International Journal on Recent Researches in Science, Engineering & Technology (IJRRSET)

A Journal Established in early 2000 as National journal and upgraded to International journal in 2013 and is in existence for the last 10 years. It is run by Retired Professors from NIT, Trichy. Journal Indexed in JIR, DIIF and SJIF.

Research Paper

Available online at: www.jrrset.com

UGC Approved Journal No: 45483

Received on: 01.03.2018 Published on: 30.03.2018 Pages : 63 - 70

ISSN (Print) : 2347-6729
ISSN (Online) : 2348-3105

Volume 6, Issue 3, March 2018.
JIR IF : 2.54
SJIF IF : 4.334
Cosmos: 5.395

MITIGATING SHOULDER SURFING ATTACK USING GRID AND COLOUR MATRIX

Deepa R[1], **Vidhya Ashok**[2]

[1,2]Assistant Professor, Department of Computer Science & Engineering
SRM Institute of Science & Technology, Chennai, 600026, India

Abstract

In realtime processing, when the user enters the Personal Identification Number (PIN) as a numeric password in mobile or stationary system, including smart phones, tablet computers, Automated Teller Machines (ATM), and Point Of Sale (POS) terminals, a direct observation attack based on shoulder surfing becomes a great concern. The PIN entry can be observed by nearby adversaries, more effectively in a crowded place. The same PIN is usually chosen by a user for various purposes and PIN may cause the user a great risk. To cope with this problem, developing an application which is between the user and the system, in each round a regular numeric keypad is colored at random, To address this problem, text can be combined with images or colours to generate session passwords for authentication. Session passwords can be used only once and every time a new password is generated. In this proposal, two techniques are proposed to generate session passwords using text and colours which are resistant to shoulder surfing. These methods are suitable for Personal Digital Assistants.

Keywords-Personal Identification Number, Shoulder-surfing attack, User authentication, Grey and Color Matrix.

I. INTRODUCTION

At present the Personal Identification Number (PIN) is a common user authentication method used in various situations, such as in withdrawing cash from an Automatic Teller Machine (ATM), approving an electronic transaction, unlocking a mobile device and even opening a door. However, a critical issue with PINs is that they are vulnerable to Shoulder-Surfing Attacks (SSAs). In other words, anyone who observes the logon procedure by looking over a user's shoulder can easily memorize his/her PIN. This kind of attack is an actual threat to use of PINs because there are many cases in which PINs are used in public places and for financial transactions. For example, a combination of an SSA and stolen or skimmed material such as a magnetic card or a mobile device enables an attacker to obtain a victim's account.

In computer security, shoulder surfing refers to using direct observation techniques, such as looking over someone's shoulder, to get the information. It is commonly used to obtain the passwords, PIN security codes, and similar data. Shoulder Surfing can also be done at a distance using binoculars or other vision-enhancing devices. In expensive, miniature closed-circuit television cameras can be concealed in ceilings, walls or fixtures to observe data entry. Thus, advanced PIN-entry methods that are resistant to SSAs, including recording attacks using a miniature video camera and smartphones, are crucial. However, SSA resistance should not be obtained by sacrificing resistance to random guessing attacks.

Although there have been many proposals to deal with these issues, most of the proposed methods are not widely accepted in practice due to various methods with the existing four digit numerical PIN. If a new method is supposed to be used in limited case, e.g., to unlock a smart phone, defining a new space such as the Android pattern lock is not a problem. However, if it is to be used for more generic purposes, compatibility matters. Requiring users to memorize longer or multiple PIN sequences would have a detrimental effect on recall, and obviously, no substantial improvement will be achieved for a long as entered information remains constant. Likewise, requiring the users to perform mathematical calculations while entering the PINs is unreasonable.

All this would raise the rate of erroneous PIN entries, which would turn annoy users and thereby reduce the acceptance of the technology. Moreover, service and the operation costs e.g., in the retail banking sector would increase due to growing number of request to reset PINs which are commonly blocked after three false entries.

