© 2015 IJSRSET | Volume 1 | Issue 3 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Authentication Scheme for Passwords using Color and Text

Vikas B O
Department of Computer Science and Engineering, SCE Bangalore, Karnataka, India

ABSTRACT

The most common method used for authentication is textual passwords. But textual passwords are in risk to eves dropping, dictionary attacks, social engineering and shoulder surfing. Graphical passwords are introduced as alternative techniques to textual passwords. Most of the graphical schemes are helpless to shoulder surfing as well as it has higher storage and computational complexity. To address this problem, text can be combined with colors to generate passwords for authentication. The combination of color and text password with efficient matching between the two provides authentication as well as security to the user. Hence using the technique of integration with color and textual password is proposed to generate passwords which are resistant to shoulder surfing.
Keywords: Graphical passwords, Recognition-based, Cued- recall based, Pure-recall based authentication scheme

I. INTRODUCTION

In any organization, regardless the size and nature of the company, information security is a major concern. The protection of information and implementation of adequate security mechanisms with respect to confidentiality, integrity and authenticity are especially important in today's increasingly interconnected business environment. Traditional textual passwords are perhaps the most prevalent and convenient authentication method because they are familiar to all users, easy to use, and cheap to implement. The known weakness of traditional user authentication is a tendency to choose passwords with predictable characteristics, which in turn reduces password strength and makes it vulnerable to various attacks as mentioned in [2]. Sufficiently secure password should be at least eight characters or longer, random, without any semantic content, with mix of uppercase and lowercase letters, digits, and special symbols. Generally, users ignore any tips and recommendations for creating a secure password. Moreover, some users write down their passwords on a piece of paper, share passwords with others or use the same password for multiple accounts. Most of the common attacks namely brute force search attack, dictionary attack, guessing attack, shoulder surfing attack, spyware attack, and social engineering attack can use these weaknesses for attacking to the system. In attempt to overcome the weaknesses of traditional textual password, graphical password schemes have emerged as a possible security enhancement. Human's ability to better recognize visual information as opposed to verbal information makes the graphical passwords easier to remember as discussed in [4]. The first graphical password based scheme was introduced by Greg Blonder in 1996. In his scheme the user is asked to click on several locations on the image to create a password. To login the user must click on previously selected locations on the image or close to those locations.

Today, there is a growing interest in graphical passwords but most of the graphical password authentication schemes have not been widely adopted.

Related Work

Currently, user authentication mechanisms fall under three main categories:

1. Biometric authentication (something you are)
2. Token-based authentication (something you have)
3. Knowledge-based authentication (something you know) as mentioned in [6]

Biometric authentication refers to the identification of some unique physical or behavioral characteristics of the user. Examples include fingerprint, iris scan, handwritten signature, voice recognition, and others. Even despite the fact that biometric passwords are very efficient, easy to manage and do not require memorizing, they are expensive solutions, which cannot be widely adopted.

Token-based authentication is a technique where in order to be authenticated the user is required to present a token. Unfortunately, the token can be easily stolen, forgotten or duplicated. Also token-based authentication scheme as mentioned in [8] is not convenient for use because special additional hardware devices are needed.
Knowledge-based authentication can be classified into two categories: textual passwords and graphical passwords. Graphical passwords include recognition-based techniques and recall-based techniques. Using recognition-based techniques, in order to pass the authentication, user is required to recognize and identify a set of images selected earlier during the registration phase.

Recall-based techniques categorized into:

1. Pure recall-based
2. Cued recall-based.

In pure recall based category, the user is asked to recall and reproduce something created or selected earlier during the registration phase without being given any hint.

In cued recall based category, the technique proposes a hint that helps the user to recall and reproduce previously created or selected password more accurately as discussed in [9]. Sending message fragments into multiple UDP packages. Normally, the OS has the ability to re-assemble packets into a complete message by referencing data in each UDP packet. The tear drop attack corrupts the offset in UDP packets which makes the system to rebuild the original packets. As the OS is unable to handle the data corruption, the most likely outcome leads to system crash.

