SeCuUI: Autocomplete your Terminal Input

Max-Emanuel Maurer
Media Informatics Group
University of Munich
Amalienstr. 17, 80333 Munich, Germany
max.maurer@ifi.lmu.de

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

ABSTRACT

With SeCuUI we present a solution that aims to increase security of data entry on public terminals. The user can enter all data requested by the terminal using her mobile device. Sensitive data can be hidden from prying eyes by exclusively showing it on the user's mobile. To speed up the whole process, the SeCuUI-client stores previously entered data on the mobile device to provide auto form filling capabilities.

Keywords

Security, privacy, mobile phones, public terminals.

Categories and Subject Descriptors

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

1. INTRODUCTION

Many people have to deal with the problem of public terminal security everyday. Especially concerning PIN-entry at ATMs a large number of proposals have been made to confine the possible number of frauds. None of them has established itself so far. This is mostly because increasing security usually leads to decreased usability. Especially input speed normally reduces immediately when using a more secure input method.

With SeCuUI we present a solution that makes use of the user's mobile device (e.g. a cell phone) to input secure information. The smaller keypad in the proximity of the user protects her from modifications at the terminal or other password theft techniques like shoulder surfing. To speed up the input on the mobile device, SeCuUI remembers user input and is then able to complete similar forms in the future automatically.

Other work in this field mostly focused on password entry. Tan et. al. [6] presented their spy-resistant keyboard. Malek et al. [3] outlined a pressure-based drawing system for passwords and Sobrado and Birget [1] presented a method where certain password icons define a clickable region. Apart from that, Sharp et al. [5] came up with the idea of moving the complete input and output to a mobile device.

SeCuUI in contrast synchronizes only the important components in a device specific manner. This way, the user can choose which value she wants to enter by which means.

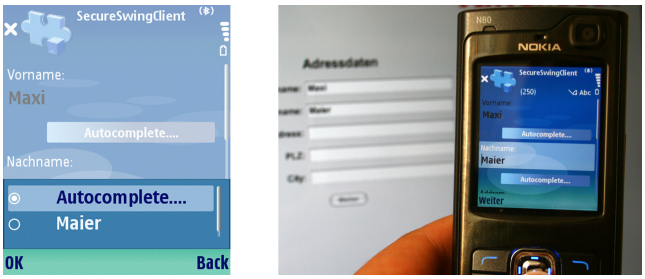

Figure 1: Using the mobile device to enter data with autocomplete feature

2. SECUUI CONCEPT

SeCuUI works with any mobile device. A small JavaME-based application is installed on the device to make it SeCuUI-ready. After that, it is capable to connect to any public terminal that runs a software based on the SeCuUI-framework.

2.1 Framework

When building a Java application with this framework the user interface elements are specified with the help of an advanced version of the XUL interface description language [4]. Any interface specified this way can be transferred by the framework to the mobile device. For SeCuUI we developed an extended version of XUL. It introduces new attributes that allow the developers to control where the components should be visible and whether they should be editable. For each input field the developer may also set the type of information. This helps the autocomplete feature to display the correct values.

2.2 Interaction Procedure

Once Alice has set up her mobile device to work with SeCuUI terminals, she can immediately use her device on public terminals capable of SeCuUI.

First she starts the application on her mobile device and selects a connection method. For our prototype we used a 2D-barcode connection with QR-Codes by Denso-Wave [2]. In this case she takes a picture of the barcode displayed on the public terminal. The mobile application analyzes the picture and connects to the public terminal.

MobileHCI09, September 15 - 18, 2009, Bonn, Germany.
ACM 978-1-60558-281-8.

Now all display components are transferred to the mobile device and Alice can use her mobile phone to enter any data she wants. If she entered a value of the same type earlier she is presented with a list of possible values. Changes on one of the devices are immediately synchronized, so Alice can decide whether to input any data on the terminal or the mobile side. Figure 1 illustrates how SeCuUI is used.

SeCuUI also gives the possibility to display some portion of the text only on the display of the mobile device. This way, private data – like the current bank account value – can be covered from prying eyes.

3. EVALUATION

3.1 Setting and Tasks

When evaluating SeCuUI we were mainly interested how much an autocomplete feature helps to increase the input speed. We conducted a user study with a desktop computer as a public terminal and provided each of our participants with the same mobile phone (Nokia N80). Each participant had to complete five different tasks in random order, three of which were important to understand the automplete-differences and are discussed here.

After a practice period, the participant had to perform the different tasks. Each task required the user to buy a predefined product out of a range of three products. After that they needed to enter their personal data and provide credit card information.

