ColorPIN – Securing PIN Entry through Indirect Input

Alexander De Luca, Katja Hertzschuch, Heinrich Hussmann
Media Informatics Group, University of Munich,
Amalienstr. 17, 80333 Munich, Germany
{alexander.de.luca, heinrich.hussmann}@ifi.lmu.de, hertzschuch@cip.ifi.lmu.de

ABSTRACT
Automated teller machine (ATM) frauds are increasing drastically these days. When analyzing the most common attacks and the reasons for successful frauds, it becomes apparent that the main problem lies in the PIN based authentication which in itself does not provide any security features (besides the use of asterisks). That is, security is solely based on a user's behavior. Indirect input is one way to solve this problem. This mostly comes at the costs of adding overhead to the input process. We present ColorPIN, an authentication mechanism that uses indirect input to provide security enhanced PIN entry. At the same time, ColorPIN remains a one-to-one relationship between the length of the PIN and the required number of clicks. A user study showed that ColorPIN is significantly more secure than standard PIN entry while enabling good authentication speed in comparison with related systems.

Author Keywords
ATM, authentication, security, ColorPIN.

ACM Classification Keywords
H5.2 [Information Interfaces and Presentation (e.g. HCI)] User Interfaces – Input devices and strategies, evaluation.

General Terms
Experimentation, Human Factors, Security.

INTRODUCTION

Authentication on ATMs is usually based on PINs. The main security problem of PIN based authentication is that there is no security built into it. Users have to actively take care of securing the input. Active security precautions include hiding the entry with the second hand, checking the ATM for manipulations, being aware of persons nearby. This way, most of the common attacks on ATMs could be avoided. Nevertheless, the huge number of ATM frauds shows that, too often, users do not care about security.

Previous research (e.g. [1]) showed that actually users themselves open security holes in authentication systems that are then exploited by attackers. It is also noted that authentication systems should be designed in a way, that they do not rely on the user to be secure.

A wide range of research tries to overcome these weaknesses to avoid or minimize security problems. Graphical passwords [3], for example, are built to be more memorable so that users can choose stronger passwords that cannot simply be stolen by educated guessing attacks and the like. Additional work has been performed to provide shoulder surfing resistant graphical passwords (e.g. [2] and [5]). A very promising approach to make PIN and password entry more secure is using indirect input. This means that the authentication tokens are not directly input but instead some kind of "detour" is used. For instance, Roth et al. [4] created a PIN entry mechanism using a cognitive trap door game to enter the digits of the PIN. For each digit, four key presses are required. The spy-resistant keyboard by Tan et al. [6] hides the input in a similar way. For one character, two to four clicks are required. Both systems are resistant to shoulder surfing while they do not provide protection against camera based attacks. An indirect input method that is partially resistant to camera attacks is presented by Wiedenbeck et al. [7]. The main problem of indirect input is that most systems that rely on this approach add significant overhead to the input.

The goal of this work was to create an authentication system based on indirect input that does not require an active user to protect the input. Additionally, the added overhead should be kept low and it should not require major hardware changes at the ATM. Further requirements of the system are strong resistance to shoulder surfing, camera attacks as well as other hardware manipulations. In this paper, we present ColorPIN, an indirect PIN entry mechanism with a one-to-one relationship between the input and the PIN that partially fulfills these requirements. We performed a user study with 24 participants that confirmed increased security (however, the system is vulnerable to intersection attacks) of the system compared to standard PIN entry. Nevertheless, ColorPIN was significantly slower than the control condition.

THREAT MODEL

We suppose an attacker that has full access to the ATM at which the authentication will take place. Additional

