Implementation of Improved Black and White Method to Prevent Shoulder Surfing

C. Bharathi Priya[1] R. Pavithra[2] S. Chetnaa [3]
[1, 2, 3]B.E. Department of Computer Science and Engineering
[1, 2, 3]Velammal Institute of Technology

Abstract— When a password is being entered in a computer system, shoulder surfing attacks are of great concern. To solve this problem, existing system used limited cognitive capabilities of a human adversary, but there was a disadvantage with the assumption. In this paper, we show that human adversaries can be more effective at eavesdropping than expected, in particular by employing cognitive strategies and by training themselves. Our novel approach called improved Black and White method indeed can break the well-known PIN entry method previously evaluated to be secure against shoulder surfing. Another contribution in this paper for information security is the authentication service which uses local database and hash.
Index Terms human adversaries, information security, shoulder-surfing.

I. Introduction

WHEN A USER enters a personal identification number (PIN) as a numeric password in mobile or stationary systems, including smartphones, 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. Among them, the PIN entry method presented by Roth *et al.* [1] 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.

II. Black and White Method

In shoulder surfing attacks, adversaries should move their eye fixations rapidly on the user interface, particularly during preprocessing, to obtain the challenge information, e.g., the layout of the keypad, in an on-time processing phase to catch the key entry information, e.g., a user's key press; and during post processing to filter the acquired information. If the time period allowed for those processes is too short or its memory requirement exceeds the human limit, then shoulder surfing should fail. To extend and effectively use the allowed time period, the existing idea is to employ covert attention. If an adversary suppresses saccadic eye movements during visual perception, she can earn more temporal chances for visual information processing within the current visual angle. This is true even while conducting covert attentional shifts to a stimulus inside the visual angle and carrying out parallel motor operations without saccadic eye movements. To reduce the memory requirement, our idea is to employ perceptual grouping. If an adversary extracts significant visual relations from lower-level features, e.g., color of squares by ignoring the individual digits, and groups them into higher-level structures, e.g., a larger polygon in the same color, based on the Gestalt principles, she can reduce the number of visual objects stored in the short-term memory. So in Covert attentional shoulder surfing, three main operations such as covert attention, perceptual grouping, and parallel motor operation, are combined together for deriving a PIN digit. In each round, attended objects are lined for easier understanding of covert attention. Covert attentional shoulder surfing can break the BW method through the modeling-based analysis.

III. Improved Black and White Method

We propose improved BW method by extending BW method, in which our proposed algorithm uses randomly generated four digits in which each digit block, is combined with the combination of two , to prevent the attentional shoulder surfing attack by extracting the PIN digit after all the user iterations got completed. To resist covert attentional shoulder surfing, it would be effective to interrupt the adversary during perceptual grouping without changing the user task significantly. One possibility is to keep the BW method, but randomize the ordering of the digits in each round so that perceptual grouping cannot be done in the way we proposed. In this case, however, the user task requires the added saccadic eye movement while searching for the location of the target digit in every round can lead to longer PIN entry time. Another possibility is to keep the numeric keypad in the regular layout, but produce more perceptual groups so that the adversary is frustrated. Toward similarity in the task of perceptual grouping, we make color groups look similar (neither the same nor opposite) in their shape because color must be distinguishable by the user. Toward complexity, we make color groups look overlapping (not separate), so that adversaries experience severe difficulties not only in holding the groups in VSTM but also in

separating them. The fundamental idea for combining similarity and complexity, is to split visually every numeric key into two halves, so as to be filled with two distinct colors simultaneously whereas each color fills half of the available keys, i.e., five out of ten keys. So there exist four color groups on the numeric keypad and two colors for every numeric key. The adversary who launches covert attentional shoulder surfing may need to perceive four color groups and attend to one of them for the next round, while the user only needs to answer either of the two colors that fill his/her PIN digit key in each round. Authentication Services are also provided by this method.

