IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON INNOVATION AND APPLICATION OF INTERNET OF THINGS AND EMERGING TECHNOLOGIES IN SMART SENSING

Received August 8, 2019, accepted August 21, 2019, date of publication August 28, 2019, date of current version September 13, 2019.

*Digital Object Identifier 10.1109/ACCESS.2019.2937948*

# On Overcoming the Identified Limitations of a Usable PIN Entry Method

**NILESH CHAKRABORTY[1], JIANQIANG LI[1], SAMRAT MONDAL[2], (Senior Member, IEEE), FEI CHEN[1], AND YI PAN[3], (Senior Member, IEEE)**

[1]College of Computer Science and Software Engineering, Shenzhen University, Shenzhen 518060, China
[2]Department of Computer Science and Engineering, IIT Patna, Patna 801106, India
[3]Department of Computer Science, Georgia State University, Atlanta, GA 30302-5060, USA

Corresponding author: Jianqiang Li (lijq@szu.edu.cn)

This work was supported in part by the National Science Foundation of China under Grant U1713212, Grant 61572330, 61836005, and Grant 61702341, and in part by the Technology Planning Project of Shenzhen City under Grant JCYJ20170302143118519, Grant GGFW2018021118145859, and Grant JSGG20180507182904693.

**ABSTRACT** In the domain of password security, research has made significant progress in handling different kinds of threats which require human intelligence factor to fix the vulnerabilities. In spite of having strong theoretical establishments, most of these defense mechanisms cannot be used in practice as humans have limitations in processing complex information. The little bit of good news is that very few research proposals in this field have shown the promises to be deployable in practice. This paper focuses on such one method - proposed by Roth *et al.* back in 2004, which provides adequate user-friendliness to enter Personal Identification Number (PIN) securely in the presence of human shoulder surfers. Surprisingly, the background algorithm of this method for validating users' responses runs in linear time on a search space of cardinality 5 and hence, the validation process does not put much load on the authenticating device. Therefore, such human identification protocol can also be integrated into the IoT infrastructure for conducting a more secured login from the client-side. Having such advantages, though remained secure for almost ten years after its release in 2004, recently, few proposals revealed some serious vulnerable aspects of the Roth *et al.*'s proposal. In this paper, we have taken an attempt to save this user-friendly form of authentication. Firstly, we have made a critical discussion on the importance of the targeted PIN entry method in the domain of usable security and then given a brief overview of the identified limitations of this protocol. Followed by this, a few initiatives have been taken to fix the identified vulnerabilities of Roth *et al.*'s proposal by revising its working principle, while the login procedure and the usability standard of this method stay unaffected.

**INDEX TERMS** Authentication, PIN, observation-attack, key-logger-attack, defense, human-intelligence-factor.

## I. INTRODUCTION

Despite its several limitations, the password seems to be the predominant form of user verification for the foreseeable future [7]. To initiate the password-based authentication, a user ($\mathcal{H}$) needs to submit the login credentials – generally username and password, through a user-interface (UI). In some malicious environments, these login credentials can be observed by an adversary ($\mathcal{A}$), standing next to $\mathcal{H}$. The observed information can later be used by $\mathcal{A}$ to impersonate the genuine $\mathcal{H}$. Hence, password-based authentication is prone to this relatively non-technical observational attack [21], [30].

The associate editor coordinating the review of this article and approving it for publication was Shaojie Tang.

### A. THREAT MODEL

There are several setups for password-based authentication consisting of logical and physical IDs. The basic idea behind such infrastructure is pretty simple. At the registration phase, $\mathcal{H}$ shares a set of information with a system ($\mathcal{M}$) and remembers a part of it – typically, username and password – for subsequent entry at the UI for authentication. If the entered username and password get matched with the corresponding pre-shared information, then only $\mathcal{M}$ allows the login and denies otherwise.


This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see http://creativecommons.org/licenses/by/4.0/

In this paper, we have focused on a passive $\mathcal{A}$ performing shoulder surfing based on a weaker threat setup. In other words, the role of $\mathcal{A}$ is played by a human (but not a system) to observe the interactions between $\mathcal{H}$ and $\mathcal{M}$ at UI so that $\mathcal{H}'$s login credential can be aquired. Following this threat model, though $\mathcal{A}$ should not posses any recording device (*e.g.,* miniature camera), some manual tools like pencil and paper can be used to make the breach happen [30].

*An extended coverage of the threat model* could also be given $\mathcal{A}$ the power to compromise the keypad of the system (*i.e.,* performing key-logger based attack [31]) when the device of the screen and the keypad are *not* integrated (*e.g.,* ATM or *Automated Teller Machine*). ***To be precise****, from the subsequent discussions in this paper, the readers will understand that the threat model allows* $\mathcal{A}$ *to record* $\mathcal{H}'$*s responses but not the generated challenges by* $\mathcal{M}$. The UI of the defense mechanisms for preventing weak shoulder surfing (or observational) attack must ensure that $\mathcal{H}$ should feel safe and secure while transcribing the login credentials in presence of humans around the login device.

### B. IDENTIFYING THE IMPACT OF THE THREAT FROM A LARGER PERSPECTIVE

Nowadays $\mathcal{H}$ uses almost the same or identical information in accessing multiple web services and IoT enabled technologies (some are more important than the others) [10]. Therefore, even a partial leakage of such information is not at all desirable. One of the popular forms of passwords is a four-digit PIN (or Personal Identification Number) which is more susceptible to observational attacks because of its shorter length and simple UI, consisting of a ten-digit numeric keypad. Since PINs are used in various kinds of devices (*e.g.,* ATM, smartphones, point of sale terminals, android applications in IoT framework [19] *etc.*) hence, protecting $\mathcal{H}'$s PIN against the observational attack has become a matter of absolute necessity. However, most of the research proposals have failed to provide a suitable environment for authentication because of the involvement of $\mathcal{H}'$s intelligence factor which seeks a strong balance between the security and usability aspects [40], [42].

### C. MOTIVATIONS AND CONTRIBUTIONS

Observational attacks can be considered as a much weaker (though prominent) form of *recording attacks*, which allow $\mathcal{A}$ to record complete interactions between $\mathcal{H}$ and $\mathcal{M}$. Since 1991, many defense strategies have been proposed to address different forms of recording attack; however, to date, very little have succeeded to gain popularity among the users. There is absolutely no doubt that most of these authentication services provide desired security standards. However, they often failed to meet an acceptable usability standard [40].

Despite such long-standing conflicts between security and usability aspects, in 2004, Roth *et al.* proposed a highly usable authentication procedure which could resist the threat of observational attack [30]. Though remained secure for almost 10 years after its release, in 2014, Kwon *et al.* showed that proposed method by Roth *et al.* fails to provide security against the observational attack [21]. In fact in [20] also, the authors spotted several drawbacks in Roth *et al.*'s work and puts an end on the acceptability of this usable and *known-to-be* secure authentication protocol. The urge of saving this user-friendly form authentication procedure primarily motivated us behind this work and following is the list of contributions made in this paper.

***Contribution 1:*** We have performed an extensive literature survey by identifying different variations of recording attacks and its weaker forms for capturing $\mathcal{H}'$s login credentials and spotted the notable existing defense strategies for handling such threats. Precisely, the outcome of this contribution gives an indication on how hard it is to design a *usable-secure* authentication technique for preventing such kind of threats and how proposed method by Roth *et al.* is an exception in meeting such a criterion.

***Contribution 2:*** We have revisited Roth *et al.*'s work and highlighted the drawbacks of this method reported in [20], [21]. Under the light of this discussion, we have also given a clear indication that proposed protocol by Kwon *et al.* [21] – for overcoming the limitations of Roth *et al.*'s mechanism, is not free from all the faults identified in [20].

***Contribution 3:*** We have modified Roth *et al.*'s proposal to fix all its vulnerable aspects reported in [20], [21]. More importantly, by keeping the login procedure almost same to the Roth *et al.*'s work in [30], our proposal allows no degradation in the usability standard. We have conducted a simulated experiment for entering $1.6 \times 10^6$ random PIN digits to the modified protocol and, demonstrated both $\mathcal{H}'$s and $\mathcal{A}'$s behaviours in the improved environment with the help of a human performance modelling toll – CPM-GOMS [17]. While the experimental result suggests that proposed modifications eliminate all the drawbacks reported in [20], the outcome of CPM-GOMS certifies that the improved method is free from the fault shown in [21].

### D. ROADMAP

Following is the organization of the paper. In Section II, we have given a sketch on the progress made so far in handling the threats related to recording attack and its different forms. In Section III, we have revisited the working principle of Roth *et al.*'s proposal and given a brief overview of the identified drawbacks of this method. In Section IV, we have taken a few initiatives to address the issues mentioned in the previous section. In Section V, we have given an insight on the strength of the proposed improvement from both the security and usability perspectives and compared our proposal with two very closely related proposals in this domain. Finally, we have drawn conclusive remarks in Section VI.

