2-ROUND HYBRID PASSWORD SCHEME

Md. Asraful Haque, Babbar Imam, Nesar Ahmad
Department of Computer Engineering, Aligarh Muslim University, U.P.-202002, India
asrafb4u@gmail.com, babbarimam5@gmail.com, nesar.ahmad@gmail.com

ABSTRACT

The most common computer authentication method is to use alphanumerical usernames and passwords. This method has been shown to have significant drawbacks. They have problems such as being hard to remember, vulnerable to guessing, phishing, dictionary attack, key-logger, and social engineering. Researchers have come out with an alternate password scheme called graphical password where they tried to improve the security and avoid the weakness of conventional password. Psychological studies say that human can remember pictures better than text. But graphical password scheme also has several drawbacks like shoulder-surfing problem, more storage space required and hard to implement compared to text passwords. In this paper, we have suggested a hybrid authentication system combining graphical and text passwords. User authentication has been verified in two steps to increase the security. We believe that in our system, users will be able to select stronger passwords through better user interface design.

Keywords: Graphical Passwords, Text Passwords, User Authentication, Security, Password-Space

I. INTRODUCTION

AUTHENTICATION refers to the process of confirming or denying an individual’s claimed identity. Passwords are the most common means of authentication which do not require any special hardware. Typically passwords are strings of letters and digits. Alphanumeric passwords are versatile and easy to implement and use. They are required to satisfy two contradictory requirements. They have to be easily remembered by a user, while they have to be hard to guess by impostor [1]. Users are known to choose easily guessable and/or short text passwords, which are an easy target of dictionary and brute-forced attacks [2, 3]. Enforcing a strong password policy sometimes leads to an opposite effect, as a user may resort to write his or her difficult-to-remember passwords on sticky notes exposing them to direct theft [4]. Text
passwords can be stolen by malicious software (e.g., keystroke loggers) when being entered from keyboards. Phishing is another serious threat to text passwords, by which, a user could be persuaded to visit a forged website and enter their passwords. To overcome the problems associated with text-passwords, the researchers have proposed the concept of graphical passwords. Graphical passwords schemes are the most promising alternative to conventional password authentication systems. Graphical passwords employ graphical presentations such as icons, human faces or custom images to create a password. If the number of possible pictures is sufficiently large, the possible password space of a graphical password scheme may exceed that of text-based password and therefore it is virtually more resistance to attacks such as dictionary attacks. An important advantage of graphical passwords is that they are easier to remember than textual passwords due to the fact that human brains can process graphical images easily. Human brains have the ability to remember faces of people, places they visit and things they have seen for a longer duration. In this way graphical passwords provide a means for making more user-friendly passwords while increasing the level of security. Besides these advantages, the most common problem with graphical passwords is the shoulder surfing problem: an onlooker can steal user’s graphical password by watching in the user’s vicinity. Many researchers have attempted to solve this problem by providing different techniques. Another common problem with graphical passwords is that it takes longer to input graphical passwords than textual passwords. The login process is slow and it may frustrate the impatient users. Since the graphical password is not widely deployed in real systems vulnerabilities of graphical passwords are still not fully understood. In modern era of computerization, a big necessity to have a strong authentication method is needed to secure all our application as much as possible.

In this paper, considering the problems of text-password and graphical passwords, we have proposed a novel hybrid password scheme which has desirable usability and security features. The structure of our paper is organized as follows. Section 2 reviews few existing graphical authentication methods. Section 3 explains our new proposed scheme. Section 4 analyzes the scheme in different dimensions. Section 5 concludes the paper with some remarks.

