International Journal of Innovative Research in Engineering Science and Technology
APRIL 2018 ISSN 2320 –981X

SECURING THE FILE SYSTEM USING IMAGE AUTHENTICATION

[1]Ms. Aiswarya.G, [2]Ms. Mathangee.A.S, [3]Ms.Meena.E

1.Department of Computer Science and Engineering,
Vivekanandha College of Engineering for Women,
Tiruchengode-637205
ishwaryaishu21@gmail.com

2.Department of Computer Science and Engineering,
Vivekanandha College of Engineering for Women,
Tiruchengode-637205
mathangee.a.s.@gmail.com

3.Department of Computer Science and Engineering,
Vivekanandha College of Engineering for Women,
Tiruchengode-637205
meenagowri97@gmail.com

CORRESPONDING AUTHOR:
Mrs. Gayathri.J, ME.,
Asst. Professor, Vivekanandha College of Engineering for Women,
Tiruchengode-637205
Email: gayathri@vcew.ac.in
Contact:8110990696

Abstract-A Graphical Based Password is one alternative for textual password. Graphical input devices enable the user to decouple the position of inputs from the temporal order in which those inputs occur, and we show that this decoupling can be used to generate password schemes with substantially larger password spaces. Users click on one point per image for a sequence of images. The next image is based on the previous click-point. Performance was very good in terms of speed, accuracy, and number of errors. CCP also provides greater security than Pass Points because the number of images increases the workload for attackers.

Keywords: Graphical Passwords, Computer Security, Authentication, Usable Security, Draw a secret (DAS), Cued Click Point (CCP).

I.INTRODUCTION

Passwords provide security mechanism for authentication and protection services against unwanted access to resources. Nowadays a security is a major issue to maintain our account over internet. So to prevent from security issue, security for our account and files is implemented by using graphical password using our own image. Text passwords and personal identifications numbers (PIN's) are the overriding easy method as they are plain and can be set up on systems easily. Textual password has been the most widely used authentication methods for decades because these are comprised of numbers, upper and lower-case letters. Textual passwords are considered strong enough to resist against brute force attack. However a strong textual password is hard to memorize and recollect. Therefore users tent to choose passwords which are small, password are suffered due to limited security and also it is very difficult to guess or hard to retain information. To overcome these problems, people adopt new methodology which is non-secure coping strategies like reusing the passwords mitigating this problem, to being a new solution or methodology for secure the password. We develop new graphical password scheme that rely on input such as cropping a portion of an image.

II.OBJECTIVES

1. Input Design is the process of converting a user-oriented description of the input into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system.

2. It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities.

3. When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the user will not be in maize of instant. Thus the objective of input design is to create an input layout that is easy to follow.

III. LITERATURE SURVEY

L. Sobrado and J.C. Birget, "Shoulder-surfing resistant graphical passwords,"

When customer feedback their security passwords in a community place, they may be at chance of assailants taking their security password. An enemy can catch a security password by direct statement or by documenting the individual's verification period. This is generally known as shoulder-surfing and is a known threat, of special concern when authenticating in community venues. Until recently, the only protection against shoulder-surfing has been cautious on the part of the customer. This paper reviews on the design and assessment of a game-like visual method of verification that is immune to shoulder-surfing. The Convex Shell Just click (CHC) plan allows a customer to confirm knowledge of the visual security password securely in a vulnerable location because customers never have to click straight on their security password pictures. Functionality examining of the CHC plan revealed that beginner customers were able to get into their visual security password perfectly and to remember it eventually. However, the protection against shoulder-surfing comes at the price of many years to carry out the verification.

S Wiedenbeck, J. Waters, L. Sobrado, and J. C. Birget, "Design and evaluation of a shoulder-surfing resistant graphical password scheme,"

In this document, we have provided a new strategy to secure user's password against malware strike. Our primary participation is that we present CAPTCHA into the world of visual protection passwords. From the protection perspective, this discovery is predicted to advance the growth of visual protection passwords. While the design of CAPTCHA is an interdisciplinary subject and the present collective knowing of this subject is still in its beginnings, we do not declare that our plan is definitely possible instantly. But, as long as the state-of-art-algorithms

cannot fix the difficult AI problems, it is potential to create a visual protection password plan with CAPTCHA that is highly immune to malware.

