# Security and Trust in Mobile Interactions: A Study of Users' Perceptions and Reasoning[1]

Tim Kindberg, Abigail Sellen, Erik Geelhoed
Consumer Applications and Systems Laboratory
HP Laboratories Bristol

HPL-2004-113
July 7, 2004*

E-mail: firstname.lastname@hp.com

This paper describes an investigation into the trust and security concerns of users who carry out interactions in ubiquitous and mobile computing environments. The study involved demonstrating an "electronic wallet" to pay for a meal in a simulated restaurant, and analyzing subjects' responses based on structured interviews. We asked the users to rank-order five payment methods including three choices for the payment target, and both wired and wireless connections. The analysis led us to classify the users into trust-, social- and convenience-oriented clusters. We provide a detailed analysis of the users' reasoning about trust-related issues, and draw conclusions about the design of secure interaction technologies for ubiquitous computing.

* Internal Accession Date Only

[1] UBICOMP 2004, Nottingham, UK, September 2004

Approved for External Publication

# Security and Trust in Mobile Interactions: A Study of Users' Perceptions and Reasoning

Tim Kindberg, Abigail Sellen and Erik Geelhoed
Hewlett-Packard Laboratories, Bristol BS34 8QZ, UK
{ tim.kindberg, abigail.sellen@hp.com, erik.geelhoed }@hp.com

**Abstract.** This paper describes an investigation into the trust and security concerns of users who carry out interactions in ubiquitous and mobile computing environments. The study involved demonstrating an "electronic wallet" to pay for a meal in a simulated restaurant, and analyzing subjects' responses based on structured interviews. We asked the users to rank-order five payment methods including three choices for the payment target, and both wired and wireless connections. The analysis led us to classify the users into trust-, social- and convenience-oriented clusters. We provide a detailed analysis of the users' reasoning about trust-related issues, and draw conclusions about the design of secure interaction technologies for ubiquitous computing.

## 1 Introduction

It is envisioned that, in the future, people will be able to spontaneously make their personal, mobile devices interact with other devices in a range of different environments, both public and private, many of which may be new and unfamiliar [4]. For example, in restaurants and other semi-public places, customers may be able to use mobile devices and services to carry out electronic transactions where they may have never visited before. For example, one view of the future is that people will carry a device that acts essentially as an "electronic wallet" (or "e-wallet"). The e-wallet can interact with some other device in a restaurant that accepts payment for a meal. Although the devices have never been associated before, it should be possible for users to make their payments with little time and effort. Moreover, users should be satisfied that they are exchanging payment reasonably securely, given what they regard as the trustworthiness or untrustworthiness of the devices and people in the environment.

The potential security threats in such environments are well known from a technical standpoint, and various ideas have been put forward (e.g. [1,5]) for securing interactions between devices. But that work begs several questions about how users perceive and reason about such systems: First, to what extent does concern about security really determine the desirability or usability of such systems? Second, if they are concerned, what are the particular points of vulnerability they perceive as most salient in such an environment, and how do they reason about the threats they present? Third, to what extent are the answers to the foregoing questions a function of the configuration of the target device and the method of connection between the devices (for example, whether or not such a connection is wireless)?

We report on a study aimed at exploring the ways in which people reason about such systems, with a particular focus on the extent to which concerns about security impact their perception. Eventually, by understanding people's reasoning processes, we hope to be able to design systems that are not only *technically* more trustworthy and secure, but which users *perceive* to be more trustworthy and secure. The contribution in this first step is to describe the types of perceptions and reasoning found in our subject group and to draw implications for further research from these observations.

## 2 Related Research

The word ‘trust’ features in several well-known senses in the technical security literature, but typically where designers and implementers of secure systems refer to legal entities or system components rather than users. A ‘trusted third party’ is one upon which each of a set of principals depends to make reliable assertions about the others. A ‘trusted computing base’ is a collection of hardware, software and other types of component whose failure could cause a breach of a security policy. A ‘trusted computing platform’, by contrast, is one that is more trustworthy than simply trusted, in that certain types of tampering and disclosure of information are impossible by construction. None of those definitions relate necessarily to trust on the part of users, with consequent questions about the usability and acceptability of systems designed without attention to users’ perceptions.

The increasing amount of research on constructing and designing secure *ubiquitous* systems has been encountering difficulties with the standard notions of trust and trustworthiness, even from a technical point of view. The difficulties arise because of the volatile nature of ubiquitous systems [4], which means that the ‘trusted computing base’ cannot be straightforwardly identified; and typically no trusted third parties exist. Cahill et al [2] describe a system for dynamically assessing risk and trustworthiness based on various types of evidence, some of which is assumed to be gathered from previous experience.

Other work [1,5, 9] has focused on spontaneous situations such as the restaurant we described, where little if anything may be known *a priori* about the other parties in the interaction, let alone their former behaviour. That work assumes that users nonetheless make dynamic decisions about the trustworthiness of other users and devices, and it enables them to construct secure communication channels to devices in the control of trusted users. It does so with, it is asserted, little overhead despite the lack of *a priori* data. Those designs beg questions about when, where, and in what users will in fact place their trust. Moreover, while the techniques to achieve secure communication have desirable technical properties, it is not known how trustworthy users will perceive them to be; or how the techniques – involving considerable human attention – play within the user’s social circumstances and other considerations.

