© 2016 IJSRSET | Volume 2 | Issue 3 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

A Research on Authentication Scheme for Session Passwords with Colour Pairs and Grid Compared with OTP

Jay Patel, Prof. Ashil Patel

Information Technology, L. D. Engineering College, Ahmedabad, Gujarat, India

ABSTRACT

To provide the security mainly authentication and authorisation is given to the system. For that purpose mostly textual passwords are being used. Now a day's graphical password are also available. The password schemes those are being used by now Days are mostly textual password and the graphical password (pattern matching), textual passwords are vulnerable to eves dropping, dictionary attacks, social engineering and shoulder surfing. Graphical passwords are introduced as alternative techniques to textual passwords. But Most of the graphical schemes are vulnerable to shoulder surfing. This paper shows the study of the available authentication schemes for session password.

Keywords: OTP, Grid, Authentication Scheme, Pattern Matching, Dictionary Attacks, Social Engineering, Shoulder Surfing, 2D

I. INTRODUCTION

Security is mainly given by two mechanism which are Authentication and authorisation. Now first we have to understand what is authentication and authorisation.

Authentication verifies "who you are?". It is a process in which the credentials provided are compared to those on file in a database of authenticated users.

For example the simple authentication is done every time when you log in to your mail account from the different computer or other device.

II. METHODS AND MATERIAL

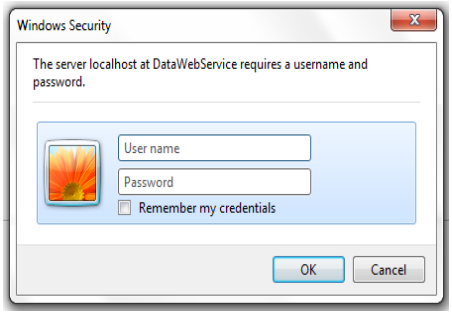


Figure 1: Authentication

Authorisation gives information about what you are authorised to do. Authorisation is the function of specifying access rights to resources related to information security and computer security in general and to access control in particular.

Figure 2: Authorisation

Another question arises "What is session?" In computer science or in particular networking, the session is a semi-permanent interactive information interchange. That is nothing but the interaction of informative communication within the limited time period.

What is session password? Now the password that is being used for the authentication for that session which means that the password is being used for the limited

period of time is session password. For every session there will be a new session password.

A. Proposed Methodology

Algorithm

Input: Colour Rating

Output: Whether User is Authenticated or not

1. Start
2. If (User is new)
   Go to Registration Phase
   Enter his personal information and Rating of Colours between 0-9
   End If
3. Login into the System and Session Starts
4. Interface of colour pairs and Grid is displayed.
5. User Enters Session Password
6. If (Session Password is Correct)
   //User is authenticated
   User Perform the set of authorised Task
7. Session Ends
8. End

