IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 4, Ver. II (July – Aug. 2015), PP 09-15
www.iosrjournals.org

Advanced Safe PIN-Entry Against Human Shoulder-Surfing

Ms.R Revathy[1,] Mrs.R.Bama[2]
[1]*PG student, Sri SaiRam Engineering College, Chennai.*
[2] *Associate Professor , Sri SaiRam Engineering College, Chennai.*

Abstract: *When users insert their passwords in a common area, they might be at risk of aggressor stealing their password. The PIN entry can be perceived by close by adversaries, more effectually in a crowded place. A new technique has been established to cope with this problem that is cryptography prevention techniques. Instead, there have been alternative approaches among them, the PIN entry was elegant because of its simplicity and accessibility. The basic BW method is focused to withstand a human shoulder surfing attack. In every round, a well ordered numeric keypad is colored at odd. A user who knows the accurate PIN digit can enter by pressing the separate color key. The IBW method is examined to be confidential against human nemesis due to the restricted cognitive abilities of humans. Also the IBW method is proven to be robust against any hacking attacks.*

Index Terms: *Personal Identification Number (PIN), Shoulder surfing attack, User authentication.*

I. Introduction

Today, the Internet has entered into our day-to-day life and services have been moved online. Beyond reading the news, looking for information, and other threat free task online, we have also become accustomed to other risk-related work, such as paying using credit cards, checking/composing emails, online banking, and so on. While we appreciate its benefit, we are placing ourselves at risk. Most present commercial websites will request their users to input their user identifications (IDs) and corresponding passwords for verification. Once a user's ID and the corresponding password are thieved by an adversary, the adversary can do anything with the user's account, which can take to a disaster for the user. As a result of enlarging concerns over such risks, securing users passwords on the web has become increasingly hypercritical.

The personal identification number (PIN) is one of the day-to-day user authentication technique used in diverse situations, such as in with drawing cash from an automatic teller machine (ATM), approving an electronic transaction, unlocking a mobile device, and even opening a door. In computer security, shoulder surfing refers to using direct inspection techniques, such as peeping over someone's shoulder, to acquire information. Since the identical PIN is usually selected by a user for diverse purposes and applied frequently, a compromise of the PIN might cause the user a serious risk. Shoulder surfing is frequently used to acquire passwords, PIN security codes, and related data.

Shoulder surfing can also be done at a long distance using binoculars or other vision-magnify devices. Inexpensive, miniature closed circuit television cameras can be hidden in ceilings, walls or fixtures to perceive data entry. Most of the known shoulder-surfing resistant PIN-entry methods apply the fact that the capacity of Short-term memory and the actual-time processing performance of a human are very restricted. The users are susceptible to malevolent people nearby or spyware inside because they can grasp the key input, especially confidential input such as a password, in mobile environs.

To stop shoulder surfing, it is recommended to shield paperwork or the keypad from view by using one's body or cupping one's hand. To deal with this problem, which is between the customer and the system, cryptographic prevention approach is hardly relevant because users are restricted in their capacity to process information. Among them, the PIN entry technique introduced was effective because of its clarity and instinctive: in every round, a structured numeric keypad is colored at odd; half of the keys are in black and another half in white, which we will call the BW method.

A customer who knows the accurate PIN digit can enter the color by pressing the distinct color key below. The primary BW method is targeted to withstand a human shoulder surfing attack. Our proposal called covert attention shoulder surfing indeed can crack the well known PIN entry technique formerly estimated to be secure against shoulder surfing.

II. BW Method And Grouping

User registration is done and after that the user is able to access the ATM application in their mobile phones. Once the user registration is complete, user will be provided with a unique PIN sent to their respective mail id. Once it got validated a user will be able to access application by entering the username and password chosen at the time of registration.

Then our application will provide users its services. Then if the user will go with ATM services, user is asked to provide the PIN digit. At this time, the BW method comes into play. The BW method divides a set of ten digits onto two odd halves, of which one is chosen as stated to the user's key entry in every round. If the chosen halves were remembered or written on a paper for n, successive rounds and recollected to acquire their grouping patterns, the shoulder surfer could recognize a single digit if the PIN. Thus the shoulder surfer is able to find the PIN by grouping the password which is entered by user.

