Enforcing Trust in Pervasive Computing with Trusted Computing Technology*

Shiqun Li[1,2], Shane Balfe[2,3], Jianying Zhou[2], and Kefei Chen[1]

[1] Dept. of Computer Science and Engineering, Shanghai Jiaotong University
Shanghai 200240, China
{sqli, chen-kf}@cs.sjtu.edu.cn
[2] Institute for Infocomm Research
21 Heng Mui Keng Terrace, Singapore 119613
jyzhou@i2r.a-star.edu.sg
[3] Royal Holloway, University of London
Egham, Surrey, TW20 0EX, United Kingdom
s.balfe@rhul.ac.uk

Abstract. Pervasive computing as a concept holds the promise of simplifying daily life by integrating mobile devices and digital infrastructures into our physical world. These devices in a pervasive environment would establish dynamic ad-hoc networks to provide ubiquitous services. The open and dynamic characteristics of pervasive environments necessitate the requirement for some form of trust assumptions to be made. Trust in this context not only includes authentication, confidentiality and privacy but also includes the belief that the devices and smart environment behave as expected. In this paper, we propose a trust enforced pervasive computing environment using the primitives provided by a TPM (Trusted Platform Module). The application scenario shows how critical information infrastructure such as services and data can be protected. In this smart environment, a person carrying a device authenticates to the environment in order to utilize its services. In this context the device and the smart environment can also test and check each other's behaviors to better perform trust negotiation.

1 Introduction

Pervasive computing as a concept holds the promise of simplifying daily life by integrating mobile devices and digital infrastructures into our physical world. It is envisioned that, in pervasive computing environments, devices carried by people will be able to spontaneously interact with other devices in order to achieve the user's communication, computation and entertainment needs. These devices would be capable of establishing dynamic ad-hoc networks in order to provide ubiquitous services.

* This work is partially supported under NFSC 60273049, 60303026 and 60473020. Both the primary and secondary authors' work was done during their attachment to the Institute for Infocomm Research under its sponsorship.

J. Lopez (Ed.): CRITIS 2006, LNCS 4347, pp. 195–209, 2006.

From a national viewpoint, pervasive computing environment is part of the critical information infrastructure. As the critical information infrastructure protection requested [3], both the infrastructure owners and the individual users of critical infrastructure services expect all services to be constantly available and trustworthy. However, a pervasive environment is an open and dynamic space. The devices and the environments in which they operate may or may not know each other and there may be no pre-configured settings that would aid in the establishment of trust relationships. Moreover, trust is subjective and changeable in these environments. So clearly stated security policies and trust models are needed to convince users (and by extension their devices) and the environments to trust each other. Here trust not only includes authorisation but also includes confidentiality, privacy and the belief that a counterpart behaves as expected.

In this paper, we are concerned with the trust establishment between devices and pervasive environments. By using TPM-enabled platforms and the primitives they provide [24], we propose a trust enforced pervasive computing environment. In this context, a person carrying a (TPM-enabled) device authenticates to an environment allowing them enter a 'smart space' and access its utilities and services. In this regard, the devices and the environment would be assured of each other's behavior is as expected.

The remainder of this paper is organised as follows: Section 2 reviews previous work in the area of trust management and authorisation. Security mechanisms for pervasive computing environments are also reviewed. A brief overview of Trusted Computing technology is given in Section 3. This section also shows how TPM-enabled platforms can be used for trust management in pervasive computing. In Section 4, we propose a trust enforced pervasive computing environment using Trusted Computing technology and briefly discuss the implementation issues of the proposal. Section 5 covers our conclusions and suggests some future research directions.

2 Related Work

Pervasive computing is indicative of devices operating in potentially unknown environments. In this sense there may be no prior trust relationship between either the devices themselves or between the devices and the environment in which they operate. On the other hand, trust is seen a prerequisite for the interaction between devices and environments. So mechanisms and trust models are needed to convince devices that the services provided by the environment are both trusted and trustworthy.

Although trust is important, it is a notoriously difficult concept to define. From a soteriological perspective, trust is what humans use to promote positive interaction and accept risk when partial information is available. McKnight et al. held an intensive survey on trust and defined a cohesive set of conceptual and measurable constructs across several disciplines [18]. They defined trust as the