J. Basic. Appl. Sci. Res., 3(2)135-141, 2013

ISSN 2090-4304
Journal of Basic and Applied Scientific Research
www.textroad.com

An Enhancement on Passface Graphical Password Authentication

Farnaz Towhidi[1], Maslin Masrom[2,] Azizah Abdul Manaf[1]

[1]Advanced Informatics School, [2] Razak School of Engineering and Advanced Technology
Universiti Technologi Malaysia (UTM), Kuala Lumpur, Malaysia

ABSTRACT

The Passface is one of the most usable algorithms among recognition based graphical password category which suffer from vulnerabilities of shoulder surfing attack and teasing the user by using several steps during login. The main objective of this study is to implement a Secure Passface (S-Passface) algorithm by changing the method of selecting the password during login phase. In the Passface algorithm, selection of a password is done by mouse while in the S-Passface, it is replaced with entering random characters corresponded to each face. Also for resistance, two passwords is used for the user that can be applied alternatively. In order to analyze security, a shoulder surfing attacking session done in company with questionnaire utilized the user's feedback on security of both algorithms. The results show that S-Passface algorithm can effectively balance the two symbiotic pillars of usability and security by increasing resistant to shoulder surfing attack. The usability of the algorithm is validated by gathering feedback from participants who tested the two algorithms in a web based interface. These finding reveal that, the S-Passface algorithm is usable in some features while it decreases in others.
KEYWORDS: Authentication Passface, Secure Passface, S-Passface, Usability, Security, Graphical Password, Password.

INTRODUCTION

Graphical Password, one of the knowledge based authentications is an alternative for conventional password based on the studies which show that people can recall pictures with higher probability than words [1]. The history of graphical password algorithms goes as far back as more than a decade ago where researchers tried to find an algorithm which is both secure and usable. Passface algorithm created in 2000, with the idea of using pictures of human faces in order to validate the identity of user [2]. During registration firstly four pictures assigned randomly to the user from among a random set of faces. In the next step, a familiarization process is started in order to help the users to imprint password in their mind. During this trial session, there was a simulated process of login that users had to go through twice. The registration was assumed to be successful if users could correctly identify their four passwords. During the login phase, a grid of nine pictures was shown to the user for four times and each time one of the passwords of the user will be displayed along with eight decoy images from the database. However, no grid contains faces found in the other grids, and the order of faces within each grid is randomized [3-7]. Although Passface method covers many usability features like easy to use, easy to memorize, easy to recognize and easy to understand [8], but there are several drawbacks with this algorithm.

Firstly, when a password is selected by mouse, it is very easy for the shoulder surfer attacker to observe the password [9]. The other problem is that during login phase, a user should select each of his passwords in a separate grid, for instance, four length passwords require a user to view the grid four times. This increases the login time which is inconvenient for the user [10]. Also another research shows users tend to select faces of their own race which cause the algorithm to be guessable by attacker [11-13]. The aim of this study is to increase the security of Passface algorithm by creating resistance to shoulder surfing attack.

RELATED WORKS

In 2004, a research on twelve different categories of faces showed that users prefer to select faces of their own race or even attractive faces more than others. The report showed that around fifty percent of Asian and white females chose a password with faces from their own race; while the males in this category were chosen over sixty percent of the time. This makes this algorithm more vulnerable to guessing attack [13-14]. A 2008 research showed the vulnerability of the Passface algorithm to description attack by showing the importance of the way that images are displayed in grid. In this research, during the login phase, an audio description played for the user in order to describe the password image which placed among the eight decoys. Then it checked whether the user can identify the password from among other pictures by audio description. This research used three different methods for placing the eight decoy pictures in the grid [15].