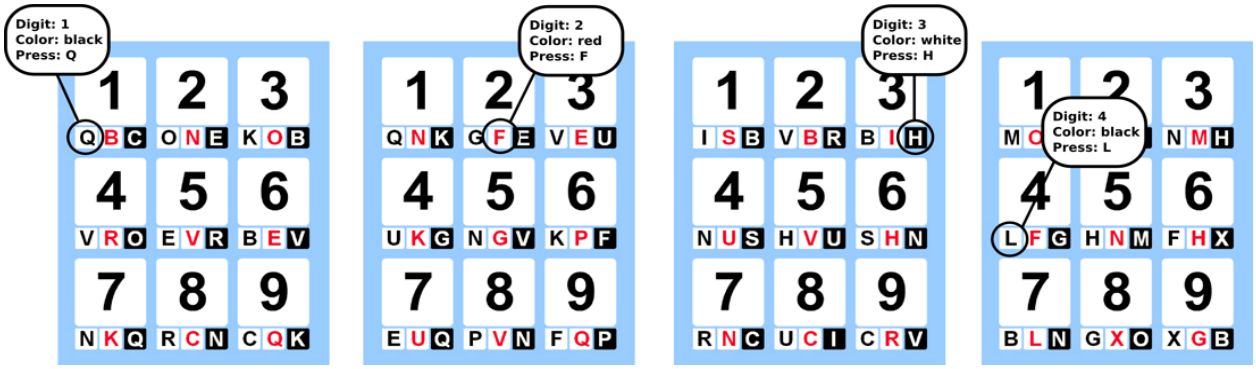

Figure 1: Exemplary PIN entry with ColorPIN. To input the PIN 1(black) 2(red) 3(white) 4(black) the user inputs the letters "QFHL". After each key press, letter assignment changes randomly.

hardware has been installed to copy the user's bank card. Additionally, the keypad has been manipulated and a camera has been added to record the input and film the screen. Another possible attack is shoulder-surfing. That is, the attacker is standing close to the ATM to gaze on the user's input.

The PIN-input method presented in this paper is mostly resistant to the presented attacks. However, if the input plus the screen is recorded for several authentication sessions of the same user, an intersection analysis can be successful. In the worst case, the user's PIN can be stolen after two attacks. However, we consider such an attack very unlikely since such massive manipulations of an ATM are more likely to be discovered in a short time.

COLORPIN CONCEPT

To achieve higher security but remain a one-to-one relationship between the length of a PIN and the required number of key presses, we slightly manipulated the authentication token itself. A PIN in our system contains of a combination of digits, of which each digit is combined with a color (black, red or white). That is, a four-digit PIN in the ColorPIN system could look like the following:

1 (black) – 2 (red) – 3 (white) – 4 (black)

The user interface consists of a keypad representation depicting the digits 1 – 9 (please note that the digit 0 has been removed due to reasons of simplicity) as shown in figure 1. On the bottom of each number, three differently colored letters can be found. Those letters are randomly assigned at the beginning of the interaction. Additionally, due to security reasons the letters are newly assigned each time the user presses a key. Each letter that is assigned to the keypad occurs in all the three colors. For instance, in figure 1 (left), the letter "Q" can be found at the bottom of digit "1" in black, at the bottom of digit "7" in white and at the bottom of digit "9" in red. These design choices are explained in the security analysis section.

To input a digit of her PIN, the user has to input the letter that is displayed at the digit's bottom in the respective color. Input is done on a conventional keyboard with one key per letter. Figure 1 exemplarily outlines a possible interaction to input the previous mentioned colored PIN. To enter the digit 1 (black), the user inputs the letter "Q". After each step the letters are randomly reassigned. To input the second digit 2 (red), the user inputs "F". Finally, the user inputs "H" for 3 (white) and "L" for 4 (black). Therefore, the whole input – which is what an attacker would have observed – consists of the character sequence "QFHL" with which the user is successfully authenticated to the ATM. This way, a one-to-one relationship between the required button presses and the length of the PIN is preserved. Due to the random letter assignment, the character sequence will most likely be completely different the next time a user authenticates with a system.

SECURITY ANALYSIS

Compared on the most basic level, the theoretical password space of ColorPIN (see table 1) makes it resistant to a number of simple attacks. For instance, educated guessing attacks are hardly successful. Even if a user chooses to take her birth date as the four-digit PIN and an attacker knows about this, there is still the secret information about the color, which is way harder to guess.

The concepts discussed in the previous section, make the system resistant to more elaborated (and more dangerous) attacks as discussed in the threat model:

Indirect input through letters: The indirect input consisting of letters is an effective counter measure against shoulder surfing as well as camera recordings of the keypad or the installation of fake keyboard hardware. Even if an attacker can see or record the whole input, the real PIN remains hidden. Additionally, this input makes the system resistant to attacks based on Trojans and other spy software. Therefore, it would theoretically be appropriate for securing online banking as well.

Using indirect input, the security of the system is (almost) completely independent of the user. While the user can still become a security problem by telling the PIN to someone or writing it down, the PIN cannot be disclosed by "insecure behavior" during the input at the ATM.

Reoccurrence of letters: Each letter used in the interface occurs in each color (but as a representation for three

different digits). That is, even if an attacker can record the whole input as well as the screen (in its four appearances) there are still 81 (3x3x3x3) possible PINs.

Reassignment of letters after key press: After each input, the letters at the bottom of each digit are randomly generated and reassigned. Without this measure, an attacker could simply start the authentication with an ATM over and over again (without trying to authenticate) until exactly the same layout as during the attack is depicted. Randomly reassigning the letters for each part of the PIN renders this attack useless.

