Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 4, April 2014, pg.422 – 426

RESEARCH ARTICLE

GRAPHICAL PASSWORD FOR EMAIL APPLICATION BY PERSUASIVE CLICK POINTS USING CENTERED DISCRETIZATION

Mr. Aniket G. Jadhav
Pune University
aniket.g.jadhav12@gmail.com

Ms. Rajashri D. Dipak
Pune University
rajashrideepak@gmail.com

Ms. Lavina P. Dadlani
Pune University
lavidadlani22@gmail.com

Mr. Mangesh K. Manke
Pune University
mangesh.manke1@gmail.com

Dr. D. Y. Patil Institute of Engineering and Technology, Ambi, Talegaon Dabhade, Pune, Maharashtra, India

Abstract

The general method which is in use nowadays is text based or alphanumeric based passwords. But this method as such has not proved to be efficient in security against password guessing attacks. Either the password is easy to guess or hard to remember. To overcome this problem we have developed authentication technique which uses pictures as passwords. According to a survey of graphical password techniques they are classified into two categories: recognition based and recall based approaches. We are also going to study the strengths and limitations of each method and will also focus on future scopes in this field. This paper focuses on integrated evaluation of the Persuasive Cued Click Points graphical password authentication system and security using centered discretization technique. This paper also gives the solution for prevention from emergence of hotspots. Hotspots are the portion of images which are more likely to be chosen as click points. Also we are here proposing a new technique for graphical authentication.

Keywords: authentication, computer security, graphical passwords, guessing attacks and centered discretization

1. Introduction

The weakest link in a computer security system is human factors. The three operations which are more common and important between human and computer are authentication, developing secure systems and security operations. In this paper we will focus on authentication problem. Some passwords that are hard to guess or break are often hard to remember.

A user has many accounts and so do many passwords to be remembered or have same password for different accounts. To overcome the various problems related to traditional username password authentication many alternative authentication methods, such as bio-metrics etc., have been used. But this paper will focus on, using pictures as passwords. By accepting the fact that humans can remember the pictures better then text, Graphical password schemes have been proposed as an alternative to text based schemes. While using this scheme if we provide large number of pictures to the user, the possible password space of a graphical password scheme may exceed that of text-based schemes which will indeed help in resisting dictionary attacks. As a user we have to do many transactions which have it own security level, and this is where we can apply this technique. Two most important things to be kept in mind are the answers to the questions such as Are graphical passwords as secure as text passwords? And what are the major implementation issues for graphical passwords? We will be using a feature, according to which system will suggest the user to select a secure password. It will also analyse the security rate and efficiency of tolerance value. It is useful for researchers and industry practitioners working in this area.

2. Background

The most prevalent authentication method is text passwords which were replaced by biometric systems and tokens but all these techniques had their own drawbacks. In 1996 Blonder defined the graphical passwords. Graphical password technique is divided mainly into two categories that are recall based and recognition based graphical techniques. The user when recognizes and identifies the images he selected at registration stage it is called as recognition based technique, whereas user when asked to reproduce the password that he selected or created at registration stage. Under recall based passwords we have two techniques a) Pass Points and b) Cued Click Points.

a) Pass Points **-** a user have to choose or select some points on the image that is nothing other than pixels of image as click points to set as a password.

b) Cued Click Points – a user in this technique has to choose click points on five different images queued in proper sequence. The next valid image will be loaded only if the user has identified the previous image correctly. This kind of process will help to reduce the severity of hotspots.

As these techniques clearly show that they belong to the category of cued click recall based scenario because they regularly triggers memory corresponding to click points.

3. Proposed System

In today's world of technology, security plays an important role in each field of organization. Various types of organizations invest money, time and computer memory for the purpose of gaining security of organizational information.

