ISSN [Online]: 2583-2654

A Graphical Pin Entry System with Shoulder Surfing Resistance

Shalini.G[1]*, Bhavana PG*[2]*, Hemalatha.S*[3] *and Kavyashree.S*[4]

[1]*Department of computer science and engineering, Dr.TTIT,kgf*
[2]*Department of computer science and engineering, Dr.TTIT,kgf*
[3]*Department of computer science and engineering, Dr.TTIT,kgf*
[4]*Department of computer science and engineering, Dr.TTIT,kgf*

Abstract: Personal identification number or PIN based authentication systems are most commonly used authentication systems. Due to maturity and simplicity, these authentication systems are vastly deployed in many different areas such as point of sale (POS), electronic door access system and in different kinds of mobile applications.However, due to limited password space and small password length, they are highly susceptible to different kinds of shouldersurfing attacks. In this paper, we have proposed a graphical PIN entry scheme that provides resistance against shoulder surfing attacks. To alleviate the shoulder surfing attack in our proposed scheme, we have used specialized interface design and indirect PIN entry method. For indirect PIN entry method we have usedextra information in the form of reference location, which is not observable for the attacker. The results of the user study show that this scheme provides a reasonable balance between security and usability.

Keywords:Authentication,Personal dentification number, Shoulder surfing

I. INTRODUCTION

There are numerous authentication schemes used to authenticate users for different purposes. our focus is on personal identification number (PIN) based authentica- tion schemes. PIN based authentication systems are widely deployed authentication systems [1].

The vast acceptance or usability of PIN based passwords is highly dependent on its simplicity and maturity. They are simple because they havea limited set of password space, only digits from 0 to 9. The password length is also small usually 4 to 6 digits long. Because of limited set of password space and shorter password length, error rate is also low [2].

Different kinds of PIN entry schemes are vulnerable to different types of attacks such as random guessing attack [3] and shoulder surfing attack.

In order to minimize the threat of brute force attack the number of attempts for unsuccessful login may be restricted to a minimum numbersuch as 3, 4 or 5. However the shoulder surfing attack is still considered to be a big challenge for different authentication schemes.

[4] Shoulder surfing is a social engineering technique looking overthe victim's shoulder.

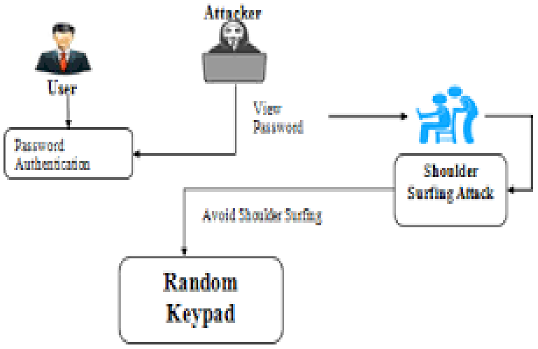


Fig 1

A very common example of shoulder surfing attack is a person standing directly behind a personin a queue of an ATM machine. He can easily look over the shoulder of a person to steal his PIN or password. [5] This situation is also true in case of someone entering his PIN or password while unlocking his mobile phone in a crowded subway or public place. The hidden cameras and surveillance devices may also aid a shoulder surfer in stealing the PIN or password of a user.

we have proposed a new graphical PIN entryscheme that provides resistance against human shoulder surfing we have tried to alleviate shoulder surfing attack [7] through a specialized sign of user interface and indirect pin entry method.

We have developed a prototype of our proposed scheme and performed a user studyto establish that our scheme provides a reasonable balance between security and usability [8].

II. SHOULDER SURFING

Shoulder surfing is a type of social engineering technique used to obtain information such as passwords and other confidential data by looking over the victim's shoulder. Unauthorized users watch the keystrokes inputted on a device or listen to sensitive information being spoken, which is also known as eavesdropping [10].

A PIN based entry method which is resistant gainst shoulder surfing attack to a limited extent.

