A Privacy-Respectful Input Method for Public Terminals

Alexander De Luca
Media Informatics Group
University of Munich
Amalienstr. 17, 80333 Munich, Germany
alexander.de.luca@ifi.lmu.de

Bernhard Frauendienst
Media Informatics Group
University of Munich
Amalienstr. 17, 80333 Munich, Germany
bernhard.frauendienst@stud.ifi.lmu.de

ABSTRACT

Nowadays, people often have to input information on public terminals. By doing so, they might disclose information to strangers looking over their shoulders. In this paper we introduce a new way of interacting with public terminals, which offers more privacy by using a personal mobile device to enter private data. It allows the users to choose which information is to be regarded personal, which can then be entered on their mobile device and is hidden from the screen accordingly. Furthermore we created a prototype and conducted a user study measuring users' input performance and to collect opinions about the system's usability and practical value. The paper concludes with some ideas to make the system even more useful.

Categories and Subject Descriptors

H.5.2 [**Information interfaces and presentation (e.g. HCI)**]: User Interfaces – *Input devices and strategies, evaluation.*

General Terms

Security, Human Factors, Theory, Verification.

Keywords

Privacy, mobile devices, public terminals, personal data.

1. PRIVATE PUBLIC INTERACTION

Interacting with services using public terminals is a common task these days. Services are for instance train ticket vending machines, public information screens, ATMs, Internet terminals, etcetera. Besides their manifold advantages – like big displays and enhanced input capabilities (touch-screens, keyboards, etc.) – that ease the users' life, public terminals comprise several privacy as well as security risks.

Whenever users are required to input personal information, this can be easily exploited by attackers. A simple and very common attack is the so-called shoulder surfing. It can either be performed non-technically by trying to spy on the input from a close spot or technically by using cameras or other equipment targeted at the display or the input device. Due to the size of public terminals and displays, this attack becomes highly efficient and is for instance commonly used in ATM frauds [9].

In this paper, an interaction technique called PocketPIN will be introduced, which has been created to enable private input on public terminals using mobile devices. The idea is to split up the user interface and input functionality between the terminal and the mobile device, which is supported by results from [6] which show that in public (non-private) spaces, users like privacy-respectful division of information and interfaces mostly to balance privacy (mobile device) with better I/O (terminal). This assumption is confirmed by the results of the user study, which will be outlined in more detail in the second part of this paper.

2. POCKETPIN CONCEPT

The basic concept of PocketPIN is to utilize the users' personal mobile equipment (mobile phones, PDAs etc.) as an input device for public terminals. Mobile devices mostly are more private and secure than terminals. Firstly, they are owned and carried around by the users. Thus, it is hard or next to impossible for an attacker to manipulate them. Secondly, their keypads are small and not fixed to a specific location (in contrast to an ATM keypad for instance) and thus hard to spy on. Users can take extra precautions for further security, like keeping the mobile device in a bag or pocket (Pocket Private Input – PocketPIN) to enter data.

2.1 Basics

When creating a system that is supposed to provide private input in public, several aspects have to be considered. First of all, privacy cannot be defined by a system but only by its users. The personal definition of privacy varies from person to person. Some consider all their personal data private while others are only worried about data like their bank or health information. Therefore, an input system for personal data has to be adjustable to the personal requirements of different users. The PocketPIN system addresses this problem by providing a privacy setting interaction by marking specific input fields as private.

Another aspect of such a system is its usability. Since users have to interact with a huge variety of services with their mobile devices, consistency and simplicity are highly important. Additionally, PocketPIN compatible terminals have to provide a non-private mode as well, since there are still a non-marginal number of persons that do not own a mobile device. Therefore, terminals should work as usual and switch to a private/secure mode if a PocketPIN compatible device is connected to them.

2.2 Interaction Flow

The PocketPIN interaction with the terminal consists of six steps as outlined in Figure 1:

1. To start the private input session with a public terminal, the user needs to establish a secure communication channel between

NordiCHI 2008: Using Bridges, 18-22 October , Lund, Sweden.
Copyright 2008 ACM ISBN 978-1-59593-704-9. $5.00

the device and the terminal, which tells the terminal to switch to private mode. A solution using visual markers as proposed in [2] will be explained in the next section.