In shoulder surfing attacks, adversaries should move their eye fixations rapidly on the user when he types the password, particularly in the crowded places to obtain the challenge information, for example when the user presses the key someone can easily acquire the information while processing. And the existing idea is covert attention.

Unfortunately, these passwords can be easily guessed or cracked. The alternative techniques are graphical passwords and biometrics. But these two techniques have their own disadvantages. Biometrics, such as finger prints, iris scan or facial recognition have been introduced but not yet widely adopted. The major drawback of this approach is that such systems can be expensive and the identification process can be slow.

There are many graphical password schemes that are proposed in the last decade. But most of them suffer from shoulder surfing which is becoming quite a big problem. There are graphical passwords schemes that have been proposed which are resistant to shoulder-surfing but they have their own drawbacks like usability issues or taking more time for user to login or having tolerance levels. Personal Digital Assistants are being used by the People to store their personal and confidential information like passwords and PIN numbers.

The nature of today's web threats over internet is changing day by day; current attacks are much more aggressive than they were in the past. This made web, network and application security extremely difficult and major issue. It is of top concern for personal as well as corporate to protect their confidential data.

The entire idea is based on the session passwords. Here, the main objective is to provide security to the confidential files, folders in computing devices through session passwords. It includes 3 phases: registration, primary level authentication, secondary level authentication (draw-a-secret). This technique is resistant to shoulder surfing. Due to dynamic passwords, dictionary attack is not applicable. Even key logger or mouse pointer tracker won't work because of its dynamic nature. Session passwords are unique that can be used only once and every time a new password is generated.

II. LITERATURE SURVEY

Various comprehensive investigations on the existing authentication schemes have been accomplished. And it has been discerned that one of the recent authentication schemes can resist all sorts of attacks. With this outcome, this proposes an authentication schemes which overcomes all the existing authentication schemes. The review reveals all the studies that are done in past.

“A User Study Using Images for Authentication” by Dhamija and Perrig, States that a graphical authentication scheme in which the user identifies the pre-defined images to prove the authentication of the user. In this scheme, during registration the user selects a set of images from a predefined set of images. Later on at the login time the user has to select the images that he had selected during the registration time to prove his authentication. But this system is vulnerable to shoulder-surfing.[1]

User Corporation: Passfaces. www.passfaces.com refers that authentication scheme was based on the principle that the user has to draw his signature by using mouse. This scheme had two stages of implementation viz. the registration phase and the verification phase. At the time of registration the user draws a signature that is extracted by the system. At the time of registration the signature is taken as an input and normalization is done and then the parameters are extracted and checking is done and the user is authenticated if the parameters get matched. But drawing with mouse is not so easy and actual parameters cannot be matched with the signature that was drawn at the registration time. This scheme is prone to forgery of signature.[2]

“The design and analysis of graphical passwords” by Jermyn, I., Mayer A., Monrose, F., Reiter, M., and Rubin, Have shown that the user has to draw a picture on the grid at the time of registration. The user has to draw the same picture on a 2D grid at the time of login. If the drawing of picture touches the same grid in same sequence the users gets authenticated. But this scheme was prone to shoulder surfing attacks.[3]

The paper entitled “A User Identification System Using Signature Written with Mouse”,by] A. F. Syukri, E. Okamoto, and M. Mambo, proposed that the authentication scheme was based on the principle that the user has to draw his signature by using mouse. This scheme had two stages of implementation viz. the registration phase and the verification phase.