	PIN	ColorPIN
token	digits	digits + colors
example	1234	1(black),2(white), 3(red),4(black)
theoretical password space	10.000 (random guess: 1:10.000)	531.441 (random guess: 81:531.441)
successful attack in one try	1:1	1:81
security depends on the user	yes	no

Table 1: Theoretical security comparison between ColorPIN and standard PIN entry.

As mentioned in the threat model, the main weakness of the system is intersection attacks. That is, if the entry can be completely recorded several times in a row, the PIN can be stolen based on intersections between the observations. However, the PIN cannot be stolen by a one time attack.

EVALUATION

The evaluation of the system was conducted with a prototype written in Flash. The study set up consisted of a standard desktop PC with a standard commercial keyboard attached (one key per letter). Additionally, a keypad (as known from ATMs) was connected to the PC to simulate the standard PIN entry. The whole interaction (including every single key press) has been logged for later analysis. A camera was installed, filming the keyboard (and the keypad) as well as the screen. The filmed material was used to analyze user behavior as well as to simulate an attack on the system.

User Study Design

ColorPIN was evaluated using a repeated measures within participants factorial design. The independent variables were *password type* (random [Color]PIN, user generated [Color]PIN) and *authentication mechanism* (standard PIN, ColorPIN). Standard PIN entry represented the control condition. The task was to authenticate with the terminal using every combination of the independent variables (*authentication system x password type* = 4 authentication sessions). The order of the independent variables was counterbalanced to minimize learning effects.

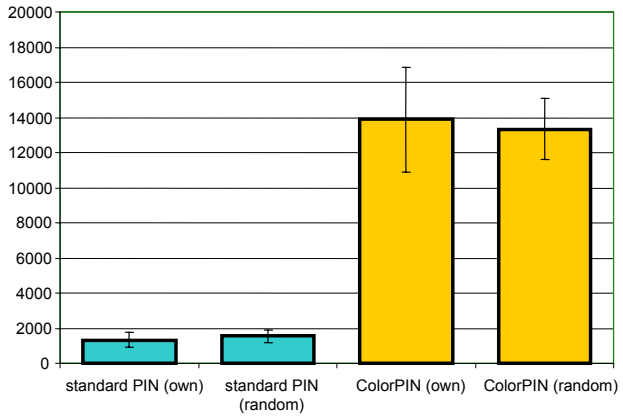

Figure 2: Authentication speed for standard PIN and ColorPIN with random and user selected (Color)PINs.

Procedure and Participants

At the beginning, the participants got an introduction to the study. The procedure, their rights as well as the prototype was explained in detail to each of them. Each participant was assigned a random identification number which at the same time was used to assign the order of tasks to them. The study then started with a questionnaire collecting basic demographic data as well as information about the participant's PIN usage. Subsequent to this, the practical part followed. Before each authentication mechanism, the participants were asked to define their own (Color)PIN. At the same time, a random (Color)PIN was assigned to them. Before using the system, they were explained in detail followed by a short training phase (one successful authentication). For each authentication session, there was a maximum of three tries to authenticate correctly with the system. Switching to the next authentication session took place after successful authentication or if it failed three times (did not occur). After finishing an authentication mechanism, the participants were asked to fill out a questionnaire containing questions about the respective system. In the end, a final questionnaire was handed out to them collecting comparison data about the systems. Ratings were given using Likert scales from 1 (disagree) to 5 (highly agree). Every key press, correction, error etc. were logged by the prototype.

We recruited 24 volunteers to participate in the study. The average age was 28 years, the youngest participant being 15 and the oldest being 57. 18 of them were male, 6 female. Choosing 24 participants allowed perfect counterbalance of the independent variables to minimize learning effects. The results are based on 96 authentication sessions performed by 24 participants.

Hypotheses

The following main hypotheses were stated for the user study: (H1) ColorPIN is more secure to observation attacks than standard PIN entry. (H2) ColorPIN is more error-prone than standard PIN entry. (H3) ColorPIN is slower than standard PIN entry.

Results

Authentication Speed: Authentication speed has been measured for each authentication session from the first key press (entering the first digit of the PIN respectively the first letter) to releasing the last key. This decision has been made to compare the actual interaction times since pressing an ok button takes the same time no matter which method was used and would be an unfair advantage for ColorPIN.

