Secure Graphical Password Authentication

Dr. Santosh S. Lomte¹, Anil H. Rokade²

¹ Principal, Department of Computer Science, VDF School of Engineering & Technology, LATUR, INDIA
² Assistant Professor, Department of Computer Science and Engineering, Hi-Tech Institute of Technology, Aurangabad, INDIA

ABSTRACT
The most common computer system uses the password schemes for security purpose. We develop Graphical password as alternatives to biometry and text password. Because text password is hard to remember and graphical password is easy to remember for human being. Our graphical password scheme is recognition-based not the recall-based. In this paper, we present innovative graphical password which is combination of Text, Number and Images. The user starts with identifying the symbol from 6x6 grid formed using 36 blocks which contains 26 alphabets, 10 numbers that is 0 to 9 and images to effectively defeat prevalent from social hacking, at time of registration user have to select 4 alphabet and 2 numbers and for login user have to remember only six images in order, if order is mismatched you cannot login. In this we use remote keyboards and disable of mouse right click.

Keywords— Authentication, symbol, security, OTP, Usability.

I. INTRODUCTION
Authentication for the user is a major problem in every system providing secure access to confidential data and personalized services. Although, today there exists number of ways to authenticate a user [1, 2], the most popular method amongst them is with passwords. In this knowledge based authentication scheme, user authenticates him/herself by presenting the knowledge of a secret string of alphanumeric characters. The secret string is called as password and it is assumed to be known only to the claimed identity and hence her identity gets verified. However, in practice, anyone who knows or guesses the password is also able to authenticate as the legitimate user. Passwords represent simple, cost effective and user friendly authentication solution since its usage requires no special hardware or training and passwords can be easily distributed, maintained and updated via telephone, fax or email. However, passwords are effective only if following two conflicting requirements are satisfied simultaneously [3].

- **Usability**: Passwords should be easy to remember and user authentication process should easy for humans and should take less time.
- **Security**: Passwords should be secure; that is, they should look random and should be hard to guess; they should be changed frequently and should be different on different accounts of the same user; they should not be written or stored down in plain text remembered for a longer time, better than the text.
- **OTP**: We use the one time password for Authentication of the user by sending message on registered cell phone, and registered e-mail ID.

An illustrative example is shown in Figure 1.
Figure 1S: What is easy to remember, a picture of Konark Temple or a set of numbers?

As we can see in Figure 1, the task of memorizing a list of ten random digits, after a few seconds of inspection, would be impossible for most of us. On the other hand, the aerial picture of Konark Temple could easily be memorized so that at some future time, it could be distinguished from various other scenes.

The fact that images are better remembered than text and can potentially be chosen from an infinite set of images makes graphical passwords an ideal replacement to text passwords, especially in environments where the text entry is awkward or limited (For example, mobile phones, Point of sale (POS) devices and ATMs).

Even though the area of graphical passwords is actively discussed in the academic arena and experimental graphical password schemes [3, 6, 7] present promising results in terms of improved memorability, overall commercial adaptations of graphical passwords have been low.

The aim of this paper is to investigate the reasons behind low commercial acceptance and provide suitable recommendations to overcome them. In the second half of this paper, based on these recommendations, we design a simple graphical password scheme, called SECURE GRAPHICAL PASSWORD AUTHENTICATION is a cued recognition based graphical authentication scheme, which allows users to choose number, text as well as images as passwords without any specific alternations to underlying authentication design and process. It also blends together the strengths of Numbers, Alphabets and Pictures (NAP) to effectively defeat prevalent forms of social hacking. In this paper we describe the complete design of SECURE GRAPHICAL PASSWORD AUTHENTICATION and argue for its potential benefits in terms of security and usability. We then provide results of user study and security analysis.

Also in future we will add two features to this paper
1. Design algorithm for database security.
2. Design the algorithm to keep data (secret string) secure from client to server.

II. METHODOLOGY

Early in graphical password, it was conceived that the picture superiority effect coupled with the large password space offered by images, would solve the password problem entirely (the conflict between the security and usability) and people would choose graphical passwords that are stronger than the text passwords. However, in practice, results were not as expected. Graphical passwords have issues in both usability and security [9, 10] Balancing them together is as difficult as it was in text passwords. As a result, even after a lot of academic attention and recommendations, graphical passwords are rarely used in practice. In this section, we review some of the common problems associated with graphical passwords. Our focus is mainly on Cognometric graphical password schemes.

