Impact Factor (SJIF): 5.301

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444
Volume 5, Issue 5, May-2018

SHOULDER SURFING ATTACK

Sneha Rampure[1], Sonali Salunke[2], Snehal Khodade[3], Padmaja Kawade[4]
[1]Department of Computer Engineering, MITCOE. Pune
[2]Department of Computer Engineering, MITCOE Pune
[3]Department of Computer Engineering, MITCOE. Pune
[4]Department of Computer Engineering, MITCOE. Pune
sneha.rampure@yahoo.com
sonusalunke26@gmail.com
snehalkhodade8@gmail.com
padmaja.kawade96@gmail.com

Abstract - When users input their passwords in a very public place, they'll be in danger of attackers stealing their secret. Associate degree assaulter will capture a secret by direct observation or by recording the people authentication session. This is often cited as shoulder-surfing and may be an illustrious risk, of special concern once authenticating publically places. Till recently, the sole defense against shoulder-surfing was the alertness on the part of the user. Shoulder surfing resistant secret authentication mechanism assure shoulder-surfing resistant authentication to user. It permits user to attest by coming into pass-word in graphical approach at insecure places as a result of user ne'er ought to click directly on secret icons. Usability testing of this mechanism showed that novice users were able to enter their graphical secret accurately and to recollect it over time.

Keywords- Shoulder surfing, attack, and authentication

I. INTRODUCTION

Information and laptop security is supported mostly by passwords that area unit the principle a part of the authentication method. The foremost common laptop authentication methodology is to use alphamerical username and parole that has important drawbacks. To beat the vulnerabilities of ancient ways, visual or graphical parole themes are developed as doable various solutions to text primarily based scheme. A possible downside of graphical parole schemes is that they're additional liable to shoulder surfboarding than standard alphameric text passwords. Once users input their passwords in a very public place, they will be in danger of attackers stealing their parole. Associate in nursing assailant will capture a parole by direct observation or by recording the individual’s authentication session. This can be cited as shoulder surfboarding and could be an identified risk, of special concern once authenticating publically places. During this paper we'll present a survey on graphical parole schemes from 2005 until 2009 that are planned to be resistant against shoulder surfboarding attacks.

Current authentication systems suffer from several weaknesses. The vulnerabilities of the matter parole are acknowledged. Users tend to choose short passwords or passwords that area unit simple to recollect, that makes the passwords unprotected for attackers to interrupt. Moreover, matter parole is liable to dead reckoning, wordbook attack, key-loggers, and social engineering, shoulder-surfing, hidden-camera and spyware attacks. To overcome the restrictions of text-based parole, techniques like two-factor authentication and graphical parole are place in use. Apart from that, applications and input devices like mouse, stylus and touch-screen that let build the looks of the graphical user authentication techniques doable. However, they're largely liable to shoulder-surfing in addition.

Passwords possess several helpful properties in addition as widespread inheritance deployment; consequently we will expect their use for the predictable future. sadly, today's normal ways for parole input area unit subject to a range of attacks supported observation, from casual eavesdropping (shoulder surfing), to additional exotic ways. Shoulder-surfing attack happens once victimization direct observation techniques, like wanting over someone's shoulder, to induce passwords, PINs and different sensitive personal data. In addition as once a user enters data employing a keyboard, mouse, bit screen or any ancient device, a malicious observer is also ready to acquire the user's parole credentials. This can be a retardant that has been troublesome to beat.

II. LITERATURE SURVEY

1. Multi-touch passwords for mobile device access

Authors: I. Oakley and A. Bianchi

Description: Draw-a-Secret code word schemes, just like the Google robot Pattern Lock, entail stroke out a form on barely screen. This paper explores techniques for increasing the richness of this input modality (multitouch input, off-target interaction) so as to extend code word entropy and resistance to observation. A formative user study highlights user perceptions and usefulness problems with reference to this style house and suggests directions for future development of this idea.

2. The doodb graphical password database: Data analysis and benchmark results

Authors: M. Martinez-Diaz, J. Fierrez, and J. Galbally

Description: We gift DooDB, a doodle information containing knowledge from one hundred users captured with slightly screen-enabled mobile device beneath realistic conditions following a scientific protocol. The database contains 2 corpora: 1) doodles and 2) pseudo-signatures that are simplified finger-drawn versions of the written signature. The dataset includes real samples and forgeries, made beneath worst-case conditions, wherever attackers have visual access to the drawing method. Applied math and qualitative analyses of the info are bestowed, examination doodles and pseudo-signatures to written signatures. Time variability, learning curves, and discriminative power of various options also are studied. Verification performance against forgeries is analyzed exploitation progressive algorithms and benchmark results are provided.

3. Graphical Password-Based User Authentication With Free-Form Doodles

Authors: M. Martinez-Diaz, J. Fierrez, and J. Galbally

Description: User authentication mistreatment straightforward gestures are currently common in transportable devices. During this work, authentication with free-form sketches is studied. Verification systems mistreatment dynamic time distortion and mathematician mixture models square measure planned supported dynamic signature verification approaches. The foremost discriminant options square measure studied mistreatment the consecutive forward floating choice algorithmic program. The consequences of the time lapse between capture sessions and also the impact of the coaching set size also are studied. Development and validation experiments square measure performed mistreatment the DooDB information, that contains passwords from one hundred users captured on a wise phone touchscreen. Equal error rates between third and eight square measure obtained against random forgeries and between twenty first and twenty second against adept forgeries. High variability between capture sessions will increase the error rates.

