Don't Queue Up! User Attitudes Towards Mobile Interactions with Public Terminals

Julian Seifert
Ulm University
Ulm, Germany
julian.seifert@uni-ulm.de

Alexander De Luca
University of Munich
Munich, Germany
alexander.de.luca@ifi.lmu.de

Enrico Rukzio
Ulm University
Ulm, Germany
enrico.rukzio@uni-ulm.de

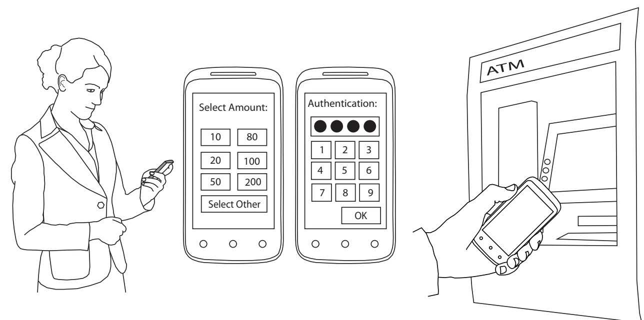
ABSTRACT
Public terminals for service provision provide high convenience to users due to their constant availability. Yet, the interaction with them lacks security and privacy as it takes place in a public setting. Additionally, users have to wait in line until they can interact with the terminal. In comparison to that, personal mobile devices allow for private service execution. Since many services, like withdrawing money from an ATM, require physical presence at the terminal, hybrid approaches have been developed. These move parts of the interaction to a mobile device. In this work we present the results of a four week long real world user study, in which we investigated whether hybrid approaches would actually be used. The results show that users accept the hybrid service as they understood that they could use down downtimes (like bus rides) to prepare the interaction with the public terminal. Our findings give novel insights about security relevant aspects such as where and when users interact with the mobile service before accessing the public terminal. So the preparation of the transaction on the mobile phone was often conducted much further away from the terminal than expected (81.0% with a distance greater than 400m) and earlier than expected (82.1% at least 5 minutes in advance).

Keywords
Mobile interaction, public terminals, security.

Categories and Subject Descriptors
H.5.2 [**Information Interfaces and Presentation**]: User Interfaces.

General Terms
Design, Human Factors, Security.

1. INTRODUCTION
Public terminals are a very convenient tool for all kinds of services. They allow for service execution at any time while reducing costs for the service provider and increasing benefits for the users. For instance, they can be used to buy snacks, drinks, tickets, or even gold. Users can benefit from interacting with these machines in many ways. However, two main challenges can be identified: (1) at times, users have to wait in line before they can start interacting with the machine and (2) public terminals are prone for manipulations by attackers or shoulder surfing attacks.



(a) (b) (c) (d)

Figure 1: Illustrating the concept of mobile transaction preparation. a) The user starts the interaction on the mobile phone and prepares the transaction by b) selecting the amount of money and c) entering the personal PIN. d) The user starts the payout through transmitting the transaction token to the automatic teller machine.

One option to address the first challenge is to increase the number of terminals. However, this comes at considerable costs for the service provider. Thus, another versatile option is to provide mobile services based on the personal smartphone of the user. For instance, users can purchase flight tickets, perform online check-ins and even present their boarding pass, all by using their smartphone. This way, both issues are addressed, as users do not have to wait in line and shoulder surfing attacks are significantly harder to conduct.

This approach is only applicable if the corresponding service does not require connection to physical objects. Thus, it is for instance, not an option for withdrawing cash from an automated teller machine (ATM). A connection between the physical service (thus the terminals) and the mobile service has the potential to provide the desired convenience and solve the previously mentioned problems.

Various approaches for mobile interactions with public terminals for payment, transportation, ticketing and access control have been investigated recently and are already commercially available. This concept is very popular in Japan where circa 60 million "Osaifu-Keitai" (mobile phones with wallet function) can be used for payment in more than 1 million shops or as membership cards or keys [4, 9]. Another example is the recent launch of Google's smartphones, which have a Near Field Communication (NFC) module that allows users to pay through touching terminals with their phone [8, 12]. Furthermore there is a large body of research which investigated architectural [1], security [2, 10] and user interface aspects [11, 6] within the given context. In particular, efficient and effective solutions can be found that protect information stored on the mobile phone and communicate them in a secure way as can be seen in the large number of available mobile banking applications and contact-less payment solutions (e.g. [3]). However, no research has analyzed the behavior and opinion of users when performing such mobile interactions with public terminals and in particular where and how much in advance they might start the interaction on their mobile device.

