IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 13, Issue 2 (Jul. - Aug. 2013), PP 14-24
www.iosrjournals.org

Persuasive Cued Click Based Graphical Password with Scrambling For Knowledge Based Authentication Technique with Image Scrambling.

BINITHA . V .M.
Computer Science and Information Systems. Department Of Computer Science, Federal Institute Of Science And Technology, Mahatma Gandhi University, Kerala, India

Abstract: *Adequate user authentication is a persistent problem, particularly with hand- held devices such as Personal Digital Assistants (PDAs), which tend to be highly personal and at the fringes of an organization's influence. Yet, these devices are being used increasingly in corporate settings where they pose a security risk, not only by containing sensitive information, but also by providing the means to access such information over wireless network interfaces. User authentication is the first line of defense for a lost or stolen PDA. How- ever, motivating users to enable simple PIN or password mechanisms and periodically update their authentication information is a constant struggle. This paper describes a general-purpose mechanism for authenticating a user to a PDA using a visual login technique called Picture Password. The underlying rationale is that image recall is an easy and natural way for users to authenticate, removing a serious barrier to compliance with organizational policy. Features of Picture Password include style dependent image selection, password reuse, and embedded salting, which overcome a number of problems with knowledge-based authentication for handheld devices. Though designed specifically for handheld devices, Picture Password is also suitable for note-books, workstations, and other computational devices. Scrambling technique is applied to make image recognition more complex during the login process and thus protecting from the common attacks in the graphical password system.*

Keywords: *Graphical Passwords, Security, Image Scrambling,KBRP.*

I. Introduction

Computer security depends largely on passwords to authenticate human users. One of the key areas in security[1] research and practice is authentication, the determination of whether a user should be allowed access to a given system or resource. However, users have difficulty to remembering pass-words over time if they choose a secure password, i.e. a password that is long and random. Therefore, they tend to choose short and insecure pass-words. The continued domination of passwords over all other methods of end-user authentication is a major embarrassment to security researchers. As web technology moves ahead by leaps and bounds in other areas, passwords stubbornly survive and reproduce with every new web site. Extensive discussions of alternative authentication schemes have produced no definitive answers. A password authentication system should encourage strong passwords while maintaining memorability. We propose that authentication schemes allow user choice while influencing users toward stronger passwords. In our sys-tem, the task of selecting weak passwords (which are easy for attackers to predict) is more tedious, discouraging users from making such choices. In effect, this approach makes choosing a more secure password the path of least resistance. Rather than increasing the burden on users, it is easier to follow the systems suggestions for a secure passwords feature lacking in most schemes replace text passwords for general-purpose user authentication on the web using a broad set of twenty five usability, deployability and security benefits that an ideal scheme might provide. To validate the end user for authentication we usually prefer to adopt the knowledge-based authentication, which involves text based passwords. The text based passwords are vulnerable to be hacked. The attackers can easily guess the text passwords with other details of the system. If we want to avoid this, the system can assign a strong password, which the attacker cannot guess. But the system assigned passwords are very di cult to memorize and remembered by the user. The study on the graphical passwords states that the click point passwords are hard to guess by the attacker and easy to remember for the users. So the password authentication system should encourage the strong password selection while maintaining the memorability of the user. This paper proposes the idea of persuasive cued click point authentication[2,3] with the technique of scrambling. This scheme influence the user to set a number of clicks from a picture and size of passwords needed. The user can also change his passwords during a week oe everyday with altered images. This scheme fully depended on the memorability of the user about his selected images. Once he could not remember which portion of the image he selected for the click, the user will not authenticate even though he is a genuine user. To overcome this kind of

problem the system should keep some policies to retain the passwords.

