mFerio: The Design and Evaluation of a Peer-to-Peer Mobile Payment System

Rajesh Balan[†], Narayan Ramasubbu[†], Komsit Prakobphol[‡], Nicolas Christin[‡], and Jason Hong[‡]
[†]Singapore Management University and [‡]Carnegie Mellon University
{rajesh, nramasub}@smu.edu.sg, {kprakobp, nicolasc, jasonhong}@cmu.edu

ABSTRACT

In this paper, we present the design and evaluation of a near-field communication-based mobile p2p payment application, called mFerio, that is designed to replace cash-based transactions. We first identify design criteria that payment systems should satisfy and then explain how mFerio, relative to those criteria, improves on the limitations of cash-based systems. We next describe mFerio's implementation and user interface design, focusing on the balance between usability and security. Finally, we present the results of a two-phase user study, involving a total of 104 people, that shows that mFerio has low cognitive load and is also fast, accurate, and easy to use – even outperforming cash in terms of speed and cognitive load in common payment situations.

Categories and Subject Descriptors

D.4.m [**Operating Systems**]: Misc; D.2.13 [**Reusable Software**]: Domain Engineering; H.5.2 [**User Interfaces**]: Mobile Payment Systems

General Terms

Design, Human Factors, Experimentation

Keywords

Mobile Computing, User Study, Mobile Payment, p2p Payment, NFC, Near-Field Communication, Digital Wallet

1. INTRODUCTION

Cell phones have evolved from mere communication devices to becoming calendars, instant messaging devices, address books, cameras, photo browsers, and shopping list organisers. Cell phones have also gained increasing relevance as a payment vehicle. It is already possible, in some places, to use a cell phone to pay for vending machine purchases, groceries, and even airline tickets [32].

This research was supported by the Singapore Management University (Grant no. 07-C220-SMU-001), and the Hyogo Institute of Information Education Foundation. Any opinions, findings, conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the Hyogo Institute, Carnegie Mellon University, or Singapore Management University.

MobiSys'09, June 22–25, 2009, Kraków, Poland.

One problem, however, is that current mobile payment solutions all require infrastructure support. In particular, they cannot work if at least one of the parties involved in the payment is not connected to some back-end payment server, via either SMS or GSM/CDMA-based technology. For example, consider the following scenario.

> *Bob takes a taxi, and tries to pay the taxi driver using his cellphone when he reaches his hotel. However, the unloading lobby is underground and neither Bob nor the taxi driver can get a signal on their wireless equipment. Bob has to dig for cash, and also has to keep track of the receipt so he can be reimbursed later.*

Ideally, there would be ubiquitous wireless networking that is reliable and secure. However, wireless connectivity can be affected by a multitude of factors ranging from bad weather to telecom carrier incompatibilities. For example, it is possible for SMS messages to be delayed by several minutes or even hours, which can lead to a poor user experience for a mobile payment system relying on SMS.

In addition to these connectivity issues, the additional cost of subscribing to a central payment service is a likely adoption barrier for small independent operators ("mom and pop" shops). Furthermore, a mobile payment system has to be usable and secure, both in terms of actual implementation, as well as perception by end-users.

In this paper, we present the design and evaluation of mFerio, a novel peer-to-peer (p2p) mobile payment system. mFerio can be implemented on smartphones, does not require any additional connectivity or infrastructure beyond the cell phones of the participants, and was designed with usability and security in mind. mFerio is comprised of three components: 1) a digital cash system, 2) an authentication system, and 3) an easy-to-use interface coupled with a secure communication protocol for making p2p payments. In this paper, we concentrate on the third aspect and defer to prior work for the first two [6, 7, 17, 22, 39].

We make the following contributions in this paper. First, we describe the challenges involved in designing a mobile p2p payment solution. In particular, we analyse the design space and examine some of the key tradeoffs between usability, utility, and security. Many of these tradeoffs are fundamental ones that any mobile p2p payment system will face. We also identify success criteria that payment systems have to meet. Second, we discuss the design and implementation of mFerio and explain how it satisfies the various success criteria. We focus specifically on the tradeoff between usability and security and explain how mFerio manages to provide a user interaction technique that provides both excellent usability and a reasonable level of security. Third, we present the results of a two-phase user study, involving a total of 104 participants, showing that mFerio is very usable – requiring no training and even outperforming cash in speed and cognitive load under common conditions.

2. DESIGN SPACE FOR MFERIO

We start by analysing mFerio's design space; drawing from both prior research [20, 31, 36, 40], and from analysis of the advantages and disadvantages of cash payments. We chose not to compare mobile payments to credit cards as credit cards require infrastructure and thus cannot be used in a peer-to-peer manner. We grouped the design criteria into three main categories: *usability*, *security*, and *auditing*. To be successful, mFerio has to be better than cash in multiple criteria, while not having any significant drawbacks.

2.1 Usability Criteria

A payment system needs to be highly usable by a large cross section of the population to be viable. The following usability criteria provide some guidance towards this goal.

Fast to use. Making a payment should not take too long. Cash is generally a fast payment system, However, as our results show, situations involving even moderate amounts of change can slow down cash transactions significantly.

Easy to use. The payment system should be easy to use by people of different ages and technical competency. Cash satisfies this criterion and is universally used.

Easy to learn. Anyone should be able to quickly learn how to make payments. Cash satisfies that criterion as well, as even young children can be taught to make cash payments.

Predictable performance. Different situations should not affect the performance of the payment system. For example, the time taken to make a payment should not depend on the payment amount. As stated above, cash's speed depends greatly on the situation.

Accurate. Users should be able to transfer exactly the amount of money involved to the intended person, without needing corrections or double checking. Cash is by and large an accurate means of payment. However, its accuracy can be affected by the situation.

Available. The payment system should be usable anywhere and anytime. This is one of the strengths of cash: once created, it essentially requires no infrastructure to be usable. On the other hand, providing high availability for a mobile payment system can be difficult to meet, as it depends on numerous external factors such as digital cash regulatory requirements across the globe, the dynamics between banks, cell-phone manufacturers, telecom service providers and retailers. In this paper, we focus solely on addressing the usability obstacles to availability (i.e., the payment system should not be rejected because it is hard to use).

In summary, a novel payment system, such as mFerio, should achieve the ease of use and (as much as possible) availability of cash, while improving on its accuracy and speed.

2.2 Security Criteria

Payment systems also need to satisfy a number of security criteria. Cash has good security properties, but offers considerable room for improvement as we discuss below.

Preserve transaction semantics integrity. The payment process must ensure that transactions semantics are well defined, and cannot be tampered with. In particular, transactions should be resilient to man-in-the-middle and replay attacks, and guarantee atomicity (i.e., interrupting a transaction will cancel the entire transaction). Usually, transfer of physical currency requires a physical interaction between the parties involved – this provides strong assurance that the transaction semantics will be maintained.

Anonymous. Without external monitoring steps, it should not be possible to identify who made a particular payment. Cash has very strong anonymity properties that make it difficult to trace [21], and a desirable payment choice for privacy-conscious users.

Tamper-proof. It should not be possible to tamper with the payment system and the monetary representation (e.g., digital cash) used. In particular, any attempts to tamper with the system should only result in the system being destroyed and not broken into. Cash, in general, remains usable even if slightly defaced. Alterations resulting in the coin or bill being unusable as legal tender can usually be detected by visual inspection.

Impossible to replicate. The payment system's monetary representation should be impossible to create or duplicate by users. Cash uses numerous physical security measures to prevent counterfeiting without expensive and specialised machinery [1]. In a mobile payment system, this property demands, for instance, that users should not be able to make a backup of their phone, make payments, and then restore their backup and "reclaim" their spent money.

Theft resilience. The system should be resistant to theft. This is one of the main vulnerabilities associated with cash. When a wallet is stolen, the victim has no recovery mechanism available, and ownership of the cash simply transfers to the thief. Mobile payment systems, such as mFerio, can cryptographically store the digital cash on the phone to prevent unauthorised use, thereby ensuring that thieves have no additional incentive to steal phones.

There are already existing solutions for the properties outlined above that can be applied to mobile payment systems. Instead of creating novel low-level security primitives, we chose to integrate existing security technologies [10, 11] into mFerio to achieve a cohesive design, with the goal of yielding a payment system that is both usable and secure.

2.3 Auditing Criteria

It is quite common for users and businesses to regularly perform audits of their spending habits. As such, including auditing criteria in the design of a mobile payment system could improve its mass market appeal. However, satisfying these criteria may require relaxing the anonymity criteria.

Accountable. It should be possible for user to accurately track all payments that they have made.

Dispute resolution. It should be possible to definitively prove that payment has been made to a particular person. This is a stronger form of the accountability criteria.

