A Rotary PIN Entry Scheme Resilient to Shoulder-Surfing

Peipei Shi, Bo Zhu and Amr Youssef
Concordia Institute for Information Systems Engineering
Concordia University, Montreal, Quebec, Canada
{pe_sh, zhubo, youssef}@ciise.concordia.ca

Abstract

The combination of tokens or cards and personal identification numbers (PINs) are widely used for authentication in many applications including automatic teller machines (ATMs) and point of sales (POSs). Recent security incidents have shown that criminals can get these authentication tokens or cards either by pickpocketing or through fake magnetic card readers. Furthermore, PINs may also be captured through shoulder-surfing or by the use of concealed miniature cameras. Upon obtaining both authentication factors, criminals can easily break into users' accounts which presents a high security risk.

In this paper, we propose a new spinwheel-like PIN entry scheme which is resilient against shoulder-surfing attacks even if the shoulder-surfer can record the entire PIN entry procedure for one time with a video device. This scheme has two variants, both of which achieve a good balance between security and usability.

1. Introduction

Currently, the security of automatic teller machines (ATMs) and point of sales (POSs) are protected by a combination of physical token, typically a magnetic card, and certain secret knowledge, e.g., personal identification numbers (PINs). A common risk of this type of protection is that magnetic stripe cards can be stolen or skimmed by fake card readers. Once it happens, the security of the authentication scheme relies only on the protection of PINs, which is subjected to different types of attacks. In this paper, we aim at designing a PIN entry scheme that is resistant to shoulder-surfing attacks.

Shoulder-surfing attacks can be divided into two categories: *cognitive shoulder-surfing* and *recording-based shoulder-surfing* [7]. In the former, the adversary depends on his/her cognitive capability to obtain PINs or other sensitive information. Due to the limited cognitive capabilities of human beings [4, 10], this type of attacks is relatively easy to defend. In contrast, in the latter, the accuracy of recording PINs has been significantly improved with concealed miniature cameras or video mobile phones. Recent reports [1, 2, 8] show that, recording-based shoulder-surfing attacks have become a serious threat to many security systems in which the authentication process rely on the combination of magnetic cards and PINs.

To address the shoulder-surfing issue, several challenge-response-based approaches were proposed [6, 7, 11, 12]. In these schemes, generally, users have to perform multiple rounds of interactions with the system, instead of entering their PINs directly. As a result, the login procedure can be very long [11, 12] which renders these schemes unsuitable for many real-world scenarios, e.g., when many customers are queuing before an ATM. Further security protection beyond the combination of a magnetic stripe card and PIN includes biometric authentication and one-time keypad [9]. These solutions are not widely used at the current time, mainly due to their specific hardware requirements and/or the extra overhead in key management. Detailed discussions about biometric authentication and one-time keypad are out of the scope of this work.

In this paper, we propose a new PIN entry scheme with two variants. Each variant provides a distinct option of balancing security conditions against two types of potential risks, namely, random guessing and shoulder-surfing assisted guessing. More importantly, a thorough security analysis is conducted so as to give a quantitative guidance on choosing an appropriate option according to a system's specific security requirements. Unlike previous work, instead of emphasizing the robustness of a specific scheme against a particular type of attacks, we indicate that there is a trade-off between protections against different types of risks, and thus the selection of an appropriate scheme should be application-dependent, i.e, by considering the types and frequencies of risks faced in the application. Moreover, a detailed usability study is included.

The rest of the paper is organized as follows. The related work is reviewed in Section 2. The details of our scheme are presented in Section 3, followed by security analysis

in Section 4. In Section 5, we discuss the usability of our scheme. Finally, we conclude our work in Section 6.

