11th International Conference on Recent Development in Engineering Science, Humanities and Management
Nutan Maharashtra Institute of Engineering & Technology, Talegaon Dabhade, Pune ESHM-18
24th-25th March 2018 www.conferenceworld.in ISBN : 978-93-87793-14-9

Shoulder Surfing Resistant using PassMatrix Techniques

Amit Mahamuni[1], Sunil Lote[2], Suchit Waghamare[3], Sachin Dhatrak[4], Prof. Aditi Das[5]

[1,2,3,4,5]*Information Technology, Nutan Maharashtra Institute of Engineering and Technology, Talegaon Dabhade, (India)*

ABSTRACT

When users insert their password in a public place, there may be a possibility that the attackers may steal their password. An attacker can capture your password by direct observation or by recording the person's authentication session process. This is known as shoulder-surfing attack, this attack is of special concern when authenticating in public places. Alternatives, the only real defence against shoulder-surfing were the alertness by the person. Shoulder surfing resistant password authentication mechanism assure shoulder-surfing resistant authentication to user. Allows user to authenticate or login in public place on any devices. Usability testing of this mechanism established that new users had the ability to enter their graphical password accurately and also to remember it after a while. However, the security against shoulder-surfing comes at the price of greater time span to carry out the authentication.

KEYWORDS: Graphical Authentication, Graphical Login, Transaction, image processing, Secrete key.

I.INTRODUCTION

Shoulder surfing is using direct observation techniques, such as looking over someone's shoulder, to get information. Shoulder surfing is an effective way to get information in crowded places because it's relatively easy to stand next to someone and watch as they fill out a form, enter a PIN number at an ATM machine, or use a calling card at a public pay phone. Shoulder surfing can also be done over a long distance with the aid of binoculars or other vision-enhancing devices.

In computer security, shoulder surfing is a type of social engineering technique used to obtain information such as personal identification numbers (PINs), passwords and other confidential data by looking over the victim's shoulder. To implement this technique attacker do not require any technical skills; keen observation of victims' surroundings and the typing pattern is sufficient.

A hidden camera allows the attacker to capture whole login process and other confidential data of the victim, which ultimately could lead to financial loss or identity theft.

Shoulder surfing also occurs in daily situations to uncover private content on handheld mobile devices; shoulder surfing visual content was found to leak sensitive information and even private information about third-parties.

II. LITERATURE SURVEY

In [1] the author I. Oakley and A. Bianchi suggests "Multi-touch passwords for mobile device access" Draw-a-Secret password schemes, like the Google Android Pattern Lock, entail stroking out a shape on a touch screen. This paper explores techniques for expanding the richness of this input modality (multi-touch input, off-target interaction) in order to increase password entropy and resistance to observation. A formative user study highlights user perceptions and usability issues relating to this design space and suggests directions for future development of this concept.

In [2] the author M. Martinez-Diaz, J. Fierrez, and J. Galbally suggest "doodb graphical password database: Data analysis and benchmark results" We present DooDB, a doodle database containing data from 100 users captured with a touch screen-enabled mobile device under realistic conditions following a systematic protocol. The database contains two corpora: 1) doodles and 2) pseudo-signatures, which are simplified finger-drawn versions of the handwritten signature. The dataset includes genuine samples and forgeries, produced under worst-case conditions, where attackers have visual access to the drawing process. Statistical and qualitative analyses of the data are presented, comparing doodles and pseudo-signatures to handwritten signatures. Time variability, learning curves, and discriminative power of different features are also studied. Verification, performance against forgeries is analyzed using state-of-the-art algorithms and benchmark results are provided.

In [3] the author M. Martinez-Diaz, J. Fierrez, and J. Galbally suggest "Graphical Password-Based User Authentication with Free-Form Doodles" User authentication using simple gestures is now common portable devices.

In this work, authentication with free-form sketches is studied. Verification systems using dynamic time warping and Gaussian mixture models are proposed based on dynamic signature verification approaches. The most discriminate features are studied using the sequential forward floating selection algorithm. The effects of the time lapse between capture sessions and the impact of the training set size are also studied. Development and validation experiments are performed using the DooDB database, which contains passwords from 100 users captured on a smart phone touch screen. Equal error rates between 3% and 8% are obtained against random forgeries and between 21% and 22% against skilled forgeries. High variability between capture sessions increases the error rates.

