iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** III **Month of publication:** March 2016

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 4 Issue III, March 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Exploring Usability Effects of Increasing Security in Click-Based Graphical Password

Rupali Navalkar[1], Prof.P.L.Ramteke[2]
[1]ME First Yr.(CSE), [2]Associate Professor ME(CSE), M.Phil(CS),PhD(Pursuing)
H.V.P.M's COET, Amravati

Abstract--Graphical passwords have been proposed to address known problems with traditional text passwords. For example, memorable user-chosen text passwords are predictable, but random system assigned passwords are difficult to remember. We explore the usability effects of modifying system parameters to increase the security of a click-based graphical password system. Generally, usability tests for graphical passwords have used configurations resulting in password spaces smaller than that of common text passwords. In this paper focuses on the integrated evaluation of the Persuasive Cued Click Points graphical password authentication system, including usability and security. An important usability goal for authentication systems is to support users in selecting better passwords, thus increasing security by expanding the effective password space. We chose to study Persuasive Cued Click-Points (PCCP),a click-based graphical password system in which users select click-points on more than one image. PCCP has been shown to have good usability, while avoiding hotspots that have been shown to affect the security of other click-based graphical password systems .
Keywords--Graphical password, authentication, persuasive technology, usable security.

I. INTRODUCTION

The problems of knowledge-based authentication, typically text-based passwords, are well known. Users often create memorable passwords that are easy for attackers to guess, but strong system-assigned passwords are difficult for users to remember .Users also tend to reuse passwords across many accounts and this increases the potential impact if one account is compromised. Alternatives such as graphical passwords use images instead of text for authentication. We chose to study Persuasive Cued Click-Points (PCCP), a click-based graphical password system in which users select click-points on more than one image . PCCP has been shown to have good usability, while avoiding hotspots that have been shown to affect the security of other click-based graphical password systems. To address this, we explored increasing security in PCCP, conducting a study modifying two parameters: the size of the images presented, and the number of click-points in each password. The study included 82 participants who completed two sessions scheduled two weeks apart. Our results show that both manipulations affect the
usability of the system and memorability of the passwords. Moreover, when adjusted to provide the same level of security, both manipulations have similar effects on usability and memorability. This suggests that when increasing security, constraints of devices and user preferences might be accommodated. For example, when designing for mobile devices, smaller images and more click-points might be used due tosmaller screen sizes.

II. BACKGROUND

Graphical password systems are a type of knowledge-based authentication that rely on the human ability to better recognize and remember images than textual or verbal information. They fall into three main categories:

A. Recall

(Also known as drawmetric) Users recall and reproduce a secret drawing on a blank canvas. Example systems include Draw-A-Secret and Pass-Go.

B. Recognition

Users recognize and identify images from a previously memorized portfolio from a larger set of decoy images. Example systems include PassFaces.

C. Cued-Recall

(also known as locimetric) Users iden-tify and target previously selected locations within one or more images. The images act as

©IJRASET 2013: All Rights are Reserved

Volume 4 Issue III, March 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

memory cues to help recall these locations. Example systems include PassPoints and Persuasive Cued Click-Points.

Click-Points:- one click-point on different images shown in sequence.Cued:- Next image displayed is based on the location of the previously entered click-point. Persuasive:-encouraging users to select more random point, and hence more difficult to guess, click-points. Other approaches to authentication are token-based systems and biometrics. While applicable in some cases, these have potential drawbacks, such as risks of loss, and privacy implications. In cued-recall click-based graphical passwords. passwords consist of clicking on specific locations on one or more images. To log in, the user must click on these previously selected locations. The user is not expected to repeat exact pixel selections.

In this paper, we focus on Persuasive Cued Click-Points (PCCP) . In PCCP, a user is presented with a number of images in sequence, and must choose one click-point per image. The first image is assigned by the system, but each subsequent image is determined by the user's previous click. PCCP is stronger against password-guessing attacks than other click-based password systems and also maintains login

times and success rates comparable to text passwords.However, to be seriously considered as a replacement for text passwords, PCCP needs to be at least as secure as standard text passwords.

Fig.1 5 click points on single image.

