Graphical User Authentication Techniques for Security: a Comparative Study

Harinandan Tunga, Diya Saha

Abstract- Nowadays, user authentication is one of the important topics in information security. Strong text-based password schemes could provide with certain degree of security. However, the fact that strong passwords are difficult to memorize often leads their owners to write them down on papers or even save them in a computer file. Graphical User Authentication (GUA) has been proposed as a possible alternative solution to text-based authentication, motivated particularly by the fact that humans can remember images better than text. In recent years, many networks, computer systems and Internet based environments try used graphical authentication technique for their user's authentication. All of graphical passwords have two different aspects which are usability and security. Different techniques for GUA have been proposed in literature over the past few years such as- Recognition Based Technique[2], Recall Based Technique[2]. This paper presents a survey of comparative study between different techniques of GUA.

Keyword- Graphical User Authentication, Recognition Based Techniques, Recall Based Techniques.

I. INTRODUCTION

Authentication is one the most important security primitive. Password authentication is most widely used authentication mechanism .Users generally use characters as passwords. But text based passwords are difficult to remember and if they are easy to remember then they are vulnerable to various kinds of attacks and are predictable. To address these authentication problems, a new alternative authentication method have been proposed using pictures as passwords. It is supported by the fact that Human brain has remarkable ability to remember thousands of images with detail. Whereas it difficult to keep text in memory. In Graphical authentication user performs some events on pictures like clicking, dragging, moving mouse authentication. 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 (GUI). For this reason, the graphical-password approach is sometimes called graphical user authentication (GUA).

II. OVERVIEW OF AUTHENTICATION METHOD

Authentication in the field of computer security is the process of attempting to verify the digital identity of the initiator of a communication, for example, a request to log in. The one being authenticated may not just be a person using a computer but it can be a computer itself or a computer program. A web trust uses "authentication" to ascertain that the users are who they say they are, basically making sure that the user who tries to perform functions in a system is, in fact, the user who is authorized to do so[1].

Revised Version Manuscript Received on June 30, 2015.

Harinandan Tunga, Department of Computer Science & Engineering, RCC Institute of Information Technology, Kolkata, India.

Diya Saha, Department of Computer Science & Engineering, RCC Institute of Information Technology, Kolkata, India.

Authentication methods can be divided into three main areas:

Token based techniques [8] such as key cards, bank cards and smart cards are widely used. security. For example, ATM cards are generally used together with a PIN number.

Fig1: Master Card

Biometric based authentication techniques [8] such as fingerprints, iris scan, or facial recognition, are not yet widely adopted. Such systems can be expensive, and the identification process can be slow and often unreliable. However, this type of technique provides the highest level of security.

Fig2: Finger Prints

Knowledge based techniques [8] are the most widely used authentication techniques and include both text-baseband picture based passwords. The picture-based techniques can be further divided into two categories recognition-based and recall based graphical technique.

Fig3: Picture Based.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

III. GRAPHICAL PASSWORD (AN ALTERNATE TO TEST BASED PASSWORD)

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 (GUI). For this reason, the authentication method in which graphical images or pictures are used as a password is sometimes called graphical user authentication (GUA). Many techniques have been designed in the field of graphical password since 1996 [4].

Why Graphical Password?

Today, authentication technology is the main measure to guarantee information security, and the most common and convenient authentication method is alphanumeric password. GUA is a promising alternative to replace the traditional alphanumeric password way of authentication. The main motivation lies with the fact that the human brain is capable of remembering graphical or pictorial objects better than texts, even psychological studies support such assumptions. And also with the advancement of technology, we are now moving forward to using touch based devices such as mobile phones, tablets, and even touch screen monitors. So with this, the alphanumeric method is much more inconvenient in such touch based devices. So, the graphical method would allow the user to just touch the various regions in screen and get authenticated.

IV. METHODS OF GRAPHICAL PASSWORD

We know graphical images are more easily recalled then text. Graphical password system based on recognition and recall based are discussed.