In [4] the author T. Kwon, S. Shin, and S. Na suggest "Covert attention shoulder surfing: powerful than expected"

When a user interacts with a computing system to enter a secret password, shoulder surfing attacks are of great concern. To cope with this problem, previous methods presumed limited cognitive capabilities of a human adversary as a deterrent, but there was a pitfall with the assumption. In this paper, we show that human adversaries, even without a recording device, can be more effective at eavesdropping than expected, in particular by employing cognitive strategies and by training themselves. Our novel approach called covert attention shoulder surfing indeed can break the well-known PIN entry method previously evaluated to be secure against shoulder surfing.

III. MATHEMATICAL MODEL

Let S be the Whole system which consists:

S= {IP, Pro, OP}

Where,

A. **IP-** is the input of the system.
B. **Pro-** is the procedure applied to the system to process the given input.
C. **OP**- is the output of the system.

A. Input

IP = {u, I, LI, ht, wt, pv, n}

Where,

1. **u** -be the user.
2. **I**- be set of images used for creating graphical password.
3. **ht** -be the height of image.
4. **wt** - be the width of the image.
5. **pv** - be the pass values of the selected image for generating graphical password.
6. **LI**- be the login indicator used at the time of login.
7. **n**- be the number of images chosen for creating graphical based password from set of images I.

B. Procedure

1. Registration phase

i. In 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.

ii. The number of images 'n' is decided by the user after considering the trade-off between security and usability of the system. The only purpose of the username is to make the user imagine of having a personal account.

iii. Then the systems will divide the selected images by using pass matrix approach into x and y grinds by calculating ht and wt of images.

iv. Then system will create the graphical based password after clicking on the images selected from I.

2. **Authentication phase**

i. A login indicator LI is comprised of a letter and a number is created by the login indicator generator module.

ii. The LI will be shown when the user logs in with his email. In this case, the indicator is conveyed to the user by visual feedback. The indicator can also be delivered through a predefined image.

iii. Generating a horizontal and vertical access control for login indicator based on the images selected by the user at the time of registration. This access control will change at every login time i.e. LI is defined for one time use only.

iv. The generated access control will be send to user registered email address or his phone number.

v. User will enter the graphical password based on generated pass-values i.e. access controls.

C. Output:

Secure and authenticated system based on Pass Matrix based graphical password system.

IV. EXISTING SYSTEM

Using traditional textual passwords or PIN method, users should type their passwords to authenticate themselves and so these passwords may be stolen easily. If someone peeks over shoulder or uses video devices for example mobile phones, shoulder surfing attacks have posed an incredible threat to user's privacy and confidentiality as cellular phones have grown to be indispensable in modern life. In the past, the graphical capability of handheld devices was weak as the color and pixels it could possibly show was limited. With all the increasing volume of mobile devices and web services, users can access their personal accounts to deliver confidential business emails, upload photos to albums within the cloud or remit money using their e-banking account anytime and anywhere. While logging in to these services in public places, they may expose their passwords to unknown parties unconsciously.

Disadvantages of Existing System: -

Security weakness- different types of attack is present such as smudge attack, DOS (Denial Of Service) attack, brute-force attack, Dictionary attack, etc.

The password is easily obtained in public place by direct observing or recording the activity of login process.

Difficult in remembering password so user can select easy textual password as it is easy to remember that way it is easy to guess for attacker. If user selects a hard password, then it is hard to remember.

Graphical password method: -

To overcome the drawbacks of text-based authentication we have developed a new password scheme which uses images, pictures as a password known as graphical password scheme. This scheme is used as an alternative to the alphanumeric password.

V. PROPOSED SYSTEM

To conquer this issue, we proposed a shoulder surfing resistant authentication system determined by graphical passwords [5], named PassMatrix. By using a one-time login indicator per image, users can explain the positioning with their pass-square without directly clicking or touching it, that is an action prone to shoulder surfing attacks. Because of the kind of the vertical and horizontal bars which cover the whole pass-image, it gives you no idea for attackers to restrict the password space even when they have multiple login records of these accounts. In PassMatrix, your password consists of only 1 pass-square per pass-image for the sequence of n images. The quantity of images (i.e., n) is user-defined. In PassMatrix, users select one square per image for a sequence of n images rather than n squares in an image as that from the PassPoints scheme [6]. PassMatrix authentication is made up of registration phase with an authentication phase as described below: At this point, the consumer creates an account which contains a username and a password. The password is made up of only one pass-square per image for any sequence of n images. The number of images (i.e., n) is decided by the user after with the trade-off between security and usability from the system. At this stage, an individual uses his/her username, password and login indicators to log in PassMatrix.

