TWO-FACED HUMAN–MACHINE INTERFACE FOR PRACTICAL ENFORCEMENT OF PIN ENTRY SECURITY

Mr. S. Suresh Kumar
Assistant Professor,
Computer Science and Engineering
Ponnaiyah Ramajayam Institute of Science and Technology [PRIST]
Tamil Nadu, India.
suresh.333.mecse@gmail.com

Mr.T. Balasathuragiri
Assistant Professor,
Computer Science and Engineering
Ponnaiyah Ramajayam Institute of Science and Technology [PRIST]
Tamil Nadu, India.
balasathuragiri.t@gmail.com

Abstract—

Users typically reuse the same personalized identification number (PIN) for multiple systems and in numerous sessions. Direct PIN entries are highly susceptible to shoulder-surfing attacks as attackers can effectively observe PIN entry with concealed cameras. Indirect PIN entry methods proposed as countermeasures are rarely deployed because they demand a heavier cognitive workload for users. To achieve security and us-ability, we present a practical indirect PIN entry method called *SteganoPIN*. The human–machine interface of SteganoPIN is two numeric keypads, one covered and the other open, designed to physically block shoulder-surfing attacks. After locating a long-term PIN in the more typical layout, through the covered permuted keypad, a user generates a one-time PIN that can safely be entered in plain view of attackers. Forty-eight partici-pants were involved in investigating the PIN entry time and error rate of SteganoPIN. Our experimental manipulation used a within-subject facto-rial design with two independent variables: PIN entry system (standard PIN, SteganoPIN) and PIN type (system-chosen PIN, user-chosen PIN). The PIN entry time in SteganoPIN (5.4–5.7 s) was slower but acceptable, and the error rate (0–2.1%) was not significantly different from that of the standard PIN. SteganoPIN is resilient to camera-based shoulder-surfing at-tacks over multiple authentication sessions. It remains limited to PIN-based authentication.

Index Terms—Authentication, human–machine interaction, personal-ized identification number (PIN) entry, security, shoulder-surfing**.**

1:INTRODUCTION

A. Personalized Identification Number Entry Security Problems

Personal identification numbers (PINs), typically constructed and memorized, are widely used as numerical passwords for user authentication or various unlocking purposes. Their appli-cation is increasing because modern touchscreens can facilitate convenient implementation of the PIN entry interface on a va-riety of commodity machines and devices, including automated teller machines (ATMs), point-of-sale (POS) terminals, debit card terminals, digital door-locks, smartphones, and tablet com-puters.

Unfortunately, when a user *directly* enters a secret PIN into such systems, security is easily compromised, particularly in public places. Nearby people can observe PIN entry by *shoulder-surfing* with or without concealed cameras [1], [2]. The *human-only shoulder-surfing* attacker is defined as a weak adversary who has no automatic recording device, but may use manual tools such as a paper and pencil [3]. The perceptual and cognitive capabilities of human-only attackers are confined to those of humans [4]. The *camera-based shoulder-surfing* at-tacker is defined as a stronger adversary assisted by an automatic recording tool, such as a wearable camera, to record and analyze entire transactions effectively even at long range [2]. Moreover, adversaries who have already mounted shoulder-surfing attacks and collected multiple PIN candidates can attempt to impersonate a user. The *active-guessing* attacker is an adversary who attempts guesses with PIN candidates. Such an attacker can become more powerful when she repeats camera-based observation of the same user and system [5]. Remote connected observation is also becoming a concern because high-resolution cameras are being distributed and networked in public places [6], [7]. The recent trend of targeting attacks and the advent of wearable computers make repeated camera-based shoulder-surfing attacks an increasingly realistic threat to the PIN user interface .The number of PIN candidates must remain sufficiently large to reduce information leakage even if a user's PIN entries are repeatedly observed by adversaries. Even partial information leakage could be harmful because users typically reuse identical or at least similar PINs for multiple systems. Furthermore, a token and/or ID often combined with a PIN can be pickpocketed or skimmed by adversaries using other physical channels [8], Thus, once a secret PIN is compromised, a user could be exposed to multiple breaches of security.

