A Robust Graphical-Based Authentication for Knowledge Level Using Persuasive Cued Click Points

S. Subadra[1], S. Ushanandhini[2]

[1]Research Supervisor, Assistant Professor, Department of Information Technology,
Sri Jayendra Saraswathy MahaVidyalayaCollege of Arts and Science, Coimbatore-5, India

[2]Research Scholar, Sri Jayendra Saraswathy Maha VidyalayaCollege of Arts and Science, Coimbatore-5, India

Abstract: ***The graphical based technique is mainly used for authentication purpose. The purpose of this paper is increasing the security space and usability and avoiding the weakness of conventional password. The graphical based password technique uses persuasive cued click point. This persuasive Cued click points was designed to reduce patterns and reduce the usefulness of hotspots for attackers. An important usability goal for authentication systems is to support users in selecting better passwords, thus increasing security by expanding the effective password space. In click-based graphical passwords, poorly chosen passwords lead to the emergence of hotspots. The graphical password technique use robust discretization method, this discrete method is used to determine a click point's tolerance square &corresponding grid. The click-based graphical passwords, encourage users to select more random, and hence more difficult to guess, click-points.***

Keywords: Authentication, Graphical password, Persuasive technology, Persuasive cued click point.

1. Introduction

A password is a form of secret authentication data that is used to control access to a resource. The passwords are used to control access to protected computer operating systems, mobile phones, ATM machines. A typical computer user may require passwords for many purposes: logging in to computer accounts, retrieving email from servers, accessing files, databases, networks, web sites, and even reading the morning newspaper online.

There are many things that are "well know" about passwords; such as that user cannot remember strong password and that the passwords they can remember are easy to guess [1]-[6].A password authentication system should encourage strong and less predictable passwords while maintaining Memorability and security. This password authentication system allows user choice while influencing users towards stronger passwords. The task of selecting weak passwords (which are easy for attackers to guess) is more tedious, avoids users from making such choices. Some drawbacks of conventional password appears like stolen the password, forgetting the password, week password. So a big necessity to have a strong authentication way is needed to secure all our application as possible, so a researches come out with advanced password called graphical password where they tried to improve the security and avoid the weakness of conventional password.

Graphical password is an authentication system [7] - [8] that works by having the user select from images in a specific order presented In a Graphical User Interface (GUI). For the reason, the graphical password approach is sometimes called Graphical User Authentication (GUA). Graphical password systems are a type of knowledge-based authentication system. This graphical based password system is mainly used to avoid weak password it's designed to make password memorable and easier for people to use and therefore more secure.

Among graphical password schemes [9] click-based graphical passwords has gained popularity. In click-based graphical password schemes [11], users click on one point per images for a sequence of images. The next image is based on the previous click-point. Certain points (hotspots) on the pictorial background are more likely to be selected by users, which makes passwords predictable. Different attack strategies are quite successful to guess click-based graphical password.

2. Related Work

Text passwords are the most prevalent user authentication method, but have security and usability problems. Replacements such as biometric systems and tokens have their own drawbacks [12], [13] .Graphical passwords offer another alternative, and are the focus of this paper. Graphical passwords were originally defined by Blonder (1996) [15].Graphical password schemes can be grouped into three general categories based on the type of cognitive activity required to remember the password: recognition, recall, and cued recall.

a. In recognition-based systems, in which a number of different images (e.g., faces, random art images) are displayed on user's screen and the user selects among these images to generate his password. This procedure can be repeated for a number of rounds to increase the password space. Although a recognition-based graphical password seems to be easy to remember, which increases the usability, it is not completely secure
b. In recall-based systems, the user needs to reproduce their passwords without any help or remainder by the system.
c. In cued-recall systems typically require that users remember and target specific locations within an image.

This feature, intended to reduce the memory load on users, is an easier memory task than recall based system. Such systems are also called locimetric as they rely on identifying specific locations. This memory task differs from simply recognizing an image as a whole. The user has to choose some of these regions to register as their password and they have to choose the same region following the same order to log into the system.

In Pass-Points [10], a password consists of a sequence of five click-points on a given image. Users may select any pixels in the image as click-points for their password. To log in, they repeat the sequence of clicks in the correct order, within a system-defined tolerance square of the original click-points. Attackers who gain knowledge of these hotspots through harvesting sample passwords or through automated image processing techniques can build attack dictionaries and more successfully guess Pass-Points passwords [16]. A dictionary attack consists of using a list of potential passwords and trying each on the system in turn to see if it leads to a correct login for a given account. Attacks can target a single account, or can try guessing passwords on a large number of accounts in hopes of breaking into any of them.