There is little help with regard to these issues in the social science literature. The considerable literature stemming from psychology and sociology, for example, makes little or no connection with technology. Work that does explore users’ perceptions of trust in relation to technology, such as research within Human-Computer Interaction, tends to focus on the internet, and people’s willingness and concerns about using Web-related services mainly for internet banking or shopping. As such, most of the work has focused on aspects such as users’ previous experience or familiarity with a particular site or vendor, various aspects of the design and layout of a Website, the quality of the content on a site, and the way in which technical aspects of a site or a network manifest themselves (such as speed of connection, feedback, reliability and so on) e.g. [3, 6] and see [8] for an overview. Recently, the topic of mobile e-commerce and users’ perceptions of trust in this context has begun to emerge in the literature. Unfortunately, such studies seek to carry over to the mobile context lessons about trust by appealing to research on the use of the internet e.g. [7,11]. There is little or no investigation of how mobile e-commerce transactions may be different, including the physical configurations of mobile devices, the fact that wireless connections are made, or the fact that there may be no history or experience of use built up in such circumstances. The study we report here, therefore, begins to explore this new territory both from a user’s perspective, and with an eye to what this means for the design of new ubiquitous computing technologies.

## 3 Method

In all, 24 subjects were recruited from a variety of non-technical people inside and (to a small extent) outside HP, with a roughly equal mix of the sexes (11 men and 13 women), ranging in age from 16 to about 60. By “non-technical” we mean that we deliberately selected people whose job roles did not involve building, designing, or programming computer systems technology. While all subjects used computers at work and occasionally at home, their jobs ranged from administration, to legal work, to architectural practice.

### 3.1 Scenario and Set-Up

In choosing the concept of an “e-wallet” and the example of visiting and paying for a restaurant meal with it, we were selecting a scenario which we thought would have many familiar elements, but which also might trigger thoughts and concerns about security issues without the need for prompting.

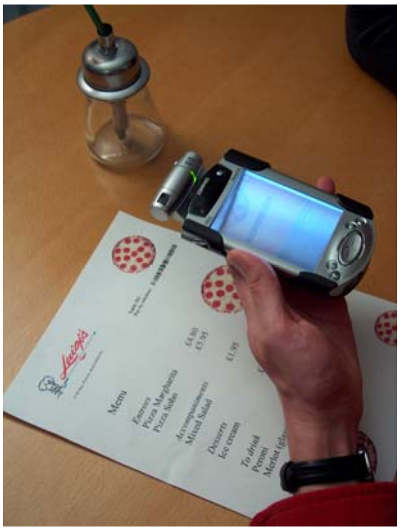

**Fig. 1.** Paying by barcode at “Luigi’s”.

Each subject was invited to our laboratory in which we set-up “Luigi’s”: a reasonably restaurant-like environment consisting of an area with tables, crockery and pictures on the wall. Each subject was then told that we wanted to introduce them to the notion of an “e-wallet” and to demonstrate several different ways in which they might use their e-wallet to pay for their meal in a restaurant situation. Since we were interested in the extent to which they might spontaneously raise issues about trust and security (as opposed to being prompted), we begin by stating that our investigation was into their reactions to the different payment methods, and to comment on which things they liked and disliked about each. An e-wallet was described as a device that provides an alternative to cash and credit/debit cards; our only mention of security was to say that the prototype e-wallet (an adapted iPAQ) would have a means of authentication such as PIN entry or thumbprint-detection that we had not yet implemented. They were also informed that the prototype e-wallet was bigger than an actual e-wallet should be. Otherwise, it and the other devices to be demonstrated operated realistically, but without exchanging actual funds.

### 3.2 Payment Methods

Five different payment methods were demonstrated involving variations in (1) whether the connection to the payment-accepting device was wireless or wired (docked with an iPAQ cradle visibly connected to the target device); and (2) whether the target that accepted their payment was either (a) a device that the waiter carried (another iPAQ), (b) an unstaffed “payment kiosk” somewhere in the restaurant (a monitor on a table by the wall with a visible connection to a machine below), or (c) a service accessed by using the e-wallet to read a “pay by wireless” barcode printed on the menu at their table (Fig. 1). These five configurations were chosen so that we could vary both the type of connection, and the nature of the target with respect to the presence and visibility of both the device itself and a human who (apparently) has control over it. Thus, the resulting five configurations consisted of:

- two kiosk systems (kiosk/docked or kiosk/wireless);
- two conditions in which a waiter carried a handheld device (waiter/docked or waiter/wireless); and
- the barcode condition (wireless, of course).

In the wireless configurations, payment involved choosing the Luigi’s payment service from a randomly-ordered list of local services that the e-wallet “discovers”, including services apparently from adjacent places. In contrast, when the e-wallet was docked or when the barcode was read, the Luigi's payment service appeared directly on the e-wallet. The service first presented a list of unpaid table numbers, from which the (anonymous) user selected their own to see their bill. On affirming and confirming payment of their bill, the e-wallet presented a "receipt" page. The kiosk presented minimal, anonymous feedback during the payment process. The menu and all pages on the kiosk and e-wallet from the payment service bore Luigi's logo.

### 3.3 Interview

After these five different payment methods were demonstrated (in counterbalanced order across subjects), we carried out a structured interview and questionnaire as follows:

- ❑ **Ranking exercise.** Part 1 of the interview consisted of a ranking exercise in which each subject was presented with five different photographs illustrating the different payment methods. They were then asked to rank-order these five methods in order of general preference using the photographs as reminders. We then asked each subject to explain the basis for their ranking, asking for as much detail as possible about their reasons. No mention or prompting of security issues was made during this part of the interview.
- ❑ **Focussed questions.** Part 2 consisted of four more specific questions asking subjects to compare and contrast: an electronic wallet with a "normal" wallet, docked connections with wireless connections, interacting with a device in the waiter's hand versus a kiosk, and using the barcode method (where there is no obvious device receiving payment) with other methods in which there was a physical receiving device (kiosk or waiter's handheld device). Subjects were prompted to consider security issues only if they did not mention any. These prompts were open and general; no specific issues were raised by us.
- ❑ **Questionnaire.** Part 3 consisted of a questionnaire in which 12 potential security issues in non-technical language (see Table 1) were read out such as "My e-wallet might send my data or money to the wrong person or device." For each of these issues, subjects were asked to fill out a series of rating scales indicating their degree of concern. For ten of the issues there were separate rating scales for each of the five payment methods.
- ❑ **Final ranking and questions.** In the fourth and final part, we asked each subject whether or not they wished to change their ranking (in light of our discussion of security issues) and if so, to explain why.