II:STEGANOPIN SYSTEM

To address camera-based shoulder-surfing attacks over mul-tiple authentication sessions and also to migrate users already familiar with the standard PIN entry system, this paper presents a novel PIN entry method called *SteganoPIN*.

The SteganoPIN system builds on the concept of challenge-response rendered over a user interface [10], [25] and physical hand protection [23], [24] to advance the following goals for PIN-based authentication.

1) *Usability*: Must use the regular numeric keypad for key entry. Must incur limited increases in PIN entry time and error rates. Must not increase the length of a long-term PIN. Must stay within the short-term memory requirements of human limitations, such as four groups of items [26], [27].
2) *Strong Security*: Must be resilient to camera-based shoulder-surfing attacks over multiple authentication sessions. Must resist active guessing attacks without allowing more advan-tage than random guessing.

A. Concept

In Greek, the word *stegano* means concealed or protected. Here, the numeric keys entered by users in plain view of adver-saries must be one-time PIN (OTP) keys that conceal a real PIN following instant derivation. To make such a derivation process simple for users, we incorporate a *two-faced keypad system*, which means a novel user interface with two numeric keypads [see Fig. 1(a) and (c)]. To make such a derivation process secure against adversaries, we incorporate a *human–machine interac-tive protection* method (see Fig. 2).

1) *Two-Faced Keypad System:* In the basic user interface of SteganoPIN, one numeric keypad is a standard keypad in *regular layout* and the other is a small separate keypad in a *random layout*. The random layout keypad is called the *challenge keypad* because it permutes ten numeric keys as a random challenge, as in Fig. 1(a). A user must use this challenge keypad to derive a fresh OTP. As in Fig. 1(b), the user first locates a long-term PIN in regular layout and subsequently maps the key locations into the challenge keypad for OTP derivation. The user then enters the OTP on a regular layout keypad called the *response keypad*, as in Fig. 1(c).

The procedure can be repeated if the PIN length (i.e., the mapped OTP length) is greater than the limitation of the user's short-term memory or if the OTP is forgotten before entry. When the user revisits the challenge keypad explicitly, the system must refresh the random challenges. Due to the random mapping between the two keypads, the system can verify the user's PIN from the OTP entry.

In the two-faced keypad system, users' familiarity with the regular key locations of the long-term PIN can ease the OTP derivation process, but as shown in Fig. 1(d), an alternative de-sign of the challenge keypad incorporates regular indicators. Our SwitchPIN [25] was an early version of this method. We first designed SwitchPIN to secure PIN entry on a smartphone from human shoulder-surfers. In SwitchPIN, the user holds a show key to switch a regular layout keypad to a random permuted keypad for OTP derivation on the smartphone's touchscreen and then releases the show key to switch back to the regular key-pad for key entry. SwitchPIN was vulnerable to camera-based shoulder-surfing attacks in only a single session and to a human shoulder-surfer over multiple sessions because the random key-pad just replaced the regular keypad in the same location. Thus, in this study, we separated the two keypads and reduced the size of the random challenge keypad.

2) Human–Machine Interactive Protection: In the user in-terface of SteganoPIN, the challenge keypad does not appear immediately; only the response keypad appears in its regular
layout and size. The SteganoPIN system instead displays a small circle, 20 mm (0.787) in diameter [see Fig. 2(a)]. It shows the challenge keypad only when a user cups a hand on the circle with the grip circularly closed in a ρ-shape [see Fig. 2(b)]. The chal-lenge keypad then shows up after a small delay and disappears immediately when the user releases the cupped hand. Using this procedure, the human user and the machine system can inter-actively protect the challenge keypad by visually occluding it from adversaries. The small size of the challenge keypad can also contribute to the visual occlusion by making the user get closer to it.