2.1 BACKGROUND

The community of security researchers and practitioners has evolved rapidly in response to threats, on the one hand increasing vigilance in practice and, on the other hand, driving research innovation. Until recently the security problem has been formulated as a technical problem. Even though text passwords are the most popular user authentication method, they have security and us-ability problems. The alternatives for text based passwords such as biometric systems and tokens have their own drawbacks .Graphical passwords, which consist of clicking on images rather than typing alphanumeric strings, may help to overcome the problem of creating secure and memorable passwords. A graphical password scheme using click point offers the best alternative for the text password, cued click points are used to exploit the memeorablity of the user that it is fully a knowledge based authentication and is discussed in this paper the security and usability problems associated with alphanumeric pass-words as the password problem. The problem arises because passwords are expected to comply with two conflicting requirements, namely

(1) Passwords should be easy to remember, and the user authentication protocol should be executable quickly and easily by humans

(2) Passwords should be secure, i.e. they should look random and should be hard to guess; they should be changed frequently, and should be different on different accounts of the same user; they should not be written down or stored in plain text.

(3)The password problem arises primarily from fundamental limitations of human long-term memory (LTM).

Once a password has been chosen and learned the user must be able to recall it to log in. However, people regularly forget their passwords.

II. Introduction To PassPoints

PassPoints[4], a new and more secure graphical password system.This work proposed a password scheme in which the user is presented with a predetermined image on a visual display and required to select one or more predetermined positions (tap regions) on the displayed image in a particular order to indicate his or her authorization to access the resource. Beyond this .This system was developed early in the evaluation of graphical passwords, and in this, the user is given with an image. The click points on the image are used as the password for user authentication. The user has to remember the order and position of the click points. The click points are not stored as such, but as a hashed value. For correct validation, discretization square is used which is the tolerance area around the original click point. The user should click on the discretization area. Here, the system does not have any influence over the selection of the click points. The user is free to set the password which the user can easily remember. Since it is being very simple, it can easily be attacked. In PassPoints, passwords consist of a sequence of click-points on a given image. Users may select any pixels in the image as click-points for their password.

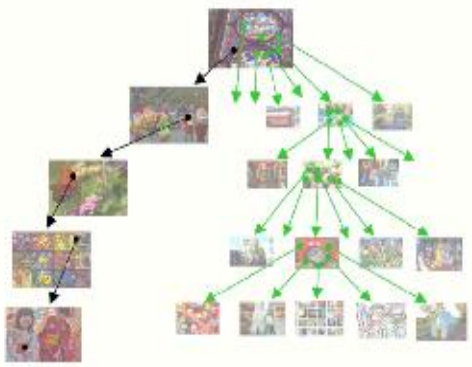

Figure 1 User Navigation through Clicks

To log in, they repeat the sequence of clicks in the correct order, within a system-defined tolerance square of the original click-points. The hypothesize that users will choose clickpoints based on their preference for certain points in the image, and that their preference for certain points will be influenced by how much they are naturally attracted to those points. Attention is the cognitive process of selectively fo cusing on one aspect of the environment while ignoring others, a mechanism that helps us prioritize sensory information. There are two different categories of visual attention models: bottom-up and top-down. Bottom-up visual attention captures

how attention is drawn to the parts of a scene or image that are salient or conspicuous. It is what naturally draws us to lo ok at the unexpected or different parts of a scene, prioritizing them from the other consistent parts. For example, if an image contains a large number of objects that are blue, and only one is yellow, human attention will instinctively focus on the yellow object. Top-down visual attention is task-dependent, based on cognitive, volitional control. With a priori knowledge about what object(s) to look for, our attention is brought to the parts of the scene containing

Figure 2 Passpoints

Those object(s). For example, if a user decides that people with dark hair are of interest for some reason, the users attention would shift between objects with features that might indicate a dark-haired person. In the PassPoints graphical password scheme a password consists of a sequence of click points (say 5 to 8) that the user chooses in an image. The image is displayed on the screen by the system. The image is not secret and has no role other than helping the user remember the click points. Any pixel in the image is a candidate for a click point.

