Modeling and Analysis of Regular PIN Entry Method and Its Improvement*

Sooyeon Shin, Sarang Na, Taekyoung Kwon**, and Hyeonjoon Moon

Sejong University, Seoul, South Korea
{shinsy80,tot}Osju.ac.kr, {tkwon,hmoon}@sejong.ac .kr

Abstract. In this paper, we present STM-GOMS, an improvement of GOMS-based model for analyzing not only usability but also security of authentication methods in the way of considering memory limitations formally in the same model. This work is based on the previous work, in which CPM-GOMS, one of GOMS variants was utilized for the same purpose, but is more extended with regard to the memory limitations of user and adversary. We apply our model to the regular PIN entry method and study three improvement attempts based on the modeling results. Two trivial improvements failed but the last one could survive in terms of security without severely deteriorating its usability.

Keywords: GOMS, Shoulder Surfing, Usability, Security

1 Introduction

Personal Identification Numbers (PINs) [10] are widely used in modern information systems for authenticating users. Unfortunately, classical regular PIN entry methods are vulnerable to shoulder surfing attacks, i.e., PINs can be stolen at a user interface quite easily. When they are used in mobile devices such as smartphones and tablet PCs, those threats are more likely to increase. To cope with this problem, there have been a number of studies of constructing new methods in the security community but a study of modeling and analysis is quite rare: To the best of our knowledge, Kwon et al.'s work was unique [7].

The basic idea given in [7] was to use a human performance modeling tool for modeling not only a user but also an adversary who is another human, in order to analyze security and usability of authentication methods. The human performance modeling tool utilized in Kwon et al.'s work was the famous CPM-GOMS [5], which is one of GOMS variants. GOMS stands for Goals, Operators, Methods, and Selection rules [1], and is a family of cognitive models for analyzing human performance and for predicting the procedural aspects of usability in terms of MHP (Model Human Processor) [2]. In the previous work, we have found

* This work was supported in part by the IT R&D program of MKE/KEIT [10039180, Intuitive, convenient, and secure HCI-based usable security technologies for mobile authentication and security enhancement in mobile computing environments]. This work was also supported in part by the National Research Foundation of Korea Grant funded by the Korean Government(MEST) (NRF-2012-R1A1B3-000965)

' T. Kwon is the corresponding author.

that the GOMS models, including CPM-GOMS, are lack of memory management and error manipulation in user modelings but as for security against shoulder surfing attacks, it is quite significant to consider both user's and adversary's memory limitations within the same formal model. Thus, it should be promising to further consider the modeling of memory as well as perceptual and cognitive tasks in the GOMS-based models.

In this paper, we present STM-GOMS, an improvement of GOMS-based model for analyzing usability and security against shoulder surfing attacks for the environments of using smart devices. As we mentioned, the principal idea and its starting point must be to consider memory limitations of humans as well as perceptual and cognitive capabilities. That is, STM-GOMS enhances CPM-GOMS in the way of manipulating memory queues in modelings. STM-GOMS can provide concrete evidence of security against shoulder surfing attacks and facilitate additional assessment items for a rigorous analysis of usability; memory and interface complexities. We then apply the STM-GOMS model for analyzing the usability and security of the regular PIN entry method. As a consequence, we show formally that the regular method is vulnerable to a shoulder surfing attack. In the same modeling paradigm, we also study three improvement attempts based on the modeling results. Two trivial improvements failed but the last one could survive in terms of security without severely deteriorating its usability. Finally, we conduct user experiments to show the results that support the validity of STM-GOMS modeling and analysis.

2 STM-GOMS

STM-GOMS stands for two things: Security and Threat Model and a model for Smart-Touch-Mobile devices. Using a regular PIN entry method (Regular PIN), we describe how to construct the STM-GOMS model and how to apply this model for analyzing usability and security of authentication methods.

2.1 Concept

Based on the view that shoulder surfers are also humans, STM-GOMS adopts the MHP for modeling the tasks of both users and shoulder surfers. There are three categories of human memory in the MHP: sensory memory (SM), working memory (WM) and long-term memory (LTM). WM is generally considered to have limited capacity. The MHP assumes that the capacity of WM is roughly 7 ± 2 chunks due to "Magic Number Seven" by Miller [8]. In modern research, Cowan suggested the capacity of WM is limited to 3-4 chunks in young adults [3],[4]. According to the Cowan's suggestion, STM-GOMS assumes that the WM's capacity is 4 chunks instead of 7 chunks.