A modern touchscreen, whether resistive or capacitive, is aimed at responding promptly and accurately to the touch of one or more fingers making tapping or dragging actions. Thus, implementation issues remain for the circular touch area, similar to those in [23] and [24]. First, there might be no response be-cause the cupped hand is bigger than a finger on a touchscreen.

Second, an inadvertent or lazy user could bypass the circle with-out satisfying the cupped hand grip. Although a touchscreen that accurately responds to a cupped hand is desirable, a *proximity sensor*, available on new smartphones, could be used as an addi-tional tool. As illustrated in Fig. 2(a), the circle is located on the touchscreen close to the proximity sensor. Both proximity (first) and touch (second) somewhere around the circle are required, and the most comfortable and effective posture satisfying the re-quirements is the cupped hand grip. If either of those conditions is released, the challenge keypad must disappear.

3) Prototype System: We implemented a prototype system of SteganoPIN to simulate a horizontal ATM interface with a smartphone (to sense both proximity and touch events on the challenge keypad) and a tablet (to implement the response key-pad), as in Fig. 3(a). For OTP derivation, the user puts a cupped hand on the circle as in Fig. 3(b) and reads the challenge keypad. For OTP entry, the user presses numeric keys on the response keypad as in Fig. 3(c). If the user forgets part of the OTP or the PIN length is greater than four digits, the user could repeat the procedure with another random challenge. Furthermore, hand use is flexible; for instance, *a single hand* for both OTP derivation and entry or *both hands* for OTP derivation work equally well. In practice, it is desirable to implement the circular touch area on both sides for right-handed and left-handed users.

B. Stegano PIN Security

To resist shoulder-surfing attacks, Stegano PIN uses a ran-dom challenge from a permuted keypad covered by a cupped hand. Adversaries could not derive a real PIN from the OTP without being able to see the challenge keypad. To investigate the security of the human–machine interactive protection of SteganoPIN, we simulated an OTP derivation process on an ATM simulation, as in Fig. 4. The user's view was the challenge keypad

inside a cupped hand, as in Fig. 4(a). However, the adversaries' view was visually occluded by the user's cupped hand and body, as in Fig. 4(b). With regard to the cupped hand,



Fig. 3. SteganoPIN concept. (a) System interface, simulation of horizontal ATM interface. Note: We put a smartphone on a tablet to use its proximity sensor. (b) OTP derivation, user view, magnified. (c) OTP entry.

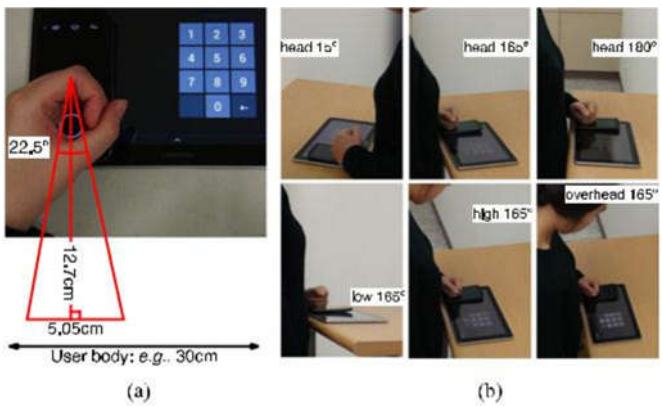

Fig. 4. Analysis of human–machine interactive protection. (a) User view of cupped hand. (b) Adversary view of cupped hand at various angles. (Note: We located the keypads horizontally at the height of real-world ATMs, 94 cm. We filmed the OTP acquisition posture from various angles and heights.)