In the first method, the nine decoy images selected randomly from a database of faces with the same age of password faces. In the second method, the choosing of decoy images is done by visual similarity to the password face. To identify which image seemed to be more similar, a group of persons evaluated to determine the resemblance of images. In the last method, the decoys images were chosen based on the similarity to verbal picture depiction of the password and eight decoys. The results of this investigation showed Passface can be used by correct selection of decoys

* **Corresponding Author:** Farnaz Towhidi, Advanced Informatics School, Universiti Technologi Malaysia (UTM), Kuala Lumpur, Malaysia. Email: farnaz.towhidi@gmail.com

which decrease the vulnerability of this method to description attack. So the decoy images are not supposed to have any considerable characteristic either relating to the person or their faces with the intention of making it tough for the user to describe it for the others [15].

The S-Passface is implemented with the idea of enhancing the security and usability of Passface algorithm, by improving the vulnerability of Passface algorithm to the shoulder surfing attack, and increase the usability during the login phase. So a web based interface designed for S-Passface and Passface for make a comparison for security and usability of both algorithms. The source code of the original Passface was needed which unfortunately was not available, therefore this algorithm is implemented based on the Passface corporation website that places a sample of this algorithm for users to test. In the following section, the details of enhanced Passface algorithm describe.

MATERIALS AND METHODS

The main idea of new algorithm is enhancing the usability and security of Passface by changing several items of original algorithm like the method of selecting password, creating two concurrent passwords and omission assigning password by system. The description of these methods is as follow.

Password Selection: The S-Passface algorithm designed for being resistant to shoulder surfing attack, based on the research which shows that switching the configuration from mouse to keyboard input, decreases the vulnerability to shoulder surfing attack [16]. Also according to "where is waldo" algorithm that proved for resistance to shoulder surfing attack, when a unique random text assigned for each picture, the user needs to input the string of codes correspondence to his password images, rather than directly selecting his password by mouse [9, 17]. With reference to these findings, during login phase of S-Passface algorithm, there is no choice to selecting the password with mouse, in return, two random characters assigned below each face. The user authenticated successfully if he could identify his password images and then enter the text below his password (Figure 2).

Figure 2. The First Round of Login in S-Passface

Alternative Password: According to research, password of the users should look random and frequently changed [18]. For making the password look random, during registration, the S-Passface algorithm allow user to select two different passwords; the first password selects among two grids of men and women faces, and the second password selects, from gallery of faces of kids and clowns. So during login phase, there are two rounds which users need to alternatively login with their two passwords.

According to Figure 2, in the first round of authentication, 18 cells of grids fill with faces of women and men while they include the first password of the user. When the user authenticate successfully through first round, the system set the login mode to second round. So during next authentication, the user will see the pictures of kids and clowns in the grid including the faces which he had selected as his password (Figure 3). So although during registration, the user selects his password from four categories of faces, only two of them are available in each round. If for any reason the attacker can identify any of the faces by capturing the screen or using camera, the password will not use in the next login. This provides an environment for the algorithm to be resistant to shoulder surfing attack.

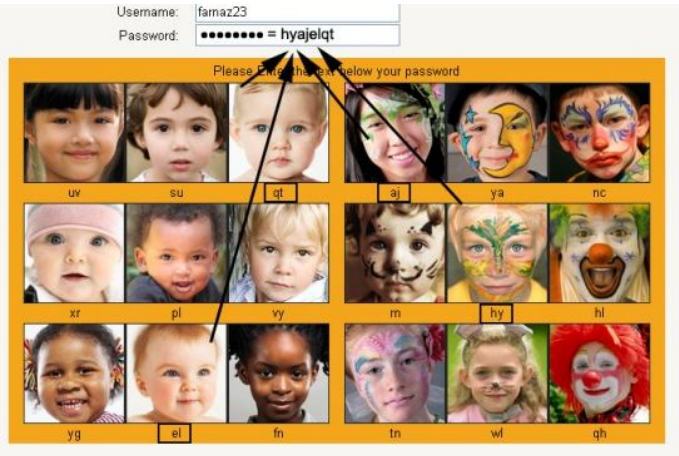

Figure 3: The Second Round of Login in S-Passface

Omission Password Assignment: The usability enhancements of Passface do based on the research on password memorability which shows that when a random password is assigned to a user, they can hardly remember it, in compare with the situation where the users can select their own passwords [19]. As in the Passface algorithm the password assigned to uses by the system, in the S-Passface users have the choice to selects their own password.