2. Related work

Roth *et al.* [6] proposed a PIN entry method which offers limited resiliency against shoulder-surfing. In their design, the keys on the keypad are randomly partitioned into a white set and a black set. Depending on the set to which the digit of the PIN under verification belongs, the user enters the key by pressing the button that has the same color as this set. Multiple rounds are needed to complete the input of a single digit of the PIN. For example, given a 4-digit PIN, it may take up to 16 rounds to complete the authentication process. Their method has three variants: *Immediate Oracle Choices* (IOC), *Delayed Oracle Choices* (DOC) and *probabilistic cognitive trapdoor game*. The first two are secure against cognitive shoulder-surfing, but are vulnerable to recording-based shoulder-surfing. The *probabilistic cognitive trapdoor game* variant offers limited resilience to recording-based shoulder-surfing. More specifically, it is resilient against the adversary who has only one record of the whole PIN entry process.

Weinshall [11] proposed two challenge-response protocols with a high complexity query and a low complexity query, respectively. Both of them require users to answer a sequence of challenges posed by the system. The challenges are based on a shared secret between the system and the user, which is a fixed set of pictures divided into two sub-groups. As indicated by the authors, this scheme has two weaknesses: users need to be trained in order to familiarize them with their associated secrets, e.g., a set of pictures; and the authentication process may take longer time than alternate methods. A later work by Golle and Wagner [3] shows that Weinshall's protocols are vulnerable to a certain attack that leverages a SAT solver. This attack can recover the user's PIN in a few seconds after recording a small number of successful logins.

The Convex Hull Click (CHC) scheme [12] is another multiple-round challenge-response authentication scheme proposed to fend off shoulder-surfing. In this scheme, users are required to select a set of icons from a larger icon database as their passwords. During the login process, in order to answer the challenge, the user must virtually find three or more of his/her password icons, mentally create a convex hull formed by these icons, and then click inside this convex hull. The user must respond to the multiple challenges correctly in order to be authenticated to the system. As a result, the login time can be very long. According to their simulation results, the mean time for correct password inputs is around 72 seconds. Additionally, no mathematical proof is provided in the paper to evaluate and justify its resilience to shoulder-surfing.

PassFaces [5] relies on users' capability of recognizing faces. A user first needs to choose a set of faces as the password, and is then trained for few minutes so as to be familiar with the chosen faces. The login may take several rounds. In each round, only one of all the faces displayed belongs to the password set. The user needs to identify those faces in the secret set correctly in order to pass the authentication. This method is designed to be resilient against cognitive shoulder-surfing.

In a recent shoulder-surfing resistant scheme proposed by Shi *et al.* [7], instead of a sequence of four digits, the PIN is defined as a sequence of four locations in a table displayed on the screen, the content of which is randomly generated by the system each round. To input the whole four digits of PIN, only four rounds are needed. This scheme can offer a strong security protection against cognitive shoulder-surfers and even recording-based shoulder-surfers who can acquire up to two records of the whole PIN entry procedure. Similar to [11, 12], a weakness of this scheme is that users need to be trained to use a new kind of PIN, instead of the regular four-digit PIN.

3. Proposed PIN entry scheme

In this section, we first present system model and adversary model of our scheme. Afterwards, two variants of our scheme are proposed.

3.1. System and adversary models

We assume that the alphabet of PIN digits is $\{0, 1, \ldots, A-1\}$, e.g., $\{0, 1, \ldots, 9\}$, although it can be readily extended to generic characters instead of digits. Let l denote the number of digits in the secret PINs. Throughout the rest of this paper, the default value of l is 4. We assume that the adversary can obtain the information stored on the magnetic stripe card, e.g., by pickpocketing or fake card readers, and thus the protection of the authentication mechanism relies on the security of PINs.

In the following, we consider three adversary models. The first type is called a *Zero-knowledge adversary*, in which the adversary only has the card (e.g., picking up a card by chance), but does not have any knowledge about the PIN. Thus the only option for the adversary in this case is to launch a random guessing attack on the ATM. The other two considered adversary models are cognitive shoulder-surfing and recording-based shoulder-surfing. In particular, in recording-based shoulder-surfing, we assume that the adversaries can acquire up to one record of the entire login process. We argue that such an assumption is reasonable in most applications that are protected by the combination of a magnetic stripe card and a PIN. For example, even if the adversary can install a concealed miniature camera over the

input screen of an ATM, the probability that the camera can record two or three login processes of the same user on the same ATM within a reasonable time frame is slim.