At the time of registration the user draws a signature that is extracted by the system. At the time of registration the signature is taken as an input and normalization is done and then the parameters are extracted and checking is done and the user is authenticated if the parameters get matched. But drawing with mouse is not so easy and actual parameters cannot be matched with the signature that was drawn at the registration time. This scheme is prone to forgery of signature.[4]

“A New Graphical Password Scheme Resistant to Shoulder-Surfing” by HaichangGao, ZhongjieRen, Xiuling Chang, Xiyang Liu UweAickelin ,referes to the scheme which is the combination of DAS and Story schemes. The user has to draw a curve along the images to prove their authenticity.[5]

“Design and longitudinal evaluation of a graphical password system”.by S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, N. Memon propose to overcome shoulder surfing attacks a new graphical password scheme in which the user has to recognise the pass objects and click in the convex hull formed of the pass objects. If the password had to be made large then it becomes crowded.[6]

"Authenticating Mobile Device User through Image Selection” by W.Jansen shown that the scheme had two phases one that is creation and the other is authentication. In the creation phase the user selects a theme that consist photos in a thumbnail size and a set of sequence of pictures as password. And then at the authentication phase the user has to recognise the images incorrect order. Each thumbnail is assigned a numeric value .Based on the thumbnails a numeric password is created. But the limit size of this password is 30.Hence Short password is created.[7]

III. SYSTEM ARCHITECTURE

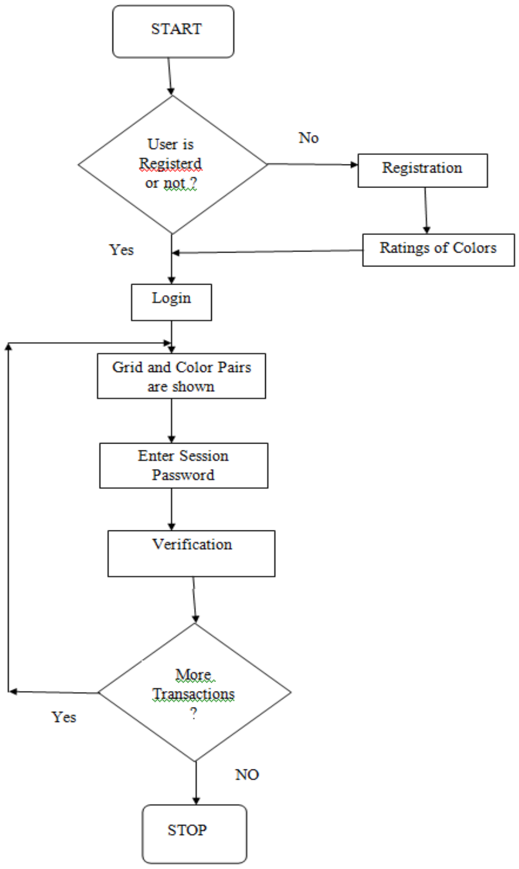


Fig 1 : Architectural Flow Diagram

System Modules

Authentication technique consists of 3 phases

1. Registration phase
2. Login phase
3. Verification phase

During registration, user enters his password in first method or rates the colours in the second method. During login phase, the user must enter the password based on the interface displayed on the screen. The system verifies the password entered by comparing with content of the password generated during registration.

Advantage:

1) The Session passwords are passwords that are used only once

2) The users input different passwords.

3) The session passwords provide better security against dictionary and brute force attacks as password changes for every session.