Since CPM-GOMS only provides operators for desktop computer systems, it is necessary to add new operators for mobile smart device environments. For this purpose, we add new operators for moving fingers and touching screens to STM-GOMS and we estimate time for operating them by conducting an experiment using a software tool on an Android smartphone. As with the extreme-expertise assumption of CPM-GOMS, we recruited 12-expert users (average age is 28.7

and average smartphone user time is 2.5 years). The estimated time for finger move and touch operators are 250 ms and 110 ms, respectively. In STM-GOMS, we assume that those two operators can be regarded as one operator (360 ms), finger move and touch, except for the case that finger touch is needed separately. The evaluation time for other operators follows CPM-GOMS.

2.2 Execution phases

STM-GOMS modeling starts with task analysis that specifies a user task and a shoulder surfer task according to the CPM-GOMS-style schedule charts [5]. The next step is to add memory parts of the MHP to those charts. Fig. 1 shows the modeling of user and shoulder surfer tasks for the first iteration in Regular PIN.

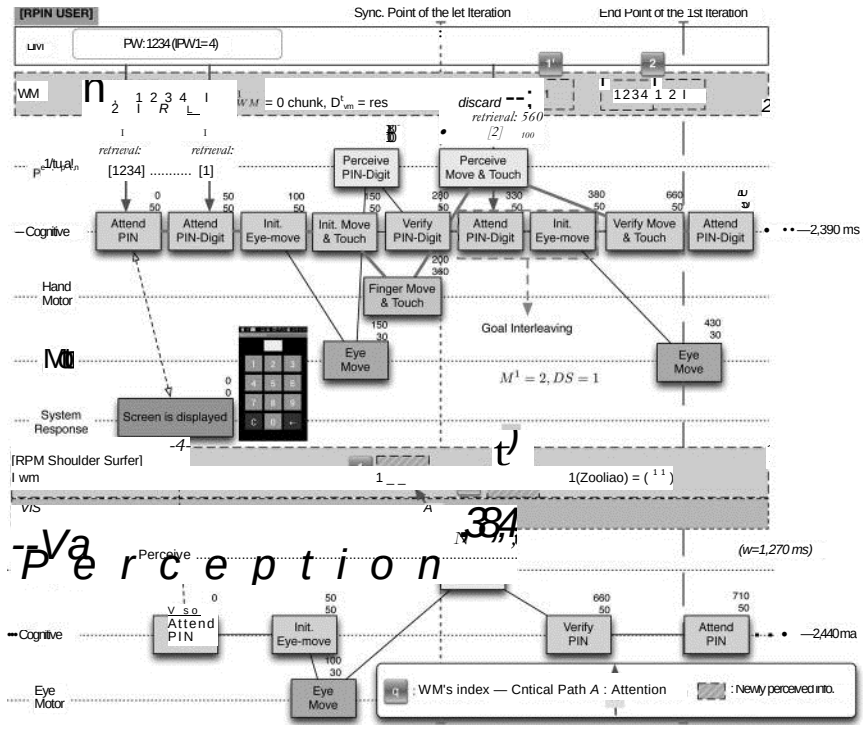

Fig. 1. The synchronized schedule charts for Regular PIN (User's PIN: "1234").

For usability analysis in STM-GOMS, an analyst firstly estimates the total execution time *(Tu)* for the user task. In the case of Regular PIN, the estimated execution time of the first iteration is 710 ms, implying T_u = 2390 ms. If the displayed screen is unchanged in two iterations, it is possible to include a part of operators in the next iteration among the previous iteration by goal interleaving. The analyst then estimates a memory complexity denoted by *CMEM* = *[RLTM RWM(DWM)1,* where $_{RLTM}$ and *RWM* are the number of the required chunks for LTM and WM, respectively, and *DWM* is the required duration for holding the new information in WM. The length of PIN corresponds to $_{RLTM}$ such that *RLTM* = 4. STM-GOMS counts not information retrieved from LTM but new information in *RWM,* such that *RWM* = 0 and *DWM* = 0 in Regular PIN.

The analyst estimates a user interface complexity denoted by *Cul = [DS, M],* where *DS* is the number of displayed screens during the user's task and *M* is the number of motor operators required for the task. In each iteration of Regular PIN, 1 eye move and 1 finger move and touch are required and the firstly displayed screen is unchanged, such that *M* = 8 and *DS* = 1 for the total task.

