Persuasive Graphical Password Authentication Using Cued Click Point

Abhilash Harishchandre, Kondiba Salve, Shrikar Ratnalikar, Omkar Ratnaparkhi
student
Computer Engineering , Govt. College of Engineering & Research Avasari, Pune , India
[1]abhie.harishchandre@gmail.com, [2]s9766397994@gmail.com, [3]ratnaparkhiomakr@gmail.com
[4]deepaksalve219@gmail.com

***Abstract*- Usable security has unique usability challenges because the need for security often means that standard human-computer-interaction approaches cannot be directly applied. An important usability goal for authentication systems is to support users in selecting better passwords. Users often create memorable passwords that are easy for attackers to guess, but strong system-assigned passwords are difficult for users to remember. So researchers of modern days have gone for alternative methods wherein graphical pictures are used as passwords. Graphical passwords essentially use images or representation of images as passwords. Human brain is good in remembering picture than textual character. There are various graphical password schemes or graphical password software in the market. However, very little research has been done to analyze graphical passwords that are still immature. There for, this project work merges persuasive cued click points, password guessing resistant protocol and file encryption application. The major goal of this work is to reduce the guessing as well as shoulder surfing attacks as well as encouraging users to select more random and difficult passwords to guess. Well known security threats like brute force attacks and dictionary attacks can be successfully abolished using this method.**

***Index Terms* - Authentication, graphical passwords, guessing attacks, computer security, Encryption.**

I. INTRODUCTION

A multitude of graphical password schemes have been proposed, motivated by the promise of improved password memorability and thus usability, while at the same time improving strength against guessing attacks. Like text passwords, graphical passwords are knowledge based authentication mechanisms where users enter a shared secret as evidence of their identity. However, where text passwords involve alphanumeric and/or special keyboard characters, the idea behind graphical passwords is to leverage human memory for visual information, with the shared secret being related to or composed of images .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 taxonomy of authentication methods. To start with we focus on the most common computer authentication method that makes use of text passwords. Despite the vulnerabilities, it's the user natural tendency of the users that they will always prefer to go for short passwords for ease of remembrance [10] and also lack of awareness about how attackers tend to attacks. 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 [10][1].To mitigate the problems with traditional methods, advanced methods have been proposed using graphical as passwords. The idea of graphical passwords first 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. Since then, many other graphical password schemes have been proposed. The desirable quality associated with graphical passwords is that psychologically humans can remember graphical far better than text and hence is the best alternative being proposed. There is a rapid and growing interest in graphical passwords for they are more or Infinite in numbers thus providing more resistance.

The major goal of this work is to reduce the guessing and shoulder surfing attacks as well as encouraging users to select more random, and difficult passwords to guess. Also integrate the file encryption application which encrypt public key, private key and model key and decrypt it for user hence forth reduce memory burden on user.

II. BACKGROUND

The community of security researchers and practitioners has evolved rapidly in response to threats, on the one hand increasing vigilance in practice and, on the other hand, driving research innovation. Until recently the security problem has been formulated as a technical problem. Even though text passwords are the most popular user authentication method, they have security and us-ability problems. The alternatives for text based passwords such as biometric systems and tokens have their own drawbacks. Graphical passwords, which consist of clicking on images rather than typing alphanumeric strings, may help to overcome the problem of creating secure and memorable passwords. A graphical password scheme using click point offers the best alternative for the text password, cued click points are used to exploit the memeorablity of the user that it is fully a knowledge based authentication and is discussed in this paper the security and usability problems associated with alphanumeric passwords as the password problem. The problem arises because passwords are expected to comply with two conflicting requirements, namely

1. Passwords should be easy to remember, and the user authentication protocol should be executable quickly and easily by humans

2. Passwords should be secure, i.e. they should look random and should be hard to guess; they should be changed frequently, and should be different on different accounts of the same user; they should not be written down or stored in plain text.
3. Once a password has been chosen and learned the user must be able to recall it to log in. However, people regularly forget their passwords.

Recall-Based Systems

Recall-based graphical password systems are occasionally referred to as *drawmetric* systems because users recall and reproduce a secret drawing. In these systems, users typically draw their password either on a blank canvas or on a grid. Recall is a difficult memory task because retrieval is done without memory prompts or cues. Users sometimes devise ways of using the interface as a cue even though it is not intended as such, transforming the task into one of cued-recall, albeit one where the same cue is available to all users and to attackers. Text passwords can also be categorized as using recall. A number of security vulnerabilities are common to most recall-based systems, as these systems share similar features.

Recognition-Based Systems

Recognition-based systems, also known as *cognometric systems* or *searchmetric systems* [17], generally ask users to memorize a portfolio of images during password creation, and then recognize their images from among decoys to log in. Humans have exceptional ability to recognize images previously seen, even those viewed very briefly. From a security perspective, such systems are not suitable replacements for text passwords, as they have password spaces comparable in cardinality to only 4 or 5 digit PINs (assuming a set of images whose cardinality remains reasonable, with respect to usability). Proposed recognition-based systems use various types of images, most notably: faces, random art, everyday objects, and icons. Renaud [17] discusses specific security and usability considerations, and offers usability design guidelines for recognition based systems.