Taxonomy of Authentication

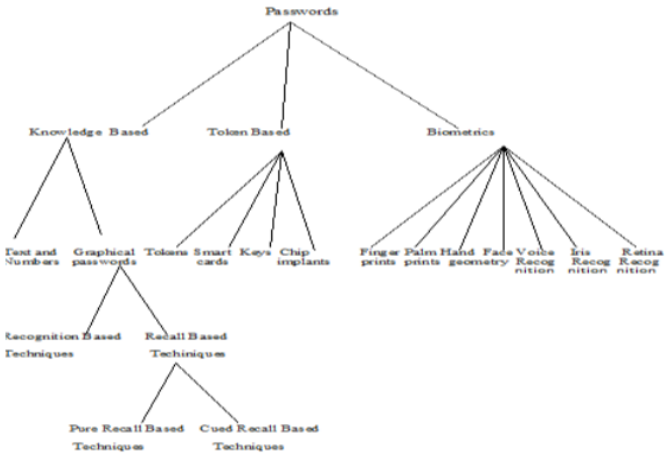


Figure 1: Taxonomy of Authentication [1]

The figure 1 is the depiction of current authentication methods Biometric based authentication systems techniques are proved to be expensive, slow and unreliable and hence not preferred by many. Token based authentication system is high security and usability and Accessibility compare then others. But this system employ knowledge based techniques to enhance security. But the current knowledge based techniques are still immature. For instance, ATM cards always go hand in hand with PIN number. The major goal of this work is to reduce the guessing attacks as well as encouraging users to select more random, and difficult passwords to guess.

A. Recognition-Based Authentication Schemes

1. Déjà Vu Algorithm

In 2000 Dhamija and Perrig proposed a new graphical authentication scheme called Déjà vu algorithm as mentioned in [5], which is based on the perception of hash visualization technique. At registration phase the user is asked to choose a certain number of images from a collection of random non-describable abstract pictures generated by a system. Later, the user will be required to identify previously selected images in order to be authenticated. The average registration and login time of this approach is much longer than in the traditional text-based approach. Also the server needs to store large number of pictures that may delay the authentication process while transferring over the network. Furthermore, the process of selecting and identifying a

set of images from the picture database can be time consuming for the user.

Figure 2: An example of Déjà vu algorithm

2. Triangle Algorithm

In 2002 Sobrado and Birget developed a new graphical password scheme called Triangle algorithm as mentioned in [5] that is aimed to deal with shoulder surfing problem. At registration phase user is asked to choose a certain number of pass objects from 1000 proposed objects. Later, to authenticate, the system displays a variety of objects on the screen and the user is asked to click inside the area that the previously selected objects form. The action repeats for several times but every time the icons on the screen will shuffle and appear in different place. Major disadvantage of this scheme refers to a very crowded display, so the user cannot distinguish the objects on the screen. Also the average registration and login time is much longer than in the traditional text-based approach. On the other hand, using fewer objects may lead to a smaller password space.

Figure 3: An example of Triangle algorithm

3. Passface algorithm

In 2000 Brostoff and Sasse from Real User Corporation proposed a new graphical authentication scheme that is called Pass face algorithm as mentioned in [9]. To create a password the user will be asked to choose a certain number of images of human faces from the picture database. At authentication phase user will be required to identify previously chosen faces in order to be authenticated. The user recognizes and clicks on the known face, and then the procedure repeats for several times. This technique is very memorable over long time periods. However, majority of the users tend to choose faces of people based on the obvious behavioral pattern, which makes this authentication scheme kind of predictable and vulnerable to various attacks. Also it takes longer for login and registration than in traditional text-based password scheme.

Figure 4: An example of Pass face algorithm

B. Pure Recall-Based Authentication Schemes

1. Draw-A-Secret (DAS) Algorithm

In 1999 Jermyn, Mayer, Monrose, Reiter, and Rubin proposed a new graphical password scheme called Draw-a-Secret algorithm as mentioned in [6]. This scheme allows user to draw a unique password on a 2D grid. At registration phase the coordinates of the grids occupied by the drawn patterns are stored in order of the drawing. During authentication phase, the user is asked to redraw the picture by touching the same grids and in the same sequence. Unfortunately, most of the users over a certain period of time forget their drawing order. Another drawback is that the users tend to choose weak graphical passwords, which as a result makes this authentication scheme kind of Predictable and vulnerable to various attacks.