II. GRAPHICAL PASSWORD SCHEMES

The past decade has seen a growing interest in using graphical passwords as an alternative to the traditional text-based passwords. Researchers are continually introducing new ideas, concepts, and features in the field of graphical authentication. There are already many approaches have been proposed in present times. Graphical password techniques can be classified into two categories: recognition-based and recall-based. In recognition-based systems, a series of images are presented to the user and a successful authentication requires a correct images being clicked in a right order. In recall-based systems, the user is asked to reproduce something that he or she created or selected earlier during the registration. Blonder gave the initial idea of graphical password in 1996. In his scheme, a user is presented with one predetermined image on a visual display and required to select one or more predetermined positions on the displayed image in a particular order to access the restricted resource [5]. The major drawback of this scheme is that users cannot click arbitrarily on the background. The memorable password space was not studied by the author either. Wiedenbeck et al [6] proposed PassPoint method in which they extended Blonder’s idea by eliminating the
predefined boundaries and allowing arbitrary images to be used. As a result, a user can click on any place on an image (as opposed to some pre-defined areas) to create a password. A tolerance around each chosen pixel is calculated. In order to be authenticated, the user must click within the tolerance of their chosen pixels and also in the correct sequence. Few grid based schemes are proposed which uses recall method. Jermyn et al [7] proposed a technique called “Draw A Secret” (DAS) where a user draws the password on a 2D grid. The coordinates of this drawing on the grid are stored in order. During authentication user must redraw the picture. The user is authenticated if the drawing touches the grid in the same order. The major drawback of DAS is that diagonal lines are difficult to draw and difficulties might arise when the user chooses a drawing that contains strokes that pass too close to a grid-line. Users have to draw their input sufficiently away from the grid lines and intersections in order to enter the password correctly. If a user draws a password close to the grid lines or intersections, the scheme may not distinguish which cell the user is choosing. Syukri et al. [8] proposed a system where authentication is conducted by having the user drawing his/her signature using a mouse. Dhamija and Perrig [9] proposed a graphical authentication scheme in which the user selects certain number of images from a set of random pictures during registration. Later user has to identify the pre-selected images for authentication. The users are presented a set of pictures on the interface, some of them taken from their portfolio, and some images selected randomly. For successful authentication, users have to select ‘their’ pictures amongst the distracters. Passface is a technique developed by Real User Corporation [10]. The basic idea is same as Dhamija and Perrig method. Here the user is asked to choose four images of human faces from a face database as their password. There is a common weakness in the above graphical password schemes: they are all vulnerable to shoulder-surfing attacks. To address this issue, Sobrado and Birget developed a graphical password technique [11]. In their scheme, the system first displays a number of 3 pass-objects (pre-selected by a user) among many other objects. To be authenticated, a user needs to recognize pass-objects and click inside the triangle formed by the 3 pass-objects. Man, et al. [12] proposed another shoulder-surfing resistant algorithm in which a user selects a number of pictures as pass-objects. 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 and many decoy-objects. The user has to type in a string with the unique codes corresponding to the pass-object. However, these methods force the user to memorize too many text strings, and their shoulder-surfing resistant property is not strong either. Chiasson et al [13] proposed a cued-recall graphical password technique. Users click on one point per image for a sequence of images. The next image displayed is based on the previous click point so users receive implicit feedback as to whether they are on the correct path when logging in. A wrong click leads down an incorrect path, with an explicit indication of authentication failure only after the final click. The visual cue does not explicitly reveal right or wrong but is evident using knowledge only the legitimate user should possess. These techniques have the potential to fill the gaps left between traditional authentication techniques, including trade-offs between security levels, expense and error tolerance [14]. But unfortunately in real scenario, these approaches are under-utilized as the authentications are usually complex and boring for users.
III. OUR PROPOSAL

Given that text passwords are easy to deploy and to use, we believe that they will continue to be popular. Graphical passwords are new and have some advantages over text password. Thus, we suggest that a combinational scheme of both text passwords and graphical passwords should be made to enhance the security by addressing common password attacks. To this end, we propose Two-Round Hybrid scheme. The proposed authentication system is divided into two phases as follows.

A. Registration Phase:
1. A user creates his profile by entering personal details and username.
2. Then he is presented with a set of 25 images as shown in Fig 1. This is the common image-set for all users.

