A SURVEY ON IMPROVEMENT OF A PIN-ENTRYMETHOD RESILIENT TO SHOULDER-SURFING ANDRECORDING ATTACKS

MAYUR SHINDE[1], ADITYA KULKARNI[2], HRUSHIKESH DOLAS[3] ,PALLAVI TEKE[4]

[1] Dept. of Computer Engineering, Sinhgad Institute of Technology, Lonavala , Savitribai Phule Pune University
[2] Dept. of Computer Engineering, Sinhgad Institute of Technology, Lonavala ,Savitribai Phule Pune University
[3] Dept. of Computer Engineering, Sinhgad Institute of Technology, Lonavala ,Savitribai Phule Pune University
[4] Dept. of Computer Engineering, Sinhgad Institute of Technology, Lonavala ,Savitribai Phule Pune University

ABSTRACT : *Personal identification numbers (PINs) are obtained by shoulder surfing, through the use of mirrors or concealed miniature cameras. Both elements, the PIN and the card, are generally sufficient to give the criminal full access to the victim's account. In this paper, we surveyed on present alternative PIN entry methods to which we provide the security against shoulder surfing and Recording attacks. These methods make it significantly harder for a criminal to obtain PINs even if he fully observes the entire input and output of a PIN entry procedure. We also surveyed on introducing the idea of probabilistic cognitive trapdoor games, which offer resilience to shoulder surfing even if the criminal records a PIN entry procedure with a camera. We studied the security as well as the usability of used methods, the results of which we also present in the paper.*

Keywords -PIN, Password, Shoulder Surfing, ATM, Cognitive Trapdoor Games, User Authentication, Shoulder Surfing Attack, Personal Identification Number, And Session Key.

I. INTRODUCTION

THIS 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 the use of PINs because there are many cases in which PINs are used in public places and for financial transactions.

When a user enters a personal identification number(PIN) as a numeric password in mobile or stationary systems, including smart phones, tablet computers, automated teller machines (ATM), and point of sale (PoS) terminals, a direct observation attack based on shoulder surfing becomes great concern. The PIN entry can be observed by nearby adversaries, more effectively in a crowded place. Since the same PIN is usually chosen by a user for various purposes and used repeatedly, a compromise of the PIN may cause the user a great risk. To cope with this problem, which is between the user and the system, cryptographic prevention techniques are hardly applicable because human users are limited in their capacity to process information. Instead, there have been alternative approaches considering the asymmetry between the user and the system.[1] Among them, the PIN entry was elegant because of its simplicity and intuitiveness: in each round, a regular numeric keypad is colored at random, half of the keys in black and the other half in white, which we will call the BW method.

A user who knows the correct PIN digit can answer its color by pressing the separate color key below. The basic BW method is aimed to resist a human shoulder surfing attack, not supported by a recording device, while its probabilistic extension considers a recording attack in part. The BW method is still considered to be secure against human adversaries due to the limited cognitive capabilities of humans. So our aim of this project is to prevent human shoulder surfing attack and to establish a secure transaction between the mobile App and Server by implementing the improved BW method. Our survey is on implementation of BW method and IBW methods are as follows which is done by Perceptual Grouping and Covert Attention.

II. PREVIOUS METHODS

Syukri designed a scheme in which authentication is carried out by sketching out the user signature with mouse. This scheme involves two levels, registration and verification. While registering, the user draws his signature using mouse, the system then extracts the signature area. During the verification level, it acquires the user signature as input, performs normalization and finally extracts the parameters of the signature. But this scheme is associated with several disadvantages such as forgery of signatures, inconvenience while drawing with mouse, difficulty in sketching the signature in the same perimeters at the time of registration. Besides this, a new graphical authentication method has been designed by *Dhamija* and *Perrig***.** This method, while creating the password allows the user to select certain number of pictures from a set of random images. Then during login, the user has to recognize the preselected portraits from the set of images. But this method is liable to shoulder-surfing.