## II. RELATED WORK

The defense mechanism for handling recording/observation attack typically follows a *challenge-response* strategy where $\mathcal{M}$ generates a *challenge* (or puzzle) ($c$) and based on her

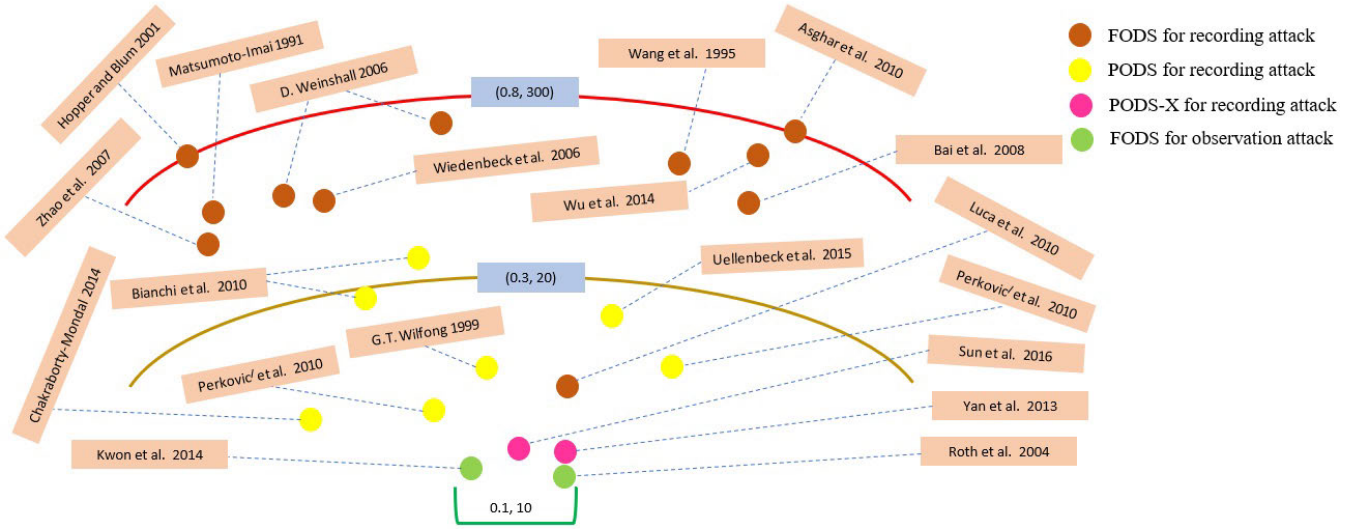


**FIGURE 1.** Performance of methods for meeting $\beta = 0.1$ and $t = 10$. The value on a arch represents order of human executability of a method falling on that arch.

original password ($p$), $\mathcal{H}$ answers to it. An answer from $\mathcal{H}$ can be considered as a response ($r$) to $c$. Existing literature [25], [40], [42] suggest that such a defense strategy can broadly be classified into two categories – (i) *Fully Observable Defense Schemes* (FODS) and (ii) *Partially Observable Defense Schemes* (PODS). Following the earlier defense model, $\mathcal{A}$ is allowed to record both $c$ and $r$. In contrast, PODS assumes that $c$ is communicated through a secure link and hence, $\mathcal{A}$ cannot access to it. *Notably*, this is a strong assumption which is very hard to be satisfied in practice [40]. After a thorough investigation, we have identified that existing methods for preventing the threat of recording/observational attack belong to one of the following four categories.

- ***FODS for recording attack*** [43] ensure that even if (with the help of recording device) $\mathcal{A}$ records both $c$ and $r$, she still cannot recover intended $p$ immediately from the recording evidence.
- ***PODS for recording attack*** [25] assure security against the recording attack only if $\mathcal{A}$ cannot access communicated $c$ by $\mathcal{M}$.
- ***PODS-X for recording attack*** [34] are not different from PODS except the fact that for using such a method, $\mathcal{H}$ carries an extra responsibility of hiding $c$ (or a part of it) from $\mathcal{A}$. However, such kind of methods carry the drawback of PODS and often get exposed to $\mathcal{A}$ due to the created *open visual-cone* by a unaware $\mathcal{H}$ [41].
- ***FODS for observation attack*** [30] carry the authentication procedure in presence of $\mathcal{A}$ who follows the threat model mentioned in Section I.

The expected usability standard provided by these methods should be substantially high as they are executed by human users who are the weakest link in the computer security [2]. In 2001, Hopper and Blum bring the concept of ($\alpha$, $\beta$, $t$)$-$*human executability* which defines the usability standard of such a method [15]. Following is the definition.

*Definition 1:* A protocol is said to be ($\alpha$, $\beta$, $t$) $-$ human executable if at least $(1 - \alpha)$ portion of the human population can perform the necessary computations for login and without errors in at most t seconds, with probability greater than $(1 - \beta)$.

The authors also suggested that to be user-friendly, a protocol should be (0.1, 0.1, 10)-*human executable*. After a careful analysis, we have found that most of the works in this domain omit $\alpha'$s value and hence, their usability standard can only be judged by the remaining two parameters $-$ $\beta$ and $t$. In Figure 1, we have shown where the existing methods belong to meet $\beta = 0.1$ and $t = 10$. The target $\beta = 0.1$ and $t = 10$ has been represented by a bucket in this figure and readers can immediately see that though comes to very close, no method, to date, falls into the bucket. The arches in the figure represent an order of *human executable* for different values of $\beta$ and $t$. A method on an arch perfectly satisfies the corresponding order of *human executable*. Also, a method above and below an arch represents a higher and lower order of *human executable* compared to that arch, respectively.

The above figure shows that proposed FODS by Hopper and Blum in [15] and Asghar *et al.* [3] are order of (0.8, 300)-*human executable* and hence, cannot be executed by a common $\mathcal{H}$. Though other FODS proposed in $-$ [4], [24], [36]–[38], [43], reduce this order, they remain far from even twice to the desired value. In contrary, proposed FODS in [12] gets much closer to this standard, however, it can protect $p$ mostly for two sessions by putting almost double memory overhead on $\mathcal{H}$ (needs to remember a PIN of length 8) [11]. Readers can get another insight from the figure: a PODS provides better usability standard compared to an FODS. However, a PODS sending $c$ in the form of vibration signal [5], [6], [35] often has more usability overhead compared to a PODS communicating $c$ in the form of audio signal [9], [25], [26], [39]. Though some PODS maintain

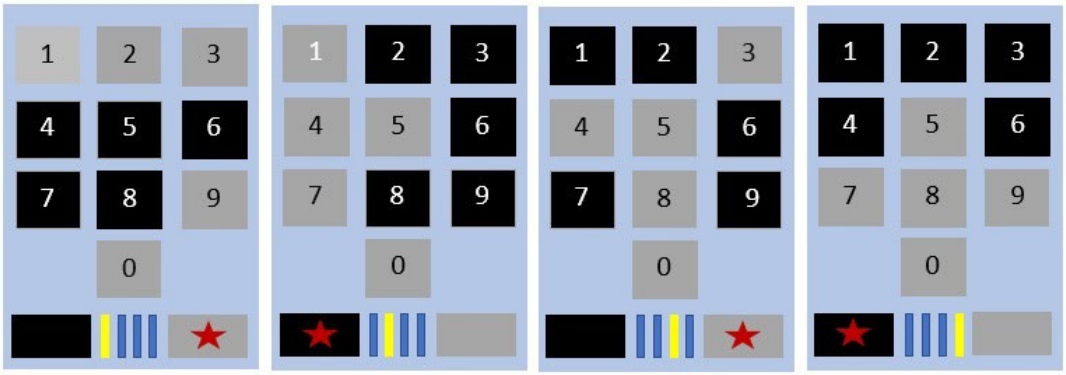


**FIGURE 2.** $\mathcal{H}'$s interaction with IOC BW method in four consecutive rounds for entering complete information about PIN digit 3. "$*$" indicates pressed color button by $\mathcal{H}$.

much shorter distance from the target [9], they ensure security based on communicated $c'$s secrecy which is hard to achieve in practice [40]. The methods belonging to PODS-X category seem to take one step closer in meeting $\beta = 0.1$, $t = 10$ [34], [41]. However, they solely depend on $\mathcal{H}'$s capability in hiding $c$ and if $\mathcal{H}$ fails to do so (because of the open visual cone [41]) then without even using any recording device, $\mathcal{A}$ can easily recover $p$ [41].

The discussion so far suggests that even most usable methods cannot meet the expected goal of usability standard and these methods have some serious security limitations. Hence, when it seemed almost impossible to design a method guaranteeing a strong balance between usability and security aspects, in 2004, Roth *et al.*'s proposal brought the first ray of hope for addressing this conflict [30]. They proposed two solutions − *Immediate Oracle Choice* (IOC) variation and *Delayed Oracle Choice* (DOC) variation, for addressing their targeted threat model (*i.e.,* observational attack) and their proposal almost reaches to the goal − $\beta = 0.1$ and $t = 10$. As the inventors of the protocol have used black and white colors for designing the UI, hence, in this literature, we have identified this weak shoulder surfing resilient method by Black-and-White or *BW* method. Though this user-friendly form of authentication remained secure for almost ten years after its release, proposals from Kwon *et al.* in 2014 and 2015 have identified several security limitations of BW method [20], [21]. Kwon *et al.* also came up with a new strategy (in [21]) which limits the risk of observational attack by providing almost the same level of usability standard. However, in Section III, we will show that the authors' proposal in [21] suffers from some of the limitations identified in [20]. Therefore, by getting close to the desired usability standard, research in this domain still seeks for a solution for preventing any form of recording/observation attack.