### 3.5 Data Analysis

The data analysis consisted of statistical analysis of the rating scales in Part 3 (using SPSS), plus qualitative analysis and coding of subjects' comments and rationale throughout. In the case of the rating scales, scores were calculated by measuring where on a 50 mm line each subject had freely made a mark indicating their level of concern, to a 1 mm accuracy [10].

For Part 1, both positive and negative points subjects mentioned for each of the five payment methods were documented in a table. In Part 2, preferences and points of contrast were noted for each of the four issues, again in a table, both before and after prompting about security. For Part 4, whether or not there had been a change in ranking and, if so, the reasons why were documented. Throughout, interesting or representative quotations were transcribed for each subject.

In the process of documenting the issues and comments, it became clear that there were very different kinds of comments that arose when people described their rationale about the five payment methods. In order to abstract from the data, each of these comments or issues was coded as belonging to one of three categories:

- ❑ Trust-oriented: These were issues or comments that related to concerns about the risk associated with using a system either because of malicious intent on the part of another person or persons, or because of failure or unreliability of some part of the system. Such comments usually expressed either uncertainty or anxiety.
- ❑ Convenience-oriented: These were issues that had to do with the ease with which a system could be used, its convenience (or lack thereof), or how its design affected the usability of the system.
- ❑ Socially-oriented: These were issues that related to the social interaction with others such as the waiter, the accountability of one's actions to others in a restaurant, social protocols, and the value of human interaction.

The few comments that did not fall into the above categories were left uncoded.

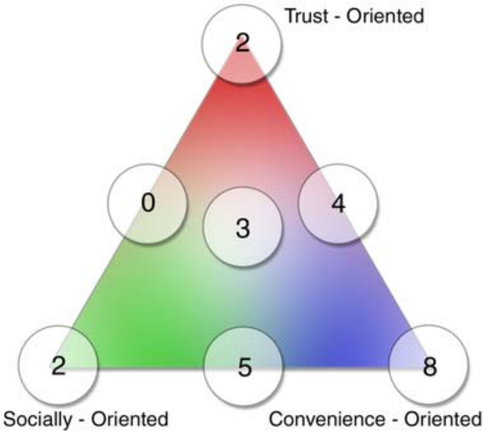

**Fig. 2.** Numbers of subjects in clusters.

## 4 Results and Discussion

We will begin by describing how subjects ranked the five different payment methods, and the different types of rationale that subjects used to explain their ranking. As we shall see, sometimes trust issues played a role in these rationales, and sometimes they did not. We will then go on to describe the trust issues that arose for different subjects, and the degree to which subjects seemed aware of these potential issues. The relationship between awareness and rationale will then be discussed.

After that, we will look more closely at how subjects reasoned about trust and security, and the range of factors that impacted subjects' perception of different kinds of mobile systems.

### 4.1 Subjects' Ranking and Rationale

Part 1 of the interview, in which subjects were asked to rank-order the five payment methods and explain their rationale for doing so, gave us a number of insights into the ways in which people perceive, reason about and envision their use of technology. For example, it was clear that, purely on the basis of this first part of the interview, across the 24 subjects, there were very different kinds of rationale that people were using to justify their preferences amongst the five methods. For the most part, such rationales were not heavily based on trust and security issues: almost 2/3 (15) of the subjects gave explanations in which trust and security played no identifiable role at all.

To clarify and characterize the kinds of reasoning processes people *did* use, we looked for a way of meaningfully clustering the 24 subjects. To do this, we began by studying the coded reasons given for each ranking. In drawing on these three classes of explanation, each subject could be seen to be using some combination of these dimensions to explain their choices. As such, we found that they could be broadly placed within a triangular landscape in which each of the vertices represented a rationale entirely based on reasons belonging to that category (see Fig 2). This allowed us to see at a glance clusters of subjects with common kinds of rationale, as well as the ways in which those rationales diverged from others. For example, if a subject gave reasons that were entirely convenience-oriented, that subject was placed in the lower right vertex of the triangle. If the reasons were entirely socially-oriented or trust-oriented, they were placed in the corresponding vertices. Likewise, rationales which contained a mix of issues were placed in the appropriate place in the triangle.

Looking at each cluster in turn gives us insights into the relationship between a subject's rationale and their ranking. It further shows how subjects in the same cluster can sometimes end up with rankings similar to others in the same cluster, and sometimes can use the same *class* of explanation to arrive at a different set of preferences. Let us examine these more closely:

**Convenience–oriented:** One third of all subjects gave entirely convenience-related reasons for their rankings. Of these eight people, six of them ranked the two waiter conditions lowest because having to call the waiter over was very much seen as detracting from the ease and convenience with which one could pay one's bill. In addition, the step of having to physically dock with the waiter's device was an extra negative factor resulting in the waiter/dock condition finding its place at the bottom of the ranking for seven of these eight subjects.

