International Journal of Computer Networks and Applications
Volume 2, Issue 2, March – April (2015)

RESEARCH ARTICLE

Security Enhancement in Shoulder Surfing Attacks using Passpoints for Random Similar Images (PRSIm)

Dr. A. Meiappane,
Associate Professor, Manakula Vinayagar Institute of Technology, Pondicherry, India.

Dr. V. Prasanna Venkataesan
Associate Professor, Department of Banking Technology, Pondicherry University, Pondicherry, India.

V. Premanand
PG Student, Manakula Vinayagar Institute of Technology, Pondicherry, India.

Abstract –There exists many security primitives which use an alphanumeric password which uses hard cryptographic methods. Also the users struggle to remember the password for various internet services and if the user has a same password for various services then it is insecure. To avoid this, graphical passwords are designed and made more secure, memorable and also easier to use since the user is going to just click certain passpoints rather than typing an alphanumeric password. However, this scheme has achieved a limited success and due to its simple architecture it is not used widely. Passpoints also suffer a major drawback of shoulder surfing attacks when the passpoints are exposed in front of others. So to improve the security of this system we introduce a new system called Passpoints for Random Similar Images (PRSIm). This system use a set of similar images and have a common passpoints from which the password is been derived. While logging in a user a random image is generated and displayed from which the user have to identify a common passpoints which is already registered. So the user clicks the passpoints to derive the password which confuses the attackers while we have multiple login in front of them. Thus it is more secure than any other passpoints scheme and also eliminates the shoulder surfing attacks which are analyzed and the results are been given.

Index Terms – Graphical Passwords, Passpoints, authentication, tolerance value and security.

1. INTRODUCTION

In today's world, network security is formulated as a major problems and it is a technical issue for all the internet security systems. The alphanumeric passwords are used from the traditional systems which have usability problems where the users cannot maintain or remember various passwords for various web services. Now a days the technologies are developed that a password cracker can identify about 80% of passwords within 30 seconds which is done by a security team in a large company. On the other hand the passwords which are more secure and difficult to crack are very difficult to remember, also people will use a single password for different accounts or services because they can only remember a limited number of passwords [1, 2].

In order to improve the password authentication scheme there are many alternatives which have been proposed e.g. Biometrics, Token based authentication, Graphical Passwords, Multiple factors scheme which uses two or more authentication schemes. Here we are going to focus on single factor scheme. Numerous graphical password related schemes are given survey among which some common password systems are [3],

1. Recognition based systems.
2. Pure recall based systems.
3. Cued recall based systems.

In Recognition based systems the user can choose an image, icon, or a symbol from a large collection which is used for authentication [4]. The Recognition based schemes are very easy to remember but it takes a large space for storing the passwords and requires many rounds for image recognition which makes the system tedious.

In Pure recall based systems the user need to reproduce the passwords without any cues or hints. The best example for this scheme is Draw a Secret (DAS), where a peculiar shape is drawn in a grid [5]. The user should reproduce the same shape to authenticate them. The system is simple and quick to use but have shoulder surfing problems.

In Cued recall based systems the image is shown on a screen and the user should click on a few points which are pre-defined by them during registration [6]. So the user should click on the correct regions to log in thus it is more secure and thus solves shoulder surfing problems.

RESEARCH ARTICLE

Thus after the usage of CAPTCHA, which is the mechanism used for BOT protection [7] the graphical passwords came into existence to eradicate the difficulties in traditional password system. And the graphical passwords are more attractive and new to the user and many systems using graphical passwords came to existence which overcomes the alphanumeric password systems [8]. As already mentioned humans have tendency to choose weak passwords and similarly for DAS systems it is proved that humans choose mostly predictable patterns [24]. In this paper we focus about the passpoint systems and usage of some similar natural images with the click based Blonder graphical system and develops a system called Passpoints for Random Similar Images (PRSIm), where similar images are generated for each login which has exactly same passpoints. Similarly, several images are generated which have same properties and the discretization grids for the system recognizes the password.