Cued-Recall Systems

Cued-recall systems typically require that users remember and target specific locations within an image. This feature, intended to reduce the memory load on users, is an easier memory task than pure recall. Such systems are also called *locimetric* as they rely on identifying specific locations. This memory task differs from simply recognizing an image as a whole. Hollingworth and Henderson [3] show that people retain accurate, detailed, visual memories of objects to which they previously attended in visual scenes; this suggests that users may be able to accurately remember specific parts of an image as their password if they initially focused on them. In an ideal design, the cue in an authentication system is helpful only to legitimate users (not to attackers trying to guess a password).

Cued-recall graphical password systems date back to Blonder's patent [4]. PassPoints, its successor, launched research in the cued-recall subclass sometimes called *click-based graphical passwords.*

III. PERSUASIVE CUED CLICK-POINT (PCCP)

To address the issue of hotspots, PCCP was proposed [7]. As with CCP, a password consists of five click points, one on each of five images. During password creation, most of the image is dimmed except for a small view port area that is randomly positioned on the image as shown in Figure. 6. Users must select a click-point within the view port. If they are unable or unwilling to select a point in the current view port, they may press the Shuffle button to randomly reposition the view port.

Figure 1: the PCCP password creation interface

The view port guides users to select more random passwords that are less likely to include hotspots[13]. A user who is determined to reach a certain click-point may still shuffle until the view port moves to the specific location, but this is a time consuming and more tedious process[14].

IV. DISCUSSION

"Will Graphical passwords circumvent Text based passwords?"

Here we briefly exam some of the possible techniques for breaking graphical passwords and try to do a comparison with text based passwords.

- ***Dictionary attacks***
  Since recognition based graphical passwords involve mouse input instead of keyboard input, it will be impractical to carry out dictionary attacks against this type of graphical passwords. For some recall based graphical passwords [11], it is possible to use a dictionary attack but an automated dictionary attack will be much more complex than a text based dictionary attack. More research is needed in this area Overall; we believe graphical passwords are less vulnerable to dictionary attacks than text-based passwords.
- ***Guessing***
  Unfortunately, it seems that graphical passwords are often predictable, a serious problem typically associated with text-based passwords. More research efforts are needed to understand the nature of graphical passwords created by real world users.
- ***Shoulder Surfing***
  Like text based passwords, most of the graphical passwords are vulnerable to shoulder surfing. At this point, only a few recognition based techniques are designed to resist shoulder-surfing.
- ***Spy ware***
  Except for a few exceptions, key logging or key listening spy ware cannot be used to break graphical passwords. It is not clear whether "mouse tracking" spy ware will be an effective tool against graphical passwords. However, mouse motion alone is not enough to break graphical passwords. Such information has to be correlated with application information, such as window position and size, as well as timing information.
- ***Social engineering***
  Comparing to text based password, it is less convenient for a user to give away graphical passwords to another person. For example, it is very difficult to give away graphical passwords over the phone. Setting up a phasing web site to obtain Graphical passwords would be more time consuming.

V. PROPOSED SYSTEM

Now-a-days, all business, government, and academic organizations are investing a lot of money, time and computer memory for the security of information. Online password guessing attacks have been known since the early days of the Internet, there is little academic literature on prevention techniques[16]. This project deals with guessing attacks like brute force attacks, and dictionary attacks as well as shoulder surfing attacks. This project proposes a click-based graphical password system. During password creation, there is a small view port area that is randomly positioned on the image. Users must select a click-point within the view port. If they are unable or unwilling to select a point in the current view port, they may press the Shuffle button to randomly reposition the view port. The view port guides users to select more random passwords that are less likely to include hotspots. Therefore this works encouraging users to select more random, and difficult passwords to guess. Also system adds delay time in viewport repositioning in order to repel user from frequently repositioning viewport and hence selecting weak password.

Brute force and dictionary attacks on password-only remote login services are now widespread and ever increasing. Enabling convenient login for legitimate users while preventing such attacks is a difficult problem Automated Turing Tests continue to be an effective, easy-to-deploy approach to identify automated malicious login attempts with reasonable cost of inconvenience to users. This project proposes a new Password Guessing Resistant system, derived upon revisiting prior proposals designed to restrict such attacks. While password guessing resistant system limits the total number of login attempts from unknown remote hosts, legitimate users in most cases (e.g., when attempts are made from known, frequently-used machines) can make several failed login attempts before being challenged with an Automated Turing Test.

This proposed system also provides protection against shoulder surfing attacks. While login attempt if user feel that someone is shoulder surfing then he can click on random point on image so system gives away random image other than login image seed so that user can afterword click on bogus area (defined as lower right hand corner of image) which suggest system that user is legitimate and again provide user with legitimate image from user seed.