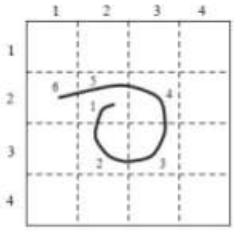


Figure 5: An example of Draw-a-Secret (DAS) algorithm

2. Grid selection algorithm

In 2004 Thorpe and Oorschot proposed a new graphical authentication scheme that is called Grid selection algorithm as mentioned in [7]. Firstly, within a large selection grid user chooses a smaller grid for drawing. This adds an extra degree of complexity to the password. Then the user zooms in this piece of grid and creates a drawing like in original Draw-a-Secret (DAS) scheme. This technique of authentication dramatically increases the password space. However, it introduces additional job to memorize and time to input the password. In other words, the security enhancement is achieved by sacrificing password usability and memorability.

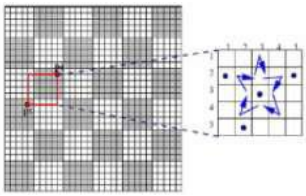


Figure 6: An example of Grid selection algorithm

3. Syukri et al. algorithm

In 2005 Syukri, Okamoto, and Mambo proposed a new graphical authentication scheme called Syukri et al. algorithm as mentioned in [4]. During the registration phase user will be asked to draw the signature with an input device. At verification phase the system extracts the parameters of the signature that are stored in the database. The biggest advantage of this approach is that signatures are hard to fake. Also there is no extra job to memorize the password.

The main drawback is that drawing signature with a mouse is not an easy task. The obvious solution to this problem would be usage of a pen-like input device instead of mouse. However, such devices are not widely used and adding new hardware can be expensive as mentioned.

Figure 7: An example of Syukri et al. algorithm.

C. Cued Recall-Based Authentication Schemes

1. Blonder algorithm

In 1996 Blonder proposed a new graphical authentication scheme that is called Blonder algorithm. During the registration the user is asked to click on several locations on an image to create a password. At authentication phase the user has to click on previously selected locations on the image or close to those locations. The image acts as a hint for the user to recall graphical passwords and therefore this method of authentication is considered more convenient than unassisted pure recall-based schemes as discussed in [6]. Major problem this scheme faced with is that the number of predefined click areas is relatively small so the password had to be quite long to be secure. Also, the usage of predefined click areas required simple and plain images, instead of complex, real-world and crowded scenes.

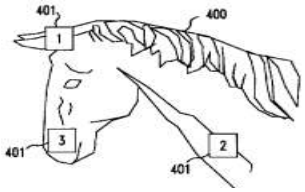


Figure 8: An example of Blonder algorithm

2. Pass logix v-Go algorithm

In 2002 Pass logix Inc. Company developed a new graphical authentication scheme called Passlogix v-Go algorithm. At registration phase the password is created by a chronological situation with repeating a sequence of actions. In this method user is asked to click on various items on the image in the correct sequence in order to be authenticated. One drawback is that this technique provides only a limited password space, therefore causing the password to be kind of guessable or predictable as discussed in [4].

Figure 9: An example of Passlogix v-Go algorithm

3. Pass Point algorithm

In 2005 Wiedenbeck, Waters, Birget, Brodskiy, and Memon proposed a new graphical authentication scheme that is called PassPoint algorithm as mentioned in [6]. During the registration the user is asked to click on several locations on an image. At authentication phase the user has to click on previously selected locations on the image or close to those locations. This method covers the limitations of Blonder algorithm because the images that are used for this method should be rich enough, complex and crowded. Any pixel in the image is a candidate for a click point so there are thousands of possible memorable points and combinations. One drawback is that it takes more time to input the password than text-based password users spend.

Figure 10: An example of Pass Point algorithm

D. Security

Security is a primary goal and the main requirement for any user authentication mechanism. A lot of strategies exist for attacking to the system. Unfortunately, none system offers the perfect security, therefore schemes must be evaluated according to their vulnerabilities and susceptibility to different attacks as discussed in [10].