In terms of positive comments, the barcode condition was the overall favourite for six of the eight people, mainly because it was seen to be about being more "in control" of the process: not having to call a waiter and not having to get up from the table. The kiosk/wireless condition generally was ranked as the next favourite, again for reasons of not being dependent on anyone else to pay, plus the added possibility of being able to connect from one's table. Two people in this cluster, however, were more strongly "pro-wireless" in ranking both the wireless connection with a kiosk as well as a wireless connection with a waiter as amongst their top three configurations. Both of these subjects believed that they would be able to wirelessly connect with the waiter without necessarily getting them to come over to the table. Finally, the kiosk with dock generally was somewhere in the middle of the ranking: on the positive side, not having the waiter involved was seen to speed up the process, but on the negative side, the need to dock raised the possibility of queues, especially in busy times in the restaurant.

**Socially-oriented:** Only two subjects gave entirely socially-oriented rationales for their ranking. The reasons they gave all related to social interaction and the ways in which different methods of payment supported or interfered with ongoing social protocol within the restaurant setting. Both of these people could be called "waiter-friendly" in that, in contrast to the convenience-oriented people who viewed waiter involvement as negative, interaction with the waiter was seen as a valuable aspect of the experience of being in a restaurant. Both ranked the two waiter conditions as their top preferences, with the docked interaction rated as better than the wireless one. Interaction with the waiter was seen not only as a positive social experience, but someone with whom one could talk in case of problems, to let them know they enjoyed the meal, and so on.

With regard to the two kiosk conditions and the barcode condition, the main issue was how they would affect how one would be viewed by others. In other words, the concern here was one's accountability to others in terms of being seen to have paid, and being seen to be valuing the interaction with others. One of the subjects viewed interacting with a kiosk (and especially docking with it) as removing oneself more and more from the social situation. These methods were the least preferred conditions. For the other, paying by barcode was the least preferred condition because, she reasoned, it would be less obvious to others in the restaurant that she was engaged in paying than if she was seen interacting (and especially docking) with a kiosk.

**Trust-oriented:** Only two subjects were entirely oriented to trust and security issues as the basis for their ranking. Interestingly, both gave different sets of trust-oriented reasons resulting in different rankings.

One subject based her ranking on a mistrust of both wireless connections and involvement of the waiter. Mistrust of wireless connections appeared to come from a lack of experience with this type of connection, the idea that the information might go somewhere she wouldn't know about, or that something might come "in between" her device and the receiving device. Mistrust of the waiter revolved around fears that someone might impersonate the waiter, or that the waiter might be inherently untrustworthy. For these reasons, this person ranked the kiosk/dock condition as favourite, followed by the barcode condition. The waiter/dock was ranked third, followed by kiosk/wireless, with waiter/wireless the least preferred.

The other subject's rationale appeared to be based entirely on a mistrust of other people, whether that meant the waiter or other people in the restaurant. For this reason, the barcode condition was the favourite in that people were taken entirely out of the loop. The waiter conditions were ranked next on the basis that even if the waiter was untrustworthy, at least one could identify the person with whom one was dealing. Finally, the kiosk conditions were ranked last because other people in the restaurant might be able to see the screen and therefore (he thought) view private information.

**Mixed rationales:** For the remaining 12 subjects, their rationales and resultant rankings could be seen to be some mixture of concerns spanning two or even three of the themes of trust, social or convenience. In these mixed rationales, the strength of one kind of factor over any other was idiosyncratic. For example, within the cluster of people who gave trust and convenience-oriented rationales for their rankings, for some subjects it was clear that convenience factors were more important, and others that trust issues were more important. Likewise, those people using all three classes of explanation each derived their own patterns of explanation and own resulting ranking.

### 4.2 Awareness and Trust

In the previous section we looked at the extent to which different subjects were *predisposed* to express and use trust and security issues as a basis on which to make choices about the five payment methods. That raises the question of whether this predisposition is related to a person's general level of awareness: it may be that the more awareness one has of potential risks, the more likely one uses that knowledge to reason about different systems.

We measured awareness of trust-related issues by counting the number of distinct points each subject raised throughout Parts 1, 2 and 4 of the interview. (We did not include the trust-related concerns we ourselves had raised in Part 3.) This analysis included both negative and positive comments made in relation to different points, since both were taken to indicate awareness of potential vulnerability or risk. Further, it included points that subjects spontaneously raised, as well as those that they made when we prompted them to comment on trust and security. Note that when we prompted them, it was by asking generally for "security and trustworthiness issues" in comparing payment methods, and not by mentioning specific issues. Thus it was up to the subjects to generate these issues themselves.

We identified 22 different kinds of trust-related points overall. Individuals mentioned as few as one and as many as nine different ones throughout the course of the interview, with a mean across subjects of 4.8. The points that the subjects raised, together with the number of subjects who mentioned them, are discussed in more detail in the next section (Section 4.3). However, in Figure 3, we show a breakdown of their mean frequency organized by subject and cluster. Because the clustering depended on issues raised in Part 1 (including trust-related ones) we separate out the number raised in total (including Part 1) from the number of distinct points raised in the rest of the interview (shown in brackets).

Because of the small sample sizes for some of the clusters, statistical difference tests would be inappropriate. However, the means do indicate some interesting relationships between a subject's orientation or predisposition, and awareness of trust issues. Figure 3 shows, first, that the difference between the two means (total points minus additional points) for each cluster increases as we move away from the social-convenience axis towards the trust-oriented vertex. While we would expect no difference in means along the social-convenience axis (because no trust-related points are raised in Part 1), it is interesting that people who do raise trust-related points in the initial ranking exercise continue to do so throughout the rest of the interview. Another way of putting this is that such people not only appear to have an initial predisposition to think of trust-related issues, but will find more given more opportunity to do so.