Covert observation shoulder surfing can crack the BW method by the modeling-based analysis. So in Covert observation shoulder surfing, we have three major functions such as perceptual grouping, covert attention and motor operation, are merge together for obtaining a PIN digit.

1) Covert Attention: To effectively and essentially use the allowed time period, our idea is to enroll covert attention. If an adversary represses saccadic eye movements during optical perception, she can obtain more temporal possibility for Visual information processing within the present visual angle. This is true even while organizing covert attention moves to a stimulus inside the optical angle and bringing out parallel motor operations in the absence of saccadic eye movements.

2) Perceptual Grouping: To shorten the memory specification, our idea is to get perceptual grouping. If an adversary remove significant visual relations from lower-level features and groups them into higher-level formation. Selective attention can make some of them seem more salient at a glance and processed efficiently in visual short-term memory (VSTM). Presume that the shoulder surfer is at one meter distance to a 4.3" smart phone. The one block distance in the proximity group implies the visual angle of 0.58◦ whereas the whole display is within the visual angle of 5.05◦. It is possible that two perceptual groups are constructed in mind and stored in VSTM.

3) Parallel Motor Operation: The single digit on that square can be identified as a PIN digit, but there may not be enough time to write it down on a paper nor to memorize it accurately. In every n round, there remains only a single square in the selected perceptual group due to the logarithmic decrease. Thus, we employ the motor operation in parallel i.e., a surreptitious handwriting without saccadic eye movements, to save time and memory. When only a single square remains in the perceptual group, the shoulder surfer identifies the corresponding digit.

III. Improved Bw Method

In this method a new strategy has been implemented that will entirely neglect shoulder surfing even a well practiced perceptual grouper could not break the PIN digit invade by the user in a standard

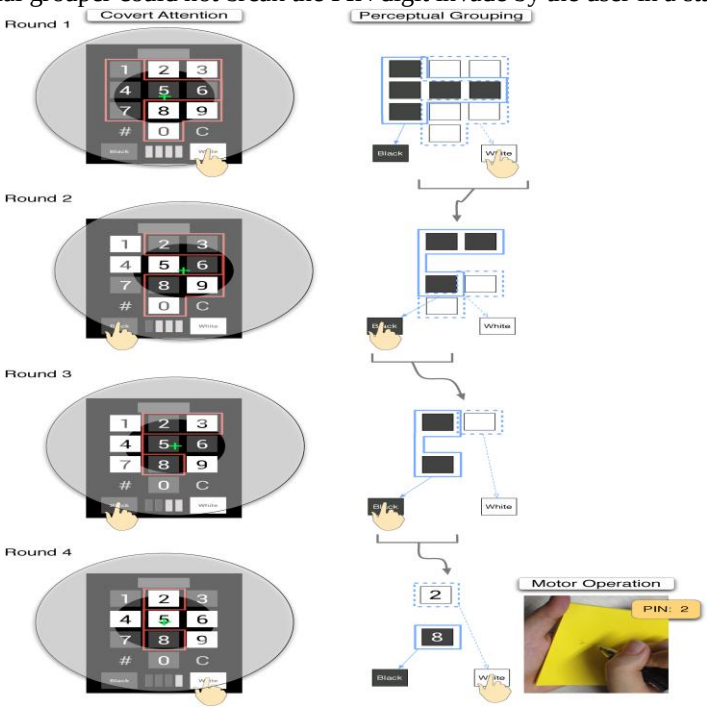

Fig.1. Covert attention shoulder surfing example. (Three major operations, covert attention, perceptual grouping, and motor operation, are merged together for obtaining a PIN digit, consider 2 in this example.)

Fig. 2. Improved BW method (a) Prototype implementation. (b) Running example. (Note: User enters either of two colors represented on the correct PIN digit key. Entered PIN digit is 6 due to black (from yellow/black), blue (from blue/white), yellow (from yellow/black), and black (from blue/black).)

Way. Let R denote a set if four colors and/or patterns modifiable. Let R= {black, blue, white, yellow} or R= {black, white, dotted, diagonal lines}, for a color visually impaired people. Roughly speaking, the improved method runs as follows: The system shows a set of ten digits, P= {0,?, 9}, on the standard numeric keypad with two cleave colors, selected from P, in every numeric key.

The left out colors will fill five splits, respectively, in the similar way. The user manages the PIN digit and occupies one of its colors by the color key. The customer and the system replicate this method for n rounds that the PIN digit is recognize by intersection, and until the complete PIN digits are recognize.

