2009 Third International Conference on Emerging Security Information, Systems and Technologies

A PIN Entry Scheme Resistant to Recording-based Shoulder-Surfing

Peipei Shi, Bo Zhu, and Amr Youssef
Concordia Institute for Information Systems Engineering
Concordia University
Montreal, Quebec, H3G 2W1, Canada
{pe_sh, zhubo, youssef}@ciise.concordia.ca

Abstract

Two-factor authentication techniques using combination of magnetic cards and personal identification numbers (PINs) are widely used in many applications including automatic teller machines and point of sales. Similar to other valuable personal possessions, cards can be easily stolen by pickpockets. Furthermore, recent security reports show that magnetic cards can be easily duplicated using fake card readers and PINs can be obtained by shoulder surfing legitimate users' PIN entry processes. With this combination, criminals can easily break into users' accounts which represents a great threat. In this paper, we propose a new PIN entry scheme which is resistant against shoulder-surfing attacks conducted by shoulder-surfers with normal cognitive capabilities. Additionally, this scheme offers a relatively good level of security when the shoulder-surfer can record the entire login procedure for one or two times with a video device. Mathematical analysis of the proposed scheme is also presented.

Keywords: Secure PIN entry, shoulder surfing

1. Introduction

Nowadays, most payment services at Point of Sales (PoSs) and bank account services at Automatic Teller Machines (ATMs) are protected by a combination of certain unique information stored on a physical device, typically a magnetic stripe card, and PINs. To be successfully authenticated, an adversary has to obtain both information.

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 the PIN, and thus is subjected to shoulder-surfing attacks.

Apparently, the effectiveness of shoulder-surfing attacks is highly dependent on the adversary's ability to record the victim's login process. In the simplest scenario, the shoulder-surfer may just stands behind the victim and looks over his/her shoulder to obtain passwords, PINs or other sensitive information. Despite its effectiveness against normal PIN entry schemes, this type of shoulder-surfing attacks is relatively easy to defend against since shoulder-surfers are limited by their cognitive capabilities.

Unfortunately, recent reports [1, 9] show that, with the help of advanced technologies, such as concealed miniature cameras and video mobile phones, the adversaries' capabilities of observing and recording the login process have improved significantly. This class of shoulder-surfing attack has become a serious threat to many security applications that rely on the combination of magnetic stripe cards and PINs to perform the authentication.

In this paper, we distinguish between the above two types of attacks by naming them as *cognitive shoulder-surfing* and *recording-based shoulder-surfing*, respectively.

To address the shoulder-surfing issue, several challenge-response-based approaches are proposed [7, 12, 13]. In order to protect users' PINs, they usually require users to interact with systems multiple rounds and do not provide direct feedback. As a result, the login procedure can be very long [12, 13], which makes these schemes unsuitable for many real-world scenarios, e.g., when there is a long queue of customers waiting for account services in front of an ATM. Hence, it is desirable to design a solution applicable in the scenarios where the requirements on both security and real-time response are important.

Further security protection beyond the combination of a magnetic stripe card and PIN includes biometric authentication [3] and one-time keypad [8, 10]. These solutions are not widely used at the current time, mainly due to their requirements of specific hardware and/or the extra overhead in key management. In addition, there also exist specific types of attacks aiming at these solutions. For instance, many commercial fingerprint scanners can be reliably fooled using a combination of cheap kitchen supplies and a digital camera [4]. Detailed discussions about biometric authentication and one-time keypad are out of the scope

978-0-7695-3668-2/09 $25.00 © 2009 IEEE
DOI 10.1109/SECURWARE.2009.43

of this paper.

In here, we propose a new PIN entry scheme in which the PIN is not a sequence of 4 digits but a sequence of 4 locations. Compared to previous work, our scheme excels in achieving a good balance between security and usability. According to our mathematical analysis, this design can offer a strong security protection against adversaries with limited surfing capability, e.g, when the adversary is limited to acquiring only up to two records of the whole process. The usability issue is addressed from two aspects: the time required by the authentication process and the interface design. Our scheme has a short response time while providing strong protection against shoulder-surfing attacks at the same time. In addition, we also discuss few methods that can enhance the usability of our scheme.