Brute force search attack attempts to decipher the password by searching and testing for all possible combinations of alphanumeric characters until finding the correct key. For some graphical password schemes the most effective way against brute force search attack is to enlarge the password space by increasing the capacity of the picture library. In general, graphical passwords are less vulnerable to brute force search attacks than traditional text-based approach. However, recall-based methods of authentication tend to have bigger password space unlike recognition-based technique.

Dictionary attack attempts to reveal the password by running through a possible series of dictionary words that are compiled based on knowledge or assumptions considering the user's typical behavior. In general, graphical passwords are less vulnerable to dictionary attacks than traditional text-based approach. Users of recognition-based methods usually use a mouse for input, so it has no purpose to carry out the dictionary attacks against this kind of graphical authentication. Employment of a dictionary attack for recall-based methods is much more complex than in text-based dictionary attack but the speed of retrieving will slow down.

Shoulder surfing attack refers to obtaining the password of a particular user during login through direct observation or external recording devices. Text-based passwords like most of the graphical password schemes are vulnerable to shoulder surfing attack. Only a few of recognition-based techniques are designed to resist shoulder surfing and none of the recall-based techniques are considered resistant to shoulder surfing.

Guessing attack is a very common problem for both textual and graphical authentication approaches because users usually create short and simple passwords that give a convenience for guess work. Users of text-based approach and the users of some graphical password schemes tend to choose weak passwords with predictable characteristics.

Spyware attack refers to any unauthorized software installed without the user's permission that collects information about user's computational behavior by tracking the keyboard input. In general, graphical passwords are less vulnerable to spyware attacks than traditional text-based approach. Since for inputting the graphical password users exploit the mouse, through the mouse motion alone is not enough to break graphical passwords.

Social engineering attack includes any method used to gain access to the system under false pretenses by exploiting human psychology. In general, graphical passwords are less vulnerable to social engineering attacks than traditional text based approach. Also it reduces the possible password revealing because the explanation of graphical password to another person by

verbal interpretation is much more difficult.

Table 1: Types of common attacks

ATTACKS	Brute Force
	Dictionary
	Guessing
	Shoulder Surfing
	Spyware
	Social Engineering

E. Challenges for Authentication Schemes

Existing approaches such that users often create memorable passwords that are easy for attackers to guess, but strong system-assigned passwords are difficult for users to remember. Despite the vulnerabilities, it's the user natural tendency of the users that they will always prefer to go for short passwords for ease of remembrance and also lack of awareness about how attackers tend to attacks. The disadvantage of this system is that the strong system-assigned passwords are difficult for users to remember and does not overcome shoulder surfing and its attacks on user.

II. METHODS AND MATERIAL

The proposed system will overcome shoulder surfing and act as a resistance towards hidden camera attacks using the combination of color and text password which in turn also reduce the guessing attacks as well as encouraging users to select more random, and difficult passwords to guess. The proposed work merges color and text password approaches to limit the attacks by shoulder surfing and password guessing resistant protocol as mentioned in [1].

Modules

1. Registration Module
2. Hybrid Color and Text Module

1. Registration Module

When we run the application, a login form turn up, allowing the user to enter the username and hybrid password. The form appeared consists of two buttons- Signup, Sign in.

If the user is already a registered one, then clicking on the "Sign in" button would advance him to the second phase of the application. If the user is not a registered member, then on doing the above action would generate a message box conveying "username does not exist". Thus, in order to make use of the application, the person must get registered. Consequently, on clicking the "Signup" button on the login form would display a window allowing the user to enter his details such as address, phone number, email id, city, pin code, contact number. Then, the user has to enter the hybrid password as a combination with color displayed in the form page and subsequently, user has to click on the "next" button below that interface. On doing so, registration is successful. The password entered has to be remembered as hybrid pair-based password, also known as Color and Text combined password. Clicking the "next" button in the registration form would automatically generate the user-id based on the existing users. All the information inserted by the user is stored on to the database. Thereby, again the login form is displayed, where the user now clicks on "Sign in" button advancing him to the second phase of the application.