Zhao and Li proposed a shoulder-surfing resistant scheme "S3PAS". [9] In this make different combinations of password. Select approximate middle symbol of invisible triangle as a password. It provides higher security. [3]

But selection of middle symbol in large triangle is difficult. *Jermyn, et al*. introduced a technique called "Draw a Secret". In this password technique user draw a picture as a password which is similar to registered password. For authentication picture draw on same grids in same order. It is vulnerable shoulder surfing. Drawing password is very difficult task. *Passface* is an approach proposed by the Real User Corporation in which the user is allowed to choose four images of human faces from the face database as their password. During the verification phase, the user is provided with a grid of nine faces, one already chosen during the registration and eight decoy faces. The user identifies the selected face and clicks anywhere over it. This course of action is repeated for four times, and the user is ascertained as genuine if he recognizes all faces accurately. A new innovative authentication scheme is proposed by Jansen for mobile devices. While creating the password, the user chooses a theme of snapshots in thumbnail size and the sequence of those snapshots is fixed as password. As each of the thumbnail is associated with numerical value, the sequence of images form numerical password. The only drawback with this method is that the password space is not large, as no of images is limited to 30. To overcome shoulder-surfing challenge, many methods have been proposed. One of such technique is designed by Man, et al. In this system, the user selects many portraits as the pass objects. Each pass object is allotted an inimitable code. During the verification process, the user has to input those unique codes of the pass objects in the login interfaces presented by the system. Though the scheme resists the hidden camera, the user has to memorize all pass object codes. In this way, many other graphical authentication schemes and their drawbacks are presented in a latest survey paper.

III. SECURITY NOTIONS FOR PIN-ENTRY METHODS

Guessing Attack (GA)

In a guessing attack (GA), the attacker guesses a user's PIN and inputs it to pass the test. A smart attacker might use the fact that the distributions of PINs and passwords are not uniform. However, to simplify analysis, we make an idealized assumption that the distribution of PINs is uniform. We also have to take into account that the user (and the attacker) may be allowed to fail several times until s/he inputs the correct PIN. For example, a typical ATM permits three trials. Therefore, we give the following definition for the security of a PIN-entry method against a guessing attack. [2]

Shoulder Surfing Attack (SSA)

In a shoulder-surfing attack (SSA), the attacker observes the logon procedure by looking over the user's shoulder, and tries to recover that user's PIN. This SSA is most familiar in many of the common places. One best example is shoulder surfing attack during PIN entry at ATMs. The SSA may be done directly through the human eyes or by using any electronic devices such as fixing a skimmer device or miniature cameras at ATMs. [7]

Human Shoulder Surfing Attack (HSSA)

The HSSA is one of the types of SSA. A shoulder-surfing attack without any recording device or an electronic device is commonly known as a human shoulder-surfing attack (HSSA) .This attack is mainly performed by a human by looking over the shoulder of another person to know his logon procedures and PIN. The HSSA is mainly performed by looking at the PIN during the entry process and trying to recollect it later. In these recent years, the human adversaries had become more powerful to recollect the PIN that was shoulder surfed. [9]

Recording Attack (RA)

The recording attack (RA) is a type of SSA where the human adversaries use a skimming device or miniature cameras to record the session and hack the PIN or any data of the user. Small cameras are fixed by the human adversaries to record the particular session such as PIN entry session, and then collect the data needed by playing the videos even from the remote system. Such type of attacks is of great concern at ATM.

IV. SECURITY EVALUATION

Here we stated some security evaluations that are pressed (leaves) and the number of PIN digits (clovers) already entered.

Modeling-based Analysis

As we discussed in Section V-A, the improved method was modeled and analyzed in CPM-GOMS during the design phase. Note that x = 700 and y = 100, only 100 MS more than the BW method and obviously not enough for perceiving four perceptual groups that look overlapping. Due to the step of $a, b, c, d \leftarrow \rho(P)$ in the algorithm, four colors are shuffled at random in every round; a particular color is not more likely to be assigned (for example, to *a*) and entered. We conclude that covert attentional shoulder surfing is infeasible against the improved method based on this analysis.

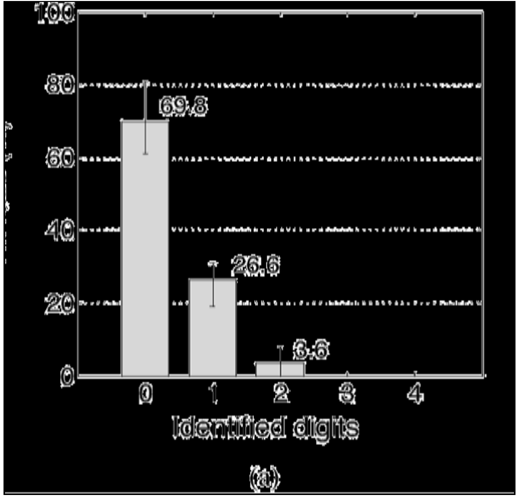

Figure 1 Average hit ratio over five days as a function of number of identified PIN digits

