International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 04 | Apr 2022 www.irjet.net p-ISSN: 2395-0072

Graphical Password by Image Segmentation

Eshita Agrawal[1], VijayKumar A[2]

[1]PG Student, School of computer science & IT, Jain (Deemed-to-be University), Bangalore
[2]Professor, School of computer science & IT, Jain (Deemed-to-be University),Bangalore.

Abstract- **The most common computer authentication method is using alphanumeric usernames and passwords. It has been shown that this method has significant disadvantages. For example, users tend to choose passwords that are easy to guess. On the other hand, when a password is hard to guess, it's often hard to remember. To address this problem, some researchers have developed authentication methods that use images as passwords. In this article, this paper provides a comprehensive overview of existing graphical password techniques. These techniques fell into two categories: recognition-based and memory-based approaches. Later the strengths and limitations of each method and point out future research directions in this area will be discussed in detail. This project also tries to answer two important questions: "Are graphical passwords as secure as text-based passwords?"; "What are the main problems in the design and implementation of graphical passwords?" This survey is useful for information security researchers and professionals interested in finding an alternative to text-based authentication methods.**

Keyword: ***recognition-based approach, memory-based approaches***

1. INTRODUCTION

[1]The different kinds of passwords used today are mainly based on recognition and recall, just to name a few. In recall based, someone is needed to regenerate the password, he keep at the time of registration method. The disadvantage during this process is that it depends on recall of password and if the user does an error the authentication is denied.

In the recall-based process, chances are somebody will replicate equivalent projected password "Draw a Secret" in which users are asked to draw some text or shape on a grid.

On the opposite side, the recognition based technique, a group of pictures that consists of a set of pass images is given to the user which they are asked to acknowledge and determine their pass image was chosen at the time of registration.

[2]The other technique of user access is that user should choose a low resolution image that was preserved earlier. This was projected by Hayashi, et al. The oil painting filter helps in decreasing the standard of the original image which was chosen by the user throughout the initial registration phase. This process is most helpful within the device with a decent color display.

[3]'Deja vu' is another visual image technique that was introduced by Dhamaija and Perrig. During this method, user is given some random pc generated pictures and the user must choose the pass image. Throughout the authentication, the user has to select a similar pre-registered image to prove his identity.

In general, images of nature and animals are memorized easier than computer graphic images. Memory of the nature needs additional storage. However, Secure and usable graphical password is desired.

2. LITERATURE SURVEY

The paper proposes a method that lets in user to enter an image as a password and only the user knows what the image looks like as a whole. Upon receiving the image, the system segments it into a series of images and stores them accordingly. When the user next logs into the system, he will receive the segmented image in encrypted order. If the user now selects the parts of the image in an order to create the original image they submitted, the user is considered authentic. Otherwise the user will not get access.

The system uses image segmentation based on coordinates. The coordinates of the segmented image allow the system to fragment the image and store it in different parts. In effect, the system segments the image into a grid and stores each part in appropriate order but when logging in, the picture shows broken and messed up. At this point, only the user who provided the image knows what the actual image looks like and must move the pieces horizontally from left to right, one row at a time, according to the order the pieces were placed on the page place image. So, after a successful attempt, the user is granted access.

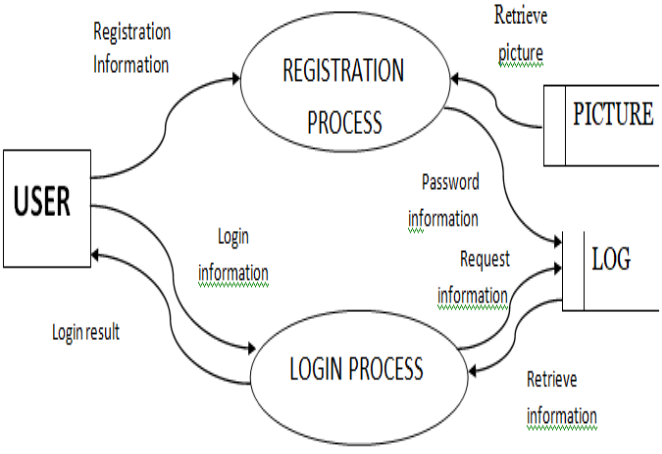
Modules and their Description

The system comprises of 5 Modules:

1. Image Submission
2. Image Fragmentation
3. Image parts storage
4. Part Jumbling
5. Authentication

Description:-

1. **Image Submission**
   - User can submit an image.
2. **Image Fragmentation**
   - System then fragments/divides the image into an 8x8 grid.
3. **Image parts storage**
   - The image parts are separated and stored accordingly.
4. **Part Jumbling**
   - The parts are then provides to user in a jumbled order.
5. **Authentication**
   - After selecting the parts in order of original image, a successful authentication is done else not.



