ISSN (Online): 2319-8753
ISSN(Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization *Volume 4, Special Issue 5, April 2015*

International Conference On Emerging Trends in Engineering and Technology (ICETET'15)

On 13th & 14th March 2015

Organized by

Pandian Saraswathi Yadav Engineering College, Arasanoor, Sivagangai, Tamilnadu, India

Modeling Anti Phishing System for E-Banking Based on Graphical Password Authentication Scheme

P.Mahadevi[1], R.Sukumar[2]

PG Scholar, Department of CSE, Sethu Institute of Technology, Tamilnadu, India[1]

Professor, Department of CSE, Sethu Institute of Technology, Tamilnadu, India[2]

ABSTRACT:Security has been an affair from the birth of computer systems and experts accept accompanying aegis issues with usability. Phishing is the attack that becomes popular recently. It is an attempt to obtain confidential and private information of individuals or companies for monetary or other gains. Phishing attacks have been recorded in the history in banking and e-commerce domains. Secured systems accept to be accessible to advance advised security. In this work graphical password authentication with sound signature is used. Graphical Passwords, while usable, does not assume to accept the aegis all-important to alter argument passwords. A graphical password system with a supportive sound signature to increase the remembrance of the password is discussed in this paper. In proposed work a click-based graphical password scheme called Cued Click Points (CCP) is presented. In this work a password consists of sequence of some images in which user can select one click-point per image. In addition to the work user is asked to select a sound signature corresponding to each click point. This sound signature will be used to help the user in recalling the click point on an image.

KEYWORDS:cued click points, Graphical password authentication, sound signature, Phishing.

I. INTRODUCTION

Online transactions are nowadays become very common and there are various attacks present behind this. In these types of various attacks, phishing is identified as a major security threat and new innovative ideas are arising with this in each second so preventive mechanism should also be so effective.

Thus the security in these cases be very high and should not be easily tractable with implementation easiness. Today, most applications are only as secure as their underlying system. Since the design and technology of middleware has improved steadily, their detection is a difficult problem.As a result, it is nearly impossible to be sure whether a computer that is connected to the internet can be considered trustworthy and secure or not. Phishing scams are also becoming a problem for online banking and e-commerce users.

A graphical password system with a supportive sound signature to increase the remembrance of the password is discussed. The image-handling part allows users to settle on pictures or to introduce their own the pictures

The pictures the photographs area unit keeps beside a set of images provided by the system. For this password system to figure well, it's vital that the photographs be fairly tangled, with many attention-grabbing details that might be chosen as click regions (e.g., geographic maps, bailiwick pictures, cityscapes, sure landscapes, and renaissance paintings). The password choice part permits the user to pick a brand new password. Assumptive the user has already logged in (by victimization either a graphical or a traditional password), the user enters the "password" command. The system then produces the user for a user name and current password. If the system accepts the present password, it lets the user specify a brand new image (or keep the present image), and set the protection parameter r for sturdy discrimination (or keep a default value).

The graphical password schemes we have a tendency to think of during this study have the property that the area of passwords are often thoroughly searched briefly order if associate degree offline search is feasible. So, any use of those schemes needs that guesses be mediate and confirmed by a sure on-line system. In such situations, we have a tendency

ISSN (Online): 2319-8753
ISSN(Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 4, Special Issue 5, April 2015

International Conference On Emerging Trends in Engineering and Technology (ICETET'15)

On 13th & 14th March 2015

Organized by

Pandian Saraswathi Yadav Engineering College, Arasanoor, Sivagangai, Tamilnadu, India

to believe that our study is that the 1st to quantify factors relevant to the protection of user-chosen graphical password advises against the employment of a Pass faces TM-like system that allows user selection of the password, while not some means that to mitigate the dramatic effects of attraction and race that our study quantifies. As already incontestible, for sure populations of users, no obligatory limit on the quantity of incorrect password guesses would do to render the system adequately secure since, e.g., 100% of the passwords of males might are guessed by simply 2 guesses .