V. ANALYSIS OF BLACK AND WHITE METHOD

Although the BW scheme was evaluated to be resilient against practical attacks our survey of the method will reveal various concerns about its security and reliability. [4]

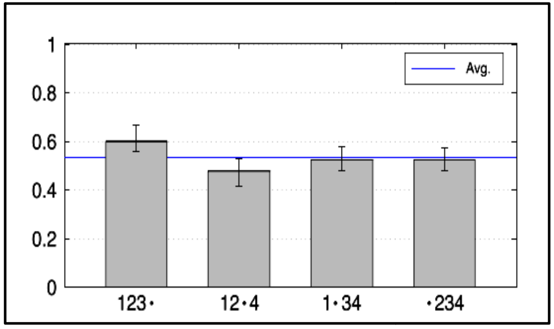

Figure 2 Experimentally obtained round redundancies of the IOC BW method.

The height of each bar gives the redundancy rate for the round marked with a dot.

We surveyed the fact that perceiving the black and white keypad separations as visual patterns, in contrast to attending to the explicit digits, was sufficient in singling out the key digit and demonstrated that the BW method could be defeated in practice. Also we further investigate the security of the BW method, both experimentally and theoretically, covering not just the BW method, but also the DOC BW method and the RR variants. The list of concerns to be discussed includes round redundancy, unbalanced key presses, frequent system errors from ambiguity, and recording non-resilience.

A. Round Redundancy

The BW scheme specifies for $4= [log_2\ 10]$ rounds to be executed for every PIN digit. However, since $[\log_2 10] = 3.32$is much closer to 3 than 4, one of the four rounds that are used to enter each PIN digit could quite often be redundant.

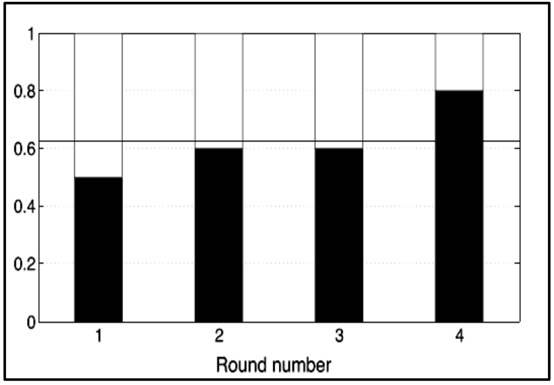

Figure 3 Experimentally obtain ratios of black and white button presses for the IOC BW scheme

B. Unbalanced Color Selection Frequencies

The BW scheme specified the colors to be given to each of the two 5-digit sets, after each regrouping of the digit space into two new halves. We conducted an experiment to test whether the black (B) and white (W) inputs from the users would be equally likely.

C. Digit Identification Failures in the DOC BW Method

The DOC version of the BW method was devised to prevent the user from inadvertently exposing the black and white patterns for too long. However, this version requires higher mental effort from the user, such as remembering a sequence of colors. It was estimated that the mean probability of user errors would be 0.2 for the DOC BW method, which is higher than the 0.09 expected of the IOC BW method.

D. Inadequate Recording Resilience

The RR variant of the BW method attempts to provide security against adversaries that are equipped with camera-based recording devices. The approach was to remove one round from the 4-round process required for each PIN digit entry. This creates ambiguity in the PIN digits to the observer (and to the PIN entry system), and the adversary is forced to guess the correct 4-digit PIN from a pool of possible PINs.

E. Comments on Other BW Configurations

Recall that the original BW PIN entry method allowed for flexibility in the PIN character set to be used and in the length of the PINs. We had focused on just the 4-digit PIN configuration, because practical interest in this case greatly overwhelms those in all other cases. Furthermore, it is rather straightforward and easy to extend our results to the cases of decimal digit PINs of lengths other than 4. However, analyzing the BW method that utilizes a character set of size other than 10, which might still be of interest for certain applications, will require further work.

VI. PROPOSED APPROACH

Goals and Design Policy

We propose a shoulder-surfing-attack-resistant authentication method that uses icons and a touch panel liquid crystal display. This authentication method is named “Secret Tap method. The goals and design policy are described as follows:

Covert observation resistance

Maintain the resistance strength at a level that prevents the authentication information from being revealed to other individuals, even if the authentication operation is performed numerous times.

