. Goldberg et al. [17] developed an interesting mechanism in which user has to draw anything onto a touch sensitive screen. Dictionary attack & Shoulder Surfing may be possible attacks on the mechanism.

Blonder [18] Passlogix [19-21] & Wiedenbeck et al. [22-24] developed a very popular mechanism in which user has to click on several pre-registered regions in a right sequence. It is very user friendly but may be hard to remember the right sequence. Brute Force Search, Guess, Shoulder Surfing may be some possible attacks on the mechanism. With keeping such an interesting mechanism in mind we are here proposing a very new CLICK TO ZOOM-
INSIDE (CTZ) password authentication mechanism. In a very first look, it can be viewed similar to Pass Points [23, 24], Passfaces [25], Davis [26] and Cued Click Points [27].

We also have conducted an in-lab user study with 20 participants and a total of 200 trials. Users had a very high success rates. They could quickly create, recognize and re-enter their passwords and were found very correct. Participants rated the system positively and indicated that they strongly preferred CLICK TO ZOOM-INSIDE (CTZ). They also appreciated the implicit feedback telling them whether their latest click-point was correctly entered. A first round security analysis of this new scheme is also presented. Hotspots [28] (i.e. areas of the image that users are more likely to select) are a concern in click-based passwords, so CLICK TO ZOOM-INSIDE (CTZ) uses a large set of images that will be difficult for any hacker. For our proposed system, hotspot analysis requires proportionally more effort by attackers, as each image must be collected and analyzed individually. CLICK TO ZOOM-INSIDE (CTZ) appears to allow greater security than Pass Points or CCP; the work-load for attackers of CLICK TO ZOOM-INSIDE (CTZ) can be arbitrarily increased by augmenting the number of images in the system. For understanding the problems in practical implementation of CLICK TO ZOOM-INSIDE (CTZ), it is projected for environment where shoulder-surfing is a serious threat. To secure our authentication from shoulder surfing type attacks, we are using WIW scheme with our scheme.

5.2 Click to Zoom-Inside Authentication

The CLICK TO ZOOM-INSIDE (CTZ) authentication is a proposed alternative to Pass Points and Cued Click Points schemes. It is a parallel research to Cued Click Point. I mean by it that we have borrowed some features from clued click point scheme and proposed a very new and high secure authentication mechanism. In CTZ, users have to click on one point of some specific regions of a large theme image consists of several objects, shown by dotted line. He has to click 6 times to create a password. Each click in the specific region results the next image which is the zoom image of the specific region and the user has to click again on some specific areas shown dotted in this given image which results the next image. The sequence of clicked images creates a password. User has to click the specific areas in a right sequence. A wrong click leads down an incorrect path, with an explicit
indication of authentication failure only after the final click. Users can click the regions only to the extent that their click-point dictates the next image. If they dislike the resulting images, they could create new password by clicking some new areas involving different images.

Similar to the Pass Points and Cued Click Point studies, our example system had images of size 451x331 pixels. The theme image has 101 specific areas in which the user can click. This suggests a minimum set of 101 images is required at each stage. The number of images would quickly become quite large. So we propose re-using the image set across stages. By re-using images, there is a slight chance that users see duplicate images. If the user will not get the correct next-image, the implicit feedback of incorrect password will be shown on the screen finally. A major usability improvement over Pass Points is the fact that genuine users get immediate feedback about an error when trying to log in. When they see an incorrect image, they know that the latest click-point was incorrect and can immediately cancel this attempt and try again from the beginning.

5.3 WIW Scheme

The theme idea of WIW scheme [29] is borrowed from a well known puzzle game Where Is Waldo. In the scheme a user choose an alphabet for his password. At each time of login system randomly spells a string from the alphabet. A technical challenge is that it should be easy for the user to identify each of those strings and in the mean time; it is much difficult for an attacker to recognize any of those strings. A password is formed via a sequel of zoom images which will create on clicking a region inside the theme image. One after another, chosen areas are displayed on screen as a next image in a fixed order. One image is used for one letter. In an image there are many regions among which there are a few so called pass-regions. Pass-regions are pre-chosen by the user as a part of his password. They are recognizable only to the user. A combination of appearances and locations of those pass-regions spells a letter. From login to login, in each theme image the locations of the pass-regions are randomly changed and their appearances are perturbed such that the letter spelled varies randomly. In this way designed scheme become secure from an attacker hardly know those letters and may film the user's login process.
5.4 Implementation of Click to Zoom-Inside (CTZ) scheme

We have developed our scheme preliminarily in Computer Science Lab for Engineering Graduates of our Institute. We call this lab Network Security Lab. We have also conducted in-lab trial of our proposed scheme with 20 Computer Science Graduate students and 10 from diverse fields (but they all were regular web user); 10 of them were females and 20 males.