A. *Recognition-Based Technique [2]:* In this type of technique, users will select pictures, logos or any symbols from pre-stored image. For authentication process user need to recognize the image, which he choose as a password[5]

B. *Recall-Based Technique [2]*: Again recall-based password authentication are categorize in two parts: Pure Recall Based Technique and Cued Recall Base.

   a) *Pure Recall-Based Technique [2]:* In this category, users need to reproduce their passwords without being given any hints or gesture. Although this category is easy and convenient, but it seems that users hardly can remember their passwords similar to DAS (1999) and Qualitative DAS (2007) [5].

   b) *Cued Recall-Based Technique[2*] : In this category, the technique proposed a framework of reminder, hints and gesture that help the users to reproduce their passwords or help users to make a reproduction more accurate similar to Blonder Algorithm (1996) and Pass-point (2005) [5].

V. RECOGNITION BASED TECHNIQUE

Recognition based technique require the user to identify and recognize the secret, or part of it, that the user selected before. Generally during password creation the users are required to memorize a series of images, and then must recognize their images from among decoys to log in.Various recognition based password schema are explained below:

A. *Dhamija and Perrig* [4] proposed a graphical authentication scheme based on the Hash Visualization technique. In their authentication system, user selects a certain number of images from a set of program generated random pictures (Figure4). For a user to be authenticated, he or she would have to identify the pre-selected images. One weakness of their system is that the server needs to store the seeds of the selected images of each user in plain text. Also, it is a bit time consuming and tedious for the users to select images from the database.

B. *Akula and Devisettys algorithm* [4] is similar to the technique proposed by Dhamija and Perrig. The main difference is that they make the authentication more secure and require less memory. They did this by using hash function SHA-1, which produces a 20 byte output. The authors also suggested that this could be deployed on the Internet, cell phones and PDA's. Weinshall and Kirkpatrick[4] proposed and study several authentication schemes. They conducted a number of user studies. The various studies includes picture recognition, object recognition, and pseudo word recognition. In the picture recognition study, out of a database of 20,000 images, a large set of images are selected (100-200 images). Then the user is trained to recognize the set of images.

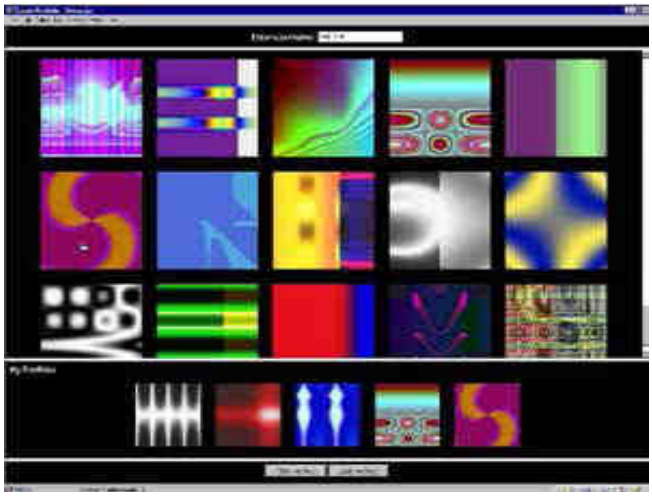

Fig4: Graphical Authentication scheme by Dhamija and Perrig[4]

C. *Sobrado and Birget* [3] developed a graphical authentication technique that is considered to be shall ensuring resistant. In the first scheme, the system will display a number of pass-objects (pre-selected by user) among many other objects. To be authenticated, a user needs to recognize pass-objects and click inside the convex hull formed by all the pass-objects (Figure 5). In order to make the password hard to guess, Sobrado and Birget suggested using 1000 objects, which makes the display very crowded and the objects almost indistinguishable, but using fewer objects may lead to a smaller password space, since the resulting convex hull can be large. In their second algorithm, a user moves a frame (and the objects within it) until the pass object on the frame lines up with the other two pass objects. The authors also suggest repeating the process a few more times to minimize the likelihood of logging in by randomly clicking or rotating. The major disadvantage of their scheme is that, the authentication phase or login

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

phase could be very slow.