Image-based passwords were proved to be easier to recollect in several user studies. As a result, users can set up a complex authentication password and are capable of recollecting it after a long time even if the memory is not activated periodically. However, most of these image-based passwords are vulnerable to shoulder surfing attacks (SSAs). This type of attack either uses direct observation, such as watching over someone’s shoulder or applies video capturing techniques to get passwords, PINs, or other sensitive personal information.

There are numerous authentication schemes used to authenticate users for different purposes. In this paper, our focus is on personal identification number (PIN) based authentication schemes. PIN based authentication systems are widely deployed authentication systems [1]. The vast acceptance or usability of PIN based passwords is highly dependent on its simplicity and maturity. They are simple because they have a limited set of password space, only digits from 0 to 9. The password length is also small usually 4 to 6 digits long. Because of limited set of password space and shorter password length, error rate is also low.

III. LITERATURE REVIEW

1. Graphical Password Authentication: Cloud Securing Scheme

Graphical password is one of the alternative solutions to alphanumeric password as it is very tedious process to remember alphanumeric password. When any application is provided with user friendly authentication it becomes easy to access and use that application. One of the major reasons behind this method is according to psychological studies human mind can easily remember images than alphabets or digits. In this paper we are representing the authentication given to cloud by using graphical password. We have proposed cloud with graphical security by means of image password. We are providing one of the algorithms which are based on selection of username and images as a password. By this paper we are trying to give set of images on the basis of alphabet series position of characters in username. Finally, cloud is provided with this graphical password authentication.

2. *Paivio, T. Rogers, and P. Smythe, “Why are pictures easier to recall than words?” Psychonomic Science, 1968.*

Pictures of objects were recalled significantly better than their names on the first two of four free recall trials. Recall for the two modes did not differ in intertrial organization but striking differences occurred as a function of input serial order. Picture superiority occurred for terminal input items on Trial 1, and both terminal and early items on Trial 2. The findings are discussed in terms of verbal and nonverbal (concrete) memory codes

3. 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.

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 attentional shoulder surfing indeed can break the well-known PIN entry method previously evaluated to be secure against shoulder surfing. Another contribution in this paper is the formal modeling approach by adapting the predictive human performance modeling tool for security analysis and improvement. We also devise a defense technique in the modeling paradigm to deteriorate severely the perceptual performance of the adversaries while preserving that of the user. To the best of our knowledge,

this is the first work to model and defend the new form of attack through human performance modeling. Real attack experiments and user studies are also conducted.

4. S3PAS:A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme

The vulnerabilities of the textual password have been well known. Users tend to pick short passwords or passwords that are easy to remember, which makes the passwords vulnerable for attackers to break. Furthermore, textual password is vulnerable to shoulder-surfing, hidden camera and spyware attacks. Graphical password schemes have been proposed as a possible alternative to text-based scheme. However, they are mostly vulnerable to shoulder surfing. In this paper, we propose a Scalable Shoulder Surfing Resistant Textual-Graphical Password Authentication Scheme (S3PAS).

S3PAS seamlessly integrates both graphical and textual password schemes and provides nearly perfect resistant to shoulder-surfing, hidden-camera and spyware attacks. It can replace or coexist with conventional textual password systems without changing existing user password profiles. Moreover, it is immune to brute-force attacks through dynamic and volatile session passwords. S3PAS shows significant potential bridging the gap between conventional textual password and graphical password. Further enhancements of S3PAS scheme are proposed and briefly discussed. Theoretical analysis of the security level using S3PAS is also investigated.

5. Fake Pointer: An Authentication Scheme for Improving Security against Peeping Attacks Using Video Cameras

Peeping attacks in the real world are a threat to user authentication. What is worse, an emerging attack method such as video capture makes traditional measures against peeping attack insufficient. This paper presents a unique user authentication scheme named "fake Pointer" as a solution to peeping attacks conducted by video capture. It makes it difficult for attackers to obtain a secret even if someone captures an authentication scene using a video camera.