## III. REVISITING IOC BW METHOD

As mentioned in the previous section, Roth *et al.* proposed two variations of BW method − IOC BW and DOC BW methods, for dealing with the considered threat model in this paper. Both IOC BW and DOC BW methods work in the same fashion except the fact that the latter one at first shows 4 consecutive numeric keypads which can identify any single PIN digit and then asks $\mathcal{H}$ to enter the 4−length response sequences. From $\mathcal{H}'$s responses, DOC BW then identifies the intended PIN digit uniquely. In [30], Roth *et al.* showed that DOC BW is a more powerful model than the IOC BW method for defeating $\mathcal{A}$. However, the report in [20] proved that DOC BW method may not always resolve the ambiguity from $\mathcal{H}'$s responses and hence, correct responses by $\mathcal{H}$ may also lead to a login failure. The incapability of DOC BW method of validating a genuine $\mathcal{H}$ from the sequence of correct responses puts an end to its acceptability to the research community. Therefore, some salient research in this domain have only dealt with the other variation of the BW method [20], [21] and this study also is no exception to that.

With a little overhead of entering each PIN digit in multiple (precisely four) rounds, following interaction happen between $\mathcal{H}$ and $\mathcal{M}$ in each round for accomplishing a login session by using IOC BW method.

- $\mathcal{M}$ divides the conventional numeric keypad consisting of ten digits into two equal halves.
- One half gets white and the other half gets black colors.
- $\mathcal{H}$ identifies the color, which appears on her PIN digit and presses the corresponding color button as a response.

The color buttons for accepting $\mathcal{H}'$s responses are placed below the UI. In Figure 2, we have shown an example for entering a single PIN digit in four consecutive rounds by $\mathcal{H}$ through the UI of IOC BW method. In each round, after receiving the response, the size of the group containing the original PIN digit decreases logarithimically [30]. Hence, at the end of the fourth round, correct responses by $\mathcal{H}$ creates a group size of cardinality one, containing the original PIN digit only. In Algorithm 1, we have presented the working principle of IOC BW method (courtesy: [20]).

The operator $\gamma \circ \pi$ in Algorithm 1 derives two sets of similar sizes from the given parameter. Following is the brief description of $\gamma \circ \pi$ operator. Let cardinality of two sets $\mathcal{Q}$ and $\widehat{\mathcal{Q}}$ be denoted by $q = |\mathcal{Q}|$ and $\widehat{q} = |\widehat{\mathcal{Q}}|$, respectively. $\gamma \circ \pi$ operator divides

**Algorithm 1** IOC BW (Systematic Authentication Procedure)

**Initialize:** $\mathcal{Q} := \{0, 1, \ldots 9\}$; $\widehat{\mathcal{Q}} := \emptyset$
**for** round = 1 to 4 **do**
  (L, R) $\leftarrow \gamma \circ \pi(\mathcal{Q})$; (O, P) $\leftarrow \gamma \circ \pi(\widehat{\mathcal{Q}})$;
  *display* in_Black = L $\cup$ P; in_White = R $\cup$ O;
  [$\mathcal{H}$ submits PIN color by hitting black/white button];
  receive $\mathcal{H}'$s input: choice $\in$ {black, white};
  **if** (choice = black) **then**
    $\mathcal{Q} \leftarrow$ L; and $\widehat{\mathcal{Q}} \leftarrow \widehat{\mathcal{Q}} \cup$ R;
  **else**
    $\mathcal{Q} \leftarrow$ R; and $\widehat{\mathcal{Q}} \leftarrow \widehat{\mathcal{Q}} \cup$ L;
*return* $\mathcal{Q}$;

- $q$ into $\lceil \frac{q}{2} \rceil$ and $\lfloor \frac{q}{2} \rfloor$.
- $\widehat{q}$ into $\lceil \frac{\widehat{q}}{2} \rceil$ and $\lfloor \frac{\widehat{q}}{2} \rfloor$.

Followed by the aforementioned procedure, this operator assigns

- $\lceil \frac{q}{2} \rceil$ and $\lfloor \frac{q}{2} \rfloor$ elements to the sets L and R, respectively.
- $\lceil \frac{\widehat{q}}{2} \rceil$ and $\lfloor \frac{\widehat{q}}{2} \rfloor$ elements to the sets O and P, respectively.

Based on $\mathcal{H}'$s response, the set $\mathcal{Q}$ holds the *probable candidates* for a PIN digit and $\widehat{\mathcal{Q}}$ contains the *rejected candidates*. It is not hard to see that for the initial values of $q = 10$ and $\widehat{q} = 0$, $q + \widehat{q}$ yields to 10 in each round of the algorithm. With the brief introduction to the essential facts related to the IOC BW method, next, we will discuss the *identified drawbacks* (**ID**) of this login setup.

### A. ID BASED ON THE DESIGN OF IOC BW METHOD

In Algorithm 1, we have shown how authentication process is carried out by IOC BW method. On a closer look, it can be seen that

- Prior to receiving $\mathcal{H}'$s response in the first round, five numeric keys get white and other five get black color. Therefore, the ratio of black and white button presses (as a response) in the first round would always be 1 : 1.
- In the second round, three probable candidates for intended PIN digit get black and two get white color. This indicates that the ratio of black and white button presses in the second round would be 3 : 2.
- If $\mathcal{H}$ hits white color button as a response in the second round, then the ratio of black and white button presses in the third round would again be 1 : 1. However, in this case, the intended PIN digit will be obtained from the submitted response in the third round only. The fourth round will become a *redundant* round in this scenario where, in the fourth round, $\mathcal{H}$ will always press the black button.

The aforementioned discussion indicates that IOC BW method has a biasness in receiving black color as a response. In [20], authors portrayed this fact more systematically to prove that the ratio of black and white button presses in IOC BW method is 5 : 3. The authors also simulated 400, 000 random PIN digit entries (each takes 4 rounds) by using IOC BW method and showed that black and white colors were pressed for 1, 000, 449 and 599, 551 times, respectively, during 1, 600, 000 rounds. Hence, the ratio of black and white key presses was observed as 1.67 : 1. Due to this unbalanced ratio between the responses, Kwon *et al.* also reported that from the 4, 00, 000 response sequences, they ***never found*** the following six response patterns − BBWW, BWBW, BWWW, WBWW, WWBW and WWWW. (ref. to page 4, *Section* B in [20]). In a nutshell, it is inferable that $\mathcal{A}$ is more likely to choose the correct responses if she selects the black color. The overall success probability of guessing the 4−length response sequence also increases to $1/10$ due to the absence of some of the response patterns.

Furthermore, the round redundancy in IOC BW method helps in increasing the efficiency of $\mathcal{A}$ in obtaining the original PIN digit as the redundant round puts no load on $\mathcal{A}'$s concentration, performing the covert-attentional shoulder surfing attack (a brief description of the threat model has given in the next section). Kwon *et al.* proved that one of the four rounds in IOC BW method is redundant with the probability 0.53 [20]. Two IDs coming out from the aforementioned discussions have been summarized below.

**ID-I:** IOC BW method suffers from round redundancy (*i.e.,* sometimes 4 rounds may not at all be required to identify a PIN digit) and this allows $\mathcal{A}$ to improve her efficiency while performing the covert-attentional shoulder surfing attack [20].

**ID-II:** The black and white key presses during PIN entries in IOC BW method are unbalanced. Kwon *et al.* showed that response from $\mathcal{H}$ tends more towards black color in IOC BW method. Such a biasness in responses can also be exploited by $\mathcal{A}$ for performing the guessing attack to weaken the security standard of the scheme [20].

### B. ID BASED ON THE COGNITIVE CAPABILITIES OF $\mathcal{H}$

The considered threat model in this paper limits the strength of $\mathcal{A}$ as no external resources (*e.g.,* concealed camera) can be used for performing the attack. Despite this limitation, the major threats on IOC BW method come from the amazing facts related to $\mathcal{H}'$s (and as a matter of facts $\mathcal{A}'$s too) cognitive capabilities studied and established in the literature of cognitive psychology and neuroscience. For example, the *visual short term memory* (VSTM) of human is capable of storing about four integrated objects in it [23], whereas the fragile VSTM exceeds this limit [33].

Form the working principle of IOC BW method, readers can notice that the group containing the original PIN digit of $\mathcal{H}$ contains maximum five elements or probable candidates in it and the group size decreases subsequently in the following rounds. The capacity of VSTM and group size in IOC BW method play a key role in the authors' proposal in [21] for compromising the security of this method. We have summarized the proposed attack model by Kwon *et al.* in the form of the Algorithm 2.

