© 2015 IJSRSET | Volume 1 | Issue 2 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Human Interaction in Shoulder Surfing Security

S. Geethanjali, J. Mary Monika, V. Nandhini
Department of Computer Science and Engineering, Velammal Institute of Technology, Chennai, Tamilnadu, India

ABSTRACT

We propose a web application based security system. When a user interacts with a computing system to enter a secret password, shoulder surfing attacks are of great concern. This system overcomes the problem of shoulder surfing. Previous system proposed a methodology in which the user has to remember all the events performed. This limits the system usage. Our novel approach enhances the shoulder surfing security with human interaction; indeed can break the well-known PIN entry method previously evaluated to be secure against shoulder surfing. To overcome the problem, we design a multi-color number panel. This interface provides the user, a higher level of security that the shoulder surfer cannot be aware of the process the user undergoes. The color pattern in the number panel changes periodically so that for each user is provided a different pattern.
Keywords: human adversaries, information security, shoulder-surfing

I. INTRODUCTION

The main aim of this project is to prevent human shoulder surfing attack and to establish a secure transaction by implementing the color matching algorithm. 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, bank lockers, online net banking sites 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 was elegant because of its simplicity and intuitiveness: in each round, a regular numeric keypad is colored at random, all the keys are divided into four quadrants and each quadrant is given different colors. None of the quadrants in the entire panel will have the same color.

A user who knows the correct PIN digit can answer its color by pressing the separate color key below. The basic 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. This method is still considered to be secure against human adversaries due to the limited cognitive capabilities of humans.

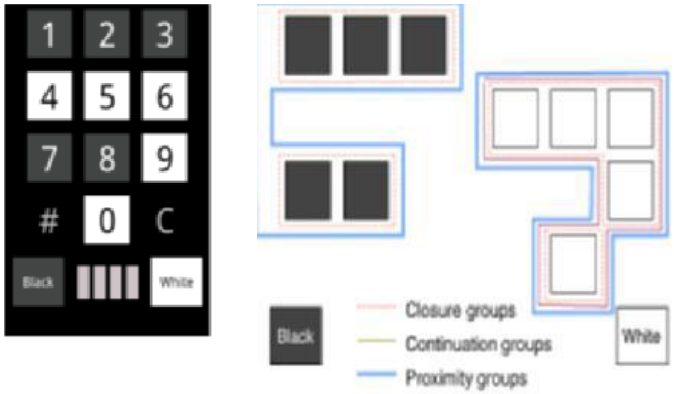
II. METHODS AND MATERIAL

A. 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.



(a) (b) (c)

Figure 1: Black and White Method (a) BW challenge on keypad. (b) Perceptual groups in black. (c) Perceptual groups in white

B. Improved Black and White Method

Improved BW method is proposed by extending BW method, in which the 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, 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.

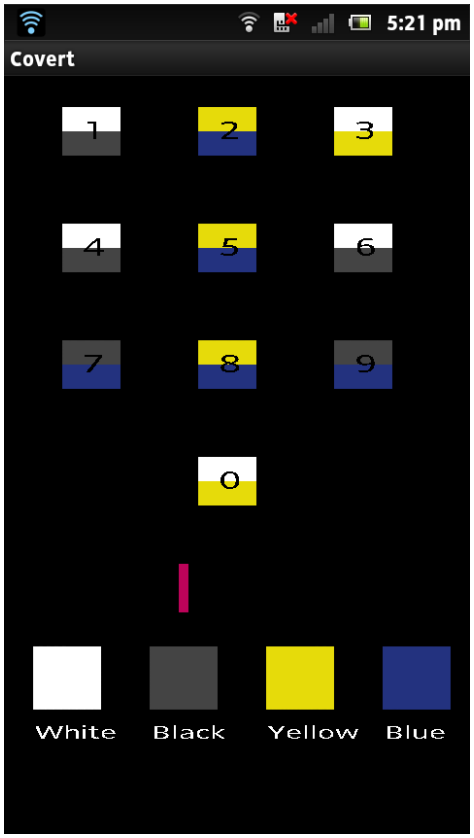


Figure 2: Improved Black and White Method

C. Multi-Color Number Panel

We propose a new type of number panel with multiple colors. In this panel each number key is divided into four quadrants, each quadrant is given a different color. No two quadrants will have the same color. There are totally ten colors used in this model. User has to enter the PIN by choosing the corresponding color in the quadrant. Each number of the PIN corresponds to a particular color in the panel. We propose a two type of pattern to choose the corresponding color to each number of the PIN. Since we use a two different type of pattern, for each user the pattern will change. The pattern will sometimes remain the same for consecutive users. It will be difficult for the shoulder surfer to find the PIN number since the pattern changes for every user. Color matching algorithm is the key behind this multi-color number panel. No color will repeated in the same quadrant this is achieved by color matching algorithm. With this algorithm we achieve the disadvantage of pressing the number multiple times. In our model for every number only single click is made. The click event is made easy with easy click.