We also assume that the verifier keeps a record on the number of successive PIN entry failures. Once detecting that this number reaches a predetermined threshold (e.g., 3), the verifier will retain the card and suspend the usage of the relevant account, until the PIN is reset through a secure channel, e.g., at a bank branch. In addition, for convenience, this counter is automatically reset upon a successful login. To prevent potential misuse, e.g., a smart attacker may first make a few guesses below the threshold and then wait the counter to be reset by legal users, in our design, upon a successful login the legitimate user will be notified previous PIN entry failures, if any.

Throughout the rest of this paper, we focus our discussion on the ATM environment, although our scheme is also applicable to other scenarios, such as POS terminals and portable digital assistants (PDAs).

3.2. PIN entry method

Our goal is to design a secure yet user friendly PIN entry scheme. In addition, in order to provide different options for balancing security levels against zero-knowledge adversary and shoulder-surfers, our scheme contains two parameterized variants: Variant One ($VO(N)$), and Variant Two ($VT(N)$).

3.2.1.Variant One. Suppose that the user has inserted the bank card into an ATM machine, and his/her personal PIN of the card is $X_1X_2X_3X_4$, ($X_i \in \{0, 1,\ldots, \text{A-1}\}$). In this variant, after the welcome message, the verifier displays a set of L co-centered rotating wheels each of which is equally divided into A sectors as shown in Figure 1. Each sector is marked with a digit randomly chosen from the alphabet, i.e., 0 to $A-1$, and each digit in the alphabet is displayed exactly once within each circle. Circles can be rotated either clockwise or anticlockwise. We denote the four circles from the innermost to the outermost as the 1^{st}, 2^{nd}, 3^{rd} and 4^{th} circle, respectively. To input the PIN, the user needs to align all PIN digits along one sector in the correct sequence, i.e., align X_i in the i^{th} circle. A control button is pressed to indicate the completion of the PIN alignment process. Figure 2 shows an alternate graphical user interface (GUI) for $VO(1)$ that might be appropriate in some applications.

Upon the completion of the PIN entry process, there are A aligned inputs contained in the wheel. For example, assume that Figure 1 shows the final input of a PIN entry process, the aligned inputs include {8121,9243,7774,5838,3985,6607,2496,1012,4559,0360}. The verifier checks all these potential PINs. If any of them

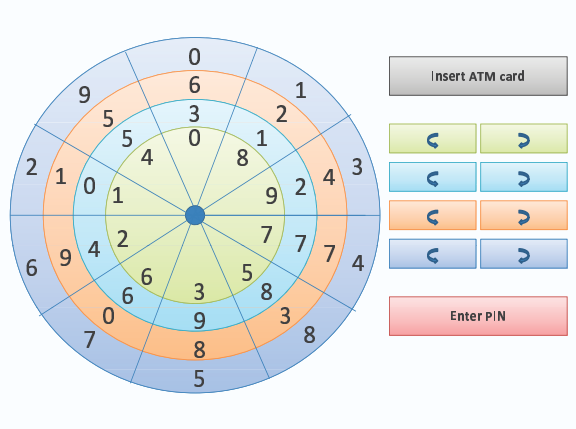

Figure 1. Example for $VO(1)$

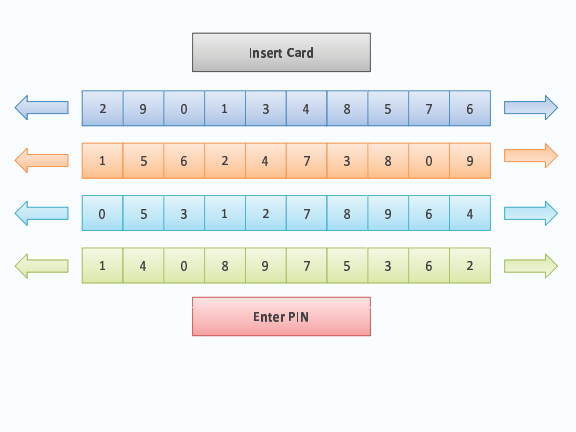

Figure 2. An alternate GUI for $VO(1)$

matches the genuine PIN corresponding to the bank card inserted, the verifier will give the user access to the linked account. Otherwise, an error message is displayed, and the counter of the number of successive PIN entry failures is increased by 1.