A "zero-knowledge" approach of ne'er showing an image cluster double offers immunity from eavesdropping, however separate tests showed that once teams were reused, the subjects' accuracy improved. They failed to confuse the destructors with the photographs on that that they had been trained, and so might use our ways for extended times while not the requirement for preparation. A sound signature recognitions password system is introduced, as from the present relationship system, we have a tendency to incorporated sound signature by clicking the image a beep sound is introduced, a similar sound is created altogether the photographs, if we have a tendency to proceed a similar click purpose altogether the photographs with similar sound then the authentication proceeded to the login page, there we will browse out the vital messages.

II. RELATED WORK

Metrics:

The Study of Pass Points, examining the effects of image choice and size of the tolerance region, and comparing Pass Points to text passwords. All these studies were conducted in-lab and consisted of having users create a password and practice until they entered it correctly ten times. At the end of the session, users logged in with their newly memorized password. They returned one week later to log in again; in addition, for one study they also returned at the 6-week mark. Unless specifically testing the size of the tolerance region, their prototype used a tolerance region of 20 × 20 pixels and all images were 451 × 331 pixels in size. In the study comparing Pass Points to text passwords, they found that graphical passwords were slower to enter than text passwords and users made more mistakes in the initial learning phase [3], yet they conclude that Pass Points is sufficiently memorable because users made fewer errors with Pass Points when they logged in after one and six weeks. For the second study [4], they compared tolerance squares of54 size 20 × 20, 14 × 14, and 10 × 10 on a 19-inch screen at a resolution of 1024 × 768 pixels. The stated conclusion was that while using a smaller tolerance square led to a larger password space, squares of 10×10 pixels were too small to be usable, and they recommended tolerance regions of 14 × 14 pixels or larger. A third study compared the usability of different images. They concluded [3] that image choice had little impact on the memorability of passwords; users performed equally well on the four images tested. The issue of "hotspots", areas on the image that users were more likely to select, was briefly considered but they concluded that further investigation was required to determine whether these were a problem.

III. PROPOSED METHODOLOGY

In the proposed work we have integrated sound signature tohelp in recalling the password. So far No system has been devolvedwhich uses sound signature in graphical password authentication sound signature or audio can beused to recall facts like images, text etc. In life we seevarious examples of recalling an object by the sound related tothat object enters User ID and select one sound frequency which user wantto be played at login time, a tolerance value is selectedwith will decide that the user is legitimate or attacker. User has to select sequence of imagesand clicks on each image at click points of his choice to create detailed vector. And then Profilevector is created.The goal is to analyse to what extent these protocols provide enough redundancy to detect attackers in different scenarios. We implemented representatives of the following protocol families. To begin our analysis, we represented the click-point data graphically on the images themselves.

The purpose of our proposed multiple click based graphical authentication system is to enhance the image-based authentication in both security and usability. In particular, there are mainly three operational: that is, image selection, sequence clicking and secret coding. In the step of image selection which refers to the concept and technique from the choice-based schemes, users are required to choose a category from the set of image pool and then the final image for the following step. In the second step, we further develop an action of sequence clicking that users should give their own secrets by using series of clicks.The step of secret coding, which requires users to code something (e.g., a digital

ISSN (Online): 2319-8753
ISSN(Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization *Volume 4, Special Issue 5, April 2015*

International Conference On Emerging Trends in Engineering and Technology (ICETET'15)

On 13th & 14th March 2015

Organized by

Pandian Saraswathi Yadav Engineering College, Arasanoor, Sivagangai, Tamilnadu, India

number or a letter) on their selected images. Compared to other graphical password schemes, scheme mitigates the 'hot-spot' problem in Pass points and further improves the security of Story and Cued Click Points.