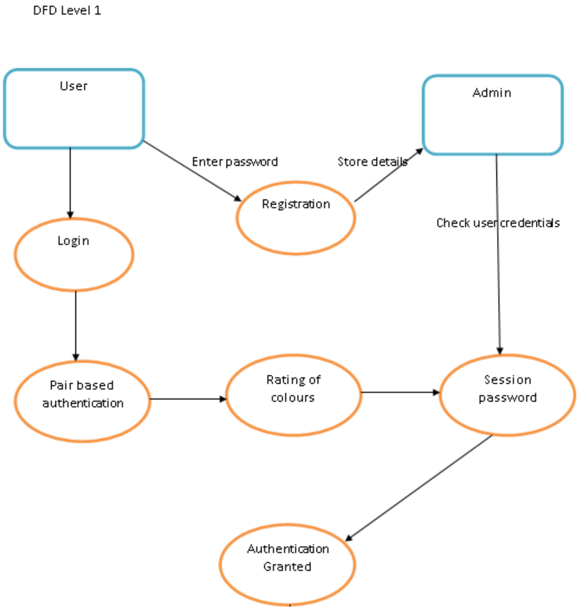
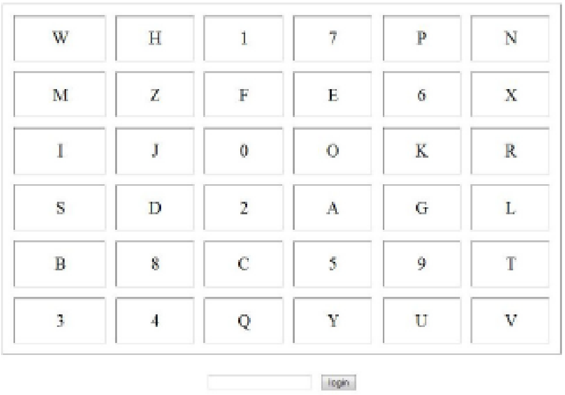


Fig 2: Data Flow Diagram

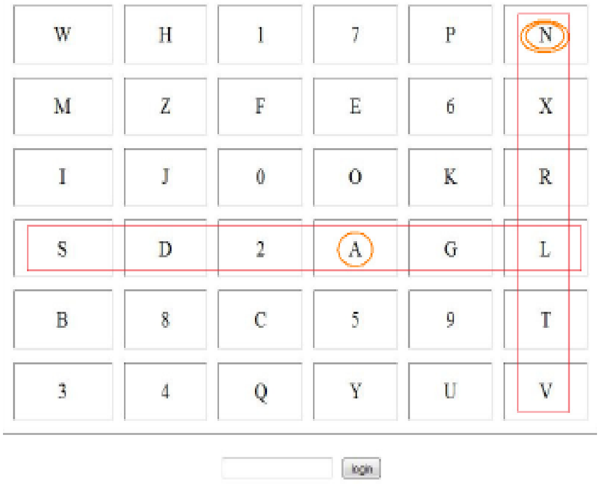
IV. METHODOLOGY

Pair-based Authentication scheme Module:



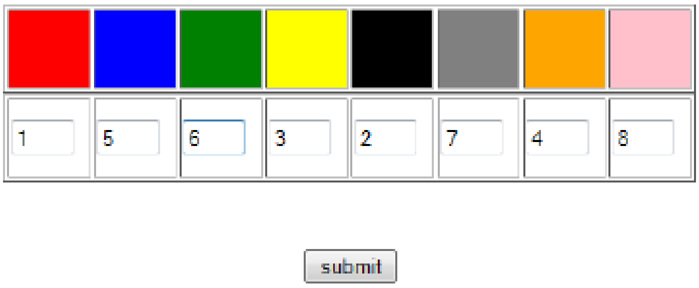
W	H	1	7	P	N
M	Z	F	E	6	X
I	J	0	O	K	R
S	D	2	A	G	L
B	8	C	5	9	T
3	4	Q	Y	U	V

During registration user submits his password. Maximum length of the password is 8 and it can be called as secret pass. The secret pass should contain even number of characters. Session passwords are generated based on this secret pass. During the login phase, when the user enters his username an interface consisting of a grid is displayed. The grid is of size 6 x 6 and it consists of alphabets and numbers. These are randomly placed on the grid and the interface changes every time. User has to enter the password depending upon the secret pass. User has to consider his secret pass in terms of pairs. The session password consists of alphabets and digits. The first letter in the pair is used to select the row and the second letter is used to select the column. The intersection letter is part of the session password. This is repeated for all pairs of secret pass.