2.1 Usability Issues

Security experts often say that users are the weakest link in a security system [1, 7]. Users misunderstand how to use security mechanisms and do not realize the need for such a protection. User behavior is essentially goal driven and security is usually a supportive task. Users are happy to circumvent the security measures, if security measures try to impede their primary tasks. It is imperative therefore to consider carefully the usability of the proposed authentication scheme. As explained earlier, authentication process should take less time, it should be easy and stress free for the users. However, graphical passwords present some problems in terms of the efficiency (time to execute) and affordance.

2.2 Security

Compared to text passwords, graphical passwords are weak against some of the common attacks on passwords schemes. We list down some of the common attacks and how related proposals have tried to mitigate them.

2.2.1 Brute force and dictionary based attack

Simplest of the attack against any authentication scheme is to randomly guess the correct password. For example, an attacker needs 10,000 attempts to correctly guess a four digit Personal Identification Number PIN. Dictionary attack is more sophisticated attack than brute force. Here, instead of random guessing, attacker tries to crack the password using a dictionary of most common passwords.

2.3 OTP

We used the one time password for Authentication purpose, we achieve this by two ways first is registered users own mobile phone and send him/her a four digit Personal Identification Number PIN. Dictionary attack is more sophisticated attack than brute force. Here, instead of random guessing, attacker tries to crack the password using a dictionary of most common passwords.

2.4 Remote(Login) keyboard

We have used remote keyboard, because of if, we use physical keyboard the hacker can easily theft our password by using keyboard recorder. Also we disabled
right click of Mouse, because any one can copy the code or password.

III. PRIOR APPROACH

We did the literature the survey of Existing graphical passwords and have following observations that laid the foundation for this work.

3.1 Personal vs. Random images

The success of the graphical password scheme strongly depends on the type of images used [8]. For example, user can create a portfolio using personal images or random images. Both approaches have advantages and disadvantages. Psychological results show that self-generated or personal images are better recognized than those that are not. However, such images are insecure in practical setting due to their vulnerability against guessing attacks. System-chosen random images on the other hand, are more secure against guessing attacks, but they are difficult to remember than personal images [4, 5]. Ideally, we desire an authentication scheme that can merge together the security benefits of system-chosen images and memorability gains of self-chosen images.

3.2 Cognitive flexibility

We must realize that cognitive flexibility is important to accommodate people with different cognitive ability [13]. For users who do not want the visual way of working or prefer the traditional text passwords, graphical passwords should inhabit some alternate mechanism that allows them to select and enter text passwords.

3.3 Selection of decoy images

As we said earlier, locating password images involves visual search which consumes time. In order to improve the efficiency, the selection of decoy images becomes crucial, in a sense that these images should be both visually and semantically distinct so that users are not confused while locating their password images.

3.4 Cued Recognition

A cued recognition is an interesting approach to graphical passwords design. In such schemes, a cue is given to the user that helps her in the recognition of portfolio images. Best example of such a scheme is a Story scheme [11], where the story or the semantic relationship between the images assists user in the recognition of chosen password images. However, the cue should be designed carefully so that it only helps the legitimate user and not the attacker.

3.5 Drawmetric Schemes

Drawmetric schemes are recall based authentication schemes, which require user to remember and repeat a visual drawing on predefined grid cells. Draw-A-Secret (DAS) [11] is one such scheme. In DAS, during enrolment, user creates a password consisting of an outline drawing of a figure on top of an image or a grid. To authenticate, she must recollect the drawing from her memory and redraw at the same place as before in the grid.

However, the password space of such schemes is small as users prefer to draw symmetric images and with less number of strokes [12]

3.6 Locometric Schemes

Locometric schemes like Pass points are based upon human skill to locate preselected points within an image. For example, in Pass points scheme, the password is constructed with a series of random clicks on predefined regions of an image. In order to login, user must repeat clicking on the same locations and in correct order. The Pass Points.