Based on the Gestalt principles [22] the formation of groups in the *Step* 3 of this algorithm is performed by

**Algorithm 2** Attack Model on IOC BW

1: **for** round $=1$ to 4 **do**
2: **if** (round $=1$) **then**
3: $\mathcal{A}$ forms and eyes on two numeric groups $\mathcal{G}$ containing five black and five white numeric digits**;**
4: **else**
5: $\mathcal{A}$ eyes on the group $\mathcal{G}$ containing the original PIN digit**;**
6: $\mathcal{A}$ *observes* the color response $r$ by $\mathcal{H}$**;**
7: **if** (round $=1$) **then**
8: $\mathcal{A}$ selects the group $\mathcal{G}$ corresponding to $\mathcal{H}'$s color response and discards the other one**;**
9: **else**
10: $\mathcal{A}$ performs *some computations* $\varphi(\mathcal{G}, r)$ which returns a group $\mathcal{G}^{/}$ which is a subgroup of $\mathcal{G}$**;**
11: $\mathcal{A}$ mentally replaces $\mathcal{G}$ by $\mathcal{G}^{/}$**;**
12: $\mathcal{A}$ identifies the original PIN digit from the singleton group $\mathcal{G}$**;**

perceptual grouping of objects of two reverse colors – black and white, [13], [16]. Instead of recognizing each colored numeric key individually, the formation of such groups reduces the number of information in VSTM. From the obtained $r$, *some computations* $\varphi(\cdot)$ in *Step* 10 of the Algorithm 2 indicates perceptual grouping operation on the numeric keys having the same color [21]. By suppressing saccadic eye movements, parafoveal vision helps $\mathcal{A}$ in *Step* 6 to observe the color response by $\mathcal{H}$ [29]. Foveal vision range of $\mathcal{A}$ comes into play for performing the perceptual grouping and reduce the group size in *Step* 10 [29]. The higher memory-bound of VSTM is capable of storing maximum information displayed in *Step* 3 for performing the attack and since then, each passing round reduces the load on VSTM. Therefore, mainly relying on the capacity of VSTM and perceptual grouping operation, $\mathcal{A}$ reveals the original PIN digit in *Step* 12. The attack strategy described in Algorithm 2 has been named as *covert-attentional shoulder surfing* by Kwon *et al.* [21]. Based on the discussion in this section, the following ID of IOC BW method can be summarized.

**ID-III:** IOC BW method fails to provide security against the covert-attentional shoulder surfers. The proposal from [21] shows that by performing a three-step operation – (a) covert attention [27], [29] (b) perceptual grouping [22] and (c) motor operation [8], the security of IOC BW method can be compromised.

**Faults in Kwon *et al.*'s proposal:** In [21] authors proposed an easy-to-use method which protects the PIN against the covert-attentional shoulder surfing attack while usability standard remains almost the same. However, their proposal fails to address *ID-I*. In fact, from the example set by Kwon *et al.* [21], the issue related to *ID-I* can be established immediately.

Figure 3 shows that from the response in *first round*, $\mathcal{M}$ derives $\{0, 3, 6, 7, 9\}$ as the probable PIN digits.

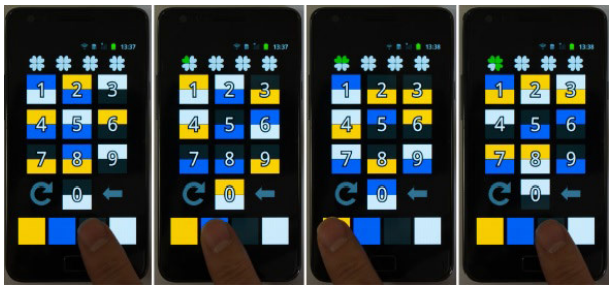

**FIGURE 3.** $\mathcal{H}'$**s interaction with Kwon *et al.*'s proposal in four rounds for entering PIN digit 6. This figure has been taken from Fig. 8 in [21].**

The response in the *second round* shrinks the set to $\{6, 7\}$. Finally, from the response in the *third round*, $\mathcal{M}$ derives the PIN digit 6 uniquely. Hence, the *fourth round* becomes a redundant one in this scenario.

## IV. PROPOSED MODIFICATIONS

In this section, we have aimed to modify the *ID*s of IOC BW method without affecting its usability standard. Our proposal under the scope of this section is three folds.

- First, we have incorporated noisy data in the design of the IOC BW method to eliminate the round redundancy. This initiative overcomes the weakness of IOC BW method when there are odd-sized sets of remaining candidate PIN digits.
- Followed by the aforementioned contribution, we have modified the procedure for assigning colors to the numeric keys in IOC BW method. This attempt brings the ratio of black and white key presses to almost $1:1$ to uniformize the distribution of colors.
- Finally, we have changed the order of entering responses in IOC BW method. The new ordering though keeps usability standard unaffected (verified by using CPM-GOMS tool [17] in Section V), it makes covert-attentional shoulder surfing attack much harder to perform.

We have named the modified version of the IOC BW method as *modified-IOC* BW or *MIOC BW*.

### A. ELIMINATION OF REDUNDANT ROUND

From the working principle of Algorithm 1, we can predict occurrences of the following situations in IOC BW method. Submitted response by $\mathcal{H}$ in the first round helps $\mathcal{M}$ to derive a set of 5 *probable PIN digits* before the beginning of the second round. After the second round, the set is then decomposed into two groups – one group of 3 numeric digits in black color and another group of 2 numeric digits in white color. In this situation, if $\mathcal{H}'$s PIN digit belongs to the group of cardinality 3, then after the completion of the second round, at max $\lceil \log_2^3 \rceil = 2$ more rounds will be required to distinguish the intended PIN digit uniquely. In contrast, if $\mathcal{H}'$s PIN digit belongs to the group of cardinality 2, then $\lceil \log_2^2 \rceil = 1$ more rounds will be sufficient for identifying the PIN digit and the fourth round will become a redundant one. Figure 4 depicts generation of a redundant round in IOC BW method.

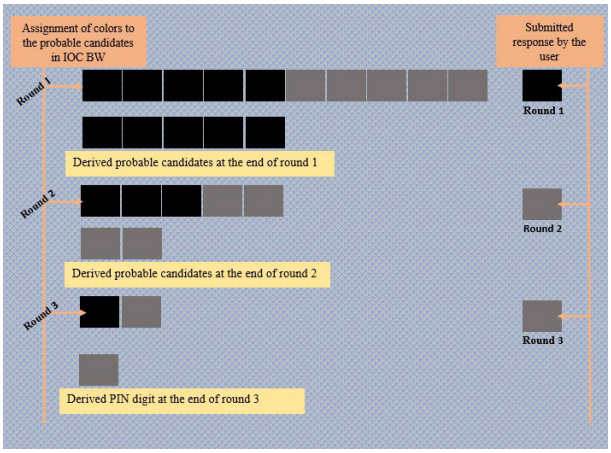


**FIGURE 4.** Response sequences in IOC BW method causing redundant round.

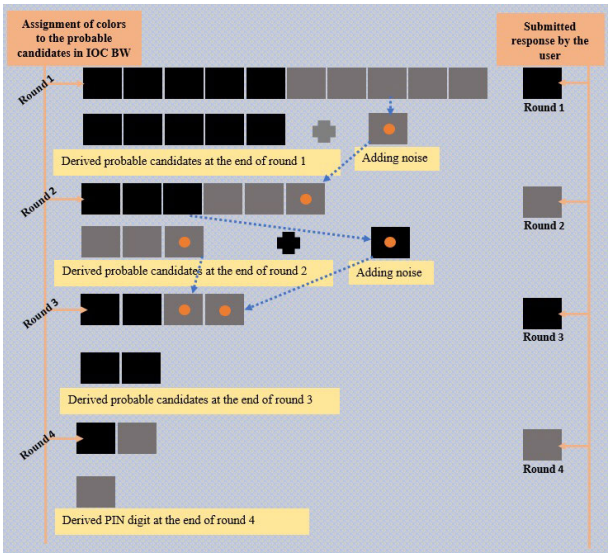


**FIGURE 5.** Eliminating redundant rounds in MIOC BW method based on the noisy digits. The square boxes marked by a dot indicate the noisy digits. The distribution of colors here still follows the proposed mechanism by Roth *et al.* in [30].

The incorporation of noisy digit takes care of the aforementioned issue. Readers can notice that with the help of a noisy digit, if the number of probable candidates in IOC BW method is increased from 5 to 6 at the end of the first round, then $\mathcal{H}$ should face $\lceil \log_2^6 \rceil = 3$ more rounds (at max) before $\mathcal{M}$ can identify the intended PIN digit by $\mathcal{H}$. The value of $\log_2^6$ yields to 2.59, which maintains almost the same distance from 2 and 3 and hence, there is a possibility that $\mathcal{H}$ sometimes may need to face only two more non-redundant rounds after submitting the response in the first round. Therefore, the addition of a single noisy digit *does not always ensure* the elimination of redundant round.

However, if we add another noisy digit to the set of 3 *probable candidates*, derived from the response in the second round, then the cardinality of this set will be increased to 4. Addition of noise in this stage confirms that after receiving a response in this round, $\mathcal{M}$ must conduct $\log_2^4 = 2$ more rounds to identify the PIN digit unambiguously. It can be noticed that a noisy digit is only being added to the set probable PIN digits of odd size and that too is selected randomly from the set of *rejected candidates*. Figure 5 depicts the elimination of redundant rounds in MIOC BW method.

*Remark 1:* The addition of noises ensures that response from $\mathcal{H}$ at the end of the second round derives a set of probable candidates having cardinality 4. This, in turn, indicates that at the end of the second round, $\log_2^4 = 2$ more rounds will always be required to identify the intended PIN digit uniquely. Therefore, by eliminating round redundancy, MIOC BW method puts more load on $\mathcal{A}$'s mind.