This project deals with the click based graphical password system. As the user gets attracted to most predictable areas, on an image the hotspots issue may lead to less security. So, in order to provide high security, the system uses persuasive technology, along with cued click point as base system which will guide user to select a strong password. The PCCP's design follows FOGG's principle of reduction, by making it easy to choose strong password and principle of suggestion, by providing suggestion during the process of choosing a password. During this process, images are slightly shaded or either Grayscale or are blurred except for a randomly positioned viewport. Instead of positioning the viewport specifically it is positioned randomly: in order to avoid hotspots, since this may help the attackers to improve guesses. The viewport size was intended to offer a variety of distinct point but still cover only an acceptably small fraction of all possible points. Users are supposed to click points within viewport and could not click outside the viewport. But if users don't want or are unable to select the click point on the provided viewport, then they can press the SHUFFLE button so as to reposition the viewport, randomly. The viewport and SHUFFLE buttons are only appeared or provided during the passwords, creation and during the phase of or process of confirmation login, the images are displayed normally, without shading or blurring rest of the image or viewport.

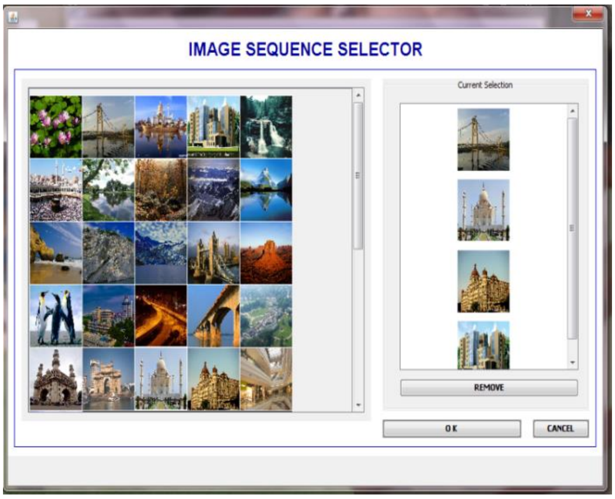

Fig 1. Image Sequence Selector Viewport.

System aims at:-

1) Users will be selecting click-points that may fall
2) The click points distribution across users will be randomly dispersed and will not form new hotspots.
3) The login security success rates will be more than original CCP system.
4) The login security success rates will increase, when tolerance value is lower.
5) User will feel that their passwords are more secure with PCCP system.

The theoretical password space for a password system is total number of unique password that could be generated according to system specifications. Ideally, larger theoretical password space lowers the likelihood that any particular guess is correct for given password. For PCCP, theoretical password space is $((w * h) / t^2)^c$ where size of image in pixels (w * h) is divided by size of tolerance square (t^2) to get total number of tolerance squares per image , raised to power of number of tolerance squares per image, raised to power of number of click points in a password (c, usually set to 5).

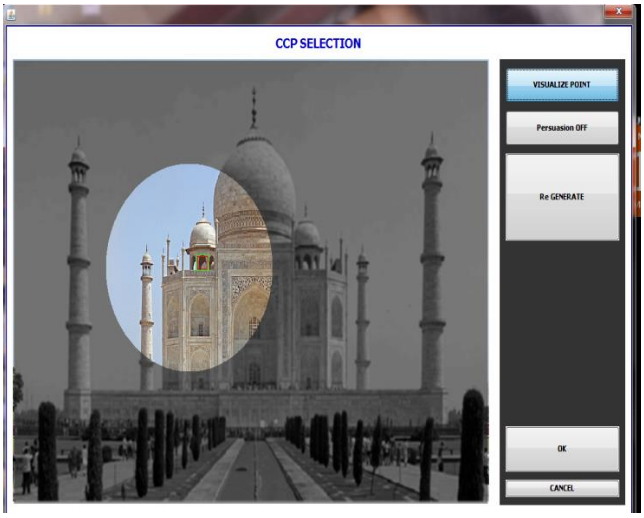

Fig 2. Cued Click Point Selection Viewport

Protection against brute force and dictionary attacks on password – This project deals with the guessing attacks like brute force attacks and dictionary attacks. Enable login to the authorized user while providing prevention to such attacks is most difficult. Automated turing tests, is an effective and an easy to deploy approach that may help to identify automated malicious login attempts within reasonable cost of inconvenience to users. This project uses a new Password Guessing Resistant Protocol (PGRP), in order to restrict such attacks. The PGRP limits the total number of login attempts from unknown remote hosts; so legitimate users can make many failed login attempts before being challenged with an ATT.