Algorithm - Improved Safe PIN Entry: pseudo code {*comment}
1: (I,J) ← γ(π(I)) {*primary sets: I,J,K,L}
2: (K, L) ← γ(π(I))
3: (W, X) ← (∅ ,(∅ ,) {*eliminated sets: W, X,Y,Z}
4: (Y, Z) ← (∅ ,(∅ ,)
5: **for** i = 1, · · ·, m **do**
6: (i, j, k, l) ← ρ (P) {*permutation of colors}
7: display (I ∪ X and J ∪ W) and (K ∪ Z and L ∪ Y)
{*odd splits of I ∪ X in i, J ∪ W in j}
{*remaining splits of K ∪ Z in k, L ∪ Y in l}
8: input choice ∈ i, j, k, l {*user's input}
{*partition the selected and the other sets}
9: **if** choice = i **then**
10: (Y, Z) ← γ(π(W ∪ X ∪ J))
11: (W, X) ← γ(π(W ∪ X ∪ J))
12: (K, L) ← γ(π(I))
13: (I, J) ← γ(π(I))
14: **else if** choice = j **then**
15: (Y, Z) ← γ(π(W ∪ X ∪ I))
16: (W, X) ← γ (π(W ∪ X ∪ I))
17: (K, L) ← γ(π(J))
18: (I, J) ← γ(π(J))
19: **else if** choice = k **then**
20: (W, X) ← γ(π(Y ∪ Z ∪ L))
21: (Y, Z) ← γ(π (Y ∪ Z ∪ L))
22: (I, J) ← γ(π(K))
23: (K, L) ← γ(π(K))
24: **else**
25: (W, X) ← γ(π(Y ∪ Z ∪ K))
26: (Y, Z) ← γ(π(Y ∪ Z ∪ K))
27: (I, J) ← γ(π(L))
28: (K, L) ← γ(π(L))
29: **end if**
30: **end for** {*for loop runs for m rounds}
31: **return I** {*a single digit is recognized}

1) Formal Illustration: We officially report the enhanced technique in Algorithm 1. Let π: I∗ → I∗ and ρ: X∗ → X∗ indicate odd permutations of sets, I and X, respectively. Let γ be a specific task that partitions a set having y elements into two sets having y/2 and y/2 elements, respectively. γ ($\pi(\cdot)$) then means two odd partitions. The algorithm starts with partitioning I at odd two times; four primary sets, two of which are match together: I, J and K, L is acquired. Four empty sets called terminated sets, two of which are also paired: W, X and Y, Z are initialized.

The following strategy is then run for m rounds. First, X is permuted to be (i ,j ,k ,l). A odd half of the numeric keys, five splits, are colored with i; upper and lower splits are selected at odd from I ∪ X. The other half of the numeric keys are colored with j; upper and lower splits are selected at odd from J ∪ W. Again, another odd half of the numeric keys are colored with k; then available splits are selected from K ∪ Z. The other half of the numeric keys are colored with l; available splits are selected from L ∪ Y. Accordingly, each numeric key include two distinct colors while every color is dispersed into five numeric keys.

When the user enters a distinct color key (for example, i; in Algorithm 1, if choice = i then), the equivalent main set (for example, I) is partitioned twice at odd; four new main sets, two of which are paired, are acquired. Before this partitioning, however, the other paired main set (for example, J) and two terminated sets (for example, W and X) according to I, must be partitioned at odd two times; four new terminated sets, two of which are paired, are acquired in advance. Algorithm 1 defines these elaborately. Note that the main sets are reduced in their size between the rounds. After running m rounds of this method, a single digit remains in I; so I is returned as the recognized PIN digit. The algorithm must be run for n digits of the PIN; m × n.

2) Prototype Example: Fig. 2 shows the design of our Prototype execution and represents an example input series for the PIN digit, 6. The four-leaf clovers at the top specify the number of color keys pressed and the number of PIN digits previously entered.

