Abstract — In computer security, shoulder surfing refers to using direct observation techniques, such as looking over someone's shoulder, to get information. It is commonly used to obtain passwords, PIN security codes, and similar data. Shoulder surfing can also be done at a distance using binoculars or other vision-enhancing devices. Inexpensive, miniature closed-circuit television cameras can be concealed in ceilings, walls or fixtures to observe data entry. To prevent shoulder surfing, it is advised to shield paperwork or the keypad from view by using one's body or cupping one's hand. 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. The novel approach called covert attentional shoulder surfing indeed can break the well known PIN entry method previously evaluated to be secure against shoulder surfing. Another contribution is the formal modeling approach by adapting the predictive human performance modeling tool for security analysis and improvement. 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. 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.

I INTRODUCTION

The 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. For example, a combination of an SSA and stolen or Skimmed material such as a magnetic card or a mobile device enables an attacker to obtain a victim’s private information and to withdraw money from that victim’s account.

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.

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 implementation of BW method and IBW method are as follows which is done by Perceptual Grouping and Covert Attention.
BW also referred as BLACK AND WHITE method came into play when the user will go with ATM service in mobile app. The BW method partitions a set of ten digits into two random halves i.e. Black and White, of which one is selected according to the user’s key entry in each round. Consecutive rounds will be proceeded to identify single pin. It consists of 4 iterations. Each iteration follows conceptual grouping. This BW method consists of four iterations each iteration process refers to pin entry of single pin.

So there exist four color groups on the numeric keypad and two colors for every numeric key. The adversary who launches covert attention 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.

The proposed system is 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.
automatically clustered to determine the user’s selected symbol; this approach has the benefit of allowing users to authenticate at their natural speed, rather than with a fixed dwell time. Additionally, the absence of a visible trigger does not divulge the number of symbols in the password. Results from preliminary investigations indicate that quick (3 seconds for a 4 digit PIN) authentication is possible using this scheme, but more work is needed to account for calibration error, and to dynamically adapt system parameters to the characteristics of individual users.

Daphna Winchell from School of Computer Science and Engineering, proposed paper “Cognitive Authentication Schemes Safe against Spyware” [3]. In this paper proposed the challenge response entry on publicly observable Touch Screens” [4]. This paper proposed about the present the proposed protocols drawbacks: First, training is required to familiarize the user with the secret set of pictures. Second, depending on the level of security required, entry time can be significantly longer than with alternative methods. It described the user studies showing that people can use these protocols successfully, and quantifies the time it takes for training.

Desney S. Tan, Pedram Keyani, Mary Czerwinski, they proposed paper titled “Spy-Resistant Keyboard: Towards More Secure Password Entry on Publicly Observable Touch Screens” [4]. This paper proposed about the present the Spy-Resistant Keyboard, a novel interface that allows users to enter private text without revealing it to an observer. They described a user study that ran to explore the usability of the interface as well as additional security provided by it. Results indicate that although users took longer to enter their passwords, using the Spy-Resistant Keyboard rather than a standard onscreen soft keyboard resulted in a drastic increase in their ability to protect their passwords from a watchful observer.

II PROJECT MODULES

The project will include the following main tasks:

- User Registration and E-Mail
- Black and White BW-Method
- Improved Black and White IBW-Method
- Session Key Method
- Authentication and Services

III SECURITY NOTIONS FOR PIN-ENTRY METHODS

In this section, we define the criteria used to evaluate the security of a PIN entry method. We adopt a quantitative approach so that the vulnerability of a method may be numerically represented. We are particularly interested in two major threats, shoulder-surfing attacks and guessing attacks, and the trade-off between them. In our model, we define a tester as the target system that performs authentication, such as an ATM or a mobile device. A legitimate user and an attacker try to pass the PIN-entry test requested by the tester.

A. Guessing Attack

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 [10]–[12]. 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.

B. Shoulder Surfing Attack (SSA)

In a shoulder-surfing attack, the attacker observes the logon procedure by looking over the user’s shoulder, and tries to recover that user’s PIN. The strongest variant of this attack is a recording attack (RA), in which the attacker employs a recording device to record the entire authentication recording session. Let us call an attack without any recording device a human shoulder-surfing attack (HSSA).

IV. NEW PIN-ENTRY METHOD

On the basis of the above guidelines, we present a new PIN-entry method. The basic layout of our method comprises a horizontal array of digits from 0 to 9 and randomly arranged colors.

A. Black and White Method/ BW 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.

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.

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.

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, 1, 2, 3, 4, 5, 6, 7, 8, 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 PIN digits are identified.
ALGORITHM FOR IMPROVED PIN ENTRY: PSEUDO
CODE
{ *comment *}
1: A, B ← γ(p(A)) { *primary sets: A, B, C, D *}
2: C, D ← γ(p(A))
3: O, P ← (Ø, Ø) { *eliminated sets: O, P, Q, R *}
4: Q, R ← (Ø, Ø)
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 *}
{ *remaining splits of C∪R in c, D∪Q in d *}
8: input choice ∈ {a, b, c, d} { *user’s input *}
{ *partition the chosen and the other sets *}
9: if choice = a then
10: Q, R ← γ(p(O∪P∪B))
11: O, P ← γ(p(O∪P∪B))
12: C, D ← γ(p(A))
13: A, B ← γ(p(B))
14: else if choice = b then
15: Q, R ← γ(p(O∪P∪A))
16: O, P ← γ(p(O∪P∪A))
17: C, D ← γ(p(B))
18: A, B ← γ(p(B))
19: else if choice = c then
20: O, P ← γ(p(Q∪R∪D))
21: Q, R ← γ(p(Q∪R∪D))
22: A, B ← γ(p(C))
23: C, D ← γ(p(C))
24: else
25: O, P ← γ(p(Q∪R∪C))
26: Q, R ← γ(p(Q∪R∪C))
27: A, B ← γ(p(D))
28: C, D ← γ(p(D))
29: end if
30: end for { *for loop runs for m rounds *}
31: return A { *a single digit is identified *}

C. Session Key Method
We propose Session key Method. It is a new PIN-entry method. The basic layout of our method comprises a vertical array of digits from 0 to 9, juxtaposed with another array of ten familiar objects such as + and / etc.

For simplicity, we assume that the number of digits in PIN is four, although the proposed method may be applied to any case with N ≥ 2 digits. We need a total of four rounds. The first round is the session key decision round, and the remaining three rounds are PIN-entry rounds. In the session key decision round, ten randomly arranged objects are displayed to the user. The user recognizes the symbol immediately below the first digit of his/her PIN as the temporary session key and presses “OK.”

In the example shown where the PIN is 2371, the user recognizes symbol as the session key because it is collocated with the first digit of the PIN, 2. The remaining rounds are PIN-entry rounds, in which the i th digit of the PIN is entered in their i th round for i = 2, 3, 4.

In each of these rounds, the user is again given a random array of ten objects, and s/he enters a PIN digit by rotating the object array and aligning the session key with the current PIN digit. For this task, the user can use two additional buttons (“Left” and “Right”).

In the example round shown the user presses the “Right” button twice so that symbols moves to the position immediately below 3, and then presses “OK.”

D. 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 PIN is 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 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.

V 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. 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.

VI REFERENCES


Second Author Mrs V.Valarmathi, Master of Technology I Information Technology, working as an Assistant Professor in SKR Engineering College.