2. The terminal sends its data requirements to the mobile device. This mainly consists of a description of personal data required from the user.

3. The user selects private input fields on the terminal screen. Alternatively (e.g. if the terminal lacks appropriate input mechanisms) the private fields can be selected and marked directly on the mobile device.

4. With respect to the user's choice, the mobile device creates the user interface for the required data. The terminal additionally adapts its UI so that all the private information is hidden and private fields are marked as such.

5. The user enters the personal data (partially at the mobile device, partially at the terminal). The only feedback on the terminal side are asterisks for filled out fields.

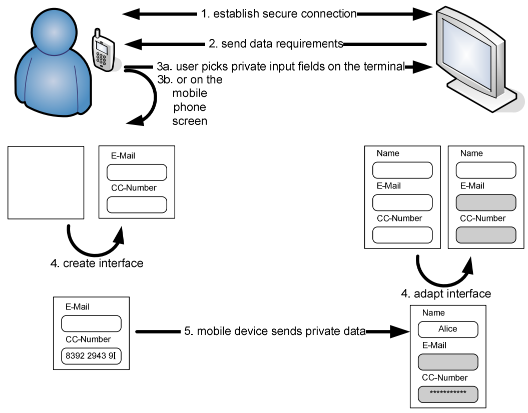

1. establish secure connection
2. send data requirements
3a. user picks private input fields on the terminal
3b. or on the mobile phone screen
E-Mail
CC-Number
4. create interface
Name
E-Mail
CC-Number
Name
E-Mail
CC-Number
4. adapt interface
E-Mail
CC-Number
8392 2943 9|
5. mobile device sends private data
Name
Alice
E-Mail
CC-Number
••••••••••••

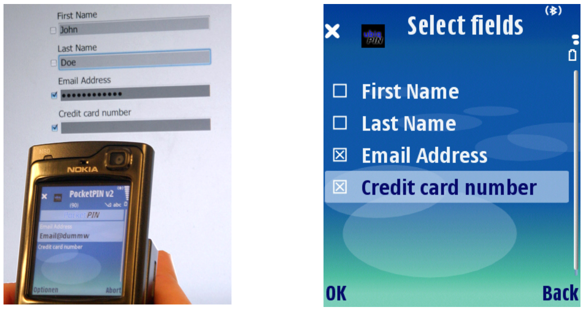
Figure 1: PocketPIN Interaction Flow

2.3 Ad-Hoc Privacy Preferences

In [6], Hutchings et al. state that interface allocation and division of information should be changeable by the users during runtime. This process should be easy and quick.

The ad-hoc privacy settings of PocketPIN follow this suggestion. The selection of private input fields was realized by placing checkboxes next to the fields on the terminal screen as shown in Figure 2 (left). When checked, the respective field is marked as private. Additionally, a selection menu for the fields has been implemented on the mobile device, which can be seen in Figure 2 (right). This menu is created dynamically after the data requirements have been sent by the terminal (see Figure 1, step 2).

After the user has chosen the private input fields, the mobile phone and the terminal create the respective input forms. On the terminal side, the form is shown with all input fields for personal data, the private fields are grayed out. On the phone, a form only consisting of the private fields is shown. This decision has been taken due to the limited screen size of mobile devices. There is a slight danger that users may be confused by such an approach, but we hope this is not the case. This had to be clarified in the user study. Whenever a field is filled out, its content is masked with asterisks on the terminal to give visual feedback to the user that the data has been successfully submitted. This approach is illustrated in steps 4 and 5 in Figure 1.


First Name: John
Last Name: Doe
Email Address: ••••••••••••
Credit card number

Select fields
☐ First Name
☐ Last Name
☒ Email Address
☒ Credit card number

Figure 2: Interaction with the prototype (left) and selection of private input fields using the mobile phone (right)

3. PROTOTYPE

A mobile phone JavaME prototype and a JavaSE server application have been implemented to evaluate PocketPIN. To establish a secure connection between the phone and the server, an approach based on the visual marker connection proposed by Claycomb et al. in [2] has been used. When users want to create a connection to the terminal, they take a photo of a visual marker displayed on the screen (QRCode [4]). The marker is decoded and information like the Bluetooth address etcetera to create the secure connection are extracted from it. For further information please refer to [2]. This method has been chosen for its simplicity, effciency, and ease of deployment. Nevertheless, any other secure ad-hoc connection technique could be used as well. For communication, open source libraries have been used: implementations of MD5 [1] (for the public key hash) as well as RSA and OAEP (for encrypting communication from the client to the server). Markers are decoded using the Google ZXing API [5]. To create them, the encoder from [12] was ported to Java.

