IJRRECS/October 2013/Volume-1/Issue-6/1617-1622 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

DESIGN, IMPLEMENTATION AND EVALUATION OF KNOW LEDGE BASED AUTHENTICATION MECHANISM USING PERSUASIVE CUED CLICK POINTS

M.Adinarayana[1], V.Krishna Reddy[2], Ch.Srinivasulu[3]

[1]Dept of IT, J.B. Institute of Engineering & Technology, Hyderabad, A.P, India
[2]Associate Professor, Dept of IT, J.B. Institute of Engineering & Technology, Hyderabad, A.P, India
[3]Associate Professor, Dept of IT, J.B. Institute of Engineering & Technology, Hyderabad, A.P, India

ABSTRACT:

For the users strong system allocated passwords are tricky to memorize and hence a system of password authentication have to promote strong passwords at the same time preserve the memo ability. The users are persuaded to choose protected passwords, permitting the choice of the user although manipulating them towards stronger passwords. Persuasive Cued Click-Points is effectual at dropping hotspots and reject patterns that are formed by the click points within the password at the same time still preserving usability. Click-based graphical passwords are the systems of Graphical password that are a kind of knowledge-based verification that endeavours to influence the capability of human to be familiar with and consider images than verbal or textual information. Cued Click-Points which is a Precursor to Persuasive Cued Click-Points was intended to decrease patterns and to decrease the convenience of hotspots for attackers and make usage of single click-point on images of five different revealed in sequence to a certain extent than five click-points on one image. Persuasive Technology was used to encourage and manipulate people to perform in a desired manner. A validation system that applies the technology of Persuasive should direct and give confidence to the users to choose stronger passwords, while do not compel system-generated passwords. By adding a characteristic of persuasive to Cued Click-Points, the users were encouraged by the Persuasive Cued Click-Points to choose less expected passwords, and to build it more complicated to choose passwords where all the five click points are hotspots.

Keywords: Password authentication, Persuasive Cued Click-Points, Graphical password, Persuasive Technology.

1. INTRODUCTION:

Impressive passwords that are simple were often created by the users intended for attackers to estimate. For the users strong system allocated passwords are tricky to memorize and hence a system of password authentication have to promote strong passwords at the same time preserve the memorability [8]. The users are persuaded to choose protected passwords, permitting the choice of the user although manipulating them towards stronger passwords. Persuasive Cued Click-Points is effectual at dropping hotspots and reject patterns that are formed by the click points within the password at the same time still preserving usability [1]. The most accepted user verification method is the text password, however has the problems of protection and usability problems. Click-based graphical passwords: The systems of Graphical password shown in fig1 are a kind of knowledge-based verification that endeavours to influence the capability of human to be familiar with and consider images than verbal or textual information [5] [11]. A complete review of graphical passwords is obtainable in cued-recall click-based graphical passwords in which the user recognize and target earlier selected sites inside one or additional images. The passwords comprises of a sequence of five click-points on the image given in PassPoints [6]. Pixels in the image can be selected as click-points by the user for their password. Within a region of system-defined tolerance of the original click-points, the sequence of clicks in the accurate order was repeated to log in [15]. Even though PassPoints is comparatively exploitable, safety limitation put together passwords easier for attackers to forecast. Persuasive Technology was used to encourage and manipulate people to perform in a desired manner. Persuasive Cued Click-Points has comparable rates of the success to the other schemes of authentication assessed Cued Click-Points which is a Precursor to Persuasive Cued Click-Points was intended to decrease patterns and to decrease the convenience of hotspots for attackers and make usage of single click-point on images of five different revealed in sequence to a certain extent than five click-points on one

image. [3] [7]. Users decide on their images merely to the amount that their click-point concludes the subsequent image. The areas of the image that have superior probability of being selected by users as click-points of the password are Hotspot [14].

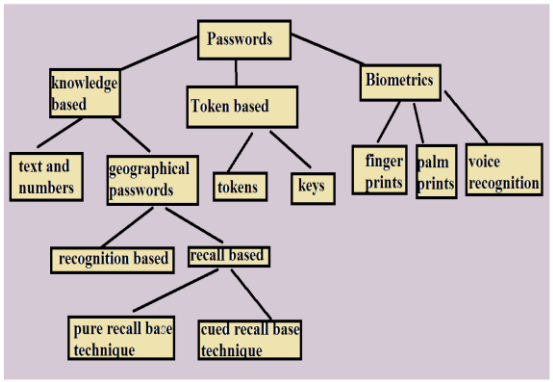

Fig1: Taxonomy of Password Authentication methods

All the way through harvesting sample passwords, attackers who gain knowledge of these hotspots can construct attack dictionary and more effectively estimate the Pass Points passwords.