An open angle (about 22.5°) appeared below the user's thumb (25-year-old graduate student, 160 cm). But as in Fig. 4(a), the width of the open angle grew only to 5.05 cm until it was hin-dered and occluded by the user's body, which was more than 30cm in width. The distance between the cupped hand and the user's body was measured to be 12.7 cm. Thus, we were unable to film inside that angle due to visual occlusion. In our simulation, we changed the location of the adversary to various *angles*, from leftmost (0°) to rightmost (180°), and also *heights* (low, head, high, overhead), but we were not able to film or read the challenge keypad, as in Figs. 4(b) and 5. The

only way to discover the challenge keypad was by interrupting the visual angle between the user and the challenge keypad, which was impractical without being detected. The only concern was that on the overhead snapshot at 180°, a dim light was detected inside the cupped hand, but the photograph did not reveal any challenge keys. Nonetheless, the circular touch area must be in-stalled horizontally as close to the user's body as possible. Even a high-speed camera was very unlikely to capture the challenge keys because of a small delay in their appearance when ac-cessed and the visual occlusion incurred by the movement of the cupped hand when finished.

Overall, SteganoPIN satisfies strong security goals. That is, SteganoPIN is resilient to camera-based shoulder-surfing attacks over multiple authentication sessions if the system is properly installed and used. It is secure against active guessing attacks.

III. USABILITY EVALUATION METHOD

To investigate the performance of SteganoPIN regarding PIN entry time and error rate, we conducted a user study with our prototype system. We hypothesized that users could without difficulty authenticate themselves to the SteganoPIN system by generating an OTP on the basis of a long-term PIN. Although we predicted that SteganoPIN would be slower than the stan-dard system in PIN entry time, we needed to investigate: Is SteganoPIN more error-prone than the standard PIN system? Does the PIN type (that is, easy or complex) affect the perfor-mance of PIN entry? Does SteganoPIN become slower in the longer term intermittent use case? Do users feel it is easy to use SteganoPIN, particularly to manipulate the PIN key locations on the keypad? Finally, are users going to choose SteganoPIN for security-sensitive applications?

A. Participants

A total of 48 participants (19 women, 29 men, mean age: 30.0 years, SD: 6.9 years, age range: 20–49 years) were re-cruited from local universities. After the approval of the Ethical Review Board, we recruited the participants and tried to balance their majors and ages. All participants were asked to bring any corrective eyewear they needed, resulting in (corrected-to) nor-mal eyesight for all. Forty-five participants were right-handed, and three were left-handed. They already had experience with the standard PIN entry system. We gave each of them a small gratuity for participation.

B. Apparatus

The participant's task was making a PIN entry with four-digit PINs. For each task, we implemented the standard PIN entry system and the SteganoPIN system on the Google An-droid platform by simulating the horizontal interface of an ATM with a Galaxy Tab 10.1 (10.1 , 1, 280 × 800 pixels, 149 ppi). The evaluation

prototype system differed from the one in Fig. 3 in that it did not use the smartphone and its prox-imity sensor because of the difficulty in time synchronization between the devices. To accommodate left-handed users, we