2. Hybrid Color and Text Module

The second phase of the module contains Login form page. Here the user has to enter his Hybrid password with respect to the color displayed. The color on the form page is shuffled each time the user enters the page. This provides enhanced security to the password hence called hybrid password. As the colors are shuffled, the user has to enter the particular password for that particular color in the sequence. The sequence in which the color and text was registered, the user has to enter according to the color displayed. Then the entered password is verified with the database, if the user entered hybrid password matches with the database hybrid password the user login is successful. If the user entered password does not math with the database an action would generate a message box conveying "Password entered is In-Correct".

System Architecture

The work flow for the implemented module of Hybrid color and text architecture is shown in the below figure 11.

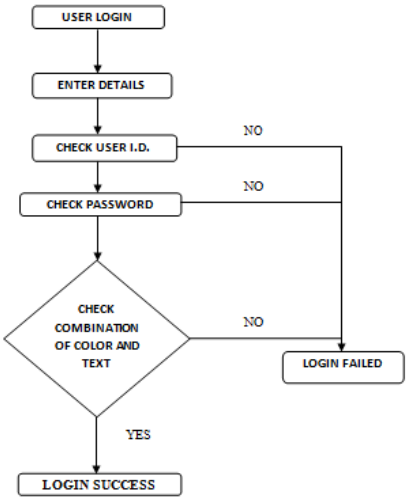


Figure 11: Architecture for the implemented module of Hybrid color and text.

Algorithms

Step 1 : Initialize m color images

Step 2: Take password as the input from Password field

Step 3: Register Process

If No of entered password characters == n

divide n by m and store each (n/m)

character-password with respect to all m color in database

else

alert msg "enter password!!!"

Step 4: Login Process

If fpoint(database points)==fpoint(new points)

Login successful

Else

Login Unsuccessful

III. RESULTS AND DISCUSSION

Regarding the common attacks in graphical passwords and based on research conclusion is given in the form of comparison among different schemes in the table 2 below

Table 2: The attacks resistance in graphical user authentication algorithms

ALGORITHMS		ATTACKS					
		Brute Force	Dictionary	Shoulder Surfing	Guessing	Spyware	Social Engineering
Recognition - Based	1.1 Déjà vu	NO	YES	NO	NO	YES	YES
	1.2 Triangle	NO	YES	YES	NO	YES	YES
	1.3 Passface	NO	NO	NO	NO	YES	YES
Pure Recall-Based	2.1 DAS	YES	NO	NO	NO	YES	YES
	2.2 Grid Selection	-	-	NO	-	-	-
	2.3 Syukri et al	YES	NO	NO	NO	YES	YES
Cued Recall-Based	3.1 Blonder	NO	YES	NO	NO	YES	YES
	3.2 Passlogix v-go	NO	-	NO	-	NO	-
	3.3 Passpoint	NO	YES	NO	NO	-	-
Hybrid Color and Text	4.Color and Text (Proposed Scheme)	YES	YES	YES	YES	NO	YES

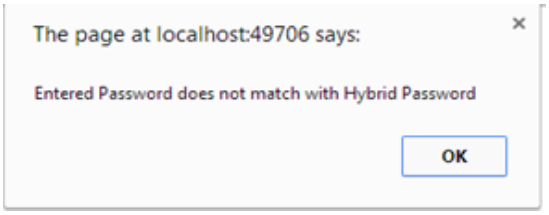
Regarding the storage complexity of graphical passwords and based on research conclusion is given in the form of comparison among different schemes in the table 3 below

Table 3: The Time and Storage complexity in graphical user authentication algorithms

ALGORITHMS		SPACE COMPLEXITY (n is number of Components)
Recognition - Based	1.1 Déjà vu	O(n)
	1.2 Triangle	O(n)
	1.3 Pass face	O(n)
Pure Recall-Based	2.1 DAS	O(n)
	2.2 Grid Selection	$O(n^2)$
	2.3 Syukri et al	O(n)
Cued Recall-Based	3.1 Blonder	O(np)
	3.2 Passlogix v-go	O(n)
	3.3 Passpoint	O(n)
Hybrid Color and Text	4.Color and Text (Proposed Scheme)	O(n)

Snapshot 1: User LOGIN with registered username and Hybrid password

Snapshot 2: User registration is successful and proceed for login form



Snapshot 3: When USER enters invalid password, error dialogue box showing "Entered password does not match with hybrid password".

