International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 01 | Jan -2017 www.irjet.net p-ISSN: 2395-0072

A Survey on "Pass sequence acting as OTP using Login Indicator preventing Shoulder Surfing attacks"

Amit Kalamkar, Sweta Chaugule, Swati Lavate, Dinesh Dalvi

Student Computer Department, SKN SITS Lonavala, Maharashtra, India

---

Abstract - *Shoulder-Surfing is a recognized hazard where an attacker can capture a password by means of direct observation or by way of recording the authentication. There were some graphical schemes resistant to SSAs; however they have got substantial usability drawbacks, generally in the time and effort to log in. In this paper, we suggest and compare a brand new shoulder-browsing resistant scheme which has a proper usability for PDAs.The new scheme requires users to attract throughout their password pix orderly in preference to click directly on them. Authentication based on passwords is used in large part of programs for laptop security and privacy. However, human efforts consisting of choosing bad passwords and inputting passwords in an insecure manner are regarded as the weakest link in authentication chain. While choosing alphanumeric strings, customers tend to select passwords both quick and significant for easy memorization. This evolution brings superb comfort however also increases the opportunity of disclosing passwords to SSAs. Attackers can take a look directly or use outside recording gadgets to acquire users credentials. To conquer this hassle, we proposed a novel authentication device Pass Matrix, based totally on graphical passwords to resist SSAs assaults. With a one-time login indicator the pass sequence generated each time is different which offers no trace for attackers to determine the password. We additionally applied a Pass Matrix prototype on Android and carried out actual user experiments. From the experimental end result, the proposed system achieves higher resistance to Shoulder browsing attacks even as retaining usability.*

Key Words: **Pass images, Pass value, Login Indicator, Shoulder Surfing Attacks (SSAs) and Authentication**

1. INTRODUCTION

Nowadays with the rapid and unstoppable growth in the development field of technology has created the scope of becoming the use to of it. Where the authentication plays a vital role for ensuring the users identity. And for ensuring the identity username and password must be verified. But the most importantly the attention is given to the password which must be hide from the world to protect ones repository.

Till now we used the textual passwords for the authentication purpose which may be comprised of lower case letters, upper case letters or the alphanumeric combinations of one another. Somehow the textual password is considered strong enough for resisting against the brute force approach.

Sometimes the long and complicated textual passwords become hard to memorize and collect. However by selecting the simple textual passwords may increases its vulnerability for attacks or intrusions. One of the most commonly and easily happened attack is the Shoulder surfing attacks (SSAs).

SSAs are the attacks which can be happened at any point of time just by looking over someone's shoulder while entering the passwords. It may happen by direct observing or by using video capturing technique to get passwords, PINs or other sensitive personal information. In the whole authentication process the human action such as choosing the bad and weak password for a new account and putting the passwords in an insecure way for later logins is considered as the weakest link in the authentication chain.

To overcome all these drawbacks an alternative is available for setting the password as Graphical images in a place of textual passwords. Graphical passwords have the tendency to bridge the gap of inputting the password and getting attacked. As memorizing the images, for a long time with Long Term Memory (LTM) is easier then verbal representation. They also create a scope of vulnerable to SSAs but the extent of getting attacked is reduced by various means.

In this paper we present a novel and secure Graphical Authentication System which provides an advanced security to the passwords with combination of Pass images selected

from the collection of images or from our local data storage. Security is provided by on click method on pass images which generates the pass value for the corresponding click and results in generation of pass sequence. Every time the pass sequence is generated by the Login Indicator in the background for single login session which acts as OTP i.e. one time password which is sent to the user's mail id .Prevention from the SSAs is provided by generating the Pass sequence for every login session and which gets useless after termination of that session.

2. Related Work

Both are not immune as expected to SSAs and other brute force attacks More advancement in the security is provided with the Graphical images in the way of generating the pass sequence every time. So various aspects in graphical passwords are as follows:

2.1: Pass Value System

The images selected from the collection of images are divided into pass squares having associated pass value for each pass square. On clicking, the corresponding pass value or pixel value is traced and recorded. For every image the pass values are generated on clicking on each image all the time and the sequence formed by the pass values is only resides till termination of that session.

2.2: Pass Matrix Algorithm

The algorithm used is Pass Matrix which divides each pass image into a grid of matrix of 7 X 11 form having the horizontal and vertical bar values. Those values are randomly generated by the login indicator in each login session which corresponds to different different pass values for the click.