IV. Architecture of Improved BW Method

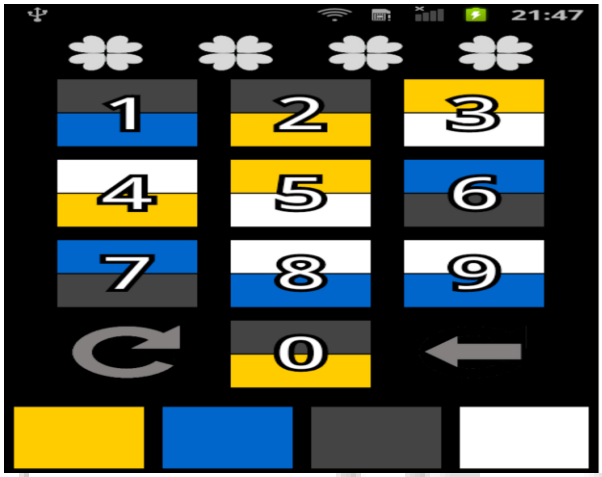


Fig. 1: Architecture of improved BW method

In this Method we implement a new Strategy that will completely neglect Shoulder Surfing even a Well Trained Perceptual Grouper could not Crack the PIN Digit Entered by the User in a Conventional Way. Let P denote a set of four colors and/or patterns customizable. Let P = {black, blue, white, yellow} or P = {black, white, dotted, diagonal stripes}, for a color blind person. Roughly speaking, the improved method runs as follows: The system displays a set of ten digits, *A* = {0, ???, 9}, on the regular numeric keypad with two split colors, chosen from P, in each numeric key; and the four color keys below. A color is chosen at random from P and fills five random splits of distinct keys; each split could be either upper or lower one. The remaining colors fill five splits, respectively, in the same way. The user attends to the PIN digit and enters either of its color through the color key. The user and the system repeat this procedure for *m* rounds that the PIN digit is identified by intersection, and until all the PIN digits are identified.

V. Algorithm for Improved Pin Entry: Pseudo Code

{*comment}

1: A,B ← γ(π(A)) {*primary sets: A,B,C,D}
2: C,D ← γ(π(A))
3: O, P ← (∅, ∅) {*eliminated sets: O,P,Q,R}
4: Q,R ← (∅, ∅)
5: for i = 1, · · · ,m do
6: a, b, c, d ← ρ(P) {*permutation of colors}
7: display (A ∪ P and B ∪ O) and (C ∪ R and D ∪ Q)
{*random splits of A ∪ P in a, B ∪ O in b}
{*remnant splits of C ∪ R in c, D ∪ Q in d}
8: input choice ∈ a, b, c, d {*user's input}
{*patition the chosen and the other sets}
9: if choice = a then
10: Q, R ← γ(π(O ∪ P ∪ B))
11: O, P ← γ(π(O ∪ P ∪ B))
12: C, D ← γ(π(A))
13: A, B ← γ(π(A))
14: else if choice = b then
15: Q, R ← γ(π(O ∪ P ∪ A))
16: O, P ← γ(π(O ∪ P ∪ A))
17: C, D ← γ(π(B))
18: A, B ← γ(π(B))
19: else if choice = c then
20: O, P ← γ(π(Q ∪ R ∪ D))
21: Q, R ← γ(π(Q ∪ R ∪ D))
22: A, B ← γ(π(C))
23: C, D ← γ(π(C))
24: else
25: O, P ← γ(π(Q ∪ R ∪ C))
26: Q, R ← γ(π(Q ∪ R ∪ C))
27: A, B ← γ(π(D))
28: C, D ← γ(π(D))
29: end if
30: end for {*for loop runs for m rounds}
31: return A {*a single digit is identified}

q Elements into two sets having ⌜ q/2⌝ and ⌞q/2⌟ elements, respectively. γ(π(·)) then means two random partitions. The algorithm starts with partitioning A random two times; four primary sets, two of which are paired: A,B andC,D are obtained. Four empty sets called eliminated sets, two of which are also paired: O, P and Q, R are initialized.The following procedure is then run for m rounds.First, P is permuted to be a, b, c, d. A random half of thenumeric keys, five splits, are colored with a; upper and lowersplits are chosen at random from A∪P. The other half of the numeric keys are colored with b; upper and lower splits are chosen at random from B ∪ O. Again, another random half of the numeric keys are colored with c; available (remaining) splits are chosen from C ∪ R. The other half of the numeric keys are colored with d; available splits are chosen from D∪Q. Consequently, every numeric key incorporates two distinct colors while each color is scattered onto five numeric keys. If the user enters a separate color key (for example, a; in Algorithm 1, **if** choice = a **then**), the corresponding primary set (for example, A) is partitioned twice at random; four new primary sets, two of which are paired, are obtained. Before this partitioning, however, the other paired primary set (for example, B) and two eliminated sets (for example, O and P) according to A, must be partitioned at random two times; four new eliminated sets, two of which are paired, are obtained in advance. Algorithm 1 states these formally. Note that the primary sets are reduced in their size through the rounds. After running m rounds of this procedure, a single digit remains in A; so A is returned as the identified PIN digit. The algorithm should be run for *n* digits of the PIN; $m \times n$.

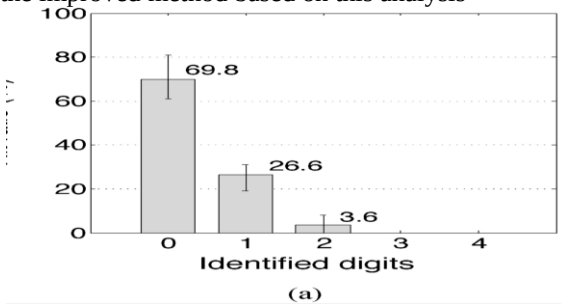
VI. Prototype Example

Fig.2. shows the layout of our prototype implementation and illustrates an example input sequence for the PIN digit, 6. The four-leaf clovers at the top indicate the number of color keys

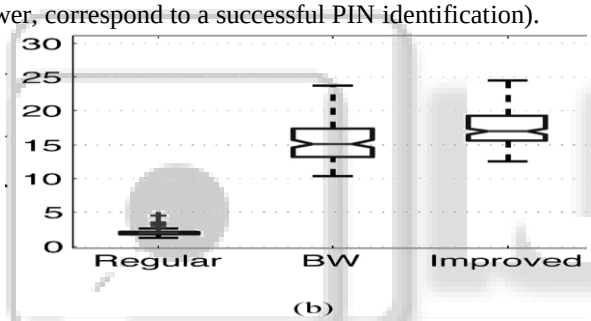
VII. SECURITY EVALUATION

pressed (leaves) and the number of PIN digits (clovers) already entered.