In order to run a real world user study, we implemented an interaction concept which combines the advantages of mobile services on the smartphone and stationary service machines, such as ATMs. In short, the user creates a transaction token using the smartphone which contains all information about the service transaction. Then, this token is transmitted to the public terminal and the service items are delivered. For instance, if a user wants to withdraw cash from her bank account, she uses her mobile phone to prepare the transaction (see Figure 1a). After specifying the amount of money and authenticating (Figure 1b,c), the user goes to the ATM terminal and transmits the transaction token (e.g. by means of near field communication (NFC)). By doing so, the withdrawal is triggered (see Figure 1d). In addition, the whole transaction can also take place at the terminal only.

2. CONCEPT OF MOBILE SERVICE USE

The concept of mobile interaction with terminals is based on splitting the process of the service into two parts: preparation and execution. The advantages from the user's point of view are flexibility and reduced interaction times with the terminal which leads to shorter waiting times. Flexibility in terms of location and time allows users to perform the preparation in individual contexts. Thus, the preparation can happen during downtimes of the user such as during bus rides. At the same time, users can perform the preparation in a secure environment of their choice which prevents attackers from spying on the user's PIN. Here one has to rely on the user to choose a secure and private context as many already do when using one of the popular banking apps offered by many banks.

Scenario: Alice is in the metro heading downtown where she is going to meet friends in a cafe. She needs to withdraw cash firstly. As she is late and does not want to wait in line at the ATM, she starts the banking application on her smartphone and prepares the transaction. That is, she selects from a list of favorites the amount of money and authenticates to finish preparation. When she arrives at the station, she goes to the special express ATM, touches it with her mobile phone and picks up the money.

In case the mobile phone is lost after preparation, firstly the finder does not know the authentication code to unlock the phone, secondly most ATMs have CCTV that will record an illegal withdraw and thirdly the user can lock all financial transactions with the mobile phone by calling her bank. A mobile service as suggested in this paper does not have a higher security risk compared with existing mobile banking and payment solutions such as Google Wallet or the widely deployed "Osaifu-Keitai" phone in Japan.

To start the payout, the user in the scenario performed a touch gesture with the phone on the terminal. This can be implemented using different technologies. For instance, NFC allows for fast and secure exchange of information [12].

It should be noted here that this paper is not about presenting a new and optimal solution for the implementation of such a hybrid approach but about gaining insights on if and how hybrid approaches would be used in a (semi-)realistic scenario.

3. USER STUDY DESIGN

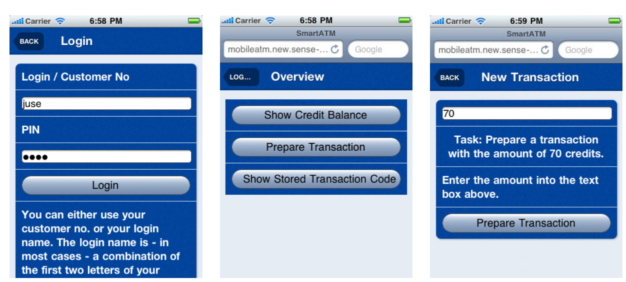
We conducted a user study in order to investigate the following questions. (1) Do users exploit downtimes for configuring transactions? (2) Do users prefer to perform the interaction mobile or on a terminal and what are reasons for using either of the two options? (3) Where and when are users preparing transactions? (4) How do users perceive this system from a usability perspective and (5) how do they feel in terms of security?

In order to investigate these questions, we designed a study structured in two phases. In the first phase, participants used the systems for four weeks. In the second phase, participants filled in a post-hoc questionnaire concerning their experiences with the systems.