To log in, the user has to click again closely to the chosen points, in the chosen sequence. Since it is almost impossible for human users to click repeatedly on exactly the same point, the system allows for an error tolerance r in the click locations (e.g., a disk with radius r = 10 or 15 pixels). This is done by quantizing (discretizing) the click locations, using three di erent square grids, as described in [3]. Each grid has width 6r between grid lines (horizontal or vertical). Each one of the three grids is staggered with respect to the previous grid by a distance 2r vertically and a distance 2r horizontally. If there were only one quantization grid then a

Figure 3(a)Actual click

Figure 3(b) Predicted Click in Passpoints

Selected click point could be close to a grid line and small variations in the user's clicking could lead to a click in a different grid square, thus leading to the wrong password. On the other hand, one can prove that with the three staggered grids every point in a two dimensional image is at distance at least r from the grid lines of at least one of the three grids; we say that the point is safe in that grid. We pursue heuristic-based strategies for purely automated dictionary generation (e.g., based on click-order patterns), and strategies to prioritize these dictionaries using image processing methods to identify points that users are more likely to choose.

3.1 Cued Click Points (CCP)

Cued Click Points [2] [3] [5] was designed to reduce patterns and to reduce the usefulness of hotspots for attackers. Instead of five click-points on one image, CCP uses one click-point on five different images. The next image displayed is based on the location of the previously entered click-point; it creates a path through an image set. Creating a new password with different click-points results in a different image sequence. One best feature of Cued Click Point is that the explicit indication of authentication failure is only provided after the final click-point, to protect against incremental guessing attacks. The cued click point method uses a series of images for click point password creation. The position of the click point on the previous image decides the next image to appear. It offers cued-recall and introduces visual cues that instantly alert valid users if they have made a mistake when entering their latest click-point (at which point they can cancel their attempt and retry from the beginning). The image used has the size 451x331 pixels and a tolerance square of 19x19 pixels. The candidate image or image, thus have approximately 400 squares. To have better discretization, 3 overlapping squares are assigned. So, in a candidate grid there could be 1200 squares. If a click on the first image is correct (by considering the tolerance squares), the user gets the next correct image.

Once the user practiced with the usage of click point password, user can readily understands when he/she clicks the wrong point, by looking at the next image. In this scheme also user is free to select the graphical password without systems intervention. So the attackers can easily guess the hot spot, which is the area where most of the users will tend to click. If the hacker[2] is succeeded in guessing the hot spots in the images then the hacker can log in to the system easily.

3.1.1 Persuasive Technology

Persuasive Technology [2] used to motivate and influence people to behave in a desired manner. An authentication system which applies Persuasive Technology should guide and encourage users to select

Stronger passwords, not the system-generated passwords[6]. Even though the users are guided, the resulting passwords must be memorable. This persuasion makes the password stronger by avoiding the hot spots in almost all the cases. The click points are more randomly scattered to avoid the correct guess by the attackers. The users must not ignore the persuasive elements and the resulting passwords must be memorable. As detailed below, PCCP 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 (not comprised entirely of known hotspots or following a predictable pattern). The formation of hotspots across users is
minimized since click-points are more randomly distributed.

3.2 Persuasive Cued Click Points (PCCP)

Using a skewed password distribution the attackers can guess the password in the previous graphical password schemes. Without the system guidance most of the users clicks on the hotspot in each image. In this method the system influence the user to select more random clicks, and also maintains the user memorability. In this scheme when the image is displayed the randomly selected block called the view port only clearly seen out. All the other parts of the image are shaded, so that the user can click only inside the view port. This is how the PCCP influence the user to select the position of the click point. The view ports are selected by the system randomly for each image to create a graphical password. It will be very hard for the attackers to guess the click point in all the images.