B. Hartanto, B. Santoso, and S. Welly, "The usage of graphical password as a replacement to the alphanumerical password,"

The weaknesses of the textual security password have been well known. Customers usually pick short security passwords or security passwords that are memorable, which makes the security passwords insecure for assailants to break. Furthermore, textual security password is susceptible to shoulder-surfing, hidden-camera and malware strikes. Visual security password techniques have been suggested as a possible alternative to text-based plan. However, they are mostly susceptible to shoulder-surfing. In this document, we recommend a Scalable Shoulder-Surfing Proof Textual-Graphical Password Verification Scheme (S3PAS). S3PAS easily combines both graphical and textual security password techniques and provides nearly perfect safe from shoulder-surfing, hidden-camera and malware strikes. It can substitute or exist together with traditional textual security password systems without modifying current customer security password information. Moreover, it is safe from brute-force strikes through powerful and unpredictable period security passwords. S3PAS reveals significant potential connecting the gap between traditional textual security password and graphical security password. Further improvements of S3PAS plan are suggested and temporarily mentioned. Theoretical research of the security level using S3PAS is also examined.

IV. GRAPHICAL PASSWORDS

A graphical password is an authentication system that works by having the user select from images, in a specific order, presented in a graphical user interface. A graphical password is easier than a text-based password for most people to remember. Graphical passwords offer better security than text-based passwords because many people, in an attempt to memorize text-based passwords, use plain words.

GRAPHICAL AUTHENTICATIONS TECHNIQUES

The graphics authentication techniques can further be divided into two categories of graphical techniques:

- Recognition based
- Recall based

RECOGNITION BASED

Recognize image in the viewfinder and overlay it with image further more it shows how to recognize different images and how to react on user clicks on the overlaid elements.

RECALL BASED

We would discuss two types of picture password technique in this section:

- Reproducing a drawing
- Repeating a selection

REPRODUCING A DRAWING

Jermyn proposed a technique, called "Draw-A-Secret (DAS)", which allows the user to draw their unique password. The basic concept behind Draw a Secret (DAS) is that humans excel at image recognition and memory, so "passwords" should be designed to leverage that ability. Initial implementations simply tracked the ability of people to use a stylus to draw a free-form shape on a touch- sensitive screen. But the people behind the new work have previously refined the technique by parsing the shapes with a flexible grid, which allowed them to more accurately recognize key features such as changes in the stroke's direction. The primary limitation of this DAS system is the user's ability to accurately redraw a complex shape from memory

REPEATING A SELECTION

Blonder designed a graphical password scheme in which a password is created by having the user click on several locations on an image. During authentication, the user must click on the approximate areas o those locations. Pass point has developed a graphical password system based on this idea. In their implementation the users must click on various items of the image in the correct sequence in order to be authenticated. The "Pass Point" system by Wiendenback extended Blunder's idea by eliminating the predefined boundaries and allowing arbitrary images to be used. As a result, a user can click on any place on an image (as opposed to some pre-defined areas) to create a password. This technique is based on the discretization method proposed by Brigit. Adrian Perrig was reported to be working on a system (called Map

Authentication) that was based on navigating through a virtual world. In this system the user can build their own virtual world.

V. POSSIBLE ATTACKS ON GRAPHICAL PASSWORD TECHNIQUES

Graphical passwords are not widely used in practice. The possible techniques for breaking graphical pass-words are given below and a comparison with text-based passwords.

DICTIONARY ATTACKS

This is the major problem with the text based passwords. Recognition based graphical passwords involve the user to input using mouse instead of keyboard; it is impractical to carry out dictionary attacks against this type of graphical passwords. For some recall based graphical passwords, it is possible to use a dictionary attack but an automated diction-arty attack will be much more difficult than a text based dictionary attack.

GUESSING

This is the serious problem usually associated with the text based passwords. Graphical Passwords tend to predict. It is found that people often choose weak and Predictable graphical passwords. Similar predictability is found among the graphical passwords created with the DAS technique.

