An Approach Towards Usability Parameter for Graphical Based Authentication System

[1.] Priti C. Golar, [2.] Dr. Brijesh Khandelwal

[1]Research scholar
Department of Computer Science & Engineering
Amity University
Raipur, (Chhattisgarh), India
priticgolar@gmail.com
[2]Associate Professor
Département of Computer Science & Engineering
Amity University
Raipur, (Chhattisgarh), India
bkhandelwal@rpr.amity.edu

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 23 May 2021

Abstract: Authentication systems are the protective barrier of any software. The authentication system can be classified as Token based, Biometric based and Knowledge based. This research study is based on knowledge based authentication system. As an initial step the existing knowledge based authentication system has been studied for its highlights, comparative facts, advantages and disadvantages. For acceptance of any secure system the usability aspect is the first step in the authentication process. The various usability evaluation parameters of the existing systems and an approach towards developing a modified usable authentication system have been briefly discussed. Future scope of other dimensions viz. randomness and security and a deep study have been highlighted as the concluding remark of this research work.

Keywords: Authentication system, usability, randomness, security.

1. Introduction

Authentication is the process of information security. Authentication methods can be divided into following three main areas:
(1) Token based
(2) Biometric based
(3) Knowledge based
In Token based systems, such as key cards, and smart cards are widely used. Many token-based systems also refer knowledge based techniques to enhance security. For example, PIN number associated with DEBIT/CREDIT cards.[1]. In Biometric based authentication techniques, such as fingerprints, iris scan, etc., are not yet widely adopted. The major drawback of this approach is that such kinds of systems can be expensive, and the identification process can be slow and often unreliable [1]. Knowledge based techniques are the most important authentication techniques and which include both text-based and picture based passwords. The picture-based techniques can be further divided into two types: recognition-based and recall-based graphical systems [9]. In recognition-based techniques, a set of images provided to a user and then recognizing and identifying the images user selected during the registration phase [2]. Using recall-based techniques, a user is asked to reproduce something new password that he or she created or selected earlier during the registration phase [9]. Graphical password schemes have motivated partially by the fact that humans can remember pictures better than text.

2. Literature Review

In this section, seven major paper along with their various parameters for comparison and problem identification have been elaborated.

Table 1. Findings, Shortcoming, advantages authored by Patra K,Nemade B, Mishra P (2016), with respect to usability [1].

Parameter	Findings	Shortcomings	Advantages

Authentication Process	Apply persuasion on Cued Click Point which uses circular tolerance.		Password Space can be increased due to circular Tolerance
Image Selection	Displaying of 2nd image depends upon the 1st image.	Predefined image displayed. 50 images are used.	
Login Time		More Login time due to CCP.	
Memorability	High		

Table 2. Findings, Shortcoming, advantages authored by Boonkrong (2019) with respect to usability [2]

Parameter	Findings	Shortcomings	Advantages
Authentication Process	Grid based system (Grid Cell-30,60,90,120,150&180)		Depending on the requirement the size of the grid can be change.
Image Selection	User has to select 8 cells. Each cell is filled with random numbers between 0-9.		
Success Rate		Grid increases then success rate decreases.	
Memorability		Controversy in Grid size and Memorability	
Users	Heterogeneous group of people		
User Satisfaction	Created Questionnaires.		

Table 3. Findings, Shortcoming, advantages authored by Jerome P, Ariel M(2019)with respect to usability [3]

Parameter	**Findings**	**Shortcomings**	**Advantages**
Authentication Process	Applying Random Grid Traversal Technique		Effectively overcome hotspot guessing attacks and alleviate shoulder-surfing attacks.
Image Selection	Single image is replaced with several independent images.		
Login Time		Authentication speed is less	
Memorability		Memorability and registration speed is less	
Users	Homogeneous Users	30 Users	
Storage		Images stored in database.	
External Devices		To capture the audio signal headset is required.	

Table 4. . Findings, Shortcoming, advantages authored by Zujevs N(2019)with respect to usability[4]

Parameter	**Findings**	**Shortcomings**	**Advantages**

Authentication Process	Array concept consists of color, shape and number.		Can protest passwords from shoulder surfing. No need additional devices. Passwords are easier to remember. Can be implemented on Mobile and ATM Entropy is good.
Image Selection	Combining several images in one picture.		
Login Time		More login Time	
Users	Homogeneous users	32 Users	
Storage		Password stored in the form of pictures.	

Table 5. Findings, Shortcoming, advantages authored by Nida A., Quasim A(2019)with respect to usability [5].

