International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Authentication Using Text and Graphical Password

Mayur H Patel[1], Nimit S Modi[2]

[1]Computer Engineering Department of Sigma Institute of Engineering, Vadodara, India

[2]Assistant Professor Department of CE Sigma Institute of Engineering, Vadodara, India

Abstract: ***This paper introduces images based Graphical Password to protect user data or unauthorized access of information. In that password is created from images and text password. Current system is based on only text password but it has disadvantages small password mostly used and easy to remember. This type of password is easy to guess through different attack i.e. dictionary attack and brute force attack. In this paper we have proposed a new image password scheme. In this Recognition based technique is used with Alpha-Numerical password which provide more security and easy to remember text and graphical password.***

Keywords: Brute force attack, Authentication, Graphical Password, images, security, dictionary attack**..**

1. Introduction

Security is most important in our daily life. There are Three types of Authentication 1) Biometric based Authentication 2) Token based Authentication 3) Knowledge based Authentication [4]. Graphical Password was originally defined by Blonder (1996). Knowledge based authentication can be possible by using Text based Password and Graphical Password. Text Based Password is based on numerical value, alphabets and some special characters. Graphical password is based on Recognition techniques, Recall Based Techniques and Cued Recall Based Techniques. Recognition Based System also has known as Cogno metric Systems [3] or Searchmetric Systems. This technique is based on images. During Registration time user has to select image from predefined images. For successful login user must has to select this images. Recall based System also known as drawn metric systems [3] because users recall and reproduce a secret drawing. In these systems users typically draw their password either on blank canvas or on a grid. Recall is a difficult memory task for remembering a password. Cued Recall Based System is also known as loci metric systems [3]. In these systems identifying specific locations. In this system provides a framework of reminders, hints and gestures for the users to reproduce their passwords or make a reproduction that would be much more accurate.

2. Proposed System

My Proposed System is divided into two parts 1) Registration Phase 2) Login Phase.

Registration Phase:

Registration Phase is divided into three phase:

First Phase

- In user has to enter the basic details like name, birthdate, email id, phone number.

Second Phase:

- In User has to enter the Username and Text Password.

Third Phase:

- In third phase User has to enter Graphical Password based on selection of the images from the Groups. In that three groups are there Famous Places, Famous People and Reputed Company Name in the world.
- User has to select at least one image from one group and maximum image selection for each group is only two

Login Phase:

Login Phase is divided into two phases:

First Phase:

- In first phase for existing user has to enter user name and text password.
- If password is wrong which does not match with User Name then user must check its username.

Second Phase:

- In second phase user has to select images from the group. User has to identify and select images which are selected during Registration Phase.
- If graphical password is wrong then User has to try again for Login.

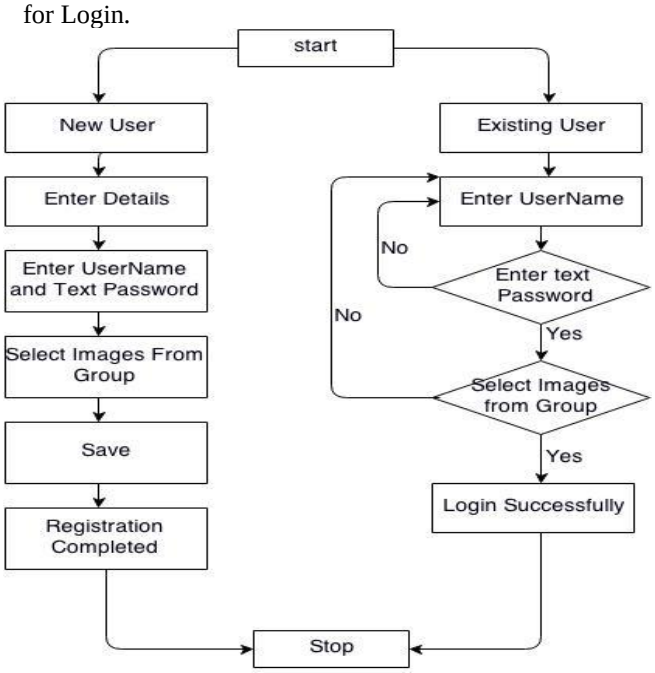

Figure 1: Architecture Diagram of Proposed System

3. Implementation

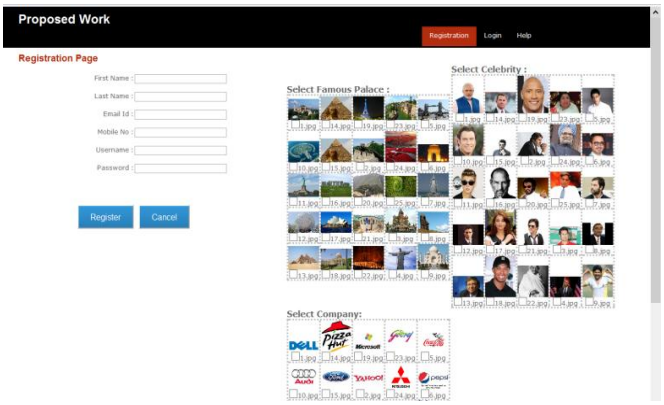

Figure 2: Registration Part of Proposed System

For Registration Part Text Password is stored in Secure Hash Algorithm which Provide more Protection from SQL injection Attack and Graphical Password stored in database as a binary format. So Attacker does not know which binary number is stored for which image.

