ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (7-14), Month: April - June 2015, Available at: www.researchpublish.com

Carp: An Image Based Security Using I-Pas

[1]Ashwini B Gawali, [2]Priyanka D Patil, [3]Manasi P Khade, [4]Sayli N Kokate, [5]Archana C Lomte

[1,2,3,4,5]Computer Department, JSPM's BSIOTR, Pune,India

Abstract: **Access to computer systems is most frequently based on the use of alphanumeric passwords. However, users have difficulty remembering a password that is long and random-appearing. Instead, create short, simple, and insecure passwords. Graphical passwords have been designed to try to make passwords more memorable and easier for people to use and more secure. Using a graphical password, users click on images rather than type alphanumeric characters. Designing a new and more secure graphical password system called Pass Points. In Pass Points system, its security characteristics, and the observed study we carried out comparing Pass Points to alphanumeric passwords. The results show that the graphical group took larger and made more errors in learning the password, but that the difference was mostly a result of just a few graphical participants who had difficulty learning to use graphical passwords. In the longitudinal trial the two groups performed similarly on memory of their password, but the graphical group took more time to input a password.**

Keywords: **Authentication, Graphical Password, Security, CaRP, Captcha, dictionary attack, Pass Points, PIN, password using attack, security primitive, Copyright, Click Points, tolerance.**

I. INTRODUCTION

Security practitioners and researchers have made stride in protecting systems and, correspondingly, individual users digital assets. Users interact with security technologies either passively or actively. For passive use understandability may be sufficient for users. For active use people need much more from their security solutions: ease of use, Memorability, efficiency, effectiveness and satisfaction. Today there is an increasing identification that security issues are also fundamentally human-computer interaction issues [5]. Authentication is the process of determining whether a user should be allowed access to a particular system or resource. It is a critical area of security research and practice. Alphanumeric passwords are used widely for authentication, but other methods are also available, including biometrics and smart cards [11]. Biometrics raise privacy concerns and smart cards usually need a PIN because cards can be lost. As a result, passwords are still leading and are expected to continue to remain so for some time [10] yet traditional alphanumeric passwords have drawbacks from a usability standpoint, and these usability problems tend to translate directly into security problems. Users who fail to choose and handle passwords securely open holes that attackers can exploit [9]. The "password problem," [3], arises because passwords are expected to conform 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 Copyright is held by the owner.

II. BACKGROUND ON PASSWORDS

A. Alphanumeric Passwords Problems:

The password problem arises largely from boundaries of humans' long-term memory (LTM). Once a password has been chosen and learned the user must be able to recall it to log in [5].But, people regularly forget their passwords. Decompose and interruption explains why people forget their passwords. Items in memory may compete with a password and prevent its accurate recall. If a password is not used frequently it will be even more at risk to forget. A further difficulty is that

users have many passwords for computers, networks, and web sites. The large number of passwords increases interference and is likely to lead to forgetting or confusing passwords. Users typically cope with the password problem by decreasing their memory load at the expense of security.

Users' tendency to handle alphanumeric passwords insecurely arises largely from long-term memory (LTM) limitations. Users have difficulty remembering complex, pseudo-random passwords over time. The Power Law of Forgetting [2] describes rapid forgetting soon after learning, followed by very slow decay over the long-term. Psychological theories have identified decay over time and interference with other information in LTM as original reasons for forgetting [5]. A user is likely to forget a password that is not used regularly, as the memory is not "refreshed" or "activated" sufficiently often. When users have multiple passwords, today practically a universal condition, interfering becomes a possibility. The user may either unwanted items the elements of the different passwords or remember the password but confuse which system it corresponds to.

1. Write down their passwords.
2. Have multiple passwords; they use one password for all systems or small variation of a single password.

A password should consist of a string of 8 or more random characters, including upper and lower case alphabetic characters, digits, and special characters [13]. A random password does not have meaningful content and must be memorized by rote, but rote learning is a weak way of remembering.

B. Graphical Passwords:

In this report of the concept an image would appear on the screen, and the user would click on a few chosen regions of it. If the correct regions were clicked in, the user would be authenticated. Memory of passwords and efficiency of their input are two key human factors criteria. Unforgettable has two aspects:

(1) How the user chooses and encodes the password and
(2) What task the user does when later retrieving the password.