Cash, by itself, has no provisions for auditing. There are no automatic receipts or mechanisms for dispute resolution. It is possible to layer these features on top of the existing cash system, but they are not available by default. We decided to support both auditing criteria in mFerio; making its anonymity properties weaker than that provided by cash. mFerio uses automatic receipts to provide accounting – allowing the two parties involved in the payment transaction to know more about each other than a corresponding

Success Criteria	Implementation Details	Evaluation Results	Satisfied$_{mFerio}$	Satisfied$_{Cash}$	Relative to Cash
Usability Criteria					
Fast to Use	Section 3.3	Section 5.5.1	$\surd$	$\surd$	Better in Some Situations
Easy to Use	Section 3.3	Section 5.5.2	$\surd$	$\surd$	Same
Easy to Learn	Section 3.3	Section 5.5.2	$\surd$	$\surd$	Same
Predictable Performance	Section 3.3	Section 5.5.4	$\surd$	$\times$	Much Better
Accurate	Section 3.3	Section 5.5.3	$\surd$	$\surd$	Same
Available	—-	Section 7.1[a]	$\times$	$\surd$	Worse
Security Criteria					
Anonymous	Section 3.1	Section 3.2[b]	$\surd$	$\surd$	Slightly Worse
Transaction Semantics	Section 3.1	[10, 11][c]	$\surd$	$\surd$	Same
Tamper-Proof	Section 3.1	[5, 7, 26][c]	$\surd$	$\surd$	Same
Impossible to Replicate	Section 3.1	[6, 26][c]	$\surd$	$\surd$	Same
Theft Resilience	Section 3.1	[11][c]	$\surd$	$\times$	Much Better[d]
Auditing Criteria					
Accountable	Section 3.2	Section 5.5.5	$\surd$	$\times$	Much Better[d]
Dispute Resolution	Sections 3.2 and 3.3	Section 5.5.5	$\surd$	$\times$	Much Better[d]

[a]We discuss some of the factors affecting mFerio's availability in this section
[b]We get anonymity by design as explained in Section 3.2
[c]We use well-designed protocols that have been rigorously validated by other researchers
[d]Feature is completely unsupported by Cash

This table list the success criteria for mFerio. The "Implementation Details" column lists where the implementation for that criteria is described while the "Evaluation Results" column lists where the evaluation for the criteria is presented. The "Satisfied$_{mFerio}$" and "Satisfied$_{Cash}$" columns graphically summarises how well mFerio and Cash satisfy each of the criteria respectively – ticks ($\surd$) are good while crosses ($\times$) are bad. Finally, the "Relative to Cash" column provides a quick comparison between mFerio and Cash (mFerio is the baseline) for that criteria.

Table 1: Success Criteria for mFerio

cash transaction. However, no external party knows anything about the transaction. We believe that this is the right tradeoff between auditing and anonymity. If desired, the auditing features can be turned off to achieve complete anonymity.

2.4 Summary of Criteria

Table 1 summarises the various success criteria, listed above, for mFerio. For each success criteria, it indicates where, in this paper, the implementation details relevant to that criteria are discussed. It then lists where the evaluation results (either in this paper or in related work) for that criteria are presented. It also provides a graphical indication of how well mFerio and cash satisfies each criteria. Finally, it provides a short comparison between mFerio and cash (with mFerio as the baseline) for each criteria. Overall, mFerio is able to satisfy most of the criteria extremely well – the exception being availability which is discussed in Section 7.1.

3. BUILDING MFERIO

We next describe the implementation of mFerio, and relate it to the design considerations presented in Section 2. In particular, we discuss the specific mFerio implementation details that allow it to satisfy each of the three main success criteria groups (shown in Table 1) listed previously.

In the p2p exchanges mFerio aims to support, there are only two parties, the *Initiator* and the *Recipient* – but no central bank. In our design, either party can be *Receiving* or *Sending* payment, resulting in four possible user roles (initiating a payment request, initiating a payment, receiving a payment request, receiving payment)– mFerio supports all four roles. We now discuss how mFerio satisfies each of the three criteria starting with the security criteria, followed by the auditing criteria, and ending with the usability criteria.

3.1 Satisfying the Security Criteria

The security criteria has two main parts; 1) physical security concerning the communications channel and the tokens exchanged between the phones, and 2) user security concerning the sequence of operations that the user must do to complete a transaction. Both are necessary elements for a secure payment system – a highly secure token is useless if the user protocol allows users to pay unintended people while a good user protocol is compromised if the tokens and/or communication channel can be easily tampered with.

3.1.1 Enforcing Physical Security Requirements

A key requirement for a mobile payment solution is a secure monetary token. In this paper, we defer to prior work for an implementation of a secure monetary token – Davies [9] provides an overview of the various digital payment tokens. In a deployed implementation, it is likely that the specific token used will depend greatly on the deployment environment (which country, bank, agency, etc. is deploying the solution). Hence, it seems prudent to concentrate our resources on other aspects of the mobile payment system – that will remain constant across multiple deployments.

In addition to the secure monetary token, to achieve its physical security requirements, mFerio extensively relies on hardware support to provide secure wireless communication mechanisms, fast and secure authentication, and secure data storage. Note: we expect mFerio to store about $500 at most – consistent with the limits imposed by complementary stored-value systems [12, 27].

Secure wireless communication mechanism. To promote ease of use, mFerio should use a wireless communication medium for transactions. This medium must be highly secure, both from systems and usability perspectives (i.e., people can easily perform any necessary actions quickly and correctly).

We chose to use near-field communication (NFC) as mFerio's wireless medium. NFC has three primary advantages over other mechanisms; First, NFC has a very short range, on the order of 1-2 inches (2.5-5cm), making it hard for intruders to intercept communications. Users can clearly see anyone trying to intercept a transaction; in contrast to longer range protocols such as WiFi and Bluetooth. Second, it is quick and easy to set up a NFC connection with another nearby NFC device – simply move one device near the other. This is in contrast to Bluetooth peering which is tedious and slow to set up. Third, NFC has a straightforward conceptual model for users – they know exactly what device they are communicating with, as opposed to longer-range wireless protocols.

Fast secure authentication. We designed mFerio to require users to authenticate themselves to the mobile phone before use. Any of the authentication mechanisms such as pincodes [2, 13], graphical passwords and distortion functions [15], or biometric-based mechanisms [34, 35] can be used with the mFerio application. A full comparison of the usability of the different authentication mechanisms is beyond the scope of this paper. For this paper, we used a Wizard of Oz approach [18] (where the system appears to be fully functional but is actually faked under the covers) for biometric fingerprint authentication. It is important to note that mobile authentication mechanisms have their own flaws but they are still better than not having any authentication at all – as is typically the case with cash payments. We designed mFerio to be able to use any authentication mechanism that gains market dominance.

Secure data storage. The last hardware requirement is secure storage (also referred to on cellphones as a secure element), which should only be accessible if authentication credentials have been successfully provided. This storage will contain the cash and the personal details of the user. If this storage is hardware protected, it ensures that thieves will not be able to access the cash and personal details on a stolen cellphone. As such, this eliminates an extra temptation for thieves as users cannot tamper with the electronic cash by hacking the data storage area. These secure hardware protected chips have already been released by several manufacturers such as Gemplus, Sony, and IBM.

The above mentioned hardware enforced security mechanisms coupled with a secure monetary token satisfy the *Tamper-Proof*, *Impossible to Replicate*, and *Theft Resilience* security-related success criteria (Table 1).

3.1.2 Detailed Payment Protocol

Hardware-enforced security as discussed above is still only a partial solution and mFerio's payment protocol must still enforce transaction semantics (in the database sense of the term). As such, mFerio mandates authentication before transactions can take place, and uses a protocol that guarantees transaction atomicity (i.e., completed transactions should be correctly registered by both parties involved, with the same being true for incomplete transactions).

Authentication increases the number of user steps, potentially impacting usability negatively. However, in this case, security outweighs usability concerns. We adapted existing atomicity protocols already deployed in NFC payment systems [10] and electronic wallet protocols [11] instead of building one from scratch.

Two-touch payment protocol. We use a two-touch protocol, where both parties must touch phones twice to complete the transaction. The first touch exchanges identifying information, using certificates, ensuring that both parties know who they are transacting with, and also establishes a transient secure shared key, which makes the transaction resilient to replay attacks and tampering by external parties. The second touch finalises the transaction. While it is possible to use a single-touch protocol where the whole transaction completes after just one touch of the phone, it also opens up the possibility of errors where payments could be made to someone other than the intended party. Hence, we chose to err on the side of caution, favouring security over usability in this case.

We chose to use the Even-Goldreich-Yacobi protocol [11] to implement monetary exchanges. An alternative would have been Brands' one-time spending certificate [3] which is more tolerant of compromises of the secure storage element. However, Brands' protocol is primarily designed for asymmetric transactions, e.g., involving a point-of-sale and a payer, and would require considerable modifications to be adapted to a peer-to-peer protocol. Conversely, the Even-Goldreich-Yacobi protocol can be implemented without significant changes, in mFerio. The main extension is an atomicity requirement: if the transfer fails, the balance must revert back to the original state before the transaction.

We chose a counter-based mechanism for mFerio as deployed in the Even-Goldreich-Yacobi protocol, rather than a digital coin-based mechanism because a counter based mechanism provides a constant level of overhead; in contrast, digital coins are indivisible, and therefore may require additional overhead when the payer does not have the exact change. The main drawback of counter-based mechanisms is their dependence on a secure element; but as mentioned before, a secure element (secure data storage) is readily available in modern cellular phones, making the counter-based approach viable for mFerio.

Thus, in the mFerio payment protocol, the payer's wallet and payee's wallet, first (during the first touch), agree on the amount of the transaction and authenticate each others certificates. Then, the payer's secure element makes sure that the amount of the transaction does not exceed the wallet's balance, deducts money, and signs the payment message. When the phones touch again (second touch in the two-touch protocol), the payer's wallet sends the payment message. The payee's observer verifies the payment message and adds the amount to the wallet's balance if the message is valid. The payee's wallet returns an electronic receipt as a proof of a transaction. The transfer of payment message and digital receipt must be atomic. If any of the transfers fail the balance must revert back to the original state before the transaction. This method of ensuring atomicity, typically used in databases and financial transactions, minimises message transfers in the protocol.