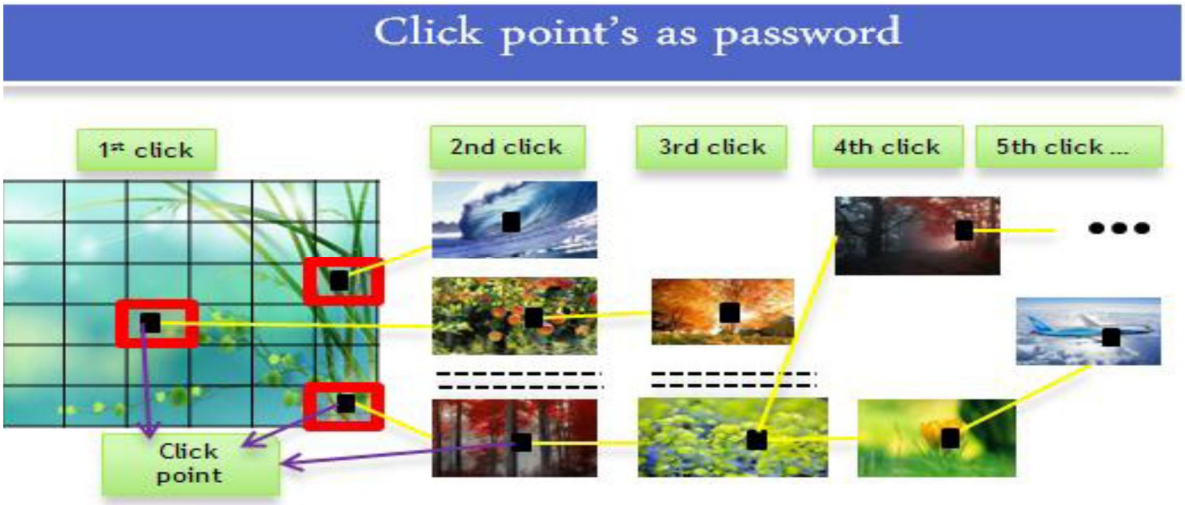


Fig. 2 with CCP, users select one click-point per image. The next image displayed is determined by the current click-point.

III. METHODOLOGY

A. Persuasive Technology

Persuasive Technology was first articulated by Fogg as using technology to motivate and influence people to behave in a desired manner. Persuasive Technology is the emerging field of "interactive computing systems designed to change people's attitudes and behaviours". An authentication system which applies Persuasive Technology 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

©IJRASET 2013: All Rights are Reserved

resulting passwords must be memorable. As detailed in the next section, 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 (not comprised entirely of known hotspots or following a predictable pattern). As a result, the system also has the advantage of minimizing the formation of hotspots across users since click points are more randomly distributed.

B. Persuasive Cued Click Points

Previous models have shown that hotspots are a problem in click-based graphical passwords, leading to a reduced effective password space that facilitates more successful dictionary attacks. We investigated whether password choice could be influenced by persuading users to select more random click-points while still maintaining usability. Our goal was to encourage compliance by making the less secure task (i.e., choosing poor or weak passwords) more time-consuming and awkward. In effect, behaving securely became the path-of-least-resistance. Using CCP as a base system, 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.

Fig. 3 PCCP Create Password interface. The viewport highlights part of the image

The theoretical password space for a password system is the total number of. unique passwords that could be generated according to the system specifications.

IV. SYSTEM MODULE

The system designed consist of three modules such as user registration module, picture selection module and system login module. Shown in (fig 4.)

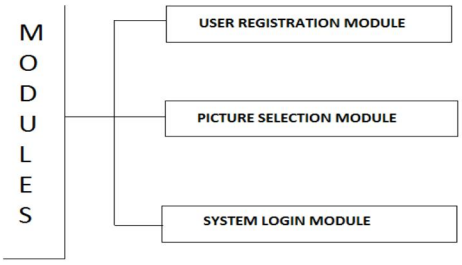


Fig. 4 System design modules.

In user registration module user enter the user name in user name field and also suitable tolerance value (tolerance value is use to compare registration profile vector with login profile vector). When user entered the all registration phase, these user registration data stored in data base and used during login phase for verification. In picture selection phase. there are two ways for selecting picture password authentication.

User defines pictures: Pictures are selected by the user from the hard disk or any other image supported devices.

System defines pictures: pictures are selected by the user from the database of the password.