### B. ADJUSTING THE COLOR DISTRIBUTION IN MIOC BW

In Algorithm 1, it can be noticed that 3rd and 4th steps of the algorithm are responsible for the color distribution in IOC BW method. After adding noises to the set of *probable candidates* in Section IV-A, we have revised the color distribution property for MIOC BW method so that the omitted response patterns – mentioned in Section III-A, can be captured.

- *Firstly,* we have defined a function $\pi(\mathbb{S}, k, B, W)$ which primarily checks the validity of the argument $|\mathbb{S}| \geq k$. If the argument holds, the function assigns color "$B$" to randomly selected $k$ elements from the set $\mathbb{S}$. Followed by this step, $\pi(\cdot)$ allocates color "$W$" to the rest of the elements of set $\mathbb{S}$. The colored elements are finally returned to a set. *For example*, the added noise to the set $\mathcal{Q}$ ensures that the values of both $q$ and $\widehat{q}$ always stay even. Therefore, $\pi(\mathcal{Q}, \frac{q}{2}, \text{black}, \text{white})$ distributes both the colors in a uniform and random manner to the input set's elements.
- *Secondly,* we have defined an operator $\eta \circ \kappa$ which takes a set and a color as input parameters. From the inputs, it identifies the elements of the set marked by the input color. The identified elements are then may be returned to another set. *For example*, let $\eta \circ \kappa$ takes set $\mathbb{S}$ (containing colored numeric keys) and color $\overline{c}$ as inputs. The operator spots the digits in the set colored by $\overline{c}$ and the spotted digits are then returned to another set.
- *Finally,* we have defined a function *add_noise*$(\mathbb{S}_1, \mathbb{S}_2)$ which adds a digit to the set $\mathbb{S}_1$ from the set $\mathbb{S}_2$.

Based on the above notations, we have modified the Algorithm 1 (ref. to Section III) in the form of Algorithm 3.

#### 1) CORRECTNESS PROOF

*Step* 3 in Algorithm 3 suggests that a noisy digit is added to the set $\mathcal{Q}$ whenever $|\mathcal{Q}|$ becomes odd. Therefore, the value of $|\mathcal{Q}|$ always stays even. As $|\mathcal{Q}| + \widehat{\mathcal{Q}}$ yields to a even number, hence, the value of $|\widehat{\mathcal{Q}}|$ cannot also be odd. Now, function $\pi(\cdot)$ in *Step* 4 distributes both the colors black and white in a uniform manner to the set of probable candidates for PIN. Hence, the ratio between *black key press* : *white key press* by $\mathcal{H}$ should be 1 : 1.

**Algorithm 3** MIOC BW (Color Asignment Strategy)

**Initialize:** $\mathcal{Q} := \{0, 1, \ldots 9\}$; $\widehat{\mathcal{Q}} := \emptyset$
**for** round = 1 to 4 **do**
  **if** ($|\mathcal{Q}| = odd$) **then** add_noise($\mathcal{Q}$, $\widehat{\mathcal{Q}}$);
  $X \leftarrow \pi(\mathcal{Q}, \frac{q}{2}$, black, white);
  $Y \leftarrow \pi(\widehat{\mathcal{Q}}, \frac{\widehat{q}}{2}$, black, white);
  *display* $X \cup Y$;
  [$\mathcal{H}$ submits PIN color by hitting black/white button];
  receive $\mathcal{H}'$s input: choice $\in$ {black, white};
  **if** (choice = black) **then**
    $\mathcal{Q} \leftarrow \eta \circ \kappa(X$, black);
    $Y \leftarrow \eta \circ \kappa(X$, white); $\widehat{\mathcal{Q}} \leftarrow \widehat{\mathcal{Q}} \cup Y$;
  **else**
    $\mathcal{Q} \leftarrow \eta \circ \kappa(X$, white);
    $Y \leftarrow \eta \circ \kappa(X$, black); $\widehat{\mathcal{Q}} \leftarrow \widehat{\mathcal{Q}} \cup Y$;
*return* $\mathcal{Q}$;

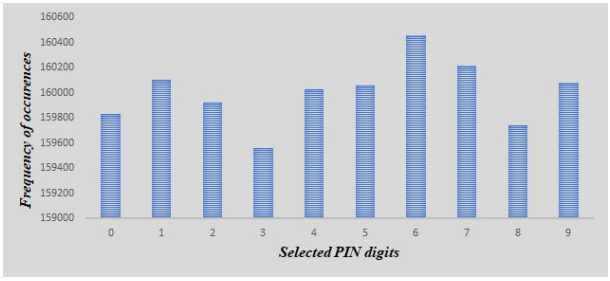


**FIGURE 6.** Frequencies of PIN digits which appeared as input in 1, 600, 000 run of MIOC BW method.

Based on Algorithm 3, MIOC BW method eliminates biasness in color distribution to the numeric keys and resolves the issue related to *ID-II*. Likewise in [20], we have conducted a simulation-based study to see the impact of our proposed improvement on the MIOC BW method.

#### 2) RESULT OF SIMULATION BASED STUDY

In [20], authors executed Algorithm 1 for $4 \times 10^5$ times and reported six omitted response patterns mentioned in Section III-A. Also, the ratio between *black key press* : *white key press* found to be 1.67 : 1. To perform a more extensive analysis, we have executed Algorithm 3 for $16 \times 10^5$ times (the login environment was simulated in NetBeans IDE 8.0.2.) and found that

- The ratio between *black key press* : *white key press* is improved to 1.004 : 1 (very close to the ideal ratio 1 : 1).
- Including the six omitted response pattens (*i.e.,* BBWW, BWBW, BWWW, WBWW, WWBW and WWWW) all sixteen response patterns appear.

The input PIN digits to MIOC BW method were chosen randomly by our simulator and there was no significant skewness in selecting the PIN digits. *Notably*, while selecting 10 digits for $16 \times 10^5$ times, the differences between mean and median was only 42.5. In Figure 6 and Figure 7, we have shown the distribution of input PIN digits to MIOC BW method and the frequencies of the observed response patterns, respectively.

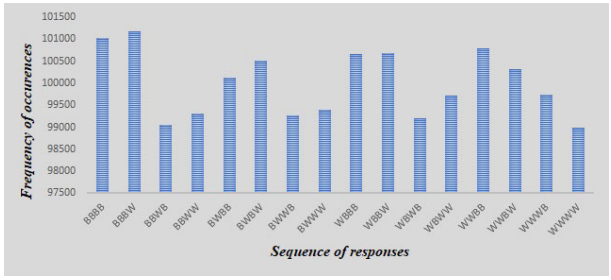


**FIGURE 7.** Frequencies of response patterns for entering a PIN digit in MIOC BW method. These frequencies were obtained after executing MIOC BW for 1, 600, 000 times for different PIN digits.

*Remark 2:* MIOC BW method degrades $\mathcal{A}'$s performance as the presence of all response patterns along with balanced color responses reduces the chances of guessing attack.

### C. REORDERING $\mathcal{H}'$s Responses In MIOC BW Method

Based on Algorithm 2 in Section III-B, we have summarized Kwon *et al.*'s proposal in [21] for demonstrating the threat on IOC BW method. From our earlier discussion in Section III-B, it is quite evident that four consecutive rounds for entering a single digit in IOC BW method open up the opportunity for covert-attentional shoulder surfers. In case of attacking IOC BW method, while $\mathcal{A}'$s strength relies on information processing capability by using VSTM, we have utilized the limitation of VSTM's storage capacity (*i.e.,* in the form of recall operation) to defeat the adversary in the proposed environment.

For MIOC BW method, we suggest a new ordering for entering the responses. The information regarding $i^{th}$ ($0 \leq i \leq 3$) PIN digit will be entered in the $j^{th}$ ($0 \leq j \leq 15$) round when $j$ *mod* 4 equalizes with $i$. For example, $\mathcal{M}$ receives color responses for $0^{th}$ PIN digit in 0, 4, 8 and and $12^{th}$ round. To accommodate with this change, MIOC BW method

- Maintains two different lists corresponding to *probable candidates* and *rejected candidates*. For the $i^{th}$ PIN digit $d_i$, let $pL\_d_i$ and $rL\_d_i$ denotes the list of probable and rejected candidates, respectively.
- Inherits proposed color assignment and noise insertion strategies from Algorithm 3 and to avoid the risks associated with redundant rounds and unbalanced key presses.

Algorithm 4 shows how MIOC BW method derives a 4−length PIN from $\mathcal{H}'$s responses in the newly defined order. Based on the Algorithm 4, from Figure 8 to Figure 9, we have demonstrated the systematic authentication procedure carried out by MIOC BW method for the PIN 3850. The symbol "$*$" indicate the color button press by $\mathcal{H}$. The lists in the green and orange backgrounds indicate the probable and rejected candidates, respectively, created from the submitted responses in the respective rounds in MIOC BW method.

