Recognition and Recall based Graphical Password Authentication

I.Sarfraz Ahmed, S.Vivek

II Year Computer Science and Engineering
S , Coimbatore
isarfarazahamed@gmail.com

Abstract— **Now a days, Internet has become the essential requirement for most of the people. Online payment and transaction has been made in our day-to-day activities. Human Interaction with computers and smartphones through several applications become unavoidable for which authentication is mandatory to secure the user's information against Cybercrime. User authentication is the most fundamental component in all computer security systems. Thus the primary goal of this paper is to provide secure authentication that guards against hacking. It also explores the information about strengths and weaknesses of passwords. The secondary goal is to bring awareness in mass about the possible threats they can suffer from and provide solutions by keeping a strong password and to introduce a new idea of presenting graphical authentication.**

***Keywords*— Graphical Password, Recognition, Recall, Authentication, Security**

I. Introduction

Security experts and researchers have made their determinations to guard the systems and individual users' personal data. Due to the increase in the usage of internet and networked systems, threats over them are getting increased day by day. Thus, there is an abundant need for securing and protecting the user from such wicked activities.

Generally, the username and password is the basic authentication for any applications irrespective of the application which may be small or huge, standalone or networked, web portal or online transaction. Alphanumerical usernames and passwords is the commonly used for any authentication purpose. However, from various analysis it is found that the user can evoke only a limited number of passwords.

As a result, to avoid the complexity of remembering the password, they choose a simple and easy password. Either they have a habit of writing the passwords somewhere in their dairy or use the same or similar passwords for different accounts at different applications. As an alternative, Biometrics are used which is one of the unique identity to increase the security but it requires lot of investments [1], [2]. To increase security to next level, some researchers have established authentication methods that use pictures as passwords or some other second level authentication.

II. NEED FOR PASSWORD PROTECTION

A password is an information associated with an entity that confirms the entity's identity. A password is an undisclosed word known only to the user. A password delivers access to a service for a specific user based on proved identity of the user. However, if the password is seized, predicted or stolen, someone could impersonate user and can do any activities such as sending emails, take money from bank account and even more. Sometimes, passwords can provide diverse access permissions to different users.

In general, anybody can access any data or information if password is not allotted but requiring a username and password to access various sensitive areas allows you to restrict access to only a chosen few people who know the secret codes. Thus, password protection is very important for any type of computer related activities.

III. ATTACK SCENARIOS

A number of password cracking exist. The following sub-sections discuss the general ways of password cracking methods and their applicability.

A. Password Guessing

This is a technique in which the attacker usually guesses the users' passwords arbitrarily until one password works. Password guessing will be much easier if the attacker knows the personal information or some other passwords of the user. Investigations and analysis conclude that the many of the users choose their family member names, personal information and favourite games as their password. Also, due to lack of awareness, they make their personal details open [3].

Conversely, Password guessing is not very effective and sophisticated technique to crack passwords since sometimes, it may not end up with successful cracking. Similarly, it will take long time and requires huge amounts of network bandwidth considerably. It is easily noticed and stopped. More techniques such as brute force mechanism, phishing etc are available in market.

B. Key loggers

A Key logger is a method of tracing the key hits on a keyboard by a user. The attacker will trace the password without the knowledge of the user. Every key that is pressed are recorded and finally it reveals the password and even discloses the personal information about the user. Now, the case become even worse due to technological development with which the abilities of capturing the screen and sending mail have been added [4]. These are also names as spywares [5], [6].

Even any machine with internet connection in public could execute a key logger. The public user cannot determine the trustworthiness of the system. In some system, the online virtual keyboards are available however, there is no alternative pressing the keys for a password. Key logging is one of the most threatening attacks since it executes as a background process that cannot be identified and indeed collects the user's personal information such as passwords, Account Number, credit card number etc.

C. Brute Force Approach

A brute force attack is an attack on a password, where all possible character combinations are tried until the correct one is found. A major advantage of this method is that it is possible to find the correct password after a complete cycle [7]. However, it is not possible to work out manually since increase in the number of characters increase the complexity and so manual try become ineffective. For short passwords, it will give the effective results. However, for long passwords, the program can be written and executed which takes short time to complete. The technique is easy to implement and practically fast, since pre-computation is not necessary in determining the passwords. Also, since the execution is linear, it is easy to stop the cracking process and can continue later.

D. Phishing

Phishing, also referred to as brand spoofing or carding, is a variation on “fishing,” the idea being that bait is thrown out with the hopes that while most will ignore the bait, some will be tempted into biting. It is an act of sending an e-mail to the user claiming to be an established legitimate organization in an attempt to scam the user and make them to surrender their private information that will be used for identity theft [8]. Generally, the link in the e-mail directs the user to visit a website where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers that the legitimate organization already has. Using techniques and tools used by Spammers, Phishers can deliver specially crafted emails to millions of legitimate live email addresses within a few hours (or minutes using distributed Trojan networks).