III. EXISTING SYSTEM

Using ancient text passwords or PIN methodology, users have to be compelled to kind their passwords to certify themselves and therefore these passwords is disclosed simply if somebody peeks over shoulder or uses video devices like cell phones shoulder water sport attacks have posed a good threat to users' privacy and confidentiality as mobile devices are getting indispensable in fashionable life. Within the period, the graphical capability of hand-held devices was weak; the color and element it might show was restricted. With the increasing quantity of mobile devices and net services, users will access their personal accounts to send confidential business emails, transfer photos to albums within the cloud or remit cash from their e-bank account anytime and anyplace. Whereas work into these services publically, they'll expose their passwords to unknown parties unconsciously.

DISADVANTAGES

(1) Security weakness

(2) The easiness of obtaining passwords by observers in public,

(3) The compatibility issues to devices,

IV. PROPOSED SYSTEM

To overcome this obstacle, we tend to plan a shoulder surfing resistant authentication system primarily based on graphical passwords, named PassMatrix. Employing a one-time login indicator per image, users will suggests the situation of their pass-square while not directly clicking or touching it that is associate action liable to shoulder aquatics attacks. As a result of the look of the horizontal and vertical bars that cowl the complete pass-image, it offers no clue for attackers to slim down the watchword area though they need over one login records of that account. In PassMatrix, a watchword consists of just one pass-square per pass-image for a sequence of n pictures. The quantity of pictures (i.e., n) is user-defined. In PassMatrix, users select one sq. per image for a sequence of n pictures instead of n squares in one image as that within the PassPoints theme. Pass-Matrix's authentication consists of a registration part associated an authentication part as represented below: At this stage, the user creates associate account that contains a username and a watchword. The watchword consists of just one pass-square per image for a sequence of n pictures. The quantity of pictures (i.e., n) is set by the user when considering the trade-off between security and value of the system. At this stage, the user uses his/her username, watchword and login indicators to log into PassMatrix.

ADVANTAGES

1. Highly secured
2. Device compatible
3. Easy to handle

V. SYSTEM ARCHITECTURE

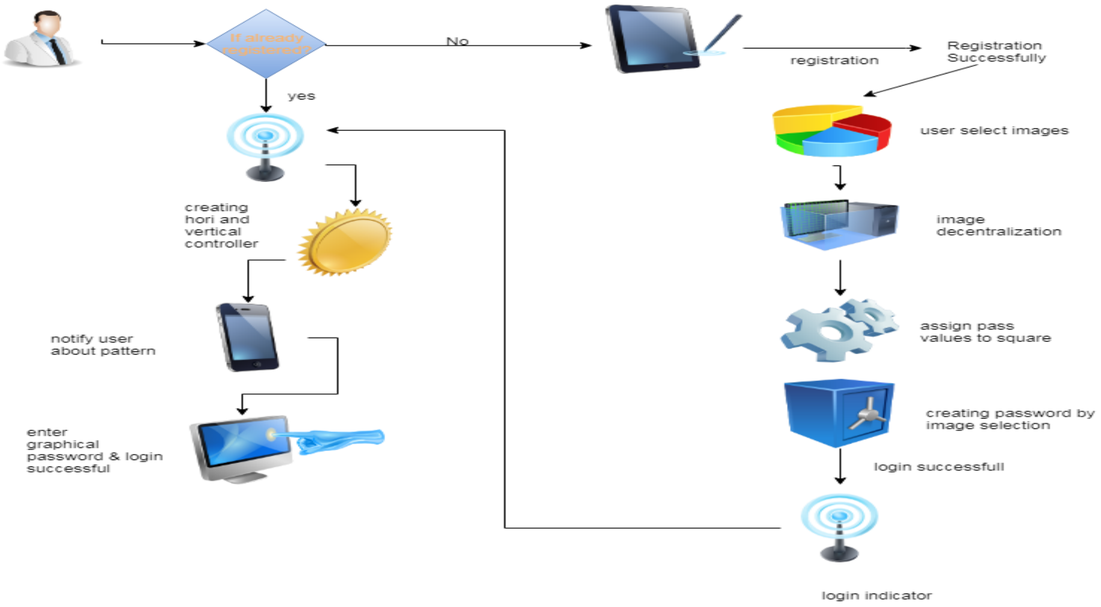
If already registered?
No
yes
registration
Registration Successfully
user select images
image decentralization
assign pass values to square
creating password by image selection
login successfull
login indicator
creating hori and vertical controller
notify user about pattern
enter graphical password & login successful

Fig. System Architecture

VI. CONCLUSION

Proposed a shoulder surfing resistant authentication system supported graphical passwords, named PassMatrix. Employing a one-time login indicator per image, users will show the placement of their pass-square while not directly clicking or touching it that is Associate in nursing action prone to shoulder surfboarding attacks. As a result of the planning of the horizontal and vertical bars that cowl the complete pass-image, it offers no clue for attackers to slim down the positive identification area albeit they need over one login records of that account. Moreover, we be inclined to implement a Pass Matrix image on automatic man and meted out user experiment to judge the memo ability and usefulness. The experimental result showed that users will log into the system with a median of 1:64 tries (Median=1), and also the Total Accuracy of all login trials is 93:33% even period of time once registration. The entire time consumed to log into PassMatrix with a median of 3:2 pass-images is between 31:31 and 37:11 seconds and is taken into account acceptable by 83:33% of participants in our user study. Supported the experimental results and survey knowledge, PassMatrix may be a novel and easy-to-use graphical positive identification authentication system, which might effectively alleviate shoulder-surfing attacks.

REFFERENCES

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