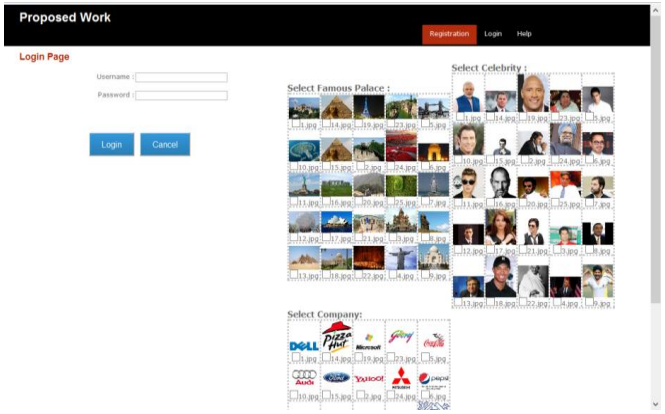

Figure 3: Login Part of Proposed System

For Login Part users must have to identify both Text Password and Graphical Password. If anyone is wrong then user cannot Login to System. So Proposed System Provide two Layer of Security.

4. Result

Proposed System comparison is based on ISO Usability Features, Entropy, Password Space and How much time is required to break a Proposed System. ISO Usability Features all Stratified by Proposed System. So it can be Applicable in Real World

Table 1: Comparison based on ISO Usability Features

Row	System Name	Usability Features								
		Effectiveness	Efficiency	Satisfaction						
		Reliability and Accuracy	Applicable	Mouse Usage	Create Simply	Meaningful	Memorabilit	Simple Steps	Nice Interface	Training Simply	Pleasant picture
1	Proposed System	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

5. Graphical Password Entropy

It is used for that the system is how much secure from the attacker. If entropy is more than the security of system is better otherwise attacker can easily break the security.

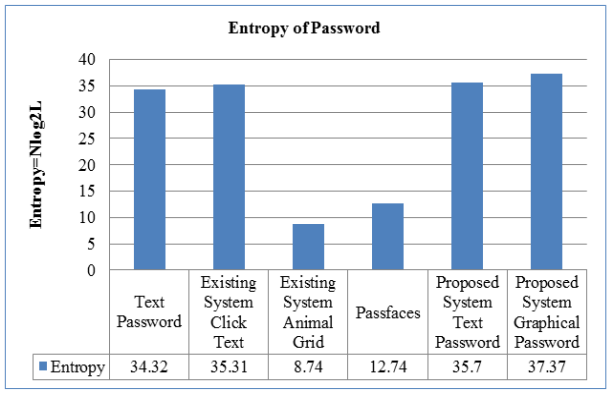

Figure 4: Column Chart for Entropy

6. Graphical Password Space

Users can pick any element for their password in GUA; the raw size of password space is an upper bound on the information content of the distribution that users choose in practice. It is not possible to define a formula for password space but for all algorithms it is possible to calculate the password space or the number of passwords that can be generated by the algorithm. As shown in graph Proposed System Provide more Password Space than any other Graphical Password Space. So proposed System provide more security if attacker want to break the security then millions of comparison required that is impossible.

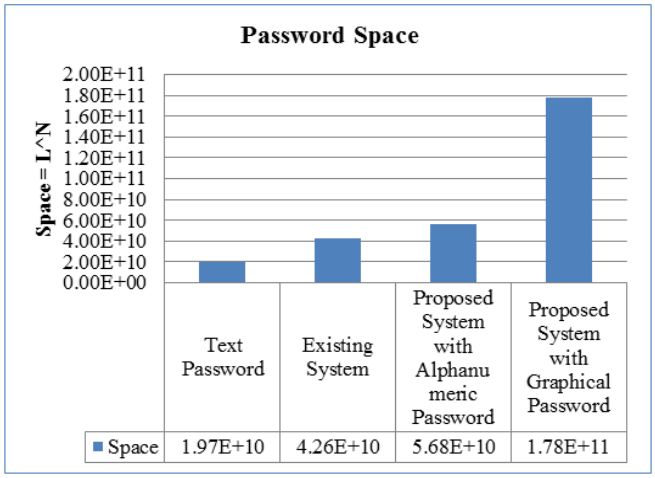

Figure 5: Column Chart for Password Space

7. Time Required to Break the Proposed System

1000 People are employed to work 8 hours per day without any stop in a human guessing attack and that each person takes 30 seconds to finish one trial. It would take them an average

$\frac{0.5 \times 62^6 \times 30}{3600 \times 6 \times 1000 \times 365}$ = 109 Years required for Text Password to break.