To further enhance security, we also explicitly require users to re-authenticate themselves multiple times, at key points, during the two-touch protocol. In practice, this approach is only possible if the authentication step is fast and hassle-free. If this assumption proves to be false, alternative strategies, such as single authentication with flexible lock-out timers are available [15]. We revisit this issue in the user study where we ask participants to choose between different types of payment protocols. The results, shown in

Section 5.5.5, reinforce our decision to use a two-touch protocol and multi-point authentication.

Thus the two-touch protocol, coupled with the atomicity considerations discussed above, allows mFerio to satisfy the *Transaction Semantics* criteria.

3.2 Satisfying the Auditing Criteria

A key part of the two-touch protocol discussed previously is the exchange of identifying information between transacting parties after establishing a session key. Identifying information in the two-touch protocols clearly reduces mFerio's anonymity. However, no other party (including banks, certificate authorities, and monitoring agencies) will know anything about the transaction. Thus, mFerio satisfies the *Anonymous* success criteria; but not as much as cash does. Apart from enhanced security, a secondary benefit of compromising anonymity through the use of a two-touch protocol is that it allows us to create automatic signed receipts of each transaction. Availability of signed receipts make accountability and conflict resolution much easier. For true anonymity, mFerio can be easily modified to use pseudonyms instead of actual names – however, that is not in the current implementation. These mechanisms allows mFerio to satisfy the *Auditing Criteria* listed in Section 2.

3.3 Satisfying the Usability Criteria

We implemented several features in mFerio to make it as usable as cash payments while preserving strong security. Firstly, mFerio tells users exactly where they are in the transaction stage (two-touch protocol) and how much more needs to be done – similar to web-based shopping cart checkouts. We display the user's current monetary balance on almost every protocol screen. In addition, mFerio requires users to explicitly confirm the full details of the payment (receiver and amount) involved in a transaction. Once the user has confirmed an action, a transaction summary screen is displayed, where we show both the current, and the expected post-transaction cash balances. This design allows users to a) know exactly how much money they have, and b) completely understand the financial implications of any transaction.

Furthermore, mFerio makes it easy to recover from errors. At any time, the user can click the cancel button and stop the whole process. Before secure keys are exchanged with the other party (first touch in two-touch protocol), the user can also use the back button to go back and change anything they desire. After the first touch in the two-touch protocol, any changes will require cancelling the payment and starting a new one because letting the user go back after exchanging keys would compromise security.

Using User Feedback to Design mFerio. One of our main user study goals was to evaluate the usability of our design decisions. Along with that, we also gathered user feedback to choose among some competing design choices of various mFerio application features. The key design choices we verified in our user studies were

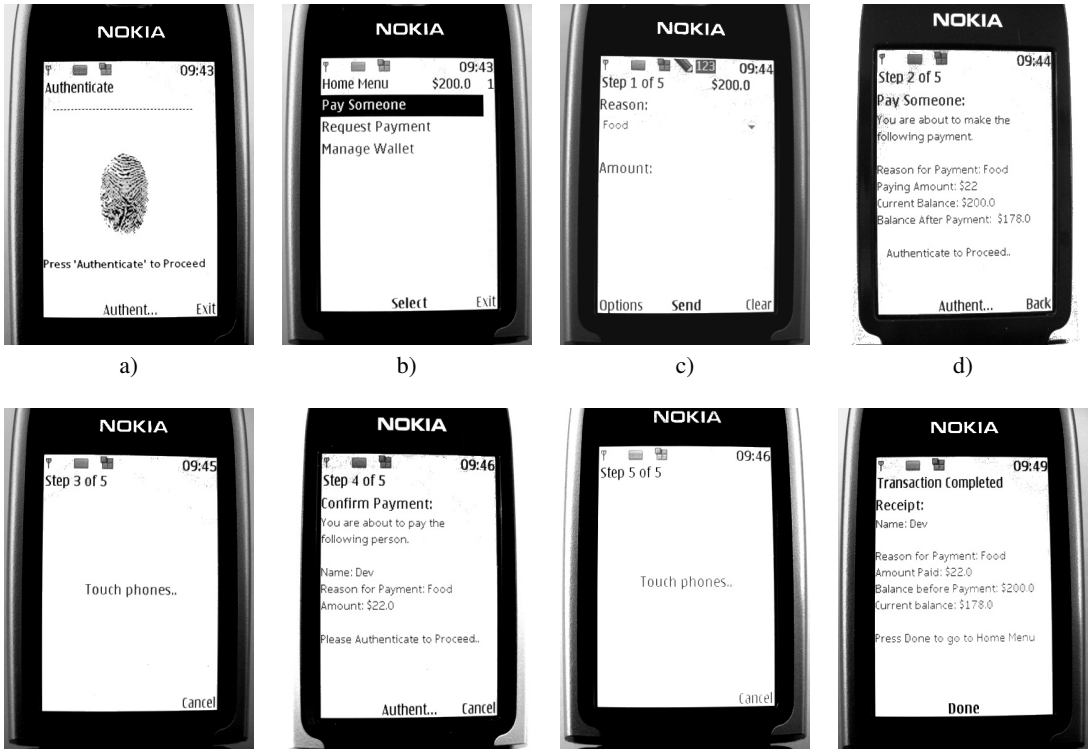
- **One-touch or Two-touch Protocol?**: mFerio uses a two-touch protocol, as described in Section 3.1.2), to ensure that users are confident of who exactly they are paying. However, a two-touch protocol does require a few more steps (and a corresponding increased amount of time) than a one-touch protocol. We verify whether users actually prefer the increased security of a two-touch protocol over the speed of a one-touch protocol in Section 5.5.5.
- **Authentication Mechanism**: mFerio requires users to authenticate themselves before they can perform payment transactions. However, how should this authentication be done? Should the user re-authenticate themselves at every key transaction point? Is a single authentication when starting the mFerio application sufficient? Should there be a timer that triggers re-authentication? If so, what kind of timer (fixed or inactivity-based?) should it be? To gain clarity, we presented users with different possible authentication mechanisms and the results are described in Section 5.5.5.
- **Method for Receiving Transaction Requests**: As stated at the start of Section 3, mFerio can be used in four modes. In all those modes, one party has to receive a request (either for payment or to make payment) from the other party. One key usability decision was deciding how to accept those requests in mFerio. One possibility was for mFerio to always accept requests as long as the user was not performing a transaction at the moment. Another alternative was to require the user to actively state (by entering a special mFerio mode) that they were willing to receive requests. This explicit step increases the burden on the user, but decreases the possibility of the user accidently responding to transient transaction requests. We presented our users with various options for receiving payment requests and present the results in Section 5.5.5.
- **Specifying Reason for Payment**: mFerio automatically creates receipts for each transaction. However, a receipt, by itself, may not be that useful months, weeks, or even days later as many transactions may look similar. Hence, mFerio provides a way for users to annotate their receipts with a reason for the transaction (buying food for example). Section 5.5.5 describes the various options tried and the user response.

Overall, the various mechanisms implemented into mFerio, coupled with the user-driven selection of various targeted features, allow mFerio to satisfy all but the availability criteria specified in Section 2. This claim is well backed-up by the results of our usability tests (shown in Sections 5 and 6). The availability criteria, unfortunately, depends on more than a good implementation and requires market support. We discuss some factors affecting mFerio's availability in Section 7.1.

3.4 The mFerio p2p Mobile Payment System

In this section, we put everything together and show the end-to-end mFerio application. We developed mFerio as a J2ME application on Nokia 6131 phones with built-in NFC capability. Figure 1 shows the sequence of steps needed to perform a p2p transaction with mFerio. The user clicks on the mFerio application and then performs the following steps:

1. The user first authenticates herself, using, for instance, a fingerprint reader on the mobile phone.
2. The user then selects a task from the main menu. She can either initiate a transaction to pay someone or initiate a transaction to request payment. She can also receive payment requests on this screen. Finally, she can do basic management (a feature not tested in this study) of her transaction preferences. For the rest of the description, we assume that the user has decided to pay someone.
3. The user performs the first transaction step. She enters the payment reason from a pre-defined pull down list, types in the amount to be paid, and clicks okay to proceed. Note that the current step is shown on the top left of the screen.
4. In the transaction's second step, the user confirms the reason for payment and the payment amount. She has to re-authenticate at this screen to confirm the payment.



In this example, the user is initiating a payment. The sequence of steps for other three payment modes of mFerio (ask for payment, receive payment, and receive request for payment) are similar. The user (a) first authenticates herself using a biometric fingerprint reader, (b) chooses to pay someone, then (c) selects a reason from a predefined list, and enters an amount to pay. The user (d) sees how much will be paid, (e) touches her phone with the recipient's phone, and then (f) confirms the payment. Once confirmed, the user (g) finalises the payment, and then (h) gets a receipt.

Figure 1: Screenshots of the mFerio Application

5. The user then brings her phone next to the recipient's phone. The recipient must be running mFerio and be in receive mode. During this first connection, a private session key is created for use by both the initiator and the recipient using the Diffie-Hellman protocol. Each party's mFerio application then encrypts basic information such as name and exchanges it with its peer using the adapted Even-Goldreich-Yacobi protocol.

6. Basic information about each party is next displayed along with the transaction details. For example, as shown in Figure 1f), the initiator will see the recipient's name, the payment amount and reason for payment, and the values of her stored cash before and after the transaction. The recipient will see something similar. Both parties must re-authenticate themselves to proceed to the final step.

7. The phones touch again to finalise the payment transaction (using the Even-Goldreich-Yacobi protocol).

8. A "transaction complete" summary page is shown. This page is then stored as an automatically signed receipt.

4. EVALUATION METHODOLOGY

In this section, we explain how we evaluated the performance of mFerio. Our goal was to determine if it satisfied the success criteria described in Section 2 and summarised in Table 1.

