Special Issue Published in International Journal of Trend in Research and Development (IJTRD), ISSN: 2394-9333, www.ijtrd.com

The Shoulder Surfing Resistant Graphical Authentication Technique

[1] Ch Gopal Krishna and [2]R Bala Dinakar
[1]PG Student, [2]Assistant Professor
[1,2]Department of Computer Applications, Godavari Institute of Engineering and Technology, Rajahmundry, India

***Abstract*—**This evolution brings great accessibility but also increases the probability of exposing passwords to shoulder surfing attacks, Authentication based on passwords is used largely in applications for computer security and confidentiality. However, human actions such as choosing bad passwords and inputting passwords in an insecure way are regarded as ”the weakest link” in the authentication chain. Rather than arbitrary alphanumeric strings, users incline to choose passwords either short or meaningful for easy to memorization When users input their passwords in a public place, they may be at risk of attackers stealing their password. An attacker can capture password by direct observation or by recording the individual's authentication session. This is referred to as shoulder-surfing and is a known risk, of special anxiety when authenticating in public places Attackers can observe directly or use external recording devices to collect users' credentials to avoid this problem the process of pass matrix, based on graphical passwords to resist shoulder surfing attacks. With a one-time valid login indicator and circulative horizontal and vertical bars covering the entire scope of pass-images, Pass Matrix offers no suggestion for attackers to figure out or narrow down the password even they conduct multiple camera-based attacks.

Keywords*—Shoulder surfing attacks, pass matrix, pass image, pass objects, password security.*

I. INTRODUCTION

Various graphical password authentication arrangements were developed to address the problems and weaknesses associated with textual passwords. Based on some studies such as those in humans have a better aptitude To memorize images with long-term memory (LTM) than verbal representations. Image-based passwords were proved to be easier to recollect in several user studies. Traditionally, alphanumeric passwords have been used for user authentication. While today other methods with biometrics and smart cards are possible alternatives, passwords are likely to remain dominant for some time because of concerns about reliability, privacy, security, and ease of usage of other technologies [1]. Various graphical password authentication schemes [5],[2], [3], [4] were developed to address the problems and Weaknesses associated with textual passwords. Founded on some studies such as those in [8], [9], humans have a better ability to memorize images by long-term memory (LTM) than verbal representations. Image-based password were proved to be easier to recollect in several user studies[6],[7],[8].a result, users can set up a complex Authentication password and are capable of recollecting it after a long time even if the memory is not activated periodically. However, most of these image-based passwords are susceptible to shoulder surfing attacks (SSAs). This type of attack either uses direct observation, such as watching over someone's shoulder or applies video capturing techniques to get passwords, PINs, or other sensitive personal information[9], [10], [11].

1. Passwords should be easy to remember, and the user Authentication protocol should be executable quickly and easily by humans.
2. Passwords should be secure, i.e., they must look Random and should be hard to guess; they should be changed frequently, and should be different on different accounts of the same user they should not be written down or stored in plain text.

II. PROPOSED METHODOLOGY

This development brings great convenience but also increases the probability of exposing passwords to shoulder surfing attacks. Attackers can observe directly or use external recording devices to collect users' credentials. To overcome this tricky, we proposed a novel authentication system Pass Matrix, based on graphical passwords to resist shoulder surfing attacks. With a one-time valid login pointer and circulative horizontal and vertical bars covering the entire scope of pass-images, Pass Matrix offers no hint for attackers to figure out or narrow down the password even they conduct multiple camera-based attacks. a lot of research on password authentication has been done in the literature

III. RESULTS

Then the results of the implementation of graphical authentication system to resistant shoulder surfing attacks