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. Background and Related Work

Roth et al. [7] proposed a PIN entry method which offers limited resiliency against shoulder-surfing. In their method, the keys on the keypad are randomly partitioned into two sets, one set is white while the other is black. Depending on the set to which the digit of the PIN under verification belongs, the user enters the key with the same color as the set. Multiple rounds are needed to complete the input of a single digit of the PIN. The same process is repeated until the whole 4-digit PIN is entered. 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. It aims at the case where a shoulder-surfer may acquire one record of the whole login process.

Weinshall [12] proposed two challenge response protocols, one with a high complexity query and the other with a low complexity query. In both protocols, users need to answer a sequence of challenges posed by the login terminal. The challenges are based on a shared secret between the login terminal 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 [2] 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 few seconds after recording only a small number of successful logins.

The Convex Hull Click Scheme (CHC) [13] is another multiple-round challenge-response authentication scheme proposed to fend off shoulder-surfing. In this scheme, the user needs to select a set of icons, out of a larger number of icons, as their password icons. During the login process, to respond to 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.

PassFaces [6] relies on the user's capability of recognizing faces. The user first needs to choose a set of faces as the secret, and have a few minutes of training to be familiar with the chosen faces. The login may take several rounds. For each round, among all the faces displayed only one belongs to the secret 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.

3. Proposed PIN Scheme

3.1. System and Adversary Models

In this paper, we assume that the verifier (e.g., the ATM) is trusted to perform the authentication process correctly, and a sequence of t positions are known only to the user and the verifier. The default value of t is 4. As to the capability of adversaries, we assume that they 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.

We consider both cognitive shoulder-surfing and recording-based shoulder-surfing. In particular, in recording-based shoulder-surfing, we assume that adversaries can acquire up to two records of the whole login process. We argue that such a limitation on the capability of the adversary 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, which is subjected to the limit on the storage or the time frame of regular security checks on ATMs, is slim.

We assume that the verifier keeps a record on the number of successive failed inputs. After three failed attempts, the

verifier will retain the card and terminate the usage of the related account on any ATM, 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. We are aware of the fact that this rule may be misused to launch discontinuous attacks. More specifically, a smart attacker may first make two guesses. If the attacker fails, he/she will wait until the counter is reset, before trying another two. Hence, in our design, the legitimate user will be notified by previous failed login attempts (if any) upon a successful login. As a result, the maximum number of retries that the adversary can make without being detected is two.

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

3.2. PIN Entry Method

For each login, after the user inserts his/her bank card into the ATM, the machine displays an $A \times A$ table, each cell of which contains a number from the set $\{0,\ 1, \ldots, A-1\}$. The assignment of numbers to cells is executed in such a way that A copies of every number in the set are randomly assigned to the cells in the table. Since the PIN in our scheme is a sequence of 4 positions, in the first step, the user needs to input the number displayed within the cell corresponding to the first position. Afterwards, a new $A \times A$ table is generated, and the second number is keyed in according to the second position. The same process is repeated until the user has input 4 numbers. At the end of the login process, if the user inputs all the numbers correctly according to the secret, i.e., the sequence of 4 positions, he/she is authorized to access the account.

The assignments of numbers to the cells in any two displays are completely independent. Note that, although the whole login process consists of four steps, unlike previous work [7, 12, 13], there is only one-round selection per PIN digit in our scheme.

Besides the random assignments of numbers, during the generation of tables, we also consider introducing a colorful display to improve the usability of our scheme, which is discussed in Section 5. Since the distribution of colors are determined independently from the assignments of numbers, security analysis presented in Section 4 is applicable to both the general scheme without colors and the colored designs presented in Section 5.

4. Security Analysis

4.1. Cognitive Shoulder-Surfing

There has been some interesting research on the cognitive capabilities of human beings. In 1956, Miller [5] noted that the limitation on short term memory (STM) is 7 plus or minus 2 symbols. A more recent work by Vogel *et al.* [11] 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 [11]. This discovery is based on the neurophysiological evidence.

According to our design, there will be A$\times$A numbers on the ATM screen per display/step and only one number is input by the user at a time. If we define the combination of the number that a user inputs at one step and the corresponding A positions as a *knowledge set*, then the whole login process generates 4 knowledge sets. Apparently, according to previous research in human's cognitive capabilities [5, 11], remembering all the knowledge sets are far beyond the cognitive capabilities of a typical adversary.