A second perhaps more important point is that subjects who are convenience-oriented show themselves to be, on average, nonetheless quite highly aware of trust-related issues. For example, if we look at the mean number of trust-related points raised after the initial ranking exercise (when discussion of trust and security was prompted), the convenience-oriented people raised as many points on average as the trust-oriented people. In other words, it appears that subjects who used a convenience-oriented rationale were in fact quite aware of potential security risks, but chose not to take into account such issues in their ranking. By contrast, the two socially-oriented subjects started out their interviews without raising such issues and continued to demonstrate very little awareness of points of vulnerability throughout, even when prompted.

So far, then, the data suggest that there is no simple relationship between a predisposition to using trust issues as a rationale, and awareness of those issues. Another way of exploring this relationship is to ask whether deliberately raising subjects' awareness of potential issues might cause people to alter or rethink their original choices. Here, we can look at the final section of the questionnaire. At this point, we had prompted discussion on a number of trust and security topics, and had asked subjects to consider 12 potential security issues in detail. Subjects were then asked whether they wanted to change their general preferences for the 5 methods we had presented them with.

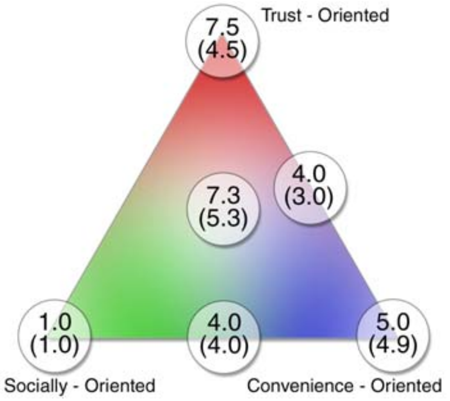

**Fig. 3.** "Awareness scores". By cluster, the mean number of trust-related points across subjects in the whole interview; and (in brackets) the mean number of additional points raised after the ranking exercise in Part 1.

In all, only seven of the 24 subjects said that, when all was said and done, they would change their rankings. Interestingly, however, only four of these people expressed reasons to do with increased awareness or concern about security issues. The remaining three people who changed their rankings did so because they had changed their opinions about which conditions would be the most efficient and convenient.

### 4.3 Reasoning About Trust-related Issues

In this section we examine the subjects' reasoning about trust-related issues in more detail by looking both at the points the subjects themselves raised in the interviews, and then by examining the degree of concern they indicated for the issues we raised in the rating scale questionnaire. We then examine their reasoning when comparing technologies.

The 22 trust-related points that the subjects raised throughout the interview, grouped by category and ordered by the total frequency of occurrence, were as follows:

**Attacks on the E-Wallet:** The most frequent references were to attacks on the e-wallet, where subjects identified four vulnerabilities. Five felt the e-wallet was particularly attractive to thieves; four remarked on the total amount that might be lost if the e-wallet was acquired by a thief; fourteen referred to the relative protection of an e-wallet which, unlike a conventional wallet, presented a challenge to the user's authenticity; and three thought the e-wallet could be hacked over the network.

**Human Agent:** The subjects made a total of eighteen references to who might be a safeguard or attacker and, in some cases, where they would make an attack: a waiter either in or out of sight; another member of staff; another customer; or someone outside the restaurant.

**Attack on Communications Link:** The communication link scored next in the frequency of references, with a total of fourteen. Ten referred to insecurities of the wireless link, four explicitly to eavesdropping. Interestingly, two mentioned direct connection by dock as a point of vulnerability:

they thought malicious access to their e-wallet would be easier than with wireless. Two were generally concerned about whether communications were encrypted.

**Authenticity of Receiving Device:** Thirteen subjects referred to the authenticity or otherwise of the device their e-wallet communicated with (the “receiving device”). Some users referred to the possibility that their wireless communications might end up at a device that either presented itself spuriously by name as a device belonging to Luigi’s, or which they chose by mistake from the list of discovered devices. Others were concerned that, while they could identify the device they were communicating with, it itself might turn out to be untrustworthy – for example, the waiter’s own device could be used to steal payments.

**Attack on Device:** A total of eight references concerned the possibility that either the kiosk or the waiter’s device could be hacked into, by staff or by a third party.

**Doubt about Payment:** There were five trust-related references related to doubts about whether payment had been correctly made: it might not be taken at all; more might be taken than was warranted; the user might mistakenly pay the wrong bill.

**Context:** There were five references to security afforded by the context of the restaurant: two references to branding as a sign of authenticity, and three to what was “close” or “local” as being more trustworthy. E.g., one subject thought that wireless transmissions were trustworthy as long as they were local to the restaurant.

**Other:** Finally, two subjects thought that another customer might cheat and pay the subject’s cheaper bill; three were concerned about what happened to their payment or their personal information after they had apparently successfully paid the restaurant; one considered that any unfamiliar technology (such as those we demonstrated) was not deserving of his trust; and a sixth thought that people might exploit the feedback from his transaction on the kiosk (even though it was anonymous).

When we compare the points of vulnerability that the subjects generated themselves with the twelve potential trust issues we raised in Part 3 of the interview, (on the basis of our technical knowledge of attacks and failures), it is interesting to note that the subjects collectively showed some awareness of almost all of our issues. (See Table 1 for a list of these issues.) Only one issue we had posed had no counterpart among the subjects’ points: no-one raised the possibility that, to paraphrase, “People could intercept and change my transmission”.

For the rest of the issues we asked about in Part 3, the degree of correspondence in ranking between the subjects’ ratings of concern and the awareness they showed is mixed – and thus, as the previous section suggests, “awareness” is not always to be equated with concern. In particular, there is good correspondence between the subjects’ most frequently mentioned point, about an “attacker (who) acquires and breaks into the e-wallet”, and the Part 3 issue rated topmost in degree of concern – to paraphrase, that “someone might get hold of my e-wallet and hack into it”. However, the second- and third-ranked Part 3 issue, that “the system might be unreliable and take the wrong payment” and that “someone could hack into my e-wallet while I carry it”, correspond with points ranked rather lower down in frequency of mention.