**Algorithm 4** MIOC BW (Systematic Authentication Procedure)

**Initialize:** $\forall\, i \in \{0, \ldots, 3\}$
$pL\_d_i := \{0, 1, \ldots 9\}$; $rL\_d_i := \emptyset$;
PIN $:= \emptyset$;
**for** round $= 0$ to $15$ **do**
  $i :=$ round mod 4;
  $X \leftarrow \pi(pL\_d_i, \frac{|pL\_d_i|}{2}$, black, white);
  $Y \leftarrow \pi(rL\_d_i, \frac{|rL\_d_i|}{2}$, black, white);
  *display* $X \cup Y$;
  [$\mathcal{H}$ submits PIN color by hitting black/white button];
  receive $\mathcal{H}'$s input: choice $\in$ {black, white};
  **if** (choice $=$ black) **then**
    $pL\_d_i \leftarrow \eta \circ \kappa(X$, black);
    $Y \leftarrow \eta \circ \kappa(X$, white); $rL\_d_i \leftarrow rL\_d_i \cup Y$;
  **else**
    $pL\_d_i \leftarrow \eta \circ \kappa(X$, white);
    $Y \leftarrow \eta \circ \kappa(X$, black); $rL\_d_i \leftarrow rL\_d_i \cup Y$;
  **if** ($|pL\_d_i| = odd$) **then** add_noise($pL\_d_i$, $rL\_d_i$);
**for** i$=$ 0 to 3 **do**
  PIN $:=$ PIN$\cdot pL_d_i$; ▷ "$\cdot$" does concatenation
*return* PIN;

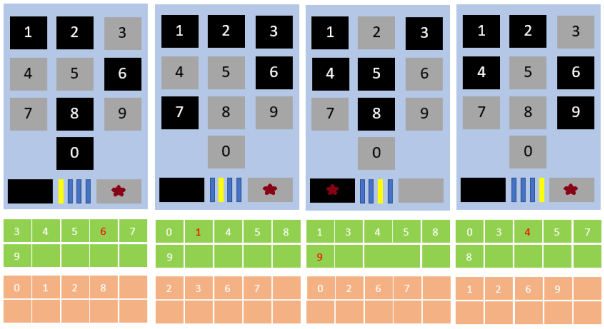

**FIGURE 8.** Responses for each PIN digit 3850 in the first four consecutive rounds.

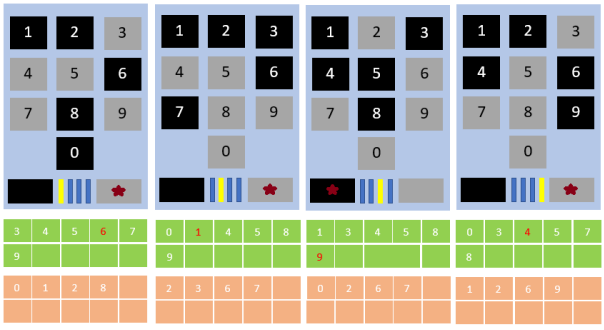

**FIGURE 9.** Responses for each PIN digit 3850 in the second four consecutive rounds.

### 1) THE IMPACT OF REORDERING

The impact of reordering on the security of the method can be best explained under the light of Figure 2 and the figures in this page. Note that following the direction in Figure 2, $\mathcal{A}$ already stores some information in VSTM in the very first round from the response of $\mathcal{H}$. Thereafter, the information in each round are *related* to the information in the previous round and with each passing round, the amount of information (obtained after perceptual grouping) reduce gradually. In [21], authors have proved that – the same computation by $\mathcal{H}$ in each round and relation between consecutive rounds in IOC BW method allow $\mathcal{A}$ to perform successful covert-attentional shoulder surfing attack. In contrast, from Figure 8 to Figure 11, it can be seen that the consecutive rounds in the MIOC BW method are not related to any single PIN digit.

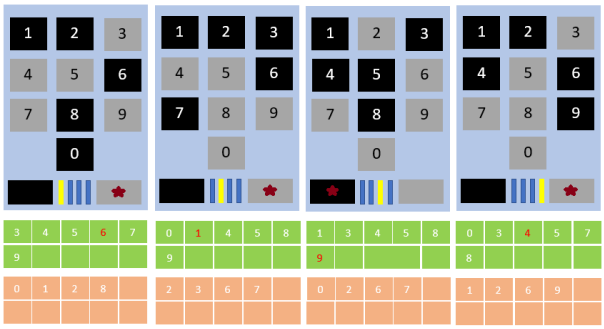

**FIGURE 10.** Responses for each PIN digit 3850 in the third four consecutive rounds.

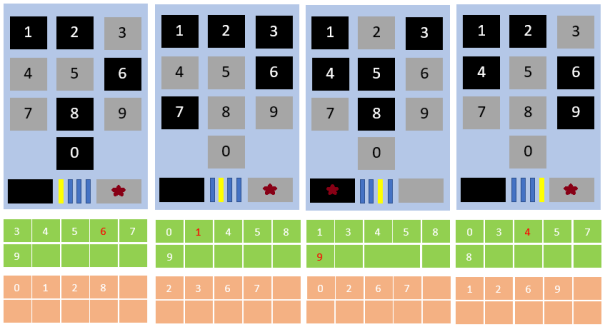

**FIGURE 11.** Responses for each PIN digit 3850 in the fourth four consecutive rounds.

Therefore, the accumulated information after *each fourth round* (except the last) does not allow $\mathcal{A}$ to derive any single PIN digit. Now, at the end of *first four consecutive rounds* in MIOC BW method (ref. to Figure 8), $\mathcal{A}$ may store four independent perceptually formed groups each of which is related to a single PIN digit. However, while entering into the *second four consecutive rounds* (ref. to Figure 9), $\mathcal{A}$ needs to recall each group from the *first four consecutive rounds*. Now, the time required to perform the recall operation is suggested to be at least 550 ms and it may vary up to approximately 3000 ms [14]. Therefore, though computation in MIOC BW remains same for $\mathcal{H}$, the modification puts additional load on $\mathcal{A}'$s mind (in the form of recall operation) compared to IOC BW method. The additional time required for recall

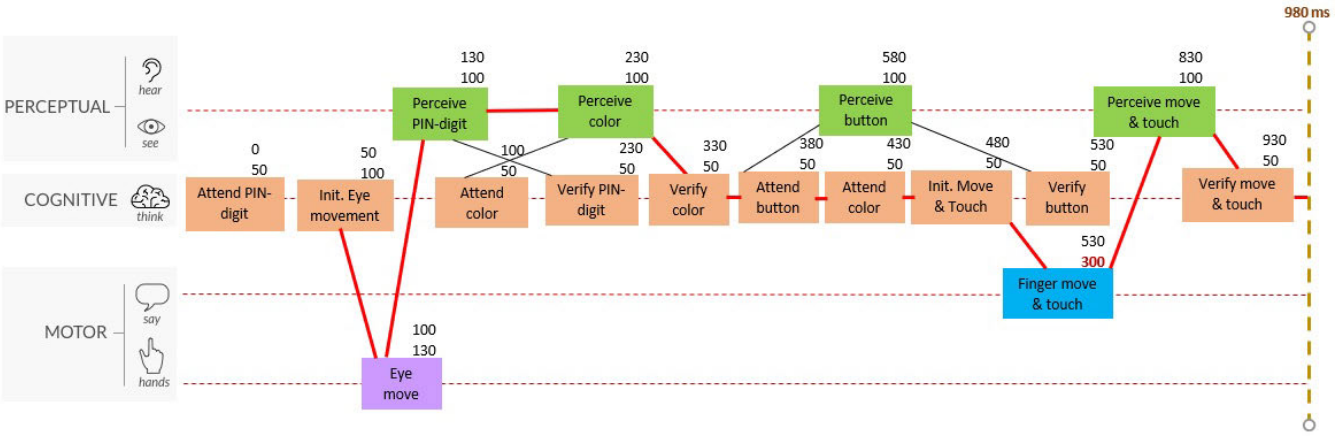


**FIGURE 12.** Modelling of $\mathcal{H}'$s response time in MIOC BW method. The bold red line refers to critical path which suggest minimal time required to accomplish a task.

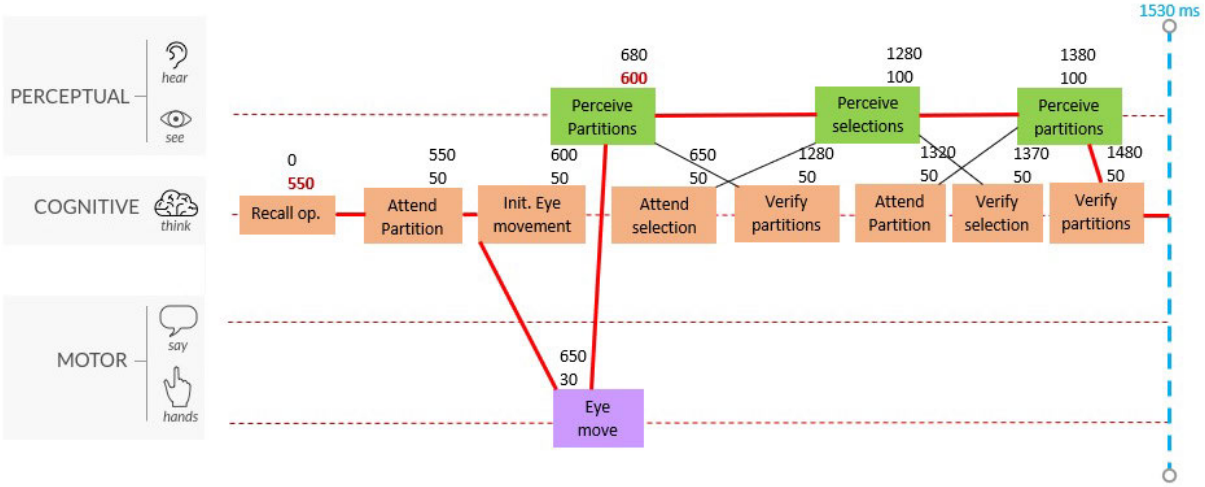


**FIGURE 13.** Modelling of $\mathcal{A}'$s performance in MIOC BW from the fifth round onwards. The bold red line refers to critical path by considering the interleaving operators.

operation prevents $\mathcal{A}$ to breach the security of the MIOC BW method.