TEST AND ANALYSIS USABILITY

For creating a feedback on usability of both algorithms, an online questionnaire creates that fills up with fifty two students. This sample includes thirty male and twenty two women from three universities, includes University Technology Malaysia (UTM), University Malaya (UM), and University Kebangsaan of Malaysia (UKM). According to research, all the usability features classified to three categories of "Satisfaction", "Effectiveness" and "Efficiency" which shows in Table 1. Each of the usability attribute have special characteristic as following [16, 20]. This Table shows the usability attributes according to ISO standard that can satisfy users in each Graphical Password Algorithm [21-22]. All these attributes explain in the next section [20].

Easy to Use: The graphical password should provide no complication in usage of mouse or keyword, so creating and selecting password should be easy for the user.

Easy to Create: This phase refer to simple method of creating password. Although the password in graphical password can selects among a group of image or by drawing a shape, but the process of creation should be fast and simple to the user.

Table 1 Usability Features of Graphical Password Algorithm

Usability Features	Attributes	Attributes for Image Password
Satisfaction	Easy to Use	Use the Mouse or Keyboard
	Easy to Create	Simple Way to Create Password
	Easy to Memorize	Meaningful and Memorable
	Easy to Execute	Simple Steps of Activities
	Fast to Execute	Fast to Execute
	Pleasant Interface	Select Good Interface
	Pleasant Pictures	Pleasant Pictures
Effectiveness	Reliability	Reliability
Efficiency	Acceptable in Real World	Acceptability

Easy to Memorize: Several attributes provide more memorability which should be considered in designing new algorithm like using high quality and colorful picture in the recognition category and also using natural picture with high spot for recall category.

Easy and Fast to Execute: Some of graphical password is so complicate that needs several training session which is exhausted for the user, so the design should be without any complication. Also the duration of login and registration phase, should not take long as it brings more chance for the attacker to compromise password.

Pleasant Pictures: Using high quality and color picture, especially in portraits bring more satisfaction for the user.

Reliability: There is always a question. How much the user can accept the new algorithm in the real world? The answer of this question covers this attributes of usability.

Acceptance: The average of usability and security indentify how much the user can accept the algorithm as a real authentication in daily activity.

TEST AND ANALYSIS SECURITY

The attacking session designed for validating the vulnerability of Passface and Secure Passface to shoulder surfing attack. This has been done by using the Center for Advanced Software Engineering (CASE) Lab of UTM University

and fifty two student of Master degree of Software Engineering in Information Security. The participant one by one attended the attacking session, by examiner who started a brief introduction to Passface and S-Passface. Then a form distributed to participant with two sections. The first part collected demographic information including sex, course and level of study and the university. In the second part of questionnaire, there were two grids with twenty images of decoys which included the password of examiner. The participant had to play the role of shoulder surfer attacker, to attack the examiner for two times in each algorithm. This attacker had an option to sit next to or behind the examiner, or even move from one side to other, to find a best condition for observing the password.

After preparing all these preconditions, the examiner started to login to his account with Passface algorithm, to select his three images of password while attacker tried to observe the password. When the examiner could successfully authenticate, the attacker filled the questionnaire by finding the password among decoys images in the questionnaire. This process repeated for the second time, for creating an attack for twice. In the second step, the examiner started to login to his account with S-Passface algorithm, to select his four images of password. In this part the examiner entered the two random characters below each faces of his password. The attacker filled the form by trying to capture the screen and keyboard at the same time in order to find the password.

USABILITY RESULTS

The Table 2 shows the results of usability questionnaire which validate two algorithms as follow:

Easy to Create: For analyzing this feature it was asked "Which algorithm has simple and easy steps through registration?" The reason for stressing on registration is because creating password is done only in registration phase. 56% of users see the Passface registration more easily in creating password in compare with 38% of others.