There are several points of awareness without counterpart in the Part 3 issues. Those issues deliberately do not mention the identity of the attacker; so there is no 1-1 correlation with the users’ points about which “human agent” might be a point of vulnerability or security. The dock as a point of insecurity, and the contextual issues of branding and locality, are interesting points that the subjects raised but which do not themselves have any bearing on *de facto* (from a technical point of view) security. The other uncorrelated points are either refinements of Part 3 or are too vague to correlate exactly (e.g. “wireless net is insecure”).

### Wireless versus docked connections

One of the key issues that subjects both spontaneously raised and were asked about was the difference between docked and wireless connections with regard to trust and security. When subjects were explicitly asked in the interview to tell us which they thought was more secure, eight of the subjects said they

**Table 1**. Potential security issues raised in part 3 of the interview, and results of significance tests comparing amount of concern for wireless (W) versus docked (D) conditions. The first two issues did not have separate rating scales for the W and D conditions.

| **Issue (paraphrased from questionnaire)** | **P values**[1] | **Result**[2] |
|---|---|---|
| I might lose my e-wallet, leaving it open to hackers if in the wrong hands. | N/A | N/A |
| People could wirelessly access my e-wallet even while I carry it. | N/A | N/A |
| People could eavesdrop on the connection. | p < .006 | W > D |
| People could intercept and change my transmission. | p < .007 | W > D |
| My e-wallet might send data or money to the wrong person or device. | p <.001 | W > D |
| Restaurant / service provider could capture info about me I don't want them to have. | n.s. | – |
| Receiving devices such as kiosks or handhelds might be subject to hackers. | n.s. | – |
| Other people could pretend to be me and access my bill. | p < .019 | W > D. |
| The system might be unreliable & take my payment incorrectly. | p <.028 | W > D. |
| I might not get clear or timely feedback. | p <.037 | W > D |
| I might make a mistake entering data into my e-wallet. | p < .019 | W > D |
| I would not have a receipt in a long-lasting form. | n.s. | – |

[1] Results of ANalysis Of VAriance (ANOVA). P values less than .05 are significant; "n.s." means not significant.

[2] "W>D" means significantly more concern for wireless than docked conditions.

thought docked connections were more secure, three people said wireless connections were more secure, and the remaining 13 people either had no opinion, or thought they were equal.

Of the people who felt a docked connection was more secure, for three of them, it was clear that the anxiety they felt about a wireless connection had to do with the fact that the wireless method meant they had to choose from a range of services, and that they, or the system might inadvertently choose the wrong service to pay. Two people felt that a docked connection protected them from possible malicious intervention of the signal by person or persons unknown. E.g.,

> "I feel safer docking it because you do connect with something so you know where you are and what you're doing but with wireless you never know if there's someone who can log in on it."

This latter quote also indicates the more general sense of unease about wireless. For the remaining three people, knowing where the information is going when the connection is not perceptible was a problem. E.g.,

> "Unless you physically walk up to the station and dock and have a look I wouldn't know where it's gone – it [the information] just disappears into oblivion."

Interestingly, however, three people expressed the opposite view when comparing docked versus wireless connections. One person could not tell us why, but simply said that it was her hunch wireless was more secure. Another reasoned that "it would be easier to take information off it if it was physically connected to another device." The third person was uncomfortable with the idea of physically handing over his e-wallet in order to dock it:

> "You don't really want to part with it, do you? You e-wallet is yours. You don't know what the other guy is doing."

It was clear that in this case, the potential risk here referred to the waiter having it within his control, and could do something nefarious when out of its owner's hands.

Finally, most people refused to commit themselves to a point of view in our discussions of docked versus wireless connections. For five of these, there were no comments made to the effect that they distinguished between the two types of connection on the basis of trust and security at all. For another three, the reason they made no distinction was that they commented to the effect that they trusted the technologists to ensure that all aspects of the system were secure. E.g.,

> "I'm willing to put my faith that people are doing enough to make these things as secure as possible."

The remaining people in this group (5) did indeed express a range of concerns about wireless connections being insecure or unreliable. Nonetheless, none of them was willing to state that they thought wireless connections would be less secure than docked ones.

It appears, then, that people do express more of an inherent mistrust of wireless versus physical connections when we look at the results of the interviews, but very few people were willing to commit to this view or clearly explain why they felt that way. By contrast, when we examine the results of the rating scales, the results were much more clear-cut. Here we found that for seven of these issues, the wireless conditions gave rise to significantly more concern than the docked conditions, as shown in Table 1. There were no statistical interactions here: this result did not depend on whether the conditions involved a waiter or a kiosk.

This analysis shows that once different potential security concerns are raised, people indicate more concern about wireless methods of payment than with docked methods. However, left to their own reasoning, they may overlook these concerns, have only vaguely formed rationales for a preference for physical over wireless connections, or indeed may rationalise in favour of wireless connections over docked ones.

**Kiosk versus handheld interactions**

We next turn to the issue of interacting with different kinds of physical receiving devices: a stationary kiosk in the restaurant versus a handheld device in the waiter's hand. Here again we have the subjects' comments in the interviews, including those they made when we asked them to compare interactions with a kiosk versus a handheld device; and we have the rating scale data in which subjects expressed their concern for 10 different issues as a function of method of payment.

