Protection against Online Password Guessing Attacks by Using Graphicals Passwords

Kiran Babu T.S, Ragav Krishna.R

Abstract: Usable security has unique usability challenges because the need for security often means that standard human-computer-interaction approaches cannot be directly applied. A very pivotal usability goal for authentication systems is to support users in selecting secure passwords. Users often create predictable and easy to remember passwords that are easy for attackers to hack or guess, but system-assigned passwords which are inherently strong are difficult for users to remember. We are proposing alternative methods wherein graphical pictures are used as security agents (passwords). Graphical passwords fundamentally use images or representation of images as passwords. Pictures are more lucid and easy to remember for the human brain than textual character. There for, this paper merges persuasive cued click points and password guessing resistant protocol. The pith and main intent of this work is to reduce the guessing attacks as well as encouraging users to select passwords that are random and thus logically become more difficult to guess. The rudimentary security threats including brute force attacks and dictionary attacks can be successfully abolished using this method.

Keywords - Authentication, graphical passwords, guessing attacks, computer security.

I. INTRODUCTION

There has been a great deal of hype for graphical passwords since two decade due to the fact that Primitive's methods suffered from an innumerable number of attacks which could be imposed easily. Here we will progress down the ramifications of authentication mechanisms. To start with we throw light on the most prevalent computer authentication method that makes use of text passwords. Despite the vulnerabilities and cons, it's the user natural predilection of the users that they will always prefer to go for short passwords for ease of remembrance and also lack of awareness about how attackers tend to attacks. The flip side is that they are broken mercilessly by intruders by several simple means such as masquerading.

Eaves dropping and other rude means say **dictionary attacks**, **social engineering shoulder surfing attacks**. To mitigate the problems with conventional methods, advanced and novel methods have been proposed using graphical as passwords. The crux of graphical passwords inceptionally described by Greg Blonder (1996). For Blonder, graphical passwords have a predetermined image that the sequence and the tap regions selected are interpreted as the graphical password.

Manuscript received December, 2013.

Kiran Babu T.S, Asst. Professor, Dept of Computer Science & Engineering CMR Institute of Technology (CMRIT) 132, AECS Layout, IT Park Road Bangalore 560 037,India.

Ragav Krishna.R, BE Scholar, Dept of Computer Science & Engineering CMR Institute of Technology (CMRIT) 132, AECS Layout, IT Park Road Bangalore 560 037, India.

Since then, many other graphical password schemes have been put forward. The threshold quality associated with graphical passwords is that psychologically humans can remember graphical far better than text and hence is the best alternative being suggested. There is a exponentially growing interest in graphical passwords for they are more or infinite in numbers thus providing more resistance.

The pith and main intent of this work is to reduce the guessing attacks as well as encouraging users to select more random, and difficult passwords to guess.

The following Figure 1.1: is the depiction of current authentication methods Biometric based authentication systems techniques are proved to be expensive, dilatory and vulnerable and hence disregarded by many. Token based authentication system is bolstered with high security, usability and Accessibility compare to others. But this system employs knowledge based techniques to strengthen the security. But the current knowledge based techniques are still inchoate. Quintessential of this is that ATM cards always go hand in hand with PIN number.

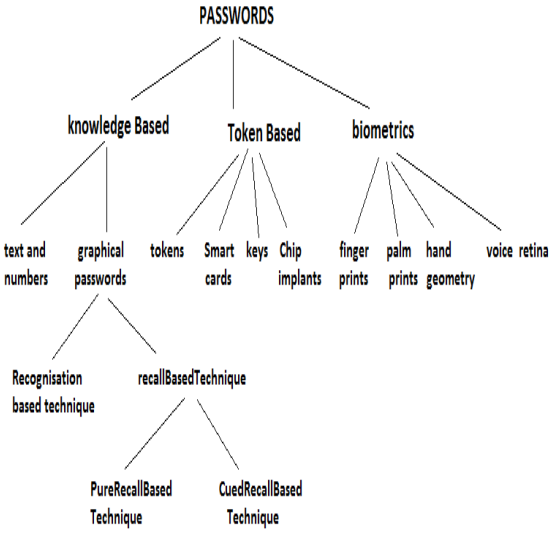

Figure 1. Taxonomy of Password Authentication Techniques.

So the knowledge based techniques are the most wanted techniques to improve real high security. Recognition based & recalls based are the two names by which graphical techniques could be classified.

II: EXISTING SYSTEM

Existing approaches to Users often create memorable passwords that are easy for intruders to surmise, while strong system-assigned passwords are difficult for users to remember. Despite the jeopardy, it's the natural tendency of the users that they will always prefer to go for short passwords for ease of remembrance and also lack of awareness about the threat posed by the attackers. Unfortunately, these passwords are broken mercilessly by

intruders by several simple means such as masquerading, Eaves dropping and other rude means say dictionary attacks, shoulder surfing attacks, social engineering attacks.

III: PROPOSED SYSTEM:

Our proposal is to reduce the guessing attacks as well as encouraging users to select more arbitrary, making it strenuous to guess. The proposed system work on
Pass Points Module, Cued Click Points Module. And Merging of persuasive cued click points and password guessing resistant protocol.