The above scheme, called $VO(1)$, can be generalized into $VO(N)$ by dividing each circle into $N \times A$ sectors, instead of A sectors. In this case, each digit in the alphabet is displayed exactly N times, instead of once, within each circle.

3.2.1.Variant Two. Similar to VO, each circle is equally divided into A sectors, and each digit in the alphabet is displayed exactly once within a circle. However, the wheel in VT contains only two circles, as shown in Figure 3. As a result, in order to input a 4-digit PIN, VT needs two rounds to complete the PIN entry process. More specifically, X_1X_2

and X_3X_4 are entered in round one and round two, respectively. Note that, the position of the aligned input X_1X_2 is not necessary to be the same as that of the aligned input X_3X_4.

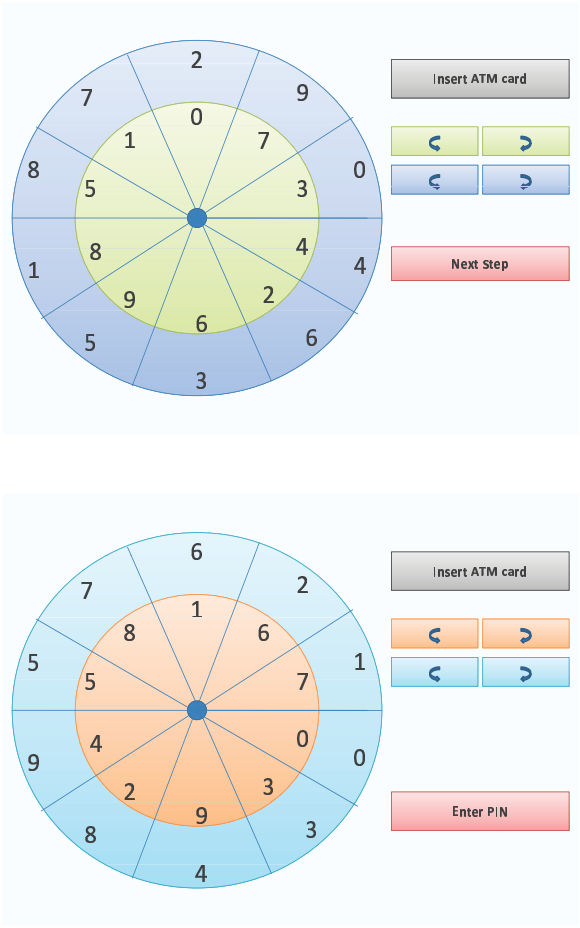

Figure 3. Example for VT(1)

After the two rounds, the verifier checks all A potential PINs and verifies whether there exists an input equal to the genuine PIN. Based on the result of the verification, the verifier will grant or deny the access to the corresponding account.

Again, $VT(1)$ can be generalized in the same as $VO(N)$ by dividing each circle of the wheel into $N \times A$ sectors, instead of A sectors. Then each digit in the alphabet is displayed exactly N times, instead of once, within a circle. Due to the limitation on the display area of an ATM machine, the typical setting of N is 1, 2 or 3.

4. Security analysis

In this section, we analyze the security of the two variants of our scheme under three types of adversary models, i.e., zero-knowledge (ZK) adversary, recording-based shoulder-surfing (RSS) and cognitive shoulder-surfing (CSS). Let P_{Ad-r}^{Var} denote the probability that an adversary successfully gets the secret PIN within r attempts in a specific variant of our scheme under one of the three adversary models, where Ad and Var denote an adversary model and a variant of our scheme, respectively. In the following, we first analyze each adversary model when $r = 1$, and then discuss the case when $r = M$, where M is the maximum number of successive PIN entry failures allowed, before the verifier retains the card and suspends the usage of the relevant account.

