IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Volume 11, PP 36-39

Simple Text Based Shoulder Surfing System Using Resistant Graphical Password

Mr. Krishnashankar Lodh[1], Akash R. Gupta[2], Bhupendra Singh Rawat[3],
Abhishek Kumar Mathur[4], Prof. Rajesh Gaikwad[5]
1,2,3,4 (Student,, Slrtce, Mira Road(E) Maharashtra, India)
5(Professor, Department Of Computer Engineering, S L.R T C E, Mira Road (E), Maharashtra, India)

Abstract : *In The Password Scheme Security Process, High Percentage Of Users Are Familiar With The Textual Password Scheme Instead Of Graphical Password Scheme But In Text-Based Password Scheme Leads To A Threatening Security Problems. Text-Based Shoulder Surfing Resistant Graphical Password Schemes Is Both Secure And Efficient Enough. In This Proposed Scheme, We Propose An Improved Text-Based Shoulder Surfing Resistant Graphical Password Scheme By Using Color Pattern In Much Efficient Form And Pattern. The Security And Usability Scheme Can Easily Be Researched In Well-Mannered Efficient Way In Our Proposed System. It Is Better Solution Against Shoulder Surfing.*

Keywords —*Graphical, Shoulder-Surfing, Authentication.*

I. INTRODUCTION

Now A Day, There Are Various Applications Related To Authentications In Terms Of Secure Portals And Platforms Like Banking, Online Banking, Online Social Platforms Which Is Very Promising As Per The Degree Of Privacy And Security, The Textual Bases Password Surfing Leads To High Threatening Of Leaking The Information By Various Unwanted Means Like Shoulder Surfing, Cameras Proposed A Text-Based Shoulder Surfing Resistant Graphical Password Scheme. To Get The Session Password In S3pas, The User Has To Mix His Textual Password On The Login Screen. The Technique Of The Proposed Scheme Is Simple And Easy To Learn And Remember For Users And Most Of Them Are Familiar With Textual Passwords Than The Graphical Passwords. The User Can Easily And Efficiently Login The System Without Using Any Physical Keyboard Or On-Screen Keyboard.

II. Literature Review

In The Starting Of The 20century In The Year 2002, Birget And Sobardo They Both Proposed Three Shoulder Surfing Resistant Graphical Password Schemes. Finally, There Was Three Named Such As The Triangle Scheme, The Moveable Scheme And The Intersection Schemes Comparing To The Three Schemes In Which Movable Frame Scheme And The Intersection Scheme Have High Failure Rate.So In The Triangle Scheme, The User Has To Choose And Memorize Several Pass-Icons As His Password. In Every Time Whenever Login The User Has To Find Three Pass-Icons Among A Set Of Randomly Chosen Icons Displayed On The Login Screen, And Then Click Inside The Invisible Triangle Created By Those Three Pass-Icons. In 2006, Wiedenbeck Et Al Proposed The Convex Hull Click Scheme As An Improved Version Of The Triangle Scheme With Superior Usability And Security. To Login The System, The User Has To Correctly Respond Several Challenges. In Each Challenge, The User Has To Find Any Three Pass-Icons Displayed On The Login Screen, And Then Click Inside The Invisible Convex Hull Formed By All The Displayed Pass-Icons. However, The Login Time Of Convex-Hull Click System May Be Too Long And More Tedious. In 2009, Gao Et Al Proposed A Shoulder Surfing Resistant Graphical Password System, Color Login, In Which The Background Color Is A Important Factor For Reducing The Login Time. However, The Probability Of Accidental Login Of Color Login Is Too High And The Password Space Is Too Small. Most Of The Users Are Familiar With Textual Passwords And Conventional Textual Password Authentication System Have No Shoulder Surfing Resistance, Zhao Et Al. In The Year Of 2007, Proposed A Text-Based Shoulder Surfing Resistant Graphical Password System, In S3pas To Get A Session Password In Which The User Has To Find His Textual Password And Then Follow A Special Rule To Mix His Textual Password To Login The System. However, The Login Process Of Zhao Et Al.'S System Is Complex And Tedious. In 2011, Sreelatha Et Al. Also Proposed A Text-Based Shoulder Surfing Resistant Graphical Password System By Using Several Colors. Clearly, As The User Has To Additionally Memorizing The Arrangement Of Several Colors, The Memory Burden Of The User Is High. In 2012, Rao Et Al Proposed A Text-Based Shoulder Surfing Resistant Graphical Password System, Ppc. To Produce Several Pass-Pairs The User Has To Mix His Textual Password To Login The System, And Then