Figure 4 User interface of PCCP

Users are allowed to click anywhere in the view port. There is an option for changing the viewport position also. This option is called the Shuffle. There is a limit on the number of times the shuffle option to be used. While users may shuffle as often as desired, this significantly slows password creation. The viewport[1] and shuffle button appear only during password creation. Figure 4 User interface of PCCP During later password entry, the images are displayed normally, without shading or the viewport, and users may click anywhere on the images. Like PassPoints and CCP, login click-points must be within the defined tolerance squares of the original points. The theoretical password space for a password system is the total number of unique passwords that could be generated according to the system specifications. Ideally, a larger theoretical password space lowers the likelihood that any particular guess is correct for a given password. Whereas text passwords have very skewed distributions resulting in an effective password space much smaller than the theoretical space, PCCP is specifically designed to significantly reduce such skews. The recall studies of the PCCP approach proved that remembrance of the graphical password is much better than the text-based passwords.

III. Scrambling

With the current development of ubiquitous wireless network technology and digital multimedia devices, wireless image/video data transmission is becoming more prevalent. As a result, information security becomes a key problem for consumers, companies and governments. Security of image and video data is very important in many areas, such as video-on-demand, confidential remote video conferencing, security communication, and also in military applications. Image scrambling (i.e., encryption) technologies are very useful tools to ensure image security by transforming the image into an unintelligible image[7]. Scrambling makes the image unrecognizable to prevent eavesdroppers from decoding the true form or meaning of the image using the human visual system or a computer system. Image scrambling [8] is a useful approach to secure the image data by scrambling the image into an unintelligible format. This paper introduces a new parameter based M-sequence which can be produced by a series shift registers. There are currently several techniques to perform the image scrambling. In addition, a new image scrambling algorithm based on the M-sequence is presented. Image scrambling is used to make images visually unrecognizable such that unauthorized users have difficulty decoding the scrambled image to access the original image. This article presents two new image scrambling algorithms based on Fibonacci p-code, a parametric sequence. The first algorithm works in spatial domain and the second in frequency domain (including JPEG domain). A parameter, p, is used as a security-key and has many possible choices to guarantee the high security of the scrambled images. The presented algorithms can be implemented for encoding/decoding both in full and partial image scrambling, and can be used in real-time applications, such as image data hiding and encryption. Examples of image scrambling are provided. Computer simulations are

This has shown to demonstrate that the presented methods also have good performance in common image attacks such as cutting (data loss), compression and noise. The new scrambling methods can be implemented on grey level images and 3-color components in color images. A new Lucas p-code is also introduced. The scrambling images based on Fibonacci p-code are also compared to the scrambling results of classic Fibonacci number and Lucas p-code.

Two new image scrambling algorithms based on Fibonacci p-code. One is working in spatial domain, the other is for frequency domain (including JPEG domain). The security keys of our image scrambling algorithms are parameters p and i, and the size of original image. There are many possible choices for security keys so that the scrambled image is di cult to decrypt by unauthorized users, and thus, greater security is

guaranteed. A new Lucas p-code is also introduced. The scrambling images obtained from Fibonacci p-co de are compared to the scrambling results of classic Fibonacci number and Lucas p-code. This will demonstrate that the classical Fibonacci number is a special sequence of Fibonacci p-code when
p=1. Additionally, this will show the di erence of scrambling results by using the Fibonacci p-code and Lucas p-code.

4.1 P-Fibonacci And P-Lucas Transform

Fibonacci p-code [9] and a new Lucas p-code are introduced in this section. A new 1-D transform and a new 2-D transform are generated for both Fibonacci p-code and Lucas p-co de. The inverse 2-D transform used for recovering the original image is also presented