The fake Pointer has two unique features to ensure security against such a peeping attack. One is that fake Pointer provides a double-layered interface for a secret input. This interface makes it difficult for attackers to identify a legitimate user's secret even if they have a video record showing a target user's authentication action. The other feature is that fake Pointer uses two secrets: a fixed secret and a disposable secret. This feature enables change of a secret input operation in each authentication, which is also a necessary feature for ensuring security. This feature makes it difficult to extract a secret by statistical inference even if an attacker has many video records of the same user.

IV. SYSTEM REQUIREMENTS

1) User has to register themselves by giving all the information about their details when user click on register button this system will get registered
2) User can able to login by giving user id and password once login success user will get home page else validation message will show to user login page itself.
3) User need to select the locations on the image while getting the registration.
4) User should remember this password, should been necessary while getting logged in always
5) At the time of login, OTA will be generated to the mail. Using the OTA user needs to get logged in.
6)

V. METHODOLOGY

In this method user has to register by giving his information such as userid, user name, password, valid

e- mail id etc, and after giving this information, randomly three images will be assigned to the user, in those images he has to select the coordinate squares of the images as the graphical password. The details of coordinates of all images will be stored in the database with respect to the specific user.
After successful setting of the coordinates of the images, those details will be stored in the database, concatenating all the three images coordinates and generate hash code for that and store in the database with respect to the user.
Registered user will be login to the application by using his userid and password, if the userid and password is valid One Time Password (OTP) will be sent to the user's e- mail, whereas OTP contains the random pair of vertical and horizontal slider coordinate points of all the three images. After successful login, three assigned images will be displayed to the user with horizontal and vertical sliders, user has to set the horizontal and vertical sliders for all the three images, where the OTP coordinate value should be equal to the coordinates chosen by the user at the time of password setting. The hash code will be generated for all OTP coordinates by concatenating. if the hash code is matched with the existing hash code user can successful enter in to the home page, else, process ends and login page will display.

I. *MD-5 ALGORITHM*

Step1: Append Padding Bits

1) Padding means adding extra bits to the original message. So in MD5 original message is padded such that its length in bits is congruent to 448 modulo 512. Padding is done such that the total bits are 64 less, being a multiple of 512 bits length.

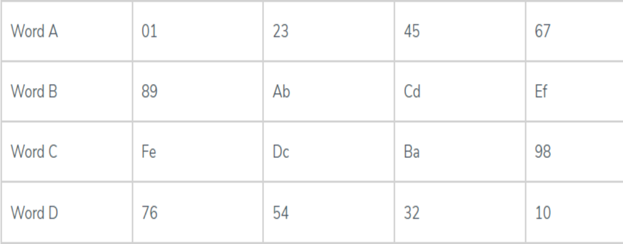
2) Padding is done even if the length of the original message is already congruent to 448 modulo 512. In padding bits, the only first bit is 1, and the rest of the bits are 0.

Step 2: Append Length

After padding, 64 bits are inserted at the end, which is used to record the original input length. Modulo 2^64. At this point, the resulting message has a length multiple of 512 bits.

Step 3: Initialize MD buffer.

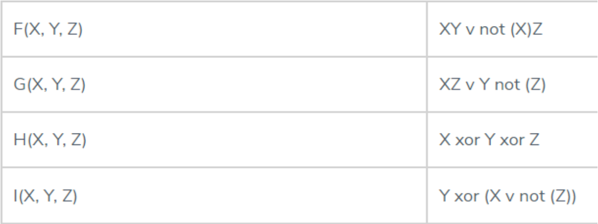
A four-word buffer (A, B, C, D) is used to compute the values for the message digest. Here A, B, C, D are 32-bit registers and are initialized in the following way



Word A	01	23	45	67
Word B	89	Ab	Cd	Ef
Word C	Fe	Dc	Ba	98
Word D	76	54	32	10

Step 4: Processing message in 16-word block

MD5 uses the auxiliary functions, which take the input as three 32-bit numbers and produce 32-bit output. These functions use logical operators like OR, XOR, NOR.



F(X, Y, Z)	XY v not (X)Z
G(X, Y, Z)	XZ v Y not (Z)
H(X, Y, Z)	X xor Y xor Z
I(X, Y, Z)	Y xor (X v not (Z))

The content of four buffers are mixed with the input using this auxiliary buffer, and 16 rounds are performed using 16 basic operations.