Fig: Graphical Password Example

In a graphical password system, a user needs to choose memorable locations in an image. Choosing memorable locations depends on the nature of the image itself and the specific sequence of click locations. To support memorability, images should have semantically meaningful content because meaning for random things is poor [7]. Depending on the graphical password system, at recovery time users will be presented with either a recognition task or a cued recall task. In a graphical password system based on recognition, the user has to be able only to recognize previously seen images, making a binary choice of whether the image is known or not known. In password system use a mediator form of recollection between pure recall and recognition, cued recall.

III. ISSUES

Password space plays an important role in achieving high security. Large number of pictures will cause bigger password space in Graphical Password models than in text based ones [6]. Therefore, it makes the system almost more protected to attack like dictionary attacks but yet there is not known pre-existing dictionaries to search for graphical information. Two

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (7-14), Month: April - June 2015, Available at: www.researchpublish.com

mainstreams of modern Graphical Passwords are click-based approach and image selection-based approach. It is not easy to plan automated attacks in Graphical Password; to detail this issue one can take an example where human beings are able to identify a person's face faster than a computer [9]. Studies have shown that because human can recall picture passwords easier and faster than text ones, therefore graphical authentication system are more usable than textual. Main disadvantage of image recognition passwords is the limited number of images shown on the screen each time, for instance in Pass [10].

1. **Security** we have briefly examined the security issues with graphical passwords.
2. **Usability:** One of the main arguments for graphical passwords is that pictures are easier to remember than text strings. Beginning of user studies are accessible in some research papers seem to support. But, present user Studies are still very restricted, connecting only a small number of users.
3. **Reliability:** The major design issue for recall-based methods is the reliability and accuracy of user input detection. In this category of process, the inaccuracy tolerances have to be set carefully – overly high tolerances may lead to many false positives while overly low tolerances may lead to many false negatives.

IV. SYSTEM DESIGN

The system designed consists of three modules such as user registration module, image selection module and system login module:

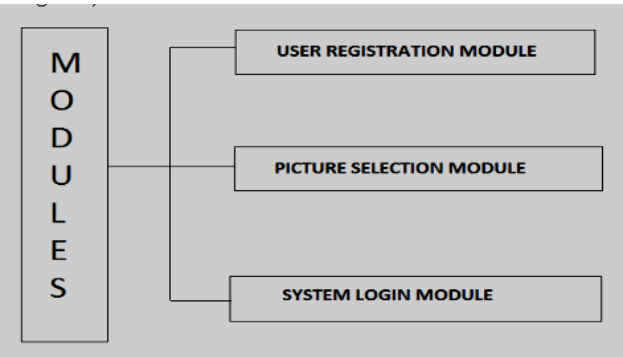

Fig: System Modules

In user registration module user enter the user name in user name field and also suitable tolerance value. When user entered the all user details in registration phase, these user registration data stored in data base and used during login phase for verification.

In image selection phase there are two ways for selecting image password authentication.

1. User defines image: Pictures are selected by the user from the hard disk or any other image supported devices.
2. System defines pictures: pictures are selected by the user from the database of the password system.

In image selection phase user select any image as passwords and consist 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. During password creation, most of the image is dim except for a small view port area that is randomly positioned on the image. Users must select a click-point within the view port.

During system login, the images are displayed normally, without shading or the viewport, and repeat the sequence of clicks in the correct order, within a system-defined tolerance square of the original click-points.

V. DESIGN OF PASS POINTS

Developed a graphical password scheme based on original idea that overcomes its limitations of needing simple, artificial images, predefined regions, and consequently many clicks in passwords. The scheme:

(1) Allows any image to be used and
(2) Does not need artificial predefined click regions with well-marked boundaries – a password can be any randomly chosen sequence of points in the image [11].