4.1. Zero-knowledge adversary

Under the zero-knowledge adversary model, the adversary knows nothing about the secret PIN, and thus can only launch a random guessing attack.

In $VO(N)$, whatever choice the adversary makes, $N \times A$ distinct inputs are submitted for the verification. Thus, we have:

$$P_{ZK-1}^{VO(N)} \approx \frac{N \times A}{A^4} = \frac{N}{A^3} \quad (1)$$

Note that, as shown in Equation (1), $\frac{N}{A^3}$ is an approximation of $P_{ZK}^{VO(N)}$. This is due to the fact that, except for the case $N = 1$ where the above expression corresponds to the exact value of $P_{ZK}^{VO(1)}$, for $N > 1$, there may exist repeated values among all the $N \times A$ inputs submitted. Since in our design N is a small number (e.g., 2 or 3), such an approximation is acceptable.

Similarly, for $VT(N)$ where the two rounds of the PIN entry process are executed independently from each other, we have

$$\begin{aligned} P_{ZK-1}^{VT(N)} &= P_1^{VT(N)} \cdot P_2^{VT(N)} \\ &\approx \frac{N \times A}{A^2} \cdot \frac{N \times A}{A^2} = \frac{N^2}{A^2} \end{aligned} \quad (2)$$

where $P_1^{VT(N)}$ and $P_2^{VT(N)}$ denote the probability that in $VT(N)$ an adversary inputs the secret X_1X_2 and X_3X_4 in the first and second rounds, respectively.

4.2. Recording-based shoulder-surfing

In the following analysis, under the recording-based shoulder-surfing model, we assume that the adversary acquires a record of the whole PIN entry process. All variants of our scheme fail, if the adversary can obtain more than one record of the whole PIN entry process.

In $VO(1)$, an adversary can easily deduce that the secret PIN is among the A distinct aligned inputs. Apparently, $P_{RSS-1}^{VO(1)}$ is $1/A$. Similarly, for $N > 1$, $N \times A$ aligned inputs are checked in $VO(N)$, although some of these inputs might be repeated. Since in our design N is a small number (e.g., 2 or 3), $P_{RSS-1}^{VO(N)}$ is approximately $1/(N \times A)$.

Similarly, in each round of $VT(N)$ there are $N \times A$ inputs subjected to the verification. Therefore, the probability that an adversary successfully guesses the correct digits can be computed in the same way as the calculation of $P_{RSS-1}^{VO(N)}$ in $VO(N)$. Since there are two rounds in $VT(N)$, we have:

$$P_{RSS-1}^{VT(N)} = (P_{RSS-1}^{VO(N)})^2 \approx (\frac{1}{N \times A})^2 = \frac{1}{N^2 \times A^2} \quad (3)$$

4.3. Cognitive shoulder-surfing

There has been some interesting research on the cognitive capabilities of human beings. In 1956, Miller [4] noted that the limitation on short term memory (STM) is 7 plus or minus 2 symbols. A more recent work by Vogel *et al.* [10] shows that STM of normal people is limited to three to four symbols. Few subjects were able to remember five symbols in their STM throughout the experiments conducted in [10]. This discovery is based on the neurophysiological evidence.

Let L denote the maximum number of characters that a human being can memorize during cognitive shoulder-surfing. In $VO(N)$, the best strategy for an adversary is to memorize $\lfloor L/4 \rfloor$ aligned inputs. According to previous research results [4, 10] about the cognitive capabilities of human beings, we know that $\lfloor L/4 \rfloor \geq 1$. Since each input has the same possibility of being the secret PIN and in each login attempt the adversary can test only one of inputs, we thus have $P_{CSS-1}^{VO(N)} = P_{RSS-1}^{VO(N)}$.

In $VT(N)$, an adversary has to make a decision about the distribution of her cognitive capability. Let L_1 and L_2 denote the number of characters that the adversary plan to memorize in the first round and the second round, respectively. Thus, we have $P_{CSS-1}^{VT(N)} = P_{RSS-1}^{VT(N)}$, when the following conditions is satisfied: $\lfloor L_i/2 \rfloor \geq 1$, where $i = 1,\ 2$.