The colors in all the quadrants of the number panel will shuffle for each user. Refresh button is used to reshuffle the colors. This method entirely differs from the improved black and white method. This proposed system is a web application. The bottom of the screen contains the ten buttons with different colors. User has to click the color buttons that are present at the bottom. Depending on the position of the number and the quadrant user has to click the color button. Since two patterns are used user has to click the buttons carefully.

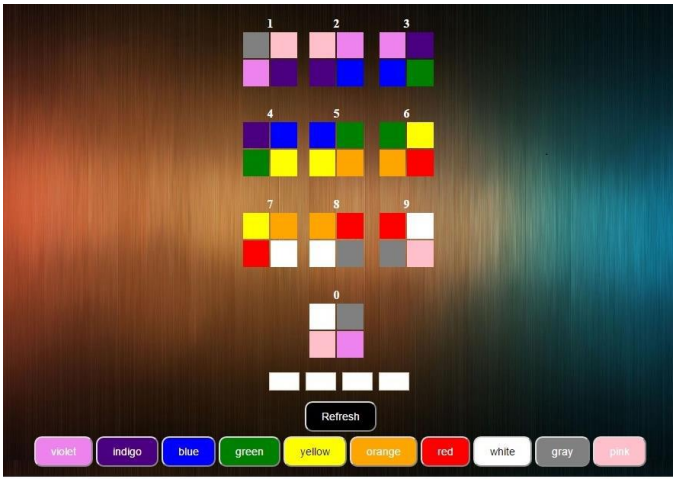


Figure 3: Multi-color number panel

D. Color Matching Algorithm

The PIN number which is to be entered has four digits; these four digits are related to the four quadrants accordingly. The algorithm works in such a way that it relates each color button at the bottom to each color present in the number buttons. For the first digit of the PIN user has to click the color present in the first quadrant of the number, for the second digit click the button corresponding to the color present in the second quadrant of the number. For the third digit click the color present in the third quadrant of the number, same as that for the fourth digit click the color button that coincides with the color in the fourth quadrant of the number. The same pattern is followed for the third and fourth digits. This method corresponds to the first pattern, where first digit corresponds to the color in the first quadrant and second digit corresponds to the color in the second quadrant and so on.

The second pattern works in the following way. Here user has to click the color buttons as that of the first method but the pattern alone differs. This will make the shoulder surfer difficult to find the digits of the personal identification number. In the second pattern, for the first digit user has to click the color button at bottom of the screen which coincides with the color in

the third quadrant of the number. For the second digit user has to click color button that matches with the color in the second quadrant of the number. Similarly for the third digit user will be clicking color button that matches with the color in the first quadrant of that number. And for the last digit user will be clicking the color button at the bottom that matches with the color in the fourth of the number. These two patters will differ for the consecutive users.

III. RESULTS AND DISCUSSION

A. Performance Analysis

Modeling-based Analysis: As we analysed the working of the black and white method, improved black and white method, our proposed system produces the result within a short period, this notes for the time complexity of the system. Here the user has to perform the click event only once for every number, this makes the system work much faster than the existing systems. Whereas in black white method user has to perform the click event until the digit of the personal identification number is obtained and in the improved black whit method user has to perform the click event twice for every digit of the personal identification number, by making the click event twice it makes the shoulder surfer to find out the number during some worst cases.