![Figure 1: Image-set for registration](image)

The user has to select any number of images from this set. Even he may choose a single image more than once. This selection will act as the password of his first round of authentication.
3. Next he will choose any picture from the stored image database or from the local memory at his own choice.
4. Now the user will select a point in the image and then type a text password. Password will be associated with that Point of Interest (POI). Each POI is described by a square (center and some tolerance in both X and Y axis).
B. Login Phase:
1. In round-1, a user is asked for his user name and graphical password (correct selection of images in a correct sequence). The order of images within the set will be random at every login time. This authentication step is shown in Fig 2.
2. After supplying this, and independent of whether or not it is correct, in round two authentications, the user is presented with the pre-selected image.
3. Here the user first clicks on the pre-defined POI. It is not possible for anyone to choose the exact point. We have to assign an acceptable tolerance to POI to minimize the false positives and false negatives. For an actual point \((x, y)\) we allow the user to click any point which has the X-coordinate in between \((x-5)\) to \((x+5)\) and Y-coordinate in between \((y-5)\) to \((y+5)\). It means the allowable click-area will be a square of length10.
4. After selection of correct POI user is presented with a text box where he has to type the text password as shown in Fig 3.
5. After the successful entries in both rounds the user is allowed to access his account.

![Figure 2: Round-1 Authentication](image-url)
IV. ANALYSIS OF THE SCHEME

A. Usability Features:

In human computer interaction and computer science, usability usually refers to the elegance and clarity with which the interaction with a computer program or a web site is designed. Typical dictionary definitions show ‘usability’ to be a noun to the adjective ‘usable’, which means that something is capable of being used, or is convenient and practicable for use. Our scheme has the following usability features:

- Easy to use and memorize
- Easy to create the password
- Design and view mode is acceptable

B. Password Strength:

Wikipedia define the password strength as the likelihood that a password can be guessed by an unauthorized person or computer. Passwords easily guessed are known as weak or vulnerable; passwords very difficult or impossible to guess are considered strong. The terms weak and strong are relative and have meaning only with regard to specific password systems. The necessary quality of the password depends on how well the password system limits attempts to guess a user's password, whether by a person who knows the user well, or a computer trying millions of possibilities [15]. In this section, we will discuss the password strength of our scheme by considering both the password space of the text password and the graphical password parts.

The password space of first round authentication will be \( R_1 = \sum_{i=1}^{p} 25^i \); where \( p \) is the maximum number of images used to form the password.

Now consider the round-2 authentication. Let \( M \times N \) be the size of the image portfolio and suppose the size of the allowable click-area is \( n \times n \) for any POI. So the available numbers of POI are \( \frac{M \times N}{n^2} \). A text password of maximum length \( q \) characters has password space \( \sum_{j=1}^{q} c^j \), if
characters are selected uniformly at random and independently from an alphabet of \( C \) characters. Naturally the password space of second round authentication will be \( R_2 = \frac{M \times N}{n^2} \times \sum_{j=1}^{q} C^j \).

If we combine these two steps, we will achieve the overall password space of our scheme which is \( P = R_1 \times R_2 \).

**C. Resisting Brute Force and Dictionary Attacks:**

Dictionary attack is normally used to crack the text password. In hybrid scheme, first round authentication is based on graphical password and second round also involves mouse input, so it will be impractical to carry out dictionary attacks against this scheme. Effort required in brute-force is directly proportional to the password space. In our scheme password space is very large. So an enormous effort is required to apply a brute force attack against our scheme. The attack programs need to automatically generate accurate click-positions to imitate human input, which is particularly difficult for this scheme.

**D. Mitigating Keylogger Attacks:**

Keylogging is a common method for stealing user text passwords. A keylogger is a malicious software which intercepts keystrokes on an infected machine as a user types. For example, Microsoft Windows provides (un-documented) interfaces facilitating interception of system events including keystrokes. With our hybrid scheme, a user would use the keyboard for the text password part, and mouse clicks for the graphical parts. Thus, a naive keylogger cannot obtain the graphical parts. More sophisticated malware can capture both user screen contents and mouse clicks to recover a graphical password, with more effort. But it is not clear whether “mouse tracking” spyware will be an effective tool against graphical passwords. However, mouse motion alone is not enough to break graphical passwords. Such information has to be correlated with application information, such as window position and size, as well as timing information.

