International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:2682
Vol.5, No.7, July 2016 DOI:10.15693/ijaist/2016.v5i7.74-80

COLOR COUNTER AGAINST COVERT ATTENTION : HUMAN ADVERSARIES ARE MORE POWERFUL THEN EXPECTED

Dr.M. Ramesh Kumar[1], Dr.S.Sangeetha[2] ,C.Sasikala[3] , K.Prabhu[4], G.S.Pugalendhi [5],

1,2 Associate Professor, Department of Computer Science and Engineering,

VSB College of Engineering Technical Campus, Coimbatore, TamilNadu, India.

3, 4, 5 Asst Professor, Department of Computer science and Engineering,

VSB College of Engineering Technical Campus, Coimbatore, TamilNadu, India.

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

Keywords- **human adversaries, information security, shoulder-surfing.**

1. 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.

2. 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 attention 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.

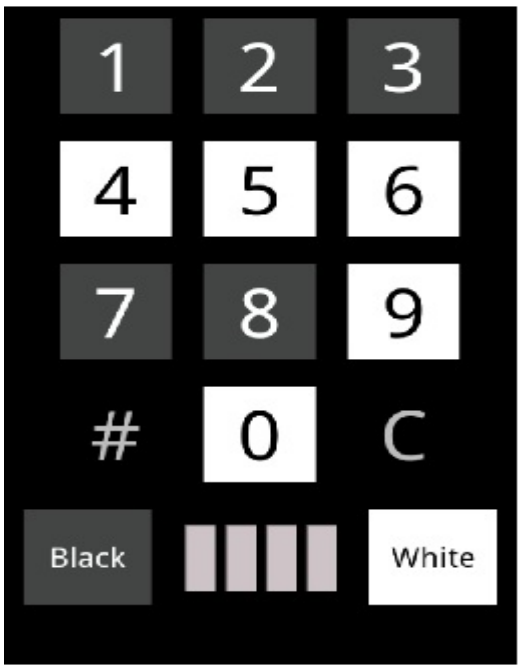


Figure 1. Keypad of BW Method

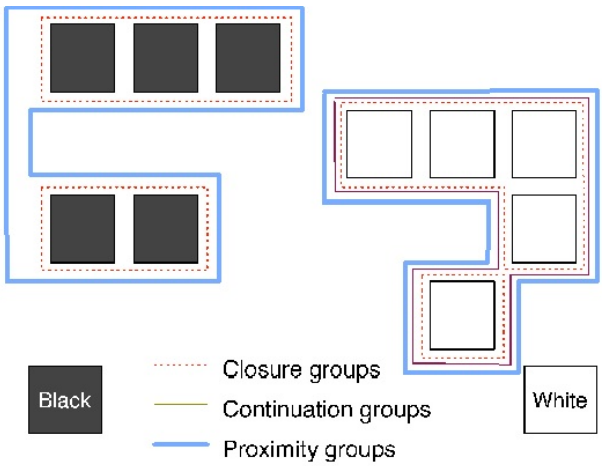


Figure 2. Perceptual grouping in BW Method

In each round, the regular numeric keypad is colored at random in two distinct colors; half of the numeric keys in black and the other half in white. The user is required to answer the present color of the PIN digit key immediately by pressing a separate color-indication key below the keypad. Since the random half of the numeric keys in the same color are selected together in every single round, multiple rounds are played for

identifying a single (entered) digit by intersection.

For entering the *n*-digit PIN, $m \times n$ rounds are necessary, i.e., 16 rounds for a four-digit PIN. Since only simple binary selections are required for the PIN entry, the BW method is truly intuitive to users. A significant drawback is the numerous rounds of key entry.

3. ADVANCEMENT IN BLACK AND WHITE METHOD

We propose improved BW method by extending BW method, in which our proposed algorithm uses randomly generated ten digits in which each digit block, is combined with the combination of four, 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 four halves, so as to be filled with four distinct colors simultaneously whereas each color fills quarter of the available keys. So there exist ten color groups on the numeric keypad and four 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

4. ARCHITECTURE OF THE COLOR MODEL

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 ten colors and/or patterns customizable. Let P = {set of any 10 colors} or P = {4 digit binary format symbols from 0 to 9}, 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 four split colors, chosen from P, in each numeric key corresponding to its positions(top left, top right, bottom left and bottom right); and the ten color keys below.