Seven subjects said they thought a kiosk was more trustworthy and secure than interacting with a handheld device. All of these judgments were made on the basis that essentially machines are more trustworthy than people. If a device is portable, then people can take them and do things with bad intent. By contrast, a fixed device like a kiosk would not be subject to the same risks:

> "There isn't a person there, there's a machine. When you go to a hole in the wall, you think: a machine isn't going to do anything untoward to you. Machines are not programmed to do that, machines are just programmed to do a certain thing."

> "I prefer something stationary [the kiosk]. I feel it's more trustworthy than a handheld but I don't know why I feel that. Maybe because it's a large piece of machinery. You know that's stationary whereas an individual – something that's portable, you may wonder where that's going."

Only one person adopted the opposite point of view. In this subject's opinion, a handheld device is more secure precisely because it is in someone's hand. As he said:

> "It's a psychological thing. It's the fact that somebody's there so you're paying this person as opposed to something you don't know."

The majority of people, however, were unwilling to commit or make broad generalisations about whether one kind of receiving device would be less secure than another. Nine of this group expressed no opinion or recognized no difference with respect to interacting with a kiosk versus a handheld device in terms of trust and security. Two people said positive things about having a human in the loop, and thus seemed to lean toward trusting the handheld more as a receiving device, but were unwilling to commit on this point. The remaining five people expressed more mistrust in relation to the handheld device but this was also said to be a function not of the device itself, but on the trustworthiness of the waiter.

Looking at the rating scales, unlike the issue of docked versus wireless connections, there were, in general no statistical differences in level of concern between the two kiosk conditions and the two handheld device conditions. (Further, there were no interaction effects here. In other words, the differences between kiosk and handheld conditions did not depend on whether the connection was wireless or not.) One exception to this was in response to the issue of the "devices or network being unreliable". Here, we found that people expressed significantly more concern in the kiosk conditions than the handheld conditions: ANOVA (see Table 1) gave $p < .013$; no significant interaction.

### Barcode method versus other methods

In the barcode method the subjects were exposed to an aspect of ubiquitous computing rather than simply mobile computing: the users dealt with a physical token of the restaurant's payment service (a menu with a barcode) rather than any obvious device.

While the subjects tended to be decided about the barcode method in terms of convenience and social factors (many ranked it high because of its convenience, or low because it had poor social connotations), they were less clear about its trust-related properties. When asked whether they had a preference in terms of "security and trustworthiness" between the barcode and the other four methods, only five subjects felt able to express a definite preference: three thought the barcode method was more secure or trustworthy than the other methods, and two thought it less.

Two of those who thought the barcode method was more secure reasoned that this was because of the absence of anyone else involved. E.g.:

> "No-one else is there and it's all done in front of you."

No-one else is present during wireless access to the kiosk either, but the quote suggests an absence of remote vulnerabilities that two other subjects echoed E.g.:

> "I always feel if you're closer to something you're safer to do it."

However, another subject lowered the barcode method in his final ranking because it cut out the human; yet another wondered whether someone else might find it easier to leave without paying.

The third subject who preferred the barcode method did so because the branding of the menu – and the physicality of the menu – served to reassure him. This thinking seemed to be based on the idea of something's being visibly owned or controlled by the restaurant – which is similar to another's reference to the kiosk as an "electrical representative" of the restaurant.

Of the two subjects who thought the barcode method less trustworthy or secure than the others, one was concerned about not being able to identify the receiving device: "The unknown where the information is going to flow." The other realized that the branding of the menu was not in fact a guarantee of security:

> "Someone could put a different barcode on the table which could make the payment go somewhere else."

On the other hand, one subject thought barcodes reduced risk: "Reading the barcode means (it) won't connect to wrong service." Another put this more ambiguously:

> "I can't read barcodes but a machine can … so I'm going to put my trust into that machine."

In declaring trust, that second quote illustrates a sense of venturing into the unknown with the barcode method, which several other subjects echoed.

Turning to the rating scale data, perhaps the most remarkable result was that the concern ratings for the barcode method lay mid-way between the two docked methods and significantly below the two wireless methods for the two communications-related issues of eavesdropping and message interception. In other words, a method which in fact involves only wireless communication was rated as though it involved something with the distinctive protection of docked communication. This raises the question of whether, in some users' minds, they were "docking" with the menu in a sense – and hence the remarks quoted above that, for example, "it's all done in front of you."

## 5 Implications

These results raise several important implications for the design of technology for ubiquitous computing environments.

First, it shows that people bring to bear very different kinds of reasons when making judgments about technologies. Trust and security issues may play a role, but other kinds of issue may be equally or even more important, like ease of use and convenience, or social ones. These other kinds of issue may be deliberately traded off or discounted in making decisions and reasoning about technology. As we saw, people who oriented themselves toward convenience as a major determinant of their preferences actually showed themselves to be quite aware of potential risks when prompted. Furthermore, even after deliberately raising discussions about trust and security, most subjects still clung to their original decisions, indicating the extent to which these other kinds of factors may hold sway despite raising awareness of potential risks.

One important implication of all of this is that, when designing technology, features which may impact ease of use or which can be seen to enforce social protocols may be at least as important to "get right" as features that assure people about their trust and security. So, for example, in designing an e-wallet device, it may be as important to build in a way of signaling to others in a restaurant that a person has paid as to deliver feedback ensuring a transaction has taken place with the right device. In other words, enforcing the social protocol may be as important as reassuring the user about the security of their transaction. Designers and technologists need to take these larger issues on board, and they may well be faced with trade-offs in doing so.

Second, the subjects in our study revealed a range of concerns to do with potential vulnerability or risk in relation to the technologies we presented them with, and in the circumstances we described. People varied not only in the extent to which they seemed aware of different risks, but also in the extent to which they could articulate them. Interestingly, most of the perceived risks that subjects generated as a group did in fact reflect the set of real technical risks that might exist in such systems.