**E. Mitigating Phishing Attacks:**

Phishing is another common technique for stealing passwords by fooling users to enter such information into a fraudulent website spoofing a legitimate one (e.g., a bank site). Social engineering tactics are often used (e.g., “urgent account update”, requests to verify fake transactions, etc.). In hybrid system, the image portfolio of first round authentication may be same to all users. So an expert phisher can steal the password of first part easily. But in second round authentication, it is very difficult to crack even users’ text password. Our text password is associated with a POI which is graphical part. Without the knowledge of users’ image profile, the phisher does not know what images to present in order to extract a POI. So obtaining its round-2 password is very difficult.

**F. Resisting Shoulder Surfing Attacks:**

Like text based passwords, most of the graphical passwords are vulnerable to shoulder surfing. At this point, our policy provides a solid resistance against shoulder surfing attack. In first round authentication, the user is presented with a set of 25 images. Naturally the size of each image will be very small and each login time the order of the images will be random. This technique is specially deployed to make an imposter confused who is trying to memorize the authentication details from the backside.
V. CONCLUSION

Our authentication scheme is a combination of text passwords and graphical passwords. Again first round of graphical authentication is a recognition based technique whereas second round of graphical authentication is a recall based technique. So we have used the term ‘hybrid’ to denote our scheme. We do believe that our design will prove to be more usable and adequately secure for user authentication than existing text-based password and graphical password methods. An obvious and necessary next step is a user study, ideally both a lab study and a field study leveraging our real-world deployment. The scheme can be useful for highly secure systems. Proposed scheme will provide the following advantages:

1. Users’ current sign-in experience is partially preserved.
2. A text password alone which is stolen (e.g., by phishing or any other means) does not compromise an account.
3. Random order of images in round-1 authentication provides a resistance to the shoulder surfing attacks.
4. Password space is very large.
5. It can be implemented in software alone, increasing the potential for large-scale adoption on the Internet.

Current graphical password techniques are still immature. The field is new and open for future works.

ACKNOWLEDGMENT

First and foremost, we offer our gratitude to the almighty Allah whose blessings have helped us to complete this work. We would like to thank Mr. Sarosh Umar, Reader of Aligarh Muslim University for his valuable advice throughout the work. We are also grateful to Mr. Mohsin Abbas Rizvi, Web developer in Vinove Pvt. Ltd. and Mr. Mohd Anjum, guest faculty at AMU for their help during the implementation phase.

REFERENCES


Nesar Ahmad is presently working as a Professor in the Department of Computer Engineering, Aligarh Muslim University, India. He has nearly twenty years of teaching experience. Nesar Ahmad obtained his B.Sc (Engg) degree in Electronics & Communication Engineering from Bihar College of Engineering, Patna (Now NIT, Patna) in 1984 and M.Sc (Information Engineering) degree from City University, London, U.K., in 1989. He received his Ph.D degree from Indian Institute of Technology (IIT), Delhi, India, in 1993. Earlier he worked as a Senior Scientific Officer in Microprocessor Applications Program at IIT Delhi. He was with King Saud University, Riyadh during 1997-99 as an Assistant Professor. Before joining AMU, he worked as an Assistant Professor in the Department of Electrical Engineering, IIT Delhi till December 2004. His current research interests mainly include Soft Computing, Web Intelligence and E-Learning. He has authored many papers in various International Journals and Conference proceedings.

Md. Asraful Haque was born in 1985 in West Bengal, India. He received his Master degree in Computer Science and Engineering (Specialization-Software Engineering) from Aligarh Muslim University. Presently he is an Assistant Professor (Ad-hoc basis) in Aligarh Muslim University. He has more than three years of teaching experience. His area of interests includes Software engineering, Operating Systems, Data Structure, Image Processing and Internet Security. He has authored several papers in different international journals and conferences.

Babbar Imam received his B.Tech degree in Computer Science and Engineering from Aligarh Muslim University in 2009. He is presently pursuing his Master degree in Software Engineering from the same University. He has two years of teaching experience. His area of interests includes Software engineering, Artificial Intelligence, Image Processing and Computer Security.