We created a test system for the first study phase that allowed participants to perform transactions. Users were instructed that a transaction is similar to the process of withdrawing money from an ATM: Firstly, participants have to configure the transaction (typing in a given amount of money). Secondly, they get a virtual payout at the terminal. In this study, participants received 50 Cents credit for each successful transaction as an incentive (up to a limit of 20 transactions). Further transactions were counted as a lot for a lottery after the study, where participants could win gift vouchers.

In this study, users could create transactions in two different ways. (a) *Hybrid:* Preparation on the mobile phone and execution by entering the transaction code at the terminal. For this, they opened a mobile web page on their own mobile phone, logged in, and performed the preparation (see Figure 2). When the configuration was finished, they received a text message and an email with a five-digit transaction code. In order to execute the transaction, the participant entered this code at a public terminal that served as an ATM dummy (see Figure 3). (b) *Terminal only:* The second option was to perform all steps directly at the terminal.

The terminal (see Figure 3) was set up on a university campus in a highly frequented faculty building near a coffee shop. It could be



(a) (b) (c)

Figure 2: Graphical user interface of the mobile transaction configuration system. a) Login screen, b) service overview, c) transaction preparation for creating a transaction code.

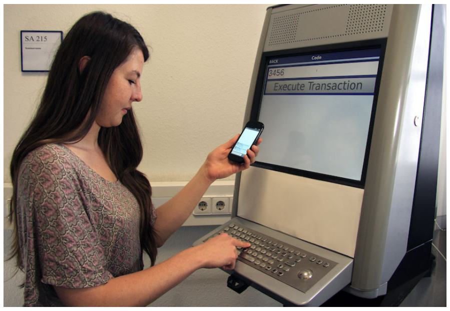


Figure 3: A study participant completing a transaction on the terminal computer by entering the five digit transaction code that she received after preparing the transaction.

easily accessed by all participants at all times during the study. All participants were students, therefore, they all were nearby the terminal anyway which was close to their lecture theaters, labs, cafeteria, learning zones and offices of their lecturers. No participant had to come to the campus only to execute a transaction.

Following the observations by De Luca et al. ([7]), we simulated waiting times at the terminal by displaying a counter that showed the number of seconds until the user could start interacting with the terminal. We modeled the waiting times for terminal-based transactions with $t_{ATM} = \sum_{i=0}^{Q} 28s + (30s * r_i)$. Q models the number of persons waiting in line and is a random variable with values $\{0, 1, 2, 3\}$ whereas the distribution is {0=70%; 1=24%; 2=5%; 3=1%} (cf. [7]). r is a random variable ranging from $\{0.0..1.0\}$. We performed a pretest for measuring the average time for performing a transaction with the study ATM terminal (M=43s, SD=15s). As users, who prepared a transaction on their mobile phone can also experience waiting times before executing the transaction by entering the transaction code at the terminal, we also modeled waiting times for this with $t_{Mobile} = \sum_{i=0}^{Q} 9s + (5s * r_i)$. As additional temporal regulation, participants were allowed to perform only one transaction within 60 minutes in order to motivate them to perform the transactions in a broader variety of contexts.

4. STUDY RESULTS

We recruited 13 participants who performed transactions either with the hybrid or with the terminal only version of the system (four female) and filled in the post-hoc questionnaire. Their average age was 24 years (22-29). All were students (computer science, economics, and humanities), used mobile phones for several years (M=9.2; SD=2.2) and were using a smartphone (e.g. Apple iPhone, HTC Desire, Samsung Galaxy S) at the time of the study in combination with an unlimited data plan. They reported that they withdraw money 1-2 times a week (max. 3). In average, they estimated the maximum waiting time they would be willing to wait with 220s (SD=157.6s). In total, the participants performed 320 transactions in the four weeks of data collection. The great majority was performed using the hybrid version (254). Only a few times users performed the configuration of transaction on the ATM terminal (36). The remainder of recorded transactions was invalidated by the users by creating new transaction codes while old codes were not entered at the ATM yet. Nine participants performed a transaction at the terminal at least once (M=3.54; SD=4.18). The other participants used the mobile version exclusively.