Parameter	**Findings**	**Shortcomings**	**Advantages**
Authentication Process	Mainly four stages are involved in the whole process are Picture Selection, Picture Division, Pattern Generation and Grid Shuffling.		Minimize shoulder surfing attack.
Image Selection	In authentication the image will be displayed to the user with same grids, but in shuffled form.		
Login Time		More login time	
Memorability	User has to remember 3 distinct points.		
User Satisfaction	Created Questionnaire		

Table 6. Findings, Shortcoming, advantages authored by Ansari S, Rokade J, Khan I, Shaikh A (2018)with respect to usability [6]

Parameter	**Findings**	**Shortcomings**	**Advantages**
Authentication Process	Sequence of image is provided to the user.		Ease for users to remember the password. Avoid Hotspot coverage
Image Selection	One click per image.		
Memorability	Ease to remember		
Storage		Images stored in the database	

Table 7. Findings, Shortcoming, advantages authored by Thorpe J, MacRae B(2014) with respect to usability [7]

Parameter	**Findings**	**Shortcomings**	**Advantages**
Authentication Process	Background image is provided to the users.		Presentation Effect is simple and acceptable.
Image Selection	Image Presentation style that drawing the curtain where the image is covered.		
Memorability	Memorability is good due to only one password reset occurred.		
Users		35 Users	
Login Time	25sec.		

User Satisfaction	80%

In the domain of authentication system, following are some more literature available which can support for developing a novel system under usability parameter.

Chiasson S and et.al (2012) includes evaluation and implementation of usability and security parameters an integrated evaluation of the Persuasive Cued Click Points Graphical Passwords schemes[8]. Biddle R and et.al (2012) highlighted novel features of existing approaches. It also covers both usability and security aspects including system evaluation[9]. Saeed S and Sarosh Umar M (2015) proposed a novel graphical authentication system that is a hybrid technique, combination of both recognition based and dynamic graphics. This new study demonstrated that the new scheme is robust, secure and high usability[10]. Andrea B, Ian O and Hyoungshick K. (2016) proposed three feasibility studies of PassBYOP examining its usability, security and its reliability[11].

Bellam A. (2013) stated that to increase the security on five number of images, process of click point was done. It also encourages user to select more secure password[12]. Khalifa H and et. al (2013) proposed and evaluated Edge Pass a new algorithm which extract the edges of pass images for a graphical system. In this the experimental results increases the effectiveness of the proposed system[13]. Radha A. (2013) presents a persuasion technique with dynamic user blocks to increase the security level. This system influence the user to create a password which is more secure [14]. Kumar Sarohi H and Ullah Khan F(2013), highlighted various issues regarding usability and security[15].

3. Approach Towards Usability Parameter

Based on the above mentioned research papers and their detail analysis, the prominent way towards the usability approach can put forward the problem definition. The various usability parameters can be synthesized to build up a novel graphical password system. The usability parameter since defines the acceptance of the system by the end users in various domain and complex environment needs a detail analysis. The various dimensions under which usability parameter can be evaluated, are given in following table no. 8.

Table 8. Details of Usability Evaluation Parameters

Usability Evaluation Parameter	**Description**
Authentication Process	Defines the complete Authentication Process.
Image Selection	Appearance and Presentation of an image
Login Time	Calculated from start to end process of Authentication.
Memorability	Indicates that how much time is required to recall the password.
Success Rate	Success Rate can be calculated on short term and long term basis.
Users	Homogeneous or Heterogeneous group of people
User Satisfaction	Can be conducted through Questionnaire
Storage	Password stores in the form of images or coordinates.
External Devices	For compatibility of the system.

The existing and the requirement towards building a novel graphical knowledge based system is discuss below.

1.1. Authentication Process

Authentication process is based on displaying the sequence of images. In some authentication process images are present in the Grid Cells. Image present in the form of array. So in proposed system images can be displayed randomly. A geometrical shape can be utilized to explore the authentication process.

1.2. Image Selection

According to the existing theories the user selects the most likely images depending on the favorite or peripheral events. The existing systems reflects combining several images in one picture or one click per image. The proposed system can be thought of one or more click on more than one images with multiple object.

1.3. Login Time

It is one of the concern area where the user can enter the secure system in a minimum login time. Since various images and the correct location of the password can require more login time. The proposed system should design in such a way that it requires less login time and should have an easy authentication process. The proposed system can contain a 2-tier/ 3-tier authentication process as to provide a more secure environment.

1.4. Memorability

Provided with the predefined set of images, many of the existing systems had used the concept of hotspot, tolerance area and prominent objects as to recall the correct password coordinate or pixels. The proposed system can be inline with the existing system with an addition of multiple object concepts and a circular tolerance area.