### 2) CORRECTNESS PROOF

In [21], authors have used *human performance modelling tool* CPM-GOMS [17], to show the insecurity in IOC BW method. To prove the correctness of our claim about the MIOC BW method, we have also used the same tool suggested by Kwon *et al.* [21]. Figure 12 shows gantt chart returned by CPM-GOMS after evaluating task completion time for $\mathcal{H}$ in each round in the MIOC BW method. On the other hand, Figure 13 shows gantt chart returned by CPM-GOMS after evaluating task completion time for $\mathcal{A}$ in each round from the *fifth round* onwards. From both the figures, it is not hard to see that while it takes 960 ms to obtain a response from $\mathcal{H}'$s side in each round, $\mathcal{A}$ needs at least 1530 ms to derive any meaningful information from the fifth round onwards. Hence, by maintaining a significant margin of $1530 - 960 = 570$ ms, reordering of rounds in the MIOC BW method prevents $\mathcal{A}$ from performing the covert-attentional shoulder surfing attack.

## V. PERFORMANCE EVALUATION AND COMPARISONS

Our study from the previous section suggests that MIOC BW method adds noise to the odd set of probable PIN digits for

- Eliminating round redundancy.
- Imposing a balance between black and white key pressing.

By rectifying these drawbacks of IOC BW method, the proposed modification ensures that $\mathcal{A}$ does not get any advantage while

- Guessing a color response.
- Trying to derive a PIN digit earlier than the fourth round related to a PIN digit.

Before any further discussion, we have introduced a notion, *hardness factor*, which indicates how much effort a

covert-attentional shoulder surfer needs to put in order to compromise the security of a system.

*Definition 2: Hardness factor* is the ratio between required time by $\mathcal{A}$ to get the relevant information from a round to perform the attack *and* required time by $\mathcal{H}$ for generating and submitting the valid response in a round.

Here, the required time for both attack and response is an output of the tool CPM-GOMS. *Notably*, in this tool, every operator is represented by a box (a task) with a duration. The task duration time is a widely accepted generalization in the production system architectures [1], [8], [18], [28]. Therefore, the output of this tool can be considered as the expected average time for accomplishing a task (*e.g.,* for generating a response by $\mathcal{H}$ or deriving a PIN by $\mathcal{A}$). One of the advantages of such an evaluation is that the outcome remains static independent of the users' set and hence, the result is considered as more reliable.

Clearly, if the value of *hardness factor* exceeds 1, then $\mathcal{A}$ fails to perform the attack. The reordering of rounds in MIOC BW method yields the value of *hardness factor* to $\frac{1530}{960} = 1.593$. Hence, by following the correctness proofs in the previous section, MIOC BW method fixes all the vulnerable aspects of IOC BW method and provides much better security standard against the considered threat model.

We have also implemented MIOC-BW method in PHP (version 5.6.35) platform in Windows 10 for conducting a usability experiment. Almost like in [21], we took help from 12 participants (3 females and 9 males) for conducting the test. Followed by a small training-phase, each participant was requested for login for 3 times. The participants were using a laptop for the login purpose and entering responses by *clicking* on the black and white response buttons. As it takes at least 300 ms more time to perform *Click* operation compared to *Touch* operation [32], therefore, we may expect $300 \times 16 = 4800$ ms faster response time while logging by using a smartphone. Hence, to remain close to the reported scenario in [21], we subtracted 4.8 seconds from the obtained login time by using the laptop. While the participants failed to login 9.0% of times (3 out of 33 attempts), the obtained average login time after the adjustment was recorded as 13.47 seconds. Therefore, MIOC BW method meets $\beta = 0.1$ and $t = 13.47$ which are reasonably close to the ideal values $\beta = 0.1$ and $t = 10$. Figure 14 shows the adjusted login time for each successful login attempt.

We have also compared MIOC BW method with the existing two significant proposals in this domain *i.e.,* Roth *et al.*'s proposal in [30] and Kwon *et al.*'s method in [21]. Table 1 shows a comparative view among the methods.

The above table indicates that some identified limitations in IOC BW method remain in Kwon *et al.*'s proposal. FC method guarantees security against the covert-attentional shoulder surfers and it increases response time a little bit compared to IOC BW method. MIOC BW, in comparison with the other proposals, provides highest security standard without any degradation in the usability aspect. The values in the last column of Table 1 has been generated based on the output of the human performance modelling tool CPM-GOMS.

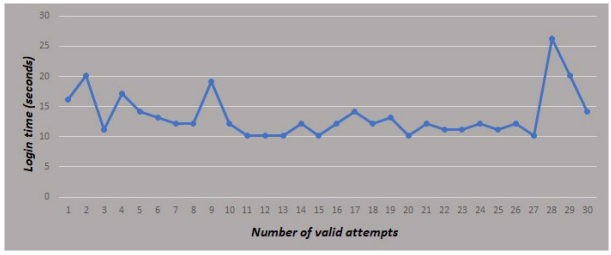


**FIGURE 14.** MIOC BW login environment: Obtained login time for each successful login attempt by 12 participants.

**TABLE 1.** Comparative analysis among the weak shoulder surfing attack resilient methods. † The Kwon *et al.*'s method has been denoted as FC method. ∗ needs further investigation. ⊗ response time per round by $\mathcal{H}$ for IOC BW and FC methods are taken from the report in [21].

| Method name | Redundant round | Balanced response | Hardness factor | Response time/round ⊗ |
|---|---|---|---|---|
| IOC BW | Yes | No | 1 | 960 ms |
| FC † | Yes | Yes ∗ | 1.462 | 1080 ms |
| MIOC BW | No | Yes | 1.593 | 960 ms |

## VI. CONCLUSION

Human adversaries may threat any weak shoulder surfing attack resilient method by exploiting its vulnerable aspects. In this paper, we have proposed a few modifications to the famous IOC BW method to regain its high security standard against all the known forms of observational attacks. One of the advantages of our proposal also comes from the usability aspect as the proposed MIOC BW method keeps the high usability standard of IOC BW method unaltered. Furthermore, with the capability of providing security against key-logger based attack for some devices (in case of disjoint keypad from the device screen *e.g.,* ATM), we hope that the proposed protocol can truly be a deployable solution in practice, especially in crowded places.

## REFERENCES

[1] J. R. Anderson, M. Matessa, and C. Lebiere, "ACT-R: A theory of higher level cognition and its relation to visual attention," *Hum.-Comput. Interact.*, vol. 12, no. 4, pp. 439–462, Dec. 1997.
[2] I. Arce, "The weakest link revisited [information security]," *IEEE Security Privacy*, vol. 1, no. 2, pp. 72–76, Mar./Apr. 2003.
[3] H. J. Asghar, J. Pieprzyk, and H. Wang, "A new human identification protocol and coppersmith's baby-step giant-step algorithm," in *Proc. Int. Conf. Appl. Cryptogr. Netw. Secur.* Berlin, Germany: Springer, 2010, pp. 349–366.
[4] X. Bai, W. Gu, S. Chellappan, X. Wang, D. Xuan, and B. Ma, "PAS: Predicate-based authentication services against powerful passive adversaries," in *Proc. Annu. Comput. Secur. Appl. Conf. (ACSAC)*, Dec. 2008, pp. 433–442.
[5] A. Bianchi, I. Oakley, and D. S. Kwon, "The secure haptic keypad: A tactile password system," in *Proc. SIGCHI Conf. Hum. Factors Comput. Syst.*, Apr. 2010, pp. 1089–1092.
[6] A. Bianchi, I. Oakley, J. K. Lee, and D. S. Kwon, "The haptic wheel: Design & evaluation of a tactile password system," in *Proc. Extended Abstr. Hum. Factors Comput. Syst.*, Apr. 2010, pp. 3625–3630.

[7] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of Web authentication schemes," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2012, pp. 553–567.

[8] S. K. Card, T. P. Moran, and A. Newell, *The Psychology of Human-Computer Interaction*. Boca Raton, FL, USA: CRC Press, 2017.

[9] N. Chakraborty and S. Mondal, "Color pass: An intelligent user interface to resist shoulder surfing attack," in *Proc. IEEE Students' Technol. Symp.*, Feb./Mar. 2014, pp. 13–18.

[10] A. Das, J. Bonneau, M. Caesar, N. Borisov, and X. Wang, "The tangled Web of password reuse," in *Proc. Netw. Distrib. Syst. Secur. Symp. (NDSS)*, vol. 14. 2014, pp. 23–26.

[11] A. D. Luca, "Designing usable and secure authentication mechanisms for public spaces," Ph.D. dissertation, Dept. Fac. Math., LMU Münich, Münich, Germany, 2011.

[12] A. De Luca, K. Hertzschuch, and H. Hussmann, "ColorPIN: Securing pin entry through indirect input," in *Proc. SIGCHI Conf. Hum. Factors Comput. Syst.*, Apr. 2010, pp. 1103–1106.