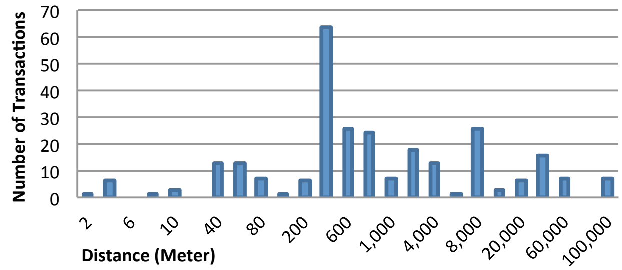


Figure 4: Distribution of distances between the location where the users prepared the transaction on the mobile phone and the ATM.

The mobile web page, which allowed participants to prepare transactions with their mobile phones, also recorded the current location through accessing the GPS-coordinates (using the Webkit API). Analyzing these locations shows that participants were 4.7 km away from the ATM terminal on average (SD=11.4 km). Summarizing the distances into a limited number of classes reveals that the distance varies strongly (see Figure 4). Only few transactions were prepared within a distance of 100 m. Due to GPS aberrations that occur especially when trying to determine the current position while being indoors, we can assume these transactions to be performed inside the university building, where the ATM terminal was located. Most transactions (42.4%) were prepared within a distance of 400 m to 800 m.

Looking at the time duration between mobile preparation and terminal interaction shows that the majority of transactions were prepared and executed within three hours (83.9%). In 41% of all cases, the users went to the terminal within 5 minutes after preparing the transaction. Figure 5 shows how much in advance they prepared the transactions.

Evaluating which version of the system the participants preferred reveals three usage patterns. (1) Four participants used both options throughout the study in arbitrary and randomized order. (2) Four participants used the hybrid version only. (3) Four participants used the terminal at the beginning of the study and used the hybrid version for the rest of the time.

After using the system for four weeks, participants filled in a post-hoc questionnaire. As reasons for using the hybrid version, participants indicated that they liked the flexibility to prepare the transaction anywhere. Participants reported that they performed the mo-

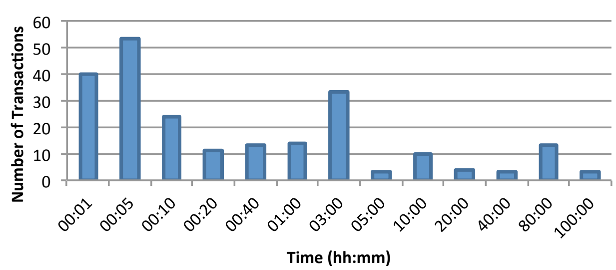


Figure 5: Distribution of durations between starting the transaction on the mobile phone and interaction with the ATM.

bile transaction preparation during downtimes, for instance, while they were using the local public transport. Others reported to perform preparation at home before they left, in cafes or on the way to the terminal. One participant reported to having prepared the transaction on the mobile device while standing next to terminal because another participant was occupying it. Participants stated that the hybrid version is faster and more comfortable to use. For instance, one statement was that 'I spend less time at the ATM as I can prepare the transaction e.g. on the train.'

One participant addressed the security aspect by stating that it would be impossible for an attacker to observe the interaction since the user can do this, for instance, at home. Reasons for performing the interaction using the terminal only version were that the battery of the mobile phone ran out of power, or that they arrived at the terminal without previously preparing the transaction. Also, participants indicated that they were performing transactions on the terminal out of curiosity. One participant emphasized that the terminal only version is more failure-resistant as it cannot run out of power, get lost, or get damaged.

The post-hoc questionnaire included also questions of the system usability scale (SUS) questionnaire for comparing the hybrid and the terminal version regarding general aspects such as *appreciation, system complexity,* and *ease of use* [5]. The results for both systems were similar for all but one statement. Users agreed on average with 4.2 (SD=0.6) (on a 5-point Likert scale: 5 = fully agree) with the statement 'I think that I would like to use this system frequently' for the hybrid version. For the terminal only version the average was 2.7 (SD=0.6). Comparing the two system versions directly, all of the participants indicated explicitly that they would prefer to use the hybrid version of the system if they had the choice.