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (7-14), Month: April - June 2015, Available at: www.researchpublish.com

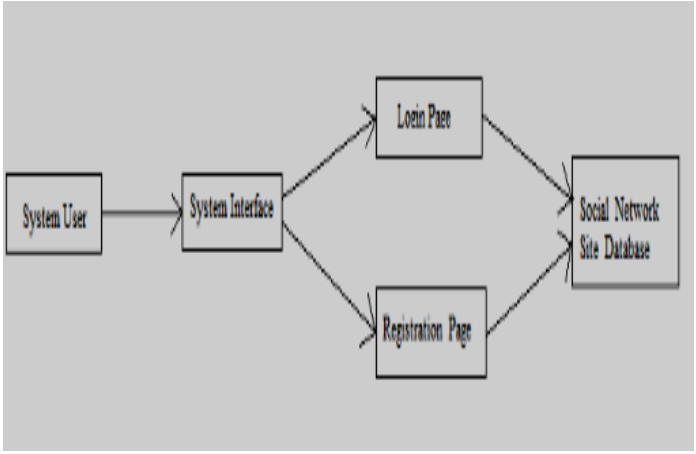

Fig: Flow of PassPoint System

Complex images can have hundreds of remarkable points; so for example, with 5 or 6 click points one can make more passwords than 8-character Unix-style passwords. The user has to click close to the chosen click points, within some set acceptance distance, e.g., within .25 to .50 cm from the users click point [12]. The tolerance is required because the user's click point literally is a single pixel, which is too precise for a user to click on successfully.

Fig: User choice in Pass Points

The tolerance, which is changeable in the system, gives a margin of error around the click point, in which the user's click is accepted as correct. The password space is the set of all passwords that are possible for a given password scheme and for a given setting of parameters. For example, for alphanumeric passwords of length 8 over a 64character alphabet, the number of possible passwords is 648= 2.8 x1014. In Pass Points if the image size is 1024 x752 (i.e., roughly the full screen), with a tolerance around the click point of 20x20 pixels, and with passwords consisting of 5 clicks, the password space will have size 2.6 x1016.

During password creation, the first image can be selected by the user from the system. We will find out the X and Y co-ordinates of the click-point. For each click-point in a subsequent login attempt, this number is retrieved from the database and used to determine whether the click-point falls within the tolerance (correct region or correct X and Y coordinates) of the original point.

VI. ALGORITHM STEPS

The Graphical Password follows two process which include Server side Registration for validating the user to access the online banking account and Client side Login Process to perform the remote access to the bank account which include verification and image password authentication process.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (7-14), Month: April - June 2015, Available at: www.researchpublish.com

A. Registration Process:

1) Enter Username
2) Select Image for password

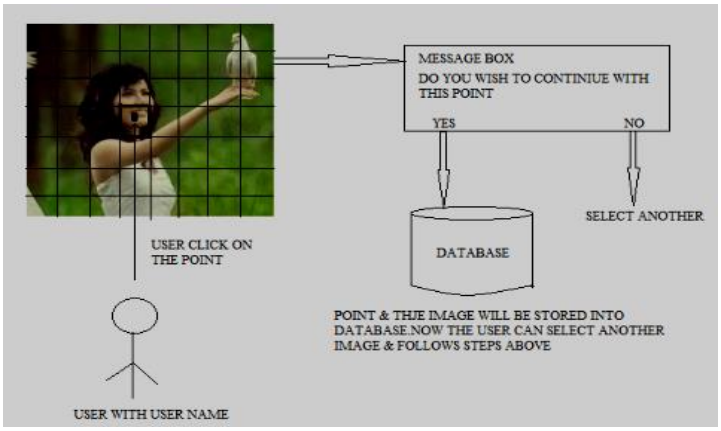

Fig: Image Password Selection

3) Click Point's as a password

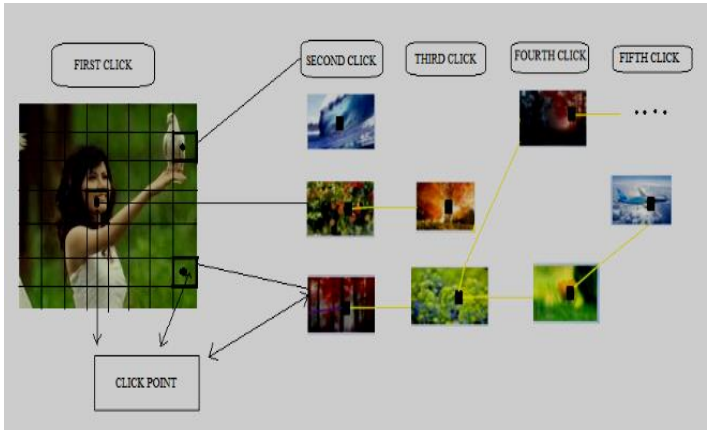

Fig: Image Click point's

4) Store username and all the point's of image into Database.