4. EVALUATION

To evaluate PocketPIN, a large screen in the hallway of the university, usually a public information terminal for students has been chosen. This screen was extended with a mouse and a keyboard. The location seemed appropriate since it is private enough to be controlled by the testers to avoid interruptions by by-passers and the like. The mobile PocketPIN software was installed on a Nokia N73.

The goal of the study was to compare PocketPIN to a privacy-less interaction mode as well as a privacy-enforcing interaction mode with the assumption that PocketPIN provides an appropriate balance between privacy and usability, which is a major feature of divisible interfaces as stated by Hutchings et al. in [6].

4.1 User Study Design

For the usability evaluation, an intra-subject factorial design has been chosen. The independent variable in the study was *privacy mode* with three possible levels: 1. All data has to be entered without obfuscation at the terminal (no privacy). 2. All data has to be entered using the mobile phone (full privacy). 3. The users can choose private data fields using the mobile phone selection tool or the terminal selection (the actual PocketPIN prototype). The task for each experimental condition was to fill out a form containing first name, last name, e-mail address and credit card number.

Performing this task in condition one (no privacy) acted as the control condition to compare the results of the study.

The dependent variables measured in the experiment were *task completion time, user satisfaction* and *experienced privacy*. The order of the three experimental conditions (filling out the form in each level of the independent variable) was uniformly distributed over the participants to minimize learning and ordering effects.

4.2 Hypotheses

Based on the expected outcome of the experiment, hypotheses were formulated: (H1) Filling out the form using the privacy-less mode will be faster than using PocketPIN and full privacy mode. (H2) The participants will feel more private (secure), when using PocketPIN than using the terminal only version. (H3) PocketPIN is an appropriate trade-off between privacy und usability.

4.3 Participants

The study was conducted with twelve participants with an average age of 25 years, four of them female and eight male. The youngest participant was 21, the oldest 31 years old. All own a mobile phone and rate their experience handling it as high. Choosing twelve participants allowed to have the order of the experimental conditions evenly distributed amongst the participants (3 privacy mode levels result in 6 possible orders).

4.4 Procedure

At the beginning, the prototype was explained to the participants and they were allowed to gather initial experience with the interaction until they felt familiar with it. As mentioned before, every participant had to perform the same task (filling out the form) in each level of the privacy mode. That is, each participant had to fill out the same form three times. A short explanation was given and the subjects were instructed to fill the form with real data and to try to perform the task as fast as possible. The completion times for the different conditions were measured without the participants' knowledge. After each condition, a short questionnaire collecting demographic data had to be filled out. This should provide a deletion of the short-term memory as well as to give the participants a short relaxation time. After the final condition, additional questions collecting the participants' opinions were asked in a final questionnaire. Likert scales from 1 ("don't agree") to 5 ("highly agree") were used.

4.5 Results

4.5.1 Performance

As expected, filling out the form using the privacy-less mode was the fastest input method (Figure 3) with a mean of 21.8s (sd: 7.7s) compared to full privacy mode (mean: 63.3s; sd: 19s) and PocketPIN (mean: 74.25; sd: 28s). A statistical analysis using ANOVA shows that this result is highly significant ($F_{2,22}$=37.146, p<.001). Bonferroni post hoc tests reveal significant differences between privacy-less compared to PocketPIN ($CI_{.95}$ = -73.85 (lower) – 30.99 (upper), p<.001) and privacy-less compared to full privacy ($CI_{.95}$ = -55.04 (lower) – 27.96 (upper), p<.001). These results correlate with the opinion of the participants, rating privacy-less the fastest with 4.7, full private 3.0 and PocketPIN 3.4, and confirms hypothesis H1.