Easy to Use: In the usability questionnaire it was asked "In which algorithm selecting your password is easier for you (Using mouse in Passface or keyboard in S-Passface)?" Around 75% of users find the Passface algorithm much easier to use, in compare with 26% of remain.

Easy to Memorize/Remember: Two questions focused on this features of usability. First, "In which algorithm you can memorize your password easier?" and second "According to you in which algorithm you can remember your graphical password easily?" The average of result shows that during registration, 56% of users, and in the login phase, around 60% of users can more easily memorize and remember their password through S-Passface algorithm.

Easy to Execute: For analyzing this feature, two questions asked first, "Registration in which algorithm is simpler and faster according to you?" and second "The login process in which algorithm is simpler and faster?" According to Table2, 63% of users in the registration, and around 60% of users in the login phase believed that the new features of Secure Passface like omitting of mouse, using random text and changeable password make the algorithm more complex than the previous one.

Fast Execution: Two questions can collect user's feedback on this feature. The first one asked "In which algorithm can you finish the registration faster?" and the other "In which algorithm can you select your password faster (considering the round and recognizing the password)?" According to 63% of users the registration phase in Passface finished quicker than S-Passface and also 59% of users find the S-Passface login faster than Passface.

Table 2 Summary of Usability Feedback

Satisfaction During Registration		
Features	**Passface**	**S-Passface**
Easy to Create	56 %	38 %
Easy to Remember	34 %	60 %
Easy to Execute	63 %	32 %
Fast Execution	63 %	35 %
Pleasant Interface / Pictures	38 %	66 %
Satisfaction During Login		
Features	Passface	S-Passface
Easy to Use	75 %	26 %
Easy to Memorize	43 %	56 %
Easy to Execute	60 %	35 %
Fast Execution	35 %	59 %
Pleasant Interface / Pictures	32 %	71 %
Effectiveness		
Features	Passface	S-Passface
Reliability	40 %	71 %
Efficiency		
Features	Passface	S-Passface
Acceptability on Security	22 %	75 %
Acceptability on Usability	50 %	43 %

Pleasant Interface and Pictures: The results shows that all users are satisfy in interface and design of S-Passface algorithm during registration and login. The result in Table2 shows that 66% of users liked the picture and interface of S-Passface registration and 71% of users satisfied with the interface of login phase.

Reliability: For having a feedback on how the users can trust the S-Passface algorithm a question asked that "Do you like to use this algorithm as login part of your online authentication system?" According to Table 2, 71% of users accepted to use S-Passface as part of their authentication.

Acceptability: For having a feedback on acceptability of two algorithms, a question asked: "From security point of view, which of these algorithms would you prefer to select for your authentication?" Also a same question asked for usability acceptance which was "From usability point of view, which of these algorithms would you prefer to select for your authentication?" According to Table 2, 75% of users accept the S-Passface algorithm to Passface according to security point of view but the result show that the new algorithm loss usability which was expectable (50% of users prefer the usability of Passface algorithm). This results shows that always there should be a balance between usability and security. Increasing usability cause decreasing security and vice versa.

Table 3 Summary of Security Feedback

Features	Passface	S-Passface
Switching Password	21 %	81 %
Random Text	23 %	71 %
Omitting Assigning Password	21 %	74 %

Three separate questions considered in online questionnaire to find the user idea about the security of both algorithm. Firstly it asked "How do you think about the switching password in S-Passface Algorithm?" According to Table3, around 81% of users approved that switching system will make the S-Passface algorithm more secured but 21% of users believe that the switching system will decrease the usability of algorithm. In the next steps the user opinion about random text gathered by questioning "Selecting password in original algorithm is done by mouse clicking. In the S-Passface it replaced with entering text below each picture. Which algorithm is more secure?" Results of Table 3 reveals that 71% of users approved that elaborating the mouse usage in S-Passface algorithm makes it more secured than Passface, this result proves the idea that omitting mouse during login, makes the algorithm to be more secured in shoulder surfing attack.