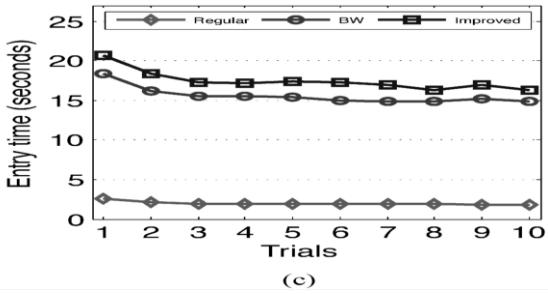
1) *Modeling-based Analysis:* As we discussed in Section V-A, the improved method was modeled and analyzed in CPM-GOMS during the design phase. Note that x = 700 and y = 100, only 100 MS more than the BW method and obviously not enough for perceiving four perceptual groups that look overlapping. Due 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



(a) Average hit ratio over five days as a function of number of identified PIN digits (Note: four identified digits, but not fewer, correspond to a successful PIN identification).



(b) Comparison of entry time.



(c) Average entry time over ten successive trials

Fig. 3: (a) illustrates a much improved result over that in (b). No one succeeded in covert attentional shoulder (c) Average entry time over ten successive trials

Surfing (deriving the four-digit PIN correctly) against the improved method over the five day period. No one was able to guess even three PIN digits. All the participants missed every PIN digit in 69.8% of the trials over five days. In 26.6% and only 3.6% of trials, respectively, participants found a single or two PIN digits. The participants who guessed one or two digits commonly reported that they tried to follow one chosen color group to the best of their ability. As for identifying a single digit (the best outcome in this experiment), there was a significant training effect between days 1 and 3 ($t(9) = -4.811$, $p < 0.001$) but no significant learning effect found between days 3 and 5 ($t(9) = 1$, *n's.*($p = 0.343$)). Day 3 was a peak day and the hit ratio did not increase after that. Based on both analytic and experimental results, the improved method is significantly more resilient to the covert attentional shoulder surfing but one concern remains: 26.6% (higher than a random guess) of the case attackers were able to guess one digit. If the attacker could mount a long-term attack over multiple trials, she is more likely to collect PIN digits faster than random guessing. We unofficially checked that 1) a random shuffling of digits or 2) an exchange of colors in every two rounds could be a possible resolution.

VIII. AUTHENTICATION & 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.

IX. CONCLUSION

Human adversaries can be more powerful than expected when shoulder surfing. The covert attentional shoulder surfing proposed in this paper is to our knowledge the first sophisticated counter-attack of humans against the system, previously evaluated to be secure. What we have learned from the weaknesses of the BW method is that achieving both security and usability is truly challenging and prone to erroneous designs due to the lack of formal treatment. We adapted the CPMGOMS method for resolving this problem because it is effective in modelling a skilled user. The estimated performance in our modelling was quite close to the experimental results. Our novel idea of modelling the adversary was also effective in analysing security and devising an improved method. The new attack was successfully modelled and experimented. It was interesting that participants who enjoy fast-paced video games were better at shoulder surfing, and the training effect was remarkable.

REFERENCES

[1] V. Roth, K. Richter, and R. Freidinger, "A PIN-entry method resilient against shoulder surfing," in Proc. ACM Conf. Comput. Commun Security, 2004, pp. 236–245.

[2] M. I. Posner, "Orienting of attention," Quart. J. Experimental Psychology, vol. 32, no. 1, pp. 3–25, 1980.

[3] D. G. Lowe, Perceptual Organization and Visual Recognition. Norwell, MA, USA: Kluwer, 1985.

[4] S. K. Card, T. P. Moran, and A. Newell, "The keystroke-level model for user performance time with interactive systems," Commun. ACM, vol. 23, no. 7, pp. 396–410, 1980.
[5] B. E. John and W. D. Gray, "CPM-GOMS: An analysis method for tasks with parallel activities," in Proc. ACM SIGCHI Conf. Human Factors Comput. Syst., 1995, pp. 393–394.
[6] 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.
[7] Banking—Personal Identification Number (PIN) Management and Security—Part 1: Basic Principles and Requirements for Online PIN Handling in ATM and POS Systems, Clause 5.4 Packaging Considerations, ISO 9564-1:2002, 2002.
[8] 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. Comput. Security Appl. Conf., Dec. 2008, pp. 433–442.
[9] H. Gao, X. Liu, S. Wang, and R. Dai, "A new graphical password scheme against spyware by using CAPTCHA," in Proc. ACM Symp. Usable Privacy Security, 2009, pp. 15–17.