D. *Triangle Scheme* [5] In 2002, Triangle algorithm proposed by a group which created several numbers of schemes which can overcome shoulder surfing attack. Their first scheme named, Triangle which is shown in Fig 5. In this method, the system randomly put a set of N objects which could be a hundred or a thousand on the screen. In addition, there is a subset of K objects previously chosen and memorized by the user. In other words, these K objects are the user passwords. During login the system will randomly select a placement of the N objects then the user must find three of his password objects and click inside the invisible triangle created by those three objects or click inside the convex hull of the pass objects that are displayed. In addition, for each login this challenge is repeated a few times using a different display of some of the N objects. Therefore, the probability randomly clicking in the correct region in each challenge is very low.

Fig 5: Triangle Scheme, 2002

E. *Movable Frame Scheme* [5], In 2002, this model produced using the same ideas and assumptions as Triangle scheme with the same designers. In this method the user must locate three out of K objects which these three are user passwords. As it is shown in Fig 6, only three pass objects are displayed at any given time and only one of them is placed in a movable frame.

Fig 6: Moveable Frame Scheme, 2002

F. *Man, et al.*[4] proposed another shoulder-surfing resistant algorithm. In their method, a user selects a number of pass-objects which are nothing but thumbnails of images. Each pass-object has several variants and each variant is assigned a unique code. During authentication, the user is challenged with several scenes. Each scene contains several pass-objects (each in the form of a randomly chosen variant) and many decoy-objects. The user has to type in a string with the unique codes corresponding to the pass-object variants present in the scene as well as a code indicating the relative location of the pass objects in reference to a pair of eyes. The argument is that it is very hard to crack this kind of password even if the whole authentication process is recorded on video because where is no mouse click to give away the pass-object information. However, this method still requires users to memorize the alphanumeric code for each pass-object variant. Hong, et al. later extended this approach to allow the user to assign their own codes to pass-object variants. Figure 7 shows the log-in screen of this graphical password scheme. However, this method still forces the user to memorize many text strings and therefore suffer from the many drawbacks of text-based passwords.

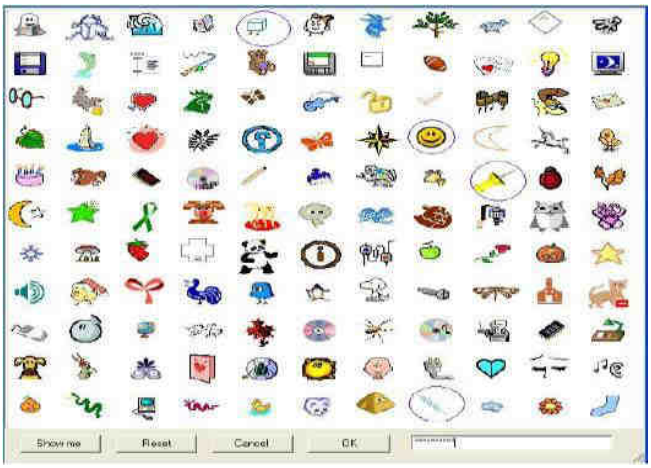

Fig 7: Man et al

G. *Passface Technique*[4]- it is supported by the fact that human brain can quickly recognize familiar faces. During registration user has to select 4 faces. The registration is complete if the user correctly identifies 4 passfaces two times consecutively. During login user is presented with a login screen consisting of grid of faces. User has to select 4 faces: one face from each of 4 grids of 9 faces. It has been cited by Davis et al. [3] Passfaces can be predictable as they are affected by race, gender and attractiveness.

Fig 8: Passface Graphical Authentication Scheme

H. *Jansen* [4] proposed a graphical password mechanism for mobile devices. During the enrollment stage, a user selects a theme (e.g. sea, cat, etc.) which consists of thumbnail photos and then registers a sequence of images as a password (Figure 9). During the authentication, the user must enter the registered images in the correct sequence. One drawback of this technique is that since the number of thumbnail images is limited to 30, the password space is small. Each thumbnail image is assigned a numerical value, and the sequence of selection will generate a numerical

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

password. The result showed that the image sequence length was generally shorter than the textural password length. To address this problem, two pictures can be combined to compose a new alphabet element, thus expanding the image alphabet size.