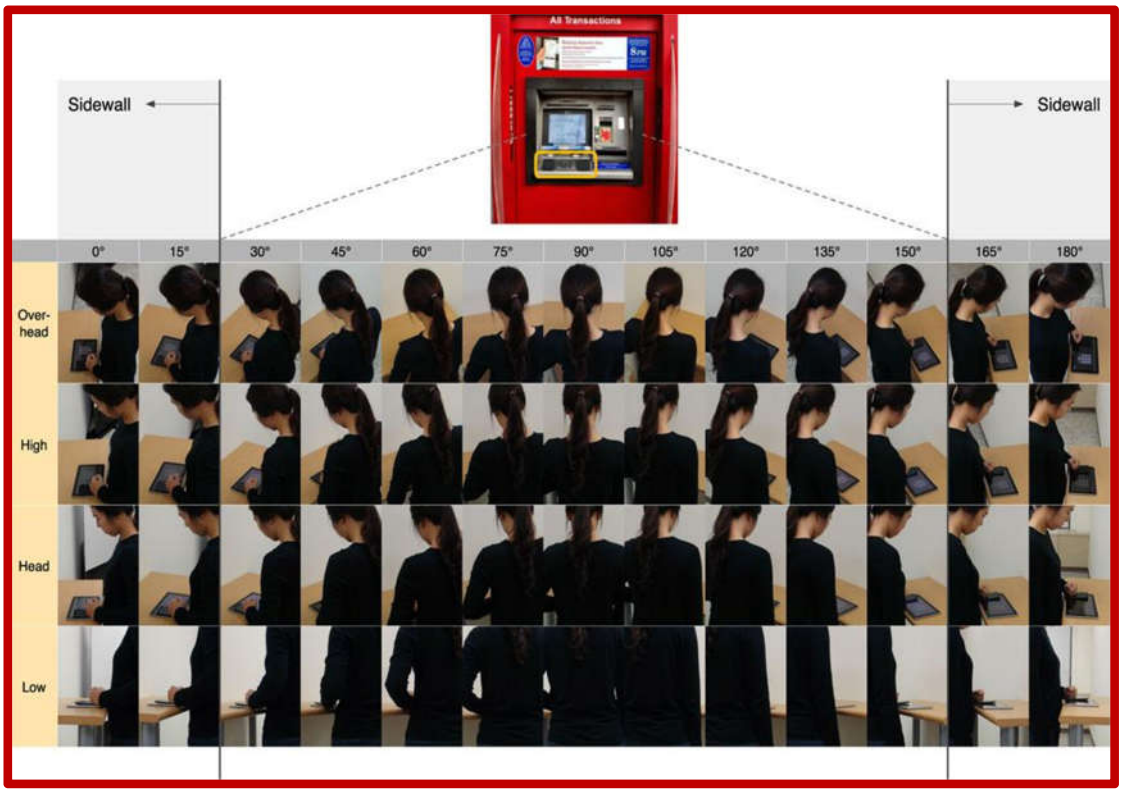

Fig. 5. Angles of camera-based shoulder-surfing. (Note: A thick round rectangle on the ATM indicates a possible place that human–machine interactive protection can take place. For the handedness of users, we simulated putting it symmetrically on both sides of the keypad. Due to the effect of sidewalls installed in the example ATM, visual angles of 30° and 150° might be more occluded.)

Added an option to reverse the location of the challenge and response keypads. The system was made to log an interaction for later analysis with regard to the PIN entry time and au-thentication results. A Sony HDR-PJ580 video camcorder was used for taking still photos and filming videos for later anal-ysis. An Apple Cinema 23 display (resolution 1920×1200, pixel density 98.44, brightness 270 cd/m^2 , and response time 14 ms) was used for playing videos and displaying photos for analysis.

C. Independent Variables

Our experimental manipulation used a within-subject facto-rial design (2×2 repeated measures) to investigate the usability of our system with two independent variables: *PIN type* (system-chosen PIN, user-chosen PIN) and *PIN entry system* (standard PIN, SteganoPIN). Note that system-chosen PINs were emu-lating difficult (or complex) PINs, and user-chosen PINs were considered easy PINs. The order in which the participants ex-perienced the PIN type and entry systems combinations was counterbalanced.

For the combination of user-chosen PIN and SteganoPIN, we added a subsequent user session to investigate the slightly longer-term (Day 5) usability: *longer term intermittent use case study*. It was intended to see whether participants could keep using the SteganoPIN system with the same PINs they did in the Day 1 sessions.

D. Dependent Measures

As objective measures, we measured the *PIN entry time*, which is considered the performance of PIN entry systems, and the *error rate* of the PIN entry. The PIN entry time was measured for a successful authentication session, from the be-ginning of the authentication session to the last key release of PIN/OTP entry. The error rate was measured as the number of failed evaluation trials divided by the total (success + failure) number of evaluation trials.

As subjective measures, during the main (Day 1) experiment, each participant was asked to respond to the following post-test questions using a five-point Likert scale (1 = very low, 2 = low, 3 = moderate, 4 = high, 5 = very high).

1) *Security*: How secure do you think this PIN entry method is against camera-based shoulder-surfing attacks, after know-ing what a camera-based shoulder-surfing attack is and how realistic it is?
2) *Ease of Use*: How easy to accomplish a PIN entry do you think this PIN entry method is for user authentication?
3) *Selection*: How likely would you be to choose this method for security-sensitive applications in public places?