This proposed system also provides protection against key logger, spyware as computer mouse is used rather than the keyboard to enter or select graphical passwords, it may help or provide protection of password from key loggers.

4. Security

4.1) Guessing Attacks:

PCCP provides security against brute force attack. Brute force attack is trial and error method used to decrypt the encrypted data like passwords, personal identification number. In this system, while password creation, there is a small persuasive area (viewport) is generated on image. Users should select or click points in this viewport region. This viewport will guide user to select random portion of image and not the hotspots. So, this proposed system encourages users to choose difficult passwords that are generated randomly and difficult to guess.

PCCP works against brute force attack, which is commonly biggest threat in network security and preventing resources from such unauthorized access becoming serious problem. PCCP provides the protection against such dangerous threats and preserve cloud resources. PCCP also provide protection against dictionary attack. Dictionary attack is attempted by entering every word in dictionary to crack the password. Also dictionary attack is achieved by trying to decrypt key of an encrypted message of a document. Dictionary attacks are successful because many users uses simple and easy to guess words for setting their passwords. These words can be easily found by attacker in English dictionary. PCCP provides full protection against dictionary attacks, as system is setting password by randomly generating images. In addition to this it provide fake image sequence to user, when user clicks on wrong image or point. In case if the person is an hacker then password entering will confusing task. This facility provides protection against dictionary attack. PCCP is resisting the key logger spyware. Since proposed system used mouse for setting password and keyboard is totally avoided, this protects the system from key loggers. As key logger traces the keyboard keys to find out password, it is totally avoided to use keyboard for setting graphical password.

PCCP avoids the hotspots for setting graphical password. Normal user always chooses hotspots to set the passwords for easy to remember. But it will help the attacker to easily trace the password. As proposed system guides the user to select password within given persuasive area, it will avoid hotspot. For example, if user choosing tower of "Taj Mahal" to set the password, it will threat to security, hence proposed system will show viewport on wall of Taj Mahal, that are hard to guess and more secure. In this way, proposed system avoids hotspot and provides better security to specific system. In case user is unwilling to choose system generated password user can choose password of own choice.

4.2) Capture Attack:

Capture attacks occur when attackers have been directly obtain part of password or whole password capture attacks are attempted by tricking user information.

4.2.1) Shoulder Surfing

Shoulder surfing attack is found where attacker is observing user while login. It's direct observation like looking over someone's shoulder while user is putting their credentials to get information. Observing approximate location of click points may be reduces the number of guesses that are necessary to know the users password. With the help of reducing click regions system can provide more protection. A more alternative should be provided by off the visualization option to provide more security, but it will be difficult to remember the user where is actual click point. By providing "Visualization Off" option, the proposed system plays strong protection role against shoulder surfing attack.

4.2.2) Social Engineering

One primary study suggests that, password sharing through verbal communication is impossible with proposed system. In PCCP extreme efforts required to describe each image in detail and its click points in detail. Describing each clicked point in detail is more difficult. For man-in-middle attack only one image for every click point need to be collect, but the correct image would be identified by the legitimate user only. Even if attacker have collected all images of password need to be keep in order they been set. Attacker who have collected even all images may click on hotspots, since user have been clicked elsewhere. All client server communication is been made security, to maintain privacy of user click points and corresponding images.