We evaluated mFerio in two phases. The goal of the first phase (Phase 1) was to test the effectiveness of the mFerio user interface, and to fix any deficiencies found before investing the effort to build a full system. Thus, we built a complete user interface that followed the exact sequence of steps detailed above, including exchanging information using NFC. However, we did not implement any of the security mechanisms needed for cash exchange as they were unnecessary for validating the user interface – allowing us to focus on key usability criteria without interference from other components. A secondary goal of the phase 1 study was to identify key design decisions that required user input (Section 3.3).

In the second phase (Phase 2), we implemented the complete secure mFerio application, including the key exchange and encryption schemes necessary to guarantee the transaction security.

In both phases, we tested the speed, accuracy, and ease of use of mFerio relative to cash transactions. In phase 1, we also asked users to test specific components of mFerio such as the receipt feature and various authentication methods. In phase 2, we conducted a full cognitive load test, using the NASA TLX method [14], of mFerio and cash transactions to measure exactly what the differences between mFerio and cash are.

In addition, in phase 2, we conducted system performance tests to measure exactly how long the security protocols took to complete a transaction – the performance figures for the rest of mFerio are omitted as it simply involves moving from one screen to another which takes negligible time. The phase 1 study is detailed in Section 5 while the phase 2 study is detailed in Section 6.

5. PHASE 1 STUDY: BASE PROPERTIES

We next describe our phase 1 user study. The primary goal of this first study was to assess how well mFerio met the base criteria laid

Expt Code	Amount in Wallet ($)	Payment Amount ($)	Change Received ($)	Objective
CB 1	10 (1 five, 2 twos, 1 one)	2	None	1 bill exchanged with no change.
CB 2	80 (1 fifty, 2 tens, 2 fives)	75.16	4.84	Few bills with change involved
CB 3	85.16 (1 fifty, 2 tens, 3 fives, 1 ten cent, 1 five cent, 1 one cent)	75.16	N/A	Few bills where participant needed to dig for exact change

The participant was the one paying with the experimenter receiving the payment.

Table 2: Core Task Set 1 – Cash

Expt Code	mFerio Starting Value ($)	Payment Amount ($)	Change Received ($)	Objective
mFB 1	80	−75.16	N/A	Using mFerio to pay experimenter
mFB 2	80	+75.16	N/A	Using mFerio to receive payment from experimenter

The participant had to initiate all payments. In one experiment, the participant had to pay the experimenter. In the other, the participant received payment.

Table 3: Core Task Set 2 – mFerio

out earlier. A secondary goal was to gather detailed process data to help identify areas for future improvements and research, and to allow us to refine the design for the subsequent phase 2 user study. We simulated the use of a fingerprint reader for fast authentication by asking the users to press a button on the phone to simulate the fingerprint reader (we added a little delay after the button press).

5.1 Method

We divided the experiments into three sets: tasks involving cash, tasks involving mFerio, and a set of tasks to capture any learning effects. The evaluation was within-subjects, but the task sets were not randomly ordered (cash experiments came first and then the mFerio experiments). Participants performed the cash experiments first and then used mFerio. We chose this approach as we do not believe there are any learning effects going from cash to mFerio since people are already highly familiar with cash payments. Tasks within each core task set were counterbalanced, however.

Each individual task took about 1 minute to complete, and had the same basic structure: participants were asked to either receive payment or pay the experimenter (the amounts involved was provided to them). A task was considered finished when the transaction was completed. To minimise bias, the choice of whether a participant received or sent payment was randomly determined.

After each individual task, participants were provided a simple questionnaire that asked them to rate, on a 5-point Likert scale, a) whether they thought the task was quick to perform, b) how easy they found the task, and c) how confident they were that they completed the task correctly. At the end of each set of tasks, participants were given a longer questionnaire.

Task set 1 – Cash. In these baseline experiments, we measured the time taken by participants to complete three typical cash transactions – using those times to establish a baseline target for mFerio. The cash tasks are described in Table 2. Each individual task started with all money inside the wallets of both the participant and the experimenter, and the wallets kept in their usual place (inside a purse, pocket, etc.). The task was considered finished when the final bills were received, counted, and returned into the appropriate wallet.

Task set 2 – mFerio. In this set of experiments, participants were asked to use mFerio to both pay someone and to send payment to someone. In both cases, the participant was the initiator of the transaction. At the end of the user study, the participant was asked to redo one of the two tasks in this set (chosen randomly) to observe any learning effects. The tasks for this set are described in more detail in Table 3. For each of these tasks, the participant had to click an icon to start the mFerio application. A task was considered complete when the user reached the final confirmation screen and clicked done on that screen (see Fig. 1h).

Task set 3 – mFerio Learning. After completing all the mFerio tasks in Set 2, the participants were asked to repeat the first task they did in Set 2. This was to detect any mFerio learning effects.

5.2 Participants and Setup

We recruited a total of 75 undergraduate students for our phase 1 study. Participation was open to all students at our university, and we solicited participation through flyers, student association emails, and also through specific emails sent to students who had previously registered with the university-wide subject pool list. All 75 students did the same set of cash and mFerio tasks. Each user study took about 30 minutes to complete.

Our participants were a mix of students from technical and non-technical majors. We asked each participant to complete a short (2–3 minutes) demographics survey to determine their familiarity with cell phone technology. The possible answers were, 1) Have you used MMS on your phone? 2) Have you browsed the Internet from your phone? 3) Have you synchronised your phone with any other device or software? 4) Have you installed applications on your phone? Based on the (yes/no) answers given, we categorised users into three buckets – “novice”, “intermediate”, and “expert”.

In addition, we asked each participant to state how important their cell phone was to them by answering the following question: How important is your phone to you? The possible answers were, 1) Not very important. I can go for a day or more without it; 2) Somewhat important. A few hours without it probably will not do any harm; and 3) Very Important, I have to have it with me all the time. Table 4 shows the phase 1 participant demographics.

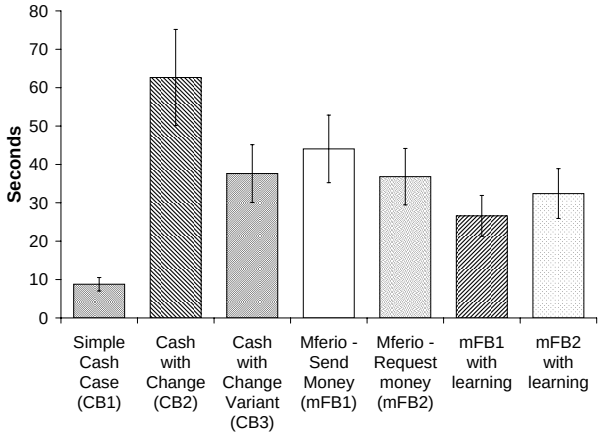
Participants were compensated at a flat rate of $10 SGD on completion of all tasks. We stressed that they were not under time pressure, and could take as long as they needed to complete the task – a deliberate bias against our goal of fast transaction times.

5.3 Experimental Procedure

The participants worked alone in a lab for the duration of the study. For all experiments, a tester played the role of the other person involved in the p2p transaction. Participants were provided phones, basic training in how to use the phone and the NFC capability, and instructions for each task in the study. The training period

Total number	75
Gender	Male (35), Female (40)
Proficiency level	Novice (22), Intermed. (30), Expert (23)
Phone importance	Low (8), Medium (36), High (31)

Table 4: Demographic statistics for Phase 1 Study.



The error bars indicate standard deviations. Pair-wise t-tests of the results show significance at 5%.

Figure 2: Measured Speed of mFerio and Cash

lasted less than five minutes, and involved the participant entering alphanumeric input into a text box and then transferring that input to another phone using NFC. This training helped teach the participants how to use the phone's NFC feature, and helped ensure that participants were comfortable with the data entry features of the Nokia 6131 NFC phone (e.g., backspace, decimal point, etc.). We did not train our participants to use mFerio – the first time they saw and used the application was during the real experiment.

5.4 Data Collected

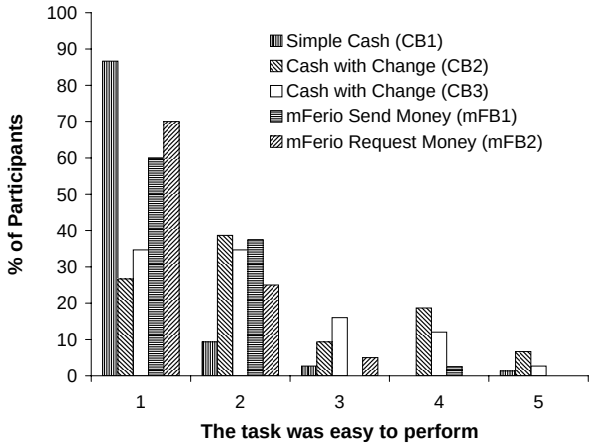
We obtained completion times for each task and subtask (i.e., time to progress from one screen to another) by instrumenting the phones. We also observed the participants during the study and noted where they had trouble, were confused, or made mistakes. Finally, we measured our participants perceptions, through an exit survey, on quality of training, ease of use of mFerio, and user reported performance for each subtask.