4) Ease of Learning: How easy to learn do you think this PIN entry method is as a new authentication method?

5) Ease of OTP: How easy to manipulate do you think the PIN key locations are for OTP derivation in SteganoPIN?

As a subsidiary question to the usability of SteganoPIN, we asked about user effort.

E. Procedure

At the instructional meeting, we explained our user study and demonstrated the standard and SteganoPIN systems. We also explained the realistic threat of camera-based shoulder-surfing attacks and the basic concept of our protection method. We then collected demographic information.

On Day 1, we asked participants to follow a tutorial session for each PIN entry system. The tutorial session included entering the PIN 1234, *successfully* in each system. We told them how to use the location of the PIN keys like a pattern in SteganoPIN. For combinations with user-chosen PINs, we asked each partic-ipant to register his/her own choice first. For combinations with system-chosen PINs, we ran our system to produce hard PINs at random with the restriction that each digit should be different, e.g., 9276, and that three or more sequential digits, such as 123 or 987, should not occur.

In each evaluation, participants were given a short training time until they felt comfortable (mostly with three success-ful authentication attempts) and were then asked to demon-strate successful authentication. Finally, we asked the partic-ipants to enter their PINs for evaluation. The evaluation task was to authenticate him/herself using our prototype system. For each combination, the participants were allowed a maximum of three evaluation trials, but the maximum case never happened. After finishing each combination, they were asked to fill out a post-test questionnaire. There was a short break between each combination.

At the end of Day 1, we asked participants to remember their user-chosen PINs and to return for Day 5 sessions. On Day 5, we conducted the longer-term intermittent use case study to see whether the participants could remember how to use our method. We asked the participants to recollect their PINs before each evaluation and to enter them again on SteganoPIN without system instruction. The user-chosen PINs used on Day 1 were again used by each participant.

F. Data Analysis

A 2 × 2 (PIN type × PIN entry system) repeated measure-ANOVA was used for evaluation of PIN entry time. In the longer term use case of user-chosen type, a paired-samples *t*-test was used for comparison of Day 1 and Day 5 uses. McNe-mar's tests were used for evaluation of error rate, and Wilcoxon signed rank tests were used for evaluation of postquestionnaires, respectively.

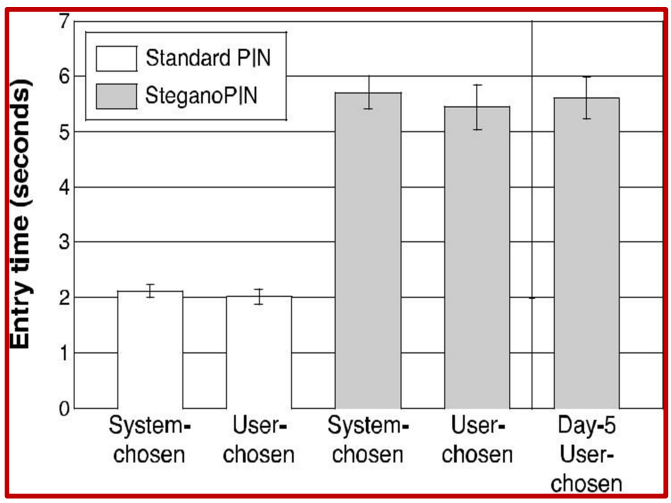

Fig. 6. PIN entry time of successful authentication, measured from when authentication was possible to the moment the last input key was released. (Note: Error bars represent 95% confidence intervals. Time measured from when the challenge keypad was activated was only below 4 s in SteganoPIN.)