B. Flowchart

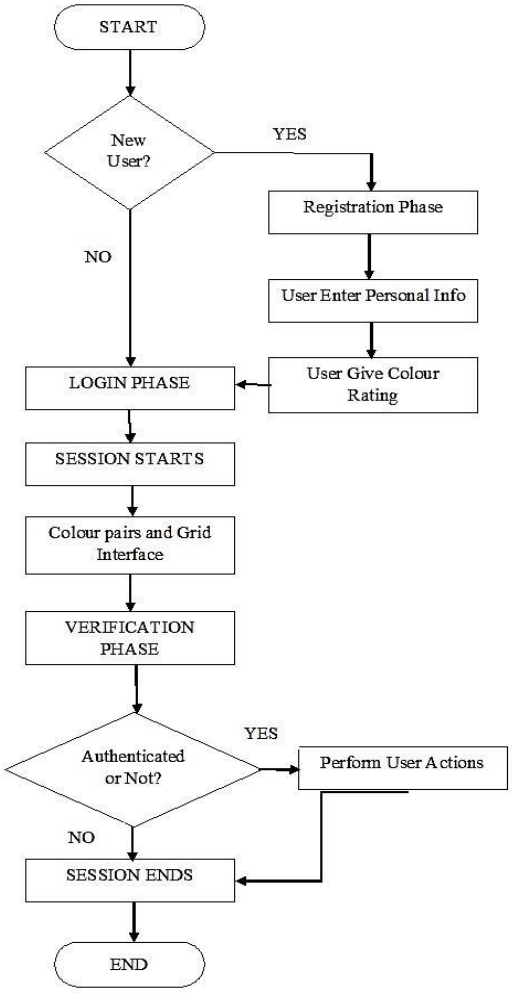


Figure 3: Flowchart of Proposed Methodology

III. RESULTS AND DISCUSSION

A. Implementation

This technique is using 2D grid and colour pairs for session passwords generation. Registration is done for the new user and at that time user will give colour rating, during login time, based on the colour pairs and grid displayed a session password will be generated. For the authentication scheme, ratings given to colours, and grid displayed during login, session password is verified by the system.

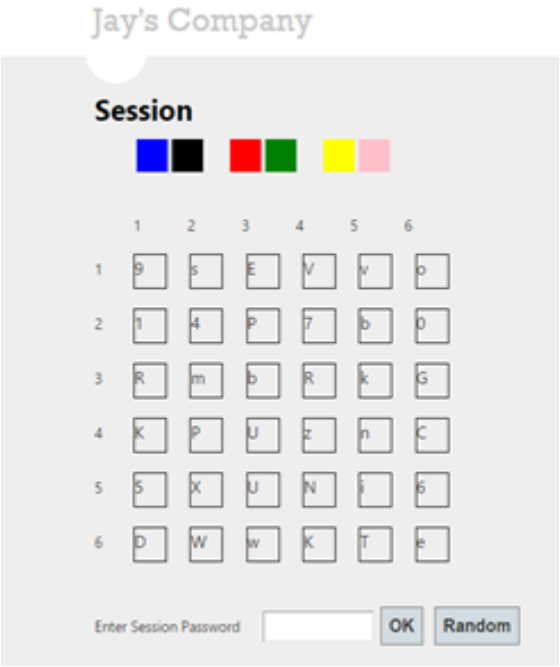


Figure 4: colour pairs and grid of Proposed Methodology

COMPARISION

Comparison of Randomness

The measures of Randomness of the Proposed System and OTP can be computed as follows.

For OTP with Numbers only

OTP with numbers only is nothing but the series of six digits from 0 to 9. So the possible Combinations of series of six digit numbers of OTP generation can be given by ${}_{10}P_6 = 151200$.

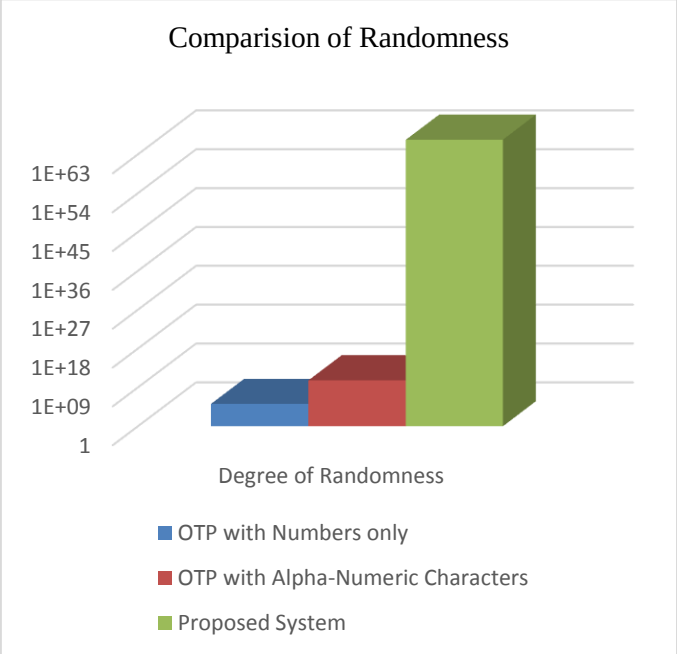
For OTP with Numbers only

Now OTP with alpha-numeric characters are nothing but the series of six digits containing 26 Capital letters, 26 Small latters, and 10 numerical digits that is 0 to 9. Here, the possible combinations of series of six digit numbers of OTP generation can be given by permutation ${}_{62}P_6 = 4.426165\times10^{10}$.