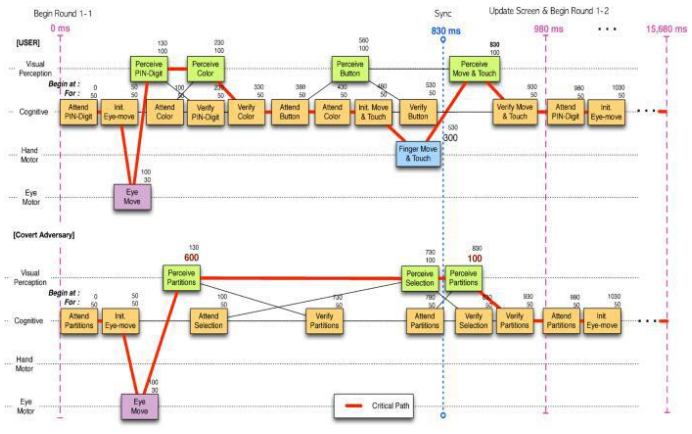


Figure 4: Performance Analysis of Black and White method

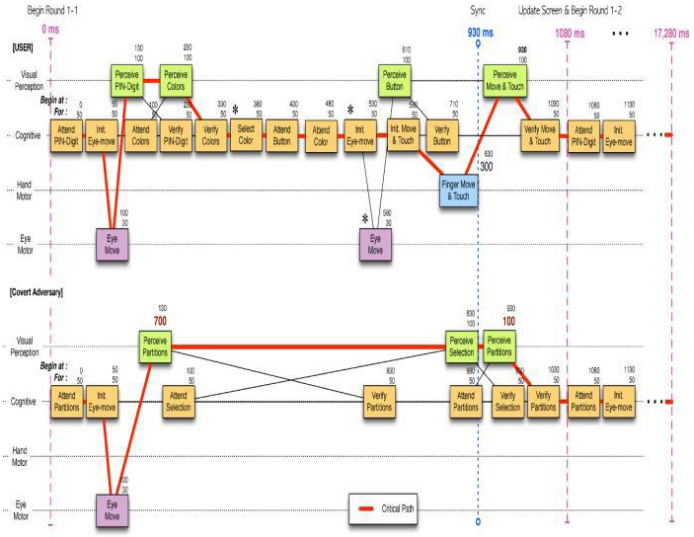


Figure 5: Performance Analysis of Multi Color Method.

The two graphs give the difference in the Black and White method and the Multi-color method. The difference in the position of the eye move shows the differentiation in the way in which the user enters the number for authentication. Also the length of the critical path tells the critical region faced by the user in both the methods. Critical region last longer in the Black and White method when compared to our proposed method in the design part. The graph clearly explains the difference in the working steps and the difficulties of the Black and White method and our proposed method.

B. Authentication & Services

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 Application 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.

IV. 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 counterattack of humans against the system, previously evaluated to be secure. What we have learned from the weaknesses of the improved 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 this multi-color number panel for resolving this problem because it is effective in modeling a skilled user. The estimated performance in our modeling was quite close to the experimental results. Our novel idea of modeling the adversary was also effective in analyzing security and devising an improved method. The new attack was successfully modeled and experimented. It was interesting that participants who enjoy fast-paced video games were better at shoulder surfing, and the training effect was remarkable. The proposed system is effective in achieving the output in a time span less than what the Black and White method took for producing the output. Also has a good critical path variation in the design part rather than with user interface difficulty of our proposed system.

V. ACKNOWLEDGEMENT

We express our sincere gratitude to our concerned guide Asst. Prof. Mrs. Pranamita Nanda, Department of computer science and engineering, for her inspiring guidance towards the progress on the topic "SHOULDER SURFING" and her valuable information for the development of our paper. We would like to get experts comments to help improve our paper.

VI. 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.

[10] A. D. Luca, K. Hertzschuch, and H. Hussmann, "ColorPIN-securing PIN entry through indirect input," in Proc. ACM SIGCHI Conf. Human Factors Comput. Syst., 2010, pp. 1103–1106.

[11] N. Hopper and M. Blum, "Secure human identification protocols," in Proc. Adv. Cryptology-ASIACRYPT, 2001, pp. 52–66.

[12] D. Weinshall, "Cognitive authentication schemes safe against spyware," in Proc. IEEE Symp. Security Privacy, May 2006, pp. 295–300.

[13] P. Golle and D. Wagner, "Cryptanalysis of a cognitive authentication scheme," in Proc. IEEE Symp. Security Privacy, May 2007, pp. 66–70.

[14] 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.

[15] P. Dunphy, A. P. Heiner, and N. Asokan, "A closer look at recognitionbased graphical passwords on mobile devices," in Proc.