Definition : The Fibonacci p-code[10,11] is a sequence defined by,

$$F_p(n) \begin{cases} 0 & n < 1 \\ 1 & n = 1 \\ F(n \quad 1) \; F(n \quad p \quad 1) & n > 1 \end{cases}$$

where p is a nonnegative integer. From the definition above, Fibonacci p-code sequences will di er based on the p value. Specially,
(1) Binary sequence: p=0, the sequence is powers of two, 1, 2, 4, 8, 16……etc
(2) Classical Fibonacci sequence: p=1, the sequence is 1, 1, 2, 3, 5, 8, 13, 21……etc
(3) For the large values of p the sequence starts with consecutive 1?s and immediately after that 1, 2, 3, 4 ...p Sample sequences are shown in Table

p \ n	1	2	3	4	5	6	7	8	9	10	11	…
0	1	2	4	8	16	32	64	128	256	512	1024	…
1	1	1	2	3	5	8	13	21	34	55	89	…
2	1	1	1	2	3	4	6	9	13	19	28	…
3	1	1	1	1	2	3	4	5	7	10	14	…
4	1	1	1	1	1	2	3	4	5	6	8	…
…												
∞	1	1	1	1	1	1	1	1	1	1	1	…

Table 1 Fibnacci p-code sequence with different p value

4.2 Image Scrambling Algorithm In The Spatial Domain

The presented image scrambling algorithm in the spatial domain (shown in Figure 4.2) is designed to change the image pixel position using the 2-D P-Fibonacci Transform. Color images have three color components and the scrambling algorithm is applied to each color component individually. Grayscale images are treated as color images with one component. The presented algorithm is a lossless image scrambling method The Detailed description of the algorithm explained below for scrambling and unscrambling of images.

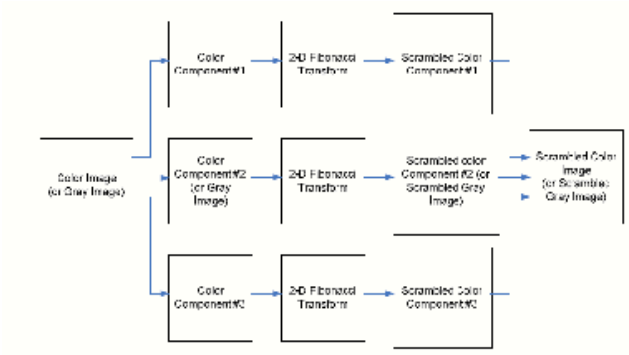

Figure 5 Block diagram of spatial domain scrambling

Algorithm for image scrambling

Step1:Choose the key parameter p, Calculate the row and column coefficient matrices of 2D p-Fibnaacci Transform

Step2:separate the 2D color image to three color component .Each component is a 2D matrix.

Step3: Apply 2D P-Fibnaacci transform to each color component to set the scrambled color component.

Step4 Recombine the three scrambled components to get the scrambled Image for password selection

The above algorithm says how to scramble the given digital images in spatial domain.

4.3 KEY BASED RANDOM PERMUTATION (KBRP)

A permutation, also called an "arrangement number" or "order," is a rearrangement of the elements of an ordered list ***S*** into a one-to-one correspondence with *S* itself. The number of permutations on a set of *n* elements is given by ***n!*** (***n*** factorial) A random permutation is a permutation containing a fixed number ***n*** of a random selection from a given set of elements. There are two main algorithms for constructing random permutations. The first constructs a vector of random real numbers and uses them as keys to records containing the integers 1 to ***n***. The second starts with an arbitrary permutation and then exchanges the *i*th element with a randomly selected one from the first *i* elements for *i* = 1, ..., ***n.*** Key Based Random Permutation (**KBRP**) is a method that can generate one permutation of size n out of ***n!*** permutations. This permutation is generated from certain key (alphanumeric string) by considering all the elements of this given key in the generation process. The permutation is stored in one-dimensional array of size equal to the permutation size (***N***).

This technique is used to generate the row and column coefficient matrices of each image components.

4.4 IMPLEMENTATION ASPECTS

Image based mutual authentication [12] has become now more reliable, when the scrambling technique applied [7].Users will me users should keep the click points to enter into the system, because the image get scrambled and it will be rearranged according to the scrambling algorithm discussed above. User have the provision to select his favorite areas according to his interest.