4.4. Multiple attempts by the adversary

Let M denote the maximum number of successive PIN entry failures allowed, before the verifier retains the card and terminates the usage of the relevant account.

In the zero-knowledge adversary model, each random chosen input has the same probability of being the secret PIN. Thus, we have $P_{ZK-M}^{Var} = M \cdot P_{ZK-1}^{Var}$. Similarly, in the recording-based shoulder-surfing model, each recorded input has the same probability of being the secret PIN. Thus, we have $P_{RSS-M}^{Var} = M \cdot P_{RSS-1}^{Var}$.

As to the cognitive shoulder-surfing model, in $VO(1)$ and $VO(N)$, if $\lfloor L/4 \rfloor \geq M$, we have $P_{CSS-M}^{Var} = M \cdot P_{CSS-1}^{Var}$. Otherwise, we have:

$$P_{CSS-M}^{Var} = \lfloor \frac{L}{4} \rfloor \cdot P_{CSS-1}^{Var} + (M - \lfloor \frac{L}{4} \rfloor) \cdot P_{ZK-1}^{Var} \quad (4)$$

Similarly, in $VT(N)$, if $\lfloor L_i/2 \rfloor \geq M$ for $i = 1,\ 2$, we have $P_{CSS-M}^{Var} = M \cdot P_{CSS-1}^{Var}$. Otherwise, we have:

$$P_{CSS-M}^{Var} = A \cdot P_{CSS-1}^{Var} + (M - A) \cdot P_{ZK-1}^{Var} \quad (5)$$

where $A = min\{\lfloor L_1/2 \rfloor, \lfloor L_2/2 \rfloor\}$. Based on Equation (5), the best strategy of an adversary in the cognitive shoulder-surfing model and $VT(N)$ is to equally spread his/her cognitive capability to the two rounds.

4.5. Summary of security analysis

In Table 1, we summarize the security levels of the two variants proposed in terms of the probability that an adversary successfully guesses the secret PIN in one attempt, i.e., P_{Ad-1}^{Var}.

Table 1. P_{Ad-1}^{Var} **for** $VO(N)$ **and** $T(N)$

Adversary Type	VO(N)	VT(N)
Zero-knowledge	$\frac{N}{A^3}$	$\frac{N^2}{A^2}$
Recording-based	$\frac{1}{N \times A}$	$\frac{1}{N^2 \times A^2}$
Cognitive shoulder-surfing	$\frac{1}{N \times A}$	$\frac{1}{N^2 \times A^2}$

From Table 1, we observe that there is a trade-off between the security level against zero-knowledge adversary and that against recording-based/cognitive-based shoulder-surfing. Let N_{max} denote the maximum value allowed for N, taking into account the usability concerns. Then, on one hand, $VO(1)$ and $VT(N_{max})$ are the most secure variants against zero-knowledge adversary and recording-based/cognitive-based shoulder-surfing, respectively. On the other hand, $VO(1)$ and $VT(N_{max})$ are the least secure variants against recording-based/cognitive-based shoulder-surfing and zero-knowledge adversary, respectively.

In practice, in the design of a secure system, one needs to consider all the possible attacks and then find an appropriate balance between different security requirements. For example, assume that an ATM system is designed to allow only one person to enter the transaction area at a time. Thus, only zero-knowledge adversary and recording-based shoulder-surfing are concerned. Assume that the security requirements against zero-knowledge adversary and recording-based shoulder-surfing are P_{ZK}^{max} and P_{RSS}^{max}. In

addition, assume that there exist estimated probabilities that the conditions for launching a given type of attacks are satisfied according to previous statistical data, e.g., reported events of card loss or installation of hidden cameras on ATM machines. Let denote such probabilities for zero-knowledge adversary and recording-based shoulder-surfing as P_g and P_r, respectively. During the design, we need to minimize the value of $P = P_{ZK}^{Var} \cdot P_g + P_{RSS}^{Var} \cdot P_r$, while at the same time ensure that $P_{ZK}^{Var} \leq P_{ZK}^{max}$ and $P_{RSS}^{Var} \leq P_{RSS}^{max}$.