The trial consists of one-hour session for an individual in our lab. First they all signed the consent form for the trial. They were also given printed instructions booklet for operating the system during the session. This introductory booklet included showing them an example theme image consists of several regions and how they create next image by clicking any one region on the image. We also explained that the next zoom image in the sequence depended on where they clicked on the current displayed image. It was also mentioned in the booklet that if they suddenly saw an image they did not recognize during the Login phases, then they might be following a wrong path. Participants completed two practice trials followed by 10 real trials. In total, 251 real CTZ trials were completed.

Algorithm of the trial may be designed as follows. The phases indicated in steps 1, 2, and 5 represent the password phases used in later analysis.

1. Create phase: Create a password by clicking sequentially on one point in each of six images. The next image is the zoom (big size) image of the clicked region.

2. Confirm phase: Confirm this password by reselecting the same regions in the image. Users incorrectly confirming their password could retry the confirmation or return to Step 1. A new password started with the same initial theme image, (the theme image consists of similar objects in the regions but may have placed at a different position in the image).

3. Queries: user is asked for two queries about how ease the CLICK TO ZOOM-INSIDE (CTZ) password scheme for creating passwords and prediction memorability of those passwords.

4. Mental Relaxation Time: A Mental Rotations Test (MRT) puzzle [9] for mental refreshment is also given to users. This paper based task was used to divert users for one
minute by giving them a visual puzzle to complete in order to clear their working memory.

5. Login phase: Log in with their current own created password. If users noticed an error during login, they could cancel their login attempt and try again. Alternatively, if they did not know or remember their password, they could create a new password, returning to Step 1 of the trial with the same initial theme image as a starting point. If users felt too frustrated with the particular images to try again, they could skip this trial and move on to the next trial.

Participants completed as many trials as they wished in the one-hour session, to a maximum of 10 (4 practice + 6 real trials). At the midpoint, participants took a break and completed a demographics questionnaire. The last ten minutes is the time for open-ended questionnaire about their perceptions and opinions for our graphical password scheme. For each participant, data from the two practice trials were discarded, so all results included in this paper are based on data from the subsequent trials.

In another time we have given one further task to the participants: to complete a trial with our Pass Points-style system, where they selected five points on one image. The experimenter was careful to identify the second system as “another scheme we have designed for their opinion” rather than the “old” system, to not bias participants into thinking that they should rate CLICK TO ZOOM-INSIDE (CTZ) more favourably. Users were then asked which scheme they preferred. The scheme is protected from the shoulder surfing WIW scheme which makes it more secure than other competitive schemes available till date. The password will be protective even if someone had seen the password creation session. But users found to be confused regarding shoulder surfing security.

Three methods were used to collect data in this study: system logs, questionnaires, and observations. The system recorded the exact pixel coordinates of each click-point on every image visited by participants for every Create, Confirm, or Login attempt, along with the time of each event. A post-test questionnaire was used to know about users perceptions and opinions about the scheme. A second questionnaire was used to collect the demographic data to help framing the results of the study. Users were also asked two online questions
immediately after successfully confirming their password to get an immediate reaction of how easy it was to create the password and how difficult they expect it would be to remember their password in a week.

Finally, an observer sat with each participant throughout the session, noting any difficulties or unexpected behavior as well as comments made by the participants. The participants may ask any question to the observer or seek help where they required between trials where they would not affect the timings.

5.5 Results

Participants can use the resubmit button as soon as they saw any incorrect zoom image and realized they were on the wrong step. This effectively cancelled the current trial as resubmitting returned them to the initial image where they could start entering their password again. Some times, participants restarted again the trial session even when they saw the correct image because they might forgot the password images. Failed login attempts (where users pressed the login button and were explicitly told that their password was incorrect) occurred only when users clicked on the wrong object image for the last image in the sequence since they did not receive any implicit feedback for that click-point. Because these were so few, failed login attempts are included in the restart counts. Participants said that confirming the password helped them to remember it. This fact is reflected the Restarts.

Table 5.1 which shows that the majority of restarts occurred during the Confirm phase.