For any password authentication scheme,the prime task is to become a valid user of that system. For performing this each user have to provide the user id and password for creating the account just like in the conventional (textual) login system by specifying the username and password. This is for keeping an entry in the administrative level for further use for checking the intended user is authenticated or not. When a new user is intended to become a valid user ,the user have to select the new user and proceed. On the way to registration it will ask the userid and password,and the user should provide it through textual passwords. Now the user is entering to the PCCP System, here the textual password is replaced by the graphical password via clickpoints (cued). Hence the user have to select the decide how many click points needed to create the password and it will effect the strength of the password security. In order to improve the total security strength of the target system the number of click points used can also be increased while creating the graphical passwords. This can be achieved by setting the number of click point to be received from the user as a predefined value, say v. A number of view ports, which is equal to v are made visible on the image, for the user to click on it.

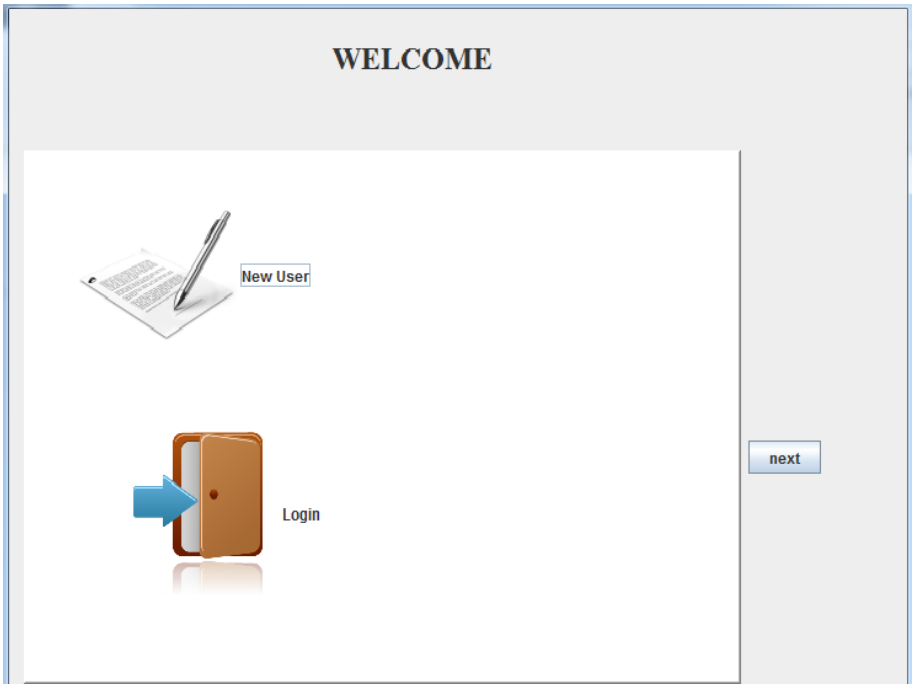

Fig 6 . New User SignUp : GUI

4.5 View port size

The effective password space is determined by the area of the view port of all images displayed for the password creation. The password strength is increased with the password space. So to create a strong graphical password, which cannot be guessed easily, the area of the view port should be higher. It can be done by deciding how many times the we can select the shuffle button which is directly proportional to the maximum number of viewports possible for an image. Then the number of click points also effecting as a predominant factor for ensuring the security. This idea may increase the strength of the password but this will decrease the user memorability of the password.

Fig 7 .Actual image for password Creation

4.5 Discretization of view port

In some occasions the user may accidentally click the point which is very near to the viewport, while logging in. If the user is genuine then he/she must be correctly logged in. Since we follow a very strict validation method, which requires the user to click on the view port, the genuine user cannot be allowed to use the application. To avoid this situation, we can compute the discretization are for the view port displayed on

each image. The user clicks are tolerated up to the discretization area. But this may reduce the robustness of the system.

4.6 Authentication of a valid user

The user after registration process have to memorise the click points what he selected to make the password.