©IJRASET 2013: All Rights are Reserved

Volume 4 Issue III, March 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

V. USABILITY

Large images and more click-point increases the theoretical password space but decreases usability.

Achieve better usability & memorability for approximately equivalent password space.

Hypothesis:
Increasing the number of click-points will decrease usability.
Increasing the size of the image will decrease usability.
For conditions with approximately comparable theoretical password spaces, the condition with the larger image size will have better usability.

A. Usability Results

Success Rates

: Success rates on first attempt, within 3 attempts and multiple attempts (eventual success) per phase.

	First Attempt			Within 3 Attempts			Eventual Success		
	Session 1		Session 2	Session 1		Session 2	Session 1		Session 2
Condition	Login	Recall-1	Recall-2	Login	Recall-1	Recall-2	Login	Recall-1	Recall-2
S5	91%	87%	25%	100%	95%	37%	100%	99%	42%
S6	83%	89%	28%	99%	93%	40%	100%	93%	48%
S7	92%	85%	18%	99%	91%	32%	100%	96%	42%
L5	91%	82%	18%	100%	94%	33%	100%	94%	45%
L6	94%	93%	18%	98%	97%	27%	100%	100%	36%
L7	92%	82%	5%	100%	96%	14%	100%	100%	36%

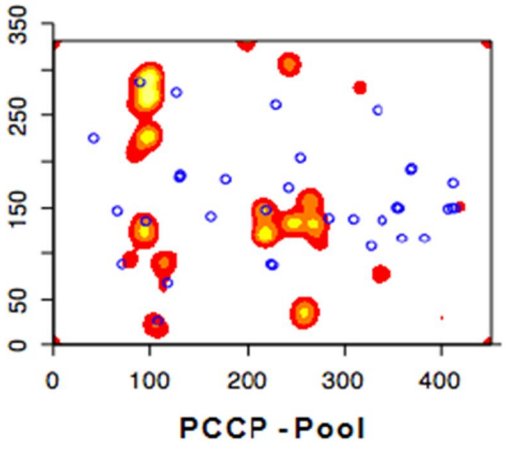
Table 4: Regression tests for success rates for each phase, only the most relevant measure is reported.

	First Attempt		Within 3 Attempts
	Session 1		Session 2
	Login	Recall-1	Recall-2
Number of Click-points	$p = 0.906$	$p = 0.762$	$\mathbf{p = 0.043}$
Image Size	$p = 0.914$	$p = 0.643$	$\mathbf{p = 0.017}$

Lower value of p in session-2 supports both the Hypothesis 1 & 2.

B. Analysis of Password Distributions

1) Click-Point Clustering: Passwords should be as random as possible while still maintaining memorability.
Different users tend to select similar click-points creating what are known as *hotspots.*



©IJRASET 2013: All Rights are Reserved

VI. ADVANTAGES

Hard disk locking.
System log in and log out process.
Folder Locking.

VII. CONCLUSION

In this paper, we explored the issue of how increasing the security of a click-based graphical password scheme would affect usability and memorability. We tested PCCP with different parameters in order to evaluate its usability when the theoretical password space is increased. We found that increasing the number of click-points or increasing the image size both have usability and memorability impacts.

We explored the effects of number of click-points and image size on user behaviour resulting in clustering of click-points. We found no evidence that the number of click-points had an effect, but it appeared that larger images led to less clustering. An important usability and security goal in authentication systems is to help user˝s select better passwords and thus increase the effective password space. We believe that users can be persuaded to select stronger passwords through better user interface design. As an example, we designed Persuasive Cued Click-Points (PCCP) and conducted an usability study to evaluate its effectiveness. We obtained favorable results both for usability and security. PCCP encourages and guides users in selecting more random click-based graphical passwords.