IV. Graphical Password

Graphical passwords are an alternate to alphanumeric passwords in which users click on images to authenticate themselves rather than typing alphanumeric words [9]. Graphical passwords are more memorable compared to the alphanumeric passwords, because it is easier to remember an image of flower than a set of alphabets and numbers. Several psychological studies have recognized that human brains have outwardly higher memory to distinguish and recall graphic information like photos in contrast to verbal or text based information [10].

Suppose an 8-character password is necessary to gain entry into a particular computer network. Instead of w8KiJ72c, for example, a user might select images of the earth (from among a screen full of real and fictitious planets), a tree near the house, a living things from the picture, a bottle of grape juice, and a particular bangle from the set of jewels.

Using images instead of characters will also support the user to increase the security as the alphanumeric corpus size is limited. A dictionary search can often hit on a password and allow a hacker to gain entry into a system in seconds. But if a series of selectable images is used on successive screen pages, and if there are many images on each page, a hacker must try every possible combination at random.

If there are 100 images on each of the 8 pages in an 8-image password, there are 1008, or 10 quadrillion (10,000,000,000,000,000), possible combinations that could form the graphical password! If the system has a built-in delay of only 0.1 second following the selection of each image until the presentation of the next page, it would take (on average) millions of years to break into the system by hitting it with random image sequences. Thus, in the case of graphical password, the size of the corpus is infinity if it is in the case of multiple numbers of images or if it is in the case of multiple points in a single image [11]. We can use only 26 alphabets and 10 numbers in the case of alphanumeric password, but in the case graphical password the corpus size is not limited.

Graphical passwords techniques are categorized into two main techniques: recall-based and recognition-based graphical techniques.

In recognition-based techniques, Authentication is done by challenging the user to identify image or images that the user had selected during the registration stage. Another name for recognition-based systems is search metric systems. It is generally require that users memorize a number of images during password creation, and then to log in, must identify their images among them [12].

In recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage [13], [14]. According to the survey presented by Suoet al. [15], several techniques have been proposed based on these two techniques that has various disadvantages. This paper presents the hybrid method that makes use of both the techniques.

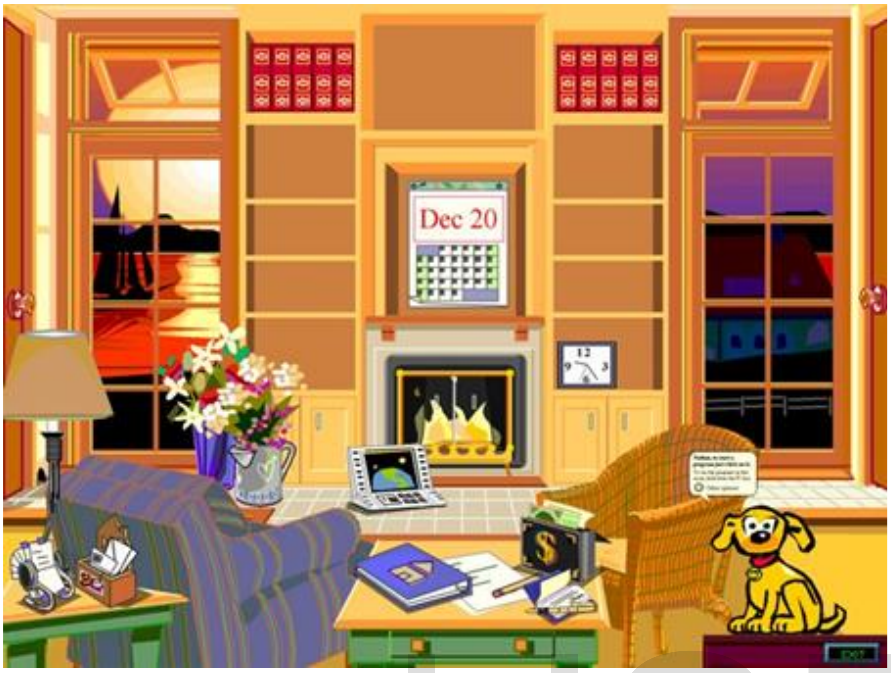
V. Recognition AND Recall based System

In this paper, a hybrid method has been proposed that uses both recognition based and recall based technique for password authentication.

In the proposed system is designed using 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 of previously selected locations. The image can assist users to recall their passwords and therefore this method is considered more convenient. In our implementation, the image is given to the user. During registration, user must click on various items in the image. For each selected are, the users are requested to enter the question related to that object and they are supposed to provide the answer for the same. In this example, the user is requested to select the 3 objects along with the question and answer related to those objects.

