



Pass matrix: Efficient Authentication Mechanism to Protect User Data

¹M.Lakshmi Usha,²P. Radhika Krupalini

¹Final Master of Science in Computer Science, Dept of Computer Science, Ideal college of Arts and Sciences.,
Vidyuth Nagar, Kakinada, E.G. Dist., A.P., India.

²Associate Professor, Dept of Computer Science, Ideal college of Arts and Sciences., Vidyut
Nagar, Kakinada, E.G. Dist., A.P., India.

ABSTRACT:

We present a safe graphical verification arrangement named Pass Matrix that defends users from flattering fatalities of bear surfing attacks when entering passwords in community through the custom of one-time login indicators. A login indicator is arbitrarily made for each pass-image and will be unusable after the meeting dismisses. The login pointer delivers better safety in contradiction of shoulder surfing attacks, meanwhile users use an active pointer to point out the position of their passwords slightly than snapping on the key thing straight.

KEYWORDS: textual passwords, surfing attacks, password.

1 INTRODUCTION

Numerous graphical password authentication schemes were industrialized to speech the glitches and faintness allied with textual passwords. Founded on some studies humans have a healthier aptitude to learn images with long-term memory (LTM) than oral representations. Image-based passwords were demonstrated to be informal to recall in numerous user studies. As an effect, users can set up a composite authentication password and are proficient of recalling it subsequently a long time even if the recall is not galvanized intermittently. But, most of these image-based passwords are weak to shoulder surfing attacks (SSAs). This category of attack either uses shortest opinion, such as seeing over someone's shoulder or applies video apprehending techniques to get passwords, PINs, or other complex own material. The human actions such as indicating bad passwords for new accounts and entering passwords in an unconfident way for later logins are stared as the weakest link in the verification chain. So, an verification scheme must be calculated to overawed these susceptibilities.

2. LITERATURE SURVEY

2.1Text-based password schemes have integral safety and usability glitches, foremost to the growth of graphical password arrangements. Though, greatest of these alternative arrangements are susceptible to spyware attacks. We suggest a new arrangement, using CAPTCHA (Completely Automated Public Turing tests to tell Computers and Humans Apart) that retentive the compensations of graphical password schemes, while concurrently evitation the cost of opponents by orders of greatness.

2.2we planned a stroke-based textual password verification scheme. It uses forms of strokes on the network as the origin passwords and lets users to login with text passwords via old-style input devices. The way provides sturdy resilient to hidden-camera and shoulder-surfing. Furthermore, the system has elastic ugmentations to lock the authentication course. The study of the refuge of this tactic is also conversed.

3. PROBLEM DEFINTION

Pass-Matrix is susceptible to chance guess attacks based on hot-spot analyzing. TEXTUAL passwords have been the most extensively used verification method for periods. Included of numbers and upper- and lower-case letters, textual passwords are careful robust sufficient to fight against physical force attacks. Rendering to an object in Computer world, a safety team at a large business ran a system password cracker and astonishingly cracked about 80% of the employees' passwords within 30 seconds. Written passwords are frequently unconfident due to the trouble of upholding strong ones.

4. PROPOSED APPROACH

We suggested a unusual authentication system Pass Matrix, based on graphical passwords to counterattack shoulder surfing attacks. With a one-time valid login display and circulative parallel and

vertical bars cover the whole scope of pass-images, Pass Matrix offers no suggestion for attackers to number out or narrow down the PIN even they conduct manifold camera-based attacks. A lot of research on password verification has been done in the works.

5 SYSTEM ARCHITECTURE



Fig. 5. A password contains three images (n=3) with a pass square in each. The pass squares are shown as the orange-filled area in each image.

6 PROPOSED METHODOLOGY

Admin

Admin has to login with valid username and password. After login positive he can do certain operations such as view all user, their particulars and approve them, Opinion all users graphical authentication points, view all blocked users, View unlog requests and clear them, upload leaflets with image and view all uploaded documents with rank and comments of it, View users results diagram based on number of users lively and congested, View the documents results based on rank.

User

User should catalogue before responsibility some operations and also set graphical verification points while registration. After registering positive he can login by using valid user name and password and also graphical authentication points. Login successful he will do particular operations like view shape details, Chang graphical authentication points, search documents and download/View and comment on it/recommend to others , View all recommended documents.