2. RELATED WORK ON VARIOUS AUTHENTICATION TECHNIQUES

The user authentication are been categorized into three main mechanisms, they are Authentication using Biometrics (something you are), Authentication using Tokens (something you have), Authentication using Knowledge (something you know) [6, 24]

2.1 Authentication using Biometrics

This process refers to the identification of some physical or behavioral characteristics of the user which is unique includes fingerprints, palm print, knuckle print, iris scan, handwritten images, voice recognition and many more. In spite of the fact that biometrics are the most efficient and easy to use, it is very expensive to implement and cannot be adopted for the online services [9, 10]

2.2 Authentication using Tokens

Authentication process is a technique which requires the user to present a token, these tokens cannot be easily stolen, reproduced or forgotten. But an additional hardware is needed which cannot be provided for online services since it is inconvenient [11].

2.3 Authentication using Knowledge

The main categories of this authentication method is Textual Passwords and Graphical Passwords where we are going to concentrate on the graphical passwords which includes recognition-based, recall based and cued-recall based techniques. To pass the authentication in the recognition based techniques the earlier selected images should be identified by the user during the registration phase. In the recall based authentication the user must reproduce the created or selected points from a specific image during login [12]. Where as in Cued recall based authentication the user must select the set of points in a specific order accurately which the user has registered already.

3. ALGORITHMS FOR VARIOUS GRAPHICAL PASSWORDS

3.1 Triangle Algorithm

Triangle algorithm was developed in 2002 by Sobrado and Birget [13], which is mainly dealt with shoulder surfing problem, in this algorithm the user is asked to select a certain number of objects from N number of proposed objects (may be a few hundred or few thousand). To authenticate the user has to select the previously selected objects from the proposed images. But the objects are been shuffled and appears in different locations. The main disadvantage of this algorithm is the system is crowded and it is very difficult for the user to distinguish the images.

Figure 1. Authentication in Triangle Algorithm

3.2 Passface Algorithm

The Passface algorithm was developed by Brostoff and Sasse in 2000 [14] who proposed a new graphical scheme. The user is been asked to select a certain number of images of human faces from a database of images containing different human faces. During authentication the user must recognize the previously selected images from a grid in a shuffled manner. The people can select the images based on some obvious behavioral pattern then it can be easily predictable [18] so the system is more vulnerable on various attacks.

Figure 2. Authentication using Passface Algorithm

RESEARCH ARTICLE

3.3 Draw a secret Algorithm

The DAS Algorithm was proposed by Jermyn, Mayer, Monrose, Reiter, and Rubin in 1999 [15], in which the user is allowed to draw a unique pattern password in a 2D grid during registration and stored as an order of the pattern. During authentication the user redraws the pattern by touching the same points in the grid in same sequence. The main disadvantage is that the user selects weak graphical passwords which make the authentication mostly predictable and the system is vulnerable on various attacks [16].

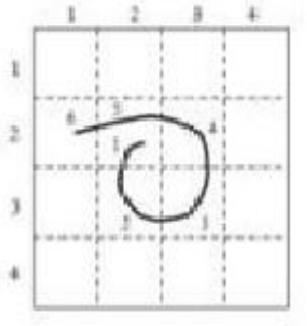

Figure 3. Authentication in Draw a secret Algorithm

3.4 Syukri et al algorithm

The syukri et al algorithm was proposed by Syukri, Okamoto, and Mambo in 2005 [17] which is a new graphical authentication where the user is asked to draw a signature with help of an input device and during authentication the system identifies the signature by extracting the parameters of the user's signature. The biggest advantage is that the signature are hard to be reproduced and there is no memorizing of password but the main drawback is that we cannot use a mouse to put a signature, a pen like input device is required which requires an additional hardware.

Figure 4. Authentication in Syukri et al algorithm

3.5 Blonder Algorithm

Blonder proposed a new algorithm for graphical authentication in 1996 [6], where an image is been used and the user must click on several locations on that particular image during registration and must reselect the same locations in similar order for authentication. The image acts as a hint for the user to reproduce the password thus this system is the most convenient of the other pure recall-based schemes. The major disadvantage is the defined click areas are very small and not so accurate and it uses only simple images which are sketched and we can't use the real world images [18, 19].