Thus, during their authentication process, user must click the pre-selected objects in the image in any order. For each selected object, the questions that they have entered during their registration phase will be displayed and they are supposed to recall and type the correct answer. The main advantage of this method is that the selected objects can be clicked in any order. Also, the users can answer them easily since the questions are framed only by them which helps to remember them.

Fig 1 is an illustration for the proposed method. The image has various objects and the user selected object is marked with a circle and given a number for each selected to match with the questions. The questions and answers for all the selected objects are also given.



1. Question : What is your Pet Name?
   Answer : puppy
2. Question : What is your favourite flower?
   Answer : jasmine
3. Question : What is your month of birth?
   Answer : january

roposed method

VI. FEW MEASURES FOR SECURING THE PASSWORD

Here is a list of few measures taken if you land somewhere wrong.

- If you believe there is a risk your password/s have been captured by another person (accidentally or deliberately) change the affected password/s immediately.
- If you believe there is a risk your passwords have become compromised due to malware, immediately change your passwords for all of your online accounts on a different, uninfected computer. Do not enter any passwords on your computer until it has been cleaned of malware. If you enter your new passwords on your infected computer, they will be immediately captured in the same way as the old passwords. Refer to professionals that will help you to remove malware from your computer.
- Always give significance to change the passwords for accounts that are most imperative and treasured.
- A long password with alphanumeric characters are strongly acceptable than the weak small passwords.

VII. CONCLUSIONS

tection is first and sometimes last line of defense.
to aware the people about some of the possible
vords and some measures to prevent them from
stolen. Password cracking programs are growing
there are many discussions pertaining to their
blem is not their existence but the misuse of them.
e a habit of using strong passwords which reduces
f password being hacked. Graphical passwords are
olution against cracking. The proposed solution
omp structure for the hackers to guess and
curity when compared to the existing solutions. In
d like to implement the method in online sites and
plexity of the proposed method by comparing the
sting techniques using various parameters such as

VIII.

IX.

X.

XI.

XII.

XIII.

XIV.

XV.

XVI.

XVII. REFERENCES

[1] K. Gilhooly, "Biometrics: Getting Back to Business," in Computerworld, May 09, 2005.

[2] A. Jain, L. Hong, and S. Pankanti, "Biometric identification," Communications of the ACM, vol. 33, pp. 168-176, 2000.

[3] D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes," in Proceedings of the 13th Usenix Security Symposium. San Diego, CA, 2004.

[4] Doja, M. N., & Kumar, N. (2008, August). Image authentication schemes against key-logger spyware. In Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2008. SNPD'08. Ninth ACIS International Conference on (pp. 574-579). IEEE.

[5] D. Hong, S. Man, B. Hawes, and M. Mathews, "A password scheme strongly resistant to spyware," in Proceedings of International conference on security and management. Las Vergas, NV, 2004.

[6] 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.

[7] J.-C. Birget, D. Hong, and N. Memon, "Robust discretization, with an application to graphical passwords," Cryptology ePrint archive 2003.

[8] Dhamija, R., Tygar, J. D., & Hearst, M. (2006, April). Why phishing works. In Proceedings of the SIGCHI conference on Human Factors in computing systems (pp. 581-590). ACM.

[9] De Angeli, L. Coventry, G. Johnson, and K. Renaud, "Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems," International Journal of Human -Computer Studies, vol. 63, no. 1-2, pp. 128–152, 2005.

[10] Kirkpatrick, "An experimental study of memory," Psychological Review, vol. 1, pp. 602–609, 1894.

[11] S. Madigan, "Picture memory," in Imagery, Memory, and Cognition: Essays in Honor of Allan Paivio, J.Yuille, Ed. Lawrence Erlbaum Associates, 1983, ch. 3, pp. 65–89.

[12] K. Renaud and E. Smith. Jiminy: "Helping user to remember their passwords". Technical report, School of Computing, Univ. of South Africa, 2001.

[13] J. Thorpe and P. C. v. Oorschot, "Graphical Dictionaries and the Memorable Space of Graphical Passwords," in Proceedings of the 13th USENIX Security Symposium . San Deigo, USA: USENIX, 2004.

[14] 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.

[15] Suo, X., Zhu, Y., & Owen, G. S. (2005, December). Graphical passwords: A survey. In *Computer security applications conference, 21st annual* (pp. 10-pp). IEEE.

[16] A.Suresh (2016), "Speech Stress Analysis based on Lie Detector for Loyalty Test", in International Journal of Printing, Packaging & Allied Sciences,(IJPPAS) ISSN: 2320- 4387, *Vol. 04, No.01, December 2016,* pp.*631* – 638.