Output-

After all, rounds have performed, the buffer A, B, C, D contains the MD5 output starting with lower bit A and ending with higher bit D.

5.I.1 PASS MATRIX FOR LOGIN AUTHENTICATION

PassMatrix's authentication consists of a registration phase and an authentication phase as described below:

Registration phase Figure 2 is the flowchart of the registration phase. At this stage, the user creates an account which contains a user-name and a password. The password consists of only one pass-square per image for a sequence of n images. The number of images (i.e., n) is decided by the user after considering the trade-off between security and usability of the system [42]. The only purpose of the username is to give the user an imagination of having a personal account. The username can be omitted if Pass Matrix is applied to authentication systems like screen lock. The user can either choose images from a provided list or upload images from their device as pass-images. Then the user will pick a pass-square for each selected pass- image from the grid, which was divided by the image discretization module. The user repeats this step until the password is set.

Authentication phase Figure 3 is the flowchart of the authentication phase. At this stage, the user uses his/her username, password and login indicators to log into Pass Matrix. The following describes all the steps in detail: 1) The user inputs his/her username which was created in the registration phase.

2) A new indicator comprised of a letter and a number is created by the login indicator generator module. The indicator will be shown when the user uses

OVERVIEW

Pass Matrix is composed of the following components:

Fig 2 (Please see page 65)

Fig 3 (Please see page 65)

VI. CONCLUSION

In this work, we have developed a PIN based authentication system that is resilient against shoulder surfing attack. Our authentication scheme is resistant against naked eye-based shoulder surfing attack as well as recording based shoulder surfing attack, provided the attacker has only one video recording of a successful authentication process. To accomplish this objective, we have used a specialized interface design and indirect pin entry method. The security analysis also shows that our scheme provide resistance not only against human shoulder surfing attack but also against recording-based shoulder surfing attack without compromising the security against random guessing attack. Furthermore, we have conducted a user study to check the usability of our scheme. The results of our usability study show that the minimum average time required for login is 22 seconds and average error percentage is 8.8%. By looking at the results of security and usability study, we can conclude that our proposed scheme provides a reasonable balance between security and usability.

Acknowledgement

This work was supported by National Natural Science Jiangsu Province Natural Science Foundation.

REFERENCES

[1] J. Bonneau, C. Herley, P. C. v. Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," in 2012 IEEE Symposium on Security and Privacy, May 2012, pp. 553–567.

[2] M. Harbach, A. De Luca, and S. Egelman, "The anatomy of smartphone unlocking: A field study of android lock screens," in Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, ser. CHI '16. New York, NY, USA: ACM, 2016, pp. 4806–4817.

[3] J. Bonneau, S. Preibusch, and R. Anderson, "A birthday present every eleven wallets? the security of customer- chosen banking pins," in Financial Cryptography and Data Security, A. D. Keromytis, Ed. Berlin, Heidelberg: Springer

Berlin Heidelberg, 2012, pp. 25–40.

[4] M. Harbach, E. Von Zezschwitz, A. Fichtner, A. De Luca, and M. Smith, "It's a hard lock life: A field study of smartphone (un)locking behavior and risk perception," in Proceedings of the Tenth USENIX Conference on Usable Privacy and Security, ser. SOUPS'14. Berkeley, CA, USA: USENIX Association, 2014, pp. 213–230.

[5] 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.

[6] M. Lee, "Security notions and advanced method for human shouldersurfing resistant pin-entry," IEEE Transactions on Information Forensics and Security, vol. 9, no. 4, pp. 695–708, April 2014.

[7] A. Bianchi, I. Oakley, V. Kostakos, and D. S. Kwon, "The phone lock: Audio and haptic shoulder-surfing resistant pin entry methods for mobile devices," in Proceedings of the Fifth International Conference on Tangible, Embedded, and Embodied Interaction, ser. TEI '11. New York, NY, USA: ACM, 2011, pp. 197–200.

