International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622
International Conference on Industrial Automation And Computing (ICIAC- 12th & 13th April 2014)

RESEARCH ARTICLE OPEN ACCESS

Analysis of Graphical Based Password

Vishal S Ramteke
Information Technology
Y.C.C.E
Nagpur, India
vishal.s.ramteke@gmail.com

prof .Amol d Gaikwad
Information Technology
Y.C.C.E
Nagpur, India
amolgaikwad.ag@gmail.com

Abstract—
Passwords provide security mechanism for authentication and protection services against unwanted access to resources. For such authentication generally text (alphanumeric) is used. It is well-known, however, that passwords are susceptible to attack: users tend to choose passwords that are easy to remember, and often this means that they are also easy for an attacker to obtain by searching for candidate passwords. A graphical based password is one promising alternatives of textual passwords. In this paper, we conduct a comprehensive survey of the existing graphical password techniques and proposed a new technique. We discuss the strengths and limitations of each method and point out the future research directions in this area and also major design and implementation issues are clearly explained. Our scheme is resistant to shoulder surfing attack and many other attacks on graphical passwords.
Our technique is very useful for any computer related application such as web authentication, desktop &laptop logins, critical servers.
Keywords— graphical password, authentication, hack, security.

I. INTRODUCTION

One of the major functions of any security system is the control of people in or out of protected areas, such as physical buildings, information systems, and our national borders. Computer systems and the information they store and process are valuable resources which need to be protected. Computer security systems must also consider the human factors such as ease of a use and accessibility. Current secure systems suffer because they mostly ignore the importance of human factors in security. An ideal security system considers security, reliability, usability, and human factors. A password is a form of secret authentication data that is used to control access to a resource. The password is kept secret from those not allowed access, and those wishing to gain access are tested on whether or not they know the password and are granted or denied access accordingly. The use of passwords goes back to ancient times. They would only allow a person in if they knew the password. Nowadays the most common computer authentication method to access to computer networks and systems is based on the use of alphanumerical usernames and passwords. Traditional strong password schemes could provide with certain degree of security; however, the fact that strong passwords being difficult to memorize often leads their owners to write them down on papers or even save them in a computer file. As a result, security becomes greatly compromised. Conventional passwords have been shown to have significant drawbacks. Users do not follow their requirements, for example; users tend to pick passwords that can be easily guessed (weak password) or choose meaningful words from dictionaries, which make textual passwords easy to break and vulnerable to dictionary or brute force attacks. On the other hand, if a password is hard to guess, then it is often hard to remember. Users have difficulty remembering a password that is long and random appearing. So, they create short, simple, and insecure passwords that are susceptible to attack.

Graphical passwords have been proposed as a possible alternative to textbased, motivated particularly by the fact that human can remember pictures better than text. Psychological studies have shown that people can remember pictures better than text (R.N Shepard 1987). Pictures are generally easier to be remembered or recognized than text, especially photos, which are even easier to be remembered than random pictures (Xiaoyuav Suo 2009). The idea of graphical passwords was originally described by Greg Blonder in 1996. An important advantage of GP is that they are easier to remember than textual passwords. Human beings have the ability to remember faces of people, places they visit and

things they have seen for a longer duration. This method has been categorized to recognition-based (image selection and click-based) and recall-based.. Usability and security should be considered simultaneously to achieve a good authentication system. Usability features are ease of use, ease to create, ease to memories, ease to learn and satisfaction of the overall system design and layout. User friendliness in both recognition and selection of pass-objects from the given images, familiarization or a lengthy password setup process can be counted under usability. Common security attacks like brute-force search, spy ware, shoulder surfing, social engineering, and forgery. Problems like requiring a large image database, uneasy to repeat mouse clicking at the same position, as well as images being too simple to cause collisions on points selected for different users, storage-efficient as all images are created when needed. Rather than optimizing the password space and the strength against brute force attacks because proposed graphical passwords are mostly vulnerable to shoulder-surfing overcoming this issue without adding any extra complexity into the authentication procedure is researcher's goal these days. Simply adopting graphical password authentication also has some drawbacks therefore some hybrid schemes based on graphic and text were developed. Thus, graphical passwords provide a means for making more user-friendly passwords while increasing the level of security.

II.OVERVIEW OF THE AUTHENTICATION METHODS

Due to recent events of thefts and terrorism, authentication has become more important for an organization to provide an accurate and reliable means of authentication. Currently the authentication methods can be broadly divided into three main areas. Token based (two factor), Biometric based (three factor), and Knowledge based (single factor) authentication [7], also shown in the Figure 1.