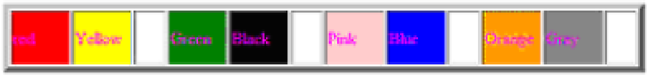
W	H	1	7	P	N
M	Z	F	E	6	X
I	J	0	O	K	R
S	D	2	A	G	L
B	8	C	5	9	T
3	4	Q	Y	U	V

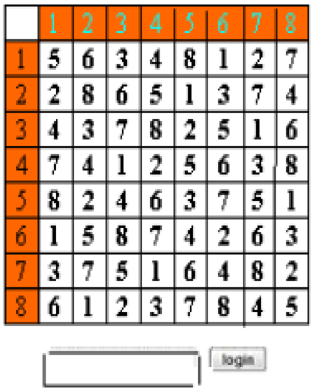
Hybrid Textual Authentication Scheme Module:



🟥	🟦	🟩	🟨	⬛	▨	🟧	▨
1	5	6	3	2	7	4	8

The User should rate colours from 1 to 8 and he can remember it as “RLYOBGIP”. Same rating can be given to different colours. During the login phase, when the user enters his username an interface is displayed based on the colours selected by the user. The login interface consists of grid of size 8×8. This grid contains digits 1-8 placed randomly in grid cells. The interface also contains strips of colours. The colour grid consists of 4 pairs of colours. Depending on the ratings given to colours, we get the session password.





	1	2	3	4	5	6	7	8
1	5	6	3	4	8	1	2	7
2	2	8	6	5	1	3	7	4
3	4	3	7	8	2	5	1	6
4	7	4	1	2	5	6	3	8
5	8	2	4	6	3	7	5	1
6	1	5	8	7	4	2	6	3
7	3	7	5	1	6	4	8	2
8	6	1	2	3	7	8	4	5

Registration Module:

This module is used to registered user Details in three parts. They are Name authentication password, Color Priority Password and Other details. First, user is going to enter the normal password but it using capital A-Z letters and 0-9 Numbers. Second the user to put the colour priority in six colours.

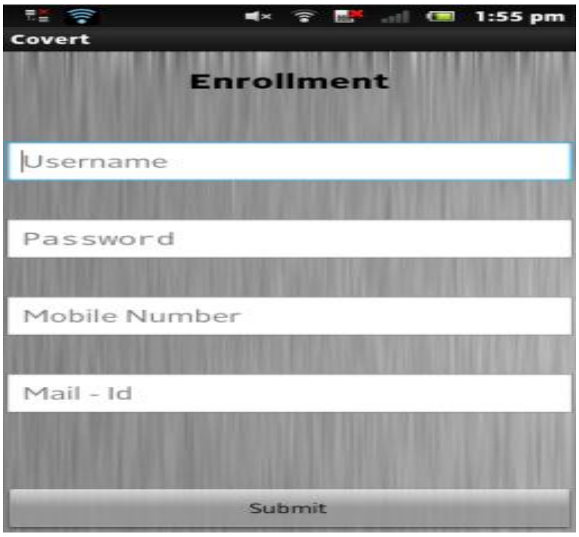
Authentication and services:

Once the user entered the pattern is manipulated and a PIN is identified, it will check with the local database provided by android operating system using SQL Lite. This process is to prevent unwanted server end process handling playful requests

Mobile Application in Transaction:

Step1. The application can be downloaded from mobile store entering user’s IP address. Application screen will appear.

Step2. Once user touch the screen, he/she need to signup new account registration and fill all the details given in the enrollment.If he is having an account user will login .



Step 3. Password is verified for service using grid and colour matrix method.

V. CONCLUSION

In this paper, by analysing the existing password entry methods under the new framework, password entry methods given a new guideline. This method provides an advanced security against human shoulder surfing attacks. Main aim of this paper is to resist a human shoulder surfing attack which is not supported by a recording device. Towards similarity in the task of perceptual grouping, this paper have grid and color matix. By using this method ,human shoulder surfing attack can be mitigated and establish a secure transaction between the mobile application and the server.

