Chapter XVI
Trust and Accountability

Sebastian Ries
Technical University of Darmstadt, Germany

ABSTRACT

Ubiquitous computing implies that literally any activity in everyday life can be assisted or accompanied by networked computers. Therefore, the concepts of everyday social life must be carefully reflected on when developing applications for ubiquitous computing. The present chapter focuses on the concepts of trust and accountability. First, both concepts are introduced with their everyday semantics. Second, we explain why trust is relevant for ubiquitous computing, and introduce the main issues for dealing with trust in computer science. Third, we show how accountability can be achieved in distributed systems using reputation and micropayment mechanisms. In both sections, we provide a short overview of the state-of-the-art and give detailed examples for a deeper understanding. Finally, we provide a research outlook, again arguing for the integration of these concepts into future ubiquitous computing applications.

INTRODUCTION

Introduction of the Social Concepts of Trust and Accountability

Trust and accountability are two well-known concepts in everyday life. In real life, trust can serve as the basis for decisions subject to risk and uncertainty, and accountability helps to prevent misuse of common or shared goods. For the introduction of the common meaning of both concepts we refer to the Merriam-Webster Online Dictionary (Merriam-Webster, 2006):

For the definition of **trust** we find among others the following: trust is the "assured reliance on the character, ability, strength, or truth of someone or something," and the "dependence on something future or contingent" (Merriam-Webster, 2006).

Merriam-Webster Online Dictionary defines **accountability** as "the quality or state of being accountable; especially: an obligation or willingness to accept responsibility or to account for one's actions" (Merriam-Webster, 2006).

Relation to Ubiquitous Computing

In Bhargava, Lilien, Rosenthal, and Winslet (2004), Bhargava et al. point out that "trust [...] is pervasive in social systems" and that "socially based paradigms will play a big role in pervasive-computing environments." We believe that the concepts of trust and accountability, which are well-known from real-life experiences, are important and promising enablers for ubiquitous computing.

According to Weiser's vision (Weiser & Brown, 1997), ubiquitous computing will become a *calm technology* with many invisible computers, sometimes called smart devices. Due to the human-centric approach of ubiquitous computing, smart environments are expected to *support the users in everyday tasks and to provide personalized services*, for example, timekeeping or ordering food when the fridge is empty, respecting the user's habits. The devices in such a smart environment will be *heterogeneous* regarding their support for communication channels, storage, user interfaces, and power supply. Therefore, smart devices are expected to complement each other by using the potential of the devices available in the environment. Furthermore, there will not be a well-known infrastructure, which is hosted by only a few service providers. Instead, many users' and providers' smart devices—which can be known or unknown—will share their capabilities with other devices. Therefore, arbitrary devices can act as providers and consumers of information or services, which leads to *highly dynamic collaboration*.

Since ubiquitous computing aims to support users in everyday tasks, applications like the "intelligent fridge," may have legal or financial implications. Therefore, the confidence of users in the capabilities of these applications is an important factor for their acceptance. In the case of trust-aided applications, we believe that the user has to be able to control and to adjust the parameters, which are a basis for decisions in an easy and accessible way. There is the need for helpful user interfaces, which, for example, allow a user to adjust the parameters for trust, to define trust management policies, and to get a survey of their own reputation values or micropayments that have been made.

As ubiquitous computing enforces the interaction of many devices, the user will sometimes not know which devices are interacting in each task. Thus, it is especially important that the user is able to configure which devices are trusted for which contexts and tasks. In addition to trust, accountability can help to enforce responsible usage of shared resources in smart environments, and delimit a possible exploitation of entities participating in those environments.

Lessons to Learn

In the second section, we first explain the notions and properties of trust, and show the prerequisites for successfully transferring it to ubiquitous computing. Furthermore, we introduce the main components for the integration of trust into applications and give a short survey of the state-of-the-art. For a deeper understanding of trust modeling, we present examples of two trust models before we come to the conclusion of the section.

The third section starts with an introduction of the concept of accountability. We subsequently show how reputation and micropayment systems can be used to enforce accountability. For both approaches we provide a classification and a short survey of the state-of-the-art. Finally, we present the conclusion for this chapter.

TRUST

In ubiquitous computing, as in real life, trust can serve as a basis for risky engagements in the presence of uncertainty. It is an interesting challenge to evaluate the trustworthiness of the devices that surround users in ubiquitous computing envi-