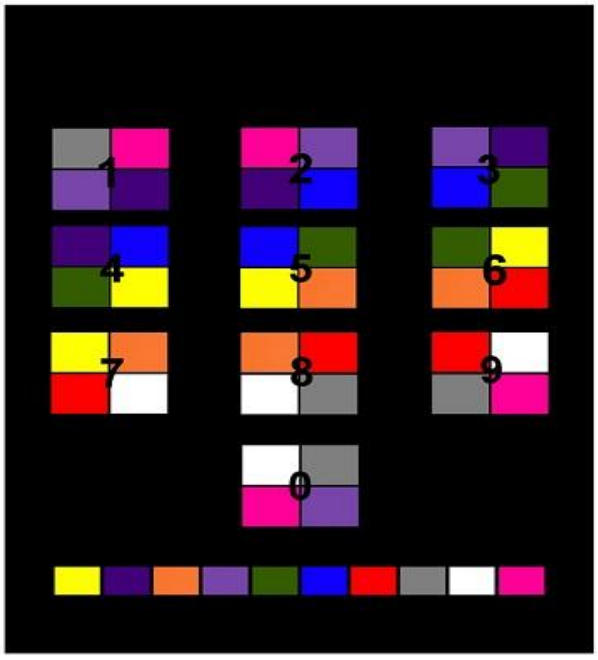


Figure 3. Keypad of the Color Model

The logic of implementation is the first PIN digit corresponds to the first position, i.e. top

left and other digits correspond to the other positions respectively. The user should press color of his PIN number in order to enter his the first PIN digit. The same procedure is followed for all the other digits, in order to enter the complete PIN number.

5. ALGORITHM FOR IMPROVED PIN ENTRY

1: function PIN entry (NEW, A) returns a refresh or false

2: init CB=set of 10 colors;

3: init NEW=set of 4 digits;

4: repeat until new is empty

5: new ← empty

6: for each PIN a in new do

7: {

8: Note the PIN digit's position;

9: Save it as P;

10: Note the corresponding position color of the PIN digit

11: Save it as PC

12: if (CB ← PC)

13: Press the color from CB;

14: Refresh ();

15: }

16: else

17: {

18: return failure;

19: }

20: new++;

21: }

22: return false;

There is a function PIN entry with parameters NEW and A, where new represents the array of 4 digits of the PIN number and a represents the index of each and every PIN digit.

Initialize a set of 10 colors to CB and a set of 4 digits to NEW. For every index of the PIN digit, Note the index of the PIN digit and save it as P; then note the corresponding position color of the PIN digit and save it as PC. Now, check whether the color in PC belongs to CB.

If this condition is true then press the corresponding color from CB and after the entering of a digit the Refresh function is being made. Otherwise it returns a failure as the verification process is not satisfied.

Increment is made to NEW as the index value is changed after the entry of each PIN digit. If the function PIN entry is not satisfied or if all the index of the PIN digit has been entered the code returns a false statement leading to the end of the operation.