However, in fact there was only a loose mapping between the actual technical risks inherent in such systems and subjects' perception of them. More specifically, most of the people in our study could articulate only a handful of the potential risks these systems present, even when prompted. Often, if they did raise a concern, it may only have been vaguely articulated (e.g. "wireless is insecure"). In addition, some potential threats were either never mentioned, or only mentioned very infrequently, such as the risk of interception of a transmission, or of possible abuse of the customer's information. On the other hand, other kinds of risks were much more salient, such as the risk of an e-wallet being lost, stolen or broken into. The potential risks that human agents presented were also highly salient.

A design dilemma that stems from these findings is how to trade actual security against users' perceptions of trust-related issues. An obvious approach is to look at the issues people showed relatively high awareness of and concern about, such as the possibility of paying the wrong device or service, and to design techniques that not only provide actual security but which allay concerns that otherwise might be barriers to acceptance. Conversely, designers also need to look at the threats that the subjects showed little awareness of, and consider designing techniques that enable users to negotiate them securely but without inconvenience. For example, there was little awareness of how a "physical hyperlink" such as a barcoded menu may be inauthentic. Taken generally across ubiquitous environments, this could become a significant threat and there is a need to protect users from potential problems without detracting from the ease of access to the hyperlinked services.

Third, the results point to the ways in which different technology configurations can cause people to radically alter their perception and opinions of the risks inherent in a technology. Subjects in this study expressed much more mistrust about wireless connections than they did about physical ones. To some extent this had to do with unfamiliarity, but the overriding issue seemed to be that of tangibility and the reassurance of having things within one's sight and grasp. While subjects were not clearly able to articulate their specific concerns at first, when presented with the possibilities, the configurations that made use of wireless connections were cause for far greater concerns than those that did not.

Likewise, introducing the human element through the use of a handheld receiving device presented problems for many of the subjects. Human intervention introduced uncertainty into the system, which a kiosk did not. Such views also implied that subjects were more willing to be trusting of the technologists designing the system than the people who might use them. In addition, the fact that a person could take a device "out of sight" raised concerns that visible, stationary devices did not. This was also reflected in subjects' perception of the barcode configuration. Both removing the potentially untrustworthy human from the process, as well as having things "within sight" were seen as positive aspects. The implication here is that some factors, such as the visibility and tangibility of a system, and the role of human agents, need careful consideration in the design of these technologies from the standpoint of users' reasoning about trust and security. These findings are a first step toward understanding those factors.

## 6 Conclusion

We have presented the results of a study of users' perceptions of and reasoning about trust and security for five payment methods in a simulated restaurant. The study has highlighted the different ways in which trust, convenience and social factors figure in the users' rankings of the payment methods. It also showed how users' awareness of and concern about points of vulnerability varies, and how they reason about them. We noted variations in the users' responses between wireless and docked connections, and between the waiter's handheld device, a kiosk and a barcoded menu as the 'target' for payment. We drew several conclusions about the issues we face in designing systems for secure interaction in ubiquitous systems.

All of this must be considered as a first exploratory step. After all, users' reactions within a simulated environment may bear a tenuous relation to how people might actually act and reason in real situations. As a next step, we are considering how to carry over this study into a working public environment with greater realism in the threats it may present, and with more realistic potential costs for the user.

## References

1. Balfanz, D., Smetters, D.K., Stewart, P., and Wong, H.C. Talking to strangers: authentication in ad-hoc wireless networks. *Proc. Network and Distributed System Security Symposium*, February 2002.
2. Cahill, V., Gray, E., Seigneur, J.-M., Jensen, C.D., Chen, Y., Shand, B., Dimmock, N., Twigg, A., Bacon, J., English, C., Wagealla, W., Terzis, S., Nixon, P., di Marzo Serugendo, G., Bryce, C., Carbone, M., Krukow, K., and Nielsen, M. Using Trust for Secure Collaboration in Uncertain Environments, *IEEE Pervasive Computing*, Vol. 2(3), July-September 2003, pp.52-61.
3. Hoffman, D., Novak, T., and Peralta, M. Building consumer trust online. *Communications of the ACM,* Vol. 42(4), 1999, pp. 80-85.
4. Kindberg, T., and Fox, A. System Software for Ubiquitous Computing. *IEEE Pervasive Computing*, Vol. 1(1), 2002, 70-81.
5. Kindberg, T., and Zhang, K. Validating and Securing Spontaneous Associations between Wireless Devices. *Proc. 6th Information Security Conference (ISC'03),* October 2003.
6. Neilsen, J. *Designing Web Usability*, 1999, New Riders.
7. Siau, K. and Shen, Z. Building customer trust in mobile commerce. *Communications of the ACM,* Vol. 46(4), 2003, pp. 91-94.
8. Siau, K., Sheng, H. and Nah, F. Development of a framework for trust in mobile commerce. *Proceedings of the Second Annual Workshop on HCI Research in MIS*, Seattle, WA, 2003, pp 85-89.
9. Stajano, F., and Anderson, R. The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks. In B. Christianson, B. Crispo and M. Roe (Eds.) *Proc. 7th International Workshop on Security Protocols*, LNCS, Springer-Verlag, 1999.

10. Stone, H., Sidel, J., Oliver, S., Woolsey, A. and Singleton, R.C. Sensory Evaluation by Quantitative Descriptive Analysis, *Food Technology*, Nov 1974, pp. 24-34.

11. Ventakesh, V. Ramesh, V., and Massey, A. P. Understanding usability in mobile commerce. *Communications of the ACM*, Vol. 46(12), 2003, pp. 53-56.