1.5. Success Rate

Success rate can be calculated without errors. For simplicity the set of images with more objects can be provided in initial stage. This would help the end user to recall their password which would ultimately increase the success rate. In proposed system success rate must be calculated daily, weekly and monthly basis.

1.6. Users

In most of the existing systems homogeneous group of people were used. In proposed system heterogeneous group of people can be considered to avoid any kind of prejudice.

1.7. User Satisfaction

After providing the proper training and implementation of the secure system the review from the end users is a necessary step. The threshold values provided in the feedback will define the degree of user satisfaction towards the proposed system. Many of the existing research work had shown the identical approach for finding the user satisfaction towards the respective authentication system.

1.8. Password storage in the database

In most of the existing systems password stored in the form of images. In proposed system password can be stored in the form of co-ordinates to reduce the memory space.

1.9. External Devices

Variety of external devices such as scanner, web camera, fingerprint device etc. has been used in the existing systems. The major disadvantage renders in the damage or improper functioning and even the extra cost for these external devices is of a major concern. The proposed system thus avoids any such external device except a choice between code or generation of OTP number.

Conclusion

The critical study and the comparative facts arise a scope of defining a novel and usable knowledge based authentication system. The highlights of the major advantages and major disadvantages have uplifted the various evaluation parameters under the usability aspects. This research work has been

initially worked upon the existing features under the mentioned nine evaluation parameters and an approach for developing a novel authentication system.
A future scope of this research work is to have a deep study and knowledge to analyze the various usability evaluation parameters. In addition to develop a secure system the randomness and various attacks equally matter.

References

1. Patra K,Nemade B, Mishra P. (2016). Cued-Click Point Graphical Password Using Circular Tolerance to Increase Password Space and Persuasive Features. *Procedia Computer Science : 877-0509 ELSEVIER.*
2. Boonkrong S. (2019).An Analysis of Numerical Grid-Based Authentication. *School of Information Technology Suranaree University of Technology Thailand ACM Association for Computing Machinery.*
3. Jerome P, Ariel M. (2019).Jumbled PassSteps: A Hotspot Guessing Attack Resistant Graphical Password Authentication Scheme *Basedon the Modified Pass Matrix Method ICCSP, January 19–21, Kuala Lumpur, Malaysia ACM Association for Computing Machinery.*
4. Zujevs N. (2019). Authentication by Graphical Passwords Method ‘Hope'. *Solent University, Southampton, UK., IEEE.*
5. Nida A., Quasim A.(2019). Conundrum-Pass: A New Graphical Password Approach. *IEEE, International Conference on Communication, Computing and Digital Systems.*
6. Ansari S, Rokade J, Khan I, Shaikh A.(2018). Graphical Password Scheme Using Cued Click Point and Persuasion with Multiple Images. *International Journal on Recent and Innovation Trends in Computing and Communication, Vol. 6(4) :2321-8169.*
7. Thorpe J, MacRae B.(2014).The Presentation Effect on Graphical Passwords. *ACM, 978-14503-2473-1/14/04.*
8. Chiasson S, Stobert E, Paul C, Oorschot V, Forget A.(2012).Persuasive Cued Click- Points: Design , Implementation and Evaluation of a Knowledge-Based Authentication Mechanism. *IEEE Transactions on Dependable and Secure Computing, Vol. 9(2) :1545-5971/12/831.00.*
9. Biddle R, Chiasson S, Stobert E, Paul C, Oorschot V, Forget A. (2012).Graphical Passwords : Learning from the First Twelve Years. *ACM Computing Survey.*
10. Saeed S,Sarosh Umar M. (2015).A Hybrid Graphical User Authentication Scheme. *International conference on Communication, Control and Intelligent Systems. IEEE.*
11. Andrea B, Ian O,Hyoungshick K.(2016). PassBYOP:Bring Your Own Picture for Securing Graphical Passwords. *IEEE Transactions of Human Machine Systems, Vol. 46 (3).*
12. Bellam A.(2013). An Effective User Authentication Method Using Persuasive Cued Click Points. *International Journal of Computer Engineering & Science.*
13. Khalifa H, Bashier, Siong L, Hoe, Ying Han P. (2013).Graphical Password: Pass-Images Edge Detection. *IEEE.*
14. Radha A. (2013).A Persuasive Cued Click-point based Authentication Mechanism with Dynamic User Blocks *IJREAT International Journal of Research in Engineering & Advanced Technology, Vol. 1(1). March*
15. Kumar Sarohi H, Ullah Khan F. (2013).Graphical Password Authentication Schemes: Current Status and Key issues. *IJCSI, Vol. 10(2), No. 1, March.*