For security analysis, the analyst makes a synchronization between the user and shoulder surfer tasks by considering the observation point. For example, through eye move and visual perception, a shoulder surfer of Regular PIN observes the user's motor operator for key entry to obtain the user's PIN. Thus, these operators are synchronized (Sync. Point of the 1st iteration in Fig. 1). The analyst estimates a waiting time w based on the synchronization point. If the previous execution time on the shoulder surfer's critical path based on the point is shorter than the user's execution time, then the shoulder surfer has spare time (w > 0). Otherwise, the shoulder surfer dose not have enough time (w < 0) for observation. In Fig. 1, the estimated waiting time w^1 at the first sync. point is 430 ms, implying w = 1270 ms in total. The analyst also estimates the difference of the execution time, *x,* between the user and shoulder surfer. Through the synchronization for the whole tasks, the pure attack time *TA* is estimated as follows; $TA = T_u - \omega x$. The pure attack time of Regular PIN is 1170 ms *(< TO.* The first success condition of a shoulder surfing attack is *TA <Tu.*

The capabilities of both perception and memory have decisive effects on the success or failure of a shoulder surfing attack. If the shoulder surfer can perceive enough information that he/she has to perceive for the success of the attack within the limited time, the attack will succeed. Thus, STM-GOMS counts an information rate for perception denoted by /1„ such that */p = (/cp//Hp)* * 100, where *Icp* is the number of chunks that an attacker can perceive within the given time and *_THP* is the number of chunks that an attacker has to perceive to succeed the attack. In the first iteration of Regular PIN, the attacker has to perceive a single number and he/she can perceive it due to the enough perceiving time including the waiting time and the enough capacity of WM, such that Zp = 100%. The second condition of the attack is ip = 100%; if $1p$ 100%, the attack fails, regardless of the first success condition.

3 Improvement of Regular PIN

We make three types of improvements to Regular PIN; they will be referred to as Improved PIN 1, Improved PIN 2 and Improved PIN 3. We then show the results of usability and security analysis of those improvements through STM-GOMS. Through real experiments, we verify all analysis results of STM-GOMS.

3.1 Analysis of improved methods

In general, randomness tends to be useful for improving security. We first consider two types of improvements (Improved PIN 1 and Improved PIN 2) in which randomness is added to Regular PIN; using one random key pad for the whole PIN-digits entry and for each PIN-digit entry, respectively. Due to the limited space, we omit the detailed descriptions.

We obtained the results that two improvements are still insecure against shoulder surfing attacks while they have the same or low usability. We thus improve Regular PIN from the STM-GOMS view. For deteriorating the chance of successful shoulder surfing attacks, it is necessary to find a way to increase T_{HP} or to decrease I_{cp}. From this point of view, we consider another improvement (Improved PIN 3) resilient to shoulder surfing attacks without severely deteriorating usability of a user task. A user finds 4-digits PIN at the firstly displayed random key pad and remembers the four locations of PIN. The user then touches any part of the first pad and the second random key pad is given to the user. Finally, the user should touch numbers corresponding to the perceived PIN's locations in order at the second pad. Fig. 2 shows the partial schedule charts of a shoulder surfer due to the limited space. To launch a shoulder surfing attack, the attacker should perceive all numbers with the order from the first random key pad by moving eye three times. Since the attacker should perceive 3 or 4 numbers and their locations for each eye move, we set 290-387 ms with regard of CPM-GOMS; 290 ms to perceive a complex visual signal similar to a 6-letter word [6]. The necessary capacity of WM is 3. The attacker should perceive four user's inputs and the necessary capacity of WM is 4. As we mentioned, the capacity of WM is limited to 4 chunks in STM-GOMS. In WM, new information gradually pushes out older information, unless the older information is actively protected by rehearsal or by directing attention to it [9]. The previous 3 chunks perceived from the first pad will be decayed and substituted with the 4 chunks perceived newly from the second pad. Due to the limited capacity of WM, the information rate for perception is $/p = 4/7 * 100 = 57.14\%$. Although the pure attack time is larger than the user's execution time, Improved PIN 3 is secure against the shoulder surfing attack according to the second success condition.