Apparently, the same trade-off exists when we consider the scenarios where multiple attempts are possible and the idea of balancing security conditions based on application-dependent requirements and risks can be readily extende to such scenarios.

5. Usability evaluation

In order to test the usability of our proposed schemes different variants were evaluated by a group of twenty (female and 13 male) graduate students with engineering o computer science background. The average age of partici pants is about 27 years (StdDev=4.285).

At the beginning of the test session, all participants wer asked to provide their opinion, on a five point scale, for th following two statements: (Q1) There is a need to improv the security of current PIN entry method (Q2) I am willin to spend more time to enter my ATM PIN if the new schem provides more security against shoulder surfing.

After answering the above two questions, the partici pants were given a short introduction to our schemes in or der to help them understand its design objectives. Durin this introduction session, participants were also explicitl warned not to point to their chosen PIN digits, e.g., by us ing their fingers, when they are trying to align them becaus this action may help reveal their PINs to shoulder-surfers Then each participant was asked to choose a PIN numbe that she/he is familiar with and register it through our eval uation software. Each subject was allowed to try the syster for five times before the beginning of the actual testing ses sion. Both the short introduction above and the trial sessior combined, required about 5 minutes to complete.

During the test session, each user was asked to enter their PIN for 10 times using different variants. The system was designed to record the PIN entry time, and count the number of incorrect logins. Finally, after the experiment, participants were asked to (Q3) express their satisfaction about the new system, on a five point scale. Additionally, in order to have a more insight into the security of our scheme, participant were asked, (Q4), if they had a specific preferences in choosing the direction of the sector in which they align their PINs. Unlike some other graphical PIN entry scheme where complex PIN entry procedure or the images chosen by the users might be forgotten, no follow up sessions were needed in our evaluation process since our system require users to only remember their PINs which is the same requirement for current PIN entry systems.

5.1. Results

The participants' response for the first two questions are shown in Figure 4 (SA: strongly agree, A: agree, N: neutral, D: disagree, and SD: strongly disagree). Figure 5 shows the users response to the statement "I am totally satisfied with this new PIN entry scheme" for $VO(1)$ and $VT(1)$.

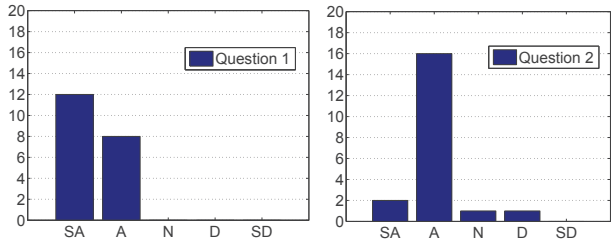

Figure 4. Answers to Q1 and Q2

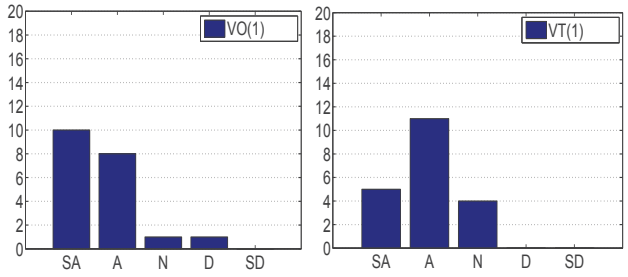

Figure 5. Response to Q3 for $VO(1)$ and $VT(1)$

Table 2 shows both mean PIN entry time and standard deviations for different variants of our proposed scheme. It is interesting to note that $VT(1)$, despite requiring two rounds to enter the PIN, has slightly shorter mean entry time compared to $VO(1)$. This can be explained by the fact that many participants felt more comfortable dealing with user interfaces having less number of digits. It should be noted that, throughout our experiments we used the *mouse* to to rotate the wheels during the PIN entry process. In practical application where touch screens or push bottoms are available, a considerable decrease in the mean entry time should be expected.