VIII. ACKNOWLEDGEMENT

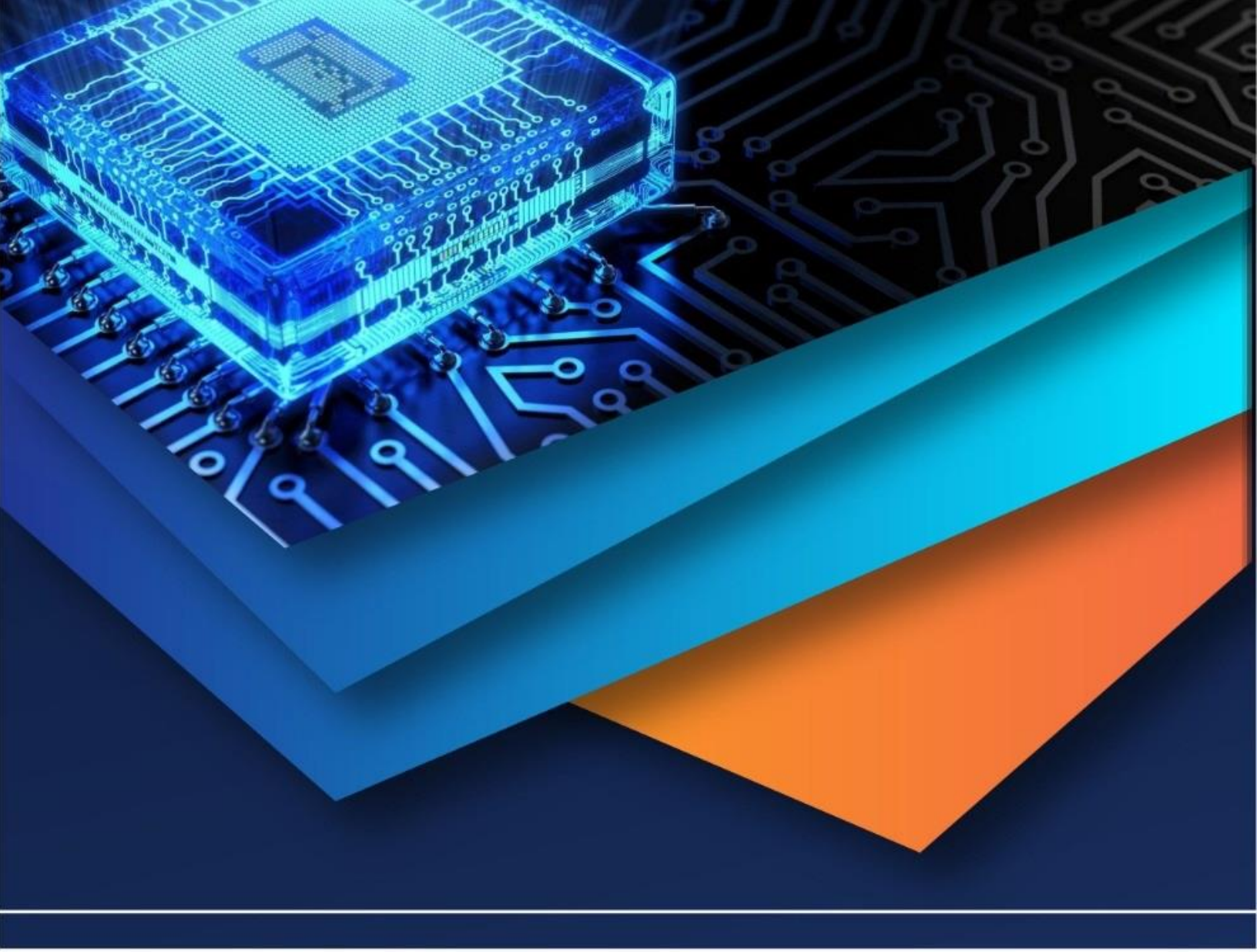
First of all we would especially like to express sincere gratitude to our parents. It gives us great pleasure and satisfaction in presenting the paper on “EXPLORING USABILITY EFFECTS OF INCREASING SECURITY IN CLICK-BASED GRAPHICAL PASSWORD”

Before we get into the depth of the things, we show our sincere gratitude towards respected teachers, guide, colleagues and all who have directly or indirectly helped us in the completion of this paper successfully

REFERENCES

[1] S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot. Inuencing users towards better passwords: Persuasive Cued Click-Points.
[2] S. Chiasson, R. Biddle, and P. van Oorschot, “A Second Look at the Usability of Click-Based Graphical Passwords,” Proc. ACM Symp. Usable Privacyand Security (SOUPS), July 2007.
[3] 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.
[4] A. Forget, E. Stobert, P. van Oorschot, and R. Bddle, “Multiple Password Interference in Text and Click-Based Graphical Passwords,”

©IJRASET 2013: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)