International Journal Of Computer Architecture And Mobility (0082-0169)

Volume 1-Issue 1, November 2012

GRAPHICAL PASSWORD (PUZZLES) AUTHENTICATION SYSTEM

Ms.Rachna Singh Thakur[*1], Shubham Pathak[*2], Rupali Patil[*3] ,Neha Kate[*4],Aditi Badkul[*5]
INDORE (INDIA)
rachnasingh.30nov@gmail.com[*1] , developer.shubham@gmail.com[*2] , rptl777@gmail.com[*3],
neha.kate151@gmail.com[*4],aditibadkul0710@gmail.com[*5]

ABSTRACT: - In this project, a graphical password system with a Puzzle to increase the remembrance of the password is discussed. In proposed work a Block-based graphical password scheme called Image Block change (IBC) is presented. In this system a password consists of Puzzles of some images in which user can select one Block-Of-Image. In addition user can change block of that image, it used to help the user to login. System showed very good Performance in terms of speed, accuracy, and ease of use. Users preferred IBC to Change image Block, saying that selecting and remembering only one Block of image was easier and helps considerably in recalling the Image- Block.

Keywords: image block change (IBC), graphical password, remembrance

1. INTRODUCTION:

For Authentication, Authorization, Confidentiality, Access Control we will use Password Authentication System. Mostly user select password that is predictable by Intruder, that's why User Need to choose memorable password with secure from Intruder, So for increase the security and for easy memorable password, the graphical password system has been developed. Images can be recognize by human is easy and Intruder cannot predict your password easily, so it is more secure than simple text based password.

2. GRAPHICAL PASSWORD:

The ubiquity of graphical user interfaces and input devices, such as the mouse, stylus, and touch screen that permit other than typed input, has enabled the emergence of graphical passwords. Graphical passwords are particularly useful for systems that do not have keyboards. In addition, they offer the possibility of addressing known weaknesses in text passwords. History has shown that the distribution of text passwords chosen by human users has entropy far lower than possible, and this has remained a significant weakness of user authentication for over 30 years. Given the fact that pictures are generally more easily remembered than words, it is conceivable that humans would select and remember graphical passwords that are stronger than the text passwords they typically select.

3. PROPOSED WORK:

While the predictability problem can be solved by disallowing user choice and assigning passwords to users, this usually leads to usability issues since users cannot easily remember such random passwords. Number of graphical password systems has been developed; Study shows that text-based passwords suffer with both security and usability problems. According to a recent news article, a security team at a company ran a network password cracker and within30 seconds and they identified about 80% of the passwords. It is well know that Human brain is better at recognizing and recalling images than text.

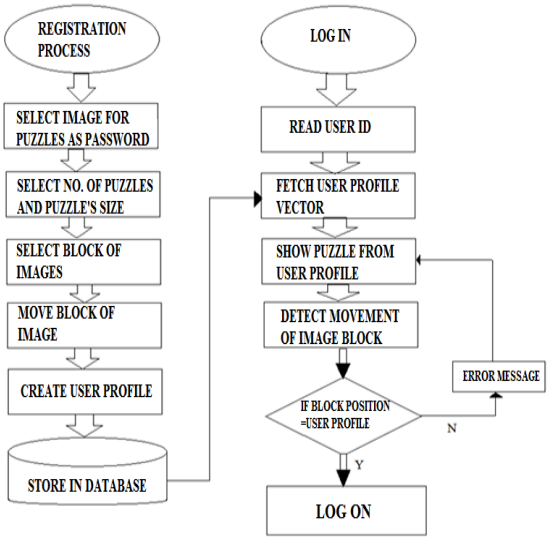

Figure 1: Flow Chart

4. RELATED WORK:

Entropy is currently used to measure text-based password strength against brute force attacks Salomon (2006). Blonder-style passwords are based on cued recall. A user clicks on several previously chosen locations in a single image to log in. Saurabh Singh and Gaurav Agarwal passwords are CCP with sound signature. A user clicks on several previously chosen locations in a single image with a particular sound to log into the system but problem with system is anybody can listen your sound and according to that sound they can predict your Actual click points.

5. RESULTS:

Data collected from 10 students. Each student was asked to register himself/herself and then each was invited to for login trail 5 times as actual user and 5 times as intruder randomly. Students were final year engineering students of age group 20-25 Y.