4.2. Recording-based Shoulder-Surfing

Compared to cognitive shoulder-surfing, the adversary is much more powerful in recording-based shoulder-surfing. Some schemes aiming at the former [6] can be trivially broken by a recording-based shoulder-surfing even when the adversary has a relatively limited recording capability. In this section, we concentrate on security analysis of our scheme for scenarios in which the shoulder-surfer can obtain up to two records of the whole login process.

4.2.1 One Login Record

If one record of the whole login process is available, a shoulder-surfer can limit the guess within the knowledge sets. More specifically, the shoulder-surfer randomly chooses a position from the set of positions assigned with the same value as the input. For each position of the PIN, the probability of making a correct guess is $1/A$. Thus, the probability of identifying the whole PIN is $1/A^4$, which ranges from 0.16% to 0.01% when the size of the table varies from 5 to 10.

4.2.2 Two Login Records

We first evaluate the probability that a shoulder-surfer can successfully guess the first position of the PIN, given that he/she can obtain two records of the whole login process. Let us denote this probability as P_1.

In our design, each number in the set (i.e., $\{0,\ 1, \ldots, A-1\}$) is repeated A times in a table. Given that the user en-

tered a number x for the first position during a login process, the shoulder-surfer can deduce that the actual position is among the set of A cells assigned with the number x by checking the corresponding record. Let $L_1 = \{l_1^0, l_1^1, \ldots, l_1^{A-1}\}$ and $L_2 = \{l_2^0, l_2^1, \ldots, l_2^{A-1}\}$ denote the sets of locations corresponding to the first input from the user in the first record and the second record, respectively. Therefore, there is at least one element that belong to both L_1 and L_2, since the actual first position of the PIN must be included in both sets.

Let N denote the set of positions that belong to both L_1 and L_2. Thus, $1 \leq |N| \leq A$. Obviously, when $|N| = 1$, the shoulder-surfer can uniquely identify the first position of the PIN, i.e., the only element in set N. In a more general case, the best strategy of a shoulder-surfer is to pick a position from set N, and the success rate of the guess is equal to $1/|N|$. As a result, P_1 can be calculated as:

$$P_1 = \sum_{|N|=1}^{A} \frac{1}{|N|} \cdot P_{1,\,|N|} \tag{1}$$

where $P_{1,\,|N|}$ denotes the probability that there are $|N|$ elements in common between the two sets of possible positions of the first inputs in the two login processes.

Since the actual first position of the PIN must be in both L_1 and L_2, $P_{1,\,|N|}$ is equivalent to the possibility that the number of elements in common between two sets, each of which is formed by randomly picking $A-1$ cells from the remained A^2-1 cells, is $|N|$. Thus, we have:

$$P_{1,\,|N|} = \frac{\mathrm{C}_{A-1}^{|N|-1} \cdot \mathrm{C}_{A^2-1-(A-1)}^{A-1-(|N|-1)}}{\mathrm{C}_{A^2-1}^{A-1}} = \frac{\mathrm{C}_{A-1}^{|N|-1} \cdot \mathrm{C}_{A^2-A}^{A-|N|}}{\mathrm{C}_{A^2-1}^{A-1}} \tag{2}$$

By combining Equation (1) and Equation (2), we can calculate P_1 as follows:

$$P_1 = \sum_{|N|=1}^{A} \frac{1}{|N|} \cdot \frac{\mathrm{C}_{A-1}^{|N|-1} \cdot \mathrm{C}_{A^2-A}^{A-|N|}}{\mathrm{C}_{A^2-1}^{A-1}} \tag{3}$$

Let P_2, P_3, and P_4 denote the probability that the shoulder-surfer correctly guesses the second, third and fourth digits of the PIN after two records, respectively, given that he/she can obtain two records of the whole login process. Let P_{PIN} denote the probability that the shoulder-surfer correctly guesses the whole PIN given two records. Thus, we have:

$$P_{PIN} = P_1 \cdot P_2 \cdot P_3 \cdot P_4 \tag{4}$$

Since the table is reset before each input from the user, if the 4 positions of the PIN are totally independent from each other, P_i's ($i \in \{1,\ 2,\ 3,\ 4\}$) have the same value. Thus, we have:

$$P_{PIN} = P_1^4 \tag{5}$$

According to Equation (5), the success rate of a shoulder-surfer correctly guesses the whole PIN ranges from 25% to 20%, when the size of the table (i.e., A) is set from 5 to 10. Since the maximum number of retries that the adversary can make without being detected is 2, our scheme can provide sufficient protection given that the shoulder-surfer can acquire two login records.