B. Login Process:

1) Enter username
2) Username verification process

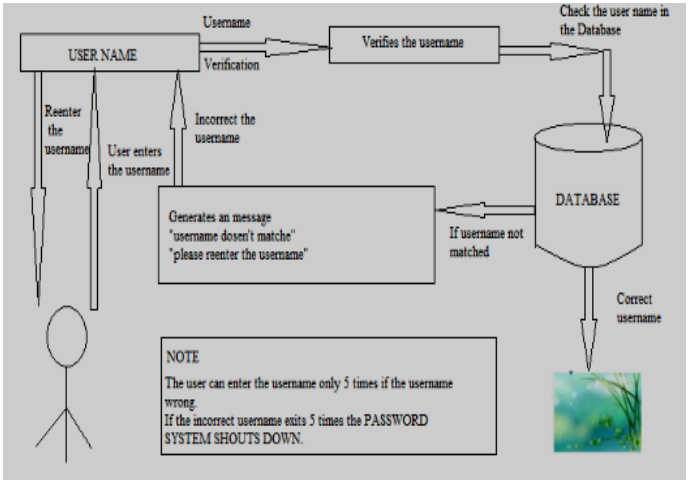

Fig: Username verification

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (7-14), Month: April - June 2015, Available at: www.researchpublish.com

3) Click point's for password

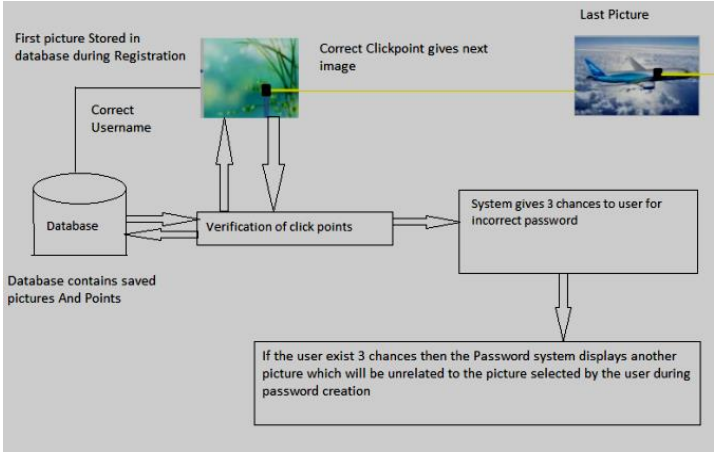

Fig: Click point's

4) Check click points into Database
5) If match then system allow to open the application.

VII. RESULT

The recorded results about the three phases of the study: password creation, learning, and retention. Created invalid passwords and had to try again. There were no password creation errors. The errors were not serious. An example of an error is that the participant entered the wrong number of points (e.g., 4 rather than 5), apparently out of inattention to the on-screen instructions. There were no significant differences in the number of attempts or the time to create a valid password.

Table: Tolerance around click points

Tolerance	Size in cm^2	Example
10 x 10	.28 cm^2	
14 x 14	.39 cm^2	

Table: Compare text and PassPoint

	Click Text	Animal Grid	Graphical Password	CaRP: Graphical Password
	vs.Text		vs.Passpoint	
Much Easier(%)	2.4	7.6	7.6	16.0
Easier(%)	45.0	48.0	26.0	45.0
Same(%)	30.0	25.0	20.0	16.0
More Difficult(%)	15.0	15.0	45.0	20.0
Much more difficult(%)	2.5	4.0	4.0	0

VIII. CONCLUSION

CaRP introduce a new family of graphical passwords, which adopt a new advance to counter online guessing attacks: a new CaRP image, which is also a Captcha challenge. A password of CaRP can be found only probabilistically by repeated online guessing attacks including brute-force attacks, a desired security property that other graphical password schemes lack. Hotspots in CaRP images can no longer be broken to increase automatic online guessing attacks, a natural openness in many graphical password systems.