5. DISCUSSION AND CONCLUSION

The number of transactions prepared on the mobile phone is much larger (79.3%) than those that were performed at the terminal only. The behavior of initially using the terminal only and then shifting to the hybrid version can be seen as a strong indicator for the hybrid version. In addition, none of the participants switched from the hybrid version to the terminal as the preferred option. These results come with two major benefits. Firstly, they indicate that service providers can reduce their costs as the number of terminals could be reduced and secondly, potential customers can save waiting time as they can prepare the transaction in advance.

At the same time, such a hybrid solution could increase the security when withdrawing money as fixed installations to spy on the users' PIN are not working anymore and the risk for shoulder surfing attacks at the ATM is reduced. This advantage is partially compensated by the potential of shoulder surfing attacks when the user is interacting with the mobile application in an inappropriate context. However, it seems that most users are aware of this and use those applications only in relatively safe settings as the intensive usage of mobile banking apps shows. The great advantage of the hybrid approach lies in the aspect that nobody knows whether a certain person interacting with a mobile phone somewhere is currently using a mobile banking application. This argument is supported by our study which shows that the preparation of the transaction on the mobile phone was often conducted relatively far away from the terminal (81.0% with a distance greater than 400m) and well in advance (82.1% at least 5 minutes in advance). This is different to the concept of an ATM where people interact directly to withdraw money.

We designed the study with goal of a very high external validity which we achieved through aspects such as a real physical terminal accessible at all times, a realistic prototype and a study duration of 4 weeks. It was, however, a limitation of our study that the participants didn't deal with significant amounts of their own money which might have had some impact on their usage behavior. A further much more sophisticated field trial (e.g. conducted by a major bank) would be required to investigate such possible effects.

6. ACKNOWLEDGEMENT

We would like to thank the participants of our user study. The presented research was conducted in the context of the Emmy Noether research group "Mobile Interaction with Pervasive User Interfaces" funded by the DFG.

7. REFERENCES

[1] Arabo, A., Shi, Q., and Merabti, M. Ubiquitous secure cash withdrawal. *Int. Journal of Database Theory and Application Vol. 2*, 1 (2009), 39–48.

[2] Bauer, L., Cranor, L. F., Reiter, M. K., and Vaniea, K. Lessons learned from the deployment of a smartphone-based access-control system. In *Proceedings of the 3rd symposium on Usable privacy and security*, SOUPS '07, ACM (New York, NY, USA, 2007), 64–75.

[3] Bianchi, A., Oakley, I., and Kwon, D. S. Using mobile device screens for authentication. In *Proceedings of the 23rd Australian Computer-Human Interaction Conference*, OzCHI '11, ACM (New York, NY, USA, 2011), 50–53.

[4] Boyd, J. Here comes the wallet phone. *IEEE Spectr. 42*, 11 (Nov. 2005), 12–14.

[5] Brooke, J. SUS: A quick and dirty usability scale. In *Usability evaluation in industry*, P. W. Jordan, B. Weerdmeester, A. Thomas, and I. L. Mclelland, Eds. Taylor and Francis, London, 1996.

[6] De Luca, A., and Frauendienst, B. A privacy-respectful input method for public terminals. In *Proceedings of the 5th Nordic conference on Human-computer interaction: building bridges*, NordiCHI '08, ACM (New York, NY, USA, 2008), 455–458.

[7] De Luca, A., Langheinrich, M., and Hussmann, H. Towards understanding atm security: a field study of real world atm use. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, SOUPS '10, ACM (New York, NY, USA, 2010), 16:1–16:10.

[8] Google. Google wallet - make your phone your wallet. `http://www.google.com/wallet/`. (Last Access: 2012/08/01).

[9] NTT DOCOMO. Osaifu-keitai. `www.nttdocomo.com/services/osaifu`. (Last Access: 2012/08/01).

[10] Panjwani, S., and Cutrell, E. Usably secure, low-cost authentication for mobile banking. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, SOUPS '10, ACM (Redmond, Washington, 2010), 4:1–4:12. ACM ID: 1837116.

[11] Sharp, R., Scott, J., and Beresford, A. Secure mobile computing via public terminals. *Pervasive Computing* (2006), 238–253.

[12] Want, R. Near field communication. *Pervasive Computing, IEEE 10*, 3 (march 2011), 4 –7.