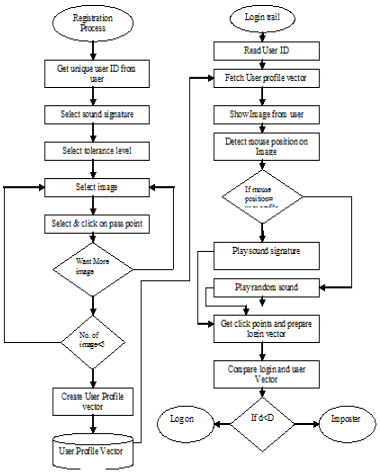

Fig: 2. Flow diagram of the proposed Methodology

The PassPoints-field study involving the Pool and Cars images yielded a large volume of data about where users clicked. We used a Gaussian kernel smoothed intensity function to summarize this data for each image [8]. We then created heap maps to depict this summary on the image area, using several color bands to represent varying intensities of click-point concentration. The most intense areas thus correspond to hotspots, forwarding probability further. A target region can be specified that determines the area for which an observation is relevant. For our simulations, we set the target region to the whole network, because we assume a traffic information application where all vehicles are interested in the speed of the other vehicles in the network.

CCP:

Previous work [3, 6, 7] has 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 In effect; behaving securely became the path-of-least-resistance. Using CCP as a base system, persuasive feature is added to encourage users to select more secure passwords, and to form it more difficult to select passwords where all five click-points are hotspots. Particularly, when users created a password, the images were shaded except for a randomly positioned viewport point.

ALGORITHM

Graphical password systems are a kind of knowledge-based authentication that attempts to obtain visual information by leveraging the human memory. A complete review of graphical passwords is available elsewhere [7]. Here is an cued-recall click-based graphical passwords (also known as locimetric [5]). In such systems, previously selected locations is identified and targeted by the user within one or more images. In order to aid recall the images will act as memory cues [2]. Example systems include Pass Points [5] and Cued Click-Points (CCP). In Pass Points, a password consists of a

ISSN (Online): 2319-8753
ISSN(Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization *Volume 4, Special Issue 5, April 2015*

International Conference On Emerging Trends in Engineering and Technology (ICETET'15)

On 13th & 14th March 2015

Organized by

Pandian Saraswathi Yadav Engineering College, Arasanoor, Sivagangai, Tamilnadu, India

sequence of five click-points on a image. Any pixels in the image will be selected by the user as click-points for their password. Users repeat the sequence of clicks in the correct order to enter the system, within a system-defined tolerance square of the original click-points. Original authors and some others will evaluate the security of this scheme [1, 6, 7]. It was found that although relatively usable, security concern remains. The major security problem is hotspots: Various similar click-points as part of their passwords will be selected by the different user. Attackers who know about these hotspot build attack dictionaries and more successfully guess Pass Points passwords [1] through harvesting typical passwords or through automated image processing techniques. A dictionary attack that consists of a list of potential passwords (ideally in decreasing order of likelihood) is used on the system in order to see if it leads to a correct login for a given account. Attacks can target a sole account, or can guess the passwords of large number of accounts with the hope of breaking into any of them.

IV. PERFORMANCE ANALYSIS

To analyse the performance, data compared from the following three datasets collected in previous studies [3, 5]: PassPoints-lab (PPLab):43 participants tested a PassPoints system with 17 different images in a lab setting with the same methodology as this current study. At least 31 passwords (155 click-points) were collected on each image. Pass Points-field (PPField):376 participants tested a PassPoints system for 7-9 weeks to access online notes for their class. Only the Pool (580 click-points) and Cars (545 click-points) images were used. These two images were selected from the set used in the PassPoints-lab study. Cued Click-Points (CCP):57 participants tested a Cued Click-Points system with the same set of 330 images and same methodology to this current study. 32 to 39 click-points were collected on each of the 17 core images from the PassPoints-lab study. Data was also collected on the remaining 313images, but the higher number of road segments also reflects in the distribution of information. In contrast to the highway case,, the aggregation protocol achieves a distribution of 60%-80% on average with a high standard deviation.

V. CONCLUSION AND FUTUREWORK

A novel approach which uses sound signature to recall graphical password click points. No previously developed system used this approach so far. This system is helpful when user is logging after a long time.

In future work other patterns may be used for recalling purpose like touch of smells, study shows that these patterns are very useful in recalling the associated objects like images or text.

ACKNOWLEDGEMENT

I would like to express my special thanks of gratitude to my college management. I would like to give my thanks to guide who gave me the golden opportunity to do this wonderful project on Graphical password Authentication In addition, I would also like to thank my parents who helped me a lot in finalizing this project within the limited time frame.