The basis of PCCP starts from here. If he is a genuine user and he could not memorise the cues for click points, he cannot enter into the system. The system will treat him as an unauthorised user. This is the strength of PCCP. It is fully exploiting the memory and thus protecting your devices like PDA's from unauthorised access and other different kinds of attacks. Thus it termed as a knowledge based password authentication scheme in which the cues leads to the validating/invalidating session .Until the user selecting his last click points the system will not remind the user whether he given the right click or not even if he is a genuine user. This will help to protct the system from shoulder surfing attack and dictionary attack.

For login process the user have to enter the textual username and then he is entering to the PCCP system. System will allow only the valid username will enter into the PCCP system . There he starts accessing the images and starts clicking the clickpoints according to the order what he have received for password creation phase. Since the order is an essential property of PCCP the user have to ensure he is accessing the right images for password selection.

Here the scrambling is applied .While in the login session the user is receiving the scrambled images of the actual image what he selected for password creation.

Fig. 8 Scrambled Image for password selection in Login Phase

Here the cues are very important factor, because this will help the users to remember easily . The scrambling process is done by the algorithm shown above and the row and column coefficients are determined by the Key Based random Permutation (KBPR) explaned in section 4.3. There is a small comparison of alphanumeric password and graphical password is shown in the figure below with different parameters.

	Image size	Grid square size (pixels)	Alphabet size/ No. squares	Length/No. click points	Password space size
Alphanumeric	N/A	N/A	64	8	2.8×10^{14}
Alphanumeric	N/A	N/A	72	8	7.2×10^{14}
Alphanumeric	N/A	N/A	96	8	7.2×10^{15}
Graphical	451×331	20×20	373	5	7.2×10^{12}
Graphical	1024×752	20×20	1925	5	2.6×10^{16}
Graphical	1024×752	14×14	3928	5	9.3×10^{17}
Graphical (1/2 screen used)	1024×752	14×14	1964	5	2.9×10^{16}

Fig Comparison of textual and graphical password.

V. Security Analysis

In this section a discussion on how the proposed system may behave for password guessing attack and capture attack.

5.1 Password guessing attack

The most basic guessing attack against PCCP is a brute force attack, with expected success after exploring half of the password space (i.e., with a theoretical password space of 2^{43}, success after 2^{42} guesses). However, skewed password distributions could allow attackers to improve on this attack model. We now consider how these could be leveraged in guessing attacks. PassPoint system hotspots of small number of users can be collected and an attack dictionary can be formed, with the use of server-side information. Then this dictionary details can be used for the guessing of the click point in an image. But this does not work in PCCP with Image scrambling scheme, because the view port is entirely changing during the scrambling phase., and so it does not include the hot spot in almost all cases. If the attackers gain the access to hash table entry of the passwords, they cannot correctly predict the original password, which are kept in a different data base .which can be encrypted also using any of the strongest encryption scheme.

5.2 Capture attacks

Password capture attacks occur when attackers directly obtain passwords (or parts thereof) by intercepting user entered data, or by tricking users into revealing their passwords. For systems like PCCP, CCP, and PassPoints (and many other knowledge-based authentication schemes), capturing one login instance allows fraudulent access by a simple replay attack. All three security schemes (PP, CCP, PCCP) are vulnerable to shoulder surfing threat. Observing the approximate location of click points may reduce the number of guesses necessary to determine the user's password. User interface manipulations such as reducing the size of the mouse cursor or dimming the image may offer some protection, but have not been tested.

Malware is a major concern for text and graphical passwords, since key logger, mouse logger, and screen scraper malware could send captured data remotely or otherwise make it available to an attacker. For social engineering attacks against cued-recall graphical passwords, a frame of reference must be established between parties to convey the password in sufficient detail. One preliminary study suggests that password sharing through verbal description may be possible for PassPoints. For PCCP with image scrambling , more effort may be required to unscramble and get the actual picture during the login phase, each image and the exact location of each click-point. Graphical passwords may also potentially be shared by taking photos, capturing screen shots, or drawing, albeit requiring more effort than for text passwords.