5.5 Results of Phase 1 User Study

5.5.1 mFerio is Fast

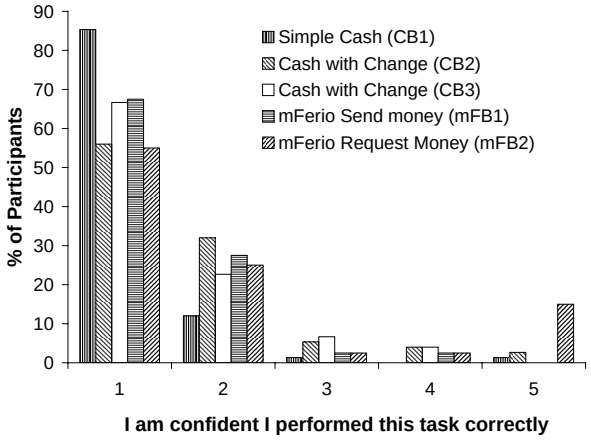
Figure 2 shows the time taken by the 75 participants to complete the 3 cash experiments (Table 2) and the 2 mFerio base case experiments (Table 3). In addition, participants were asked to repeat the mFerio base case experiments at the end of the user study to observe the effect of learning on speed of use. We also show the results for these repeated experiments.

As expected, the simplest cash experiment (CB1) was the fastest to complete. However, more complex tasks, where change was involved, was slower to complete with cash than mFerio (comparing CB2 and CB3 with mFB1 and mFB2). For task CB3, we did not tell the participants a-priori that the cashier did not have change. If the participants provided a larger amount, they were told to provide exact change. As such, we expected task CB2 (paying and getting change in return – a fairly straightforward task) to be the same or faster than task CB3 (paying exact change), but our results show



The x-axis is a 5-pt Likert scale. Scores to the left are better.

Figure 3: Perceived ease-of-use of mFerio



The x-axis is a 5-pt Likert scale. Scores to the left are better.

Figure 4: Perceived Accuracy of mFerio

the opposite. We observed that our participants were more careful about checking the amount of change they received, thus leading to slower task completion in CB2.

In addition, mFerio showed a strong learning effect (comparing mFB1 and mFB2 with the corresponding "With Learning" bars) and after just 15 minutes of use, participants showed improvements of up to 40% in performance. Hence, we conclude that the speed of using mFerio is comparable to or even faster than a large number of common cash use cases.

Participants also rated, on a 5-point Likert scale, how fast they thought mFerio was to use. mFerio scored a 1.7 (1 is best, 5 is worst) with a standard deviation of 0.75 – indicating that users were happy with mFerio's speed.

5.5.2 mFerio is Easy to Use with Minimal Training

Figure 3 shows how participants rated mFerio's ease of use on a 5-point Likert scale (lower is better). Results are promising – 60 to 70% strongly agree that mFerio is easy to use while less than 5% were either neutral or somewhat disagree. No participant strongly disagreed that mFerio is easy to use.

5.5.3 mFerio Payments are Perceived as Accurate

Figure 4 shows the perceived accuracy of mFerio (same 5-point Likert scale, lower scores better). Overall, participants were posi-

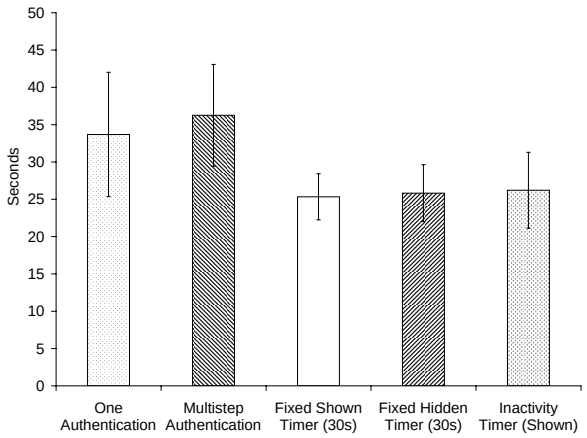


Figure 5: Task Speed in different Authentication Modes

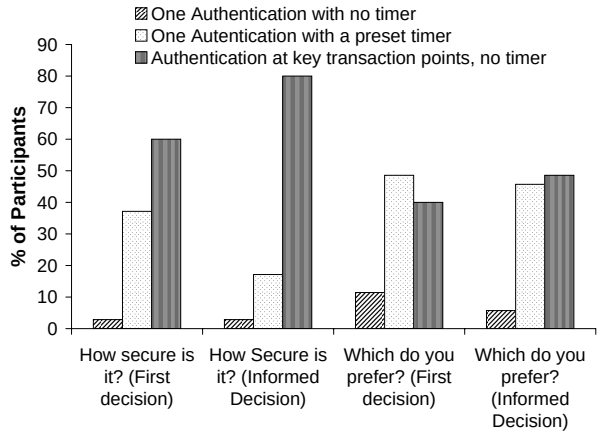


Figure 6: User Perception of Authentication Modes

tive, with 68% strongly agreeing that it is accurate. We had a few outliers, that strongly disagreed that mFerio is accurate. The outlier observations were all for the "Request Money" task (the accuracy question for this task was reverse coded); 66% of the outliers were female students; and 33% of them were expert users. We did not find any other abnormal behaviour, with respect to these outlier participants, across the other tasks that would suggest a design flaw in mFerio. Hence we do not see this as a cause for concern.

Even with these outliers, a large majority of the participants still perceived mFerio as being very accurate. Given that the participants had never used mFerio previously, these results are very encouraging. Our future work involves developing techniques to further improve mFerio's perceived accuracy.

We assessed the actual task accuracy only at the end of each task; by checking if the correct sum of money had been transferred (either physically or digitally). We did not capture any errors that took place during the task and were subsequently corrected. We found that in all cases, the amount of money transferred was correct.

5.5.4 mFerio has Predictable Performance

We estimated task performance differences for the cash experiments by calculating the difference in time and perceived ease-of-use between the cash experiments. The difference in times between CB1 and CB2 (Fig. 2) is significant at 1% (CB2 is on average 53 seconds or more than 6x slower to complete than CB1), while the difference in perceived ease-of-use between CB1 and CB2 is also significant at 1% (1.35 points, or 27%, on the 5 point scale).

However, we found no significant difference in time, perceived

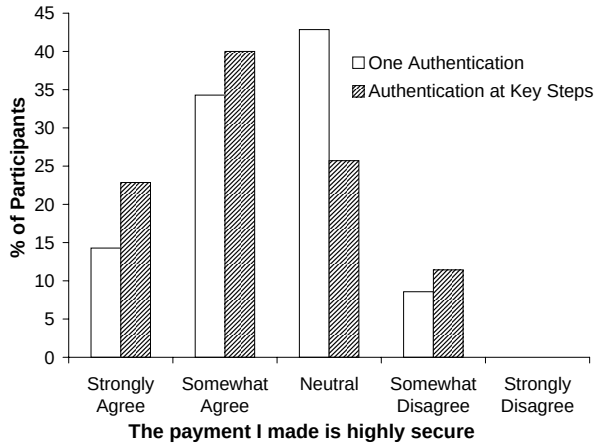


Figure 7: Perceived Security of Different Authentication Modes

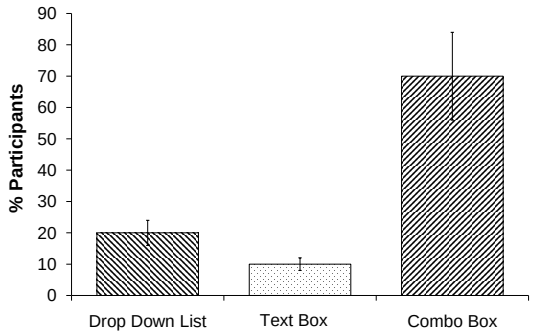


Figure 8: User Preference for Receipt Modes

accuracy, or perceived ease-of-use between different mFerio experiments. This suggests that mFerio does not suffer from unpredictable performance problems even when the payment amount changes. This was not unexpected, as paying someone $75.16 with cash requires more operations and counting than $2, whereas with mFerio, the difference is primarily a few extra text entry steps.

5.5.5 mFerio User Design Choices

In this section, we present the results of the user-verified usability choices described in Section 3.3

One-touch or Two-touch Protocol? : After completing all experiments, users were both interviewed and presented with an end of experiment survey to obtain feedback on their preferred design choices. A significant majority (90%) indicated that they preferred a two-touch protocol even though it enforces several additional steps (an extra touch, two additional confirmations) in a transaction. Users felt that the additional steps in the two-touch protocol gave them more control and better overall security.

Method for Receiving Transaction Requests : After demonstrating the automatic (mFerio automatically accepts requests when not performing transactions), and manual (an explicit receive request mode must be selected) transaction receiving modes, we asked each user which method they preferred. Our results from this survey indicate no significant difference in user preferences. 52% of the users preferred the automatic mode of receiving transaction requests, and 48% preferred having manual control over the ability to receive requests. We thus retained the automatic mode as the default mFerio mode – with a view to change it later if necessary.

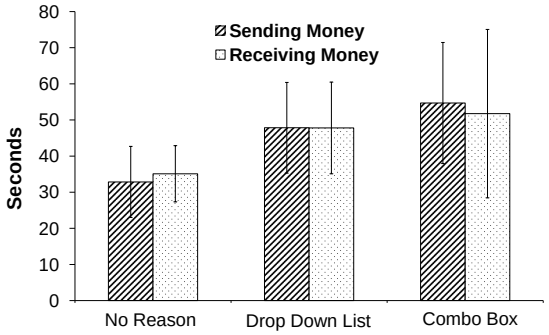


Figure 9: Task Speed in Different Receipt Modes

Authentication Mechanism : During our experiments, we asked users to execute payments using five different authentication mechanisms: One authentication step only (when starting mFerio), multi-point authentication (where authentication is needed at key points during the two-touch protocol), one authentication step at the start of the mFerio application combined with a fixed timer shown to the user, one authentication step at the start of the mFerio application combined with a fixed timer hidden to the user, and one authentication step at the start of the mFerio application combined with an inactivity timer (timer decreases only when the user stops using the cellphone) shown to the user. In the authentication modes with timers, the application would close automatically, cancelling any pending transactions, once the timers reached zero.