REFERENCES

[1] A. Adams and M. A. Sasse, "Users are not the enemy:why users compromise computer security mechanisms and how to take remedial measures,", Communications of the ACM, vol. 42, pp. 41-46, 1999.
[2] AyannugaOlanrewaju O. and FolorunsoOlusegun, "Graphic-Text Authentication of a Window-based Application," International Journal of Computer Applications, Vol. 21, No. 6, pp. 36-42, May 2011.
[3] G. E. Blonder, "Graphical password", U.S. Patent 559 961, Sep. 24, 1996.
[4] S. Chiasson, R. Biddle, and P.C. Van Oorschot, "A second look at the usability of click-based graphical passwords," In: Proceedings of the 3rd Symposium on Usable Privacy and Security (SOUPS). New York, NY, USA: ACM, 2007, pp. 1–12.
[5] S. Chiasson, P.C. Van Oorschot, and R. Biddle, "Graphical password authentication using cued click-points," In: Proceedings of the 12th European Symposium On Research In Computer Security (ESORICS). Berlin, Heidelberg: Springer-Verlag, 2007, pp. 359– 374.
[6] D. Davis, F. Monrose, and M.K. Reiter, "On user choice in graphical password schemes," In: Proceedings of the 13th conference on USENIX Security Symposium. Berkeley, CA, USA: USENIX Association, 2004, pp. 151–164.
[7] Dinesha H A, Agrawal V K, "Multi-level Authentication Technique for Accessing Cloud Services", 2013

ISSN (Online): 2319-8753
ISSN(Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization *Volume 4, Special Issue 5, April 2015*

International Conference On Emerging Trends in Engineering and Technology (ICETET'15)

On 13th & 14th March 2015

Organized by

Pandian Saraswathi Yadav Engineering College, Arasanoor, Sivagangai, Tamilnadu, India

[8] A.E. Dirik, N. Memon, and J.C. Birget, "Modeling user choice in the passpoints graphical password scheme," In: Proceedings of the 3rd symposium on Usable privacy and security (SOUPS). New York, NY, USA: ACM, 2007, pp. 20–28.
[9]. R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in Proceedings of 9th USENIX Security Symposium, 2000.
[10] P. Dunphy and J. Yan, "Do background images improve "draw a secret" graphical passwords?" In: Proceedings of the 14th ACM conference onComputer and communications security (CCS). New York, NY, USA: ACM, 2007, pp. 36–47.
[11] GayathiriCharathsandran, "Text Password Survey: Transition from First Generation to Second Generation,"
[12] .K. Gilhooly, "Biometrics: Getting Back to Business," in Computerworld, May 2005.
[13]. K. Golofit, "Click passwords under investigation," In: Proceedings of the 12th European Symposium on Research in Computer Security (ESORICS). Berlin, Heidelberg: Springer-Verlag, 2007, pp. 343–358.
[14] Horng-Twu L. and Chin-Laung L, "An efficient password authen- tication scheme based on a nit circle," Computer and Security, Elsevier, Vol. 14, No. 3, pp. 220-220, 1995.
[15]. Huanyu Zhao and Xiaolin Li, "S3PAS:A Scalable Shoulder-Surfing Resistant TextualGraphical Password Authentication Scheme,".
[16]. I. Jermyn, A. Mayer, F. Monrose, M.K. Reiter, and A.D. Rubin, "The design and analysis of graphical passwords," In: Proceedings of the 8th conference on USENIX Security Symposium. Berkeley, CA, USA: USENIX Association, 1999, pp. 1–14.
[17] D. Lin, P. Dunphy, P. Olivier, and J. Yan, "Graphical passwords & qualitative spatial relations," In: Proceedings of the 3rd symposium on Usable privacy and security (SOUPS). New York, NY, USA: ACM, 2007, pp. 161–162.
[18] Mahmud Hasan and Kamruddin Md. Nuro, "A Novel 3-Layer User Authentication System for Remote Accessibility", IEEE, 978-1-4673- 4836-2/1,2012.
[19] Massimo Tistarelli and Mark S Nixon, "Advances in Biometrics," SpringerLink, ISBN: 9783642017933 3642017932 9783642017926 3642017924, 2009.