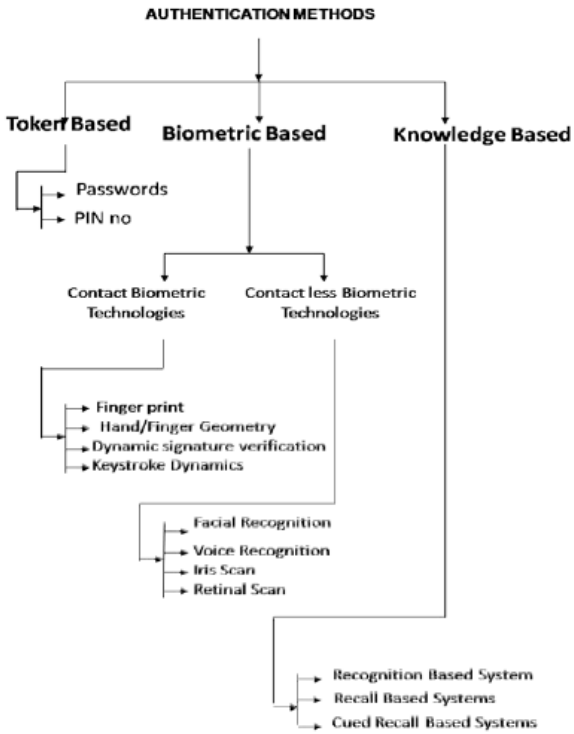


Fig. 1 Classification of Authentication Methods

2.1 Token Based Authentication:

It is based on "Something You Possess". For example Smart Cards, a driver's license, credit card, a university ID card etc. It allows users to enter their username and password in order to obtain a token which allows them to fetch a specific resource - without using their username and password. Once their token has been obtained, the user can offer the token - which offers access to a specific resource for a time period - to the remote site. Many token based authentication systems also use knowledge based techniques to enhance security. Knowledgebase techniques include both text-based and picture-based passwords. The picture-based techniques can be further divided into two categories: recognition-based and recall-based graphical techniques. Using recognition-based techniques, a user is presented with a set of images and the user passes the authentication by recognizing and identifying the images he or she selected during the registration stage. Using recall based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage.

2.2 Biometric Based Authentication:

Biometrics (ancient Greek: bios ="life", metron ="measure") is the study of automated methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits. It is based on "Something You Are". It uses physiological or behavioral characteristics like

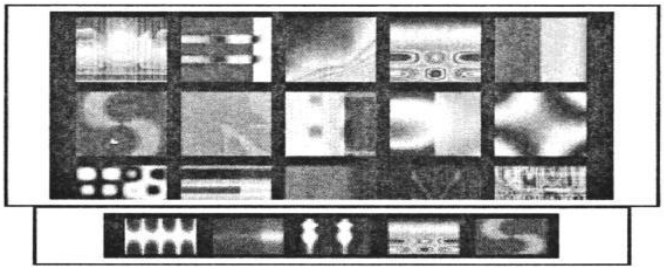
fingerprint or facial scans and iris or voice recognition to identify users. A biometric scanning device takes a user's biometric data, such as an iris pattern or fingerprint scan, and converts it into digital information a computer can interpret and verify. A biometric-based authentication system may deploy one or more of the biometric technologies: voice recognition, fingerprints, face recognition, iris scan, infrared facial and hand vein thermo grams, retinal scan, hand and finger geometry, signature, gait, and keystroke dynamics. Biometric identification depends on computer algorithms to make a yes/no decision. It enhances user service by providing quick and easy identification.

2.3 Knowledge Based Authentication:

Knowledge based techniques are the most extensively used authentication techniques and include both text based and picture based passwords. Knowledge-based authentication (KBA) is based on "Something You Know" to identify you For Example a Personal Identification Number (PIN), password or pass phrase. It is an authentication scheme in which the user is asked to answer at least one "secret" question. KBA is often used as a component in multifactor authentication (MFA) and for self-service password retrieval. Knowledge based authentication (KBA) offers several advantages to traditional (conventional) forms of e-authentication like passwords, PKI and biometrics.

II. RECOGNITION BASED TECHNIQUE

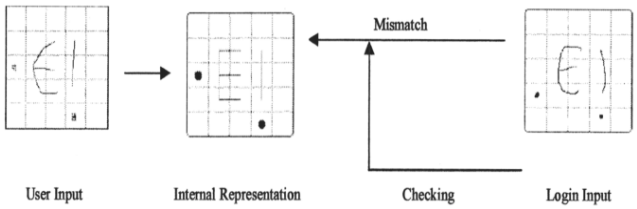
Dhamija and Perrig proposed a graphical authentication scheme based on the *Hash Visualization Technique.* In the system developed by them the user is asked to select a certain number of images from a set of random pictures which are generated by some program. Later, the user will be required to identify the pre-selected images in order to be authenticated. The drawback of this scheme is that the server needs to store a large amount of pictures which may have to be transferred over the network, delaying the authentication process. Another weakness of this system is that the server needs to store the seeds of portfolio images of each user in plaintext.



Also, the process of selecting a set of pictures from picture database can be tedious and time consuming for the user. This scheme was not really secure because the passwords need to store in database and that is easy to see.