Recording attack resistance

Maintain the resistance strength at a level that prevents the authentication information from being analyzed by other individuals even if the authentication operation is fully recorded.

Brute-force attack resistance

Maintain the resistance strength at a level that prevents the authentication process from broken more easily than by a brute-force attack on a four digit PIN. This policy follows the standard put forth in ISO 9564-1.

Usability

Maintain a level of usability that permits operators to perform the authentication operation with ease.

VII. PROPOSED SYSTEM

We have seen different methods to preventing Shoulder Surfing attacks as well as Video Recording attacks. These techniques are good to prevent the attacks. But some techniques require more steps and memory to enter a 4 digit pin. Graphical passwords have their own disadvantages.[6] Complicated passwords are difficult to remember. For this, we propose new technique i.e. Black & White method. In each round, a regular numeric keypad is coloured at random, half of the keys in black and the other half in white. The user is required to answer the present colour of the PIN digit key immediately by pressing a separate colour-indication key below the keypad. For example if the pin 1 is in White colour, then user needs to press White key present below to the key pad. BW method executes 4 rounds to enter single digit pin. That means total 16 rounds are carried out to enter 4-digit pin. The diagram shows the working of Black & White method to enter single of pin.

In the Fig No 4. the digit 1 is inserted by performing 4 cycles. After doing this, 1 is added in matrix. Similarly 4 digits of pin are entered in matrix by applying same technique & then further process of authentication starts. Although it takes more steps to enter pin, but it takes less memory to execute & also it is easy to carry out by user

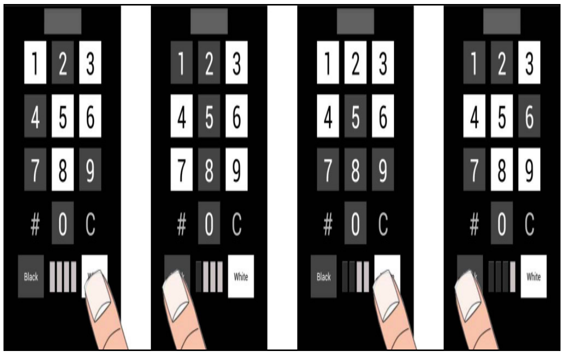

Figure 4 Digit 1 is inserted by performing 4 cycles

.

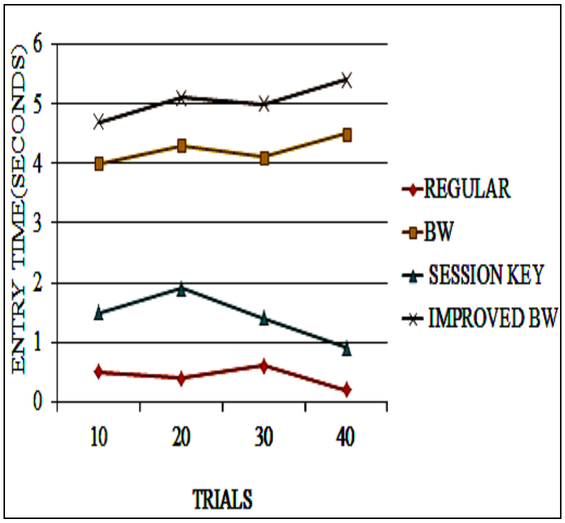

Figure 5 The graph for the comparison of PIN-entry Methods

This method shows that, even a well-trained human adversary may find it difficult to guess the PIN number even if they record the PIN entry session. As this method uses more than two colors (i.e. four colors), the PIN entry method is made protectable and entertain able for the users. This requiresan inference with better optimization techniques, which can for example; reduce entry time taken by the user that may further improve the classification accuracy.