$\frac{0.5 \times 75^6 \times 30}{3600 \times 6 \times 1000 \times 365}$ = 339 Years required for Graphical Password to break.

8. Conclusion and Future Work

Current Authentication System is based on Text Password which does not provide more security. For better security Graphical Password introduced in 1996 by blonder but It is clear from the papers reviewed that none of the technique satisfies the ISO standard for usability and security. My proposed system is based on Text Password and Graphical Password. My proposed System provides two layers of the security using Text Password and Graphical Password. It provides more entropy for security from all reviewed paper and also protect from different attack. Future work can be extending by using Salt function for providing more security to users and also increasing entropy of Text Password.

9. Acknowledgement

The authors wish to thank the Management, Principal, Head of the Department (Computer Engineering) and Guide of Sigma Institute of Engineering for the support and help in completing this work.

References

[1] Bin B.Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, and Ning Xu. Captcha as Graphical Passwords-A New Security Primitive Based on Hard AI Problems. IEEE TRANSACTIONS ON INFORMATION FORENSIS AND SECURITY, VOL.9, NO 6, June 2014.

[2] Robert Biddle, Sonia Chiasson and P.C.van Oorschot. Graphical Passwords: Learning from the First Twelve Year. School of Computer Science, Carleton University, Jan 4, 2012.

[3] Antonella De Angeli, Lynne Conventry, Graham Johnson and Karen Renaud. Is a Picture really worth a thousand words? Exploring the feasibility of graphical authentication Systems. Science Direct, 2005.

[4] Hadyn Ellis. The Science behind Passfaces. www.realuser.com,Feb 2012.

[5] P.R.Devale Shrikala, M. Deshmukh and Anil B.Pawar. Persuasive Cued Click Points with Click Draw Based Graphical Password Scheme. International Journal of Soft Computing and Engineering, Volume-3, Issue-2 May 2013.

[6] Iranna A M and Pankaja Patil. Graphical Password Authentication using Persuasive Cued Click Point, International Journal of Advanced Research in Electrical,Elecrtorics and Instrumentation Engineering, Vol.2, Issue 7, July 2013.

[7] Hossein Nejati, Ngai-man Cheung, Ricardo Sosa and Dawn C.I.Koh. DeepCaptcha: An Image CAPTCHA Based on Depth Perception. ACM digital Library, March 2014.

[8] Darryl D'Souza Phani, C.Polina, Roman V and Yampolskiy.Avatar Captcha: Telling Computers and humans apart via face classification.IEEE, 2012.

[9] Nilesh Kawale and Shubhangi Patil. A Recognization Based Graphical Password System. International Journal of Current Engineering and Technology, Vol.4, No.2, Apr 10, 2014.

[10] Mohamed Sylla, Gul Muhammad, Kaleem Habib and Jamaludin Ibrahim.Combinatoric Drag-Pattern Graphical Password. Journal of Emerging Trends in Computing Information Sciences, Vol.4,No.12,Dec 2013.

[11] Trevor Pering, Murali Sundar, John Light and Roy Want. Photographic Authentication through Untrusted Terminal. ACM digital Library. January 2003.

[12] Eiji Hayashi, Nicolas Christin, Rachna Dhamija and Adrian Perrig. Use Your Illusion: Secure Authentication Usable Anywhere. ACM digital Library. July, 2008.

[13] Roman Weiss and Alexander De Luca. PassShapes-Utilizing Stroke Based Authentication to Increase Password Memorability. ACM digital Library. October, 2008.

[14] Haichang Gao, Xuewu Guo, Xiaoping Chen, Liming Wang and Xiyang Liu. YAGP: Yet another Graphical Password Strategy. Institute of Electrical and Electronics Engineers. 2008.

[15] Mauricio Orozco, Behzad Malek, Mohamad Eid and Abdulmotaleb EI Saddik. Haptic-Based Sensible Graphical Password. Proceedings of Virtual Concept 2006. November, 2006.

[16] Adam Stubblefield and Daniel R Simon. Inkblot Authentication. Technical Report Microsoft Research. August, 2004.

[17] Arash habibil Ashkari, Samaneh Farmand, DR.Rosli Saleh, Dr.Omar Bin Zakaria. 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, 2009.

[18] http://gridsure-security.co.uk/gridsure-microsoft-uag

[19] https://www.draw.io/#LUntitled%20Diagram
[20] http://rutgersscholar.rutgers.edu/volume04/sobrbirg/sobrbirg.htm

Author Profile

Nimit S Modi received the Bachelor of Engineering Degree (Computer Engineering) from R K Engineering College and Master of Engineering degree (Computer Engineering) from Parul Institute of Technology. Currently working in Sigma Institute of Engineering as an Assistant Professor in Computer Engineering Department.

Mayur H Patel has completed Bachelor of Engineering degree (Computer Engineering) from Atmiya Institute of Technology and Science in 2012. Currently Master of Engineering (Computer Engineering) Pursing in Computer Engineering from Sigma Institute of Engineering.