5. Centered Discretization Algorithm

The proposed system uses centered discretization algorithm for graphical password so correct entries are accepted through system. This system eliminate false accept and false reject system allows fr small tolerance area. Password is composed of set of clicks on several images. At the time of sign-in, user re-enter password i.e click points in same order. Click points that comes within acceptable tolerance of original points should accepted. It is important to remember user original pixels. This system allow some level of inaccuracy since it is impossible to remember exact point on image, however approximately correct entry match with hash value as original password, so ultimately system will recognize correct user. During re-entry of password, if click points are within same grid-square and match with original click points, then entry is accepted as its hash value match with original. If we consider 1-dimensional line L, every point on that line is taken as x, which is real number. We discretize the line L into equal segment when x lies on centre of line. So even tolerance on both side of x. We are selecting tolerance r based on user preference. Now each segment's length is 2r. To ensure x is center, segment 0 may be need to offset from origin. The offset is represented by'd'. First we will assume 1-d password, which is having only one click-point x. To store password, we have to calculate offset'd' and corresponding segment identifier 'i'. Hered is stored in the clear, where I stored in hash value h(i:d)

The I computed by i = b(x-r) = 2rc and offset d = (x-r) mod 2r

To verify, re-entered click poit x' is within the region, system computes I' = b(x'-d) = 2rc which calculates same offset as original point. Note that here not necessary to x' comes within its segment, we are calculating which segment contains x' based on x's pre-determined segment. If x' within segment, then i' = i and hence h(i':d) store equal value as h(i:d). So system will accept that entry. If x' is outside of accepted tolerance r, it means that fall in different segment.

For Example, let x=23 and r= 5. i = |(x-r)/2r| = 23-5/10 = 18/10 = 1. d = (x-r) % 2r = 23-5/10 =8.
To store d=8, r=5 Calculate h(i,d) = h(1,8) = 9a5692cd. Now at the time of re-entry select nearest point, x' = 27 i' = |(x' – d)/2r| = 27-8/10 = 1. h(i,d) = h(1,8) =9a5692cd.
Select farthest point. x'=30 = |x'-d/2r|= 30-8/10 = 22/10 = 2. h(2,8) = 779f1x.

6. Conclusion

Text passwords have been replaced by a more secure and more usable system that is click based graphical passwords. Under testing conditions of the proposed system this was conducted using centered tolerance discretization approach and also robust discretization that make it less usable. As our results suggested that using robust discretization is leading to some kind of compensatory behavior. We have presented you with how the security and usability factors of click based passwords are affected by the kind of discretization technique we are using. The basic problem in Robust discretization is concept like false reject and false accept, which makes the system more unreliable from users perspective. Instead we have used centered discretization that guarantees centered tolerance and increases the password space with smaller grid squares can be used. This technique provides more usable in real world by making the system behavior more predictable(avoids false reject and false accept). This system open to further study whether Centered Discretization opens door to new types of password attacks.

References

[1] Alsulaiman, F.A. and Saddik, A.E. A Novel 3D Graphical Password Schema. IEEE International Conference on Virtual Environments, Human-Computer Interfaces and Measurement Systems. July 2013.

[2] Birget, J.C., Hong, D., and Memon, N. Graphical Passwords Based on Robust Discretization. IEEE Transactions on Information Forensics and Security, vol. 1, no. 3, September 2006.

[3] Suo, X., Zhu, Y., and Owen, G.S. Graphical Passwords: A Survey. ACSAC 2005.

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

[5] Chiasson, S., van Oorschot, P.C., Biddle, R. Graphical Password Authentication Using Cued Click-points. ESORICS 2007.

[6] Chiasson, S., A. Forget, R. Biddle, P.C. van Oorschot. Influencing Users Towards Better Passwords: Persuasive Cued Click-Points. Technical Report TR-07-16, School of Computer Science, Carleton University, Ottawa ON, 2007.

[7] Zhi Li, Qibin Sun, Yong Lian, and D. D. Giusto, "An association-based graphical password design resistant to shoulder surfing Attack", International Conference on Multimedia and Expo (ICME), IEEE.2005

[8] R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in *Proceedings of 9th USENIX Security Symposium*,2000