3. Our Contribution

The Persuasive Cued Click Points scheme [4] is effective at reducing the number of hotspots while still maintaining usability. Persuasive Technology was first articulated by Fogg [17] [18] as using technology to motivate and influence people to behave in a desired manner. An authentication system which applies persuasive technology, it's the emerging field of "interactive computing systems designed to change people's attitudes and behaviors", should guide and encourage users to select stronger passwords, but not impose system-generated passwords. To be effective, the users must not ignore the persuasive elements and the resulting passwords must be memorable. Our proposed system accomplishes this by making the task of selecting a weak password more tedious and time-consuming. The path-of-least resistance for users is to select a stronger password. As a result, the system also has the advantage of minimizing the formation of hotspots across users since click points are more randomly distributed. PT is a set of tools, media, and cues which technological solutions may implement to encourage users to behave in some desired manner.

We added a persuasive feature to encourage users to select more secure passwords, and to make it more difficult to select passwords where all five click-points are hotspots. Specifically, when users created a password, the images were slightly shaded except for a randomly positioned viewport (figure1). The viewport is positioned randomly rather than specifically to avoid known hotspots, since such information could be used by attackers to improve guesses and could also lead to the formation of new hotspots.

Users were required to select a click-point within this highlighted viewport and could not click outside of this viewport. If they were unwilling or unable to select a click-point in this region, they could press the "shuffle" button to randomly Reposition the viewport. While users were allowed to shuffle as often as they wanted, this significantly slowed the password creation process. The viewport and shuffle buttons only appeared during password creation. During password confirmation and login, the images were displayed normally, without shading or the viewport and users were allowed to click anywhere.

1. Users will be less likely to select click-points that fall into known hotspots.
2. The click-point distribution across users will be more randomly dispersed and will not form new hotspots.
3. The login security success rates will be higher than to those of the original CCP system.
4. The login security success rates will increase, when tolerance value is lower value.
5. Participants will feel that their passwords are more secure with PCCP than participants of the original CCP system

Figure 1: Persuasive Cued Click Point

3.1 Robust Discretization Method

The robust discretization method [14] is mainly used for authentication purpose. This method is mainly eliminate false accept and false reject and it also increase the password spaces since smaller grid squares can be used, and makes graphical passwords usable in real systems. It improves the usability and security space. A discrete method is used to determine a click point's tolerance square &corresponding grid. For each click point in a subsequent log-in attempt, this grid is retrieved & used to determine whether the click-point falls with tolerance of the original point. With cued click point need to determine which next image to display.

This approach involves using three offset grids to guarantee that every point in the image is a "safe" distance away from the edges of at least one grid. It was shown (figure 2) that three grids were necessary and sufficient to guarantee that for any given point in a 2-dimensional space, the system:

- "Guarantees the acceptance of approximately correct passwords". In other words, if a log-in click-point is within distance r from the original click-point then the input is accepted.
- "Guarantees the rejection of significantly wrong passwords". If a log-in click-point is at a distance greater than r max from the original click-point for some specified

tolerance, the input is guaranteed to be interpreted as different from the original click-point.

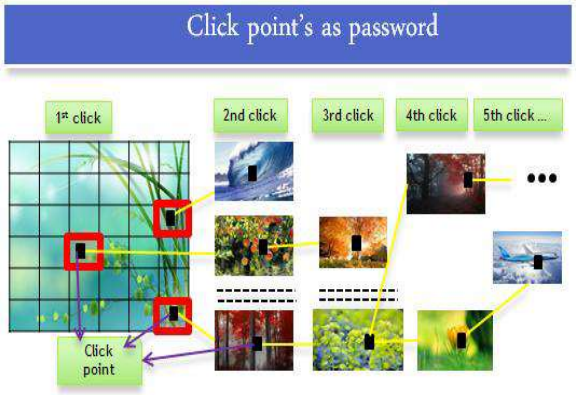

Figure 2: CCP passwords can be regarded as a choice-dependent path of images

When creating a password, one of the three grids is selected for each click-point. For each point, the system stores the grid identifier in the clear, and determines which grid-square contains the click-point. The coordinates of this grid-square are cryptographically hashed and the hash is stored along with the grid identifier. For each click-point in future login attempts, the system overlays the pre-selected grid onto the image and finds the coordinates of the grid-square containing the click-point.