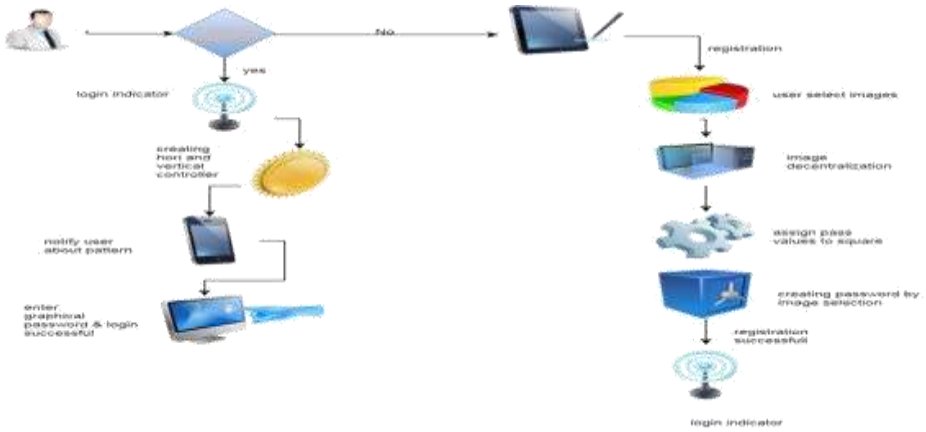
Advantages of Proposed System:

Highly secured - In the proposed system we use three different image, secret Bit, and also for pass values use OTP.

Device compatibility – Proposed system implemented in web based so it is platform independent and also operating system independent.

Resistance of Attacks- Proposed System is capable for preventing the smudge attack, brute force attack, dictionary attack and also handle the DOS (Denial Of Service) attack.

SYSTEM ARCHITECTURE



VI. CONCLUSION

In many security systems, authentication methods and techniques are available but each with its own advantages and short comings. In the above system, we have proposed an authentication system which is based on graphical password schemes. We have proposed a shoulder surfing resistant authentication system determined by graphical passwords, named PassMatrix. Using a one-time login indicator per image, users can explain the location of their pass-square without directly clicking or touching it, that's an action at risk of shoulder surfing attacks. Due to the form of the vertical and horizontal bars that covers the complete pass-image, it provides no clue for attackers to get access to the passwords even when they have multiple login records of this account. Depending on the experimental results and survey data, PassMatrix can be a novel and simple-to-use graphical password authentication system, which can effectively prevent shoulder-surfing attacks. Moreover, PassMatrix does apply to your authentication scenario and device with simple input and output capabilities. Study of the paper using a laptop and a computer we have found that PassMatrix applied system is practical in day to day life. In this system user can easily login into system without worrying about shoulder surfing and key logger attacks. In future some other important things regarding the performance of our system will be investigated like User Adaptability and Usability and Security of our system.

REFRENCES

[1] Oakley, Ian, and Andrea Bianchi. "Multi-touch passwords for mobile device access." Proceedings of the 2012 ACM Conference on Ubiquitous Computing. ACM, 2012.

[2] Martinez-Diaz, Marcos, Julian Fierrez, and Javier Galbally. "The DooDB graphical password database: data analysis and benchmark results." IEEE Access 1 (2013): 596-605.

[3] Martinez-Diaz, Marcos, Julian Fierrez, and Javier Galbally. "Graphical password-based user authentication with free-form doodles." IEEE Transactions on Human-Machine Systems 46.4 (2016): 607-614.

[4] Kwon, Taekyoung, Sooyeon Shin, and Sarang Na. "Covert attentional shoulder surfing: Human adversaries are more powerful than expected." IEEE Transactions on Systems, Man, and Cybernetics: Systems 44.6 (2014): 716-727.

[5] 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.

[6] 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.

[7] 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.

[8] 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. 4–7.

[9] 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.

[10] L. Sobrado and J. C. Birget, "Graphical passwords," Rutgers Scholar, vol. 4, 2002 [Online]. Available: http://RutgersScholar.rut-gers.edu/volume04/contents.htm