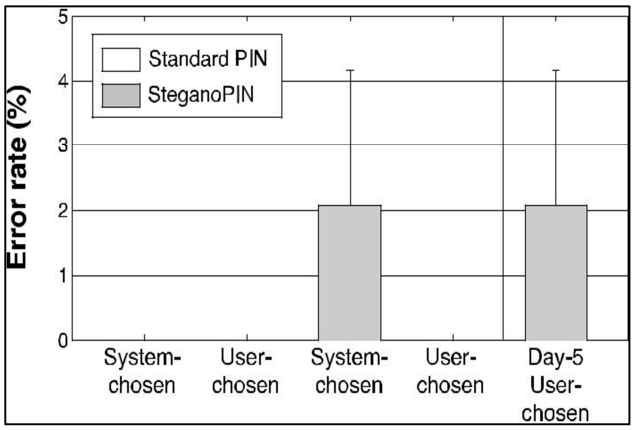

Fig. 7. Error rate of evaluation trials. (Note: Error bars represent standard errors.)

IV. RESULTS

This section presents results in which a priori significance levels were $\alpha = 0.05$.

A. Personalized Identification Number Entry Time

Fig. 6 illustrates the mean PIN entry time of successful au-thentication, for PIN entry systems in combination with random (system-chosen) or user-chosen PINs. The mean PIN entry time for the standard PIN system was significantly faster than that of SteganoPIN system ($F_{1,47} = 603.35$, $p < 0.001$). We found no other significant main or interaction effects. Overall, the stan-dard PIN system outperformed SteganoPIN in PIN entry time regardless of PIN types, as we expected.

In the longer term intermittent use case of user-chosen PINs, there was no significant difference in PIN entry time between Day 1 and Day 5 for SteganoPIN.

B. Error Rate

Fig. 7 illustrates the error rate, for PIN entry systems in com-bination with random (system-chosen) or user-chosen PINs.

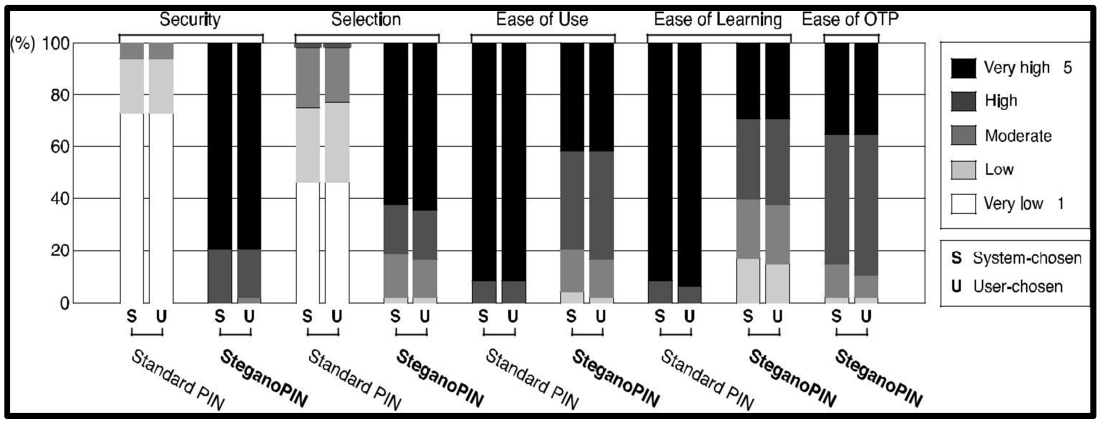

Fig. 8.Ratings from the ques tionnaires.

REFERENCES

[1] J. Long and J. Wiles, *No Tech Hacking: A Guide to Social Engineering,Dumpster Diving, and Shoulder Surfing*. Boston, MA, USA: Syngress, 2008.

[2] A. Greenberg. (2014, Jun.). Google glass snoopers can steal your pass-code with a glance," Wired. [Online]. Available: http://www.wired.com/ 2014/06/google-glass-snoopers-can-steal-your-passcode-with-a-glance/

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

[4] 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.

[5] Q. Yan, J. Han, Y. Li, and R. H. Deng, "On limitations of design-ing leakage-resilient password systems: Attacks, principles and usabil-ity," in *Proc. 19th Internet Soc. Netw. Distrib. Syst. Security Symp.*, 2012, pp. 1–16.