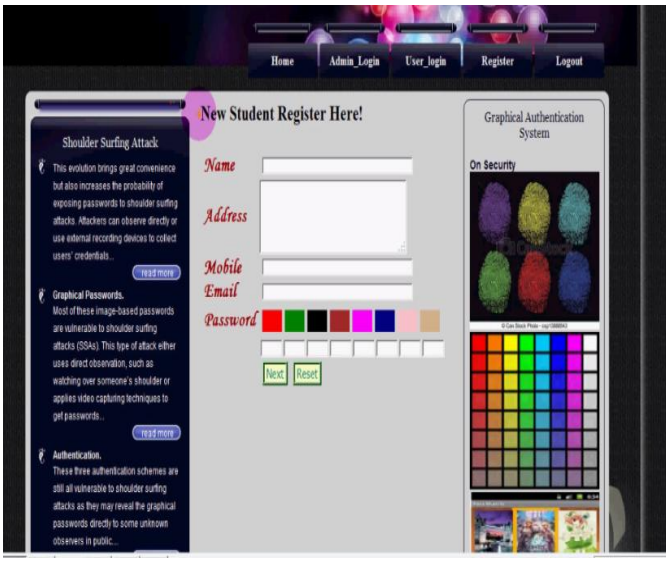

Figure 1: This is the new registration process

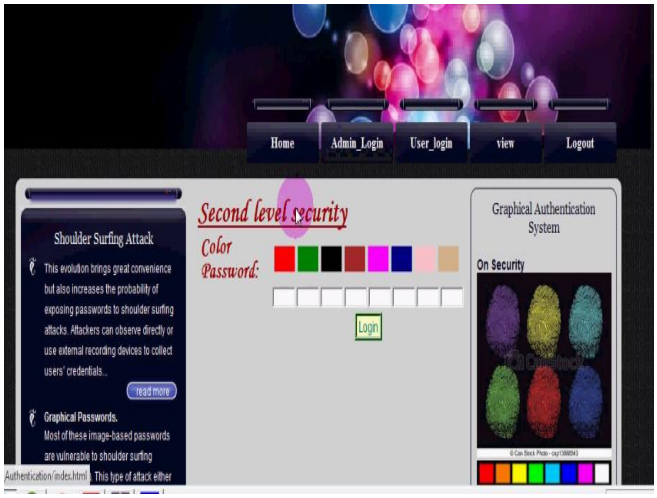

Figure 2: This is the second level new registration for security

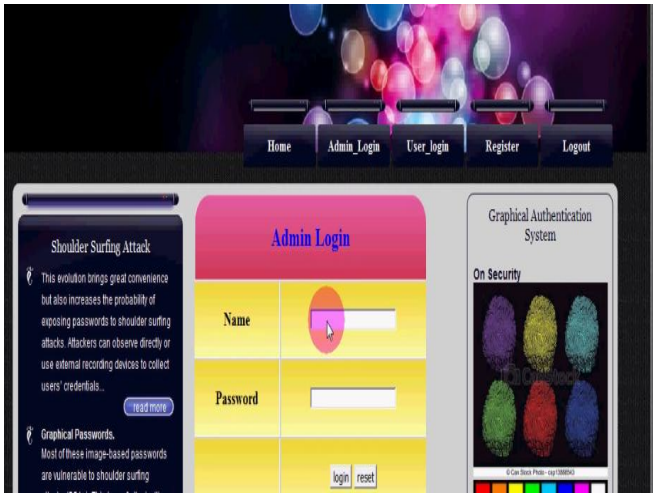

Figure 3: Admin login process

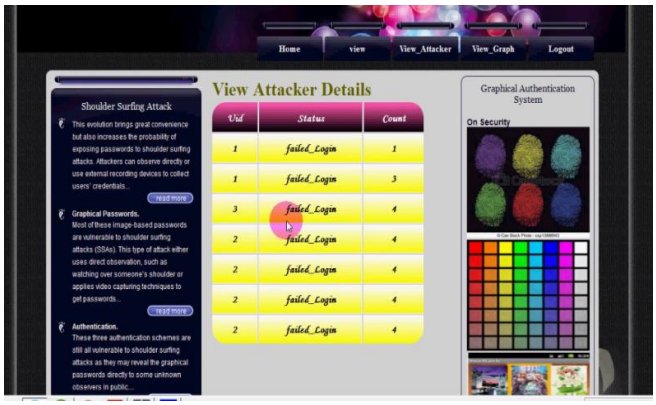

Figure 4: Then know the attacker details after the process of admin login

CONCLUSION

We analyzed the collected data from our experiments and surveys to evaluate the effectiveness of the proposed system. The results are presented in two perspectives: accuracy and usability. The accuracy perspective focuses on the successful login rates in both sessions, including the practiceogins. The usability perspective is measured by the amount of time users spent in each Pass Matrix phase. The Convex Hull Click Scheme is an effort to develop security innovations with people in mind. As such, it is an example of "usable security," an approach to design of security systems that Is gaining increasing attention At the end of this section, we also presented the statistics of the survey data from participants about their personal background and user experience on smart phones and Pass Matrix.

References

[1] Brostoff, S. and Sasse, M.A. Are Passfaces more usable thanpasswords: A field trial investigation. In McDonald S., et al.(Eds.), People and Computers XIV - Usability or Else, Proc. OfHCI 2000, Springer, 2000, 405-424.

[2] R. Dhamija and A. Perrig, "Deja vu: A user study using imagesfor authentication," in Proceedings of the 9th conference on USENIXSecurity Symposium-Volume 9. USENIX Association, 2000, pp. 4–4.

[3] "Realuser," http://www.realuser.com/.

[4] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "Thedesign and analysis of graphical passwords," in Proceedings of the8th conference on USENIX Security Symposium-Volume 8. USENIXAssociation, 1999, pp. 1–

[5] Davis, D., Monrose, F., and Reiter, M.K. On user choice ingraphical password schemes. In Proc. of the 13th USENIXSecurity Symposium, San Diego, 2004.

[6] S. Brostoff and M. Sasse, "Are passfaces more usable than passwords?a field trial investigation," PEOPLE AND COMPUTERS,pp. 405–424, 2000.

[7] 7.A. De Angeli, M. Coutts, L. Coventry, G. Johnson, D. Cameron,and M. Fischer, "Vip: a visual approach to user authentication," inProceedings of the Working Conference on Advanced Visual Interfaces.ACM, 2002, pp. 316–323.

[8] B. Ives, K. Walsh, and H. Schneider, "The domino effect of passwordreuse," Communications of the ACM, vol. 47, no. 4, pp. 75–78,2004.

[9] J. Long and K. Mitnick, No Tech Hacking: A Guide to Social Engineering,Dumpster Diving, and Shoulder Surfing. Elsevier Science,2011.

[10] T. Kwon, S. Shin, and S. Na, "Covert attentional shoulder surfing:Human adversaries are more powerful than expected," IEEETransactions on Systems, Man, and Cybernetics: Systems, vol. 44, no. 6,pp. 716–727, June 2014

[11] "Google glass snoopers can steal your passcode with a glance,"http://www.wired.com/2014/06/google-glass-snoopers-cansteal-your-passcode-with-a-glance/.