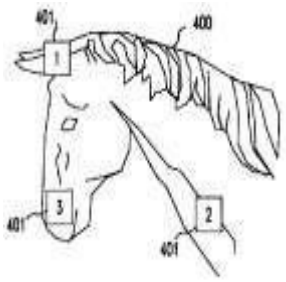

Figure 5. Authentication using Blonder Algorithm

4. PASSPOINT SYSTEM FOR CLICK BASED PASSWORDS

The Passpoints are designed to cover the limitations of the blonder algorithm consists of a high quality pictures which is rich enough to have many possible clicks, complex images may have hundreds of memorable click points, for example 5-6 click points will make comparatively stronger passwords than alphanumeric passwords. In order to login the user has to click on the already registered click points within some tolerance points say around .25 cm in the click points. The tolerance point is needed because the user has to click the password within a certain pixel and the user cannot click accurate pixel all the time for successful login. The tolerance point is adjustable to the system and margin of error is been used for a correct recognition of the user. The passpoints are more secure than alphanumeric passwords by comparing alphanumeric passwords of length 8 over 64-bit character the number of possible passwords is 64^8=2.8 x 10^{14} and in passpoints the maximum image size is 1024 x 752 (full screen) with a tolerance of around 20 x 20 pixels for passwords consisting of 5 clicks the password space will have a size of 2.6 x 10^{16}.

The Passpoints and alphanumeric passwords were been compared and studied in a laboratory [11, 20], to learn about the memorability if graphical passwords. The results showed that the participants from the graphical password group created valid passwords without difficulties than the participants of alphanumeric group. But the graphical group made more errors and took more attempts in carrying out the practice since this type of password was entirely new to them. Also all the graphical password users were able to reach the learning criteria within some minutes.

RESEARCH ARTICLE

4.1 Study of image choice

To study about the graphical use of the passwords and how it succeeds, the psychologists have studied that the images are having more focused memory than compared to words and sentences which was called as 'picture superiority effect' [21]. Thus everyday images are chosen and they are made as passwords which gives a clear knowledge about learnability and memorability while using different images. And the higher number of accurate passpoints was found when there is a constant tolerance value is given for the system and thus gives an increased performance [11, 20]. Thus it concludes that a limited knowledge is been required for the use of graphical password an thus an average user can use this authentication system easily except some rare cases also the image with poor memorable character can be also accepted if used similarly and some practice is needed because there is a chance for forgetting password because of infrequent use. As we see in using the graphical passwords we have the better results of high performance, quick learning and accuracy for people who are having poor memorability who can work easily with some practice.

4.2 Prediction in Graphical passwords

There are several studies based on the prediction of the passpoints and the portions that a human focus in common [22, 23]. The human nature is that when asked to click any particular pixels the people will focus on a particular points of same frequency which is illustrated in figure 1 which are the click points actually clicked by the users. We can see that there are click locations which are most likely given as passwords, but the users click points reduces the entropy of the click locations. Thus the users entropy of the password clicks are been observed and those entropies are been predicted. By using mean-shift segmentation algorithm [24, 25] that predicts the most likely click location with their probability values, thus the users must select the images with higher entropy of their click points.

4.3 Predicted vs Actual click locations

Figure 6 (a). Predicted Click Locations

Figure 6 (b). Actual Click Locations

In the above image the users were given the images and they were made to choose their own passpoints consisting of 5 click points and were asked to re-enter, the passpoints which has been re-entered is been taken into account. The same image is been predicted by using mean-shift segmentation algorithm with having 10 pixels of tolerance for both cases of 400 x 600 pixels image. The system predicted the points with 80% accuracy for a normal image having high entropy value. The entropy value of the image, the accuracy percentage, and increased number of click points decides the strength of the password. Thus only after 31^5 ($\approx 2.8 \cdot 10^6$) iterations we can crack a user's image password. From here we can define that an image which has more number of clicks and less entropy value is more secure. By using many advanced algorithms the passpoints are been predicted.