Interestingly, regardless of how many fields were chosen as private by the participants using PocketPIN, full privacy mode and PocketPIN had no significant difference in input speed (p>.05). Every participant that started with PocketPIN performed faster in full privacy mode and vice versa. The learning effect and the short form can explain this. Thus the attention shift between screen and mobile phone could be too long compared to the advantage gained by the terminal input.

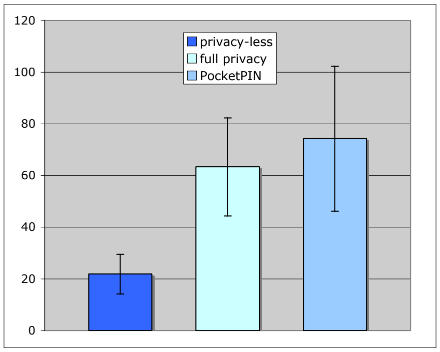


Figure 3: Input times of the three different input methods

4.5.2 User Satisfaction

Regarding ease of use, it was expected that all participants would be able to interact with the prototype without major problems, which has been the case. All three methods were rated easy to use of which the privacy-less version was rated easiest to use (4.8) followed by the PocketPIN (3.9) and the full private input (3.3). Non-parametric statistic analysis shows significance for these results ($\chi^2(2)$ = 11.81, p<.003). Post-hoc Wilcoxon tests (Bonferroni correct level of significance .0167) show that only the difference in opinion between privacy-less mode and full privacy mode is significant (T = 0, p<.0167, r=-.55). There is neither a significant difference between privacy-less and PocketPIN (T = 2, ns, r=-.42) nor between full privacy and PocketPIN (T = 2, ns, r=-.37). The interesting part is that the difference in the rating of PocketPIN and privacy-less (terminal only) version was not significant. This allows assumptions that PocketPIN is not considered harder to use than privacy-less mode, which could be due to the possibility to enter complex, non-private data directly at the terminal.

As stated before, the design decision was made to show only the private input fields. During the study, 10 out of the 12 participants reported that they would prefer to see (and maybe enter) all input fields on the mobile device. This again could be due to the fact that the form only consisted of four fields, which is supported by the very interesting statement of one user: "A*ctually, it depends on how long the form is. If it is short enough to fit on the display, I'd rather see all input fields. If the form is very long and only few input fields are private, I'd rather see only the private ones*". This will be taken into consideration in future work.

4.5.3 Privacy

Regarding privacy, the most important aspect of this work, the privacy-less mode was rated worse (1.8) than full privacy mode (4.3) and PocketPIN (3.7), which could be shown to be significant ($\chi^2(2)$ = 13.61, p<.001). Post-hoc Wilcoxon tests with a Bonferroni corrected level of significance .0167 showed that the differences in the experienced privacy between privacy-less and PocketPIN (T = 2, p<.0167, r=-.57) and full privacy mode (T = 1, p<.0167, r=-.59) are significant but no significance between the two privacy enabled modes could be shown (T = 4, ns, r=-.043). These results support hypothesis H2.

When analyzing the answers regarding the privacy features of the system, it was interesting to see that no preference regarding the privacy selection method could be found. Two participants preferred to define private input fields using the terminal, four using the mobile phone and six said they prefer having the combination of both. This result is confirmed by the observation of the study that seven people used the terminal to define the private input fields and five used the mobile phone. Interestingly, even though six participants would prefer the combination of both, none of the 12 participants switched between the modes to select input fields. That is, for those six it already seems sufficient to have the possibility to choose the appropriate mode.

4.5.4 Discussion

The major idea of this work was that PocketPIN is a reasonable trade-off between privacy and ease-of-use. The results of the evaluation support this assumption. PocketPIN was considered more private than the privacy-less mode but not less private than the full privacy mode (thus secure enough). Regarding ease of use, opinions did not significantly differ between PocketPIN and privacy-less mode, whereas for privacy-less and full privacy mode it did. Nevertheless, PocketPIN took longer for filling out the form than privacy-less mode, which could be shown to be significant. Even though slightly slower interaction is acceptable for privacy-preserving technologies, it can only be argued that hypothesis (H3) could be partially confirmed. It is expected that PocketPIN will perform better with longer forms, which should be investigated in future studies to see if (H3) can be fully validated.