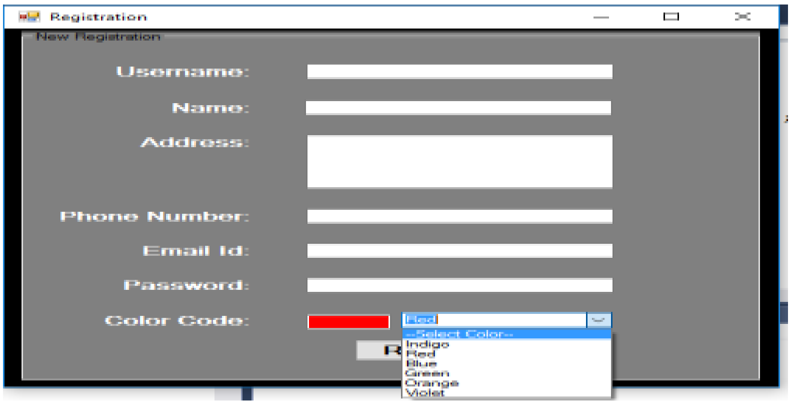
Follow Four Predefined Rules To Get His Session Password On The Login Screen. However, The Login Process Of Ppc Is Too Tedious And Complicated.

III. The Proposed System

We Will See A Simple Text Based Shoulder Surfing System Using Resistant Graphical Password Based On Texts And Colors In This Section. It Will Describe A Very Simple Text Based Shoulder Surfing System Using Resistant Graphical Password Based On Texts And Colors. In The Propose System The Alphabet Used Are As Contains As 72 Characters, Including 26 Upper Case Letters, 26 Lower Case Letters, 10 Decimal Digits, And 10 Symbols That Is ".", "/”, “@", "#", "$", "%", "&", "*", "?", And "=". This Proposed System Includes Two Phases.

1. Registration Phase

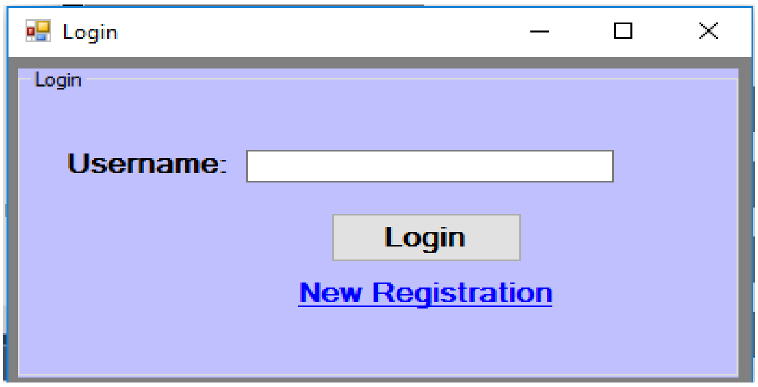
Registration Phase: The User Has To Set His Textual Password K Of Length L (8≤L≤15) Characters And Choose A Color As His Pass Color From Eight Colors Assigned By The System. The Remaining Seven Colors Not Chosen By The User Are His Decoy Colors. In Addition, The User Has To Register An E-Mail Address For Enable Again His Disabled Account. The Registration Phase Should Proceed In An Environment Free Of Shoulder Surfing. A Secure Channel Will Be Established Between The System And The User During The Registration Phase By Using Ssl/Tls Or Other Secure Transmission Mechanism. The System Stores The User’s Textual Password In The User’s Entry In The Password Table, Which Should Be Encrypted By The System.