For the Proposed System

The proposed system is containing the randomness of three level. First is the randomness of colour pairs, the second is the randomness of the grid of 36 alpha-numeric characters and the third is the randomness of selecting the Session password from the Grid according to the rating and display of the colour pairs.

Now, those available six colours can be arranged in simply (6 factorial) 6! = 720 ways. The Grid of 6×6 that is 36 alpha-numeric characters containing 26 Capital letters, 26 Small latters, and 10 numerical digits that is 0 to 9. So the number of possible ways to generate the Grid of 6×6 containing random and non-repeating 36 alpha-numeric characters can be given by the permutation $(26+26+10=62)\ {}_{62}P_{36} = 2.4069\times10^{66}$.



Comparison of Probabilistic Success

Comparison of Probabilistic Success of generating Session passwords Using OTP and Proposed System.

$$\text{Probability} = \frac{Favourable\ occurance}{Total\ search\ space}$$

Now, the success of the system can be calculated by the formula

Probability of success = 1 – Probability of failure
Here, in this case the probability of failure is nothing but the Probability of correct guess by Attacker or intruder. Hence,

Probability of success = 1 – Probability of Correct guess
Probability of success for OTP
Probability of success = 1 – Probability of Correct guess

$= 1 - \frac{Favourable\ occurance\ of\ Correct\ Guess}{Total\ search\ space}$

$= 1 - \frac{10^6}{4.426 \times 10^{10}}$

= 0.99997

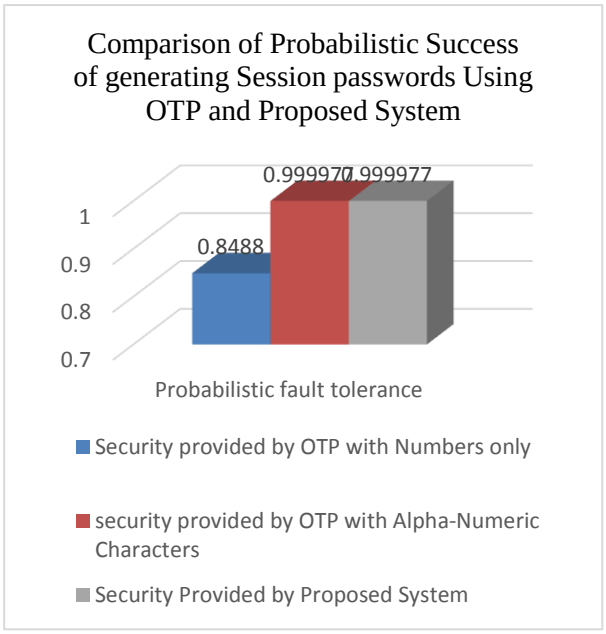
Probability of success for Proposed Method