Discretization (also called quantization) of data consists of approximating a continuum, or a very large discrete set, by a discrete set of limited size. The image is given by a function g: [0,a] × [0,b] → [0,1],where[0,a],[0,b] are intervals in the real p or in the integer z. To discretize R2, we choose a positive number q (called the quantum) and an offset (φ, ψ) (where $|\varphi|$, $|\psi| < q$), and we superimpose a square grid on the rectangle.

The grid has [a/q]+1vertical line

(Vm) x = qm +$_\varphi$ (where m = 0 . . . [a/q])
[b/q]+1 horizontal line
(Hn) y = qn +ψ (where n = 0 . . . [b/q])

This subdivides R2 into grid squares of side-length q; near the borders of R2, the grid squares are truncated. The discretization can also be described by a grid map, which tells us which points of the rectangle R2 are mapped to which grid vertices

$$g: (x, y) \in [0,a] \times [0,b] \rightarrow \left(\left[\frac{X-\varphi}{q} + \frac{Y-\psi}{q}\right]\right)$$

The set of points of R2 that are mapped to a given grid point(m, n) is

g^{-1}(m , n) = [(x , y) € R2 : qm+ $_\varphi$ <x< q(m+1)+ $_\varphi$ qn+ ψ <y< q(n+1)+ ψ];

The set g^{-1}((m; n) is called a grid square; the grid map g maps this entire grid square, namely [qm, q(m + 1)]× [qn, q(n + 1)], to the grid point (m; n). We proposed a "robust discretization" scheme, with three over-lapping grids, allowing for login attempts that were approximately correct to be accepted and converting the entered password into a cryptographic verification key. A discretization is robust if and only if it has two properties which are:

- If a location pointed to is close to an approximating a continuum, or a very large discrete set, by a discrete set of limited size. To fix the terminology, we describe a discretization of a two-dimensional (2-D) rectangular gray picture. The picture is given by a function [0; a] _ [0; b] ! [0; 1], where [0; a]; [0; b] are intervals in originally chosen location (within a specified tolerance distance < r1), then the output is the same as for the originally chosen location.
- If a location pointed to is at distance greater than r2 from the originally chosen location (for some specified tolerance distance r2 with r2 > r1), the output is guaranteed to be different than for the originally chosen location.

In our application to graphical passwords, conditions are,

1. Guarantees the acceptance of approximately correct passwords
2. Guarantees the rejection of significantly wrong passwords.

Our graphical password scheme has three components:

- Image handling
- password selections
- Log-in
- The image-handling component enables users to choose images or to introduce their own; the images are stored together with a collection of images provided by the system.
- The password selection component allows the user to select a new password. Assuming the user has already logged in the user enters the "password" command. The system then prompts the user for a user name and current password
- The log-in component presents the user with a window into which the user types the user name. The system then retrieves the user's password record and displays the user's password image.

4. Implementation

The implementation steps are:

Step1: Registration Phase: The system gets the user details as like user name, text password, mobile no, email id, city, conform password, security question and these details are stored in database for further processing. The rapid growth in the volume of available information is making it difficult for users to quickly locate pertinent information. Users come from a range of different backgrounds with varied computer literacy and Internet skills, and these users have a wide range of interests and preferences.

Step2: Create phase: Create a password by clicking on one point in each of five user-selected images presented in sequence. To create their password and then were progressively quicker in entering it during the Confirm and Login phases.

Step3: Confirm phase: Confirm this password by re-entering it correctly. Users incorrectly confirming their password could retry the confirmation or return to Module 1. A new password started with the same initial image, but generally included different images thereafter, depending on the click-points. Participants said that confirming the password helped them to remember it. Once they had successfully confirmed the password, logging on even after the distraction task was relatively easy.

Step 4: Alternate recovery phase: Answer two 10-point Likert-scale questions on the computer about their current password's ease of creation and predicted memorability. Likert-scale questions ask respondents to indicate their level of agreement with the given statement on a scale ranging from strongly agree to strongly disagree. First they answered two online questions immediately after successfully confirming each of their pass- words. They gave both "ease of creating a password" and "ease of remembering their password in a week".

Step 5: Log-in phase: Log-in with their current password. If users noticed an error during login, they could cancel their log-in attempt and try again. Alternatively, if they did not know their password, they could create a new password, effectively returning to Step 1 of the trial with the same initial 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.

5. Results

Participants used the reset button as soon as they saw an incorrect image and realized they were on the wrong path. This effectively cancelled the current attempt and returned them to the first image where they could start entering their password again. A few times, participants restarted even when they saw the correct image because they had forgotten the image. Failed log-in attempts (where users pressed the log-in button and were explicitly told that their password was incorrect) occurred only when users clicked on the wrong point for the last image.

