My Phone is my Keypad: Privacy-Enhanced PIN-Entry on Public Terminals

Alexander De Luca, Bernhard Frauendienst, Sebastian Boring, Heinrich Hussmann
{alexander.de.luca, sebastian.boring, heinrich.hussmann}@ifi.lmu.de,
bernhard.frauendienst@stud.ifi.lmu.de
Media Informatics Group, University of Munich
Amalienstr. 17, 80333 Munich, Germany

ABSTRACT
More and more services are available on public terminals. Due to their public location and permanent availability, they can easily fall victim to manipulation. These manipulations mostly aim at stealing the customers' authentication information (e.g. bank card PIN) to gain access to the victims' possessions. By relocating the input from the terminal to the users' mobile device, the system presented in this paper makes the authentication process resistant against such manipulations. In principle, this relocation makes PIN entry more complex, with a tendency to worse usability. In this paper, we present the concept as well as an evaluation that has been conducted to study the trade off between usability and security. The results show that users apparently are willing to accept a certain increase of interaction time in exchange for improved security.

Author Keywords
Security, privacy, mobile devices, PIN entry

ACM Classification Keywords
H.5.2 [Information Interfaces and presentation (e.g. HCI)]: User Interfaces – authentication.

INTRODUCTION
Public terminals provide a level of convenience in our daily lives that many people would not like to miss. Services can be accessed 24 hours, 7 days a week. Customers are no longer bound to opening or working times. Terminals include for instance train ticket vending machines, cash machines (ATMs) and check-in terminals at airports. A huge part of these services require the customers to authenticate to the system.

While privacy and security precautions in the online world have evolved extensively over the last years, public terminals have received little more than a cosmetic make-over within the 40 years after the first automated teller machine (ATM) was installed for productive use in the late '60s. Standard authentication on public terminals still requires users to enter a 4-digit PIN via an integrated keypad.

OZCHI '09, Nov 23-27, 2009, Melbourne, Australia

Figure 1: PIN-entry on a public terminal using MobilePIN.

As a consequence, a variety of different attacks has been created, mostly for ATMs (Rogers, 2007). For instance, a user's card is copied with a disguised separate reader (Skimming) while the PIN is recorded with a hidden camera. A simpler but yet effective attack is the so called shoulder-surfing, i.e. old-fashioned "looking over one's shoulder", sometimes combined with social engineering to trick victims into typing their PINs before the attacker's eyes. All these attacks exploit the same weakness: the fixed keypad, which the customers must use to input their PINs.

Thus, the advantage of public terminals is, at the same time what makes them prone to attacks: they are publicly available at (mostly) any time and therefore not resilient against manipulations.

By separating the input device from the terminal, MobilePIN has been designed to overcome these problems. It utilizes the users' mobile phones as external input devices for public terminals, which makes it resilient against manipulation by third entities. A prototype has been developed and was used to conduct a user study on the appropriateness of this approach for authentication tasks in public spaces. Since PIN-entry is a rather short task, any overhead created by an authentication mechanism might lead to decreased user satisfaction. Therefore, the main goal of the evaluation was to determine whether there is a noticeable overhead and if it is acceptable for users due to increased security.

RELATED WORK
Security-enhanced authentication mechanisms can be roughly divided into two categories. The first includes systems that, like MobilePIN, try to increase the security of traditional authentication approaches like password

and PIN. An example is the spy-resistant keyboard (Tan et al., 2005). It uses a two-step character selection that is hard for an attacker to follow, but also increases the time and the complexity to input a password. Furthermore, it is not resilient against observation attacks based on camera recordings. A similar approach of adding overhead to the input has been taken by Roth et al. (2004). They designed a PIN-entry system that requires the user to press four times to enter one digit of their PIN. Eye-tracking technology for PIN and password entry has been evaluated by Kumar et al. (2007). They compared well-known eye-tracking techniques combined with an on-screen keyboard on security as well as usability.

Interesting research has also been performed on completely different authentication approaches. The best known being biometric authentication as evaluated for ATM usage by Coventry et al. (2003). While biometry performs rather well on usability and speed, it is hard to deploy and more expensive than other approaches. The main advantage of biometry is that users do not have to recall any secret information like a PIN. In other research (Deyle et al., 2006 and Sasamoto et al., 2008), tactile feedback provided by the terminal is used to share secret information with the users and thus increase the systems security. Both approaches require additional hardware on terminal side. In contrast to these technologies, MobilePIN relies on hardware owned by the users.