7 PASSMATRIX TECHNIQUE

Step1: The user inputs his/her username which was created in the registration phase.

Step2: A new indicator comprised of a letter and a number is created by the login indicator generator module.

Step3: the user flings or drags the bars to align the pre-selected pass-square of the image with the login indicator.

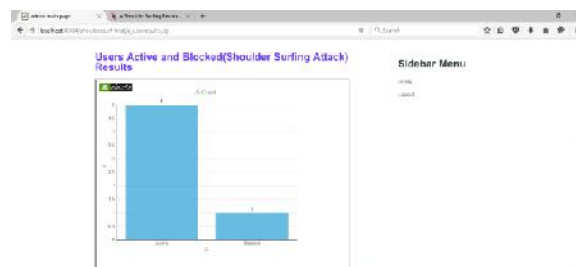
Step4: Repeat step 2 and step 3 for each pre-selected passimage.

Step5: The communication module gets user account information from the server through HttpRequest POST method.

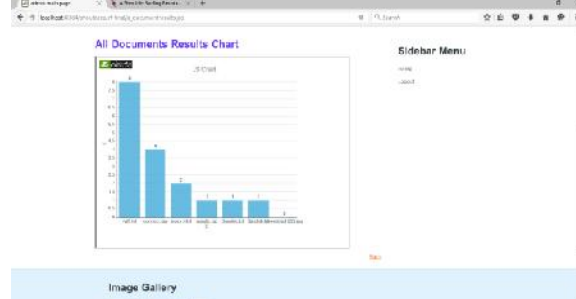
Step6: It verifies the alignment between the passsquare and the login indicator.

Step7: if all the alignments are correct in all images, the user is allowed to log into PassMatrix.

8 RESULTS



Users Active and Blocked Results



All Documents Results Chart

EXTENSION WORK:

Recommend two pictorial authentication protocols: one is a one-time-password protocol, and the extra is a password-based verification protocol. We were bright to accomplish a high level of usability while substantial rigorous security requirements. Two rules for confirmation that employs conception by means of bigger genuineness to make available both high security and high usability.

9 CONCLUSION

In command to guard users' digital property, verification is compulsory every time they attempt to admittance their private account and data. Yet, showing the authentication course in public might effect in probable shoulder surfing attacks. Uniform intricate password can be split straightforwardly through shoulder surfing. Via traditional textual passwords or PIN method, users

want to form their passwords to substantiate themselves and thus these passwords can be discovered easily if someone ganders over shoulder or uses video recording devices such as cell phones.

10 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.[

[4] 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.

[5] "Realuser," <http://www.realuser.com/>.

[6] I. Jermyn, A. Mayer, F. Monroe, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords," in *Proceedings of the 8th conference on USENIX Security Symposium-Volume 8*. USENIX Association, 1999, pp. 1–1.

[7] 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.

[8] A. Paivio, T. Rogers, and P. Smythe, "Why are pictures easier to recall than words?" *Psychonomic Science*, 1968.

[9] D. Nelson, U. Reed, and J. Walling, "Picture superiority effect," *Journal of Experimental Psychology: Human Learning and Memory*, vol. 3, pp. 485–497, 1977.

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

[11] 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.

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

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

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

[15] "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/>.

[16] Hung-Min sun, Shiuan-Tung Chen, Jyh-Haw Yeh and Chia-Yun Cheng, *A Shoulder Surfing Resistant Graphical Authentication System*, 2017

M.Lakshmi Usha is student of Computer Science Department at IDEAL COLLEGE OF ARTS AND SCIENCES, KAKINADA, AP, INDIA. Presently she is pursuing her final semester in Master of Science in Computer Science from Ideal college and she received her B.Sc(CS) from Ideal college, Kakinada in the year 2015.

P. RadhikaKrupalini is an Associate Professor of Computer Science Department at IDEAL COLLEGE OF ARTS AND SCIENCES, KAKINADA AP, INDIA. She passed M.Tech in Computer Science & Engineering from UCE, JNTU, Kakinada. She has Lectureship in Computer Science and Applications discipline and has an experience of 12 years of teaching.