

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

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

Introduction

This paper describes an ongoing investigation into the trust and security concerns of users who carry out interactions in mobile and ubiquitous computing environments. The study is motivated by future scenarios in which it is envisioned that people may be able to spontaneously make their personal, mobile devices interact with other devices in such environments—environments which may be relatively unfamiliar [1]. For example, consider a user who has finished her meal in Luigi's restaurant (which she has never visited before), and who now wishes to pay using the "electronic wallet" ("e-wallet") she carries with her. This involves an interaction between her e-wallet and some other device in the restaurant that accepts her payment. The devices have never been associated before; however, it should be possible for the user to make the payment spontaneously—that is, when the conditions are right for her. To provide an acceptable experience for the user, it should take little time and effort to associate the devices and pay. Moreover, the user should be satisfied that she is exchanging payment reasonably securely, given what she regards 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. [2,3]) for securing interactions between the user's device and any device in the environment that she trusts. But that work begs several questions about how users perceive and reason about such systems: First, what, in fact, do users trust and distrust in relatively unfamiliar circumstances such as Luigi's restaurant – and why? Second, what are the points of vulnerability that they perceive 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?

We undertook a study of users in a simulation of Luigi's restaurant in order to begin to answer these questions. We are now analysing the data, the results to be available by May. In the meantime, we describe the experimental method and analytical approach below.

Method

For the study, 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, and ages ranging from 16 to about 60. Each subject was invited to our laboratory in which we set-up 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 e-wallet 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. For example, when we showed how a user would pay wirelessly, the e-wallet first showed a realistic set of about ten services discovered in the wireless subnet from which the user must choose; those included services next door to Luigi's and services offered by customers' mobile phones, as well as services offered by Luigi's.

Five different payment methods were demonstrated involving variations in (1) whether the connection to the payment-accepting device was wireless or wired (docked); and (2) whether the target that accepted their payment was either (a) a device that the waiter carried, (b) an unstaffed "payment kiosk"

somewhere in the restaurant, or (c) a service accessed by using the scanner-equipped e-wallet to read a “pay by wireless” symbol (a 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. The resulting 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).



Figure 1. Paying by barcode at Luigi's.

After these five different payment methods were demonstrated (in counterbalanced order across subjects), we carried out a structured interview beginning with a ranking exercise in which we asked them to specify the payment methods in order of general preference. They were then asked to explain the basis of their rationale. At this point, we were careful not to prompt about trust or security issues in order to see whether any such issues arose spontaneously in their judgements of each of the methods. There then followed a series of questions and rating scales investigating a range of different, more specific issues about the five methods, many questions asking them to contrast and compare different aspects of the systems both in terms of preference, and also in terms of trust and security. Finally, on conclusion of these in-depth discussions, subjects were asked if they wished to change their initial rankings and, if so, why.

All 24 interviews were taped. The data analysis (still in progress) consists of quantitative analysis of rankings and rating scales, plus qualitative analysis and coding of subjects' comments and rationale.

Objectives

In analysing our data, the main objective is to characterise different people's mental models with regard to these systems, and assess the extent to which trust and security plays a role in their reasoning. We will do this in several ways including: cluster analysis on people's ranking of the five systems, assessing which points of vulnerability in these systems people do and do not perceive, assessing the extent to which other factors (such as ease of use, or social issues) impact people's judgements of these systems, and exploring the consistency and rationality of people's reasoning processes.

There are important implications of understanding users' mental models of trustworthiness and security for mobile/ubiquitous computing. First, such an analysis highlights potential barriers to adoption of such systems, whether or not the factors people perceive to be important *actually* reflect real security issues. Second, although it is too early in our analysis to state definite findings, the data we have gathered seems to show that, even unprompted, there are some points of vulnerability which are more salient for users than others. Using this information, we can design systems that, in addition to being inherently and technically more secure, are systems that users *perceive* as more trustworthy.

Having said all this, we recognise that one of the limitations of this study is the extent to which we were able to make Luigi's a convincing and realistic situation for our subjects. As a follow up to this work, we plan to carry out a study based in a real cafe in Bristol in order to better understand those limits and deepen our analysis of the preliminary results.

References

1. Kindberg, T., and Fox, A.: System Software for Ubiquitous Computing. IEEE Pervasive Computing, vol. 1, no. 1 (2002), 70-81.
2. Balfanz, D., Smetters, D.K., Stewart, P., and Wong, H.C.: Talking to strangers: authentication in ad-hoc wireless networks. Network and Distributed System Security Symposium; February 2002.
3. Kindberg, T., and Zhang, K. Validating and Securing Spontaneous Associations between Wireless Devices. Proc. 6th Information Security Conference (ISC'03), October 2003.