The last question was "Which algorithm is more secured in registration phase? The one which assigned your password or S-Passface where you select your own password". 74% of users found that the algorithm is more secured when they have the permission to select their own passwords. To sum up, the users believed that the extra features like switching password, random text and omitting assigning password which is used in S-Passface algorithm, increasing the security of this algorithm.

SECURITY RESULTS

The finding in Table 4 reveals that in S-Passface algorithm, none of the attacker was able to successfully compromise all four passwords of the user. Around 8% of users could compromise three pass-images, 25%, two pass-images and 35% could successfully compromise one password picture. Around 33% of users could not identify any password pictures at all. According to Table 5 around 53 percent of users could successfully identify all three password of examiner while none of users in S_Passface could identify all four passwords. Also 35% of users successfully identify two pass-image and 12.5% distinguish one password. According to this table 0 percent of user remain deactivate, so all users where successfully identify at least one password in Passface method.

Table 4 Summary of Shoulder Surfing Attack on S-Passface

	Number of Compromise Password				
	Four	Three	Two	One	Zero
First Attack	0	1	7	3	7
Second Attack	0	0	3	11	6
Total Number	0	1	10	13	13
Total Percent	0	7.5 %	25 %	35 %	32.5

Table 5 Summary of Shoulder Surfing Attack on Passface

	Number of Compromise Password			
	Three	Two	One	Zero
First Attack	7	8	5	0
Second Attack	14	6	0	0
Total Number	21	14	5	0
Total Percent	52.5 %	35 %	12.5 %	0 %

DISCUSSION

According to results, increasing the security of Passface decreases its usability. Firstly omitting mouse to keyboard input was not easy for the users; also creating password in Passface was more easily in compare with S-Passface. The reason was that when the password assigned automatically by the system in Passface, the process of

creating password finished easily in compare with the situation that users needed to select their own password. But the positive point was that, the S-Passface was more memorable in compare with Passface. This result prove the previous research which shows, users can remember the random password harder than the password of their own. So in average the new features of Secure Passface like omitting of mouse, using random text and changeable password make the algorithm more complex than the previous one. The results of attacks to S-Passface algorithm shows, this algorithm was hundred percent successful in case of shoulder surfing attack, as none of attackers could compromising all the four passwords of S-Passface in compare with Passface that at least half of attackers could compromise all three Pass-images. Even according to examiner comment, the attackers in some cases tried to guess when they found it difficult identify password, but according to results the attackers could guess password more precisely in S-Passface in compare original algorithm.

CONCLUSION

Most studies on security and usability seem to confirm the belief that the system can be either secure or usable, but researchers try to build or enhance systems which balance both. This paper proposes an algorithm for enhancement on usability and security of the "Passface", one of the recognition based algorithms. For increasing usability, it tries to cover most usability attributes based on ISO definitions of usability. In terms of security, the system tries to mitigate shoulder surfing attacks by changing the method of selecting the password during login and using a changeable password. The algorithm is validated using questionnaires and attacking session. The online questionnaire compares the two algorithms from the usability point of view and the shoulder surfing attacking session gather the reaction of both algorithms to shoulder surfing attacks. The result shows that the new system is hundred percent resistant to shoulder surfing in compare with the original one but this enhancement reduce some of usability features. As the method itself covers many usability features adding more security, helps us to name the new algorithm "Secure Passface" which in brief is named S-Passface throughout the whole paper.

ACKNOLEDGMENT

The authors would like to express their sincere thanks to the Government of Malaysia for founding their research via research University Grant Scheme (GUP Grant) with vote no: 02H07, ministry of higher education (MOHE) for the financial support of research work.