We decided to use, guided by our base-case time results (Section 5.5.1), a forty-five second limit for all the timers in our authentication experiments. The time taken to complete transaction when using different authentication mechanisms is shown in Figure 5, while the user preference for various authentication mechanisms is shown in Figure 6. From these results, we can conclude that the timers (both shown and hidden) enhance task speeds. Also, users perceive the multi-point authentication mechanisms as being more secure than the one-step authentication (with or without timers).

We asked users to state their preferred authentication mechanism without explaining to them the security differences between the different mechanisms. At the end of the user study, we explained these differences to the users and asked them to re-state their preferred authentication mechanism (at this point, most users had forgotten their previous answers). The "Informed Decision" bars in Figure 6 show the answers given by users after they were given an explanation of each mechanism. It is interesting to note that, while more users initially prefer to choose one-step authentication with a preset-time, several of them convert to choose the multi-step authentication mechanism after the debrief session.

We also captured user perceptions of payment security when they experimented with the various authentication mechanisms. These results are show in Figure 7. We see somewhat polarised results here. Among users who agreed that the mFerio payment was secure, there were more who perceived multi-step authentications as more secure than the one-step authentication with preset timers. On the other hand, among users who remained neutral or disagreed that mFerio payment was secure, there were more users who perceived one-step authentication with preset timers are more secure than a multi-step authentication mechanism. Overall, both one-step authentication with a preset timer shown to the user, and a multi-step authentication choice seem to be viable for mFerio – the one-step authentication with preset timer enhances task speed, while the multi-step authentication gives users a better sense of control in their payments. For the next phase of mFerio testing (testing a complete system), we used one-step authentication as we did not have any reasonably quick method to perform multi-step authentication. Again, we plan to revisit this design decision, as users seem to prefer multi-step authentication, if fast, reliable authentication mechanisms become commonly deployed.

Specifying Reason for Payment : mFerio provides various ways for users to annotate their receipts with a reason for the transaction (buying food for example). We compared user preference and performance when they used a simple textbox, a drop-down list, and a combobox (editable drop-down list) for annotating their receipts during a mFerio payment transaction. These results are presented in Figures 8 and 9 respectively. Although, the combobox method of receipt annotation increases time taken to complete a transaction (15 seconds more than the base case), there is an overwhelming preference for that. Hence we chose to adopt a combobox style of receipt annotation for the final mFerio prototype build.

6. PHASE 2 USER STUDY: FULL SYSTEM

In phase 2, we tested a complete mFerio implementation, with all security protocols fully implemented. This complements the phase 1 study, by 1) assessing the exact cognitive load of mFerio relative to cash, 2) testing mFerio with a more diverse population, and 3) comparing cash and mFerio in more diverse treatments. The overall experimental setup, procedure, and data collected was similar to that used in phase 1, but the experimental treatments were different.

6.1 Method

This study used three scenarios: base, time pressure, and low light. In the base scenario, participants performed eight tasks – four cash and four mFerio tasks. We used the same four tasks, as stated in Figure 5, for both the cash and mFerio experiments. We only used tasks 1B and 2B (for both cash and mFerio) for the time pressure and low light scenarios as we were primarily interested in user performance with more difficult tasks under adverse conditions.

The evaluation was within-subjects, but the task sets were not randomly ordered. In each scenario, all the cash tasks were performed in sequence first followed by the mFerio tasks (also in sequence). Each task took a minute or less to complete.

After each individual task, participants were provided a simple questionnaire that asked them to rate, on a 5-point Likert scale, a) whether they thought the task was quick to perform, b) how easy they found the task, and c) how confident they were that they completed the task correctly. They were also asked to complete the NASA-TLX survey [14] after each experiment. At the end of all the experiments, the participants received a longer questionnaire.

Scenario 1 – Baseline. The base scenario was used to obtain baseline cognitive load values for cash and mFerio.

Scenario 2 – Time Pressure. In this scenario, we told each participant that they only had 30 seconds to finish each task – simulating real-world situations where payments have to be made quickly.

Scenario 3 – Low Light. In this scenario, we lowered the lighting in the experiment room to simulate low light conditions – such as street light conditions. This simulates common situations where cash payments are made in locations without perfect lighting.

6.2 Participants and Setup

We recruited a total of 29 participants for our phase 2 study. All 29 users did the same set of cash and mFerio tasks. Each phase 2

Expt Code	Payment Amount ($)	Cash Received ($)	Objective
1A	Pay $5	N/A	Simple Cash Exchange
1B	Pay $8.65	N/A	Pay non-trivial Amount
2A	Ask for $1.30	Receive $2 and return $0.70	Collect small payment
2B	Ask for $36.40	Receive $50 and return $13.60	Collect large payment

These four experiments are used for both the cash and mFerio experiments in phase 2 (for all three scenarios). For cash experiments 2A and 2B, the participant received more than the requested amount and had to provide change (amount stated in the "Cash Received" column).

Table 5: Core Task Set – Phase 2

Total Number	29
Gender	Male (19), Female (10)
Age	20 and below (12), 20 to 30 (13) Above 30 (4)
Proficiency Level	Novice (10), Intermediate (7), Expert (12)
Importance of Phone	Low (12), Medium (14), High (3)

Table 6: Demographic Statistics for Phase 2 Study.

user study took about 30 minutes to complete.

Our participants were a mix of undergraduate students (12), graduate students (2), and teaching and support staff (15). The participants had a mix of technical and non-technical backgrounds. We used the same demographics survey as in phase 1 to identify their cell phone proficiency levels and their perceived importance of their cell phone. Table 6 details the phase 2 participant demographics.

6.3 Results of Phase 2 User Study

We observed that the speed, ease-of-use, and accuracy results from phase 2 were similar to those obtained in phase 1 – validating our phase 1 results. Due to space constraints, we only present the new security protocol performance, and cognitive score results.

6.3.1 Measured mFerio Runtime Performance

During these experiments we logged the time taken by the mFerio application to execute the two-touch protocol, using the adapted Even-Goldreich-Yacobi security protocols, described in Section 3.1.2 separately from the user transaction time. As expected, the first touch (exchanging credentials) protocol times (average: 1.069 seconds, minimum: 0.995 seconds, maximum: 1.295 seconds, standard deviation: 0.0732), were significantly lower than the second touch (making payment and signed receipt transfer) protocol times (average: 4.850 seconds, minimum: 4.697 seconds, maximum: 5.242 seconds, standard deviation: 0.150).

Overall, the results are on the high side and indicate that public-key cryptography may not be the most suitable security primitives to use on some cellphones – an area for future mFerio research and implementation. Nonetheless, even with these high protocol times, users still found mFerio faster, with significantly less cognitive load (as shown in the next section), than cash in some scenarios.

6.3.2 mFerio has low cognitive load

Table 7 shows the cognitive load scores for the three scenarios in the phase 2 user study. We computed the cognitive load scores using the method proposed by Hart [14] (ask the user to provide ratings for six dimensions of load and combine those ratings using the user-provided importance rankings). The values in the table are average scores with the standard deviation provided in brackets. The "% Diff." column is the percentage difference between Cash and mFerio for that scenario (i.e. $\frac{Cash-mFerio}{Cash} * 100$)). Positive values indicates that mFerio has lower cognitive scores than cash.

There are no scores for experiments 1A and 2A for the Time Pressure and Low Light scenarios as we did not run these experiments in those scenarios. The "% Change" columns indicate how much the value has changed from the corresponding base scenario value – a positive number indicates that the cognitive load has increased by that percentage compared to the base scenario value.

From the table, we observe that cash has lower cognitive load than mFerio only for experiment 1A in the base scenario (cash has 48.2% less cognitive load). In every other case, mFerio has lower cognitive loads – reaching a high of 68.1% lower load for experiment 2B in the time pressure scenario. Figure 10 shows the breakdown of the cognitive load components for all the base experiments – for both cash and mFerio. The figure clearly shows that, except for experiment 1A, cash has a much higher cognitive load than mFerio – for almost every load component.

We also observe, from the table, that the cognitive load for cash significantly increased in the time pressure and low light scenarios. For example, participants performing experiment 1B reported, on average, 60.8% higher cognitive load values when doing the experiment under time pressure compared to the base scenario.

The cognitive load scores for mFerio also increased in three of the four non-base scenarios (time pressure and low light). However, these increases were not significant. In the last experiment (Low Light scenario, experiment 1B), mFerio's cognitive load actually significantly decreased relative to the base load (by 22.1%). We are investigating the cause of this decrease – we suspect that it might be due to various learning effects (mFerio is not really affected by low light conditions as the phone has a built-in light source).

Overall, mFerio significantly outperformed cash, in terms of cognitive load, in a number of common scenarios. This validates our goal of building an easy intuitive system for mobile p2p payments.