2.1 Recognition Based Techniques

[4]Dhamija and Perrig proposed a graphical authentication scheme based on the hash visualization technique. In their system, the user is asked to choose a certain number of images from a series of random images generated by a program. Later, the user is prompted to identify the preselected images to be authenticated. The results showed that 90% of all participants were able to authenticate using this technique, while only 70% were successful with text-based passwords and PINs. However, the average login time is longer than the traditional approach. A weakness of this system is that the server must store the seeds of each user's portfolio pictures in plain text. In addition, the process of selecting a set of images from the image database can be lengthy.

[5]Sobrado and Birget developed a graphical password technique that addresses the problem of shoulder navigation. In the first scheme, the system displays a number of access objects (preselected by the user) among many other objects. For authentication, the user must recognize the access objects and click inside the convex hull formed by all the pass objects. To make the password difficult to guess, Sobrado and Birget suggested using 1000 objects, which makes the screen very crowded and the objects almost indistinguishable, but using fewer objects can result in a smaller password space because the resulting convex helmet is large can be. In your second algorithm, a user moves a box (and the objects it contains) until the step object in the box aligns with the other two step objects. The authors also suggest repeating the process a few more times to minimize the chances of accidentally clicking or spinning to sign you up. The main disadvantage of these algorithms is that the login process can be slow.

2.2 Recall Based Techniques

[6]Another shoulder-surfing resistant technique has been proposed. During this technique, a user selects variety of images as pass-objects. Every pass-object has many variants and every variant is allotted a singular code. Throughout authentication, the user is challenged with several scenes. Every scene contains several pass-objects (each within the variety of a randomly chosen variant) and plenty of decoy-objects. The user should type in a string with the unique codes such as the pass-object variants present in the scene in addition as a code indicating the relative location of the pass-objects in regard to a pair of eyes. [7]The argument is that it's terribly laborious to crack this sort of secret though the entire authentication method is recorded on video as a result of there's no click to grant away the pass-object information. However, this methodology still needs users to learn the alphanumerical code for every pass-object variant .Later extended this approach to allow the user to assign their own codes to pass-object variants. However, this method still forces the user to memorize many text strings and thus suffer from the numerous drawbacks of text-based passwords.

3. PROPOSED SYSTEM FOR GRAPHICAL PASSWORD BY IMAGE SEGMENTATION

Are graphical passwords are secure as text based passwords?

[8]Very little research has been done to examine the difficulty of cracking graphical passwords. Since graphics passwords are not widely used in practice, there are no reports of actual cases of graphics password cracking. Here we briefly examine some of the possible techniques for cracking graphical passwords and try to make a comparison with text-based passwords.

3.1 Brute force attack

[8]The most important protection against brute force searches is a sufficiently large password space. Text-based passwords have a password spacing of 94^N, where N is the length of the password and 94 is the number of printable characters without SPACE. Some graphical password techniques have been shown to provide a similar or larger password space than text-based passwords. Passwords based on graphical recognition tend to have smaller password gaps than recovery-based methods. Graphic passwords are more difficult to enforce than text-based passwords. Attack programs must automatically generate precise mouse movements to mimic human input, which is particularly difficult in graphical password recovery. In general, we believe that a graphical password is less susceptible to brute force attacks than a text-based password.

3.2 Dictionary Attack

[8]Since recognition based mostly graphical passwords involve mouse input rather than keyboard input, it'll be impractical to hold out dictionary attacks against this sort of graphical passwords. For a few recall based graphical passwords, it's doable to use a dictionary attack however an automatic dictionary attack are going to be rather more advanced than a text based dictionary attack a lot of analysis is required during this area. Overall, I believe graphical passwords are less liable to dictionary attacks than text-based passwords.

3.3 Guessing

[8]Unfortunately, it seems that graphical passwords are usually sure, a significant downside typically related to text-based passwords. For example, studies on the passface technique have shown that folks often opt for weak and predictable graphical passwords. Nali and Thorpe' study found similar certainty for graphical passwords created victimization the DAS technique. More analysis efforts are required to grasp the character of graphical passwords created by real users.

3.4 Spyware

With few exceptions, keylogging or keylistening spyware cannot be used to crack graphical passwords. It is not clear whether "mouse tracking" spyware will be an effective tool against graphical passwords. However, just moving the mouse is not enough to crack graphical passwords. The information must be correlated with application information such as window position and size and timing information.

3.5 Shoulder surfing

Like text primarily based passwords, most of the graphical passwords are prone to shoulder surfing. At this point, solely a couple of recognition-based techniques are designed to resist shoulder-surfing. None of the recall-based techniques are thought of shoulder-surfing resistant.

3.6 Social engineering

[8]Compared to text-based passwords, it is less convenient for a user to share graphical passwords with someone else. For example, it is very difficult to give graphic passwords over the phone. Setting up a phishing website to retrieve graphical passwords would be more time consuming.