Password Encryption decryption option is integrated with graphical password authentication system. Any encryption of password requires three keys public, private and model key. On successful login attempt system provides these keys to user in ready format hence reduce memory burden on user. Also if user forgets his password then system provides OTP code on his alternate email id so that he can login via using OTP code.

VI. PROPOSED SYSTEM ARCHITECTURE

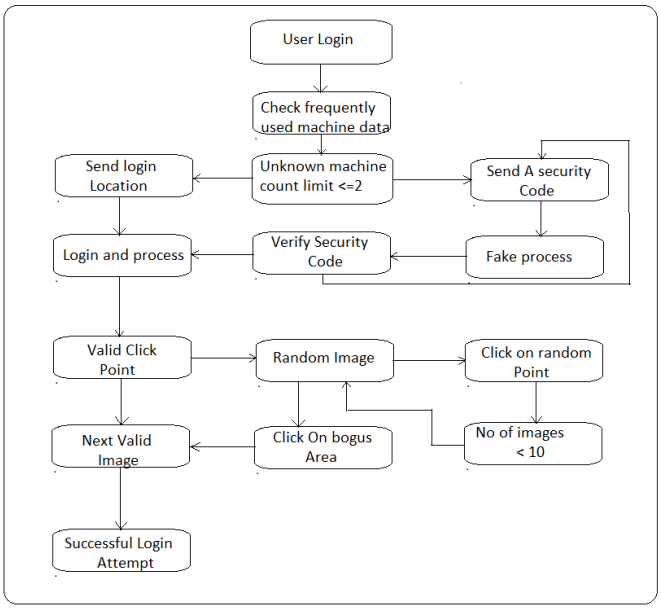

Figure 2: System Architecture

VII. CONCLUSION AND FUTURE WORK

A major advantage of Persuasive cued click point scheme is its large password space over alphanumeric passwords. There is a growing interest for Graphical passwords since they are better than Text based passwords, although the main argument for graphical passwords is that people are better at memorizing graphical passwords than text-based passwords. Online password guessing attacks on password-only systems have been observed for decades. Present-day attackers targeting such systems are empowered by having control of thousand to million node bonnets[16]. In previous ATT-based login protocols, there exists a security-usability trade-off with respect to the number of free failed login attempts (i.e., with no ATTs) versus user login convenience (e.g., less ATTs and other requirements)[15]. In contrast, Password Guessing Resistant system is more restrictive against brute force and dictionary attacks while safely allowing a large number of free failed attempts for legitimate users. Password Guessing Resistant system is apparently more effective in preventing password guessing attacks (without answering ATT challenges), it also offers more convenient login experience, e.g., fewer ATT challenges for legitimate users. Password Guessing Resistant system appears suitable for organizations of both small and large number of user accounts. Bogus area defined in image brings robustness in system. Avoid shoulder surfing attacks. Encryption application as well reduce memory burden on user.

VIII. ACKNOWLEDGMENT

We thank Mrs. P.R.Deshamukh , Asst. Professor at GCOEAR, Awasari for her cooperative efforts with us in this literature survey. We also thank Mr. D.J.Pareira , HOD, Computer Dept, GCOEAR, Awasari for giving us opportunity to work in this segment of authentication. Finally we thank all our friend reviewers for their worthy suggestion in improving this paper.

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 for Undergraduate 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.

[9] S. Man, D. Hong, and M. Mathews, "A shoulder surfing resistant graphical password scheme," in *Proceedings of International conference on security and management*. Las Vegas, NV, 2003.

[10] 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.

[11] 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 USENIX Security Symposium*, 1999
[12] Alain Forget, Sonia Chiasson, and Robert Biddle, "Shoulder-Surfing Resistance with Eye-Gaze Entry in Cued-Recall Graphical Passwords", ACM 978- 1-60558-929-9/10/04, April 10 – 15, 2010.
[13] Chiasson, Forget, Biddle, van Oorschot "Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism" IEEE Transactions on Dependable And Secure Computing, VOL. 9, NO. 2, March/April 2012
[14] Chiasson, Forget, Biddle, van Oorschot "Influencing Users Towards Better Passwords: Persuasive Cued Click-Points" Published by the British Computer Society2008.
[15] Elizabeth Stobert, Alain Forget, Sonia Chiasson,Paul van Oorschot, Robert Biddle "Exploring Usability Effects of Increasing Security in Click-based Graphical Passwords" ACSAC '10 Dec. 6-10, 2010, Austin, Texas USA
[16] Dinei Florencio and Cormac Herley "A Large-Scale Study of Web Password Habits", International World Wide Web Conference Committee, 2007
[17] K. Renaud. Guidelines for designing graphical authentication mechanism interfaces. International Journal of Information and Computer Security, June 2009.