REFERENCES

[1] R. Dhamija, and A. Perrig. “Déjà Vu: A User Study Using Images for Authentication”. In 9th USENIX Security Symposium.

[2] Real User Corporation: Passfaces. www.passfaces.com

[3] Jermyn, I., Mayer A., Monrose, F., Reiter, M., and Rubin., “The design and analysis of graphical passwords” in Proceedings of USENIX Security Symposium, August 2016.

[4] A. F. Syukri, E. Okamoto, and M. Mambo, "A User Identification System Using Signature Written with Mouse," in Third Australasian Conference on Information Security and Privacy (ACISP): Springer- Verlag Lecture Notes in Computer Science (1438), 2016, pp. 403-441.

[5] G. E. Blonder, "Graphical passwords," in Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent, Ed. United States.

[6] Passlogix, site http://www.passlogix.com.

[7] HaichangGao, ZhongjieRen, Xiuling Chang, Xiyang Liu UweAickelin, “A New Graphical Password Scheme Resistant to Shoulder-Surfing

[8] S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, N. Memon, “Design and longitudinal evaluation of a graphical password system”. International J. of Human-Computer Studies 63 (2005) 102-127.

[9] W. Jansen, "Authenticating Mobile Device User through Image Selection," in Data Security, 2014.

[10] Mun-Kyu Lee, member, IEEE, “Security Notions And Advanced Method For Human Shoulder-Surfing Resistant PIN-entry”, vol. 9, no. 4, April 2014.

[11] Justin Weaver, Kenrick Mock, Bogdan Hoanca, “Gaze-based password authentication through automatic clustering of gaze points”, 2011 IEEE.

[12] Arash Habibi Lakhkari, Dr.Omar Bin Zakaria, Samaneh Farmand, Dr.Roslo Saleh, “Shoulder Surfing Attack in Graphical Password Authentication”IJCSIS , vol. 6, no. 2, 2009.

[13] Yoshiliro Kita, Fumio Sugai, MiRang Park, “Proposal and its Evaluation of a Shoulder-Surfing Attack Resistant Authentication Method: Secret Tap with Double Shift”, ISSN, 2013.

[14] Andrea Bianchi, Ian Oakley, Dong Soo Kwon, "Obfuscating Authentication Through Haptics,Sound and Light", CHI 2011, May 7-12, 2011,Vancouver.

[15] Yogesh Babu. B, Vishwanathan.G, "Implementing Black hole Password Entry Technique For Mitigating Shoulder-Surfing Threat", International Journal, vol.2, March 2014.

[16] Lim Kah Seng, Nora Fida Ithnin and Hazinath Kutty Mammi, "An Anti-Shoulder Surfing Mechanism and its Memorability Test", International Journal of security and its applications, vol.6, no.4, October 2012.

[17] Andrea Bianchi, Ian Oakley, Dong Soo Kwon, "The Phone Lock: Audio and Haptic Shoulder-Surfing Resistant PIN Entry Methods for Mobile Devices",TEI'11 Jan 2011.

[18] T.Kwon, S.Shin, S.Na, "Covert attentional shoulder-surfing: Human adversaries are more powerful than expected, IEEE Trans. System,Man cybern.System. pp. 1-12 to be published.

[19] T.Perkovic, M.Cagalj, and N.Rakic," SSSL: Shoulder Surfing Safe Login," in Proc. Int. Conf. Softw., Telecommun. Computer Netw, 2009, pp. 270-275.

[20] Q.Yan, J.Han, Y.Li,J.Zhou, and R.H.Deng, "Designing leakage-resilient password entry on touchscreen mobile devices," in Proc. ASIACCS, 2013, pp. 37-48.:

[21] C. S. Kim and M. K. Lee, "Secure and user friendly PIN entry method," in Proc, 28th Int. Conf. Consum.Electron., 2010, p.5.1-1