CONCEPT

Whenever a user wants to authenticate with a public terminal using *MobilePIN*, the following steps have to be performed: 1. The user starts the authentication process. For instance, she inserts her credit card into the card slot of the terminal. 2. The terminal creates a visual code including the wireless address of the terminal as well as an authentication token and displays it on the screen (figure 2 a). 3. The user takes a photo of the visual marker with the mobile device camera. The information on it is used to establish a secure connection between the mobile device and the Terminal (figure 2 b). 4. When the user enters the PIN on the mobile device it is securely transmitted to the terminal (figure 2 c).

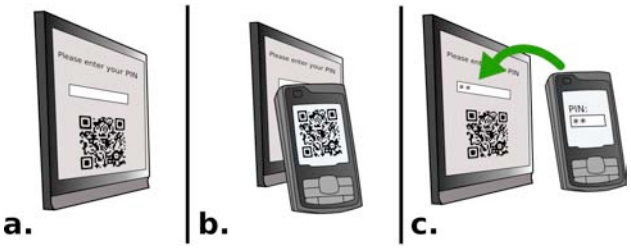

Figure 2: MobilePIN interaction.

For interoperability with existing terminals, MobilePIN has been designed to support standard PIN-entry and security enhanced mobile PIN-entry in parallel. This way, it is also suitable for users without mobile devices and others who cannot or do not want to use mobile input. In addition to enhanced security, MobilePIN has the further advantage of enabling authentication for terminals that have none or limited input capabilities.

Connection Issues

The question about how to connect the mobile device to the terminal is crucial for the system. Several aspects have to be considered: How big is the overhead created by the connection method? How easily and at what costs can it be deployed? How secure is it to establish the connection?

For the MobilePIN prototype we decided to use a marker-based connection similar to the approach proposed by Claycomb et al. [1]. For each connection, a visual marker is created and displayed on the screen. It includes all the information necessary to establish a secure connection between the mobile device and the terminal. The main reason for choosing this approach is that it is very easy to deploy (the terminal only needs a screen to display the marker) and it is reasonably secure. However, there is a huge variety of other connection mechanisms that could have been used. For instance, an NFC-based connection would be possible. The problem is that NFC-enabled devices are not widely deployed yet. Theoretically, MobilePIN can work with any technique, which is able to establish a secure connection.

Security

MobilePIN is resistant against most of the common attacks on public terminals. For instance, cameras directed at the keypad are of no use, because they work based on the assumption that the input device is always located in the same place. For MobilePIN, users will always hold their mobile devices at different positions or even hidden inside their bags or pockets.

Attacks based on manipulations of the input hardware are useless since MobilePIN works without any physical contact to the terminal. Further security can be achieved if MobilePIN is used with a master password, which grants access to the stored PIN. This would render shoulder-surfing attacks useless because thieves would have to steal both the master password and the mobile device.

Since MobilePIN requires a wireless connection to the terminal, sniffing or man-in-the-middle attacks have to be considered. Therefore, the connection algorithm has to be chosen carefully with respect to security.

EVALUATION

To evaluate the system, the prototype shown in figure 1 has been implemented. It consists of two parts: a desktop application written in JavaSE and a mobile application written in JavaME. The study took place in a laboratory at our premises. No other people could enter that room during the experiment. A laptop computer with an attached keyboard was used to simulate the terminal. To avoid influences of the users' mobile devices on the experiment, we decided to let every participant use the same mobile phone, an Nokia N73 which had the JavaME software installed and ready to use.

User Study Design

The system was evaluated using a repeated measures within participant factorial design. The independent

variable was *InputType* with two levels. The first level was input on the mobile device, the second level was standard PIN-entry, which acted as the control condition. The dependent variables measured were *input speed, error rate*, *user satisfaction* and *experienced privacy/security*. The order of *InputType* was counterbalanced between the participants to minimize learning and ordering effects.

Procedure

For each participant, the exact same procedure was applied. They were brought into the room where the tasks were explained to them. To keep the experiment as unbiased as possible, the explanation had been written down and had been repeated in exactly the same way to each participant. After that, they had to draw a random number from a bowl for anonymous identification and for connecting the log files (measuring times, errors etc.) to specific participants (respectively the questionnaire).