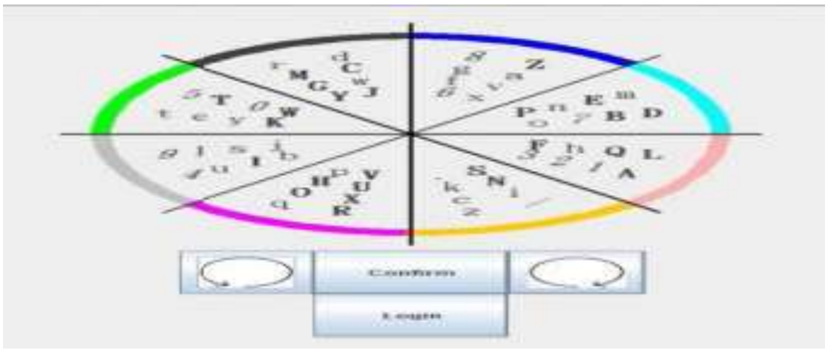
Color Code: Red

2. Login Phase

Login Phase: When User Requests To Login The System, Then The System Displays A Circle Composed Of 8 Equally Sized Sectors. That Is Our Project Login Screen. In That Login Screen Colors Of The Arcs Of The 8 Sectors Are Different, And Each Sector Is Identified By The Color Of Its Arc, Example- The Blue Sector Is The Sector Of Blue Arc. Initially, 64 Characters Are Placed Averagely And Randomly Among These Sectors. All The Displayed Characters Can Be Simultaneously Rotated Into Either The Adjacent Sector Clockwise By Using The Clockwise Button Once Or The Adjacent Sector Anticlockwise By Clicking The Anticlockwise Button Once, And The Rotation Operations Can Also Be Performed By Scrolling The Mouse Wheel. The Login Screen Of The Proposed Scheme Can Be Illustrated By An Example Shown In Fig. 1. To Login The System, The User Has To Finish The Following Steps:



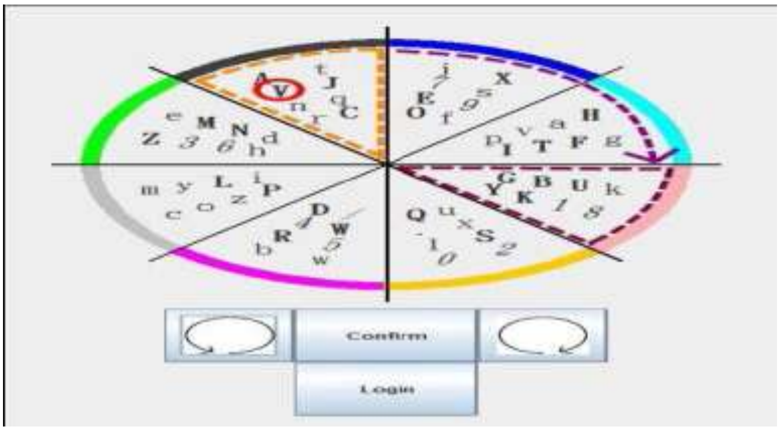
Step 1: The User Requests To Login The System.



Step 2: The Display The Login Screen It Is A Display A Circle Composed Of 8 Equally Sized Sectors, And Places 64 Characters Among The 8 Sectors Averagely And Randomly So That Each Sector Contains 8 Characters. The 64 Characters Are In Three Typefaces And Different Three Color In That The 26 Upper Case Letters Are In Bold Typeface, The 26 Lower Case Letters And The Two Symbols "." And "/" Are In Regular Typeface, And The 10 Decimal Digits Are In Italic Typeface. In Addition, The Button For Rotating Clockwise, The Button For Rotating Anticlockwise, The "Confirm" Button, And The "Login" Button Are Also Displayed On The Login Screen. All The Displayed Characters Can Be Simultaneously Rotated Into Either The Adjacent Sector Clockwise By Clicking The Clockwise Button Once Or The Adjacent Sector Anticlockwise By Clicking The Anticlockwise Button Once, And The Rotation Operations Can Also Be Performed By Scrolling The Mouse Wheel. Let I= 1.

Step 3: The User Has To Rotate The Sector Containing The I-Th Pass Character Of His Password K, Denoted By Ki, Into His Pass-Color Sector, And Then Clicks The "Confirm" Button. Let I = I + 1.

Step 4: If I < L, The System Random Permuted All The 64 Displayed Characters, And Then Goto`S Step 3. Otherwise, The User Has To Click The "Login" Button To Complete The Login Process.



If The Account Is Not Successfully Authenticated For Three Consecutive Times, This Account Will Be Disabled, And The System Will Send To The User's Registered E-Mail Address An E-Mail Containing The Secret Link That Can Be Used By The Legitimate User To Re-Enable His Disabled Account. The Login Process Of The Proposed Scheme Can Be Illustrated By An Example Shown In Fig. The User Has To Rotate The Sector (Marked With Brown Dotted Line For Illustration Only) Containing Ki (Marked With Small Red Circle For Illustration Only) Into His Pass-Color Sector (Marked With Brown Dotted Line For Illustration).

IV. Algorithms Random Number Generation

Input: 64-Character A To Z=26, A To Z=26,0 To 9=10, And ". /"=2 Output: Random Printing Algorithm:
Step1: To Generate The Matrix Wit Row And Column 8*8.
Step2: Put 0 To 63 Numbers Into Matrix.
Step3: Select One Random Number From 0 To 63.
Step4: For Putting Number Into Matrix System Check Number Is Already Parent Or Not.
Step5: If Number Present Then Perform Setp3.If Not Present Then Put Into A Matrix And Go To Setp3.
Step6: Do Step 5 Repeatedly Up To 0 To 63 Inserted Into Matrix.
Step7: Print The Matrix.
Step8: Now Get String Which Have 64 Character " A To Z=26, A To Z=26,0 To 9=10, And. /=2".