REFERENCES

1. Stobert, E., et al., *Exploring Usability Effects of Increasing Security in Click-based Graphical Passwords.* 2010.
2. Eljetlawi, A.M. and N. Ithnin, *Existing Recognition Base Usability Features of the Graphical Password.* 2010.
3. Brostoff, S. and M.A. Sasse, *Are Passfaces more usable than password.* 2000.
4. Alireza Pirayesh Sabzevar and A. Stavrou, *Universal Multi-Factor Authentication Using Graphical Passwords*, in *International Conference on Signal Image Technology and Internet Based Systems*. 2008, IEEE.
5. Davis, D., F. Monrose, and M. K. Reiter. *On User Choice in Graphical Password Schemes*. in *13th USENIX Security Symposium*. 2004. CA, USA.
6. Bandyopadhyay, S.K., D. Bhattacharyya, and P. Das, *User Authentication by Secured Graphical Password Implementation*, in *Information and Telecomunication Technologies*. 2008, IEEE: Bandos Island
7. Hu, W., X. Wu, and G. Wei, *The Security Analysis of Graphical Passwords*, in *International Conference on Communications and Intelligence Information Security*. 2010, IEEE.
8. Towhidi, F. and M. Masrom, *A Survey on Recognition-Based Graphical User Authentication Algorithms.* International Journal of Computer Science and Information Security (IJCSIS) 2009. **6**(2).
9. Kumar, V., et al., *Click to Zoom-inside Graphical Authentication.* 2009.
10. Wiedenbeck, S., J. Camille Birget, and A. Brodskiy, *Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice.*, in *Symposium On Usable Privacy and Security (SOUPS)*. 2005: PA, USA.

11. H., M.D., et al., *Towards Identifying Usability and Security Features of Graphical Password in Knowledge Based Authentication Technique*, in *Second Asia International Conference on Modelling & Simulation.* 2008. p. 396-403

12. Gao, H., et al., *A New Graphical Password Scheme Resistant to Shoulder-Surfing*, in *International Conference on Cyberworlds*. 2010, IEEE: Singapore p. 194 - 199

13. Hayashi, E. and N. Christin, *Use Your Illusion: Secure Authentication Usable Anywhere*, in *Symposium on Usable Privacy and Security (SOUPS) 2008*. 2008: Pittsburgh, PA USA.

14. Hafiz, M.D., et al., *Towards Identifying Usability and Security Features of Graphical Password in Knowledge Based Authentication Technique*, in *Second Asia International Conference on Modelling & Simulation.* 2008. p. 396-403

15. Dunphy, P., J. Nicholson, and P. Olivier, *Securing Passfaces for Description.* 2008.

16. Paul, D., N. James, and P. O., *A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords.* , in *Symposium on Usable Privacy and Security (SOUPS)*. 2006, ACM: Pittsburgh, Pennsylvania, USA. p. 56-66.

17. Man, S. and D. Hong, *A Shoulder-Surng Resistant Graphical Password Scheme - WIW*, in *International Conference on Security and Management*. 2003: Las Vegas.

18. Eljetlawi, A.M. and N. Ithnin, *Graphical Password: Prototype Usability Survey*, in *International Conference on Advanced Computer Theory and Engineering.* 2008, IEEE: Phuket p. 351 - 355

19. Yan, J., et al., *The memorability and security of passwords some empirical results.* 2000, University of Cambridge.

20. Eljetlawi, A.M., *Graphical password: Existing recognition base graphical password usability*, in *6th International Conference on Networked Computing (INC)*. 2010: Gyeongju, Korea

21. Eljetlawi, A.M. and N. Ithnin, *Graphical Password: Comprehensive study of the usability features of the Recognition Base Graphical Password methods*, in *International Conference on Convergence and Hybrid Information Technology*. 2008, IEEE: Busan p. 1137 - 1143

22. Masrom, M., F. Towhidi, and A. Habibi Lashkari, *Pure and Cued Recall-Based Graphical User Authentication*, in *Application of Information and Communication Technologies (AICT)*. 2009: Baku , Azarbyizan.