The covert attentional shoulder surfing proposed in this paper is to the knowledge the first sophisticated counter attack of humans against the system, Previously evaluated to be secure. In addition to this, the methods which are explained in the existing system (such as black white method and session key method) is also implemented in order to find a better statistics to show that the proposed method is the more secure and the safety method. The experimental results of the existing BW method and the proposed IBW method are shown in the form of graph

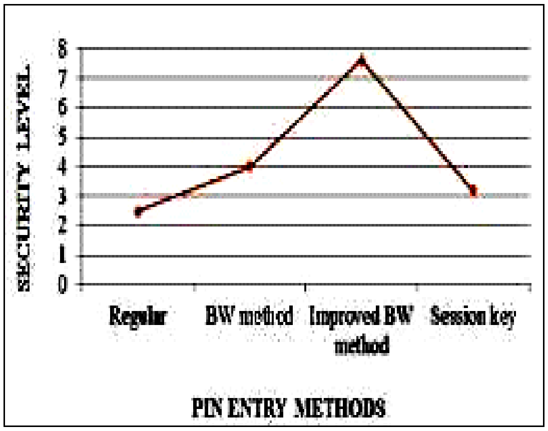

Figure 6 The graph for defining the security level of PIN entry methods

VIII. FUTURE SCOPE

Many forms of future enhancements can be done to this system. It is possible to upgrade the application and can make it adaptable to all environments. This may be done based on the optimization methods where feasibility and the number of roundstaken for the PIN entry method can be minimized. It is also based on the OOD (object- oriented design) concept. So, any further changes can be easily adaptable. Based upon the arising security issues, thesecurity of this application can be improved using latest and emerging technologies. This also includes the adaption of the selection bias in the future process.

In India, this authentication scheme is not used in any net banking application. So the banks can adopt this authentication scheme for improving their security.

Besides, this scheme can be used in:

1. Military
2. Companies to store their secret data.
3. Lockers
4. Any other application where security is the main concern.

IX. CONCLUSION

The proposed method uses an android ATM application which can be installed in the android smart phones, along with the three pin entry methods for the user to enter the PIN securely. This will increase the security level of the password or the PIN number. This aspect gives a secure PIN entry method, which mainly protects the PIN from various attacks such as Shoulder surfing Attacks, Guessing Attacks and Recording Attacks of the user.

REFERENCES

[1] H. J. Asghar, S. Li, J. Pieprzyk, and H. Wang, " Crypto analysis of the convex hull click human identification protocol," in *Proc. 13th Int. Conf. Inf. Secure.*, 2011, pp. 24–30.

[2] H. J. Asghar, S. Li, R. Steinfeld, and J. Pieprzyk, "Does counting still count Revisiting the security of counting based user authentication protocols against statistical attacks," in *Proc. 20th Symp. Internet SocNetw. Distrib. Syst. Secure. (NDSS)*, Apr. 2013, pp. 1–18.

[3] X. Bai, W. Gu, S. Chellappan, X. Wang, D. Xuan, and B. Ma, "PAS: Predicate-based authentication services against powerful passive adversaries," in *Proc. IEEE Annu. Computer Security. Appl. Conf.*, Dec. 2008, pp. 433–442.

[4] Q. Yan, J. Han, Y. Li, and R. H. Deng, "On limitations of designing leakage-resilient password systems: Attacks, principles and usability," in *Proc. 19th Internet Soc. Netw. Distrib. Syst. Security (NDSS) Symp.*, 2012

[5] S. Li, H. J. Asghar, J. Pieprzyk, A.-R. Sadeghi, R. Schmitz, and H. Wang, "On the security of PAS (predicate-based authentication service)," in *Proc. IEEE Annu. Comput. Security Appl. Conf.*, Dec. 2009, pp. 209–218.

[6] P. Dunphy, A. P. Heiner, and N. Asokan, "A closer look at recognition based graphical passwords on mobile devices," in *Proc. ACM Symp.Usable Privacy Security*, 2010, pp. 1–12

[7] S. Wiedenbeck, J. Waters, L. Sobrado, and J. C. Birget, "Design and evaluation of a shoulder-surfing resistant graphical password scheme," in *Proc. ACM Working Conf. Adv. Vis. Interfaces*, 2006, pp. 177–184

[8] H. J. Asghar, S. Li, J. Pieprzyk, and H. Wang, "Cryptoanalysis of the convex hull click human identification protocol," in *Proc. 13th Int. Conf. Inform. Security*, 2010, pp. 24–30

[9] H. Zhao and X. Li, "S3PAS: A scalable shoulder-surfing resistant textual-graphical password authentication scheme," in *Proc. IEEE Int.Conf. Adv. Inf. Netw. Appl. Workshops*, vol. 2. May 2007, pp. 467–472.

[10] H. Sasamoto, N. Christin, and E. Hayashi, "Undercover: Authentication usable in front of prying eyes," in *Proc. ACM SIGCHI Conf. HumanFactors Comput. Syst. (CHI)*, 2008, pp. 183–198