S. N.	Login ID	Trails	Time Accepted	Time Rejected
1	U1	5	5	0
2	U2	5	5	0
3	U3	5	5	0
4	U4	5	5	0
5	U5	5	5	0
6	U6	5	5	0
7	U7	5	4	1
8	U8	5	5	0
9	U9	5	5	0
10	U10	5	5	0

Table 1. Attempts by Actual users (5 attempts per login ID)

S. N.	Login ID	Trails	Time Accepted	Time Rejected
1	U1	5	0	5
2	U2	5	0	5
3	U3	5	0	5
4	U4	5	0	5
5	U5	5	0	5
6	U6	5	0	5
7	U7	5	0	5
8	U8	5	0	5
9	U9	5	0	5
10	U10	5	0	5

Table2. Attempts by Intruder (5 attempts per login ID)

Table 1 show the detail of the data generated by actual users and Table 2 contains the data generated by intruder. According to the data generated by actual user is 98% accepted and only 2% rejected but according to data generated by intruder is 100% rejected by the system which is very good for Graphical password puzzles authentication system.

6. PROPOSED ALGORITHM:

Approach to writing a program to solve such a jigsaw puzzle. There are 6 key pieces of information that you can use individually and together as clues to solving a jigsaw puzzle:

1) First section contains the broken images in random order.

2) Second section contains the outline of the full image. User need to drag and drop the cut images onto the outline image.

3) The only thing you need an "algorithm" for is snapping pieces in place.

4) So when we launch application, system will read original image and pieces from resource and display them.

5) Now pieces cannot be rotated, they can be placed as it is on the outline image that called “Image Block Change (IBC)”.

6) User can drag one piece at a time to the outline image. If the piece is placed at proper position then user can logged on.

So what kind of information will the program will be supplied - let's assume that each jigsaw puzzle piece is a small rectangular image with transparency information used to identify the portion of the puzzle piece that represent non-rectangular edges.

7. Figure caption:

Figure2. Actual image

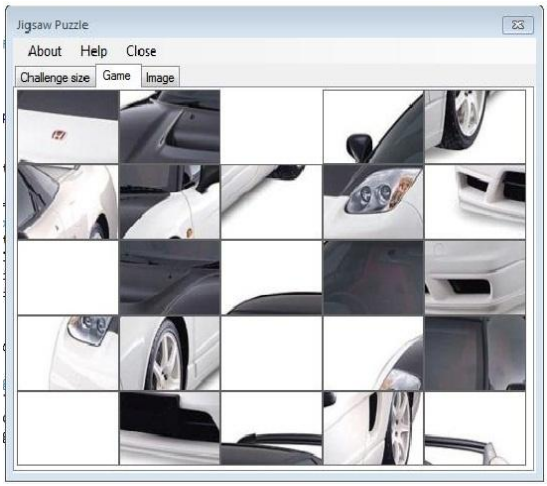

Figure3. Puzzled image

8. CONCLUSION:

We have proposed an approach which uses jigsaw Puzzles to recall graphical password image block change points.. According to result this system will provide better security and better performance.

9. REFERANCES:

[1] Saurabh Singh and Gaurav Agarwal. Integration of Sound Signature in Graphical Password Authentication System. International Journal of Computer Applications (0975 – 8887) Volume 12– No.9, January 2011.

[2] Birget, J.C., D. Hong, and N. Memon. Graphical Passwords Based on Robust Discretization. IEEE Trans. Info. Forensics and Security, 1(3), September 2006.

[3] Blonder, G.E. Graphical Passwords. United States Patent 5,559,961, 19.

[4] Davis, D., F. Monrose, and M.K. Reiter. On User Choice in Graphical Password Schemes. 13th USENIX Security Symposium, 2004.

[5] D. Weinshall and S. Kirkpatrick, "Passwords You'll Never Forget, but Can't Recall," in Proceedings of Conference on Human Factors in Computing Systems (CHI). Vienna, Austria: ACM, 2004, pp. 1399-1402.

[6] Taeg Sang Cho, Shai Avidan, William T.Freeman Massachusetts Institute of Technology Tel-Aviv University "A probabilistic image jigsaw puzzle solver"