5 Usability Issues

Like many other security applications, there is always a trade-off between security and usability. Meanwhile, usability is one of the most important factors that affect the acceptance of a new security solution in reality.

Usability in our scheme is mainly relevant to two issues: (i) the difficulty of either searching/identifying a specific position in the table; (ii) the difficulty of memorizing all the positions of a PIN.

As indicated in Section 4, the security of our design is not very sensitive to the size of the table. Thus, a natural choice is to select a small table size, and it is helpful in addressing both issues relevant to usability. In the following examples of design patterns, we set the table size to 6.

Figure 1. An example of colored patterns in displayed tables

Another method that may improve the usability of our scheme is to use a colorful display. The basic idea is to use the contrast between different colors to enhance the identification and memorization of the positions in a table. Thus, the following rule is proposed to guide the design of the login interface: for any cell, at most two of its *directly-connected* cells have the same color as itself. *directly-connected* cells refers to cells that share one and only one edge with each other. According to this rule, we can generate many different displayed patterns. Two examples are shown in Figure 1 and Figure 2. Furthermore, in

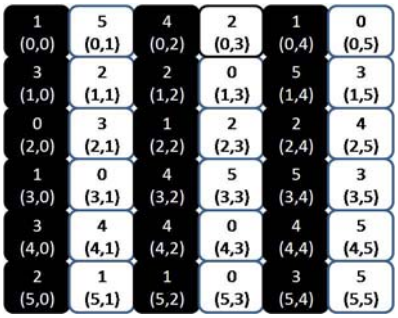

Figure 2. Another example of patterns in displayed tables

Figure 2, besides following the above rule for coloring the display, we also include the pair of coordinates as part of information displayed on each cell so as to easily identify a specific position. These coordinates might be of more help to users who find it easier to remember numbers compared to remembering a set of locations or patterns.

Some users, e.g., color-blinded people, may have difficulty in color recognition but are more sensitive to geometric shapes or paths. Thus, they may choose certain geometric shape (or path) as the PIN, where each input/position is a vertex (or an endpoint of a sub-path). Such a way of choosing a PIN has certain impacts on security, because the positions of a PIN are distinct and thus the choices of positions are not totally independent. However, we can still use P_1^4 as an approximate estimation of P_{PIN}. For example, our simulation results show that there is only around 1% difference between P_1^4 and the actual rate of guessing the PIN, when the table size is 6.

6 Conclusion and Future Work

In this paper, we proposed a new PIN entry scheme that achieves a good balance between security and usability from the perspective of response time and user interface design. Our analysis shows that, our scheme is resilient to shoulder-surfing, given that the attacker has limited capability in recording the login process. In addition, unlike previous challenge-response protocols, our scheme requires only one response per digit/position of the PIN, and thus excels in real-time response. Finally, we discussed a few methods for improving the usability of our scheme and showed two sample designs.

References

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

[2] 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.

[3] M. Kumar, T. Garfinkel, D. Boneh, and T. Winograd. Reducing shoulder-surfing by using gaze-based password entry. In *Proc. of the 3rd Symposium On Usable Privacy and Security (SOUPS 2007)*, Pittsburgh, PA, USA, July 2007.

[4] J. Leyden. Gummi bears defeat fingerprint sensors. *ISI insight*, 11-05, Nov. 2005.

[5] 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.

[6] Passfaces. http://www.realuser.com/.

[7] 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.

[8] Schlage. Scramble keypad reader (SERIII-w).

[9] C. Summers and S. Toyne. Gangs preying on cash machines. BBC NEWS Online, Oct. 2003.

[10] Swivel. PINsafe.

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

[12] 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.

[13] 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.