5. PROPOSED WORK

5.1 Passpoints for Random Similar Images (PRSIm)

Normal passpoints system have a single image where the click points are been given and for each login the same image is been displayed again and again for every login. When this process is been repeated for multiple login it may lead to shoulder surfing attacks. So in order to avoid the shoulder surfing attacks, some similar images are used here and those images will be having the same passpoints which is mapped by a grid whose points are stored and then retrieved during login. It is done by mapping those images with a grid and the clicks are given grid values thus the image is not used for authentication instead the grid values are used. Thus from this process we can reduce the shoulder surfing attacks but the tolerance value must be little high for the accuracy which may have guessing attacks.

Algorithm for registration:

1. Begin.
2. Select an image type (ex. Animal, bird, human face).
3. Select the type of sample images as prescribed.
4. Set the passpoints.

RESEARCH ARTICLE

5. Store the passpoints in a graph and store the graph points in Database.
6. End.

Algorithm for login:

1. Begin.
2. Select image type (ex. Animal, bird, human face).
3. **If** (select == Database)

   { Show (Authentication) }

   else

   { Access Restricted }

   end if
4. Display the random image from database.
5. Select the passpoints which is registered.
6. **If** (select == Database)

   { Show (Authentication)}

   else

   { Access Restricted }

   end if
7. Stop.

We have to select the image properties such that the user should click on a specific property where the images are given a specific group e.g. a list of image types are given as Dog, Cat, Duck etc. from where the user say selects dog, then the set of images of dog is given from where the user selects the passpoints. At the back-end the passpoints are stored as a graph points in which the images are been mapped similarly, thus only the image changes not its property (i.e. a face is mapped with its similar faces having the same properties) so during login the set of images are been displayed to the user and user clicks the appropriate passpoints to proceed.

Figure 7. Attempt I for Login using passpoints for random similar images (PRSIm)

Figure 8. Attempt II for Login using passpoints for random similar images (PRSIm)

5. EVALUATION AND DISCUSSION

The main objective of this paper is to reduce the shoulder surfing attacks when using the graphical passwords for authentication. So the hacker is been confused by using two or more images and thus designing more efficient system for authentication. The test and analysis gives us the result that only 12% of the hackers can identify the passpoints by performing the shoulder surfing attack which is tested from real environment of the passpoints for random similar images (PRSIm) algorithm. After some continuous login made by users and 90% of users made successful login by this process. But the major fact is that the images cannot be more complex. The simple images are used here to reduce the difficulty in searching similar images. Hence the tolerance value must be comparatively high to increase the accuracy of the password. We studied about various usability features about this passpoints for random similar images (PRSIm) algorithm and we get the results that our algorithm is more efficient and secure than other algorithms. The comparison of different schemes are been presented in table 2 and 3 the * cell is been tested in real time environment and other cells are taken from previous researches [26, 27, 28].The WEKA Data Analysis Tool is used to derive the tables and graphs presented here.

Usability features	**Facts**
Effectiveness	Reliability
Satisfaction	Easy to use, create, memorize, execute, understand. Use of simple image.
Efficiency	Easily applicable.
Intuitiveness	The interface is easy to learn and navigate.

RESEARCH ARTICLE

Low perceived workload	The interface appears easy to use, rather than intimidating.