5. RELATED WORK

Private interaction in public has been a topic in research for some time. Most focus on secure and private authentication in public. For instance, Kumar et al. [7] evaluated a prototype for shoulder-surfing resistant password entry using eye-gaze interaction. That is, PINs and passwords are entered with the eyes instead of manual input. This way, attackers have fewer chances to spy on it. The problems of this approach are the slow interaction time and calibration issues. Tan et al. [11] created an input system for touch screens that is secure to human spies due to highly increased complexity of the input. Video surveillance attacks still work fine. Additionally, the input time of password entry is considerably prolonged. While the above mentioned authors focused on increasing the security of traditional password/PIN, others evaluated alternative authentication systems on public terminals like graphical passwords by Moncur et al. [8] or biometric authentication as done by Coventry et al [3].

Sharp et al. [10] created a system that enables private input and output using PDAs. Users can censor complete displays of terminals and use their PDA to show cut-outs of the screen to read or fill in private data. Its main focus is to operate with any desktop program without modification. Thus, a lot of interaction time is needed to navigate through the screen to find the right spot. Additionally, it requires mobile devices with advanced processing and output capabilities (e.g. a big screen). In contrast to that, PocketPIN focuses on fast, easy and private ad-hoc interaction with public terminals suitable for any mobile device.

6. FUTURE WORK

The results of the study and participants' comments showed some interesting enhancements for PocketPIN that should be addressed in future work. For instance, doing privacy settings at the beginning of each interaction seems too redundant. Instead, the device could store privacy preferences or remember terminals and thus perform step 3 automatically. The same approach can be used to fill out forms automatically as known from modern web browsers to speed up the interaction with the terminal.

Another possible extension is a finer definition of the degree of privacy. So far, only two options are supported for each input field: private (input at the mobile device with asterisks on the terminal screen) and public (input at the terminal, visible to everyone). A finer granularity might be desirable. Thus, four levels of privacy for each input field could be applied. The first means zero privacy and will show the input on the terminal. The second will show asterisks on the terminal screen but plain text on the device. The third displays asterisks on both, while the last hides all information from the screen. It is to be shown whether users will benefit from this extension or if it creates a cognitive overload and results in worse usability.

7. CONCLUSION

In this paper, we presented PocketPIN, a privacy respectful input method for public terminals utilizing mobile devices. Choosing a system that lets users define their own privacy, the concept forms an appropriate trade-off between direct input at terminals, which is fast but insecure and completely private input that unnecessarily complicates interaction when dealing with information that is unimportant to the users. In a user study it could be shown that the participants accepted the idea very well and no major problems could be found throughout the interaction.

8. REFERENCES

[1] Bouncy Castle Crypto APIs. http://www.bouncycastle.org.

[2] Claycomb, W., Shin, D. Secure real world interaction using mobile devices. In Proc. PERMID 2006.

[3] Coventry, L., De Angeli, A., Johnson, G. Usability and Biometric Verification at the ATM Interface. In Proc. CHI 2003.

[4] Denso-Wave Inc. QR Code. http://www.denso-wave.com/qrcode/index-e.html.

[5] Google Inc. ZXing, http://code.google.com/p/zxing/

[6] Hutchings, H. M., Pierce, J. S. Understanding the Whethers, Hows, and Whys of Divisible Interfaces. In Proc. AVI 2006.

[7] Kumar, M., Garfinkel, T., Boneh, D., Winograd, T. Reducing Shoulder-Surfing by Using Gaze-Based Password Entry. In Proc. SOUPS 2007.

[8] Moncur, W., Leplâtre, G. Pictures at the ATM: exploring the usability of multiple graphical passwords. In Proc. CHI 2007.

[9] Rogers, J. Please enter your 4-digit PIN. In Financial Services Technology, U.S. Edition, Issue 4, March 2007.

[10] Sharp, R. Scott J., Beresford A. Secure Mobile Computing via Public Terminals. In Proc. Pervasive 2006.

[11] Tan, D., Keyani, P., Czerwinski, M. Spy-Resistant Keyboard: More Secure Password Entry on Public Touch Screen Displays. In Proc. OZCHI 2005.

[12] ThoughtWorks. .NET QRCode Library. http://www.twit88.com/home/opensource/qrcode.