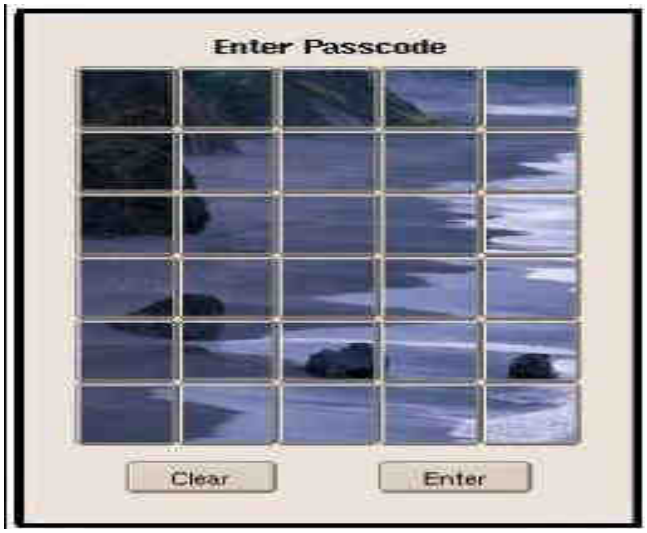

Fig 9: Graphical Authentication Scheme by Jansen Et Al

I. *Story Scheme*[5] In 2004, the story scheme proposed by categorizing the available picture to nine categories which are animals, cars, women, food, children, men, objects, nature and sport. According to Fig 10, the users have to select their passwords from the mixed pictures of nine categories in order to make a story easily to remember. There were some users who used this method without defining a story for themselves. This research showed that the story scheme was harder to remember in compare to Passface authentication[4].

Fig 10: Story Scheme, 2004

VI. RECALL BASED TECHNIQUE

In this section we discuss two types of picture password techniques: reproducing a drawing and repeating a selection. Recall-based password authentication are categorize in two parts:

A. *Pure Recall Based Technique*- In this procedure, a user generates his password without giving any clue or reminder. It follows many algorithms.

a) Draw-a-Secret(DAS)[8]- Reproduce a Drawing Jermyn, et al[8]. proposed a technique, called Draw-a-secret (DAS) [8], which allows the user to draw their unique password (Figure 11). A user is asked to draw a simple picture on a 2D grid. The coordinates of the grids occupied by the picture are stored in the order of the drawing. During authentication, the user is asked to re-draw the picture. If the drawing touches the same grids in the same sequence, then the user is authenticated. Jermyn, et al. Suggested that given reasonable-length passwords in a 5 X 5 grid, the full password space of DAS is larger than that of the full text password space.

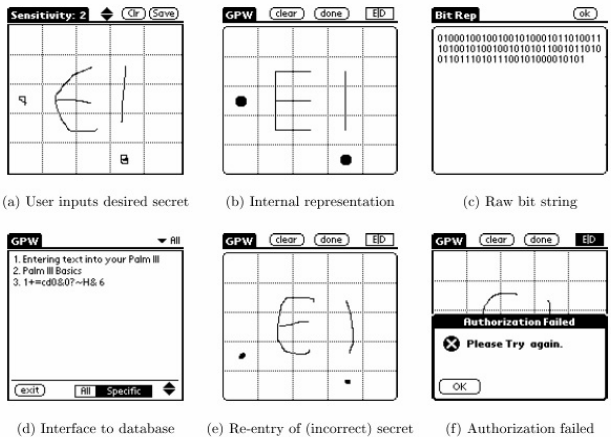

Fig 11: DAS authentication technique.

a) *Syukri, et al.* [8] proposes a system where authentication is conducted by having the user drawing their signature using a mouse (Figure 12). There are techniques included two stages, registration and verification. During the registration stage: the user will first be asked to draw their signature with a mouse, and then the system will extract the signature area and either enlarge or scale-down the signature, and rotates if needed, (also known as normalizing). The information will later be saved into the database. The verification stage first takes the user input, and does the normalization again,and then extracts the parameters of the signature. After that, the system conducts verification using geometric average means and a dynamic update of the database. According to the paper the rate of successful verification was satisfying. The biggest advantage of this approach is that there is no need to memorize ones signature and signatures are hard to fake.