Two different tasks were performed by each participant. Each task was to enter a PIN correctly, with the standard keyboard (task 1) and with the mobile phone (task 2). Counterbalancing was achieved by assigning the order of the tasks to a participant with respect to the number drawn from the bowl. Odd numbers started with task 1 while even numbers started with task 2. After finishing both tasks, each participant was asked to fill out a questionnaire. This was done to collect information about user preferences as well as basic statistical data. Likert scales from 1 (do not agree) to 5 (highly agree) were used in the questionnaire. Additionally, all interaction was logged by the system for later evaluation.

Hypotheses

For the evaluation of MobilePIN, the following hypotheses have been stated: (H1) PIN-entry on the mobile device is slower than with the keyboard of the terminal. (H2) PIN-entry on the mobile device has a higher error rate compared to standard PIN-entry. (H3) Users will consider MobilePIN more secure than standard PIN-entry.

Participants

The user study was conducted with 19 volunteers. The average age was 25 years and the male/female ratio was almost 50/50 with 9 female and 10 male participants. The youngest participant was 20 years old, the oldest 32 years. Asked about how many times they withdraw money from an ATM per month, the average answer was 4.6 times, while 1 was the smallest and 15 the highest value.

Results

User Performance

In the evaluation, user performance was based on *error rate* and *input speed.* To measure input speed, the time between the first press of a button and the correct PIN being confirmed had been chosen. Out of the 19 samples, two extreme outliers had to be removed for the analysis. A Kolmogorov-Smirnov test showed that the collected data is normally distributed for MobilePIN as well as standard PIN-entry.

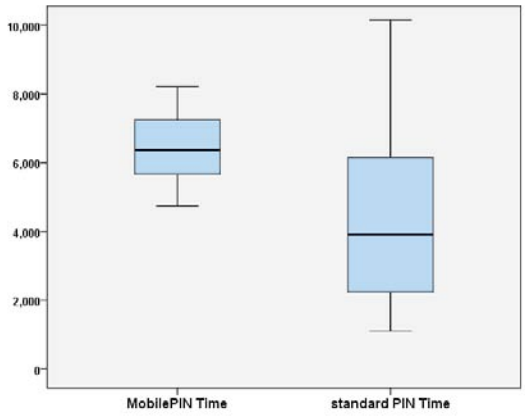

Figure 3: Times for MobilePIN and standard PIN-entry.

A paired-samples t-test was used to analyse the data. It showed that the time needed to input the correct PIN using MobilePIN (M = 6.4s, SE = 0.26s) was significantly slower than using standard PIN-entry (M = 4.4s, SE = 0.67s, $t(16) = .2.92$, $p < .05$, $r = .59$), which supports hypothesis (H1). Figure 3 outlines the results. One interesting finding is that even though the average times for the standard PIN-entry are significantly lower, there has been a higher diversity in results than for Mobile PIN.

The results show that users are faster with standard keyboards than using a mobile device. More interesting is the overall time of the interaction. While this time is the same for standard PIN, MobilePIN has an additional overhead created by the technology used for the connection between the mobile device and the terminal. The marker-based approach chosen for MobilePIN created an average overhead of 8.7 seconds. This is more than the average time for entering a PIN using MobilePIN. Thus, it creates an overhead of more than 100%. This shows that, despite its many advantages (Claycomb et al., 2006), the main problem of the marker-based approach is its speed. Even though the participants rated the speed as ok (see later), we would argue that a faster connection technology is likely to increase acceptance of MobilePIN.

A comparison of *error rates* for the two systems showed a surprising result. We distinguished between critical errors (that is the PIN was entered wrongly for three times) and non-critical errors (maximum two times wrong PIN). Surprisingly, neither standard PIN nor MobilePIN resulted in any critical errors and only one non-critical error occurred for each. During PIN-entry, the participants could correct their input as many times as required. While only one correction had been done for standard PIN, MobilePIN needed no correction. Based on those results, (H2) had to be rejected. We believe that this is due to increased habituation to entering information on mobile devices, especially for people within the age of our test group.

User Preferences

To gain a general understanding of the users' needs when authenticating with public terminals, we let them rate the

three major aspects for this kind of interaction: security, speed and error-resistance. The participants had to rate the importance of these three aspects on a Likert scale from 1 ("not important") to 5 ("very important"). The results show that error-resistance (4.5) and security (4.6) are rated notably higher than speed (3.7). Ergo, users are willing to accept slower interaction methods if this increases security. Noticeably higher error rates seem rather unacceptable.