Table 1. Usability Features

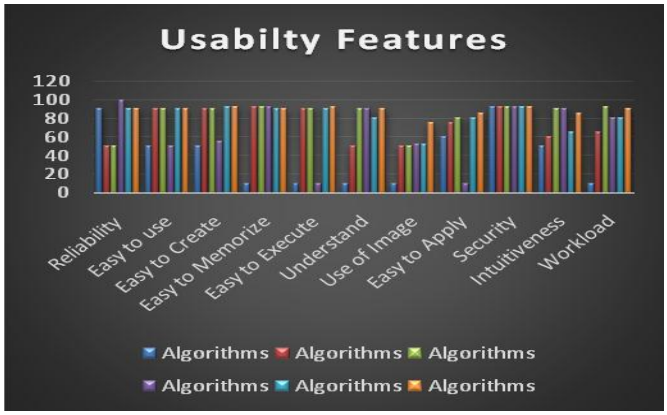

Figure 9. Graph for Usability Features

6. CONCLUSION

The most common attacks on graphical passwords are dictionary attacks, guessing attacks, spyware attacks and shoulder surfing attacks among which shoulder surfing is a major problem in Graphical password system. Thus the main idea was to eradicate this attack and this system is more efficient than any other algorithms e.g. Passpoint algorithm, Triangle algorithm, GPIP, DAS, syukri algorithm, Blonder algorithm etc. Our study of comparing with other algorithms gives us positive results and we give a better system than other traditional algorithms. Our future work focus on using high resolution graphical images with more accuracy. The passpoint have high tolerance value which is good enough for the system, even then the accuracy value should be increased at par where the tolerance value must be reduced in such a way that it is accepted by all.

REFERENCES

[1] R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in Proceedings of 9th USENIX Security Symposium, 2000.

[2] M. Kotadia, "Microsoft: Write down your passwords," in ZDNet Australia, May 23, 2005.

[3] Xiaoyuan Suo, Ying Zhu, Owen, G.S, "Graphical passwords: a survey" Computer Security Applications Conference, 21st Annual 5-9 Dec. 2005, 1063-9527, IEEE, Computer Security Application.

[4] M. Boroditsky, \Passlogix Password Schemes" (2002). http://www.passlogix.com.

[5] Lashkari, A. H., Towhidi, F., Saleh, R. & Farmand, S. (2009) A complete comparison on Pure and Cued Recall-Based Graphical User Authentication Algorithms, Second International Conference on Computer and Electrical Engineering.

[6] Blonder, G., 1996. Graphical Passwords. United States Patent, 5: 559-961.

[7] V Premanand, A Meiappane and V Arulalan. "Survey on Captcha and its Techniques for BOT Protection" International Journal of Computer Applications109 (5):1-4, January 2015.

[8] Suo, X., Zhu, Y. & Owen, G.S. Graphical Passwords: A Survey.

[9] Arulalan.V, Balamurugan.G, Premanand. V "A Survey on Biometric Recognition Techniques" International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 2, February 2014.

[10] Biddle, R., Chiasson, S. & Oorschot, P. (2011) Graphical Passwords: Learning from the First Twelve Years.

[11] Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A. and Memon, N. Authentication using graphical passwords: Basic Results. Proc. Human-Computer Interaction International 2005, in press.

[12] Gao, H., Liu, X., Dai, R., Wang, S. & Liu, H. (2009) Design and Analysis of a Graphical Password Scheme, Fourth International Conference on Innovative Computing, Information and Control.

[13] L. Sobrado and J. C. Birget, "Graphical passwords," The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4, 2002.

[14] Are Passfaces more usable than passwords? A field trial investigation - Brostoff, Sasse – 2000.

[15] Ian Jermyn, Alain Mayer, Fabian Monrose, Michael K. Reiter, and Aviel D. Rubin "The Design and Analysis of Graphical Passwords", Proceedings of the 8th USENIX Security Symposium Washington, D.C., USA, August 23–26, 1999.

[16] Lashkari, A. H., Towhidi, F., Saleh, R. & Farmand, S. (2009) A complete comparison on Pure and Cued Recall-Based Graphical User Authentication Algorithms, Second International Conference on Computer and Electrical Engineering.

[17] A.F. Syukri, E. Okamoto, M. Mambo, "A User Identification System Using Signature Written with Mouse," In Proceeding(s) of the Third Australasian Conference on Information Security and Privacy (ACISP), pp. 403-441, 1998.

[18] J.Thorpe, P.C. Van Oorschot, "Towards secure design choices for implementing graphical passwords", Computer Security Applications Conference (2004). [24] Khandelwal, A., Singh, S. & Satnalika, N. User Authentication by Secured Graphical Password Implementation.

[19] Lashkari, A. & Towhidi, F. (2010) Graphical User Authentication (GUA), LAP LAMBERT Academic Publishing, Germany.

[20] Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A. and Memon, N. PassPoints: Design and longitudinal evaluation of a graphical password system. Special Issue on HCI Research in Privacy and Security, International Journal of Human-Computer Studies, in press.

[21] Paivio, A., Rogers, T.B. and Smythe, P.C. Why are pictures easier to recall than words? Psychonomic Science 11, 4 (1976), 137-138.