Acknowledgements

This paper was developed by having [2] as the base idea and lab studies done the implementation of [1] are taken as proof for this paper. Sonia Chiasson and her friends, Members of IEEE, are honorably well acknowledged here for their fruit full research work

VII. Conclusion

The current graphical password techniques are still immature. Much more research and user studies are needed for graphical password techniques to achieve higher levels of maturity and usefulness. Two new image scrambling algorithms based on Fibonacci p-code are presented in this article: spatial domain and frequency domain algorithms (including JPEG domain).More Experimental results are needed on both color and grayscale images verify that this algorithms are lossless and show good performance in the presence of common image attacks. This algorithm introduces the technique to avoid the hotspot problem, reduces the shoulder attack. Also exploit the usability, memorability in graphical password scheme. Much more results are needed to show the effectiveness of the algorithm in 3D images.

References

[1] The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes,Joseph Bonneau University of Cambridge Cambridge, UK jcb82@cl.cam.ac.uk Cormac Herley Microsoft Research Redmond, WA, USA cormac@microsoft.com Paul C. van Oorschot Carleton University Ottawa, ON, Canada paulv@scs.carleton.ca Frank Stajanoy University of Cambridge Cambridge, UK frank.stajano@cl.cam.ac.uk

[2] Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism Sonia Chiasson, Member, IEEE, Elizabeth Stobert, Student Member, IEEE, Alain Forget, Robert Biddle, Member, IEEE, and Paul C. van Oorschot, Member, IEEE.IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 9, NO. 2, MARCH/APRIL 2012

[3] Persuasive Cued Click Points with Click Draw Based Graphical Password Scheme P. R. Devale Shrikala M. Deshmukh, Anil B. Pawar.

[4] Purely Automated Attacks on PassPoints-Style Graphical Passwords Paul C. van Oorschot, Amirali Salehi-Abari, and Julie Thorpe

IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 5, NO. 3, SEPTEMBER 2010

[5] S. Chiasson, P. van Oorschot, and R. Biddle, ?Graphical Password Authentication Using Cued Click Pointsm Pro c. European Symp. Research in Computer Security (ESORICS), pp. 359-374, Sept. 2007.

[6] The science of guessing: analyzing an anonymized corpus of 70 million passwords Joseph Bonneau Computer Laboratory University of Cambridge
jcb82@cl.cam.ac.uk. 2012 IEEE Symposium on Security and Privacy

[7] Dimitri Van De Ville, W.P., Rik Van de Walle, Ignace Lemahieu, Image Scrambling Without Bandwidth Expansion. IEEE Transactions on Cirsuits and Systems for Video Technology, 2004. 14

[8] AN IMAGE SCRAMBLING ALGORITHM USING PARAMETER BASED M-SEQUENCES YICONG ZHOU1, KAREN PANETTA1, FELLOW, IEEE, SOS AGAIAN2, SENIOR MEMBER, IEEE.

[9] Guosheng Gu, g.H. The application of chaos and DWT in image scrambling. in Proceeding of the Fifith Interational Conference on Machine Learning and Cybernetics. 2006. Dalian.

[10] S. Agaian, J.A., K. Egiazarian, P. Kuosmanen, Decompositional methods for stack filtering using Fibonacci pcodes. Signal Processing, 1995. 41: p. 101-110.

[11] David Z. Gevorkian, K.O.E., Sos S. Agaian, Parallel Algorithms and VLSI Architectures for Stack Filtering Using Fibonacci p-Codes. IEEE Transactions on Signal Processing, 1995. 43(1): p. 286-295.

[12] Mutual Image-Based Authentication Framework with JPEG2000 inWireless Environment G. Ginesu, D. D. Giusto, and T. Onali MCLab, Department of Electronic Engineering, University of Cagliari, Cagliari 09123, Italy