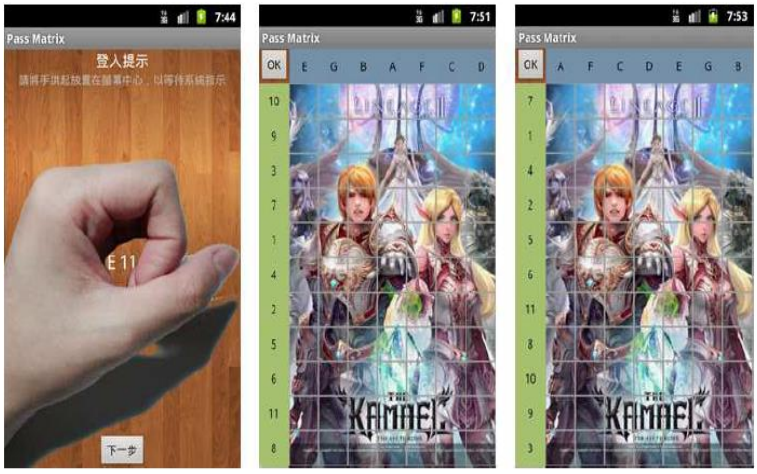


Fig: (a) The primary page of bypass Matrix, consumer can check in an account practice or start to login for experiment. (b) Users can pick from a listing of 24 pictures as their Pass images. (c) From the 7X11 squares in each photo, the users pick one as the pass square on clicking

2.3: OTP generation/Pass Sequence

Here the OTP which is nothing but the sequence generated by the login indicator in bag ground which is sent to the user's mail ID.After validating and verification that sequence the user are allowed to authenticate.

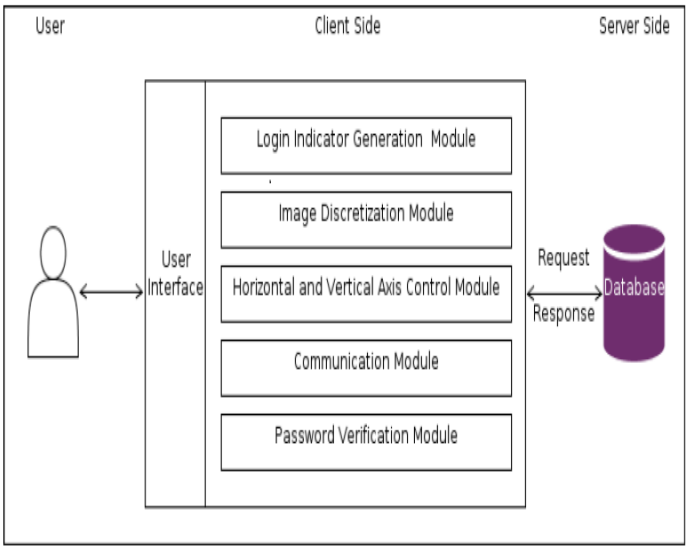
3. Proposed System

The system which we are proposing is more prone to SSAs attacks and increases the level of security.Gaphical images are provided with advancements on the basis of ON CLICK method instead of following the patterns on the images which are used earlier. The whole system works in two phases

1. Registration phase: creating a username and password using the images for the very first time

2. Authentication Phase: authorized users then uses the One time randomly generated sequence to login

3.1. System Architecture



4. Motivation

In 2006, Wiedenbeck et al. proposed Pass Points in which the user picks up several points (3 to 5) in an image during the password creation phase and re-enters each of these pre-selected click-points in a correct order within its tolerant square during the login phase. Comparingto traditional PIN and textual passwords, the Pass-Points scheme substantially increases the password space and enhances password memorizability. Unfortunately, this graphical au-thentication scheme is vulnerable to shoulder surfing attacks. Hence, based on the Pass Points, we add the idea of using one-time session passwords and distracters to develop our Pass Matrix authentication system that is resistant to shoulder surfing attacks.

5. Acknowledgement

We would like to express our gratitude towards the guide of our project Mrs. Bhavna Bahikar and all my group partners and the anonymous references who contributed to improve our paper in some way.

6. Conclusion

With the growing fashion of internet offerings and apps, users are able to get right of entry to those packages anytime and everywhere with various devices and with a view to guard customers' digital property, authentication is needed on every occasion they are attempting to get right of entry to their non-public account and statistics. However, undertaking the authentication method in public would possibly bring about potential shoulder browsing attacks. Even a complicated password can be cracked without difficulty thru shoulder surfing. using traditional textual passwords or PIN technique, users need to type their passwords to authenticate themselves and as a consequence those passwords may be discovered without difficulty if a person peeks over shoulder or uses video recording devices which include cellular telephones. Outgrowing and overcoming the issues related to security and to have a safe data storage and transfer we have proposed a system where the Pass sequence acting as OTP preventing Shoulder Surfing attacks' replaces the textual passwords in this manner. Using this approach of passwords will greatly increases the level of security and reduces the extent of various brute force and SSAs attacks.

REFERENCES

[1] Hung-Min Sun,Shiunan-Tung Chen,Jyh-Haw Yeh and Chia-Yun Cheng, A Shoulder Surfing Resistant Graphical Authentication System,Citation Information DOI 10.1109/TDSC.2016.2539942,IEEE.

[2] Roshni Rajavat, Bhavna Gala,Asmita Redekar, Textual and Graphical password Authentication scheme Resistant to Shoulder Surfing, 2015. International Journal of Computer Applications(0975-8887). Proceeding of International Conference on, 19,march 2015.

[3] 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. 17.

[4] 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.

[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.