RESEARCH ARTICLE OPEN ACCESS

Anti Shoulder Surfing

Sahil Chordia, Akansha Tambe, Jai Mulik, Shubham Patne, Monika Kute
(Computer Dept, Pimpri Chinchwad Polytechnic, India)

Abstract :- When Users Input Their Passwords In A Public Place, They May Be At Risk Of Attackers Stealing Their Password. An Attacker Can Capture A Password By Direct Observation Or By Recording The Individuals Authentication Session. This Is Referred To As Shoulder-Surfing And Is A Known Risk, Of Special Concern When Authenticating In Public Places. Until Recently, The Only Defence Against Shoulder-Surfing Was The Alertness On The Part Of The User. Shoulder Surfing Resistant Password Authentication Mechanism Assure Shoulder-Surfing Resistant Authentication To User. It Allows User To Authenticate By Entering Pass-Word In Graphical Way At Insecure Places Because User Never Have To Click Directly On Password Icons. Usability Testing Of This Mechanism Showed That Novice Users Were Able To Enter Their Graphical Password Accurately And To Remember It Over Time. However, The Protection Against Shoulder-Surfing Comes At The Price Of Longer Time To Carry Out The Authentication.

Keywords :- Graphical Authentication, Shoulder Surfing Resistant

Date of Submission: 05-03-2018 Date of acceptance20-03-2018

I. INTRODUCTION

The Shoulder Surfing Attack In An Attack That Can Be Performed By The Adversary To Obtain The User’s Password By Watching Over The User’s Shoulder As He Enters His Password. As Conventional Password Schemes Are Vulnerable To Shoulder Surfing, Sobrado And Birget Proposed Three Shoulder Surfing Resistant Graphical Password Schemes. However, Most Of The Current Graphical Password Schemes Are Vulnerable To Shoulder-Surfing A Known Risk Where An Attacker Can Capture A Password By Direct Observation Or By Recording The Authentication Session. Due To The Visual Interface, Shoulder-Surfing Becomes An Exacerbated Problem In Graphical Passwords. A Graphical Password Is Easier Than A Text-Based Password For Most People To Remember. Suppose An 8- Character Password Is Necessary To Gain Entry Into A Particular Computer Network. Strong Passwords Can Be Produced That Are Resistant To Guessing, Dictionary Attack. Key-Loggers, Shoulder-Surfing And Social Engineering. Graphical Passwords Have Been Used In Authentication For Mobile Phones, Atm Machines, E-Transactions.

II. EXISTING SYSTEM

Using Traditional Textual Passwords Or Pin Method, Users Need To Type Their Passwords To Authenticate Themselves And Thus These Passwords Can Be Revealed Easily If Someone Peeks Over Shoulder Or Uses Video Recording Devices Such As Cell Phones Shoulder Surfing Attacks Have Posed A Great Threat To Users’ Privacy And Confidentiality As Mobile Devices Are Becoming Indispensable In Modern Life. In The Early Days, The Graphical Capability Of Handheld Devices Was Weak; The Color And Pixel It Could Show Was Limited. With The Increasing Amount Of Mobile Devices And Web Services, Users Can Access Their Personal Accounts To Send Confidential Business Emails, Upload Photos To Albums In The Cloud Or Remit Money From Their E-Bank Account Anytime And Anywhere. While Logging Into These Services In Public, They May Expose Their Passwords To Unknown Parties Unconsciously.

III. PROPOSED SYSTEM

To Overcome This Problem, We Proposed A Shoulder Surfing Resistant Authentication System Based On Graphical Passwords, Named Passmatrix. Using A One-Time Login Indicator Per Image, Users Can Point Out The Location Of Their Pass-Square Without Directly Clicking Or Touching It, Which Is An Action Vulnerable To Shoulder Surfing Attacks. Because Of The Design Of The Horizontal And Vertical Bars That Cover The Entire Pass-Image, It Offers No Clue For Attackers To Narrow Down The Password Space Even If They Have More Than One Login Records Of That Account. In Passmatrix, A Password Consists Of Only One Pass-Square Per Pass-Image For A Sequence Of N Images. The Number Of Images (I.E., N) Is User-Defined. In Passmatrix, Users Choose One Square Per Image For A Sequence Of N Images Rather Than N Squares In One Image As That In The Passpoints Scheme.