6. PROTOTYPE EXAMPLE

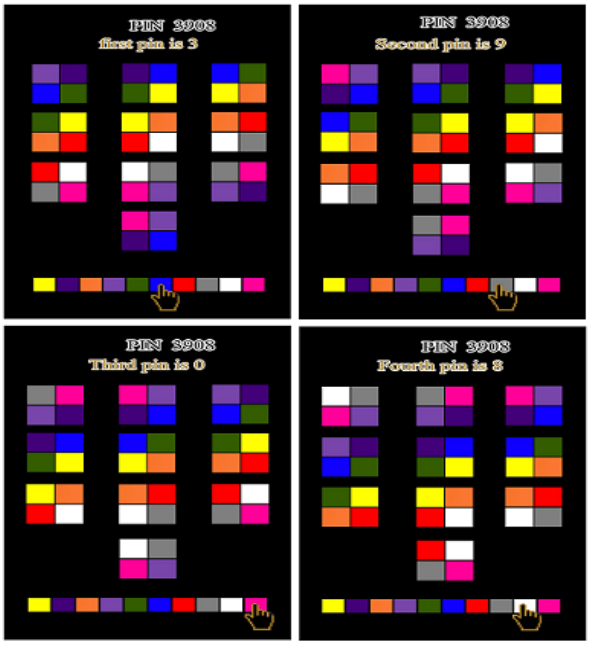


Figure 4. Accessing the Color Model

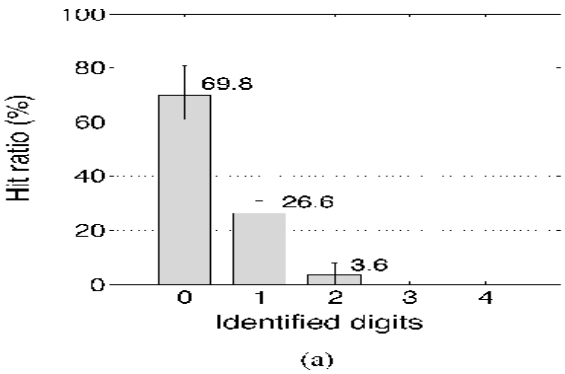
The above Figure 4 gives a complete guidance about the accessing of the color model. The keypad of the color model is a virtual keypad with ten color buttons below it. The example PIN given in Figure 4 is 3908.So if the user want to press this PIN number he does the following way of accessing. To enter the first PIN digit 3 the user has to press the first position color of the number 3 i.e. blue. The same logic is applied for the remaining colors. To get the 2nd digit 9, the user has to press the second position color of the number 9 i.e. grey. To get the 3rd digit 0 the use has to

press the third position color of the number 0 i.e. pink. Finally to get the final digit the user has to press the 4th position color of the 4th number i.e. white. Every time when a digit is being entered the keypad gets automatically changed by new combination of colors for each numeral .Care is taken to prevent the repetition of color in the same position of the numerals. The logic made here is really simple and the accessing time is very low with more secureness. Only a less human effort is made in order to interact with the system.

7. SECURITY EVALUATION

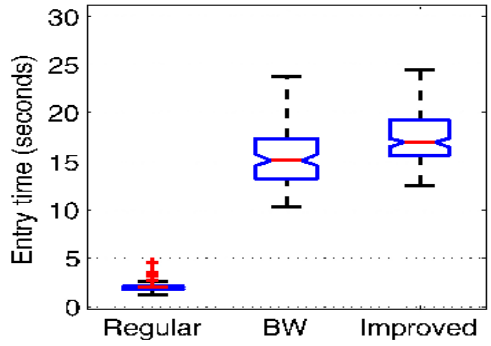
7.1) *Modeling-based Analysis*:

As we discussed in Section 5, 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 *initialization of CB* in the algorithm, ten colors are shuffled at random in every round; a particular color is not more likely to be assigned and entered. We conclude that covert attentional shoulder surfing is infeasible against the improved method based on this analysis



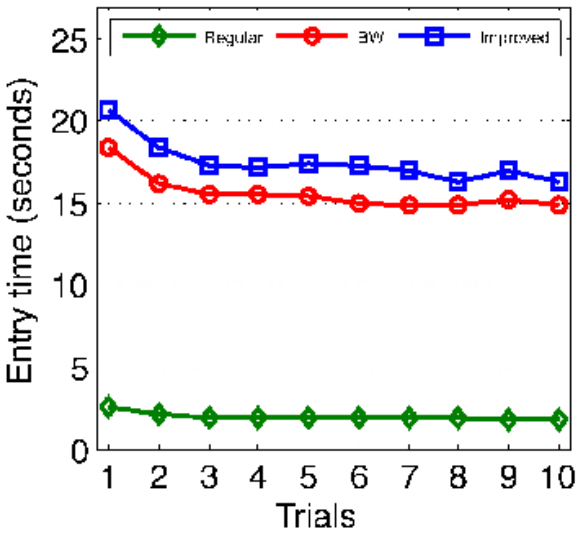
(a)

(a) Average hit ratio over five days as a function of number of identified PIN digits



(b)

(b) Comparison of entry time



(c)

(c) Average entry time over ten successive trials

Figure 5. (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 single round could be a possible resolution.

8. 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.

9. 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 analyzing 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.

.

10. REFERENCES

[1] V. Roth, K. Richter and R. Friedinger, "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 Indentification 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] S. J. Luck and E. K. Vogel, "The capacity of visual working memory for features and conjunctions," Nature, vol.390, no.6657, pp. 279-281, 1997.
[9] I. G. Sligte, H. S. Scholte, and V. A. F. Lamme, "Are three multiple visual short-term memory stores?," PLoS One, vol. 3. No. 2, p. e1699, 2008.
[10] W. S. Geisler and B. J. Super, "Perceptual organization of two-dimensional patterns," Psychol. Rev., vol.107, no.4,pp.677-708, 2000.
[11] K. Rayner, " Eye movements in reading and information processing: 20 years of research," Psychol. Bull., vol. 124, no.3, pp.372-422, 1998.

Author Profile

Dr.M.RAMESHKUMAR received P.hD in Karpagam university Tamilnadu,India.in the year of 2015. currently working as a Associate professor in the Department of Computer science and engineering VSB College of Engineering Technical Campus, Coimbatore, Tamilnadu, India.