Only successful authentication attempts were counted for this analysis. Figure 2 depicts the authentication times for the authentication mechanisms in combination with user created (Color)PINs and random (Color)PINs. Standard PIN (user generated PIN) was the fastest (mean: 1.32s; sd: 0.86s), followed by random standard PIN (mean: 1.56s; sd: 0.37s). ColorPIN with a user generated PIN was the slowest method (mean: 13.88s; sd: 5.97s) and slightly slower than ColorPIN with a random PIN (mean: 13.33s; sd: 1.74s). A 2 x 2 (*authentication mechanism x password type*) within participants analysis of variance showed a highly significant main effect for *authentication mechanism* ($F_{2,46} = 64.50$; $p<.001$). No significant interaction effect and no significant main effect for password type were found. With these results, hypothesis (H3) can be accepted. This is also supported by the questionnaire in which users rated standard PIN (mean: 4.7) notably faster than ColorPIN (mean: 3.4).

Error Rate: During the study, we measured whether a participant could correctly authenticate with the system within three tries and how many corrections (deleting the input) they needed to do that. For standard PIN entry, every participant could successfully authenticate with the system at the first attempt (no matter if the random PIN or the self defined PIN was used). Only two users (random PIN) respectively one user (own PIN) applied corrections to the input. Regarding ColorPIN, two users for each password type needed two or three attempts to authenticate. However, no authentication session failed. Six users (four random PIN and two user defined PIN) needed to use at least one correction to authenticate. The data revealed no significant differences neither between the different authentication mechanisms nor the different password types. Therefore, (H2) has to be rejected.

Security: Besides the theoretical security analysis, we used the camera material collected during the study to analyze whether ColorPIN is more resistant to a camera attack (very common at ATMs) than standard PIN entry. We simulated an attacker who is familiar with the ColorPIN system and has the full video material (without sound). The attacker had three tries to authenticate correctly. Such an attack was counted successful.

Out of the 48 authentication sessions with standard PIN entry, 37 (77%) could be successfully identified. The remaining ones were mostly cases in which the participant was hiding the PIN entry with the non-active hand. Out of the 48 ColorPIN sessions, only two could be identified (two different participants). In both cases, the users were pointing on the numbers they wanted to input to assure they were choosing the right letter. Regarding the questionnaire, the participants also considered standard PIN (mean: 2.5) less secure than ColorPIN (mean: 4.6). With respect to this data, hypothesis (H1) can be accepted.

DISCUSSION AND FUTURE WORK

The evaluation showed that due to its indirect input, ColorPIN is notably more secure than standard PIN entry. At the same time, the indirect input creates extra cognitive load which makes it slower. Even though the results of the study might have been negatively influenced by design issues (choice of colors etc.) and the short training phase, they are already promising in comparison with related work: e.g. Hayashi et al. 12.4s [2], Roth et al. 23.3s [4], Sasamoto et al. 32s [5], Tan et al. 50s [6], Wiedenbeck et al. 71s [7]. Furthermore, we can informally state that after repeated use of the system it becomes remarkably faster. In an informal study, participants achieved average times of about 3.5 seconds in the fifth authentication session. We could also observe interesting interaction strategies, e.g. based on the positions of the colored fields. In future work, we want to find out whether these observations can be confirmed in formal studies.

The additional information "color" and the lack of exploiting the users' motor memory (movements on the keyboard change every time), could lead to worse performance with respect to memorability. This is supported by the opinion of a user: "I suppose it is harder for me to remember a PIN including colors than just a PIN". As mentioned before, informally we could observe new interaction strategies that might solve this memorability problem. Therefore, this aspect surely deserves further evaluation.

REFERENCES

1. Adams, A., Sasse, M. A. Users are not the enemy. Commun. ACM 42, 12, 40 – 46.
2. Hayashi, E., Dhamija, R., Christin, N., Perrig, A. Use your illusion: secure authentication usable anywhere. In Proc. SOUPS '08.
3. Moncur, W., Leplâtre, G. Pictures at the ATM: exploring the usability of multiple graphical passwords. In Proc. CHI '07.
4. Roth, V., Richter, K., Freidinger, R. A pin-entry method resilient against shoulder surfing. In *Proc. CCS '04*.
5. Sasamoto, H., Christin, N., Hayashi, E. Undercover: authentication usable in front of prying eyes. In Proc. CHI '08.
6. Tan, D., Keyani, P., Czerwinski, M. Spy-resistant keyboard: more secure password entry on public touch screen displays. In *Proc. OZCHI '05*.
7. Wiedenbeck, S., Waters, J., Sobrado, L., Birget, J.-C. Design and evaluation of a shoulder-surfing resistant graphical password scheme. In Proc. AVI 2006.