III. RECALL BASED TECHNIQUE

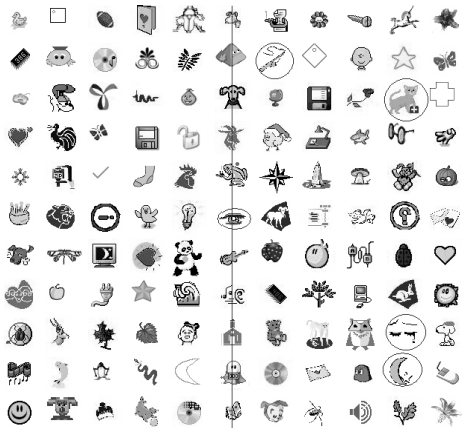
D Jermyn proposed a technique, called "Draw-A-Secret (DAS)", which allows the user to draw their unique password. The basic concept behind Draw a Secret (DAS) is that humans excel at image recognition and memory, so "passwords" should be designed to leverage that ability. Initial implementations simply tracked the ability of people to use a stylus to draw a free-form shape on a touch-sensitive screen



DAS scheme has some limitations like it is vulnerable to shoulder surfing attack if a user accesses the system in public environments, there is still a risk for the attackers to gain access to the device if the attackers obtained a copy of the stored secret, and, brute force attacks can be launched by trying all possible combinations of grid coordinates,) Drawing a diagonal line and identifying a starting point from any oval shape figure using the DAS scheme itself can be a challenge for the users, and finally Difficulties might arise when the user chooses a drawing which contains strokes that pass too close to a grid-line, thus, the scheme may not be able to distinguish which cell the user is choosing.

IV. PROPOSED TECHIQUE

When a user tries to register we will ask him to select a username and password as a sequence of images from already given frame. The local host downloads an image which consists of various themes of sequence of pictures which acts as password, those are given by server. When logging in, if the images selected by the user matches with those stored in encrypted form then server grants the user to enter the site.



IS A GRAPHICAL PASSWORD AS SECURE AS TEXT-BASED PASSWORD?

Very little research has been done to study the difficulty of cracking graphical passwords. Because graphical passwords are not widely used in practice, there is no report on real cases of breaking graphical passwords. Here we briefly exam some of the possible techniques for breaking graphical passwords and try to do a comparison with text-based passwords.

4.1 BRUTE FORCE SEARCH

The main defense against brute force search is to have a sufficiently large password space. Some graphical password techniques have been shown to provide a password space similar to or larger than that of text-based passwords. Recognition based graphical passwords tend to have smaller password spaces than the recall based methods. It is more difficult to carry out a brute force attack against graphical passwords than text-based passwords. The attack programs need to automatically generate accurate mouse motion to imitate human input, which is particularly difficult for recall based graphical passwords. Overall, we believe a graphical password is less vulnerable to brute force attacks than a textbased password.

4.2 DICTIONARY ATTCK

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 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.

4.3 SHOULDER SURFING PROBLEM AND ITS SOLUTION

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. None of the recall-based based techniques are considered should-surfing resistant. To overcome this shoulder surfing problem, we implement a new idea. When we move our mouse over the password selection area, then the mouse pointer becomes small dot point and another method is to rearrange the images randomly in the password selection image so that shoulder surfing problem can be reduced.

4.4 ADVANTAGE OF GRAPHICAL PASSWORD OVER TEXT BASED PASSWORDS

Graphical passwords may offer better security than text based password because many people in attempt to memorize text based passwords, use plain words(rather than recommended jumble of characters).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 a 8-image password, there are 100^8 or 10 quadrillion (10,000,000,000,000,000), possible combinations that could form the graphical password if the system has the built-in delay of only 0.1 second following the selection of each image until the selection of the next page it would take millions of years to break into the system by hitting it with random image sequences therefore hacking by random combination is impossible.

V. CONCLUSION & FUTURE WORK

The core element of computational trust is identity. Currently many authentication methods and techniques are available but each with its own advantages and shortcomings. There is a growing interest in using pictures as passwords rather than text passwords but very little research has been done on graphical based passwords so far. In view of the above, we have proposed authentication system which is based on graphical password schemes. Although our system aims to reduce the problems with existing graphical based password schemes but it has also some limitations and issues like the other entire graphical based password.

VI. ACKNOWLEDGMENT

We would like to acknowledge the support provided by our institution YCCE, Nagpur for successfully carrying out this work. We thank the

institution for all the facilities and infrastructure they provided us.

REFERENCES

[1] A S. Patrick, A C. Long, and S. Flinn, "HCI and Security Systems", presented at Cm, Extended Abstracts (Workshops). Ft Lauderdale, Florida, USA. 2003.

[2] 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 ACM*, vol. 42 pp. 41-46, 1999.

[3] R. Dhamija and A Perrig, "Deja Vu: A User Study Using Images For Authentication", 9th USENIX Security Symposium, 2000.

[4] A. Perrig and D. Song, "Hash Visualizations: A New Technique To Improve Real-World Security," in *Proceedings of the 1999 International Workshop on Cryptographic Techniques and E-Commerce, 1999.*

[5] S. Akula and V. Devisetty, "Image Based Registration and Authentication System," in *Proceedings of Midwest Instruction and Computing Symposium*, 2004

[6] D. Weinshall and S. Kirkpatrick, "Passwords You'll Never Forget, but Can't Recall," *in Proceedings of Conference on Human Factors in Computing Systems (CHI),* Vienna, Austria: ACM, 2004.

[7] L. Sabrado and J. C. Birget, "Graphical passwords", *The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research*, vol 4, 2002.

[8] 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.