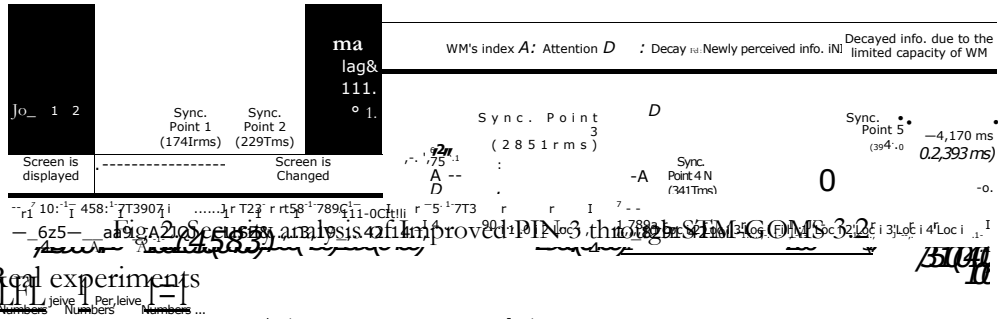

Fig. 2. Security analysis of Improved PIN 3 through STM-GOMS 3.2

Real experiments

We recruited 10 participants (8 males, 2 females) whose average age was 27.6 years. Participants who conducted usage and attack experiments for the four methods had to complete 10 sessions per each scheme. The method having the fastest average of entry time is Regular PIN. Improved PIN 2 was slower than other methods. In the attack experiments, although participants succeeded to identify the all PINs for the first three methods, they failed to guess all digits of

PIN in case of the Improved PIN 3. Table 1 shows the analysis results of STM-GOMS and experimental results for four methods. There were no significant difference between the model's analysis and experiments results. Thus, we believe the results of security and usability analysis trough STM-GOMS are reliable.

Table 1. Usability and security analysis results of Regular PIN and its improvements (Exp.: experimental results, *Ps:* attack success probability, S/F: Success or Fail)

Ver.	Usability				Security			
	CMEM	*Cui*	*Tu*	*Tu* (Exp.)	*TA*	*Ip*	*Ps* (Exp.)	S/F
Regular	Regular$_{r1}$ [4:0(0)]	[4,8]	2390 ms	1911 ms	1170 ms < *Tu*	*100%*	*100%*	S
Improved 1			2920 ms	2777 ms				
Improved 2		[4,8]	3610 ms	4079 ms				
Improved 3	[4:4(3740)	[2,13	4120 ms	3949 ms	1777 ms < *Tu*	57.14%	0%	F

4 Conclusion and Future Works

We presented STM-GOMS, an improvement of GOMS-based model for analyzing both usability and security of authentication methods in the way of considering memory limitations. We applied the STM-GOMS model to the regular PIN method and its improvements. Through real experiments, we showed the validity of analysis results of STM-GOMS. We are improving STM-GOMS to cover security analysis against other observation attacks such as a recording attack and spyware. We will apply STM-GOMS to various authentication methods.

References

1. Card, S.K., Moran, T.P., Newell, A.: The psychology of human-computer interaction. Lawrence Erlbaum, Hillsdale, N.J., (1983)
2. Card, S.K., Moran, T.P., Newell, A.: The Model Human Processor: An Engineering Model of Human Performance. In: Handbook of Perception and Human Performance. Vol. 2: Cognitive Processes and Performance, pp. 1-35 (1986)
3. Cowan, N.: The magical number 4 in short-term memory: A reconsideration of mental storage capacity. Behavioral and Brain Sciences. 24 (1), pp. 87-114 (2001)
4. Cowan, N.: The Magical Mystery Four: How is Working Memory Capacity Limited, and Why? Psychological Science. 19(1), pp. 51-57 (2010)
5. Gray, W.D., John, B.E., Atwood, M.E.: The Precis of Project Ernestine or an overview of a validation of GOMS. In: the SIGCHI conference on Human factors in computing system. (1992)
6. John, B.E., Gray, W.D.: GOMS Analyses for Parallel Activities. In: Tutorial Notes, CHI, ACM Press, New York (1995)
7. Kwon, T., Shin, S., Park, S., Park, Na, S.: Covert Attentional Shoulder Surfing: A Counterattack on the PIN-Entry Method Resilient Against Shoulder Surfing or Human Adversaries Are More Powerful Than Expected, *Submitted.*
8. Miller, G.A.: The magical number seven, plus or minus two: Some limits on our capacity for processing information. Psychological Review. 63 (2), pp. 81-97 (1956)
9. Oberauer, K., Kliegl, R.: A formal model of capacity limits in working memory. Journal of Memory and Language. 55, pp. 601-626 (2006)
10. ISO 9564-1:2002 Banking - Personal Identification Number (PIN) management and security - Part 1: Basic principles and requirements for online PIN handling in ATM and POS systems, clause 5.4 Packaging considerations.