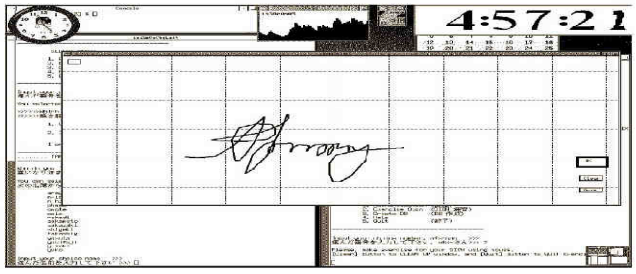

Fig 12: Signature drawn by mouse.

B. *Cued-Recall Based*- In the cued recall based technique, the image cues the user. For example to click a set of option a set of point on an image means hint and reminder help user to reproduce their passwords. It follows many algorithms, which are as followos:

a) Passlogix [6] has proposed various schemes

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

based on repeating a sequence of actions. In their v-Go scheme user has to select a background image e.g. kitchen, bathroom, bedroom and user can perform various actions with items present in image like clicking, dragging etc. Click on item is detected with the help of invisible boundaries on them. For example If kitchen is selected user can prepare meal by clicking and dragging cooking ingredients.

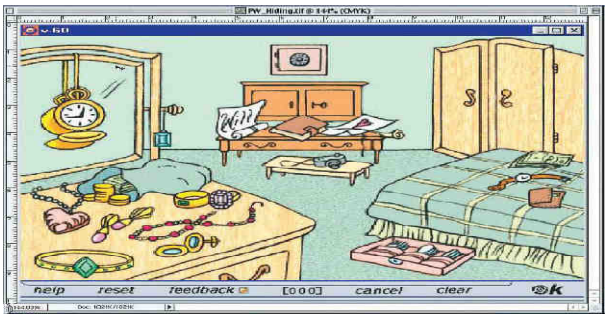

Fig13 A recall-based technique developed by Passlogix.

VII. SECURITY ANALYSIS OF GUA

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

Brute force attack [8] Text based passwords have password space of 94^N.It is difficult to do this attack on graphical passwords .We believe it is harder for this attack to succeed for graphical passwords. Recall based Password is more secure then recognition
based techniques when it comes to brute force attack. Draw-A-Secret is resistant to this attack all other authentication techniques are vulnerable to this attack.

Dictionary attacks [8] Dictionary can not be happened in GUA technique.

Spyware attack So far this attack is not possible on graphical passwords. Screen recording is possible. There are no such spywares till date. Text based passwords can be stolen using key loggers.

Shoulder surfing attack [8] Like text based passwords, most of the graphical authentication methods are vulnerable to shoulder surfing. Up till now, only a few recognition-based methods claim to resist shoulder-surfing. None of the recall-based based methods are considered should-surfing resistant.

Social engineering attack This attack practically impossible in graphical passwords as keyboard input is not involved so words in dictionary can't be used to crack the password.

Guessing attack [8][9] It is almost impossible to get graphical password by phishing or using any other human interaction method.

VIII. DESIGN AND IMPLEMENTATION ISSUES

Security[8] We have briefly examined the security issues with graphical passwords already in the above section.

Usability[8] One of the major issue for graphical authentication is that images are much more easier to remember than text strings

Reliability[8] The major design issue for recall-based methods is the reliability and accuracy of user input recognition.

Communication and Storage [8] Graphical authentication schemes require much more space for storage than text based passwords.