[8] A. Bianchi, I. Oakley, and D. S. Kwon, "Counting clicks and beeps: Exploring numerosity based haptic and audio pinentry," Interact. Comput., vol. 24, no. 5, pp. 409–422, Sep. 2012.

[9] R. Kuber and W. Yu, "Tactile vs graphical authentication," in Haptics: Generating and Perceiving Tangible Sensations, A. M. L. Kappers, J. B. F. van Erp, W.

M. Bergmann Tiest, and F. C. T. van der Helm, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 314–319.

[10] H. Sasamoto, N. Christin, and E. Hayashi, "Undercover: Authentication usable in front of prying eyes," in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ser. CHI '08. New York, NY, USA: ACM, 2008, pp. 183–192.

[11] A. De Luca, E. von Zezschwitz, and H. Hussmann, "Vibrapass: Secure authentication based on shared lies," in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ser. CHI '09. New York, NY, USA: ACM, 2009, pp. 913–916.

[12] A. Bianchi, I. Oakley, J. K. Lee, and D. S. Kwon, "The haptic wheel: Design & evaluation of a tactile password system," in CHI '10 Extended Abstracts on Human Factors in Computing Systems, ser. CHI EA '10. New York, NY, USA: ACM, 2010, pp. 3625–3630.

[13] T. Matsumoto and H. Imai, "Human identification through insecure channel," in Advances in Cryptology — EUROCRYPT '91, D. W. Davies, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1991, pp. 409–421.

[14] V. Roth, K. Richter, and R. Freidinger, "A pin-entry method resilient against shoulder surfing," in Proceedings of the 11th ACM Conference on Computer and Communications Security, ser. CCS '04. New York, NY, USA: ACM, 2004, pp. 236–245. [15] P. Shi, B. Zhu, andA.

M. Youssef, "A rotary pin entry scheme resilient to shoulder-surfing," 2009 International Conference for Internet Technology and Secured Transactions, (ICITST), pp. 1–7, 2009.

[16] T. Kwon and S. Na, "Steganopin: Two-faced human- machine interface for practical enforcement of pin entry security," IEEE Transactions on Human-Machine Systems, vol. 46, no. 1, pp. 143–150, Feb 2016.

[17] A. Papadopoulos, T. Nguyen, E. Durmus, and N. Memon, "Illusionpin: Shoulder-surfing resistant authentication using hybrid images," IEEE Transactions on Information Forensics and Security, vol. 12, no. 12, pp. 2875–2889, Dec 2017.

Fig 2: The flowchart of registration phase in Pass Matrix.