An important usability and security goal in authentication systems is to help user's select better passwords and thus increase the effective password space. It believes that users can be persuaded to select stronger passwords through better user border design. Human brains can process graphical images easily. Thus, Graphical Password schemes provide a way of making more human friendly passwords while increasing the level of security compared to other types of passwords. For graphical password schemes, security and usability represent opposite ends of a range: increasing security imply decreasing usability and vice versa. Therefore, a tradeoff is required based on user requirements. To meet user requirements we should contacts the two aspects with the special target environment when a new scheme is proposed or for selecting the suitable scheme. There is a high possibility that in the case of selecting simpler images and using them as current pictures in our system for the password part, the memorability increases and users can memorize and recall betters

REFERENCES

[1] S. Chiasson, R. Biddle, and P. van Oorschot, "A Second Look at the Usability of Click-Based Graphical Passwords," Proc. ACM Symp. Usable Privacy and Security (SOUPS), July 2007.

[2] 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.

[3] "Captcha as Graphical Passwords—A New Security Primitive Based on Hard AI Problems", Bin B. Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, and Ning Xu, VOL. 9, NO. 6, JUNE 2014.

[4] "IPAS: Implicit Password Authentication System", Sadiq Almuairfi, Parakash Veeraraghavan and Naveen Chilamkurti.

[5] A. Feldmeier and P. Karn. "UNIX Password Security-Ten Years Later". In Crypto'89, August 1989.

[6] R. Morris and K. Thompson. "Password Security: A Case History". Communications of the ACM, 22(11):594-597, 1979.

[7] A. Florencio and C. Herley. "A large-scale study of WWW password habits". In 16th ACM International World Wide Web Conference (WWW), May 2007.

[8] S. Chakrabarti and M. Singhal. Password-based authentication: Preventing dictionary attacks. Computer, IEEE Computer Society, 40(6):68{74, June 2007.

[9] S. Chiasson, R. Biddle, and P. van Oorschot. A second look at the usability of click-based graphical passwords. In 3rd Symposium on Usable Privacy and Security (SOUPS), July 2007.

[10] L. Faulkner. Beyond thieve-user assumption: Benets of increased sample sizes in usability testing. Behavior Research Methods, Instruments, & Computers, 35(3):379{383, 2003.

[11] A. Florencio and C. Herley. A large-scale study of WWW password habits. In 16th ACM International World Wide Web Conference (WWW), May 2007.

[12] B.Fogg.Persuasive Technologies: Using Computers to Change What We Think and Do. Morgan Kaufmann Publishers, San Francisco, CA, 2003.

[13] Forget and R. Biddle. Memorability of Persuasive Passwords (poster). InACM SIGCHI Student Research Competition, April 2008.

[14] Forget, S. Chiasson, R. Biddle, and P. van Oorschot. Persuasion as education for computer security. In AACE E-Learn Conference, October 2007.

[15] Forget, S. Chiasson, P. van Oorschot, and R. Biddle. Improving text pass- words through persuasion. In 4th Symposium on Usable Privacy and Security.

[16] D. Florencio and C. Herley. "A large-scale study of WWW password habits". In 16th ACM International World Wide Web Conference (WWW), May 2007.

[17] A. Adams, M. A. Sasse, and P. Lunt. "Making passwordssecure and usable". In HCI 97: Proceedings of HCI on People and Computers, pp.1-19, London, UK, 1997.

[18] H. Tao and C. Adams, "Pass-Go: A proposal to improve the usability of graphical passwords," Int. J. Netw. Security, vol. 7, no. 2, pp. 273–292, 2008.

[19] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "Pass Points: Design and longitudinal evaluation of a graphical password system," Int. J. HCI, vol. 63, pp. 102–127, Jul. 2005.