Step9: Get Number Present Into Matrix Sequentially [0][0] To [8][8] I.E., Total 64 Character.
Step10: Select Index Of String From 64 Char. Put Into That Current Location.
Step11: Do Step 9 And 10 Repeatedly Up To [8][8] Number.
Step12: Print Current Matrix With String Char.
Step13: Display A Matrix With Random Printing
Step14: Stop

V. Analysis

In This Section, We Will Describe Analysis Of Our Project. The Security And The Usability, Which Is Most Important Part Of System, Is Analyzed In This Section For Our Project.

A. Password Space: The Total Number Of All Possible Passwords With Length L Is 8 *64^L.

B. Resistance To Accidental Login: Our System Is More Resistance Of Accidental Login Since The Probability Of Correctly Responding To Password (Ki) Is 8/64, That Is 1/8, The Success Probability Of Accidental Login With The Password (Ki) With Length L, Denote By Pal (L), Is Pal (L) = (1/8) ^L

However, Since The Password Length Is A More Secret, If Hackers Want To Hack The System He Will First Guess The User Password. He Will Then Try To Hack But As The Probability Distribution Of The Lengths Of The Passwords To Be Used Is Assumed Uniform Between 8 And 15, The Probability That The Hacker Correctly Guesses The Password Length Is 1/8. Thus, The Probability Of Accidental Login Is Very Less And If The Attacker Fails To Login System Consecutively For Three Times, Then That Account Will Be Disabled, And The System Will Send E-Mail To The User’s Registered Email-Id With A Secret Link That Can Be Used By The Legitimate User To Change The Password Re-Enable His Disabled Account. Thus, Accidental Login Cannot Be Performed Easily And Efficiently Is To Be Complicated.

VI. Conclusions

Over Here In This Paper, We Have Proposed Simple Text Based Shoulder Surfing System Using Resistant Graphical Password In Which The User Can Easily Complete The Login Process Without Hesitating About Shoulder Surfing Attacks, Cameras. Proposed A Text-Based Shoulder Surfing Resistant Graphical Password Scheme. The Operation Of The Proposed Scheme Is Simple. The User Can Easily Login The System Without Using Any Physical Keyboard Or On-Screen Keyboard. Finally, We Have Analysed The Resistances Of The Proposed Scheme To Shoulder Surfing And Accidental Login.

REFERENCES

[1] L. Sobrado And J. C. Birget, “Graphical Passwords,” The Rutgers Scholar, An Electronic Bulletin For Undergraduate Research, 2002.

[2] J.C. Birget, “Shoulder-Surfing Resistant Graphical Passwords,” Draft, 2005.

[3] S. Wiedenbeck, J. Waters, L. Sobrado, And J. C. Birget, “Design And Evaluation Of A Shoulder-Surfing Resistant Graphical Password Scheme,” Proc. Of Working Conf. On Advanced Visual Interfaces, May.2006, Pp. 177-184.

[4] H. Gao, X. Liu, S. Wang, H. Liu, And R. Dai, “Design And Analysis Of A Graphical Password Scheme,” Dec.2009.

[5] B. Hartanto, B. Santoso, And S. Welly, “The Usage Of Graphical Password As A Replacement To The

[6] Alphanumerical Password,” Informatika, 2006, Pp. 91-97.

[7] Man, D. Hong, And M. Mathews, “A Shoulder Surfing Resistant Graphical Password Scheme,” Proc. Ofthe 2003 Int. Conf. On Security And Management, June 2003.

[8] T. Perkovic, M. Cagalj, And N. Rakic, “Sssl: Shoulder Surfing Safe Login,” Sept. 2009, Pp. 270-275.

[9] Z. Zheng, X. Liu, L. Yin, And Z. Liu, “A Stroke-Based Textual Password Authentication Scheme. Mar.2009.

[10] T. Yamamoto, Y. Kojima, And M. Nishigaki, “A Shoulder Surfing- Resistant Image-Based Authentication System With Temporal Indirect Image Selection,” Proc. Of The 2009.

[11] H. Zhao And X. Li, “S3pas: A Scalable Shoulder-Surfing Resistant Textual-Graphical Password

[12] Authentication Scheme,” Proc. Of 21st Int. Conf. On Advanced Information Networking And Applications Workshops, Vol. 2, May 2007, Pp. 467-472.