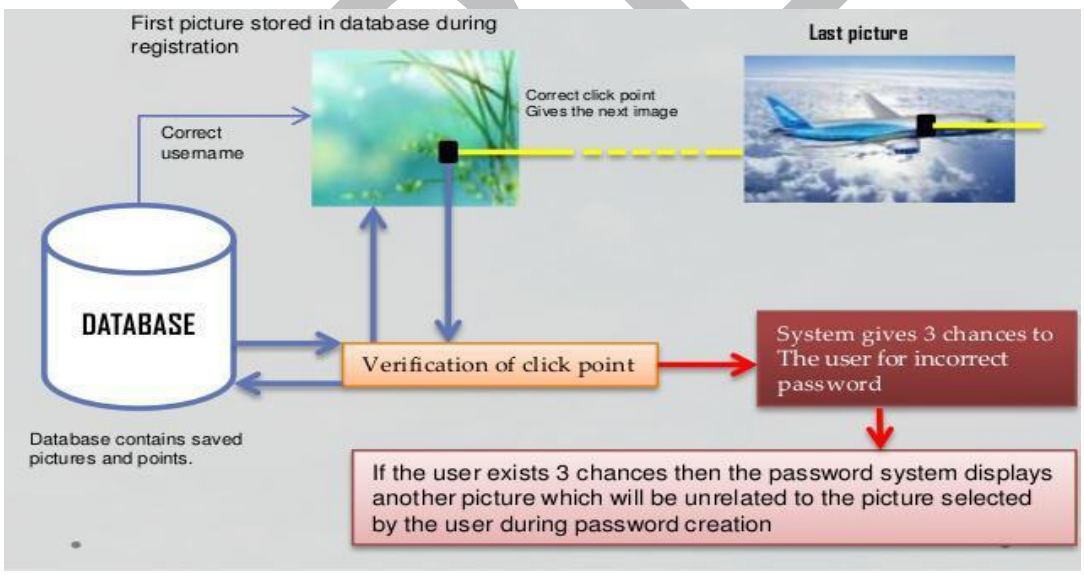
BRUTE FORCE ATTACK

In some graphical password techniques password space is similar to or larger than that of text-based passwords. The main defense against brute force attack is to have a sufficiently large password space. A brute force attack is difficult to carry against Graphical passwords than text-based passwords. Automatically generated accurate mouse movement is required in brute force attack to reproduce human input, which is mostly difficult in case of recall based graphical passwords.

VI. WORKING PRINCIPLE

In this process users click one point on each of 5 images rather than on five points on one image. It offers cued-recall and introduces visual cues that instantly alert valid users if they have made a mistake when entering their latest click-point. A wrong click leads down an incorrect path, with an explicit indication of authentication failure only after the final click. Users can choose their images only to the extent that their click-point dictates the next image. If they dislike the

resulting images, they could create a new password involving different click-points to get different images. For implementation, CCP initially functions like Pass Points. During password creation, a discretization method is used to determine a click-point's tolerance square and corresponding grid. For each click-point in a subsequent login attempt, this grid is retrieved and used to determine whether the click-point falls within tolerance of the original point. With CCP, we further need to determine which next-image to display. Using CCP as a base system, we added a persuasive feature to encourage users to select more secure passwords, and to make it more difficult to select passwords where all five click-points are hotspots. As with text passwords, Pass Points can only safely provide feedback at the end and cannot reveal the cause of error. Providing explicit feedback in Pass Points before the final click-point could allow Pass Points attackers to mount an online attack to prune potential password subspaces, whereas CCP's visual cues should not help attackers in this way. Another usability improvement is that being cued to recall one point on each of five images appears easier than remembering an ordered sequence of five points on one image.



System architecture

VII. CONCLUSION

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 decade's .Present-day attackers targeting such systems are empowered by having control of thousand to million nodes. 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). In contrast, PGRP is more restrictive against brute force and dictionary attacks while safely allowing a large number of free failed attempts for legitimate users. PGRP 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. PGRP appears suitable for organizations of both small and large number of user accounts.

REFERENCES

[1] Blonder, G.E. Graphical Passwords. United States Patent 5,559,961, 1996.

[2] Passlogix, "www.passlogix.com," last accessed in June 2005.

[3] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy and Nasir Memon, "Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice", SOUPS'05 Conference, July 6-8, 2005, Pittsburgh, PA, USA.

[4] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy and Nasir Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system", *International Journal of Human-Computer Studies* (Special Issue on HCI Research in Privacy and Security) 63, 102-127, 2005. - Elsevier Ltd, http://www.science<tirect.com.

[5] Jean-Camille Birget, Dawei Hong and Nasir Memon, uGraphical

Passwords Based on Robust Discretization", IEEE Transactions on Information Forensics and Security, Vol. 1, No.3, September 2006.

[6] L. D. Paulson, "Taking a Graphical Appraoch to the Password," *Computer*, vol. 35, pp. 19, 2002.

[7] Passfaces. http://www.realuser.com Last accessed: December 1, 2006.