IV. Session Key Method

Here we introduced third PIN-entry method called session key entry method. The primary plan of our technique composes an erect array of digits from 0 to 9, compared with other array of ten prominent objects such as + and / etc. For clarity, we presume that the number of digits in PIN is four; however the advanced method might be applied to any instance with N ≥ 2 digits. Here four rounds required overall. The initial round is the session key selection round, and the last three rounds are PIN-invade rounds. In the session key selection round, ten oddly organized objects are exhibited to the user. The user identifies the symbol quickly which is displayed beneath the initial digit of her/his PIN as the short term session key and presses "OK." button. In the shown example where the PIN is 4371, the user identifies symbol as the session key since it is juxtaposed with the initial digit of the PIN, 4. The last three rounds were PIN-entry rounds, over which the i th digit of the PIN is invaded in the r th round for i = 2, 3, 4. In every round, the user is once again given a set of odd array of ten objects, and she/he invades a PIN digit by inter changing the object array and placing the session key with the present PIN digit. To this process, the user can utilize two extra buttons ("Left" and "Right"). In the example shown in Fig. 3(a) and (b), the user presses the "Right" button two times so that symbols shifts to the location quickly, and then presses "OK.". However, as shown in the following example, ordinary human attackers frequently fail to do this because the objects array moves very rapidly

Fig.3. User recognizes the object & fixes the object as temporary session key.

Fig.3 (a) User selects the object using the Right or Left shiftkeys

Fig.3 (b) After entering the entire pin the user clicks the "OK" button.

V. Authentication And Services

Once the user entered pattern is manipulated and a PIN is identified, it will be checked with the local database provided by android OS using SQL Lite. This process is to prevent unwanted server end process handling playful requests. A one way hash is generated for the validated PIN and is sent to server in public channel so that an active attacker cannot extract the PIN by monitoring the channel. Once got authenticated by server a quick response to the mobile app will redirect the user to the services. In ATM services cash withdrawal, deposit and fund transfer can be done securely using the concept of virtual money which is already employed by many other applications successfully in the web. This reduces the overhead complexities in the server and will provide the user an ease of access to the banking Services

Fig.4 Banking Services

Fig.4 (a) Amount Withdrawal

Fig.4 (b) Fund Transfer

VI. Conclusion

We considered the challenges of securing users passwords on the internet and shown some equivalent effort in this field. Also we have discussed how to secure users' passwords which is being thieved by adversaries. Human adversaries are more strong than awaited when shoulder surfing. The advanced system reduced the difficulties of shoulder surfing or eves dropping by introducing the different PIN entry methods. The covert attention shoulder surfing suggested in this paper is to expertise the first experienced counter-attack of humans against the system, formerly estimated to be secure. Here what we have well read from the delicacy of the BW method is that obtaining both securities and usability is honestly demanding and subject to incorrect plan due to the absence of formal remedy. Also we have introduced a new PIN-entry technique that has proposed security against human shoulder-surfing attacks. This is feasible by successfully enlarging the part of memory needed by a shoulder surfer.

References

[1]. "Security Notions and Advanced Method for Human Shoulder-Surfing Resistant PIN-Entry" IEEE TRANSACTIONS 2014, Mun-Kyu Lee, Member, IEEE.

[2]. "Drag-and-type: a new method for typing with virtual keyboards on small touch screens", IEEE TRANSACTIONS 2014, Taekyoung Kwon, IEEE, Sarang Na, IEEE, Sang-ho Park.

[3]. "Novice and Expert Performance of Key Scretch: A Gesture-Based Text Entry Method for Touch-Screens" IEEE TRANSACTIONS, 2014, Vittorio fuccella, Mattia de Rosa, and Gennaro costagliola, Member, IEEE.

[4]. "Differentiated Virtual Passwords, Secret Little Functions, and Codebooks for Protecting Users From Password Theft" IEEE TRANSACTIONS 2014, Yang Xiao , senior member, IEEE ,Chung – Chin Li, Ming Lei, and Susan V. Vrbsky.

[5]. "Capacitive Touch Communication: A Technique to Input Data through Devices Touch Screen**"** IEEE TRANSACTIONS, 2014, Tam Vu, Akash Baid, Simon GAO, Marco Gruteser, Richard Howard, Senior Member.

[6]. "Cognitive authentication schemes safe against spy ware," in Proc. IEEE Symp. Security Privacy, May 2006, D. Weinshall.

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

[8]. "A review of visual memory capacity: Beyond individual items and toward structured representations," J. Vision, 2011, T. F. Brady, T. Konkle, and G. A. Alvarez,