Probability of success = 1-Probability of Correct guess

$= 1 - \frac{Favourable\ occurance\ of\ Correct\ Guess}{Total\ search\ space}$

$= 1 - \frac{6! \times 7.803 \times 10^{58}}{2.4069 \times 10^{66}}$

= 0.99997



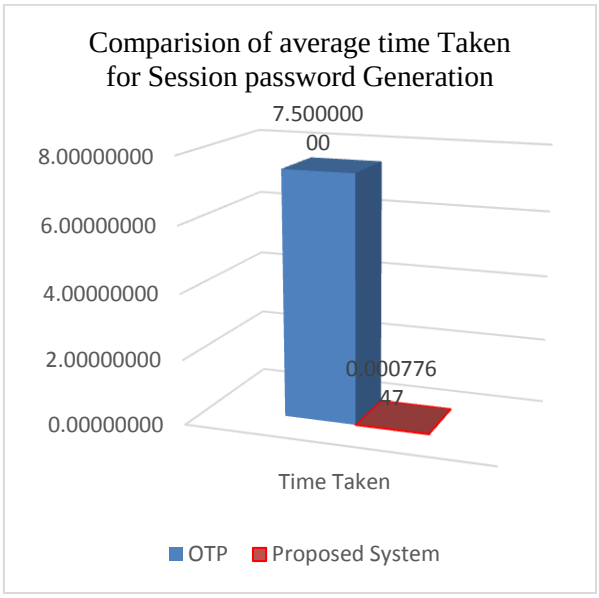
Comparison of average time taken for Session Password Generation

Average time taken for session password generation by Proposed System is calculated as follows. Here are some results calculated in ticks with frequency of 1851183 and hence the time is calculated in milliseconds and microseconds.

Ticks	Time (milliseconds or microseconds)
13079	7.065 milliseconds
139	75.08 microseconds
141	76.16 microseconds
138	74.54 microseconds
145	78.32 microseconds
137	74.00 microseconds
141	76.16 microseconds
176	95.07 microseconds
145	78.32 microseconds
136	73.46 microseconds

So, the average time taken is 776.647 microseconds that is 0.77664 milliseconds.

While at the other hand an Average time taken for session password generation by OTP contains the OTP generation time as well as the time taken to send the OTP through the Network. OTP generation also takes some milliseconds but after that server has to send that OTP to the requested Mobile Phone device and that consumes 3 to 12 seconds in average case scenarios. In best case scenario its 3 seconds nearly, and in worst case scenario the OTP may not receive by the User on mobile phone device.



IV. CONCLUSION

In this paper the research has been done on the authentication scheme in which colour rating is to be given by user at the registration time and at the authentication time session starts and colour pairs and grid of random characters are to be displayed and from it the session password is to be generated. The proposed system is more secure from shoulder surfing attack and vulnerability. And from the comparison with OTP (one time password) the probabilistic success and degree of

randomness is achieved and time taken is reduced more effectively.

V. REFERENCES

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

[2] Ms Grinal Tuscano, Aakriti Tulasyan, Akshata Shetty, Malvina Rumao, Aishwarya Shetty. " Graphical password authentication using Pass faces", In Ms Grinal Tuscano et al. Int. Journal of Engineering Research and Applications, 2015.

[3] Y.D.S.Arya and Gaurav Agarwal," Impact of Background Images on the DAS (Draw- A-Secret) Graphical Password Authentication Scheme", In IJCA Special Issue on "Network Security and Cryptography" NSC, 2011.

[4] A. F. Syukri, E. Okamoto, and M. Mambo, "A User Identification System Using Signature Written with Mouse," in Third Australasian Conference on Information Security and Privacy (ACISP): Springer- Verlag Lecture Notes in Computer Science (1438), 1998, pp. 403-441.

[5] S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, N. Memon, "Design and longitudinal evaluation of a graphical password system". International J. of Human-Computer Studies 63 (2005) 102-127.

[6] HaichangGao, ZhongjieRen, Xiuling Chang, Xiyang Liu UweAickelin, "A New Graphical Password Scheme Resistant to Shoulder-Surfing

[7] Passlogix, site http://www.passlogix.com.

[8] S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, N. Memon, "Design and longitudinal evaluation of a graphical password system". International J. of Human-Computer Studies 63 102-127.

[9] Yi-Lun Chen, Wei-Chi Ku*, Yu-Chang Yeh, and Dun-Min Liao, "A Simple Text-Based Shoulder Surfing Resistant Graphical Password Scheme",Department of Computer Science, National Taichung University of Education, Taiwan, IEEE 2nd International Symposium on Next-Generation Electronics (ISNE) - February 25-26 , Kaohsiung , Taiwan

[10] Graphical Password Authentication Cloud securing scheme ShraddhaM. Gurav, Leena S. Gawade, Prathamey K. Rane, Nilesh R. Khochare, Computer Department, Mumbai University RMCET, Ratnagiri, India, IEEE 2014.