The obvious reason that security seems to be the most important aspect of public authentication is the possible loss of the users' possessions in case of a fraud. That is why most of the users (90%) use extra safety precautions when authenticating on a public terminal. Almost 50% even claim to use several extra security measures like hiding the PIN-entry with the other hand.

The participants had also been asked for their subjective opinion about security of the different systems. A Likert Scale from 1 ("I do not agree") to 5 ("I highly agree") had been used. The main purpose was to determine whether users felt more secure when using PocketPIN compared to standard PIN-entry. The statement "MobilePIN provides the highest possible security when entering private information" was rated 4.1 by the participants compared to 2.6 when asking the same question for standard PIN-entry. These scores highly support hypothesis (H3).

The same Likert scale has been used to let the participants rate ease-of-use of MobilePIN (4.2) and standard PIN (4.7). When asked about the experienced interaction speed, traditional input reached an average vote of 4.3 points regarding speed, while MobilePIN averaged at 3.3 points. The lower score for MobilePIN correlates with the results from the measurements. Still, the result is surprisingly good considering the huge overhead created by the connection mechanism. One possible explanation is that people enjoyed playing with the marker-based system, which they had never used before. We argue that after getting familiar with the technique it might be experienced as a bigger drawback.

The positive results of the questionnaire in combination with the good (error rate) and reasonable (input speed) result of the study support the final finding of the questionnaire. The question "I could imagine using MobilePIN to authenticate on a public terminal" averagely scored 4.2.

Summarized, it seems that increased interaction time is acceptable if the experienced security (not the actual security) is considered noticeably higher by the users of an authentication system. Outside of a lab condition, we argue that this effect will be lower. Therefore, a faster connection mechanism might be desirable.

CONCLUSION AND FUTURE WORK

In this paper, we presented MobilePIN and its evaluation. The large number of frauds on public terminal shows that there is need for new authentication methods. Our results indicate that MobilePIN is able to fill that gap since – even though being slower than standard PIN entry – it is more secure and as the results of our experiments show, users prioritize security and error-resistance over speed. Another advantage is that it is easily deployable since it only requires minor software updates at the terminal and possibly additional modules for wireless communication (e.g. Bluetooth).

Even though within our experiment users seemed to accept the overhead created by the connection method, we argue that a faster and more efficient connection mechanism should be used for real world usage. We think that users are willing to accept the rather big overhead in a lab situation but probably would not accept it if used in the field. Fortunately, MobilePIN can be easily modified to work with any secure connection technique. It is even conceivable to include support for several connection mechanisms and let the users or the terminal provider decide on the required level of security and convenience. It is even imaginable to provide authentication mechanisms that enable connection while queuing at the terminal or even on the way to the terminal.

Currently MobilePIN uses standard PINs as authentication tokens. That is, it inherits its disadvantages. For instance, some people have problems remembering PINs and thus choose simple PINs like their birthday, which decreases security. Thus, in future work we are planning to investigate the usage of alternative authentication tokens (e.g. graphical passwords) with MobilePIN. Another field that seems worth to be investigated is whether MobilePIN could provide a unified authentication method for public terminals. With this system, authentication functionality could even be added to public terminals that do not support input and thus cannot support authentication (e.g. proactive displays).

REFERENCES

Claycomb, W., Shin, D. Secure real world interaction using mobile devices. In Permid 2006.

Coventry, L., De Angeli, A., Johnson, G. Usability and biometric verification at the ATM interface. In Proc. Chi 2003.

Deyle, T., Roth, V. Accessible authentication via tactile pin entry. CG Topics, Issue 3, Mar. 2006.

Kumar, M., Garfinkel, T., Boneh, D., Winograd, T. Reducing shoulder-surfing by using gaze-based password entry. In Proc. SOUPS 2007.

Rogers, J. Please enter your 4-digit PIN. Financial Services Technology, U.S. Edition, Issue 4, Mar. 2007.

Roth, V., Richter, K., Freidinger, R. A pin-entry method resilient against shoulder surfing. In Proc. CCS 2004.

Sasamoto, H., Christin, N., Hayashi, E. Undercover: authentication usable in front of prying eyes. In Proc. CHI 2008.

Tan, D., Keyani, P., Czerwinski, M. Spy-resistant keyboard: more secure password entry on public touch screen displays. In Proc. OZCHI 2005.