During our reference task – we refer to it as task 1 – each user should enter all the data without the mobile phone. In a second task, the participant was asked to connect the device with the terminal and enter everything using the mobile phone's keyboard. The third task was identical to task 2 but the autocomplete feature assisted the user with data entry. Additionally each participant completed a questionnaire after finishing the tasks.

3.2 Results

3.2.1 Basic Data

We recruited 21 volunteers with an average age of 27 years and a nearly even male/female ratio (11 male and 10 female). Results show that the participants use public terminals for a huge variety of services. One third of them even prefers using vending machines. For 52% it depends on the situation. Two participants have no preference and only one participant prefers the personal contact to a clerk. On a Likert scale from 1 'not important' to 5 'very important' security averaged with 4.52, followed by simplicity with 4.38 and speed with 4.24. Only design was less important to the participants with 2.67.

3.2.2 Interaction Speed

During each task, the participant had to input the same contact information and the same credit card number. To minimize the thereby aroused order effects the task order was randomized. Time was measured from beginning till the end of the interaction including the connection time (does not apply for task 1).

With a desktop computer as a representation for the public terminal our reference task could be completed in 78 seconds (SD 23.0). Entering all the information using the mobile device without autocomplete feature took 237 seconds (SD 79.9) in average. With the autocomplete function activated the average time was 132 seconds (SD 43.5) (see figure 2). None of the mobile device tasks' was accomplished faster than the reference task 1. This depends on one hand that it already costs some time to connect the mobile device to the public terminal. The average connection time was 30 seconds (SD 17.1). On the other hand the reference task was very easy to accomplish since the participants had been provided with a standard QWERTZ-keyboard.

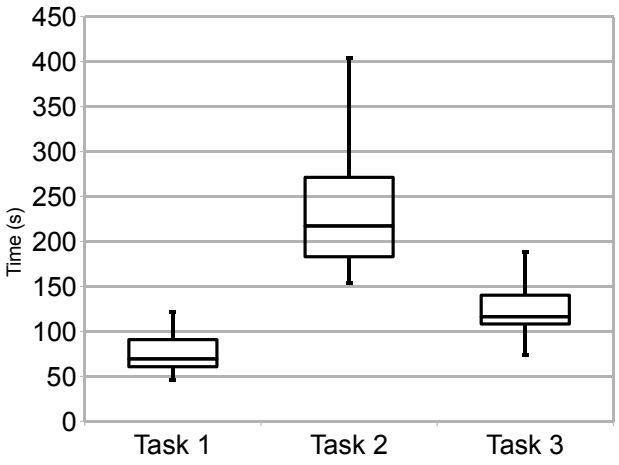

Figure 2: Average time needed to complete the different tasks.

Besides that, autocomplete did perform very well. Task 3 was completed highly significantly faster than task 2 due to the use of autocomplete ($t(18) = 9.76$, $p<.001$). When our participants were later asked to rate the input speed on a Likert scale from 1 'slow' to 5 'fast' the autocomplete task was even rated equally (3.81) to our reference task 1 (3.76).

4. CONCLUSION AND FUTURE WORK

In this paper we presented SeCuUI, a solution that enables the user to enter personal data more securely using her own mobile device. Extended with an autocomplete feature, this method nearly maintains normal input speed. The use of a mobile device is not obligatory so users can decide for themselves whether they want the additional security despite some overhead.

The concept of an autocomplete device for public terminals seems to be promising since it reduced the additional time of the interaction using a mobile device significantly. To get a better view on this issue a future study should be conducted in a more realistic environment with a real vending machine in public.

5. REFERENCES

[1] J. Birget, D. Hong, and N. Memon. Robust discretization, with an application to graphical passwords. cryptology eprint archive, report 2003/168, 2003. 2003.

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

[3] B. Malek, M. Orozco, and A. El Saddik. Novel shoulder-surfing resistant haptic-based graphical password. In *Proc. EuroHaptics*, volume 6, 2006.

[4] Mozilla Corporation. http://www.mozilla.org/projects/xul/.

[5] R. Sharp, J. Scott, and A. R. Beresford. Secure mobile computing via public terminals. In *Proc. Pervasive 2006*, volume 3968 of *Lecture Notes in Computer Science*, pages 238–253. Springer Berlin / Heidelberg, 2006.

[6] D. Tan, P. Keyani, and M. Czerwinski. Spy-resistant keyboard: more secure password entry on public touch screen displays. In *Proc. OZCHI '05*, Nov. 2005.