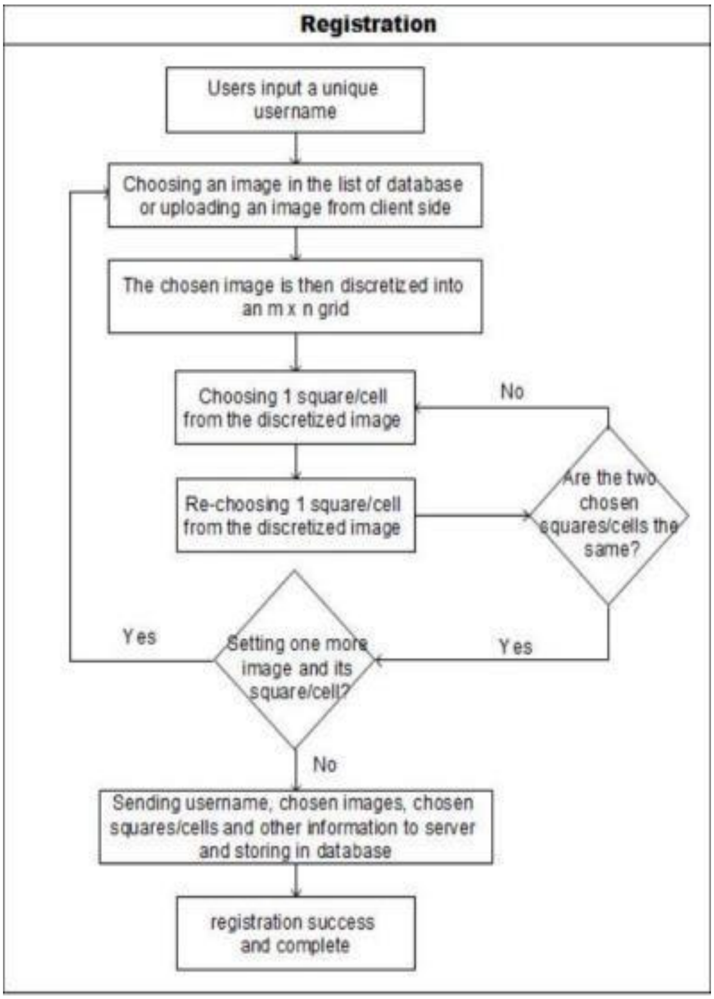
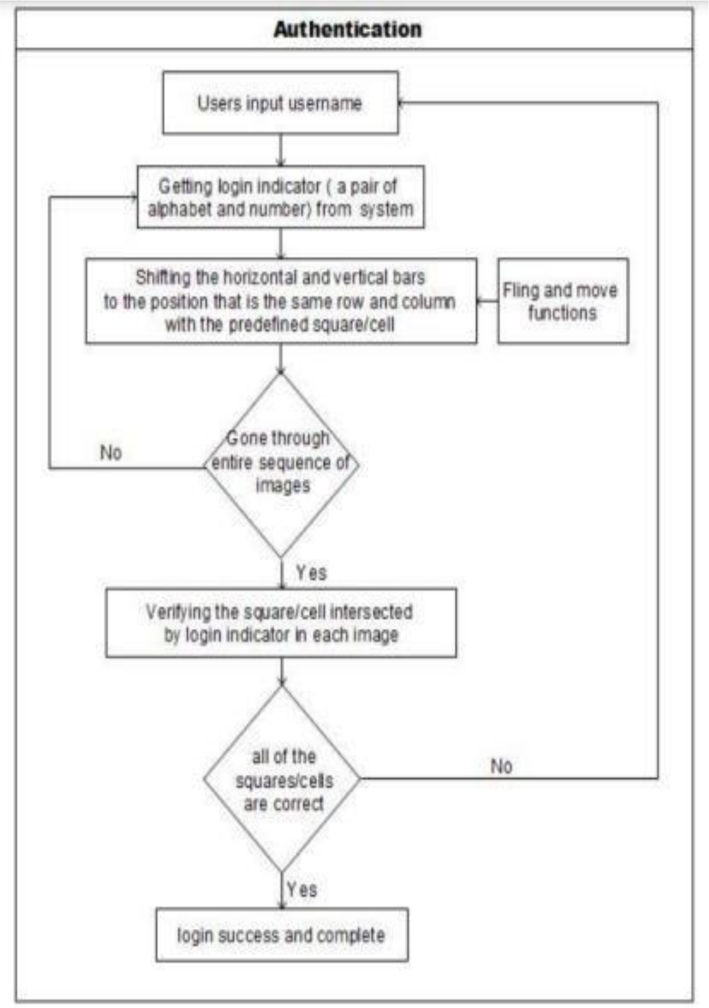

Registration
Users input a unique username
Choosing an image in the list of database or uploading an image from client side
The chosen image is then discretized into an m x n grid
Choosing 1 square/cell from the discretized image
No
Re-choosing 1 square/cell from the discretized image
Are the two chosen squares/cells the same?
Yes
Yes
Setting one more image and its square/cell?
No
Sending username, chosen images, chosen squares/cells and other information to server and storing in database
registration success and complete

Fig 3: The flowchart of authentication phase in Pass Matrix


Authentication
Users input username
Getting login indicator (a pair of alphabet and number) from system
Shifting the horizontal and vertical bars to the position that is the same row and column with the predefined square/cell
Fling and move functions
No
Gone through entire sequence of images
Yes
Verifying the square/cell intersected by login indicator in each image
all of the squares/cells are correct
No
Yes
login success and complete

.