[13] W. S. Geisler and B. J. Super, "Perceptual organization of two-dimensional patterns," *Psychol. Rev.*, vol. 107, no. 4, pp. 677–708, Oct. 2000.

[14] R. M. Hogan and W. Kintsch, "Differential effects of study and test trials on long-term recognition and recall," *J. Verbal Learn. Verbal Behav.*, vol. 10, no. 5, pp. 562–567, Oct. 1971.

[15] N. J. Hopper and M. Blum, "Secure human identification protocols," in *Advances in Cryptology—ASIACRYPT*. Berlin, Germany: Springer-Verlag, 2001, pp. 52–66.

[16] D. Jacobs, "What makes viewpoint invariant properties perceptually salient?: A computational perspective," in *Perceptual Organization for Artificial Vision Systems*. New York, NY, USA: Springer, 2000, pp. 121–138.

[17] B. E. John and W. D. Gray, "CPM-GOMS: An analysis method for tasks with parallel activities," in *Proc. Conf. Companion Hum. Factors Comput. Syst.*, May 1995, pp. 393–394.

[18] B. E. John and D. E. Kieras, "The GOMS family of user interface analysis techniques: Comparison and contrast," *ACM Trans. Comput.-Hum. Interact. (TOCHI)*, vol. 3, no. 4, pp. 320–351, Dec. 1996.

[19] D. Kunda and M. Chishimba, "A survey of Android mobile phone authentication schemes," in *Proc. Mobile Netw. Appl.*, 2018, pp. 1–9.

[20] T. Kwon and J. Hong, "Analysis and Improvement of a PIN-Entry Method Resilient to Shoulder-Surfing and Recording Attacks," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 2, pp. 278–292, Feb. 2015.

[21] T. Kwon, S. Shin, and S. Na, "Covert attentional shoulder surfing: Human adversaries are more powerful than expected," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 44, no. 6, pp. 716–727, Jun. 2014.

[22] D. G. Lowe, *Perceptual Organization and Visual Recognition*, vol. 5. Boston, MA, USA: Springer, 2012.

[23] 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.

[24] T. Matsumoto and H. Imai, "Human identification through insecure channel," in *Advances in Cryptology—EUROCRYPT*. Berlin, Germany: Springer, 1991, pp. 409–421.

[25] T. Perkovic, M. Cagalj, and N. Rakic, "SSSL: Shoulder surfing safe login," in *Proc. 17th Int. Conf. Softw., Telecommun. Comput. Netw.*, Sep. 2009, pp. 270–275.

[26] T. Perković, M. Čagalj, and N. Saxena, "Shoulder-surfing safe login in a partially observable attacker model," in *Financial Cryptography Data Security*, 2010, pp. 351–358.

[27] M. I. Posner, "Orienting of attention," *Quart. J. Exp. Psychol.*, vol. 32, no. 1, pp. 3–25, Feb. 1980.

[28] F. Radicchi, S. Fortunato, and C. Castellano, "Universality of citation distributions: Toward an objective measure of scientific impact," *Proc. Nat. Acad. Sci. USA*, vol. 105, no. 45, pp. 17268–17272, Nov. 2008.

[29] K. Rayner, "Eye movements in reading and information processing: 20 years of research," *Psychol. Bull.*, vol. 124, no. 3, pp. 372–422, 1998.

[30] V. Roth, K. Richter, and R. Freidinger, "A PIN-entry method resilient against shoulder surfing," in *Proc. 11th ACM Conf. Comput. Commun. Secur.*, Oct. 2004, pp. 236–245.

[31] S. Sagiroglu and G. Canbek, "Keyloggers: Increasing threats to computer security and privacy," *IEEE Technol. Soc. Mag.*, vol. 28, no. 3, pp. 10–17, Sep. 2009.

[32] F. Sasangohar, I. S. MacKenzie, and S. D. Scott, "Evaluation of mouse and touch input for a tabletop display using Fitts' reciprocal tapping task," in *Proc. Hum. Factors Ergonom. Soc. Annu. Meeting*. Los Angeles, CA, USA: SAGE, 2009, pp. 839–843.

[33] I. G. Sligte, H. S. Scholte, and V. A. F. Lamme, "Are there multiple visual short-term memory stores?" *PLoS ONE*, vol. 3, no. 2, 2008, Art. no. e1699.

[34] H.-M. Sun, S.-T. Chen, J.-H. Yeh, and C.-Y. Cheng, "A shoulder surfing resistant graphical authentication system," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 2, pp. 180–193, Mar./Apr. 2018.

[35] S. Uellenbeck, T. Hupperich, C. Wolf, and T. Holz, "Tactile one-time pad: Leakage-resilient authentication for smartphones," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.* Berlin, Germany: Springer-Verlag, 2015, pp. 237–253.

[36] C.-H. Wang, T. Hwang, and J.-J. Tsai, "On the Matsumoto and Imai's human identification scheme," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer-Verlag, 1995, pp. 382–392.

[37] D. Weinshall, "Cognitive authentication schemes safe against spyware," in *Proc. IEEE Symp. Secur. Privacy*, May 2006, pp. 1–6.

[38] S. Wiedenbeck, J. Waters, L. Sobrado, and J.-C. Birget, "Design and evaluation of a shoulder-surfing resistant graphical password scheme," in *Proc. Work. Conf. Adv. Vis. Interfaces*, May 2006, pp. 177–184.

[39] G. T. Wilfong, "Method and apparatus for secure PIN entry," U.S. Patent 5 940 511, Aug. 17, 1999.

[40] 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 Annu. Netw. Distrib. Syst. Secur. Symp. (NDSS)*, San Diego, CA, USA, Feb. 2012, pp. 1–16.

[41] Q. Yan, J. Han, Y. Li, J. Zhou, and R. H. Deng, "Designing leakage-resilient password entry on touchscreen mobile devices," in *Proc. 8th ACM SIGSAC Symp. Inf., Comput. Commun. Secur.*, May 2013, pp. 37–48.

[42] Q. Yan, J. Han, Y. Li, J. Zhou, and R. H. Deng, "Leakage-resilient password entry: Challenges, design, and evaluation," *Comput. Secur.*, vol. 48, pp. 196–211, Feb. 2015.

[43] H. Zhao and X. Li, "S3PAS: A scalable shoulder-surfing resistant textual-graphical password authentication scheme," in *Proc. Adv. Inf. Netw. Appl. Workshops*, vol. 2, 2007, pp. 467–472.

**NILESH CHAKRABORTY** received the master's degree from the National Institute of Technology (NIT), Durgapur, India, in 2013, and the Ph.D. degree from IIT Patna, India, in 2018, respectively. During the Ph.D. degree, he successfully completed a security project funded by the Science and Engineering Research Board (SERB), Government of India. He is currently a Postdoctoral Fellow of Shenzhen University, China. His primary research topics include password security and usable security.

**JIANQIANG LI** received the B.S. and Ph.D. degrees in automation from the South China University of Technology, Guangzhou, China, in 2003 and 2008, respectively. He is a Professor with the College of Computer and Software Engineering, Shenzhen University, Shenzhen, China. He led three projects of the National Natural Science Foundation and three projects of the Natural Science Foundation of Guangdong Province, China. His current research interests include data analysis, embedded systems, and the Internet of Things.

**SAMRAT MONDAL** (M'11–SM'19) received the Ph.D. degree from IIT Kharagpur, in 2010. He is currently an Assistant Professor with the Department of Computer Science and Engineering, IIT Patna, India. Before joining the IIT Patna, he held a faculty position at DAIICT, Gandhinagar, India, for almost one year. He was a Visiting Scholar with National Semiconductor Corporation, Santa Clara, CA, USA, for seven months. He was a Visiting Faculty Member of the University of Denver, Colorado, USA, for 11 months. His primary research interests include security and privacy, smart grid-related application, and database and data mining. His multiple research proposals have been funded by the Science & Engineering Research Board (SERB), Government of India. He has served as the technical program committee member of many international conferences. He also served as a Reviewer for journals such as the IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING (IEEE TDSC) and *Computers&Security*. He has published several research papers in reputable international journals and conferences.

**FEI CHEN** received the Ph.D. degree in computer science and engineering from The Chinese University of Hong Kong, in 2014. He is currently an Associate Professor with the College of Computer Science and Engineering, Shenzhen University, China. His research interests include information and network security, and data protection and privacy.

**YI PAN** (SM'91) received the B.Eng. and M.Eng. degrees in computer engineering from Tsinghua University, China, in 1982 and 1984, respectively, and the Ph.D. degree in computer science from the University of Pittsburgh, USA, in 1991.

He is currently a Regents' Professor and the Chair of computer science with Georgia State University, USA. He has served as the Associate Dean and the Chair of the Biology Department, from 2013 to 2017, and the Chair of computer science, from 2006 to 2013. He joined Georgia State University, in 2000, where he was promoted to a Full Professor, in 2004, named as a Distinguished University Professor, in 2013, and designated a Regents Professor (the highest recognition given to a faculty member by the University System of Georgia), in 2015. His profile has been featured as a Distinguished Alumnus with Tsinghua Alumni Newsletter and the University of Pittsburgh CS Alumni Newsletter. His current research interests include parallel and cloud computing, big data, and bioinformatics.