7. DISCUSSION

7.1 Additional Requirements for Deployment

In this paper, we presented part of the overall solution needed for a practical p2p payment system – we focused on the design and evaluation of the user interface. Before such a system can be deployed, several additional challenges need to be addressed:

Stake Holder Dynamics: A successful mFerio deployment will require cooperation from multiple stake holders, such as banks (to support the digital cash used), cellphone manufacturers and telecom service providers (to promote mFerio to their customers), retailers, regulatory bodies (to legalise p2p payments), and consumers. Unfortunately, satisfying the business and strategic goals of multiple stake holders is very difficult and achieving sufficient buy-in may require governmental and regulatory body support. A more detailed discussion of the policy changes and strategies necessary for industry adoption of mFerio is beyond the scope of this paper.

Expt Code	Base			Time Pressure					Low Light				
	Cash	mFerio	% Diff.	Cash		mFerio		% Diff.	Cash		mFerio		% Diff.
				Actual	% Change	Actual	% Change		Actual	% Change	Actual	% Change	
1A	8.2 (2.4)	12.1 (3.2)	-48.2 *	N/A									
1B	15.3 (3.3)	10.6 (3.2)	30.9 *	24.7 (9.2)	60.8 *	11.5 (4.1)	8.4	53.4 *	20.1 (6.2)	31.4 *	8.3 (1.2)	-22.1 *	59.0 *
2A	11.6 (3.5)	6.6 (2.2)	43.1 *	N/A									
2B	18.8 (4.3)	6.5 (1.8)	65.4 *	23.7 (9.0)	25.6 *	7.5 (2.4)	15.6	68.1 *	21.5 (5.5)	13.9 *	7.7 (2.2)	17.6	64.3 *

results significant at 5% (using two-tailed tests) are indicated by *; lightly shaded results are not significant.

Table 7: Cognitive Load Scores

Mass Market Appeal: Ensuring mass market appeal for mFerio is important to leverage scale economies and the network externality effect where mFerio's utility is influenced by one's social network. If the entities in a person's network are not mFerio ready, then one has to still use cash for payments. One way to increase mFerio's mass market appeal is to make it highly usable and an easy replacement for all cash transactions. This, unlike the various other challenges, is something that we can impact. Hence, we concentrated on making mFerio as usable as possible.

Phased Deployment: mFerio is more likely to succeed if it can be introduced gradually. In Singapore, one possible path is to initially introduce mFerio as a replacement for existing mobile payment systems, such as CashCard [27] or EZ-Link [12], that use NFC-enabled cards to make payments; users top up their cards at special machines. mFerio can easily be modified to support these systems initially. As the mFerio user base grows (people might prefer paying with their phones instead of carrying a separate card), the p2p aspects of mFerio can be enabled. We are currently investigating this phased deployment strategy in more detail.

7.2 Comparing mFerio With Other Systems

In this paper, we chose to compare mFerio solely with traditional cash payments. However, there are other mobile payment systems; for example, token-based NFC-enabled payment systems (CashCard, EZ-Link, etc.), SMS-based payment systems (Gpay [33], Obopay [28] etc.), and custom-application or browser-based online payment systems (Paypal Mobile [29] etc.).

These systems are fundamentally different from mFerio as they either use physical secure tokens (Cashcard etc.), or infrastructure support (SMS and online methods). Their protocols can thus be greatly simplified (to one-touch/one-step systems even) as a) the burden of authentication is moved to the infrastructure and/or tokens, and b) the usage scenarios limit the amount of user interaction needed. For example, the amount to pay is automatically computed by the token-based systems (based on length of travel etc.), the cell phone provider has verified details for all participants in an SMS-based payment systems, and Paypal authenticates all participants a-priori. In a true p2p payment system, the onus of authentication mostly falls on the participants of the system. The mFerio protocol is thus quite different and, generally, longer (to provide user input and user-visible authentication) compared to other payment systems; making direct comparisons misleading in our opinion.

7.3 User Study Limitations

Our two user studies are an important first step in identifying the usability of mFerio. However, they do have limitations. First, our participants were mostly 18 – 25 year old undergraduate students – a general population might show different results. Second, both studies were conducted in a controlled test environment – real world situations could affect mFerio's usability differently.

7.4 Effect of Demographics on Usability

We also noticed that the mFerio task completion times did not significantly vary across the experts and novices. Further, we noticed that there was no significant learning differences between the expert and novice population as well. Also, the only significant difference in the mFerio task completion time across the male and female participants was in the mFerio sending money task in phase 1(mFB1). The male participants were faster than the female participants by about 3 seconds on the average in this case. However this difference in performance across the genders disappears when learning effects are accounted for. Hence we infer that there is no significant difference in the necessary design requirements of mFerio across the expertise or gender spread.

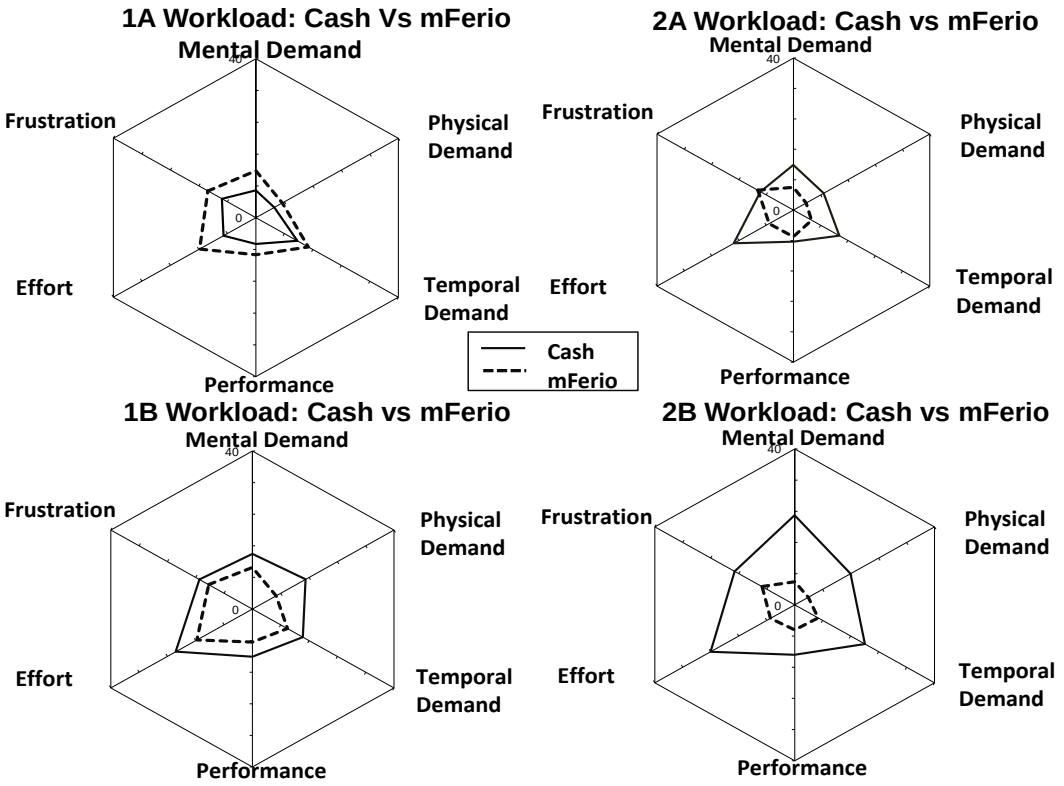
8. RELATED WORK

Davies [9] summarises various technological innovations with monetary payment systems including traditional cash and digital cash. There has also been a fair amount of past work looking at mobile payment in general. Kreyer et. al offer a typology of different mobile payment systems [19] – mFerio falls under the macropayments to stationary merchants and customer-to-customer transaction categories. They also spell out three criteria for general acceptance of mobile payment systems: cost, security, and convenience. In this paper, we focused primarily on convenience though mFerio was also designed with the first two criteria in mind.

Zmijewska [41] provides a summary of various wireless technologies for mobile payment, describing the pros and cons of 2G, 2.5G, 3G, infrared, NFC, and Bluetooth. Zmijewska also describes results from field trials showing that NFC is perceived to be more trusted due to required proximity. Near-field communication is already in wide use for contactless payments, for example, with smart cards and fixed readers. Our work here leverages the growing trend of NFC being installed on mobile phones, and focuses on making payments using phones rather than fixed readers.

Past UI research has looked at using NFC for novel interaction techniques. For example, Pering et. al [30] look at how a gesture to connect two devices together can be implemented using NFC and accelerometers and Want et. al [38] looked at how RFIDs could be used to bridge the gap between the physical and virtual worlds. Chen and Adams [8] provide a survey of different kinds of NFC technologies that could be used for mobile payments. Our work focuses less on developing novel interaction techniques, and more on using NFC to facilitate the sending or receiving of payments.

In addition to commercial smartcard payment systems [12, 25,



Each kiviat graph represents a different experiment. Each of the six axis ranges from 0 to 40 – smaller values are better.

Figure 10: Base Scenario: Cognitive Load Breakdown

27, 37], many other types of mobile payment systems have been developed. For example, SmartRestaurant [24] allows customers to order and pay for meals at university campus restaurants. U-Payment [23] describes techniques for secure and private financial transactions using mobile devices. Herzberg [16] describes many of the security issues involved in mobile payment systems. Our work differs as we are investigating the design and usability evaluation of a distributed peer-to-peer payment system, that uses mobile phones and NFC, rather than a centralised one.

Finally, there are a number of commercial companies that either have or are planning to release mobile payment solutions. For example, in addition to offerings in Japan and South Korea [32] (by service providers), Obopay Inc. [28] and Paypal [29] have already deployed mobile payment solutions with Google about to offer an additional solution (Gpay [33]). Kreyer et al [19] list several other commercial ventures. However, all these competing solutions use SMS or GPRS (requiring infrastructure) as their message protocol and do not support p2p communications. The work closest to mFerio is the mNETS [4] mobile payment system. However, even this NFC-based system does not support p2p transfers.