IX. COMPARATIVE STUDY OF GUA TECHNIQUE

Techniques	LogIn Interface	Drawback	Attack
Sobardo and birget[2]	Select objects from the no of pass objects	Difficulty in identifying Images from crowd	Brute Force
Dhamija and Perring[5]	Select images from a set of Images	Login phase could be very slow	Shoulder surfing
Jansen et al[5]	Select images based on theme	Small password space	Brute Force Shoulder surfing
Passface[5]	Select face from set of faces	User has to remember face	Brute Force Guess attack
DAS[8]	Redraw the picture	Difficulty in redrawing	Shoulder surfing
Story[5]	Select images as password to build a story	Difficult as compare to passface	Shoulder Surfing
Syukri[8]	Redraw signature	Easy to remember	Shoulder Surfing
Passlogix[6]	Select some part of a particular image	Users have to remember the sequence	Shoulder surfing

X. CONCLUSION

Results showed that graphical authentication has a high usability and that it is likely to replace text-based authentication methods in the near future. And even as of today, we can see graphical passwords being used in Windows8 OS as an alternate to text password, and also in touch based handheld devices like android smart phones, we see a pattern locking mechanism which is nothing but graphical authentication. So with the advancement in technology mainly in touch based technology, graphical authentication plays a very promising role for various authentications in such devices or gadgets. During our survey, we identify several drawbacks which can cause attacks. Therefore, it can be concluded that the common drawbacks on these some algorithms were: The users tend to select the weak passwords which are vulnerable to the graphical dictionary attack. Not all the users are familiar with using mouse as a drawing input device for graphical password. The memorize ability and usability of some of the algorithms are difficult. The users tend to select the weak passwords which can cause the password to be guessable or predictable. Users were fascinated by the pictures which drawn by other users, so frequently we can

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

see the common picture for password. The users can hardly remember the sequence of drawing after period of time.

REFERENCES

1. William Stallings and Lawrie Brown. “Computer Security: Principle and Practices." Pearson Education, 2008.
2. (IJIRSE) International Journal of Innovative Research in Science & Engineering, ISSN (Online) 2347-3207,”User Authentication By Secured Graphical Password Implementation”, Anil H. Rokade, Zafar Ul Hasan, Sonali A. Mahajan.
3. Int. Journal of Engineering Research and Applications www.ijera.com,ISSN : 2248-9622, Vol. 4, Issue 5(Version 6), May 2014, pp.179-185,www.ijera.com 179 | P a g e, “Image Based Authentication Using Persuasive Cued Click Points”, Ankita R Karia, Dr. Archana B. Patankar.
4. ‘Comparative Study Of Graphical User Authentication Approaches’, Radhika and Siddhartha Sankar Biswas, ISSN 2320–088X. IJCSMC, Vol. 3, Issue. 9, September 2014, pg.361 – 375.
5. (IJCSIS) International Journal of Computer Science and Information Security, Vol. 6, No. 2, 2009 ‘A Survey on Recognition-Based Graphical User Authentication Algorithms’, Farnaz Towhidi, Maslin Masrom.
6. ‘Multiple password authentications: A Survey’ Jagdish R. Yadav1, Vaibhav V. Bhujade2, Rajkumar Yadav3, Rahul V. Bambodkar4 IJAIEM,ISSN 2319 – 4847.
7. International Journal of Science and Modern Engineering (IJISME) ISSN: 2319-6386, Volume-1, Issue-5, April 2013,’An Ample-Range Survey on Recall-Based Graphical Password Authentication Based On Multi-Line Grid and Attack Patterns’ Navnath D. Kale, Megha M. Nalgirkar,
8. Volume: 1 | Issue : 9 | September 2012 ISSN - 2250-1991, Analysis & Design ‘Graphical Password Authentication Using Cryptography Algorithms’ Mr. Pratik A Vanjara ; Dr. Kishor Atkotiya.

Harinandan Tunga, Department of Computer Science & Engineering is with RCC Institute of Information Technology Kolkata, India for last eleven years. His present research interests include Network Security & Cryptography. He has done B.Tech(CSE) in 2003, ME(CSE) in 2006. He has 12 published papers in National & International conferences and Journals. He has supervised several undergraduate and postgraduate dissertations.

Diya Saha is the student of final year M.Tech(Department of Computer Science & Engineering) of RCC Institute of Information Technology , Kolkata, West Bengal.She has completed B.Tech(CSE) in 2014.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.