Overall, I think it's harder to break graphical passwords exploitation the traditional attack ways like brute force search, dictionary attack, and spyware. There's a requirement for a lot of in-depth analysis that investigates potential attack methods against graphical passwords.

4. REVIEW AND DISCUSSIONS

What are the main problems in the design and implementation of graphical passwords?

4.1 Security

In the previous section, I have briefly examined the security problems with graphical passwords.

4.2 Usability

[9]One of the most complaints among users of graphical passwords is that the password registration and login method takes too long, particularly with detection-based approaches. For example, throughout the registration phase, a user must choose pictures from an oversized set of choices. Throughout the authentication phase, a user has to scan several images to spot some passwords. Users might feel that this process is long and tedious. For this reason, and conjointly as a result most users aren't acquainted with graphical passwords, they typically find graphical passwords less convenient than text-based ones.

4.3 Reliability

[9]The main design issue with recall-based methods is that the responsibleness and accuracy of recognizing user input. During this sort of method, error tolerances should be set carefully: too high tolerances will cause several false positives, whereas too low tolerances can lead to many negative errors. The additional fault-tolerant the program is, the more vulnerable it's to attacks.

4.4 Storage and communication

Graphical passwords need rather more space for storing than primarily text based passwords. Tens of thousands of images might need to be maintained in a very centralized database. Network transfer delay is additionally a concern for graphical passwords, particularly for recognition-based techniques within which an outsized range of pictures may have to be displayed for every round of verification.

5. CONCLUSION

Throughout this paper, a comprehensive research has been conducted of existing graphical password techniques. The present graphical password techniques might even be classified into two categories: recognition-based and recall-based techniques.

In conclusion, this study of Image segmentation shows its pros and cons. Without any difficulty Graphical password users might be able to create a valid password; however they might need to shell out more storage area than alphanumeric users, taking more trails and time. An interesting thing with the usage of Image Segmentation is that it consists both conflicting necessities is that it is simple to bear in mind and hard to guess.

[10]Preliminary study suggests that it's tougher to interrupt graphical passwords using the standard attack methods like brute force search, dictionary attack, or spyware. However, since there's not any wide usage of graphical password systems, the vulnerabilities of graphical passwords are still not totally understood.

In future it has great scope. Security of this system can be increased by increasing the number of levels used, the number of tolerance squares used.

Challenge response interaction can be added-

In challenge response interactions, server will present a challenge to the client and the client need to give response according to the condition given. If the response is correct then access is granted.

Adding limitation on number of attempts-

Limit the number a user can enter the wrong password.

REFERENCES

[1] Xiaoyuan Suo Ying Zhu G. Scott. Owen “Graphical Passwords: A Survey” 21st Annual Computer Security Applications Conference (ACSAC 2005), 5-9 December 2005, Tucson, AZ, USA.

[2] Rohitkumar Kolay, Animesh Vora, Vinaykumar Yadav “Graphical Password Authentication Using Image Segmentation” International Research Journal of Engineering and Technology (IRJET)

[3] Maw Maw Naing | Ohnmar Win "Graphical Password Authentication using image Segmentation for Web Based Applications" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-4, June 2019

[4]http://searchsecurity.techtarget.com/definition/graphical-password

[5]http://www.google.co.in/url?sa=t&rct=j&q=&esrc=s&source=web&cd=8&ved=0CEsQFjAH&url=http%3A%2F%2Fclam.rutgers.edu%2F~birget%2FgrPssw%2Fsusan3.pdf&ei=_HPdUsH5CI7xrQe87IEo&usg=AFQjCNGUZJ80lCOHxp2_W_KeAq2a-pGF3w&bvm=bv.59568121,d.bmk

[6] Blonder, G. 1996. Graphical Passwords. United States Patent5559961.

[7] Wiedenbeck, S., Waters, J., Birget, J. C., Brodskiy, A., andMemon, N. 2005. Authentication using graphical passwords:Effects of tolerance and image choice. In *Proc. Symp. OnUsable Privacy and Security (SOUPS’05)*.

[8] Chiasson, S., van Oorschot, P. C., and Biddle, R. 2007. A second look at the usability of click-based graphicalpasswords. In *Proc. Symp. on Usable Privacy and Security(SOUPS’07)*.

[9] Dirik, A., Menon, N., and Birget, J. 2007. Modeling userchoice in the PassPoints graphical password scheme. In *Proc.Symp. on Usable Privacy and Security (SOUPS’07).*

[10] A Balamurali, M V R Harsha,V Sai Hitesh, A Sai Chaitanya ” Graphical Password by Image Segmentation” International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8, Issue-6S4, April 2019

4.1Is a graphical password as secure as text-based password?