[22] J. Findlay, "The visual stimulus for saccadic eye movement in human observers", Perception (1980) 7-21.

[23] J. Senders, "Distribution of attention in static and dynamic scenes", Proc. of SPIE, 3016 (1997) 186-194.

[24] D. Comaniciu, P. Meer, "Mean shift analysis and applications", 7th International Conference on Computer Vision (1999) 1197-1203.

[25] D. Comaniciu, P. Meer, "Mean shift: A robust approach toward feature space analysis", IEEE Transactions on pattern analysis and machine intelligence 24(5) (2002) 603-619.

[26] Lashkari A.H. and Farmand S. (2009) A survey on usability and security features in graphical user authentication algorithms International Journal of Computer Science and Network Security (IJCSNS), VOL.9 No.9, Singapore.

[27] Masrom M., Towhidi F., Lashkari A.H. (2009) Pure and cued recall-based graphical user authentication, Application of Information and Communication Technologies (AICT).

[28] Lashkari A.H., Saleh R., Farmand F., Zakaria O.B. (2009) A Wide range Survey on Recall Based Graphical User Authentications Algorithms Based on ISO and Attack Patterns", International Journal of Computer Science and Information Security (IJCSIS), Vol. 6, No. 3.

RESEARCH ARTICLE

Authors

Dr. A. Meiappane, Associate Professor, Department of Information Technology, Manakula Vinayagar Institute of Technology, Puducherry, India. He holds M.Tech. in Computer Science & Engineering and an interdisciplinary research degree Ph.D in Computer Science & Engineering (Banking Technology) from Pondicherry Central University, India. His areas of Interest include Software Engineering, POSA, and Networks and distributed computing. He is also serving to the professional societies as research paper reviewer for various journals and conferences and also reviewed software engineering books for Tata McGraw Hill. He is also a member of various professional bodies.

Dr. V. Prasanna Venkatesan, Associate Professor, Dept. of Banking Technology, Pondicherry University, Puducherry, India. He has more than 20 years teaching and research experience in the field of Computer Science and Engineering. His research interest includes software engineering, Business intelligence, Software Architecture and banking technology. He has designed Multilingual Compiler. He has many international Journal publications. He is co–author of the book titled as "Service Composition and Orchestration: Concepts and Approaches" published by VDM Verlag Dr. Muller E.K.

Mr. V. Premanand completed B.Tech. in Information Technology at 2012 and pursuing his M.Tech. Computer Science and Engineering under Pondicherry University, [MIT] Manakula Vinayagar Institute of Technology, Puducherry. His areas of interests include Computer Networks and Information Security.

	Triangle Algorithm	Passface Algorithm	Draw a secret Algorithm	Syukri et al algorithm	Blonder Algorithm	PRSIm Algorithm*
Automatic Online Guessing Attacks	Yes	No	No	Yes	Yes	Yes
Human Guessing Attacks	No	No	No	Yes	No	Yes
Relay Attacks	Yes	No	No	No	Yes	Yes
Dictionary Attacks	Yes	Yes	Yes	Yes	Yes	Yes
Brute-force attack	Yes	Yes	No	Yes	Yes	Yes
Shoulder-Surfing Attacks	Yes	No	No	No	No	Yes

Table 2. Comparison of Attacks with other Algorithm

RESEARCH ARTICLE

Usability features	Algorithms					
	Triangle Algorithm	Passface Algorithm	Draw a secret Algorithm	Syukri et al algorithm	Blonder Algorithm	PRSIm Algorithm*
Reliability	90	50	50	99	90	90
Easy to use	50	90	90	50	90	90
Easy to Create	50	90	90	55	92	92
Easy to Memorize	10	92	92	92	90	90
Easy to Execute	10	90	90	10	90	92
Easy to Understand	10	50	90	90	80	90
Use of Image	10	50	50	52	52	75
Easy to Apply	60	75	80	10	80	85
Security	92	92	92	92	92	92
Intuitiveness	50	60	90	90	65	85
Workload	10	65	92	80	80	90

Table 3. Comparison of Usability Features with other Algorithm