9. CONCLUSION AND FUTURE WORK

In this paper, we presented the design and evaluation of mFerio, a NFC-enabled mobile p2p payment system. mFerio's design was informed by analysing the key tradeoffs between usability, utility, and security – fundamental to any mobile p2p payment system.

Our analysis led us to a set of requirements for usability, security, and auditing. We then iterated our design several times to minimise the number of steps involved, while providing a strong level of security from the end-user's perspective. Finally, the results of a two-phase user study conducted with a total of 104 participants showed that mFerio is highly usable and is even faster than cash under various common scenarios. mFerio also showed lower cognitive loads than cash in a majority of cases.

The current mFerio prototype is part of a longer term project that aims to create a digital wallet-type architecture for cellphones. This digital wallet will allow users to store everything currently in their physical wallets (cash, identification, credit cards, receipts, etc.) inside their cellphones. We are already developing different aspects of a digital wallet, in parallel, and plan to work with various vendors to overcome some of the real-world challenges of deploying a digital wallet solution, such as getting mass market appeal.

In the near future, we plan to deploy a full version of mFerio in a real environment using a larger and more varied population pool. We also plan to test a variety of usable authentication schemes that can be employed on mFerio.

10. ACKNOWLEDGEMENTS

The authors would like to thank Bhatt Dev S/O Digantrai, Vidit Drolia, Anand Sujith Henry, Xiao Sa, Sridhar Venkataraman, and Dexter Huang Yaolin for their help in building the initial mFerio prototypes and for their help in conducting the phase 1 user studies.

11. REFERENCES

[1] Acquisti, A., Christin, N., Parno, B., and Perrig, A. Countermeasures against government-scale monetary forgery. *Proceedings of the Twelfth International Conference on Financial Cryptography and Data Security (FC'08)*, pages 262–266, Cozumel, Mexico, Jan. 2008.

[2] Adams, A. and Sasse, M. A. Users are not the enemy. *Commun. ACM*, 42(12):40–46, 1999.

[3] Brands, S. A. An efficient off-line electronic cash system based on the representation problem. Technical Report CS-R9323, CWI (Centre for Mathematics and Computer Science), Amsterdam, Netherlands, 1993.

[4] Chan, J. *Wallet Replacing Phones – Eventually*. CNET Asia. http://asia.cnet.com/crave/2007/09/04/wallet-replacing-phones-eventually/, Sept. 2007.

[5] Chaum, D. Blind signatures for untraceable payments. *Proceedings of the International Crytology Conference (CRYPTO)*, Santa Barbara, CA, Aug. 1982.

[6] Chaum, D. and Brands, S. Minting electronic cash. *IEEE Spectrum*, 34(2):30–34, Feb 1997.

[7] Chaum, D., Fiat, A., and Naor, M. Untraceable electronic cash. *Proceedings of 8th Annual International Cryptology Conference (CRYPTO)*, Santa Barbara, CA, Aug. 1989.

[8] Chen, J. J. and Adams, C. Short-range wireless technologies with mobile payments systems. *ICEC '04: Proceedings of the 6th international conference on Electronic commerce*, pages 649–656, New York, NY, USA, 2004. ACM Press.

[9] Davies, G. *A History of money from ancient times to the present day*. University of Wales Press, Cardiff, UK, 2002. 3rd Edition.

[10] Ecma International. *Standard ECMA-340: Near Field Communication Interface and Protocol (NFCIP-1)*. http://www.ecma-international.org/publications/standards/Ecma-340.htm, Dec. 2004. 2nd Edition.

[11] Even, S., Goldreich, O., and Yacobi, Y. Electronic wallet. *Proceedings of CRYPTO'83*, pages 383–386, Santa Barbara, CA, Aug. 1983.

[12] EZ-Link Pte. Ltd. *EZ-Link Contactless Payment Card*, Mar. 2009. http://www.ezlink.com.sg.

[13] Gheringer, E. F. Choosing passwords: security and human factors. *ISTAS'02: Proceedings of International Symposium on Technology and Society*, pages 369–373, June 2002.

[14] Hart, S. G. NASA-task load index (NASA-TLX); 20 years later. *Proceedings of the 50th Annual Meeting of the Human Factors and Ergonomics Society (HFES)*, San Francisco, CA, Oct. 2006.

[15] Hayashi, E., Christin, N., Dhamija, R., and Perrig, A. Use your illusion: Secure authentication usable anywhere. *Proceedings of the Fourth Symposium on Usable Privacy and Security (SOUPS'08)*, Pittsburgh, PA, July 2008.

[16] Herzberg, A. Payments and banking with mobile personal devices. *Commun. ACM*, 46(5):53–58, 2003.

[17] Horn, G. and Preneel, B. Authentication and payment in future mobile systems. *Journal of Computer Security*, 8(2–3):183–207, Aug 2000.

[18] Kelly, J.F. An iterative design methodology for user-friendly natural language office information applications. *ACM Transactions on Office Information Systems*, 2(1), March 1984.

[19] Kreyer, N., Pousttchi, K., and Turowski, K. Characteristics of mobile payment procedures. *Proceedings of the International Syposium on Methodologies for Intelligent Systems (ISMIS)*, Lyon, France, June 2002.

[20] Kreyer, N., Pousttchi, K., and Turowski, K. Standardized payment procedures as key enabling factor for mobile commerce. *Proceedings of the Third International Conference on E-Commerce and Web Technologies (EC-Web)*, Prague, Czech Republic, Sept. 2002.

[21] Kügler, D. On the anonymity of banknotes. *Proceedings of the 4th International Workshop on Privacy Enhancing Technologies (PET'04)*, pages 108–120, Toronto, Canada, May 2004.

[22] Kungpisdan, S., Srinivasan, S., and Le, B. P. D. A secure account-based mobile payment protocol. *Proceedings of International Conference on Information Technology: Coding and Computing*, Las Vegas, NV, Apr. 2004.

[23] Lee, K. J., Ju, J.-I., and Jeong, J. M. A payment & receipt business model in u-commerce environment. *ICEC '06: Proceedings of the 8th international conference on Electronic commerce*, pages 319–324, New York, NY, USA, 2006. ACM Press.

[24] Lukkari, J., Korhonen, J., and Ojala, T. Smartrestaurant: mobile payments in context-aware environment. *ICEC '04: Proceedings of the 6th international conference on Electronic commerce*, pages 575–582, New York, NY, USA, 2004. ACM Press.

[25] MasterCard Worldwide Suite. *Mondex*. http://www.mondex.com, Apr. 2008.

[26] Micali, S. and Rivest, R. L. Micropayments revisited. *Proceedings of the The Cryptographer's Track at the RSA Conference on Topics in Cryptology*, San Jose, CA, Feb. 2002.

[27] Network For Electronic Transfers (Singapore) Pte Ltd. *NETS CashCard Contactless Payment Card*, Mar. 2009. http://www.nets.com.sg/consumers/netscashcard/index.php.

[28] Obopay Incoporated. http://www.obopay.com, Sept. 2007.

[29] Paypal Incorporated. *Paypal Mobile Services Overview*, Sept. 2007. https://www.paypal.com/?cmd=xpt/cps/mobile/MobileOverview-outside.

[30] Pering, T., Anokwa, Y., and Want, R. Gesture connect: facilitating tangible interaction with a flick of the wrist. *TEI '07: Proceedings of the 1st international conference on Tangible and embedded interaction*, pages 259–262, New York, NY, USA, 2007. ACM Press.

[31] Pousttchi, K. Conditions for acceptance and usage of mobile payment procedures. *Proceedings of the Second International Conference on Mobile Business*, Vienna, Austria, June 2003.

[32] Rebbeck, T. *South Korea and Japan show the way on mobile payments and banking*. Analysys Research, Apr. 2006. http://research.analysys.com/articles/standardarticle.asp?iLeftArticle=2100.

[33] Riley, D. *Could Gpay be Google's Killer App?* TechCrunch. http://www.techcrunch.com/2007/09/02/could-gpay-be-googles-killer-phone-app/, Sept. 2007.

[34] Toledano, D. T., Pozo, R. F., Álvaro Hernández Trapote, and Gómez, L. H. Usability evaluation of multi-modal biometric verification systems. *Interacting with Computers*, 18(5):1101–1122, Sept. 2006.

[35] Václav Matyás, J. and Ríha, Z. Biometric authentication - security and usability. *Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security*, Portoroz, Slovenia, Sept. 2002.

[36] Varshney, U. Mobile payments. *IEEE Computer*, 35(12):120–121, Dec 2002.

[37] VISA. *payWave*. http://www.visapaywave.co.uk, Apr. 2008.

[38] Want, R., Fishkin, K. P., Gujar, A., and Harrison, B. L. Bridging physical and virtual worlds with electronic tags. *CHI '99: Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 370–377, New York, NY, USA, 1999. ACM Press.

[39] Wayner, P. *Digital Cash: Commerce on the Net*. Academic Press, San Diego, CA, Mar 1997. 2 Sub Edition.

[40] Wrona, K., Schuba, M., and Zavagli, G. Mobile payments - state of the art and open problems. *Proceedings of the Second International Workshop on Electronic Commerce*, Heidelberg, Germany, Nov. 2001.

[41] Zmijewska, A. Evaluating wireless technologies in mobile payments " a customer centric approach. *ICMB '05: Proceedings of the International Conference on Mobile Business (ICMB'05)*, pages 354–362, Washington, DC, USA, 2005. IEEE Computer Society.