3.7 Cognometric Schemes

The graphical password schemes of our particular interest are Cognometric schemes. These schemes are based upon human ability to recognize previously learned pictures. Psychological research shows that humans are proficient in recognizing the Pictures they have seen before, even within a set of distracters

3.8 NAP Tune Scheme

NAP Tune is a novel cognometric graphical authentication scheme which involves recognition of portfolio images. During account setup user creates a portfolio of 4 images or 4 characters or a 4-character word as her password and recognizes the images that corresponds to the chosen password to login. Motivation behind NAP Tune came from Alphabet charts used in kindergarten schools to teach alphabets with the help of illustrative pictures (For example, A for Apple, B for ball etc). We adopt the same concept to develop a novel authentication scheme that can serve both alphanumeric and pictorial passwords with same underlying design and interaction.

IV. OUR APPROACH

SECURE GRAPHICAL PASSWORD AUTHENTICATION is a novel cognometric graphical authentication scheme which involves recognition of portfolio images. During account setup user creates a portfolio of 4 images or 4 characters or a 4-character word as her password and recognizes the images that corresponds to the chosen password to login. Motivation behind SECURE GRAPHICAL PASSWORD AUTHENTICATION came from Alphabet charts used in kindergarten schools to teach alphabets with the help of illustrative pictures (For example, A for Apple, B for ball etc). We adopt the same concept to develop a novel authentication scheme that can serve both alphanumeric and pictorial passwords with same underlying design and interaction.

We explain the steps during registration and login below.

1. Steps during registration

Registration is one time event. During registration, we present user with a 6*6 grid consisting of 25 letters from the English alphabet set and 10 numbers (0-9) along with their pictorial representations as shown in
Figure 6. In the current prototype (for testing purpose), we have used pictures from the publically available picture dictionary.

User picks four images or characters and two numbers as password and enters the corresponding alphabet with number with in the textbox shown below the image grid. User is then free to choose any four images or four characters along with two numbers as her password. Irrespective of the selection (images or characters), he is allowed to enter only the four characters and two numbers in the textbox provided below. To illustrate, even if user chooses images of Ice-Cream, Ball, Apple and Umbrella as his password along with two numbers- ONE and TWO. He must enter IBAU12 (The associated characters and numbers with those images) in the textbox. Once the user has submitted four characters and two numbers, a confirmation message is displayed about successful completion of registration.

2. Steps during Login

During login, user sees the same 26 pictures and 10 numbers (0-9) randomly placed in the 6×6 image grid. However this time, the alphabets and numbers are replaced with a new set of numbers in the range of 0 to 9. In other words, each cell has a number instead of an alphabet associated with it as shown in Figure 1.4. In order to enter, user needs to recognize password (six images as four password characters and two password numbers) and enter the associated number in the textbox below. Users who have chosen character and number as password should recall character and numbers, only then perform a visual search for images that correspond to the characters and numbers since the characters not visible on screen, instead a number is assigned to each image and the original set of numbers has been replaced with a new set of numbers during entry. The images here act as a cue for recalling the password.

V. CONCLUSION

As India’s prime ministers mission is Digital India. Our project is helpful for making digital India by providing secure password to citizen of our country important. So far that we have developed such system that has more security as compare to other system like text, biometry, and other graphical password. In this system generates secured Password; that is, they look random and it is hard to guess; they changed frequently and they are different on different accounts of the same user. They are not written or stored down in plain text. User Authentication by secure graphical password implementation is very secured system that protects our data from unauthorized use. In this project, we have presented user authentication by secured graphical password implementation, a secure graphical
authentication scheme, very strong for banking, finance, e-commerce and sensitive organization military. Its strength lies in its simplicity and unique graphical way of working. We have designed and secure prototype of **SECURE GRAPHICAL PASSWORD AUTHENTICATION**. We discussed possible attacks on our scheme and how we could defend each of them. Results of the user study provide evidences for improved usability and memorability. Our future work includes working on the feedbacks received by the participants (using personal pictures and improving the visual search) and testing the scheme with large audience of all ages and under secure password inferences. Also we will provide the security to database by developing the algorithm for database also develop the algorithm for to keep the data secure traveling from client to server.

**REFERENCES**