IV: IMPLEMETATION

A: Pass Points Module:

Based on Blonder's original idea, Pass Points (PP) is a click-based graphical password system where a password consists of an ordered sequence of five click-points on a pixel-based image. To successfully log in, a user must click within the periphery of some system-defined tolerance region for each click-point. The image serves as a cue to help users remember their password click-points.

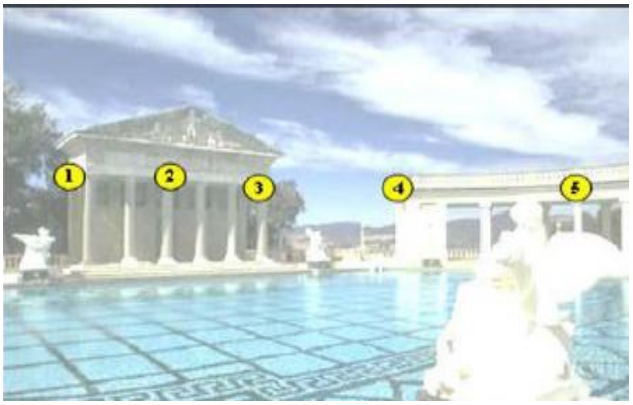

Figure 2: Pass Points

B: Cued Click Points Module:

Cued Click Points (CCP) was developed as an alternative click based graphical password scheme where users select one point per image for five images. The interface displays a solitary image at a time; the image is replaced by the next image as soon as a user selects a click point. The system prudently determines the subsequent image to display based on the user's click-point on the current image. The image thus subsequently displayed to users is based on a deterministic function of the point which is selected at the present juncture. It now presents a one to-one correspondence cued recall scenario where each image triggers the user's memory of the one click-point on that image. Further, if a user enters an erroneous click-point during login, the subsequent image displayed in response will also be erroneous. Legitimate users who see an out of place and unrecognized image know that they made an error with their previous click-point. Conversely, this inherent feedback based on the response to the current image is not helpful to an attacker who does not know the expected sequence of images.

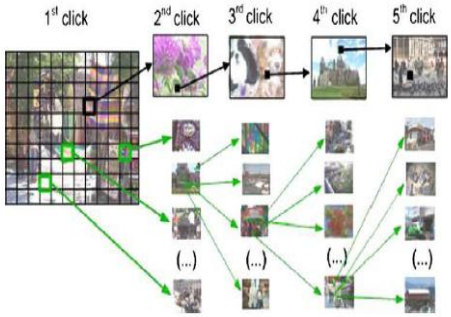

Figure 3 Cued Click points

7.2.3 Persuasive Cued Click- Points Module:

To address the issue of hotspots, Persuasive Cued Click Points (PCCP) was put forward. Commensurate to the CCP, a password consists of five click points, one on each of distinct five images. During the creation of password, most part of the image is dimmed except for a distinctly separate small view port area that is randomly positioned on the image. Users must choose a click-point within the view port. If the current view port is not suitable for any reason, they may randomly reposition the view port by making use of the shuffle button. The view port vanguards users to select more arbitrary passwords that are less likely to include hotspots. A user who is firm on a certain click-point may still shuffle until the view port moves to the prescribed location, but this is a time consuming and more strenuous process.

Figure 4 Cued Click points

V: CONCLUSION

A major advantage of Persuasive cued click point scheme is its large password space over alphanumeric passwords. There is a growing predilection towards Graphical passwords since they are better than Text based passwords, although the crux of the argument for graphical passwords is that people are better at memorizing graphical passwords than text-based passwords. Online vulnerable attack of password guessing on password-only systems have been observed for decade's .Present-day attackers targeting such systems are empowered by having control of thousand to million node botnets .We applied this approach to create the first persuasive click-based graphical password system, Persuasive Cued Click-Points (PCCP), and conducted user studies evaluating usability and security.

REFERENCES

1. Sonia Chiasson, P.C. van Oorschot, and Robert Biddle, “Graphical Password Authentication Using Cued Click Points” ESORICS, LNCS 4734, pp.359- 374,Springer- Verlag Berlin Heidelberg 2007.
2. Manu Kumar, Tal Garfinkel, Dan Boneh and Terry Winograd, “Reducing Shoulder-surfing by Using Gazebased Password Entry”, Symposium On Usable Privacy and Security (SOUPS) , July 18-20, 2007, Pittsburgh,PA, USA.
3. 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
4. R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in Proceedings of9th USENIX Security Symposium, 2000.
5. S. Akula and V. Devisetty, "Image Based Registration and Authentication System," in Proceedings ofMidwes Instruction and Computing Symposium, 2004.
6. L. Sobrado and J.-C. Birget, "Graphical passwords," The Rutgers Scholar, An Electronic Bulletin forUndergraduate Research, vol. 4, 2002.
7. Sonia Chiasson, Alain Forget, Robert Biddle, P. C. van Oorschot, “User interface design affects security: patterns in click-based graphical passwords”, Springer-Verlag 2009.
8. 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 USENIXSecurity Symposium, 1999.