Table 2. Mean and standard deviations of PIN entry time

	Mean(seconds)	StdDev(seconds)
VO(1)	11.70	1.551
VO(2)	12.74	2.553
VO(3)	16.32	3.802
VT(1)	10.57	2.983

None of the participants made any mistake while entering their PINs after the practise session. Based on the feedback from participants, they felt that the system was easy to use and does not require them to remember any new information besides their regular PINs.

As for question 4, 80% of participants said that they did not give any preference to the position of the sector in which they align their PINs. Usually, they just tried to find the position of one digit of their PIN, then aligned the remaining digits in that position. However, 20% of participants had some preferred positions into which they aligned their PINs. For example, one participant always tried to align her PIN towards the 12 o'clock direction, while another participant preferred the 3 o'clock direction. Another two participants gave preference to a random (but fixed) area of the wheel.

It should also be noted that despite the fact that the average login time using $VT(1)$ was less than the corresponding time for $VO(1)$, a larger number of participants were strongly satisfied with VO because it requires only one round for successful authentication.

6. Conclusions

In this paper, we proposed a new shoulder-surfing resilient PIN entry scheme that achieves a good balance between security and usability. Different variants of the proposed scheme display a trade-off in resisting various types of adversaries, and thus the selection of an appropriate variant can be optimized considering the types and frequencies of risks encountered in the application. Furthermore, based on the usability results, the new methods seem to be intuitive and easy to use and do not require users to memorize any other information besides their regular PINs.

7. References

[1] ATMScam. Bank ATMs converted to steal bank customer ids. http://www.utexas.edu/police/alerts/atm_scam/. Accessed Jan 16th, 2009.

[2] M. Brader. Shoulder-surfing automated. *Risks Digest*, 19, 1998.

[3] P. Golle and D. Wagner. Cryptanalysis of a cognitive authentication scheme (extended abstract). In *Proc. of the 2007 IEEE Symposium on Security and Privacy (S&P 2007)*, pages 66–70, Oakland, California, USA, May 2007. IEEE Computer Society.

[4] G. A. Miller. The magical number seven, plus or minus two: Some limits on our capacity for processing informatio. *Psychological Review*, 63:81–97, 1956.

[5] Passfaces. http://www.realuser.com/. Accessed Jan 10th, 2009.

[6] V. Roth, K. Richter, and R. Freidinger. A pin-entry method resilient against shoulder surfing. In *Proc. of 11th ACM Conference on Computer and Communication Security (CCS 2004)*, pages 236–245, Washington DC, USA, October 2004. ACM Press.

[7] P. Shi, B. Zhu, and A. Youssef. A new pin entry scheme against recording-based shoulder-surfing. In *Proc. of 3rd International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2009)*, Athens/Vouliagmeni, Greece, June 2009. IEEE Computer Society.

[8] C. Summers and S. Toyne. Gangs preying on cash machines. http://news.bbc.co.uk/2/hi/uk_news/3157214.stm, Oct. 2003. Accessed Dec 4th, 2009.

[9] Swivel. PINsafe. http://www.swivelsecure.com/?page=principlesofpinsafe. Accessed Nov 26th, 2008.

[10] E. K. Vogel and M. G. Machizawa. Neural activity predicts individual differences in visual working memory capacity. *Nature*, 428:748–751, April 2004.

[11] D. Weinshall. Cognitive authentication schemes safe against spyware (short paper). In *Proc. of the 2006 IEEE Symposium on Security and Privacy (S&P 2006)*, pages 295–300, Berkeley/Oakland, California, USA, May 2006. IEEE Computer Society.

[12] S. Wiedenbeck, J. Waters, L. Sobrado, and J.-C. Birget. Design and evaluation of a shoulder-surfing resistant graphical password scheme. In *Proc. of the working conference on Advanced visual interfaces (AVI 2006)*, pages 177–184, Venezia, Italy, May 2006. ACM Press.