2. METHODOLOGY:

Persuasive Technology was used to encourage and manipulate people to perform in a desired manner. A validation system that applies the technology of Persuasive should direct and give confidence to the users to choose stronger passwords, while do not compel system-generated passwords [4]. The users should not overlook the elements of persuasive and the passwords resulting have to be unforgettable. By adding a characteristic of persuasive to Cued Click-Points, the users were encouraged by the Persuasive Cued Click-Points to choose less expected passwords, and to build it more complicated to choose passwords where all the five click points are hotspots. Specially, when a password was created by the users, the images are to some extent shaded excluding for a viewport that is situated haphazardly, to a certain extent than specially to circumvent identified hotspots, in view of the fact that such information may possibly permit attackers to get better guesses and may possibly direct to the development of new hotspots [9] [13]. To put forward a range of distinct points the size of the viewport's is projected however still cover merely an adequately little fraction of all probable points. A click-point within this highlighted viewport is to be selected by the user and cannot click exterior of the viewport, except they decide to press the button of shuffle to haphazardly change the position of the viewport [2] [10]. Although the users may possibly shuffle as frequently as required, this considerably slows the procedure of password construction. The shuffle button and the

viewport come into view only during the creation of the password. The images are displayed in general, during the entry of later password devoid of the viewport, and users may possibly click wherever on the images. The total number of distinctive passwords that may possibly be generated according to the specifications of the system is the theoretical password space for the system of password [12]. Persuasive Cued Click-Points is specially intended to considerably decrease such skews. Preferably, an outsized theoretical password space worse the probability that any meticulous guess is accurate for a specified password.

3. RESULTS:

The success rates of the login and the recall rates were compared for the web studies of Persuasive Cued Click-Points and Text Web, no statistical differentiation were set up and it is in particular remarkable for the reason that examination of the text passwords made known that for the most part of participants has re-used the passwords across accounts, while passwords of Persuasive Cued Click-Points were dissimilar by design. The passwords of the PCCP present added security in view of the fact that reuse across systems is not probable; however this did not have an effect on the rates of success. Persuasive Cued Click-Points has comparable rates of the success to the other schemes of authentication assessed. The password entry for Persuasive Cued Click-Points takes a comparable time to the other systems in the early lab sessions, although the results point towards longer times of recall for Persuasive Cued Click-Points when passwords were recalled further than the early session.

4. CONCLUSION:

Persuasive Cued Click-Points is effectual at dropping hotspots and reject patterns that are formed by the click points within the password at the same time still preserving usability. Cued Click-Points which is a Precursor to Persuasive Cued Click-Points was intended to decrease patterns and to decrease the convenience of hotspots for attackers and make usage of single click-point on images of five different revealed in sequence to a certain extent than five click-points on one image. The success rates of the login and the recall rates were compared for the web studies of Persuasive Cued Click-Points and Text Web, no statistical differentiation were set up and it is in

particular remarkable for the reason that examination of the text passwords made known that for the most part of participants has re-used the passwords across accounts, while passwords of Persuasive Cued Click-Points were dissimilar by design. Persuasive Cued Click-Points has comparable rates of the success to the other schemes of authentication assessed.

REFERENCES:

[1] S. Chiasson, J. Srinivasan, R. Biddle, and P. C. van Oorschot, "Centered discretization with application to graphical passwords," in USENIX Usability, Psychology, and Security (UPSEC), April 2008.

[2] S.Wiedenbeck, J.Waters, J. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system," International Journal of Human-Computer Studies, vol. 63, no. 1-2, pp. 102–127, 2005.

[3] S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot, "User interface design affects security: Patterns in click-based graphical passwords," International Journal of Information Security, Springer, vol. 8, no. 6, pp. 387–398, 2009.

[4] J. Yan, A. Blackwell, R. Anderson, and A. Grant, "The memorability and security of passwords," in Security and Usability: Designing Secure Systems That People Can Use, L. Cranor and S. Garfinkel, Eds. O'Reilly Media, 2005, ch. 7, pp. 129–142.

[5] S. Chiasson, C. Deschamps, M. Hlywa, G. Chan, E. Stobert, and R. Biddle, "MVP: A web-based framework for user studies in authentication (poster)," in Symposium on Usable Privacy and Security (SOUPS), 2010.

[6] S. Chiasson, P. van Oorschot, and R. Biddle, "Graphical password authentication using Cued Click Points," in European Symposium On Research In Computer Security (ESORICS), LNCS 4734, September 2007, pp. 359–374.

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

[8] F. Tari, A. Ozok, and S. Holden, "A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords," in 2nd ACM Symposium on Usable Privacy and Security (SOUPS), 2006.

[9] S. Chiasson, A. Forget, R. Biddle, and P. van Oorschot, "Influencing users towards better passwords: Persuasive Cued Click-Points," in Human Computer Interaction (HCI), The British Computer Society, September 2008.

[10] A. De Angeli, L. Coventry, G. Johnson, and K. Renaud, "Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems," International Journal of Human-Computer Studies, vol. 63, no. 1-2, pp. 128–152, 2005.

[11] E. Stobert, A. Forget, S. Chiasson, P. van Oorschot, and R. Biddle, "Exploring usability effects of increasing security in click-based graphical

passwords," in Annual Computer Security Applications Conference (ACSAC), 2010.

[12] S.Wiedenbeck, J.Waters, J. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Effects of tolerance and image choice," in 1st Symposium on Usable Privacy and Security (SOUPS), July 2005.

[13] M. Weir, S. Aggarwal, M. Collins, and H. Stern, "Testing metrics for password creation policies by attacking large sets of revealed passwords," in Computer and Communications Security (CCS), 2010.

[14] A. Forget, S. Chiasson, and R. Biddle, "Shoulder-surfing resistance with eye-gaze entry in click-based graphical passwords." in ACM SIGCHI Conference on Human Factors in Computing Systems: Note (CHI), 2010.

[15] A. Forget, S. Chiasson, P. van Oorschot, and R. Biddle, "Improving text passwords through persuasion," in 4th Symposium on Usable Privacy and Security (SOUPS), July 2008.