<table>
<thead>
<tr>
<th></th>
<th>Create</th>
<th>Confirm</th>
<th>Login</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total no. of resubmits</td>
<td>6</td>
<td>100</td>
<td>12</td>
</tr>
<tr>
<td>Success rate</td>
<td>242/251 = 96%</td>
<td>201/251 = 80%</td>
<td>239/251 = 95%</td>
</tr>
<tr>
<td>Mean time (in Sec)</td>
<td>29.8</td>
<td>16.7</td>
<td>12.8</td>
</tr>
</tbody>
</table>

Table 5.1

Six participants completed all their trials without any resubmits, i.e. they made no errors during the entire session. In total, 189 out of 251 trials (75%) were completed without resubmits in any phase. The success rates were found to be relatively high for all phases, shown in Table 5.1. For each phase, success rates were calculated as the number of trials completed without errors or resubmits over the total number of trials.
5.5.1 Degree of accuracy

Degree of accuracy of recalling the passwords created by the participants at the time of registration is found to be relatively high. They were successfully made login by reselecting the original object images by clicking the theme or object image at the right point. The degree of accuracy can be finding by determining the maxima of the variation between the x and y coordinates of click point at the time of registration and click point at the time of login or how many click points at the time of login are out of the object region. All the click points were considered even those were unsuccessful. Analysis graph & Table 5.2 shows that there were only 12% clicks out of object region at the time of login.

<table>
<thead>
<tr>
<th>Login Attempts</th>
<th>Total click points</th>
<th>No. of out clicks</th>
<th>% of out clicks</th>
</tr>
</thead>
<tbody>
<tr>
<td>68</td>
<td>220</td>
<td>6</td>
<td>2.727272727</td>
</tr>
<tr>
<td>22</td>
<td>390</td>
<td>8</td>
<td>2.051282051</td>
</tr>
<tr>
<td>80</td>
<td>288</td>
<td>7</td>
<td>2.430555556</td>
</tr>
<tr>
<td>41</td>
<td>198</td>
<td>6</td>
<td>3.03030303</td>
</tr>
<tr>
<td>41</td>
<td>426</td>
<td>8</td>
<td>1.877934272</td>
</tr>
<tr>
<td><strong>Total %</strong></td>
<td></td>
<td></td>
<td><strong>12.11734764</strong></td>
</tr>
</tbody>
</table>

Table 5.2 Showing Degree of Accuracy while re-entering the passwords

Graph 5.1: Showing Degree of Accuracy while re-entering the passwords
5.5.2 Time involvement in password creation

Because Participants were from various fields having different mindset to understand what to do, it made a larger time to be familiar at the time of creation of Passwords, but successively when they gone through with the Next Phases; Confirm and Login they become expert and took a very less of time. Table 5.1 shows the average time taken in respective phases. It is less than a half minute in average which is quite acceptable and makes it feasible for various applications in different environment.

5.5.3 Query session

During Questionnaire session participants were provided two sets of questions. In one set for which they have to answer at the time of each confirm phase; they have to answer two queries, one weather the given task is easy to do and another was weather the created passwords are easy to remember or recall. The answer for these queries was rated from 0 to 10; where 0 represents that the participant is most unsatisfied and 10 represents that the participant is most satisfied with our system. Each participant score between 0 to 10 according to their own decision.

We have collected the results and take the average of all. The average come out is 8, which is quiet high as we expected. The second query set was delivered at the last of the one hour session. These are some general queries about their experience for our Graphical password authentication system. We are writing here a subset of such query set shown in Table 5.3. The participants scored well and recommend strongly our scheme. However, they were slightly confused regarding shoulder surfing WIW scheme used with our scheme and the result has reflected from their answer for the query S. No.2, while they all said that our proposed scheme is very attractive, easily understandable to lay man.
<table>
<thead>
<tr>
<th>S. No.</th>
<th>Queries</th>
<th>Score in average (range 0-10)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>How you found Graphical password authentication ease over alphanumeric in respect of Creation and recalling?</td>
<td>7</td>
</tr>
<tr>
<td>2</td>
<td>Someone who knows me very well or might have seen the whole session of password creation can better guess my password?</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>How you feel about our scheme for security purpose?</td>
<td>6</td>
</tr>
<tr>
<td>4</td>
<td>How ease the scheme for understand the process?</td>
<td>8</td>
</tr>
<tr>
<td>5</td>
<td>How you recommend our scheme for authentication purpose relative to existing schemes?</td>
<td>8</td>
</tr>
</tbody>
</table>

Table 5.3: Questionnaire Subset

5.5 Conclusion

The proposed CTZ scheme promises more comfortable, easy to use, more memorable and more secure authentication. With the power of graphical images more memorable to text, our scheme is also provided more memorability for the passwords. Using WIW scheme with our scheme is under consideration because participants recommended the association half heartedly; while they were appreciating our scheme. The method proposed in this chapter is also required to test it initially for security purposes. It is also required to test it for some real world applications in various environments and modify it according to the application need. We hope someday our scheme will be applicable to replace text based authentication system.
References