Since they did not receive any implicit feedback for that click- point. Because these were so few, failed log-in attempts are included in the restart counts. Participants said that confirming the password helped them to remember it. Once they had successfully confirmed the password, logging on even after the distraction task was relatively easy. This fact is reflected in Table 1 which shows that the vast majority of restarts occurred during the Confirm phase.

Table 1: Total number of restart, Success Rate, and Completion Time per phase

	Create	*Confirm*	*Login*
Success Rate	251/257(98%)	213/257(83%)	246/257(96%)
Mean Time (sec)	16.4	13.1	5.5
Total number of Restarts	7	101	14

In total, 201 of 257 trials (79%) were completed without restarts in any phase. The success rates were high for all phases, as shown in Table 1. Success rates were calculated as the number of trials completed without errors or restarts over the total number of trials. Participants were extremely accurate in re-entering their passwords. As a measure of accuracy, all individual click-points in the Confirm and Log-in phases were evaluated. This totaled 1569 click-points for the Confirm phase and 1325 click-points for the Log-in phase The graphical representation of (fig 3 & fig 4 & fig 5) create phase, confirm phase, login phase shown in below.

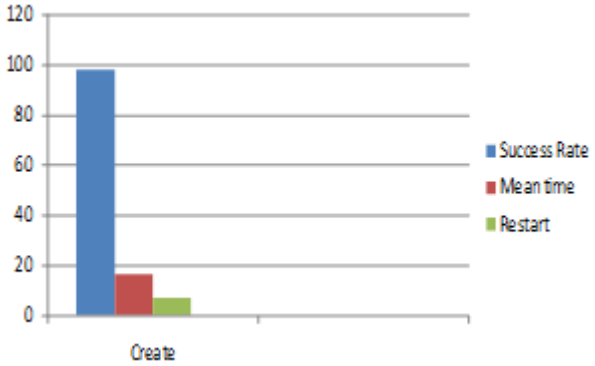

Figure 3: Graphical representation of Create phase

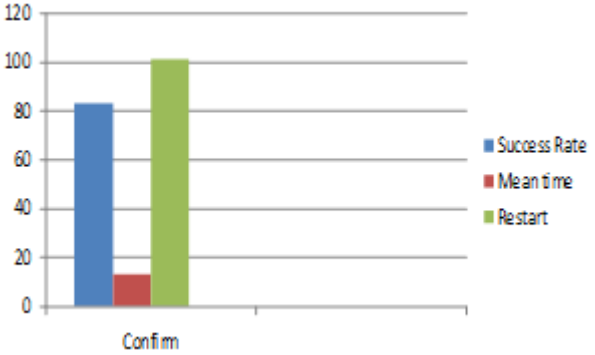

Figure 4: Graphical representation of Confirm phase

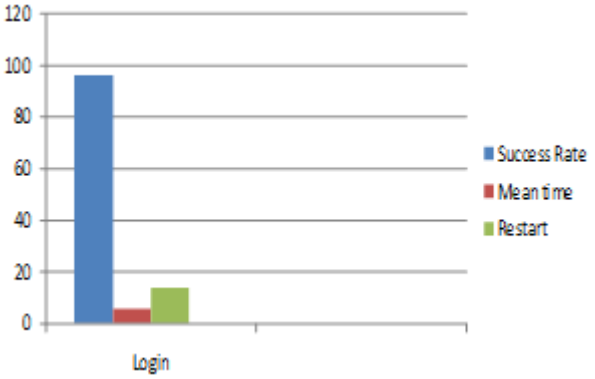

Figure 5: Graphical representation of Login phase

6. Conclusion

In this paper the graphical password technique is mainly useful for authentication purpose. The advantages of this technique is increasing usability and security space and avoiding weakness of password. The goal in authentication systems is to help user's select better passwords and thus increase the effective password space. Persuasive cued click point encourages and guides users in selecting more random click-based graphical passwords. Persuasive cued click points increases the workload for attackers and the system's flexibility to increase the overall number of images in the system allows us to arbitrarily increase this workload. The

approach has proven effective at reducing the formation of hotspots, and also provide high security success rate.

7. Future Work

In future we have planned to create a good authentication space with a sufficiently large collection of images to avoid short repeating cycles. Compared to other methods reviewed in our papers, may require human-interaction and careful selection of images and "click" regions. Future system may also need user training.