IV. CONCLUSION

Overall, the review of nine different algorithms on recognition-based, pure recall-based and cued recall-based methods has been discussed. As part of our discussion on previous works, we studied the security and usability issues of graphical authentication including six common attacks. As shown in Table 2, most of the graphical password schemes are vulnerable to brute force search, shoulder surfing and guessing attacks. As the usability of an authentication scheme as well as its security should be of a prime importance. The proposed method named Hybrid Color and Text password will provide efficient authentication system.

A major advantage of Color and Text based passwords is its short password space as well as lower database storage and computational complexity. There is a growing interest for Graphical passwords since they are better than Text based passwords, although the main argument for graphical passwords is that people are better at memorizing graphical passwords than text-based passwords.

V. ACKNOWLEDGEMENT

I am thankful to 'Mrs. Pathanjali C, Assistant Professor, Dept of CSE for her valuable advice and support extended without which i could not have been able to complete the paper. I express deep thanks to 'Dr. Prashanth C M', Head of Department (CS&E) for warm hospitality and affection towards me. I thank the anonymous referees for their reviews that significantly improved the presentation of this paper. Words cannot express our gratitude for all those people who helped directly or indirectly in my endeavor. I take this opportunity to express my sincere thanks to all staff members of CS&E department of SCE for the valuable suggestion.

VI. REFERENCES

[1] Meng, Y. (2012, June). Designing click-draw based graphical password scheme for better authentication. In Networking, Architecture and Storage (NAS), 2012 IEEE 7th International Conference on (pp. 39-48). IEEE.

[2] Hu, W., Wu, X., & Wei, G. (2010, October). The security analysis of graphical passwords. In Communications and Intelligence Information Security (ICCIIS), 2010 International Conference on (pp. 200-203). IEEE.

[3] Ma, Y., & Feng, J. (2011, August). Evaluating usability of three authentication methods in web-based application. In Software Engineering Research, Management and Applications (SERA), 2011 9th International Conference on(pp. 81-88). IEEE.

[4] Eljetlawi, A. M., & Ithnin, N. (2008, November). Graphical password: Comprehensive study of the usability features of the recognition base graphical password methods. In Convergence and Hybrid Information Technology, 2008. ICCIT'08. Third International Conference on (Vol. 2, pp. 1137-1143). IEEE.

[5] Lashkari, A. H., Towhidi, F. A. R. N. A. Z., Saleh, R., & Farmand, S. (2009, December). A complete comparison on pure and cued recall-based graphical user authentication algorithms. In Computer and Electrical Engineering, 2009. ICCEE'09. Second International Conference on (Vol. 1, pp. 527-532). IEEE.

[6] Wiedenbeck, S., Waters, J., Birget, J. C., Brodskiy, A., & Memon, N. (2005, July). Authentication using graphical passwords: effects of tolerance and image choice. In Proceedings of the 2005 symposium on Usable privacy and security(pp. 1-12). ACM.

[7] Suo, X., Zhu, Y., & Owen, G. S. (2005, December). Graphical passwords: A survey. In Computer Security Applications Conference, 21st Annual (pp. 10-pp). IEEE.

[8] Wiedenbeck, S., Waters, J., Birget, J. C., Brodskiy, A., & Memon, N. (2005, July). Authentication using graphical passwords: effects of tolerance and image choice. In Proceedings of the 2005 symposium on Usable privacy and security(pp. 1-12). ACM.

[9] Gao, H., Liu, X., Wang, S., Liu, H., & Dai, R. (2009, December). Design and analysis of a graphical password scheme. In Innovative Computing, Information and Control (ICICIC), 2009 Fourth International Conference on (pp. 675-678). IEEE.

[10] Almulhem, A. (2011, February). A graphical password authentication system. In2011 World Congress on Internet Security (WorldCIS-2011) (pp. 223-225).