Passmatrix's Authentication Consists Of A Registration Phase And An Authentication Phase As Described Below: At This Stage, The User Creates An Account Which Contains A Username And A Password. The Password Consists Of Only One Pass-Square Per Image For A Sequence Of N Images. The Number Of Images (I.E., N) Is Decided By The User After Considering The Trade-Off Between Security And Usability Of The System. At This Stage, The User Uses His/Her Username, Password And Login Indicators To Log Into Passmatrix

IV. SYSTEM ARCHITECTURE

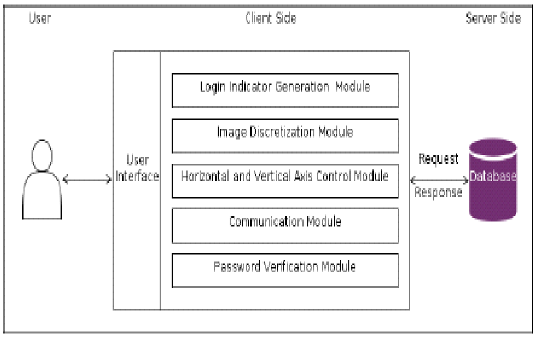
User
Client Side
Server Side
User Interface
Login Indicator Generation Module
Image Discretization Module
Horizontal and Vertical Axis Control Module
Communication Module
Password Verification Module
Request
Response
Database

Fig 1:- Anti Shoulder Diagram Flow Diagram

V. CONCLUSION

In Many Authentication Methods And Techniques Are Available But Each With Its Own Advantages And Shortcomings. In View Of Above, We Have Proposed Authentication System Which Is Based On Graphical Password Schemes. Although Our System To Reduce The Problems With Existing Graphical Based Password Schemes But It Has Also Some Limitations Any Issues Like All The Other Graphical Based Password Techniques. We Need Our Authentication Systems To Be More Secure, Reliable And Robust As There Is Always A Place For Improvement. In This Paper, Shoulder Surfing And Key Logger Resistant Text-Based Graphical Password Scheme Is Proposed. In This System User Can Easily Login Into System Without Worrying About Shoulder Surfing And Key Logger Attack In Future Some Other Important Things Regarding The Performance Of Our System Will Be Investigated Like User Adoptability And Usability And Security Of Our System.

Acknowledgements

We Would Prefer To Impart All Authors Of Analysis Papers Referred During This Paper For His Or Her Work. It Had Been Terribly Useful And Data Gaining For Any Future Analysis To Be Done In This
Field.

REFERENCES

[1]. S. Sood, A. Sarje, And K. Singh, "Cryptanalysis Of Password Authentication Schemes: Current Status And Key Issues," In Methods And Models In Computer Science, 2009. Icm2cs 2009. Proceeding Of International Conference On, Dec 2009, Pp. 1–7.

[2]. S. Gurav, L. Gawade, P. Rane, And N. Khochare, "Graphical Password Authentication: Cloud Securing Scheme," In Electronic Systems, Signal Processing And Computing Technologies (Icesc), 2014 International Conference On, Jan 2014, Pp. 479–483.

[3]. K. Gilhooly, "Biometrics: Getting Back To Business," Computerworld, May, Vol. 9, 2005. R. Dhamija And A. Perrig, "Deja Vu: A User Study Using Images For Authentication," In Proceedings Of The 9th Conference On Usenix Security Symposium-Volume 9. Usenix Association, 2000, Pp. 4–4.

[4]. S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, And N. Memon, "Passpoints: Design And Longitudinal Evaluation Of A Graphical Password System," International Journal Of Human-Computer Studies, Vol. 63, No. 1-2, Pp. 102–127, 2005.

[5]. A. Paivio, T. Rogers, And P. Smythe, "Why Are Pictures Easier To Recall Than Words?" Psychonomic Science, 1968.

[6]. D. Nelson, U. Reed, And J. Walling, "Picture Superiority Effect," Journal Of Experimental Psychology: Human Learning And Memory, Vol. 3, Pp. 485–497, 1977.

[7]. A. De Angeli, M. Coutts, L. Coventry, G. Johnson, D. Cameron, And M. Fischer, "Vip: A Visual Approach To User Authentication," In Proceedings Of The Working Conference On Advanced Visual Interfaces. Acm, 2002, Pp. 316–323.

Sahil Chordia " Anti Shoulder Surfing"International Journal of Engineering Research and Applications (IJERA) , vol. 8, no. 03, 2018, pp. 65-66