References

[1] S. Chiasson, A. Forget, R. Biddle, and P.C. van Oorschot, "User Interface Design Affects Security: Patterns in Click-Based Graphical Passwords," Int‟l J.Information Security, vol. 8, no. 6, pp. 387- 398, 2009.
[2] J. Yan, A. Blackwell, R. Anderson, and A. Grant, "The Memorability and Security of Passwords," Security and Usability: Designing Secure Systems That People Can Use, L. Cranor and S. Garfinkel, eds., vol. 7, pp. 129-142, O‟Reilly Media, 2005.
[3] S. Chiasson, A. Forget, E. Stobert, P. van Oorschot, and R. Bddle, "Multiple Password Interference in Text and Click-Based Graphical Passwords", Proc. ACM Conf. Computer and Comm. Security CCS), Nov. 2009.
[4] S. Chiasson, A. Forget, R. Biddle, and P. van Oorschot, "Influencing Users towards Better Passwords: Persuasive Cued Click- Points", Proc. British HCI Group Ann. Conf. People and Computers: Culture, Creativity, Interaction, Sept. 2008.
[5] Chiasson, S., R. Biddle, R., and P.C. van Oorschot. A Second Look at the Usability of Click-based Graphical Passwords. ACM SOUPS, 2007.
[6] E. Stobert, A. Forget, S. Chiasson, P. van Oorschot, and R.Biddle, Exploring Usability Effects of Increasing Security in Click-Based Graphical Passwords, Proc. Ann. Computer Security Applications Conf. (ACSAC), 2010.
[7] S. Chiasson, P. van Oorschot, and R. Biddle, "Graphical Password Authentication Using Cued Click Points," Proc. European Symp. Research in Computer Security (ESORICS), pp. 359-374, Sept. 2007.
[8] R. Biddle, S. Chiasson, and P. van Oorschot, "Graphical Passwords: Learning from the First Twelve Years," to be published in ACM Computing Surveys, vol. 44, no. 4, 2012.
[9] Davis,D, F.Monrose, and M.K.Reiter, "On User Choice in Graphical Password Schemes",13th USENIX Security Symposium,2004.
[10] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and Longitudinal Evaluation of a Graphical Password System," Int‟l J. Human-Computer Studies, vol. 63, nos. 1/2, pp. 102-127, 2005.
[11] P.C. van Oorschot and J. Thorpe, "Exploiting Predictability in Click-Based Graphical Passwords," J. Computer Security, vol. 19, no. 4, pp. 669-702, 2011.
[12] L. Jones, A. Anton, and J. Earp, "Towards Understanding User Perceptions of Authentication Technologies," Proc. ACM Workshop Privacy in Electronic Soc., 2007.
[13] L. O‟Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication," Proc. IEEE, vol. 91, no. 12, pp. 2019-2020, Dec. 2003.
[14] Birget, J.C., D. Hong, and N. Memon. Graphical Passwords Based on Robust Discretization. IEEE Trans. Info. Forensics and Security, 1(3), September 2006.
[15] Blonder, G.E. Graphical Passwords. United States Patent 5,559,961, 1996.
[16] Thorpe, J. and van Oorschot, P.C. Human-Seeded Attacks and Exploiting Hot-Spots in Graphical Passwords. USENIX Security Symp. 2007.
[17] Lucero, A., Zuloaga, R., Mota, S., Muñoz, F.: Persuasive Technologies in Education: Improving Motivation to Read and Write for Children. In: IJsselsteijn, W., de Kort, Y.,Midden, C., Eggen, B., van den Hoven, E. (eds.) Persuasive 2006. LNCS, vol. 3962, pp.142–153. Springer, Heidelberg (2006)
[18] B. Fogg, Persuasive Technologies: Using Computers to Change What We Think and Do. Morgan Kaufmann Publishers, 2003
[19] Jermyn, I., A. Mayer, F. Monrose, M.K. Reiter, and A.D. Rubin. The Design and Analysis of Graphical Passwords. 8th USENIX Security Symposium, 1999.
[20] Suo, X, Y. Zhu, and G.S. Owen. Graphical Passwords: A Survey. Annual Computer Security Applications Conference, 2005.

Authors profile:

S. Subadra working as Assistant Professor in the Department of Information Technology, Sri Jayendra Saraswathy College of Arts and Science, Singanallur, Coimbatore. She has 9 years of teaching experience.

S. Ushanandhini, received her B. Sc degree in Computer Science (2008) from L.R.G govt arts college for women, Tirupur and M.sc degree in Information Technology (2010) from Bharathiar university, Coimbatore. At present she is doing her M. Phil in computer science. Her research area in Advanced Networking under the guidance of Mrs. S. Subadra working as Assistant Professor in the Department of Information Technology, Sri Jayendra Saraswathy college of arts and science, Singanallur, Coimbatore.